U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

NUREG/CR-XXXX
ORNL/TM-2008/XX

Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems

Draft

Office of Nuclear Regulatory Research

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Public Electronic Reading Room at http://www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and *Title 10, Energy*, in the Code of *Federal Regulations* may also be purchased from one of these two sources.

1. The Superintendent of Documents
   U.S. Government Printing Office
   Mail Stop SSOP
   Washington, DC 20402–0001
   Internet: bookstore.gpo.gov
   Telephone: 202–512–1800
   Fax: 202–512–2250
2. The National Technical Information Service
   Springfield, VA 22161–0002
   www.ntis.gov
   1–800–553–6847 or, locally, 703–605–6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:
Address: Office of the Chief Information Officer
Reproduction and Distribution
Services Section
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001
E-mail: DISTRIBUTION@nrc.gov
Facsimile: 301–415–2289

Some publications in the NUREG series that are posted at NRC's Web site address http://www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, and transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at–

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852–2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from–

American National Standards Institute
11 West 42nd Street
New York, NY 10036–8002
www.ansi.org

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractor-prepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR-XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

212–642–4900

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

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG/CR-XXXX
ORNL/TM-2008/XX

Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems

Manuscript Completed: December 2008
Date Published: _____

Prepared by:
R. T. Wood (ORNL)
R. Belles (ORNL)
M. S. Cetiner (ORNL)
D. E. Holcomb (ORNL)
K. Korsah (ORNL)
A. S. Loebl (ORNL)
G. T. Mays (ORNL)
M. D. Muhlheim (ORNL)
J. A. Mullens (ORNL)
W. P. Poore III (ORNL)
A. L. Qualls (ORNL)
T. L. Wilson, Jr. (ORNL)
M. E. Waterman (NRC)

Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6010

M. E. Waterman, NRC Project Manager

NRC Job Code N6176

Office of Nuclear Regulatory Research

Draft

This page is intentionally left blank.

Draft

ABSTRACT

This report presents the technical basis for establishing acceptable mitigating strategies that resolve diversity and defense-in-depth (D3) assessment findings and conform to U.S. Nuclear Regulatory Commission (NRC) requirements. The research approach employed to establish appropriate diversity strategies involves investigation of available documentation on D3 methods and experience from nuclear power and nonnuclear industries, capture of expert knowledge and lessons learned, determination of best practices, and assessment of the nature of common-cause failures (CCFs) and compensating diversity attributes.

The principal results of this research effort have identified and developed diversity strategies, which consist of combinations of diversity attributes and their associated criteria. Technology, which corresponds to design diversity, is chosen as the principal system characteristic by which diversity criteria are grouped to form strategies. The rationale for this classification framework involves consideration of the profound impact that technology-focused design diversity provides. Consequently, the diversity usage classification scheme involves three families of strategies: (1) different technologies, (2) different approaches within the same technology, and (3) different architectures within the same technology.

Using this convention, the first diversity usage family, designated Strategy A, is characterized by fundamentally diverse technologies. Strategy A at the system or platform level is illustrated by the example of analog and digital implementations. The second diversity usage family, designated Strategy B, is achieved through the use of distinctly different technologies. Strategy B can be described in terms of different digital technologies, such as the distinct approaches represented by general-purpose microprocessors and field-programmable gate arrays. The third diversity usage family, designated Strategy C, involves the use of variations within a technology. An example of Strategy C involves different digital architectures within the same technology, such as that provided by different microprocessors (e.g., Pentium and Power PC).

The grouping of diversity criteria combinations according to Strategies A, B, and C establishes baseline diversity usage and facilitates a systematic organization of strategic approaches for coping with CCF vulnerabilities. Effectively, these baseline sets of diversity criteria constitute appropriate CCF mitigating strategies for digital safety systems. The strategies represent guidance on acceptable diversity usage and can be applied directly to ensure that CCF vulnerabilities identified through a D3 assessment have been adequately resolved. Additionally, a framework has been generated for capturing practices regarding diversity usage and a tool has been developed for the systematic assessment of the comparative effect of proposed diversity strategies (see Appendix A).

Draft

This page is intentionally left blank.

Draft

FOREWORD

A primary goal of quality assurance processes is to identify and remove errors from a system as soon as the errors are identified, since errors could lead to faults and thereby failures of a function or a system. This is especially important during the development of digital safety systems because an error in the safety system requirements, design, or implementation could result in a failure in redundant channels of the same safety function (i.e., a common cause failure or CCF). However, the likelihood of eliminating every error in a safety system decreases as the size and complexity of the safety system increases. Consequently, NRC regulations require licensees to incorporate diverse functions and systems into a nuclear power plant overall safety strategy to ensure that nuclear power plant abnormal operating occurrences and design basis events do not adversely impact public health and safety.

Guidance for performing diversity and defense-in-depth analyses of safety systems to identify the need for 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* (ML071790509), as well as Branch Technical Position (BTP) 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems" [Chapter 7, "Instrumentation and Controls," of NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants* (ML033580677)]. The deterministic approach described in NUREG/CR-6303, while comprehensive, has been difficult for licensees to apply to ensure (and for the NRC to confirm) that acceptable diversity and defense-in-depth has been identified and implemented in a digital safety system. This conclusion arose as licensees began developing digital safety system upgrades to their existing analog-based safety systems.

Generally, licensees attempted to follow the guidance provided in NUREG/CR-6303; however, resulting analyses typically concluded that of the diversity attributes described in NUREG/CR-6303, only the human diversity attribute and associated criteria could be applied in a manner that resulted in the least amount of regulatory uncertainty. The regulatory uncertainty arose from a lack of regulatory guidance for the NRC staff and the nuclear industry regarding what constituted acceptable combinations of diversity attributes and associated criteria incorporated or added to a safety system for mitigating the effects of CCFs.

The research described in this report does not provide guidance on how to determine the <u>need</u> for diversity in a safety system to mitigate the consequences of potential CCFs. Rather, the scope of this report provides guidance to the staff and nuclear industry <u>after</u> a license or applicant has determined that diversity in a safety system is needed for mitigating the consequences of potential CCFs identified in the evaluation of the safety system design features. Succinctly, the purpose of the research described in this report was to answer the question, "If diversity is required in a safety system to mitigate the consequencess of potential CCFs, how much diversity is enough?"

The guidance provided in this report is in the form of acceptable sets of diversity attributes and associated criteria that complement other design approaches as part of a comprehensive process for confirming that a safety system design appropriately addresses potential CCF vulnerabilities. Further, this report describes a method for quantitatively assessing the amount of diversity in a system to ensure the proposed system acceptably addresses potential CCFs identified during the NUREG/CR-6303 diversity and defense-in-depth evaluation process.

This page is intentionally left blank.

Draft

CONTENTS

Page

ABSTRACT iii
FOREWORD v
LIST OF FIGURES ix
LIST OF TABLES x
EXECUTIVE SUMMARY xi
ACRONYMS xvii
1. INTRODUCTION 1-1
   1.1 Background 1-1
   1.2 Scope of Guidance 1-3
   1.3 Research Approach 1-3
   1.4 Report Organization 1-4
2. COMMON-CAUSE FAILURE VULNERABILITIES AND DIGITAL SAFETY SYSTEMS AT NUCLEAR POWER PLANTS 2-1
   2.1 Common-Cause Failure of I&C Systems 2-1
   2.2 Problem Statement 2-1
      2.2.1 Nature of CCF 2-2
      2.2.2 Response to CCF Vulnerability 2-4
      2.2.3 Impact of Diversity on CCF Vulnerability 2-5
   2.3 Diversity and Defense-in-Depth for Nuclear Power 2-7
      2.3.1 Regulatory Position on Diversity and Defense-in-Depth 2-8
      2.3.2 Diversity and Defense-in-Depth Analysis 2-10
      2.3.3 Diversity for Nuclear Power Plant I&C Systems 2-12
      2.3.4 Diversity Usage Identification 2-17
3. DIVERSITY IN NONNUCLEAR INDUSTRIES 3-1
   3.1 Aerospace Industry 3-1
      3.1.1 Overview 3-1
      3.1.2 Guidance on Diversity Usage 3-2
      3.1.3 Diversity Usage Examples 3-3
   3.2 Aviation Industry 3-7
      3.2.1 Overview 3-7
      3.2.2 Guidance on Diversity Usage 3-8
      3.2.3 Diversity Usage Examples 3-10
   3.3 Chemical Process Industry 3-19
      3.3.1 Overview 3-19
      3.3.2 Guidance on Diversity Usage 3-20
      3.3.3 Diversity Usage Examples 3-22
   3.4 Rail Transportation Industry 3-24
      3.4.1 Overview 3-24
      3.4.2 Guidance on Diversity Usage 3-25
      3.4.3 Diversity Usage Examples 3-26
   3.5 Summary of Nonnuclear Industry Diversity Usage 3-33
4. Diversity Usage in International Nuclear Power Industry 4-1
   4.1 Context for Diversity in Nuclear Power I&C Systems 4-2
      4.1.1 Traditional Application of Diversity for Nuclear Power Plants 4-2
      4.1.2 Architectural Approaches 4-3
   4.2 International Nuclear Power Diversity Strategies 4-6

Draft

4.2.1 Darlington (Canada) 4-6
4.2.2 Sizewell (United Kingdom) 4-9
4.2.3 Chooz B (France)[95] 4-14
4.2.4 Kashiwazaki-Kariwa 6 and 7 (Japan)[100] 4-18
4.2.5 Temelín (Czech Republic) 4-22
4.2.6 Dukovany (Czech Republic) 4-24
4.2.7 Lungmen (Taiwan) 4-27
4.2.8 Olkiluoto-3 (Finland) 4-32
4.3 Summary of Nuclear Power Plant Diversity Usage 4-37
5. INTERNATIONAL CONTRIBUTIONS TO DIVERSITY 5-1
5.1 International Information Exchanges and Technical Meetings 5-1
5.1.1 Multinational Design Evaluation Program Interactions 5-1
5.1.2 International Technical Meetings on Common-Cause Failure 5-2
5.2 British Research on Diverse Software 5-7
5.2.1 General Findings of the DISPO Program 5-7
5.2.2 Practices for Achieving Diversity 5-9
5.3 International Guidance for Coping with Common-Cause Failure 5-13
5.3.1 Common Regulatory Position in Europe 5-13
5.3.2 International Standards 5-16
5.4 Diversity Considerations from the International Nuclear Power Community 5-25
6. DIVERSITY STRATEGIES 6-1
6.1 Usage of Diversity 6-1
6.1.1 Considerations for Assessing Diversity 6-1
6.1.2 Crosscutting Diversity Usage 6-2
6.2 Classification of Diversity Approaches 6-5
6.3 Diversity Strategies 6-6
6.3.1 Strategy A: Fundamentally Diverse Technologies 6-7
6.3.2 Strategy B: Distinct Technology Approaches 6-15
6.3.3 Strategy C: Architectural Variations within a Technology 6-25
6.4 Application of Diversity Strategies 6-38
6.4.1 Strategy Development Summary 6-38
6.4.2 Strategy Evaluation Approach 6-40
7. CONCLUSIONS 7-1
8. REFERENCES 8-1
APPENDIX A EVALUATING DIVERSITY IN SYSTEM DESIGNS A-1
A.1 Diversity Attributes and Criteria A-2
A.2 Information Sources A-5
A.3 Weighting A-6
A.4 Diversity Strategy Evaluation A-12
A.5 Evaluation Tool for Proposed Diversity Strategies A-17
A.6 Conclusions A-22

Draft

LIST OF FIGURES

Figure **Page**

Figure 2.1. Fault management techniques for digital I&C systems. 2-6
Figure 2.2. Representation of I&C system architecture lines of defense. 2-8
Figure 2.3. Assessment approach for satisfying D3 regulatory position. 2-11
Figure 2.4. Diversity attributes and associated criteria derived from NUREG/CR-6303. 2-13
Figure 3.1. Three-tiered architecture for the CDH system on the ISS. 3-6
Figure 3.2. Airbus A320 architecture. 3-11
Figure 3.3. Triple-triple redundancy architecture of the primary flight computer. 3-17
Figure 4.1. Coequal diverse safety systems. 4-4
Figure 4.2. Primary and secondary diverse systems. 4-5
Figure 4.3. Functionally diverse subsystems. 4-6
Figure 4.4. Fully computerized shutdown system. 4-7
Figure 4.5. Functionally diverse subsystems for Sizewell PPS. 4-11
Figure 4.6. SPIN architecture. (Adapted from Ref. 101.) 4-15
Figure 4.7. Overview of Kashiwazaki-Kariwa I&C systems. 4-18
Figure 4.8. Digital safety system at Dukovany Nuclear Power. 4-25
Figure 4.9. Overall architecture of Lungmen I&C systems. 4-27
Figure 4.10. Olkiluoto-3 I&C architecture. 4-32
Figure 5.1. ISTec diversity usage approach for a parallel diverse redundant architecture. 5-3
Figure 5.2. The different facets of diversity and their interdependence. 5-8
Figure 6.1. Baseline diversity strategies: ORNL Strategy A. 5-15
Figure 6.2. Baseline diversity strategies: ORNL Strategy B. 5-25
Figure 6.3. Baseline diversity strategies: ORNL Strategy C. 5-38
Figure A.1. Comparison of diversity strategies A-18

Draft

LIST OF TABLES

Table **Page**

Table ES.1. Overview of baseline diversity strategies xiv
Table 2.1. Diversity usage table[a] 2-18
Table 3.1. Summary of diversity usage for the Space Shuttle 3-4
Table 3.2. Summary of diversity usage for the International Space Station 3-7
Table 3.3. Summary of diversity usage for Airbus A320 3-11
Table 3.4. Summary of diversity usage for Airbus A340 3-13
Table 3.5. Summary of diversity usage for Airbus A380 3-15
Table 3.6. Summary of diversity usage for Boeing 777 3-17
Table 3.7. Summary of diversity usage for chemical process plants 3-22
Table 3.8. Summary of diversity usage for Austrian Federal Railways (Alcatel Austria) 3-27
Table 3.9. Summary of diversity usage for Paris Rail (RATF) 3-29
Table 3.10. Summary of diversity usage for LA Metro Green Line (Ansaldo/UVa) 3-31
Table 3.11. Summary of diversity usage for nonnuclear industries[a] 3-33
Table 4.1. Summary of diversity usage for Darlington 4-8
Table 4.2. Summary of diversity usage for Sizewell 4-12
Table 4.3. Summary of diversity usage for Chooz 4-16
Table 4.4. Summary of diversity usage for Kashiwazaki-Kariwa Units 6 and 7 4-19
Table 4.5. Summary of diversity usage for Temelín 4-23
Table 4.6. Summary of diversity usage for Dukovany 4-26
Table 4.7. Summary of diversity usage for Lungmen 4-29
Table 4.8. Summary of diversity usage for Olkiluoto Unit 3 4-33
Table 4.9. Summary of diversity usage for international NPPs[a] 4-37
Table 5.1. Summary of diversity usage for the ISTec example case 5-4
Table 5.2. Overview of diversity-seeking decisions from U.K. DISPO research 5-10
Table 5.3. Summary of diversity usage from the UK DISPO research findings 5-11
Table 5.4. Summary of diversity usage for the European common position 5-15
Table 5.5. Summary of diversity usage from IEC standards 5-24
Table 5.6. Comparison of diversity usage from international sources[a] 5-26
Table 6.1. Overview of diversities comprising Strategy A 6-14
Table 6.2. Overview of diversities comprising Strategy B 6-24
Table 6.3. Overview of diversities comprising Strategy C 6-37
Table 6.4. Overview of baseline diversity strategies 6-40
Table A.1. Diversity attributes and criteria A-4
Table A.2. Diversity attributes, criteria, ranks, and a diversity strategy examples A-6
Table A.3. DCE weights A-8
Table A.4. Diversity criteria usage and DAE weights A-11
Table A.5. Diversity evaluation worksheet structure A-14
Table A.6. Diversity evaluation worksheet A-19
Table A.7. Worksheet logic A-24
Table A.8. Diversity evaluation worksheet example A-38

Draft

EXECUTIVE SUMMARY

Purpose

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," within Chapter 7, "Instrumentation and Controls," of NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants*. 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. Thus, the NRC Office of Nuclear Regulatory Research (RES) engaged Oak Ridge National Laboratory (ORNL) to develop a technical basis for establishing acceptable mitigating strategies that address the potential for digital CCF vulnerabilities. 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 appropriate mitigating diversity strategies that adequately address potential CCF vulnerabilities in digital safety systems. The strategies are suitable for use by regulatory staff as comparative templates or guides to support confirmation of acceptable diversity usage in addressing CCF vulnerabilities that are identified via a D3 analysis. The purpose of this report is to document the diversity strategies developed through this research and describe the supporting technical basis.

Methods

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, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems* (ML071790509). 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 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 large number and complexity 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 safety assessment tool. Nevertheless, it is possible to define effective diversity strategies based on consensus practices and experience within other application domains.

The research approach employed for this effort began with an investigation of available documentation on diversity approaches and experience from international nuclear power and other

industries. The investigation of best practices for diversity usage focused on industries that employ similar I&C technologies and have high-consequence applications. The findings reported in this document address the aerospace, aviation, chemical process, and rail transportation industries.

For the nuclear power industry, the extensive application of digital technology for I&C systems at international evolutionary nuclear power plants (NPPs) provides a significant resource in determining 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, 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 basis 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 rationale for these strategies centers on best 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 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.

Results

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 have 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 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 and is strongly promoted in the recently issued standard on coping with CCF.[11]

By employing 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.

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 (Laddic logic) 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 a significantly different architectural approach by which to implement strategic use of this technology difference.
- **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 ES.1 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

Table ES.1. Overview of baseline diversity strategies

Diversity attribute	Strategy[a]		
	A	B	C
Design			
Different technologies	x	–	–
Different approach—same technology	–	x	–
Different architectures	i	–	x
Equipment (Manufacturer)			
Different manufacturer—different design	x	x	–
Same manufacturer—different design	–	–	–
Different manufacturer—same design	–	–	x
Same manufacturer—different version	–	–	–
Equipment (Processing)			
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 (Software)			
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 (–).

fundamental difference between systems provides an identifiable, easily recognizable diversity characteristic of system design. Acceptable variants of these three strategies were also developed.

Implementation

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:

- Classify the diversity strategy—identify what technology is employed.
- Confirm inherent diversity credit—ensure that intrinsic benefits of technology differences are not compromised.
- Identify use of intentional diversities explicitly employed to address CCF.
- 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. (Note that the diversity usage tables and diversity assessment tool developed through this research provide support for comparative evaluations against the baseline diversity strategies.)

- 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 prospects 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.

This page is intentionally left blank.

Draft

ACRONYMS

ABWR	advanced boiling-water reactor
ACE	Actuator Control Electronics
ADS	Automatic Depressurization System
AECL	Atomic Energy of Canada, Ltd.
AGR	advanced gas-cooled reactor
AIChE	American Institute of Chemical Engineers
ALARP	As Low As Reasonably Possible
ALU	actuator logic unit
ALWR	advanced light-water reactor
AOO	abnormal operating occurrence
APR	automatic power regulator
APU	acquisition and processing unit
AREMA	American Railway Engineering and Maintenance of Way Association
ARI	Alternate Rod Insertion
ARP	Aerospace Recommended Practice
ASIC	application-specific integrated circuit
ATWS	anticipated transients without scram
AVN	Association Vinçotte Nuclear
B-777	Boeing 777
BFS	Backup Flight System
BNS	Babcock Nuclear Services
BOP	balance-of-plant
BPCS	basic process control system
BTP	Branch Technical Position
C&C	command and control
C&W	caution and warning
CANDU	Canada deuterium-uranium
CCA	Common Cause Analysis
CCF	common-cause failure
CCPS	Center for Chemical Process Safety
CDH	command and data handling
CE	combustion engineering
CENELEC	European Committee for Electrotechnical Standardization
CFR	Code of Federal Regulations
CIM	communication interface module
CMF	common-mode failure
COMTRAC	Computer-Aided Traffic Control
COTS	commercial-off-the-shelf
CP-1	Chicago Pile #1
CPC	core protection calculator
CPLD	complex programmable logic device
CPU	central processing unit
CSA	Canadian Space Agency
CSF	Compagnie Générale de Télégraphie sans Fil
CSIS	Center for Semicustom Integrated Systems
CSN	Nuclear Safety Council
CUW	reactor water cleanup system
D3	diversity and defense-in-depth

Draft

DAE	Diversity Attribute Effectiveness
DAL	Development Assurance Level
DAS	diverse actuation system
DBA	design basis accident
DBE	design basis event
DCE	Diversity Criterion Effectiveness
DCS	distributed control system
DEC	Digital Equipment Corporation
DIS	digital instrumentation system
DISPO	DIverse Software PrOject
DOE	U.S. Department of Energy
DOT	U.S. Department of Transportation
DPS	diverse protection system
DRPS	digital reactor protection system
DS&S	Data Systems and Solutions
DSDs	diversity-seeking decisions
DTMs	digital trip modules
ECCS	emergency core cooling system
ECLSS	Environmental Control and Life Support System
EdF	Électricité de France
ELAC	elevator and aileron computer
EMS	essential multiplexing system
EN	European Norm
EPR	European (or evolutionary) pressurized reactor
EPRI	Electric Power Research Institute
EPS	Electrical Power System
ERA	European Railway Agency
ESA	European Space Agency
ESD	emergency shutdown
ESF	engineered safety feature
ESFAS	engineered safety features actuation system
ESS	emergency shutdown systems
FAA	Federal Aviation Administration
FBW	fly-by-wire
FCPC	Flight Control Primary Computer
FCS	flight control system
FCSC	Flight Control Secondary Computer
FDIR	fault detection, isolation, and recovery
FHA	Functional Hazard Assessment
FMCRD	Fine Motion Control Rod Drive
FMEA	failure mode and effects analysis
FPGA	field-programmable gate array
FRA	Federal Railroad Administration
FTA	Fault Tree Analysis
FWC	feedwater flow control system
GA	General Automation
GDC	general design criteria
GE	General Electric
GEIS	GE Industrial Systems
GNC	Guidance, Navigation, and Control
GPC	general purpose computer

Draft

H&B	Hartmann and Braun
HAL/S	high-order assembly language/shuttle
HBS	hardwired backup system
HIACS	Hitachi Integrated Autonomic Control System
HICS	High-Integrity Control System
HPCF	High-Pressure Core Flooder System
HSE	Health and Safety Executive
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
I/O	input and output
IAEA	International Atomic Energy Agency
IBM	International Business Machine
ICS	Integrated Control System
IEC	International Electrotechnical Commission
IL	integrity level
ILP	interlocking processor
INH	inherent use
INT	intentional use
IP	intellectual property
IPLs	independent protection layers
IPS	Integrated Protection System
IRSN	Institut de Radioprotection et de Sûreté Nucléaire (Institute for Radiological Protection and Nuclear Safety)
ISA	instruction set architecture
ISA	Instrument, System, and Automation Society
ISS	International Space Station
ISTec	Institute for Safety Technology
IV&V	independent verification and validation
JCN	job control number
JEAG	Japan Electric Association Guideline
JNR	Japanese National Railways
KK	Kashiwazaki-Kariwa (Nuclear Power Station)
LBLOCA	large break loss of coolant accident
LOP	Lines of Protection
LWR	light-water reactor
MDEP	Multinational Design Evaluation Program
MHI	Mitsubishi Heavy Industries
MSIV	main steam isolation valve
NASA	National Aeronautics and Space Administration
NASDA	National Space Development Agency of Japan
NEI	Nuclear Energy Institute
NII	Nuclear Installations Inspectorate
NMS	neutron monitoring system
NPL	non-programmable logic
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
O&M	operation and maintenance
OECD/NEA	Organisation for Economic Cooperation and Development/Nuclear Energy Agency
OL-3	Olkiluoto Nuclear Power Station

Draft

ORNL	Oak Ridge National Laboratory
OS	operating system
OSHA	Occupational Safety and Health Administration
PAC	Priority Actuator Control
PAS	Process Automation System
PASS	primary avionics software system
PCS	portable Computer System
PDP	Programmed Data Processor
PERFORM.NET	performance-enhanced redundant fiber optic replicated memory network
PESs	programmable electronic systems
PFC	primary flight computer
PFCS	primary flight control system
pfd	probability of failure on demand
PICS	Plant Information and Control System
PIEs	postulated initiating events
PL/M	program language for microcomputers
PLμS	Programmable Logic Microprocessor System
PLC	programmable logic controller
POL	Problem Oriented Language
PPS	primary protection system
PRA	probabilistic risk assessment
PRIM	PRIMary flight control computer
PRPS	primary reactor protection system
PS	Protection System
PSP	product safety plan
PSSA	Preliminary System Safety Assessment
PWR	pressurized-water reactor
RATP	Régie Autonome des Transports Parisiens (Paris Public Transportation Authority)
RC&IS	rod control and information system
RCIC	reactor core isolation cooling
RCSL	Reactor Control, Surveillance and Limitation System
RER	Réseau Express Régional (Paris Rail)
RES	Office of Nuclear Regulatory Research
RFC	Recirculation Flow Control
RHRS	Residual Heat Removal System
RMU	remote multiplexing unit
RPS	reactor protection system
RPT	reactor pump trip
RSA	Russian Space Agency
RSPP	Railroad Safety Program Plan
RTCA	Radio Technical Commission for Aeronautics
RTIF	Reactor Trip and Isolation Function
RTS	reactor trip system
SAAS	Severe Accidents Automation System
SACEM	Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance
SAE	Society of Automotive Engineers
SAIL	Shuttle Avionics Integration Lab
SAR	safety analysis report
SAS	Safety Automation System
SBP	safety bag processor

Draft

SBPC	Steam Bypass and Pressure Control
SC	Subcommittee
SC-ABFT	safety critical algorithm-based fault tolerance
SCAP	Système de Contournement à l'AtmosPhère (containment atmospheric control system)
SCAT	Systèmes de Commande des Auxiliaires de Tranche (reactor auxiliary systems control)
SDS1	Shutdown System Number 1
SDS2	Shutdown System Number 2
SEC	spoiler and elevator computer
SICS	Safety Information and Control System
SIL	safety integrity level
SIS	high-integrity safety instrumented system
SKI	Statens Kärnkraftinspektion (Swedish Nuclear Power Inspectorate)
SLCS	Standby Liquid Control System
SME	subject matter expert
SNCF	Société Nationale des Chemins de fer Français (French National Railway Company)
SPIN	Système de protection intégré numérique (Integrated Digital Protection System)
SPPA	Siemens Power Plant Automation
SPS	secondary protection system
SRM	staff requirements memorandum
SSA	System Safety Assessment
SSD	safety shutdown systems
SSDE	software development environment
SSLC	System Safety Logic Control
STS	Space Transport System (Space Shuttle)
STUK	Säteilyturvakeskus (Radiation and Nuclear Safety Authority)
SWAP	size, weight, and power
TC	technical committee
TCS	Thermal Control System
TLUs	trip logic units
TMR	triple modular redundant
TOSMAP	Toshiba Microprocessor Aided Power System Control
TXS	AREVA Teleperm XS
U.K.	United Kingdom
UA	acquisition units
UATP	Acquisition and Processing Unit for Protection
UF	functional units
ULS	Logic Safeguard Unit
UPS	uninterruptible power supply
UTPs	logic processors
UVa	University of Virginia
V&V	verification and validation
V_Frame	Vital Framework
VCP	vital coded processor
VME	VERSAbus-E
VVER	Russian-designed water-cooled water-moderated power reactor
WDPF	Westinghouse Distributed Processing Family
WENRA	Western European Nuclear Regulators' Association

Draft

This page is intentionally left blank.

Draft

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. 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. Thus, is the NRC Office of Nuclear Regulatory Research (RES) engaged Oak Ridge National Laboratory (ORNL) to develop a technical basis for establishing acceptable mitigating strategies that address the potential for digital CCF vulnerabilities. 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 appropriate mitigating diversity strategies that adequately address potential CCF vulnerabilities in digital safety systems. The strategies are suitable for use by regulatory staff as comparative templates or guides to support confirmation of acceptable diversity usage in addressing CCF vulnerabilities that are identified via a D3 analysis. The purpose of this report is to document the diversity strategies developed through this research and describe the supporting technical basis.

1.1 Background

NRC regulations require licensees to incorporate into a NPP 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.[1,2] 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. Criterion 21, *Protection system reliability and testability*, requires the capability to withstand any single failure and identifies redundancy and independence as specific design approaches. Criterion 22 addresses the assurance that the safety function will be provided to accommodate the "effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels." 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." Criterion 23, *Protection system failure modes*, specifies that a safe state be achieved in response to failures that may result from adverse environments or other anticipated conditions, such as loss of power. Criterion 24, *Separation of protection and control systems*, invokes separation as a design measure to minimize the prospect of

dependencies that could challenge the reliability, redundancy, and independence requirements of the protection system. Criterion 26, *Reactivity control system redundancy and capability*, requires the provision of two reactivity control systems based on different design principles. Finally, Criterion 29, *Protection against anticipated operational occurrences*, states that protection system designs must provide an "extremely high probability of accomplishing their safety functions" when challenged by AOOs.

As seen above, diversity usage is specifically cited in the design criteria as well as being required by regulation (i.e., the ATWS rule in 10 CFR 50.62). 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 was found to warrant consideration of additional diversity usage to supplement the traditional diversity strategies. Specifically, the NRC staff expressed its concerns about digital safety systems, including potential CCF vulnerabilities, in SECY 91-292, "Digital Computer Systems for Advanced Light-Water Reactors."[4] In item II.Q of SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,"[5] the NRC staff documented a four-point position on D3 that was subsequently modified in the associated staff requirements memorandum (SRM), dated July 21, 1993.[6]

Guidance 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*,[7] as well as in Branch Technical Position (BTP) 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," in Chapter 7, "Instrumentation and Controls," of NUREG-0800, *Standard Review Plan for Review of Safety Analysis Reports for Nuclear Power Plants*.[8] The intent of this regulatory guidance is to provide licensees and the staff a means for assessing whether additional diversity is required in a digital safety system on the basis of the safety system and NPP design features.

NUREG/CR-6303 separated 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 in NUREG/CR-6303 provides a set of recommended criteria for each of the six diversity attributes with several diversity criteria within each attribute. However, because of the number of criteria in each attribute, coupled with the number of attributes, the number and complexity of possible combinations of attributes that could be used to achieve adequate diversity in a safety system make the guidance very difficult to use as a safety assessment tool. As a result, comprehensive guidance and objective acceptance criteria have not been established 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. Primarily, two issues must be addressed: (1) determining how much diversity is required and (2) identifying what combinations of diversity attributes and criteria are most effective in avoiding CCF vulnerabilities. Consequently, the primary purpose of this research described in this report was to resolve these issues by establishing diversity strategies to adequately mitigate the effect of CCF vulnerabilities that are identified through a D3 analysis.

1.2 Scope of Guidance

This document provides the technical basis for strategies that are considered to be effective combinations of diversity criteria in mitigating potential CCF vulnerabilities for digital safety systems. The diversity strategies are presented in terms of a system-to-system comparison, but they are applicable for comparison among diverse redundancies or subsystems as well. The technical basis for the strategies relates to Guideline 2, "Determining Diversity," of the D3 assessment method described in NUREG/CR-6303. The use of these strategies supports confirmation that "adequate diversity has been provided in a design to meet the criteria established by NRC requirements."[9] Specifically, conformance to the strategies developed through this research provides reasonable assurance that the "diverse means" required in Point 3 of the Commission's four-point position on D3[6] is adequately diverse from the affected safety system. Essentially, the diversity strategies provide a basis for comparing proposed diversity usage with acceptable baseline combinations of diversity criteria.

The determination of where diversity is needed within the I&C system architecture of a NPP remains a function of the D3 analysis, which is specifically related to the following guidelines addressed in NUREG/CR-6303: Guideline 10, "Diversity for Anticipated Operational Occurrences;" Guideline 11, "Diversity for Accidents;" and Guideline 12, "Diversity Among Echelons of Defense." These strategies offer guidance on what kinds of diversity and how much diversity is needed to achieve effective combinations of diversity criteria. As a result, the strategies can be used to facilitate determination of whether two blocks (e.g., comparable elements of an I&C system architecture) are sufficiently diverse to justify a conclusion that CCF vulnerabilities, as identified in the D3 analysis, are adequately mitigated. Accordingly, further assessment of a design consistent with Guideline 6, "Postulated Common-Mode Failures of Blocks," of NUREG/CR-6303 can be informed by comparison of proposed diversity usage with that embodied in the strategies developed under this research.

1.3 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. Additionally, a framework has been generated for capturing practices regarding diversity usage and a tool has been developed for the systematic assessment of the comparative effect of proposed diversity strategies (see Appendix A). The research approach employed for this effort involved investigating available documentation on diversity approaches and experience from the international nuclear power industry as well as other industries and organizations, capturing expert knowledge and lessons learned, determining best practices, and assessing the nature of CCFs and compensating diversity attributes.

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), and the Center for Chemical Process Safety (CCPS). 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 nuclear power, the extensive application of digital technology for I&C systems at international evolutionary nuclear power plants (NPPs) provides a significant resource in determining effective strategies for addressing CCF. A focused study of international NPPs was conducted to ascertain distinct diversity approaches for consideration in developing diversity strategies. The study included Sizewell NPP in the United Kingdom, Darlington NPP in Canada, Chooz NPP in France, Temelin and Dukovany NPPs in the Czech Republic, and Kashiwazaki-Kariwa NPP in Japan. Additionally, the D3 strategies being implemented at Lungmen NPP in Taiwan and Olkiluoto NPP in Finland were reviewed.

Where available, standards and guides were identified and reviewed. Additionally, project staff pursued discussions and technical exchange with academic, technical, and regulatory experts for digital I&C applications in the international nuclear community. Based on the findings of this study, groupings of diversity criteria were established to form the core technical basis for the diversity strategies developed under this project.

In summary, diversity strategies derived from analysis of the information collected are presented in the report. Information for this report was obtained through publicly available sources such as published papers and presentations. No proprietary information is represented.

This report presents the findings and observations obtained in the course of the associated research, and such presentation does not indicate NRC endorsement of the designs and methods reported. The foreword to this report provides additional information concerning this subject.

1.4 Report Organization

The report is divided into five major sections: CCF vulnerabilities, nonnuclear industry practices, international nuclear plant experience, recent technical interactions, and diversity strategies. Background information on the nature of CCF, current D3 evaluation practices, and diversity attributes is provided in Chapter 2. Chapter 3 presents the findings from the survey of approaches to address CCF in nonnuclear industries. Chapter 4 describes D3 approaches at selected international evolutionary NPPs. Chapter 5 compiles information on other relevant research activities and results, a new standard from the International Electrotechnical Commission (IEC) on avoiding CCF, and recent domestic and international discussions about diversity approaches. Chapter 6 presents the diversity strategies that have been developed as the primary result of this project. Appendix A describes a method for systematically evaluating diversity strategies using the information gathered from the above sources.

Draft

2. COMMON-CAUSE FAILURE VULNERABILITIES AND DIGITAL SAFETY SYSTEMS AT NUCLEAR POWER PLANTS

2.1 Common-Cause Failure of I&C Systems

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."[10] The 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."[11] 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. Common-mode failure (CMF) is a subset of CCF and occurs when two or more systems or components fail in the same way.

2.2 Problem Statement

Despite the best efforts of designers, developers, implementers, reviewers, testers, suppliers, and assessors, errors happen. The types of failures that can compromise safety-critical functions arise from design mistakes or implementation errors. Failures can also result from undetected internal flaws (i.e., platform faults), system interactions, and external effects. Hazard identification and design measures can minimize the potential for some sources of failure, but unanticipated and untested conditions can still pose a risk. Quality processes detect and correct many implementation errors. However, as design complexity increases, the feasibility of exhaustive testing or comprehensive formal proof diminishes considerably. Therefore, some residual faults may remain undetected and persist as latent faults within the system. Design errors resulting from flawed, incomplete, ambiguous, or misinterpreted requirements are systematic in nature and are significantly more difficult to detect and correct as the system life-cycle phases progress. These faults and errors are, in and of themselves, not a hazard unless conditions (e.g., operational, environmental, relational, or temporal) activate the faulted state and result in a failure of a critical function. Clearly, it is a combination of common latent systematic faults and concurrent triggering conditions that constitutes the primary threat for CCF in otherwise high-quality I&C systems or components.

Any identical or fundamentally similar element of an I&C architecture, system, redundancy (i.e., parallel divisions or channels), subsystem, module, or component that appears in more than one instance or supports more than one system or component is a common element (i.e., replicated and/or shared). Such common elements should be considered to be susceptible to CCF unless compelling evidence (i.e., some adequate combinations of thorough testing, substantial usage history for a comparable application under very similar demands and conditions, extensive formal proofs, detailed hazard/threat analysis, etc.), coupled with sound engineering practices, can acceptably demonstrates otherwise. Again, as design complexity increases, the challenge of providing sufficient evidence to establish reasonable assurance that the potential for CCF vulnerability has been adequately addressed becomes more difficult.

Basically, the issue is that CCF is a credible concern for high-integrity or safety-critical I&C applications that employ complex technologies within complicated system architectures. Both traditional analog-based and more modern digital-based I&C systems are subject to latent systematic faults resulting from design errors or requirements deficiencies. However, because of the complexity of digital I&C systems and the associated inability to execute exhaustive testing, there is increased concern that the potential for latent systematic faults is greater in more fully digital I&C system architectures. In particular, since software (other than the simplest programs) in its coded state or its compiled machine language state cannot be proven to be 100% error free, residual software faults represent a primary CCF

concern. As a result, digital I&C systems receive particular emphasis in assessments of CCF susceptibility and the resulting application of techniques for avoiding or mitigating the potential for CCF vulnerabilities.

The CCF concern is not strictly limited to software-based I&C systems. I&C systems based on conventional analog modules or modern programmable digital devices are also susceptible to CCF. In particular, flawed requirements can be a technology-neutral source of systematic faults that create the potential for CCF vulnerability. In addition to lack of correctness, inconsistency and incompleteness can lead to design errors that propagate through the system development life-cycle process. Other sources of common faults that apply to both analog and digital technology include shared or defective components, fabrication errors, design mistakes, implementation errors, installation errors, operation errors, and maintenance errors. Several mitigation techniques have been developed to address CCF susceptibility for analog applications. These design measures include separation, redundancy, physical barriers, electrical isolation, functional independence, comprehensive (i.e., 100%) testing, and so forth. Signal and functional diversities are particularly well suited to provide some level of protection against requirement flaws.

It is not intended that traditional diversity usage and other design measures that address technology-neutral CCF concerns be supplanted by the diversity strategies developed from this research. Instead, the strategies developed to address the unique characteristics of digital technology and resulting CCF concerns constitute complementary diversity usage that supplements the traditional approaches. Therefore, while the strategies documented in this report focus on coping with potential CCF vulnerabilities associated with digital technology (i.e., programmable devices based on software or complex hardwired logic), these diversity strategies represent one facet of an overall approach to D3.

2.2.1 Nature of CCF

The basis for a CCF occurrence is described in IEC 62340, "Nuclear power plants—Instrumentation and control systems important to safety—Requirements to cope with common cause failure (CCF),"[11] as corresponding to the systematic incorporation of a latent fault in multiple systems or redundancies followed by the triggering of that common fault to cause a coincidental failure of some or all of the systems or redundancies.

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. Obviously, erroneous or misinterpreted functional requirements can lead to flawed system designs.

In the conceptual design and requirements specification phases, sources of faults include incomplete or inconsistent understanding of plant processes, inadequate determination of I&C system performance needs (capabilities, demands, timing, etc.), use of overly complex architectures and complicated system interactions, and deficient allocation of functions among processing components. During the system development phase, traceability of requirements and testability of the design are key factors in minimizing the potential for faults. However, inadequate design specifications can still propagate through even the most rigorous verification and validation process. Additionally the potential for common misinterpretations by designers, testers, and reviewers is not negligible. Again, the more complex the design, the more difficult it becomes to anticipate the potential consequences of intricate functional interrelationships and performance dependencies to address vulnerabilities or to sufficiently identify the range of operational states (including those corresponding to significant rare or faulted conditions) to establish adequate testing.

Some sources of latent faults in the manufacturing, installation, and commissioning phases may arise from inadequate quality control, which can result in flawed fabrication or assembly, erroneous or incomplete installation, inadequate testing, or ineffective configuration control. The impact of human interaction in the operation and maintenance (O&M) phase of the life-cycle can introduce faults due to erroneous operational input or maintenance actions, inadequate configuration control, insufficient quality control on modifications, etc. Other potential sources of common faults during the O&M life-cycle phase correspond to degradation of system performance. These factors can include aging; damage; and erroneous, incomplete, or inadequate modification.

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. Proper training, well-defined procedures, effective interfaces, and administrative controls (e.g., authorization and interlocks, scheduling, change control) can contribute to managing the occurrence of these human-induced triggers.

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."[12] Failures arising from latent faults activated by signal trajectory triggering conditions clearly correspond to conditions that either were not anticipated or properly addressed during system development and that were not exposed through testing. While inputs related to transient conditions in a plant are key elements of the signal trajectory triggering condition, other aspects of digital system performance (and system interactions) must also be considered to fully address this type of triggering condition.

Decoupling system state from plant conditions can be an effective avoidance approach to promote consistent state transitions and more-predictable resource utilization. Additionally, fault management provisions can detect, correct, or tolerate erroneous inputs to constrain the input set. Employing different variables and algorithms to effect similar functions are other means of minimizing signal trajectory commonalities. The use of different (i.e., diverse) platforms, runtime support services, and software implementations can also contribute to discriminating among internal state status and histories.

External events include transient effects, such as anomalies or failures propagating from other systems or components within the I&C system architecture, and environmental stress, such as seismic, vibratory, electromagnetic and electrical surge, and so forth. Controlling the environment where feasible, minimizing interconnections among systems or redundancies, and employing separation with physical barriers and isolation are common means of addressing these triggering conditions.

Temporal effects that can trigger failures include dependence on calendar-date or time-of-day information, synchronization with a common clock, synchronization of processes or systems, and runtime effects dependent on execution cycle histories (e.g., runtime overflows of buffers or stacks). Clearly, avoidance of year, date, and time dependencies is effective. Loose coupling of input sources and receivers and asynchronous execution of processes or functions can help to avoid timing or synchronization triggers. For interconnected systems with digital communications, timing effects arising from communication performance (e.g., delayed messages, lost messages, unexpected messages) must be considered. Periodic reinitialization of systems and software processes (i.e., software rejuvenation) can address software "aging"[13,14] by refreshing execution cycle history and mitigating accumulated pointers, stacks, buffers, etc., to help avoid internal states that could activate faults. Clearly, for safety-critical applications, this reinitialization should occur off-line or in bypass mode to avoid introducing upsets. This approach is becoming common for high-dependability applications in the financial (e.g., online transaction processing systems[15]), the telecommunications,[16] and internet (e.g., web servers[17]) industries. Additionally, staggering restarts for redundancies based on the same or similar platforms can minimize the prospect of concurrent triggering conditions arising from long-term continuous execution.[18]

A rigorous identification of fault types and triggering conditions would support a thorough, systematic evaluation of CCF susceptibilities and allow for comprehensive determination of effective design measures to substantially reduce the CCF potential. Unfortunately, the complexity of the technology and the limited understanding of direct causal effects (especially for human-induced life-cycle-process-initiated faults) challenge the ability of designers and assessors to rely upon such an approach. As a result, more-subjective assessments and best-practice remediation are employed to provide reasonable assurance that adequate CCF mitigation is provided.

2.2.2 Response to CCF Vulnerability

There are many techniques for managing digital I&C system faults that have been employed for high-integrity functions within various application domains. A hierarchy of these techniques is shown in Figure 2.1. They are generally grouped in terms of design evaluation and fault removal, fault tolerance (i.e., detection/masking and recovery), and fault avoidance and mitigation. The techniques indicated involve design approaches, life-cycle actions, technology choices, architectural configurations, and so forth.

Design evaluation and fault removal apply to detailed analyses to identify and eliminate threats to the extent practical, as well as to high-quality processes employed to minimize the potential for faults and remove vulnerabilities as they are discovered. These techniques generally promote fault avoidance at a high level and are primarily oriented toward design approaches and evaluation processes.

Fault tolerance in this hierarchy represents specific techniques for accommodating the presence of faults and avoiding consequent failure. Failsafe designs are enabled by these techniques. Detection and masking relate to identifying the presence of a fault or masking its potential effect (i.e., avoiding failure due to the fault). Diagnostics (e.g., fault identification and isolation) and voted redundancies are common techniques. Recovery relates to the response to an activated fault (i.e., failure) and enables continued execution with recapture of the prefailure state.

Fault avoidance and mitigation include design strategies to impede the propagation of the effects of faults (i.e., failures). Separation, independence, and fault containment are techniques for constraining the potential effects of activated faults, while dissimilarity/diversity and checked redundancy are means for mitigating the effect of activated faults by either precluding common faults (in the first case) or detecting and compensating for activated faults (in the second case).

The fault management techniques described above generally relate to the faults themselves and, to some degree, to the triggering conditions that activate the faults to cause failures. These fault management techniques embody supporting technical and life-cycle methods and approaches on which strategies to cope with CCF vulnerability can be based.

At the outset of I&C system architecture development, design principles are invoked to minimize the use of common elements and to limit failure propagation paths. These design considerations are effective in reducing the potential for CCF susceptibility, but their absolute, across-the-board use can result in extremely complicated, inefficient, and potentially unreliable I&C system architectures. As a result, two principal coping strategies are typically employed in responding to CCF susceptibility: (1) CCF avoidance and (2) CCF mitigation.

The objective of the first strategy is to avoid fault introduction and eliminate potential common triggering conditions to the degree feasible. Comprehensive life-cycle processes with comprehensive hazard identification and extensive verification and validation activities are employed to yield high-quality systems with the goal of approaching error-free software. Nevertheless, experience confirms that undetected errors can progress through even the most rigorous design process. As an additional aspect of the avoidance approach, design measures can be used to reduce the exposure to anticipated triggering

conditions or their concurrent application to multiple systems that may have common faults. Application of such design measures depends upon a well-founded understanding of the types of fault-trigger combinations that may be present and the design conventions that are most effective in preventing concurrent triggering of any common faults that may be present. Examples of these design measures are invariant execution of code and physical separation by barriers into different environmental control zones. However, since there is no assurance that unanticipated common triggering conditions do not exist, use of these measures cannot guarantee sufficient CCF robustness. Thus, the primary goal of this strategy is to minimize the occurrence of common faults and reduce the likelihood of triggered failures.

The objective of the second strategy is to mitigate any vulnerability to CCF through architectural provisions. First, defense-in-depth is employed to compensate for failures in other systems or functions. The IAEA defines defense-in-depth as "the application of more than one protective measure for a given safety objective, such that the objective is achieved even if one of the protective measures fails."[19] In practice, several independent systems are implemented to serve as successive barriers to prevent unsafe consequences from occurring. This aspect of the mitigation approach is especially effective against single failures. However, CCF can potentially disable multiple barriers and result in unsafe conditions. Thus, diversity is employed to provide alternate equivalent functionality or systems that are not susceptible to the same CCF as their counterpart(s) within the I&C system architecture. The difficulty occurs in identifying the full range of fault-trigger combinations that may be present and then selecting the appropriate compensating diversities. Thus, the primary realistic goal of this strategy is to mitigate the vulnerability to CCF by providing alternate or backup functions that are unaffected.

To summarize, a CCF arises when a common fault is present in multiple elements of an I&C system architecture and the occurrence of a triggering condition activates that fault in more than one instance of a CCF-susceptible element to result in a concurrent failure of a critical function. Where vulnerability to a CCF is determined or suspected, the principal responsive approaches are avoidance and mitigation. Since absolute avoidance is not generally provable and comprehensive defense-in-depth could be compromised, the use of compensating approaches to address the residual vulnerability is necessary. Thus, within a given architecture, design decisions are taken that drive the selection among diversities and other design measures.

2.2.3 Impact of Diversity on CCF Vulnerability

The use of diversity as a design measure for coping with CCF vulnerabilities is intended 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. Purpose is embodied in the functional requirements satisfied by a specific system. Process involves the life-cycle activities at each phase of the system lifetime (e.g., design, development, implementation, installation, operation and maintenance). Product consists of the implemented system, including the platform, support services, application software (or complex hardwired logic), interconnections, and distributed elements (e.g., communication nodes, power supplies, sensors, data acquisition and signal conditioning modules, logic elements, actuators). Performance includes the behavior of the system and its response to inputs and external factors or events.

The system aspects of CCF mitigation that are 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 of CCF mitigation 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

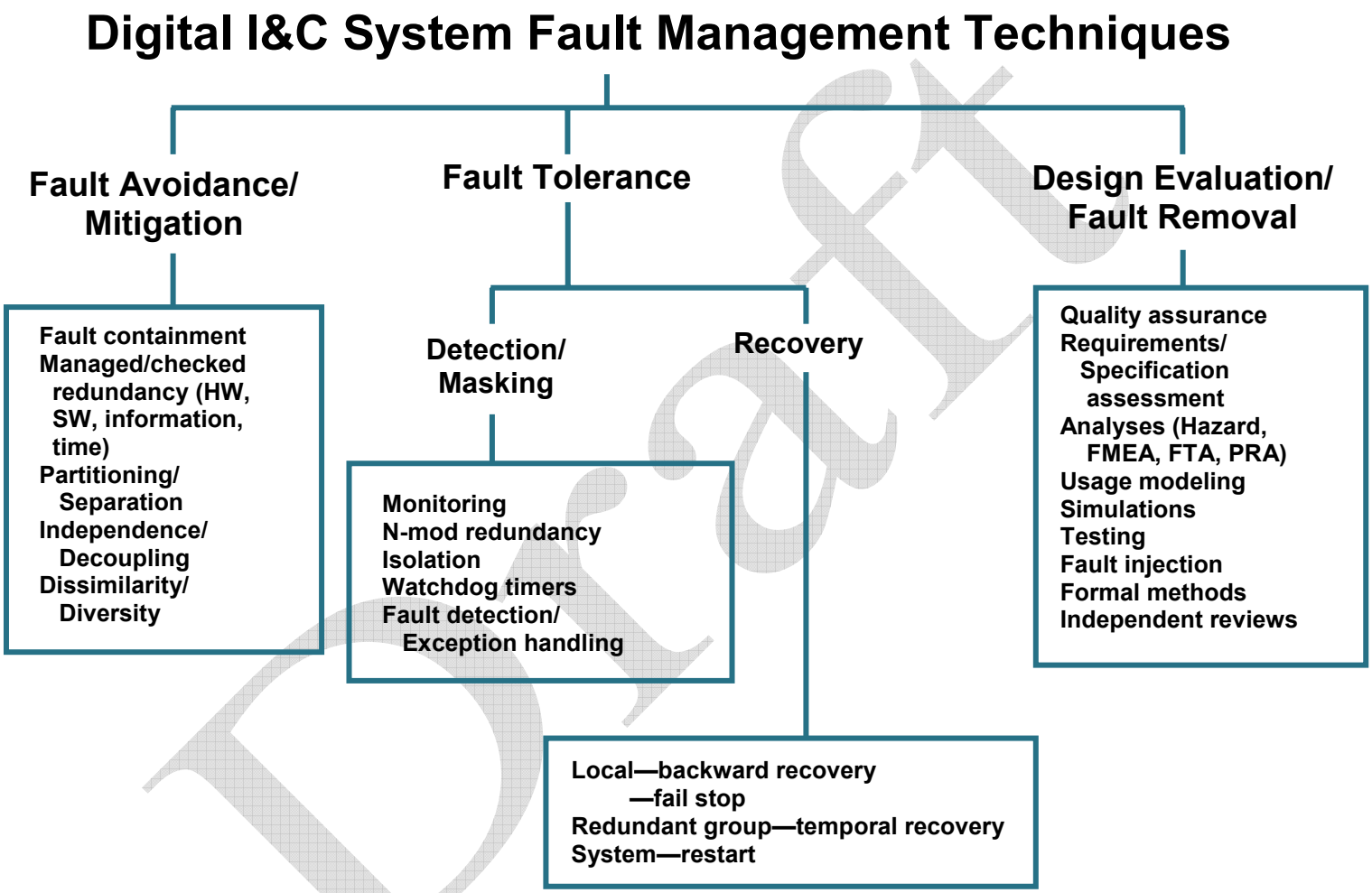

Figure 2.1. Fault management techniques for digital I&C systems.

Draft

software or logic, integrated hardware/software environment, and/or interconnections (e.g., communication, power, structure). The behavioral aspect of CCF mitigation that concerns 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 (e.g., environment or human action) may also serve as triggering mechanisms for common failure.

The impact and benefits of diversity attributes and their associated criteria are identified in terms of common fault sources (purpose and process), location of vulnerabilities (product), and common triggering conditions (performance). Essentially, the effect of each diversity attribute is characterized according to the resultant capability to minimize the introduction of common faults, mitigate the presence of corresponding vulnerabilities, manage commonality in usage (i.e., execution), and reduce similarity in susceptibility to external factors. In the development of rationales for diversity strategies, these diversity effects are expressed in terms of minimized prospects for common systematic faults, reduced occurrence of concurrent execution profiles, and/or lessened likelihood of similar responses to external influences.

2.3 Diversity and Defense-in-Depth for Nuclear Power

The overall I&C system architecture of an NPP embodies the fundamental safety principle that safe conditions must be maintained under all operational conditions (i.e., normal, abnormal, anticipated operational occurrences, and design basis accidents [DBAs]) as a primary objective of its design and implementation.

Defense-in-depth is a well-established approach for the design, construction, and operation of nuclear reactors with a substantial historical basis. It may be visualized in terms of a concentric arrangement of protective barriers or means to ensure public health and safety. Before any harmful radiological release could occur to adversely affect the public or the environment, all of the barriers (i.e., fuel rod cladding, reactor coolant system pressure boundary, containment, and emergency response) must be breached. I&C systems have an important role in maintaining the integrity of these barriers. The application of defense-in-depth to the I&C system architecture of an NPP is accomplished by incorporating independent echelons of defense (or lines of defense). Defense-in-depth for I&C systems provides multiple systems to provide independent means to maintain desired operational conditions, prevent accidents, and ensure adequate protection during adverse events (e.g., failures). The echelons of defense are defined in NUREG/CR-6303 as the control system, the reactor trip system (RTS), the engineered safety features actuation system (ESFAS), and the monitoring and indicator system. The echelons can be considered to act as progressively compensating systems with some overlapping capabilities that collectively achieve the safety objectives of an NPP even if one or more of the systems or echelons fail. The means of accomplishing a safety objective for a specific echelon of defense can involve either avoidance of adverse conditions or mitigation of their effects.

Figure 2.2 illustrates the concept in relation to a general representation of the commonly understood barriers to radiological release. In the figure, Control System, Reactor Protection, and Safety Feature Actuation represent the three automatic echelons. The fourth echelon, the monitoring and indicator system, is incorporated in the Administrative Control line of defense. The two remaining lines of defense, ATWS Protection and Diverse Actuation, represent backup or compensating systems or capabilities that mitigate potential CCF vulnerabilities. These lines of defense may be embedded within a single echelon of defense or may cross echelon boundaries. Similarly, limitation functions, which are designed to intercede to prevent operational disturbances from progressing to the point that protective action is required, may constitute an additional separate line of defense or may be embedded in an echelon of defense, such as the control system. As an example, a separate system is provided in German KONVOI reactors to actively constrain operational conditions and avoid trip conditions[20]

Within the protection echelons of defense (i.e., RTS and ESFAS), I&C systems are designed to withstand single failures to ensure accomplishment of safety functions even in the presence of random failures. The single failure design criterion is generally achieved through the implementation of

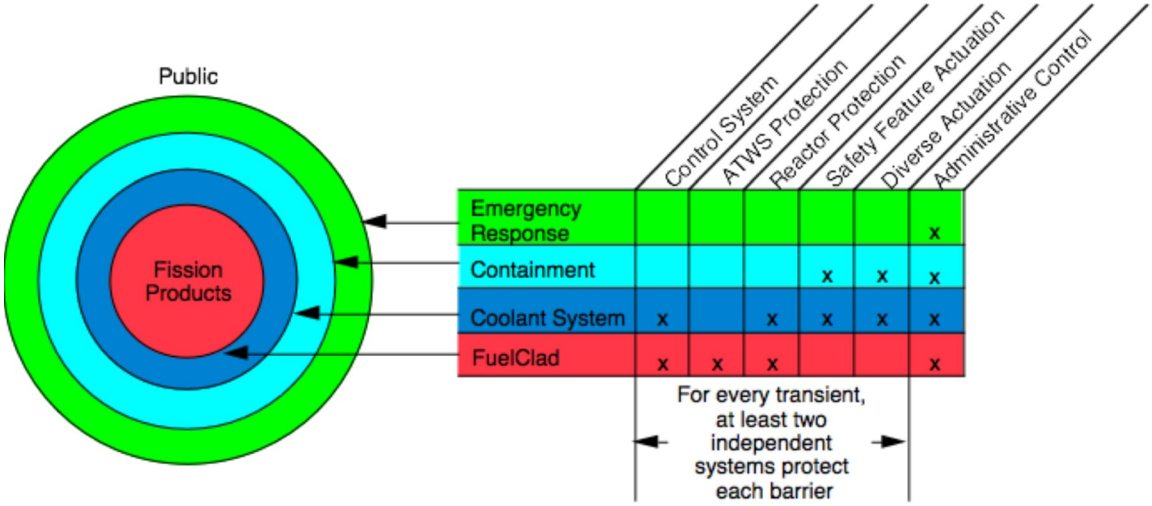

Figure 2.2. Representation of I&C system architecture lines of defense. (*Source*: Gary Johnson, IAEA. Used with permission.)

independent, parallel channels or divisions within a safety system in which redundant safety outputs are voted to determine whether to initiate an appropriate safety action. For these safety systems, functional failure occurs if the output of the voting yields an erroneous result, such as a spurious actuation or failure to act on demand. Thus, functional failures for these systems require multiple redundancies (a voting majority) to fail concurrently in conjunction with a safety demand. This condition corresponds to progression from the occurrence of a fault-trigger combination to a digital failure to a digital CCF if multiple channels within a system fail concurrently due to the common cause (i.e., common faults activated by concurrent triggering conditions). CCFs affecting multiple redundancies or systems within or among echelons of defense constitute the principal credible threat to defeating the defense-in-depth provisions within the I&C system architecture of an NPP.

Diversity is the general approach used for addressing perceived vulnerabilities to CCF of I&C system architectures because dissimilarities in technology, function, implementation, and so forth can mitigate the potential for common faults. Whereas the defense-in-depth approach to ensuring safety employs different functional barriers to compensate for failures in any one or more of the lines of defense, the diversity approach to ensuring safety uses different (i.e., dissimilar) means to accomplish the same or equivalent function, generally within one functional barrier, to compensate for a CCF that disables one or more echelons of defense.

The concept of D3 has been developed by the nuclear power industry to effectively utilize the complementary approaches of D3 to provide a more comprehensive response to the potential for CCF. Regulatory guidance has been developed to provide an assessment methodology for determining the effectiveness of defense-in-depth in the presence of CCF susceptibility and to identify where diversity is needed to mitigate CCF vulnerabilities that are identified in a D3 assessment.

2.3.1 Regulatory Position on Diversity and Defense-in-Depth

As discussed earlier, NRC regulations require licensees to incorporate into an NPP an overall safety strategy for defense-in-depth functions and systems to ensure that AOOs and DBAs do not adversely

impact public health and safety. The basis for these requirements is established in 10 CFR 50.62 and in GDC 22, 24, and 26. 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." Other related design requirements are found in GDC 21, 23, and 29. Additional relevant design criteria are also provided by the incorporation of IEEE Std. 603-1991 and IEEE Std. 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations,"[21] in 10 CFR 50.55a(h).

The NRC regulatory position on D3 is given as Point 18 (Item II.Q) in the SRM on SECY 93-087.[6] The four-point position establishes requirements for addressing the potential for CCF vulnerability. The position points are as follows:

"1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-[cause] failures have been adequately addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-[cause] failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-[cause] failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-[cause] failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above."

As discussed in SECY 93-087,[5] the four-point position on D3 was generated because hardware design errors, software design errors, and software programming errors are credible sources of CCF for digital safety systems. The safety significance of these potential digital CCFs arises from the prospect that architectural redundancy within a safety system could be defeated and more than one echelon of defense-in-depth could be compromised. The position enhances guidance on addressing the potential for CCF vulnerabilities that arise from conventional (i.e., analog) I&C implementations of safety-related functions (e.g., GDC 22, 10 CFR 50.62) by addressing the unique characteristics and concerns related to digital technology while remaining consistent with that guidance. It is noted in the introduction of Appendix A of 10 CFR 50 that "some of the specific design requirements" may require further definition and any perceived "omission does not relieve any applicant from considering these matters" in design to satisfy "the necessary safety requirements." In particular, "the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems" needs to be considered.

It is noted in SECY 93-087 and SECY 91-292 that quality and diversity are principal factors in defending against CCF vulnerabilities. Criteria for ensuring adequate quality are established in Appendix B of 10 CFR 50 and as part of the design criteria provided in IEEE Std. 603-1991 and IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"[22] which is endorsed in Regulatory Guide 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."[23] Criteria for assessing adequate diversity are provided within the review guidance given in BTP 7-19 of the Standard Review Plan (i.e., NUREG-

0800). The objective of BTP 7-19 is to confirm that vulnerabilities to CCFs have been adequately addressed by accomplishing the following:

- verification that "adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements,"
- verification that "adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements," and
- verification that "the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems."

The review guidance in BTP 7-19 expresses the key concern associated with the potential for CCF vulnerability posed by digital technology. Specifically, "[s]oftware cannot typically be proven to be error-free and is therefore considered susceptible to common-cause failures because identical copies of the software are present in redundant channels of safety-related systems." The D3 assessment method documented in NUREG/CR-6303 is cited as acceptable for demonstrating that "vulnerabilities to common-cause failures have been adequately addressed."[9]

The guidance in BTP 7-19 clarifies the treatment of CCF as a beyond-design-basis event. Specifically, the D3 requirements allow for relaxed acceptance criteria compared with the more restrictive treatment of single failures required in analyzing plant response to transients and accidents for the plant design basis. Consistent with Position 2, the effect of a CCF on plant response to design basis events may be determined on a best-estimate, rather than worst-case, basis. Thus, the acceptance criteria described in BTP 7-19 incorporate the use of best-estimate methods for plant response in determining the effectiveness of an I&C system architecture at an NPP as part of a D3 assessment.

2.3.2 Diversity and Defense-in-Depth Analysis

NUREG/CR-6303 provides guidance on performing a D3 assessment to determine the CCF vulnerability of an NPP I&C system architecture. The assessment process is illustrated in Figure 2.3. As a first step in a D3 analysis, a decomposition of the NPP I&C system architecture into a block representation is performed and a determination is made of which blocks are susceptible to a postulated CCF. As defined in NUREG/CR-6303, a block "is the smallest portion of the system under analysis for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment." Examples of typical blocks provided in NUREG/CR-6303 are "computers, local area networks, multiplexers, or PLCs."

The assessment of CCF vulnerability involves identification of common elements, interdependencies (e.g., physical, logical), and diversities. For this analysis, the typical approach is to employ a high-level representation (i.e., coarse granularity) with a black box treatment. This top-down approach is well suited for assessing the potential safety impact of prospective CCF susceptibilities. Diversity attributes are given in Guideline 2 of NUREG/CR-6303 to enable a determination of the CCF susceptibility between blocks.

To support the D3 assessment, Guideline 3 of NUREG/CR-6303 defines the following three system failure types:

I. <u>Type 1 failures</u>
"Type 1 failures happen when a plant transient is induced by the I&C system for which reactor trip or ESF actuation is needed, but may not occur because of an interaction between echelons of defense." Defense against Type 1 failures "depends upon means of accomplishing safety functions that are diverse to the shared signals or equipment."

II. <u>Type 2 failures</u>

Type 2 failures do not cause plant transients directly but constitute a failed capability for a safety action. The failure may remain undetected until environmental effects or physical equipment failure causes a plant transient or DBA to which protective equipment may not respond due to

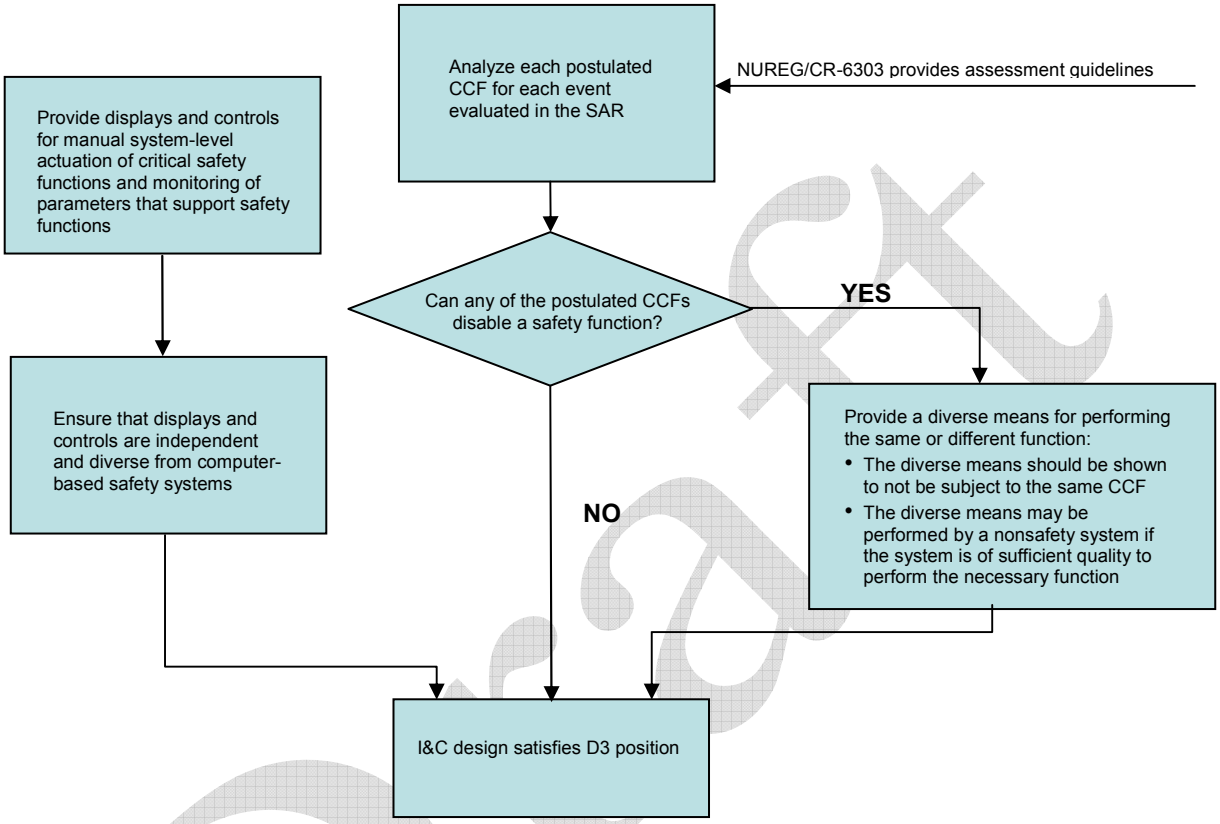

Figure 2.3. Assessment approach for satisfying D3 regulatory position.

CCF of redundant protection system divisions. Defense against Type 2 failures "depends upon some combination of diverse control system, reactor trip system ATWS mitigation equipment, ESFAS, and monitoring and indication functions that are sufficient to mitigate the postulated incident."

III. <u>Type 3 failures</u>
Type 3 failures originate from erroneous output from primary sensors that are expected to respond to a design basis event. Type 3 failures are random in nature, and signal diversity is recommended by NUREG/CR-6303 as a strategy to mitigate this type of failure.

As established in NUREG/CR-6303, assessment of defense-in-depth is performed by postulating concurrent failures of identical (or nondiverse) blocks in all redundant divisions or lines of defense while performing "best-estimate" safety analyses of Chapter 15 events from the plant safety analysis report (SAR). Blocks are to be considered identical when the likelihood of a CCF affecting each of them is not acceptably low. This implies that the probabilities of block failure are not independent and that the probability of system failure cannot be calculated by simply multiplying block failure probabilities. Concurrent failure of each set of identical blocks in all divisions should be postulated in turn (until the list of diverse blocks has been exhausted), and the result of the failure should be documented as a finding of the analysis. If the plant response exceeds specified limits for any AOO or DBA in the presence of

postulated CCF, then a CCF vulnerability exists and corrective action, such as the introduction of additional diversity, should be taken to ensure adequate protection is provided, unless the choice of no corrective action can be otherwise justified.

Diversity may be required to mitigate the effects of anticipated operational occurrences as well as accidents in the case of CCFs of Types 2 and 3. Additionally, diversity among lines of defense may be required to mitigate Type 1 failures. As observed in NUREG/CR-6303, the control system, while not classified as a safety system, still plays an important role in defense-in-depth. Although failures in the control system may challenge the protection system, the control system can mitigate most disturbances without the need for action by the protection system. Furthermore, during an incident in which one of the protection system echelons (reactor trip or ESFAS) fails to perform its safety function due to a CCF, the control system may be able to mitigate the associated disturbance.

Where the D3 assessment determines that additional diversity is needed to mitigate an identified CCF vulnerability of one or more safety functions, that diversity can be achieved through provision of a separate automatic system to back up the affected safety function(s) or through the introduction of intentional diversity and compensating design measures at the appropriate lower level(s) of the I&C system architecture (e.g., system, divisional redundancies, subsystems, modules, or components). If a potential vulnerability is determined, a more detailed evaluation of the CCF susceptibilities and corresponding mitigation approaches can benefit from a block representation with finer granularity than the high-level black box approach. For example, decomposition of a digital system into hierarchical layers (e.g., central processing unit or CPU, operating system, basic service software, application software) can serve to focus consideration of diversity and other design measures by relating relevant types of CCF (i.e., latent systematic faults and failure-triggering conditions) with specific elements susceptible to the occurrence or propagation of a failure.

2.3.3 Diversity for Nuclear Power Plant I&C Systems

NUREG/CR-6303 provides a discussion of six diversity attributes with associated criteria to identify the nature and potential effect of the diversity present. The guidance on the assessment of diversity between blocks involves identification of diversity attributes present, development of a basis to support the diversity claim, and determination of the combined impact of the claimed diversities to establish whether sufficient diversity is provided. In NUREG/CR-6303, each diversity attribute is described and associated criteria are given in order of diminishing impact.

At the heart of mitigation strategies to cope with CCFs are a judicious use of available diversities and an assessment of how each diversity attribute can compensate for CCF vulnerability. The six attributes of diversity defined in NUREG/CR-6303 are as follows:

- design diversity,
- equipment diversity,
- functional diversity,
- human diversity,
- signal diversity, and
- software diversity.

In this report, the “human” diversity attribute is designated the “life-cycle” diversity attribute to account for its true nature and to avoid the erroneous inference that this attribute involves plant operator diversity or human-versus-machine diversity. In fact, the human (i.e., life-cycle) diversity attribute relates to addressing human-induced faults throughout the system development life-cycle process (e.g., mistakes, misinterpretations, errors, configuration failures) and is characterized by dissimilarity in the execution of life-cycle processes. Additionally, the “equipment” diversity attribute is subdivided into two new

attributes to reflect the differences related to the manufactured equipment source (i.e., the manufacturer or supplier) and the differences related to logic processing components (e.g., computational or processing elements such as CPU, printed circuit board, bus architecture for microprocessor-based equipment). Thus, the single "equipment" diversity attribute is treated as two diversity attributes: "equipment manufacturer" and "logic processing equipment." Finally, the "software" diversity attribute is designated the "logic" diversity attribute to account for the different means of representing and executing functions that diverse technologies provide (e.g., software for microprocessors, hardwired logic in programmable devices, electronic circuitry for analog modules).

Figure 2.4 illustrates the diversity attributes and associated criteria defined in NUREG/CR-6303. Additionally, the subsequent descriptions of the attributes and criteria are extracted from NUREG/CR-303. As part of the discussion, indication of the prospective impact on mitigation of digital CCF vulnerabilities that may be provided by each of the diversity attributes is included in italics.

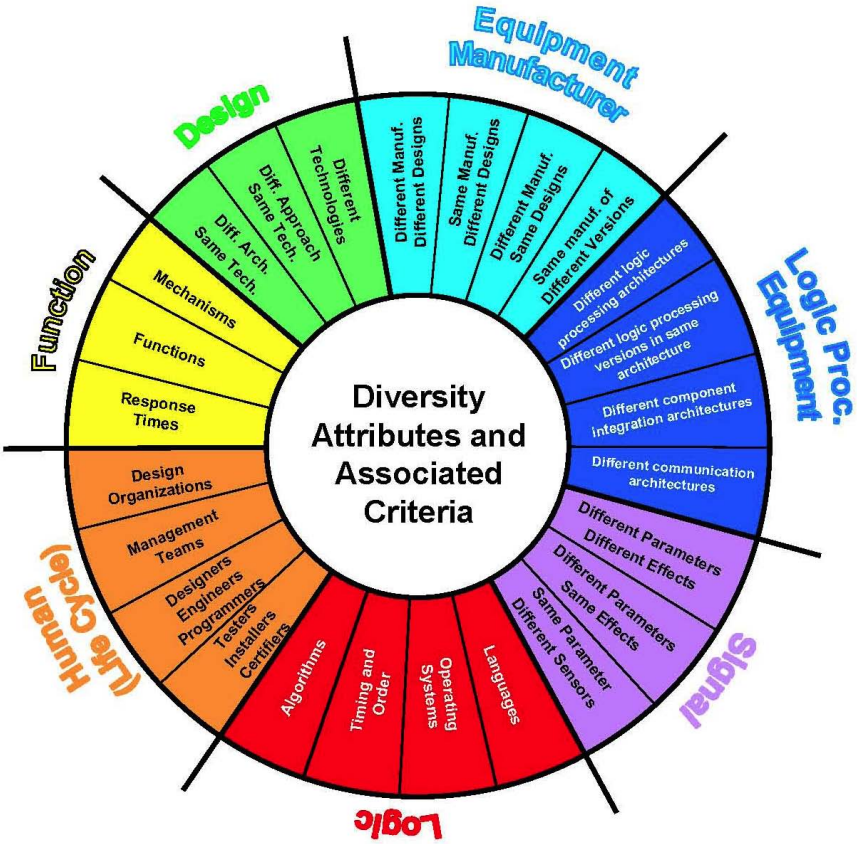

Figure 2.4. Diversity attributes and associated criteria derived from NUREG/CR-6303.

2.3.3.1 Design Diversity

NUREG/CR-6303 defines design diversity as the use of different approaches, including both software and hardware, to solve the same, or a similar, problem. The focus for this diversity is on technology, approach, and architectural differences. Essentially, the design diversity attribute relates to technology choice and usage. For this attribute, NUREG/CR-6303 identifies three diversity criteria (listed in order of effectiveness) that contribute to diversity between two designs that meet the same or similar requirements:

- "different technologies (e.g., analog versus digital)";

- "different approaches within the same technology (e.g., transformer-coupled AC instrumentation versus DC-coupled instrumentation)"; and
- "different architecture (i.e., arrangement and connection of components)."

Design diversity can impact the process, product, and performance aspects of mitigating digital CCF vulnerabilities. The impact on process can be attributed to the prospective effect of technology differences on the sources of systematic faults (e.g., errors) that may arise during the design and implementation of systems. The impact on product can relate to technology-driven differences in the structure and constituent components of systems that may reduce the likelihood of similar architectural locations for vulnerabilities. The impact on performance can involve action, timing, and dynamic response differences that may lead to different execution of function and dissimilar effects from external stress.

2.3.3.2 Equipment (Manufacturer) Diversity

NUREG/CR-6303 identifies four diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to diversity between two groups or items of equipment that perform the same or similar function(s). The focus for these criteria under the general "equipment" diversity attribute is on the source of the hardware components or aggregate system. These criteria are as follows:

- "different manufacturers of fundamentally different designs";
- "same manufacturer of fundamentally different designs";
- "different manufacturers making the same design"; and
- "different versions of the same design."

Equipment manufacturer diversity primarily impacts the process and product aspects of mitigating digital CCF vulnerabilities. The impact on process relates to the prospective effect from use of different resources (e.g., components, manufacturing lines, humans) on the sources of systematic faults (e.g., defects) in the manufacture and supply of systems. The impact on product involves the differences that may arise from the use of different equipment, which may also provide a performance impact via different responses to external influences. At a minimum, equipment manufacturer diversity can reduce potential CCF vulnerability resulting from common or identical equipment.

2.3.3.3 Equipment (Processing) Diversity

NUREG/CR-6303 identifies four diversity attribute criteria (listed in decreasing order of effectiveness) that contribute diversity in the equipment essential to providing logic processing of functions. The focus for these criteria under the general "equipment" diversity attribute is on the type of logic processing equipment employed. These criteria are as follows:

- different logic processing architecture ["different CPU architecture (e.g., Intel 80X86 architecture versus Motorola 68000)"];
- different logic processing version in the same architecture ["different CPU chip versions (e.g., Intel 80386 versus Intel 80486)"];
- different component integration architecture ["different printed circuit board designs"]; and
- different data-flow architecture ["different bus structure (e.g., VME versus Multibus II)"].

Logic processing equipment diversity impacts the process, product, and performance aspects of mitigating digital CCF vulnerabilities. The impact on process can be attributed to the prospective effect of architectural differences for logic processing on the sources of systematic faults (e.g., errors) that may arise during the design and implementation of systems. The impact on product involves susceptibility

differences that may arise from the use of different processing elements or components and from the platform difference that may be present at the macroarchitectural level. The impact on performance is related to dissimilarity in the mechanisms of processing that can lead to differences in execution profiles.

2.3.3.4 Functional Diversity

NUREG/CR-6303 characterizes two systems as being functionally diverse if they perform different physical functions. The IEC defines functional diversity as "application of the diversity at the functional level (for example, to have trip activation on both pressure and temperature limit)."[11] Therefore, there is a significant emphasis on the means of achieving a function and the nature of the function itself. NUREG/CR-6303 identifies three diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to diversity of function between two independent systems:

- "different underlying mechanisms (e.g., gravity convection versus pumped flow, rod insertion versus boron poisoning)";
- "different purpose, function (e.g., normal rod control versus reactor trip rod insertion), control logic, or actuation means"; and
- "different response time scale (e.g., a secondary system may react if accident conditions persist for a time)."

Functional diversity impacts the purpose, process, and performance aspects of mitigating digital CCF vulnerabilities. The impact on purpose clearly relates to differences in objectives, functional relationships, and computational interactions associated with different functions and can help address the potential for common CCF vulnerabilities resulting from flawed requirements. The impact on process can be attributed to the prospective effect of functional requirement differences on the sources of systematic faults (e.g., misunderstandings, mistakes, or errors) that may arise during the design and implementation of systems. The impact on performance can arise from differences in execution profile that can result from the application of different functionality.

2.3.3.5 Life-Cycle Diversity

NUREG/CR-6303 notes that the effect of human beings on the design, development, installation, operation, and maintenance of safety systems can be profound. The focus for the diversity criteria attributed to "human" influence is on life-cycle resources that constitute potential sources of systematic faults. NUREG/CR-6303 also notes that management can significantly affect diversity through resource allocation and cultural effects. Four diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to the diversity achieved throughout the life-cycle of different designs are identified in NUREG/CR-6303:

- different design organizations/companies;
- different engineering management teams within the same company;
- different design and development teams (e.g., designers, engineers, and/or programmers); and
- different implementation and testing teams (e.g., testers, installers, and/or certifiers).*

Life-cycle diversity impacts the process, product, and performance aspects of mitigating digital CCF vulnerabilities. The impact on process involves the prospective effect on potential sources of systematic error due to variations in cognition and action by different personnel engaged in design, implementation, and installation activities. The impact on product may result from the different development approaches, tool and skill sets, and resource (e.g., personnel and/or capabilities) availability that can differentiate

*This category can also include different maintenance technicians.

each implementation. The impact on performance can be attributed to human actions that may act as possible triggering conditions (i.e., unanticipated actions) or potential common in situ fault sources (e.g., maintenance errors).

2.3.3.6 Logic Diversity

NUREG/CR-6303 defines software diversity as "the use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals." In keeping with the more general consideration of different means for processing functions that is available through different technologies, the diversity attribute can be extended to address all forms of logic processing including software program execution. NUREG/CR-6303 identifies four diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to diversity between logic processing approaches adhering to the same requirements. The basis for these criteria excludes the effects of human diversity, which is encompassed in the life-cycle diversity attribute. The logic diversity criteria are as follows:

- "different algorithms, logic, and program architecture" (e.g., computation structure or execution flow);
- "different timing and/or order of execution";
- different runtime environment ["different operating system"]; and
- different functional representation ["different computer languages"].

Logic diversity impacts the process, product, and performance aspects of mitigating digital CCF vulnerabilities. The impact on process can be attributed to the prospective effect of differences in the means and form of functional instantiation on the sources of systematic faults (e.g., mistakes or errors) that may arise during the design and implementation of systems. The impact on product relates to prospective differences in the realization of logic (e.g., program) for each application and in the support services provided by each platform. These differences can reduce the potential for latent faults in common elements that may result in CCF vulnerabilities. The impact on performance includes differences in logic processing mechanisms and functional interactions that can minimize the potential for faulted states to be triggered concurrently due to commonalities in execution profile.

2.3.3.7 Signal Diversity

NUREG/CR-6303 defines signal diversity as the "use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly." In this sense, signal diversity is related to functional diversity, with one providing diverse indication and the other capturing the different functional relationships between indication and event. NUREG/CR-6303 identifies three diversity attribute criteria (listed in decreasing order of effectiveness) that contribute to diversity between measurement sources:

- "different reactor or process parameters sensed by different physical effects (e.g., pressure or neutron flux)";
- "different reactor or process parameters sensed by the same physical effect (e.g., pressure versus water level or flow sensed by differential pressure sensors)"; and
- "the same reactor or process parameter sensed by a different redundant set of similar sensors (e.g., a set of four redundant temperature sensors backed up by an additional set of four redundant temperature sensors driving a diverse design of protective equipment)."

Signal diversity impacts the purpose and performance aspects of mitigating digital CCF vulnerabilities. The impact on purpose can arise from the availability of diverse indicators for initiation of protective

action, coupled with the associated diverse underlying functional relationships, and can help address the potential for common CCF vulnerabilities due to flawed requirements. The impact on performance relates to differences in execution profile that can result from the presentation of different signal trajectories to diverse systems. An impact on product is also provided in the sense that different sensors are generally involved in achieving signal diversity.

2.3.4 Diversity Usage Identification

The effective application of appropriate combinations of the diversity attributes and associated criteria described above can mitigate the potential adverse effects arising from CCF vulnerability. The development of diversity strategies through this research depends upon determination of what constitutes acceptable combinations of those attributes and criteria. As part of the research effort, best practices and relevant experience on the use of diversity by nonnuclear industries and the international nuclear power community have been investigated. Chapters 3 and 4 present the findings of that investigation. To enhance the presentation of those findings and enable a systematic evaluation of the experience base, diversity usage tables were generated to capture the information. Table 2.1 provides a template for the tables that appear in subsequent chapters. These tables not only provide a means to document diversity usage but also encourage translation of each diversity approach into the terminology and categories established in NUREG/CR-6303, Guideline 2. The template for these diversity usage tables also provides a means for capturing proposed diversity strategies as an evaluation aid. The tables allow for direct comparison against the baseline strategies developed in this research (see Chapter 6).

Draft

Table 2.1. Diversity usage table[a]

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

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

Draft

3. DIVERSITY IN NONNUCLEAR INDUSTRIES

Within high-value, high-integrity, and safety-significant industries, failure avoidance and mitigation approaches are ubiquitously employed to decrease the likelihood of I&C system failure. These nonnuclear, high-failure-consequence industries, which employ similar I&C applications, have almost completely transitioned to digital technology. The experience and best practices of these other industries can serve as useful examples to the U.S. nuclear power industry regarding the diversity usage within digital I&C system architectures. Relevant experience and best practices for avoiding CCF within digital systems for the aerospace, aviation, chemical process, and rail transportation industries are assembled and evaluated in this chapter in terms of their relevance to nuclear power generation.

None of the other high-consequence industries is directly analogous to the nuclear power industry. Both inherent technical and regulatory oversight differences need to be considered in transferring the CCF mitigation lessons of other industries to the nuclear power domain. For example, flight control systems within the aviation industry typically do not have a readily accessible safe shutdown state, have short-term potential catastrophic control trajectories, and make frequent significant adjustments to control elements. These inherent characteristics make the requirements for probability of failure on demand more stringent for aviation than nuclear power generation. Size, weight, and power (SWAP) represent significant constraints in some of the nonnuclear application domains investigated. Not only must the prospective impact on feasibility, cost effectiveness and risk burden be considered, but a real potential exists for safety compromised if systems are too large, heavy, or consume too much power. Additionally, the nuclear power industry has significantly greater regulatory oversight (particularly in terms of prior approval of system changes) than comparable high-failure-consequence industries. Thus, economic factors such as cost, efficiency, and investment protection may have more impact on design and implementation strategies for the less comprehensively regulated industries. The differences in domain context and the nature of the safety-critical applications must be considered in evaluating the diversity usage observed in the cited example cases from these other industries.

Several industries were investigated as part of this research. Many were found to rely primarily on high-quality processes and rigorous hazard identification and resolution. However, 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. The findings from these industries are presented in this chapter.

3.1 Aerospace Industry

3.1.1 Overview

The U.S. government aerospace organization is the National Aeronautics and Space Administration (NASA). NASA performs scientific investigation and exploration of space through manned and robotic missions. It is organized into four principal mission directorates:[24]

- Aeronautics—developing and maturing flight technologies to improve exploration capabilities and enhance terrestrial applications,
- Exploration Systems—creating new capabilities and spacecraft to enable affordable, sustainable human and robotic exploration,
- Science—promoting discovery through exploration of the Earth, moon, Mars, and beyond, and
- Space Operations—providing critical enabling technologies to support the NASA mission via the space shuttle, the International Space Station (ISS), and other forms of flight support.

With such diverse applications, I&C architectures and requirements for NASA spacecraft vary considerably. This investigation focused on safety-critical applications for manned space operations, with an emphasis on the I&C architectures of the space shuttle and the ISS.

Although the flight control and life support systems for manned spacecraft and space stations share a common goal with safety systems of NPPs (namely, protecting human life and health), the nature of the safety-critical applications for the two domains are remarkably different. First, space systems face a size, weight, and power constraint that limits the equipment and distance spacing that can be employed. For example, alternate sensors or actuators may not be feasible and cable separation may be restricted. Also, shielding of electronics from radiation exposure is limited in space applications because of weight and the application environment.

Another distinction arises from the nature of the applications and the demand profile placed on the I&C systems. Flight control involves continuous action and varied (almost unconstrained) conditions whereas NPP safety involves rare action and generally well-characterized events. Given the nature of the functions, it is normally readily apparent to the astronauts when the flight control system is not functioning. Conversely, safety system action is generally uncommon so a failure to actuate may not be detected by the plant operators until a design basis event has progressed appreciably. Clearly, the absence of expected action is much more discernable than that of an unusual action. Additionally, NPPs generally have a well-defined, readily achievable safe state (i.e., shutdown) based on discrete, fast-acting or limited duration safety system responses to events whereas spacecraft flight control systems must continue to actively function for an extended period of time (throughout the mission), especially for dynamic flight phases that do not have an abort option.

The duration of manned spacecraft missions is very short (e.g., days) compared to the long operational cycle of power plants. In this sense, the ISS context is closer to that of a power plant given the sustained operation of years. The point is that intervals in which the spacecraft may be at risk to the consequences of CCF are much shorter than for NPP operation. Additionally, the time period between the prospective occurrence of a CCF and opportunities for detection and response (e.g., maintenance) is likely to be much shorter for active systems, such a flight control, applied to short duration missions.

Obviously, the context for safety-critical I&C systems in space applications is considerably different than for safety systems in NPPs. Thus, the aerospace approach to addressing the potential for CCF vulnerabilities accommodates different concerns and may not be directly applicable in the NPP context. Nevertheless, insights into strategic considerations for diversity usage are available.

3.1.2 Guidance on Diversity Usage

NASA requires CCFs to be "considered" and "assessed," but diversity is not explicitly required. The NASA Safety Manual[25] more specifically addresses redundancy as a means to achieve fault tolerance. The level of protection required is a function of the hazard severity and probability, and may be achieved by a combination of availability, reliability, maintainability (restorability), and redundancy. Use of redundancy to achieve failure tolerance requires specification of acceptable reliability and provision of sufficient redundancy to tolerate two failures or operator errors where loss of life or mission failure could occur and tolerate one failure or operator error (failsafe) where system loss/damage or personal injury could occur. Where there is sufficient time between the occurrence of a failure and the manifestation of its effect, failure tolerance can be achieved through design enabling restoration to safe operation based on ("hot" or "cold") spares, operational procedures, or maintenance. Where there is not sufficient time for recovery, functional redundancy must be provided. Functional redundancy is defined as "situation where a dissimilar device provides safety backup rather than relying on multiple identical devices."[25] Nevertheless, the use of redundancy to achieve failure tolerance requires verification that any assumption of failure independence is not invalidated by CCFs.

The NASA Software Safety Standard[26] states that non-safety critical and safety-critical software may reside on the same processor, although design provision must ensure that the safety-critical function cannot be disabled or impaired. Software within a safety-critical system is generally presumed to be safety critical and is treated accordingly. If non-safety critical software resides in the same system (i.e., on the same processor) with safety-critical software, the partition or isolation method is treated as safety-critical, but the isolated non-safety code is not. This requirement on the treatment of software is particularly important for the incorporation of commercial-off-the-shelf (COTS) software. Software design and code implementation may not compromise any safety controls or processes, cannot create any additional undocumented or unresolved hazards, and must maintain the system in a safe state during all modes of operation. Catastrophic hazards must be able to tolerate two hazard control failures (two fault tolerant) while critical hazards must be able to tolerate a single hazard control failure (single fault tolerant).[25,27]

Human-rated systems require an assessment of CCF vulnerabilities and manual override capability. Human-Rating Requirements for Space Systems[28] requires that flight software shall, at a minimum, be tested using a flight-equivalent avionics test-bed operating in a real-time. Space systems are required to be designed so that no two failures result in crew or passenger fatality or permanent disability. The space system relies upon operators as a diverse control system by requiring the crew (and ground control) to have the capability to manually override higher-level software. The space system is also required to provide the capability for autonomous operation of critical functions. The crew (and ground control) can initiate, override, or abort automatic initiation sequences. As a defense against CCFs, use of dissimilar redundancy or backups is required to be assessed. Dissimilar redundancy can be characterized in terms of "additional functional capability (hardware and associated software) to provide at least two [different] means of performing the same task."[29]

3.1.3 Diversity Usage Examples

Beyond the adherence to rigorous quality assurance practices, redundancy, fault tolerance, and backup use of human operators are NASA's primary means for achieving highly reliable systems. Mission control and the ISS use a "law of large numbers" type approach; if one system/computer fails, there are still many computers available for control. 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. The command and control architecture for manned missions uses commercially available software and hardware. "Fault protection" software routines provide the ability to recover from failures.

The flight control system of the space shuttle or Space Transport System (STS) and the station command and data handling (CDH) system of the ISS provide prominent examples of safety-critical I&C applications for human-rated space missions. These systems provide the most relevant cases of diversity usage by NASA.

3.1.3.1 Space Shuttle

Prior to the Space Shuttle, manned spacecraft computers were programmed at the machine level using assembly language. The delays and expense of the Apollo software development, along with the realization that the Shuttle software would be many times as complex, led NASA to encourage the development of a language that would be optimal for real-time computing. The result was HAL/S (or high-order assembly language/shuttle). IBM developed the primary avionics software system (PASS), which is the principal software used to operate the space shuttle during a mission using the HAL/S language. The PASS software is priority-interrupt-driven, or asynchronous—it performs computations on demand and in strict observance to a predefined order of importance.[30]

PASS is a quadruple redundant avionics system that is implemented on IBM AP-101S general purpose computers (GPCs). A fifth GPC is provided on board the Shuttle as a spare. The functional design for PASS is based on fail operational/failsafe principles. The four GPCs are synchronized at every process initiation and each subsequent input and output (I/O) action. All vital sensors are quadruple redundant as well but the input data for each GPC is equalized using median selection with threshold monitoring. The operational approach is to require agreement among the output of all four active PASS computers. If disagreement is detected, the spare PASS computer can be engaged. As previously noted, the application code was implemented using HAL/S. The priority-driven operating system (OS) was written in assembly language. As is its practice, NASA used an independent verification and validation (IV&V) team to enhance its software quality assurance. [31,32]

To protect against the prospect of a latent programming error in the PASS software that could render the Space Shuttle uncontrollable during a critical flight phase, NASA contracted with Rockwell and Intermetrics to develop a backup flight system (BFS). This system has its own set of requirements based on reduced functionality flight control laws. In addition, programmers could not reuse any of the code developed for PASS. Nevertheless, like IBM, Rockwell elected to use HAL/S as the programming language. A cyclical time-slice OS was developed for the BFS.[30] The BFS is implemented on a sixth IBM AP-101S computer. The BFS also contributes to the output comparison among the PASS computers. It also serves as the reduced functionality backup during critical flight stages should failure of the PASS be detected.[31,32] Table 3.1 provides a summary of diversity usage for the Space Shuttle.

The philosophy taken for the BFS was to develop a very simple and straightforward software program and then exhaustively test it. The result was a program that contained only 12,000 words of executable instructions, including the ground checkout and built-in test for the computer. The actual flight control portion of the software consisted of approximately 6,000 words. The remainder of the code was for the systems management functions.[33,34]

Table 3.1. Summary of diversity usage for the Space Shuttle

Diversity attribute	Usage[a]	Details
Design		
Equipment (Manufacturer)		
Different manufacturer—same design	–	All computers are the same (IBM AP-101S)
Equipment (Processing)		
Functional		
Different purpose, function, control logic, or actuation means	x	Primary flight control (PASS) vs reduced functionality backup flight control (BFS)
Life-cycle		
Different design organizations/companies	x	IBM developed PASS application software while Intermetrics and Rockwell developed the BFS
Different design/development teams (designers, engineers, programmers)	i	IBM vs Intermetrics/Rockwell
Different implementation/validation teams (testers, installers, or certification personnel)	i	IBM vs Rockwell; Used Shuttle Avionics Integration Lab (SAIL at JSC); Also NASA IV&V organizations involved

Table 3.1 (continued)

Diversity attribute	Usage[a]	Details
Logic (Software)		
Different algorithms, logic, and program architecture	x	Limited functions for BFS (minimal flight control for critical stages)
Different runtime environment	x	PASS uses priority-driven OS while BFS uses cyclical time-slice OS
Different functional representation	–	HAL/S for PASS and BFS
Signal		
Same parameter sensed by a different redundant set of similar sensors	x	Quadruple redundant sensors but equalized (cross-validation) to give identical inputs
Other Diversity Considerations		
Parallel Redundant-Checking architecture; Diverse (reduced) functional requirements; Size, weight, and power constraints	Matched computers, inputs, programs for exact comparison; Reduced functionality backup can be invoked on primary system failure (manual selection on alarm)	

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

Two CCFs of the digital I&C have been identified in operation for the Space Shuttle. During a mission, solder shorted out some CPU boards, causing two control computers to crash. Another CCF mode was discovered during simulator testing when crewmembers discovered that all four control computers locked up when executing an abort sequence. The cause was a counter that did not reset during interrupts. This fault in turn caused the code to encounter values outside the expected range for some variables that resulted in an erroneous branch to an untested execution path. [35]

3.1.3.2 International Space Station

The ISS is a cooperative endeavor among NASA, the Russian Space Agency (RSA), the Canadian Space Agency (CSA), the National Space Development Agency of Japan (NASDA), and the European Space Agency (ESA). Over 100 separate computers provide data collection, processing, communication, and control functions for the ISS. The primary station management system is the Command and Data Handling (CDH) system. Boeing provided the CDH system as the prime contractor/supplier to NASA.

The function of the CDH system is to provide command and control of the ISS. The CDH system is implemented in a three-tiered architecture of 25 computers, which are based on Intel 80386SX CPUs. These computers are interconnected by data buses and are accessed by the ISS crew via IBM Thinkpad 760XD laptops.[36]

Figure 3.1 illustrated the hierarchy of the CDH system. Tier 1 (or the control tier) consists of the Command and Control (C&C) computers, which serve as the ISS station-wide control system and interface access point for the ISS crew through the PCS. Tier 2 (or the local tier) consists of subsystem level functions for the Electrical Power System (EPS), Guidance, Navigation, and Control (GNC) system, Environmental Control and Life Support System (ECLSS), and Thermal Control System (TCS). The purpose of the Tier 2 computers is to execute system-specific application software. Tier 3 (or the user tier) computers provide the direct interface for sense and control components (i.e., the sensors and effectors/actuators).[36]

As indicated in the figure, information flow involves command proceeding down the hierarchy and telemetry (or data) proceeding up the hierarchy. Thus, the station level (Tier 1) C&C computers initiate a command, which proceeds through the subsystem level (Tier 2) to the equipment level (Tier 3) for

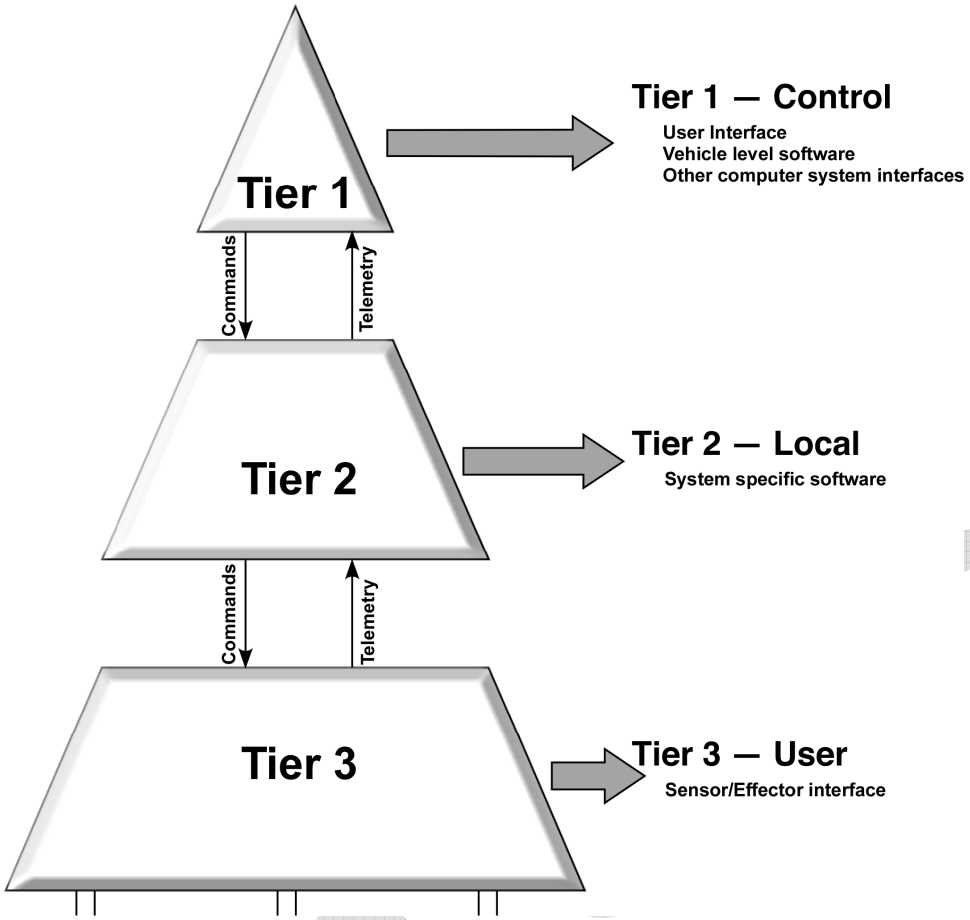

Figure 3.1. Three-tiered architecture for the CDH system on the ISS. (Adapted from Ref. 36.)

actuation. As noted, the ISS crew interfaces the system at the control tier. Direct interaction with the lower tiers is not provided. Data queries and commands must proceed through the hierarchy. [37]

The three Tier 1 computers are configured to be triple redundant to provide two-fault tolerance. The redundancy is implemented such that one computer is operational, another is a "warm" backup, and the third is powered off in "cold standby. There are five pairs of dual redundant Tier 2 computers, with the second computer in each pair powered off for cold standby (except for the GNC pair in which a "warm" backup is provided) to provide single fault tolerance. The twelve Tier 3 computers are not generally implemented in a redundant configuration although some software redundancy is provided through duplicate functions or component interfaces. [36]

Software for the CDH computers is written in Ada and includes Caution and Warning (C&W) capabilities at each level. The primary functionality implemented in each computer can be characterized as telemetry, commands, time synchronization, and fault detection, isolation, and recovery (FDIR). The FDIR functions address the computer and the data bus. Table 3.2 provides a summary of diversity usage for the ISS.[37]

On April 25, 2001, an independent computer failure coupled with a common-cause failure of the other two first level control (Tier 1) computers resulted in the failure of all three C&C computers on board the ISS.[38] More specifically, the three Tier 1 computers failed a few days after a new software packages was installed. The Tier 2 and 3 computers continued operating to keep many basic functions, such as the primary life support systems, in operation. The Tier 2 computers activated a reduced functionality failsafe mode that triggered backup functions and issued a reboot demand to the Tier 1

Table 3.2. Summary of diversity usage for the International Space Station

Diversity attribute	Usage[a]	Details
Design		
Equipment (Manufacturer)		
Equipment (Processing)		
Different logic processing architecture	–	All computers based on Intel 80386SX
Functional		
Different purpose, function, control logic, or actuation means	x	Defense-in-Depth provided through hierarchical distribution of diverse functionality; Tier 2 computers provided recovery function to reboot Tier 1 computers; Tier 1 for station functions vs Tier 2 for system/module functions
Life-cycle		
Logic (Software)		
Different algorithms, logic, and program architecture	x	Fault recovery logic embedded in Tier 2 program to respond to Tier 1 failure
Different functional representation	–	All software written in Ada
Signal		
Other Diversity Considerations		
Tiered architecture with hierarchically distributed Redundant-Checking computers; Diverse (fault detection/recovery) functional requirements; Size and power constraints	Lower tier computers detect and respond to higher tier computer upsets (request/demand reboot)	

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

computers. Subsequently, one of the disabled computers came back on line. Analysts uncovered an error in the software load that was believed to be the source of the problem.[39]

3.2 Aviation Industry

3.2.1 Overview

The civil aviation industry[*] within the United States is regulated by the Federal Aviation Administration (FAA) under the U.S. Department of Transportation (DOT). The FAA's major roles include the following:[40]

- regulating civil aviation to promote safety;
- encouraging and developing civil aeronautics, including new aviation technology;
- developing and operating a system of air traffic control and navigation for both civil and military aircraft;
- researching and developing the National Airspace System and civil aeronautics;

[*]Civil aviation is one of two major flight categories and it encompasses all non-military flight, both private and commercial.

- developing and carrying out programs to control aircraft noise and other environmental effects of civil aviation; and
- regulating U.S. commercial space transportation.

All parts of the aircraft are subject to system safety analyses. Regarding avionics, methods for analyzing the safety impacts of a system are specified by the FAA. Aircraft avionics includes all systems that enable the aircraft to fly safely or have direct control over the aircraft (i.e., high-integrity or safety-critical systems), as well as equipment that supports those systems. All equipment fitted to aircraft has to meet a series of rigorous design constraints. Airworthiness determination and certification is one of the most costly, time-consuming, and difficult aspects of building any aircraft.[41] As aircraft and aircrew reliance on digital flight control systems has become more prevalent, the safety implications posed by the reliability of these avionics systems has increased. One necessary factor of constructing avionics systems is that a flight control system (FCS) must be designed so that it avoids systematic faults and tolerates single failures. High reliability requirements are part of every aircraft system.

The technology upon which avionics systems are based has progressed markedly from mechanical and hydraulic FCSs. The early systems were both heavy and required careful routing of flight control cables through the airplane using systems of pulley and cranks. Today's fly-by-wire (FBW) control systems use computers and electrical linkages, saving weight while demonstrably improving reliability. As greater confidence and experience are gained with digital FBW control systems, reliance on manual control backups based on diverse physical flight systems (e.g., mechanical and hydraulic linkages and pneumatic instrument displays) is diminishing. The cockpit of the Airbus 380 is an example of modern aviation electronics and controls in which automatic electronic control systems provide primary and backup flight control capabilities.

The FCS represents the one of most significant high-integrity systems since it provides command and control for the primary flight control surfaces of the aircraft and its proper functioning is essential for commercial airliner flight. In fact, a failure rate better than 10^{-9} per hour is required for flight-critical avionics.[42] Given the safety-critical nature of an aircraft's FCS, it is seen to be similar in significance to safety systems at NPPs. However, just as is the case for spacecraft flight systems, there are several considerations that differentiate the treatment of the two systems. A size and weight constraint is present for avionics systems, and the demand profile is significantly different (continuous vs rare, unconstrained vs well defined, easily observed vs potentially undetectable, etc.). Thus, while insight into the treatment and value of diversity attributes may be gained from evaluating its use in this application domain, the directly applicability of these practices to nuclear power safety may be limited.

3.2.2 Guidance on Diversity Usage

As part of its regulation of civil aviation, the FAA certifies the airworthiness of FCSs. The Society of Automotive Engineers (SAE) publishes the Aerospace Recommended Practice (ARP) standard ARP 4754, "Certification Considerations for Highly-Integrated or Complex Aircraft Systems."[43] SAE ARP 4754 addresses certification aspects of highly integrated or complex systems intended for installation on aircraft while accounting for the overall aircraft operating environment and functions. SAE ARP 4754 defines the full engineering life-cycle, which includes planning, development, testing, and certification. SAE ARP 4754 also establishes guidelines for assigning Development Assurance Levels (DALs) to a system, its components, and any software based on the most severe failure conditions associated with the corresponding part. These DALs are assigned according to failure conditions classifications (i.e., catastrophic, hazardous/severe major, major, minor, and no safety effect).

The standard SAE ARP 4754 relates to aircraft system development. Additional guidelines for software development and hardware development are provided by Document (DO) 178B, "Software Considerations in Airborne Systems and Equipment Certification,"[42] and DO-254, "Design Assurance

Guidance for Airborne Electronic Hardware."[44] These guidelines are published by the Radio Technical Commission for Aeronautics (RTCA).

A safety assessment process is described in SAE ARP 4752 to generate evidence of compliance with airworthiness requirements. The primary processes involve a Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA), System Safety Assessment (SSA), and Common Cause Analysis (CCA). A CCA is required for systems assigned DALs A (Catastrophic) or B (Hazardous/Severe Major). The CCA begins after applicable separation and isolation requirements are identified to minimize commonalities and interdependencies. The CCA proceeds with Zonal Safety Analysis to identify location-specific challenges to independence, Particular Risks Assessment to common external events or influences of concern, and Common Mode Analysis to confirm assumptions of independence. This latter analysis addresses the potential effects of "design, manufacturing, and maintenance errors and the effects of common component failures."[43] Categories for common-cause faults are identified in terms of software design error, software coding error, requirements error, repair process error, environmental factors, hardware failure, hardware design error, compiler error, production process error, installation error, operational error, and cascading failures.

As a means to resolve the findings of the safety analyses, SAE ARP 4754 identifies the use of system architectural features such as redundancy, partitioning, or dissimilarity to eliminate or contain the degree to which an item contributes to a specific failure condition. However, SAE ARP 4754 does not use the same definitions of key terms as the nuclear industry. The aviation industry terms of redundancy, partitioning, and dissimilarity are comparable to the nuclear industry concepts of redundancy, isolation, and diversity.

Redundancy is the provision of more than one means for accomplishing a function. For example, redundancy can involve additional separate equipment to perform the same function as a primary piece of equipment. The redundant elements may be parallel or backup, active or passive, and/or of similar or dissimilar designs. SAE ARP 4754 indicates that redundancy is necessary to provide failsafe design protection from catastrophic failure conditions. SAE ARP 4754 further indicates that redundancy also may be necessary to meet the requirements associated with other severe failure conditions.

SAE ARP 4754 describes partitioning as a "design technique for providing isolation to contain and/or isolate faults and to potentially reduce the effort necessary for the system verification processes." Partitioning is a similar concept to isolation as used in IEEE 603.

The concept of dissimilarity as used in aircraft design is similar to the concept of diversity as used in the nuclear environment. The following excerpt from Section 5.4.1 of SAE ARP 4754 indicates that the use of dissimilarity or diversity is encouraged:

"For all but the simplest systems, it is practically impossible to guarantee the correctness and completeness of requirements or the correctness of all necessary assumptions. An architectural strategy incorporating dissimilarity can be a powerful means of reducing the potential for errors in requirements or in design implementation to cause serious effects… ." Additionally, the standard states that "[w]hen dissimilarity is used as a means of design error containment, the degree of credit should be related to the type and scope of design errors shown to be covered by the dissimilarity… . Assuming adequate independence can be shown, dissimilar design implementations of dissimilar functions can provide containment coverage for both implementation and function requirements errors."

SAE ARP 4754, Section 5.4.1.2, "Dissimilar, Independent Designs Implementing an Aircraft-Level Function," also includes the following:

"To be considered within this category, there must be substantial differences between the designs in terms of the means of preventing the top level failure condition(s), the methodology by which the designs are created, the technology through which the designs are implemented, and the operations through which

the functions are used. Validation of any assumptions of independence is of particular importance in demonstrating compliance… ."

Alternate architectures are also identified in the standard if dissimilar independent designs cannot be achieved. These include backup parallel designs, active-monitor parallel designs, and primary/secondary designs. The final case corresponds to dissimilar designs implementing a function with a primary portion satisfying the highest DAL associated with the most severe conditions and the secondary portion at a DAL that is one level lower than the primary portion.

3.2.3 Diversity Usage Examples

Aircraft manufacturers Airbus Industrie and Boeing provide the most extensive examples for digital FBW FCSs that have been developed for the commercial aviation industry. Airbus A320 serves as one of the earliest implementations and is included in this survey. Successor Airbus flight controllers and the Boeing 777 (B-777) FCS are also presented to capture the evolution of diversity usage in modern FBW systems.

3.2.3.1 Airbus A320

The A320, which was certified in 1988, represents a pioneering use of digital FBW FCSs in commercial aircraft.[45] The overall FCS is composed of diverse redundant primary and secondary control systems. The primary FCS is the elevator and aileron computer (ELAC) while the secondary FCS is the spoiler and elevator computer (SEC). The ELAC and SEC are physically and electrically separated with their own redundant sensors, communication (e.g., data/command links), and power supplies.

Each FCS consists of a self-checking pair based on two channels composed of a control computer and a separate monitor computer. These paired computers form redundant modules within each system, with the ELAC being duplicated and the SEC being triplicated. The redundant modules control redundant actuators. While one module is active, the other module is in standby mode and the redundant actuators are not active. Figure 3.2 illustrates the general architecture employed for the A320.

The pairing of control and monitor computers for the ELAC and SEC systems results in four functionally diverse implementations.[46] The control computers in each system supply flight commands based on normal laws for controlling the assigned actuators. Functional diversity arises because the control elements for the primary and secondary FCS are different. The SEC also provides a reduced functionality backup to the ELAC based on alternate flight control laws. Additionally, manual control based on direct control laws is provided through direct electrical linkage and is backed up mechanically as well.

The monitor computers implement similar functionality to the control computers, with each derived from the same functional requirements, to support comparison against the control computer outputs. This approach allows controller performance to be monitored for failures. When a failure of a control computer is detected by a monitor computer, primary control is transferred to a redundant module or, if unavailable, to a secondary FCS module. Diversity between the monitor and control computer applications within a module is promoted through use of different development teams, with some measure of forced diversity provided due to different design and implementation tools. Thus, the functions for the control and monitor computers are not necessarily identical and the programming for each provides some diversity due to personnel and tool set differences.

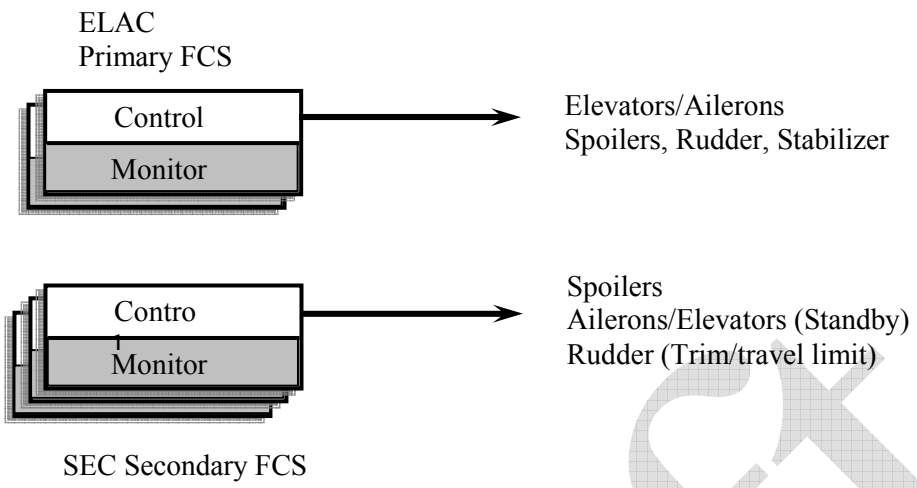

Figure 3.2. Airbus A320 architecture. (Adapted from Ref. 47**.)**

Different companies supplied the ELAC and SEC modules for the A320. Thomson-CSF (Compagnie Générale de Télégraphie sans Fil—CSF) supplied the ELAC modules, which are based on Motorola 68010 CPUs, while SFENA and Aerospatiale supplied the SEC modules, which are based on Intel 80186 CPUs.[48] For each FCS, different teams programmed each channel in different computer languages and then implemented using different compilers. For the ELAC, the control computer was programmed in Pascal while the monitor computer was programmed in C. For the SEC, the control computer was programmed in MACRO assembler while the monitor computer was programmed in Pascal.[49]

Therefore, the primary and secondary FCS for the A320 used two different design and manufacturing teams with different microprocessors (and associated circuits), different software architectures, and different functional specifications.[50] Within each FCS, separate design teams using different languages, compilers, and other design tool sets were used for the control and monitor channels.[51] Table 3.3 provides a summary of diversity usage for the Airbus A320.

Table 3.3. Summary of diversity usage for Airbus A320

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two flight control systems with different microprocessors
Equipment (Manufacturer)		
Different manufacturer—same design	x	ELAC supplied by Thomson-CSF; SEC supplied by SFENA and Aerospatiale
Equipment (Processing)		
Different logic processing architecture	x	Motorola 68010 vs Intel 80186
Functional		
Different purpose, function, control logic, or actuation means	x	ELAC and SEC fulfill a different flight control purpose based on different control laws; SEC has reduced functionality mode to back up ELAC; Each FCS provides redundancies comprised of dual

		channels for control and monitoring

Table 3.3 (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different design organizations/companies	x	ELAC and SEC supplied by different hardware/software company teams
Different design/development teams (designers, engineers, programmers)	i	Inherent difference in FCS design teams due to different organizations; Separate teams within each organization engaged to develop control and monitor channels (forced diversity through design independence and different toolsets)
Different implementation/validation teams (testers, installers, or certif. personnel)	i	Inherent difference in FCS implementation teams due to different organizations; Separate teams within each organization engaged to develop control and monitor channels
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different control laws implemented in ELAC and SEC; Reduced functionality flight controller in SEC (alternate and direct control laws implemented)
Different functional representation	x	ELAC control in Pascal vs monitor in C; SEC control in assembler vs monitor in Pascal; different compilers used
Signal		
Same parameter sensed by a different redundant set of similar sensors	x	Some data diversity due to slight time and amplitude variations for measurements
Other Diversity Considerations		
Parallel Diverse architecture with Redundant Self-Checking computer pairs; Diverse (reduced) functional requirements; Size and weight constraints	Diverse flight control computers for alternate overlapping control functions; Reduced functionality backup provides alternate automatic control; Redundant control/monitor pairs within each flight control system implemented with different languages and coding tools	

[a]Intentional diversity (x), inherent diversity (i).

3.2.3.2 Airbus A340

The Airbus A340, certified in 1992, represents an evolution of the digital FCS developed for the A320. As with the A320, the overall FCS for the A340 also employs diverse redundant primary and secondary control systems. These systems are the Flight Control Primary Computer (FCPC) and the Flight Control Secondary Computer (FCSC). The primary FCS is also identified as PRIM (meaning PRIMary flight control computer) and the secondary FCS is identified as SEC (meaning SECondary

flight control computer). In a manner that is consistent with the architecture established for the A320, both PRIM and SEC are composed of control/monitor computer pairs. These pairs constitute separate parallel channels within each system. These paired channels are replicated to provide three PRIM modules and two SEC modules. Within each module, the control channel generates the flight commands while the monitor channel generates comparative "commands." Both computers within a module compare differences in their outputs based on common input signals. If differences between the outputs exceed a threshold and persist for a sufficient interval, the module is automatically disconnected from the control path to provide a "fail fast" scheme. Control is automatically transferred to a redundant "standby" module that serves as a hot spare.[52]

Functional diversity between the primary and secondary FCS is achieved through different control laws, control elements, and reduced functionality. The PRIM system implements elaborate flight control laws for fully functional flight control, while the SEC system implements simpler, more robust flight control laws (i.e., less functions aimed at ensuring smoother flight and greater passenger comfort).[50] Other diversity usage between the PRIM and SEC systems includes different microprocessors (Intel 80386 for PRIM and Intel 80186 for SEC), different hardware suppliers (Aerospatiale for PRIM and Sextant Avionique [formerly Thomson-CSF and SFENA]), and different application development teams within the common system supplier (Aerospatiale) employing different design approaches and implementation tools (e.g., different high-level specification languages, coding techniques, programming languages, and compilers/translators were employed for the different channels within the different systems).[51] Specifically, the PRIM control channel was coded automatically in assembly language while the SEC control channel was coded manually in assembly language. Additionally, the PRIM monitor channel was programmed using PL/M (program language for microcomputers) while the SEC monitor channel was programmed using Pascal.[50,51] Table 3.4 provides a summary of diversity usage for the Airbus A340.

Table 3.4. Summary of diversity usage for Airbus A340

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two flight control systems with different microprocessors
Equipment (Manufacturer)		
Same manufacturer—different version	x	PRIM and SEC supplied by Aerospatiale (hardware by different manufacturers—Aerospatiale and Sextant Avionique, respectively)
Equipment (Processing)		
Different logic processing versions in same architecture	x	Intel 80386 vs Intel 80186
Functional		
Different purpose, function, control logic, or actuation means	x	PRIM and SEC employ different control laws and primarily manipulate different control elements; SEC has reduced functionality mode to back up PRIM; Each FCS provides redundancies comprised of dual channels for control and monitoring

Table 3.3 (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different management teams within same company	x	Independence between development teams maintained
Different design/development teams (designers, engineers, programmers)	x	Separate design teams for both FCSs and for channels within each FCS
Different implementation/validation teams (testers, installers, or certif. personnel)	x	Separate implementation teams for both FCSs and for channels within each FCS
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different control laws implemented in PRIM and SEC; Reduced functionality flight controller in SEC (alternate and direct control laws implemented)
Different functional representation	x	PRIM control channel in assembler (automatic coding) vs SEC control channel in assembler (manual coding); PRIM monitor channel in PL/M vs SEC monitor channel in Pascal; Different compilers/translators used
Signal		
Same parameter sensed by a different redundant set of similar sensors	x	Some data diversity due to slight time and amplitude variations for measurements
Other Diversity Considerations		
Parallel Diverse architecture with Redundant Self-Checking computer pairs; Diverse (reduced) functional requirements; Size and weight constraints	Diverse flight control computers for alternate overlapping control functions; Reduced functionality backup provides alternate automatic control; Redundant control/monitor pairs within each flight control system implemented with different languages and coding tools	

[a]Intentional diversity (x).

3.2.3.3 Airbus A380

In 2007, the progressive development of the Airbus digital FCS continued with the certification of the A380. The overall FCS for the A380 also employs diverse redundant primary and secondary control systems. The FCPC and FCSC of the A380 provide similar functionality to those of the A340. The primary differences between the overall FCS approaches for the two aircraft involve architectural changes. The A380 does not provide any mechanical backup for the electronic control linkages, and the FCPC and FCSC are both triple redundant (i.e., three modules of control/monitor channels) for the A380.

The diversity usage for the A380 is similar to that employed for the A320 and A340. The FCPC is supplied by Thales Avionics (formerly Thompson-CSF and later Sextant Avionique), while the FCSC is supplied by Diehl Aerospace, which is a joint venture of Thales Avionics and Diehl Group. The FCPC is

based on the Motorola Power PC CPU, while the FCSC is based on a different CPU (identified as a "SHARE" processor in Ref. 50). As before, the functional requirements for the FCPC and FCSC are different (i.e., based on different control laws for different primary control elements with a standby reduced-functionality backup provided by the FCSC). Similarly to the previous generations of the Airbus FCS, the data flow within the system is loosely synchronized between pairs and modules. Thus, slight differences arise in data values.

Finally, the different suppliers for the FCPC and FCSC result in the use of different development teams for the two systems. Within each organization, different development teams are provided for the control and monitor channels and the use of different automatic code generation tools based on different languages and different compilers/translators is enforced.[50] Table 3.5 provides a summary of diversity usage for the Airbus A380.

Table 3.5. Summary of diversity usage for Airbus A380

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two flight control systems with different microprocessors
Equipment (Manufacturer)		
Different manufacturer—same design	x	FCPC supplied by Thales Avionics; FCSC supplied by Diehl Aerospace
Equipment (Processing)		
Different logic processing architecture	x	Motorola Power PC for FCPC; Different processor for FCSC
Functional		
Different purpose, function, control logic, or actuation means	x	Primary and secondary controllers provide diverse overlapping flight control, with each using checked redundancy involving dual channels for control and monitoring; FCSC has reduced functionality
Life-cycle		
Different design organizations/companies	x	Thales jointly owns Diehl Aerospace, but the companies are managed separately
Different design/development teams (designers, engineers, programmers)	i	Inherent difference in design teams due to different organizations
Different implementation/validation teams (testers, installers, or certified personnel)	i	Inherent difference in teams due to different organizations
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different control laws implemented in FCPC and FCSC; Reduced-functionality flight controller in FCSC (alternate and direct control laws implemented)
Different functional representation	x	Control and monitor programs in different languages; different compilers used
Signal		
Same parameter sensed by a different redundant set of similar sensors	x	Some data diversity due to slight time and amplitude variations for measurements

Table 3.5 (continued)

Diversity attribute	Usage[a]	Details
Other Diversity Considerations		
Parallel Diverse architecture with Redundant Self-Checking computer pairs; Diverse (reduced) functional requirements; Size and weight constraints	Diverse flight control computers for alternate overlapping control functions; Reduced functionality backup provides alternate automatic control; Redundant control/monitor pairs within each flight control system implemented with different languages and coding tools	

[a]Intentional diversity (x), inherent diversity (i).

3.2.3.4 Boeing 777

The Boeing 777 was certified in 1995. It represents the initial and foremost example of the Boeing approach to digital FCS. The B-777 primary flight control system (PFCS) was supplied by GEC-Marconi Avionics Ltd.[53] The PFCS consists of three parallel channels that are physically and electrically separate. Each channel contains an identical primary flight computer (PFC). The PFCs are the central controllers of the PFCS. The PFCs are connected to data buses to enable transmission of commands to four Actuator Control Electronics units (ACEs) and also to permit information exchange among the controllers.

The channels share their data for equalization to permit direct comparison of consistent computational outputs. In addition, the channels conduct a median selection among their shared outputs to validate each final actuation command.[54] The need for agreement among the channels creates the potential for Byzantine faults.[55] However, the chosen implementation approach provides Byzantine-fault tolerance through bus and data synchronization to address asymmetric faults in communication and command validation to address asymmetric values in functional outputs.[52]

In addition to satisfying numerical reliability targets for the PFCS, Boeing also addressed deterministic goals in its design. These goals were as follows: (1) "[n]o single fault, including common [cause] hardware fault, regardless of probability of occurrence, should result in an erroneous … transmission of output signals without a failure indication" and (2) "[n]o single fault, including common [cause] hardware fault, regardless of probability of occurrence, should result in loss of function in more than one PFC."[56]

Consequently, the concept of triple modular redundancy is employed for all hardware resources of the PFCS (e.g., computing systems, airplane electrical power, hydraulic power, and communication pathways). In particular, triple modular redundancy is used in the design of each PFC through the provision of three internal computational lanes.[57] Essentially, the PFCS consists of three identical channels composed on three dissimilar (or diverse) lanes. Thus, the design constitutes a "Triple-Triple Redundancy" architecture.

As shown in Figure 3.4, three-version dissimilarity is integrated into the design through the use of different hardware (i.e., three different microprocessors). Each PFC consists of three dissimilar computational lanes, with each lane containing its own microprocessor, power supply, and communication interface.[58] The three identical PFCs are designated as Left, Center, and Right. Each PFC receives data from all three of the flight control data buses, but transmits only on its associated bus as shown in the figure. Cross-channel comparisons for median selection are performed based on communications across different buses (e.g., the Left PFC compares its current command against Center and Right commands received across the "C" and "R" buses).

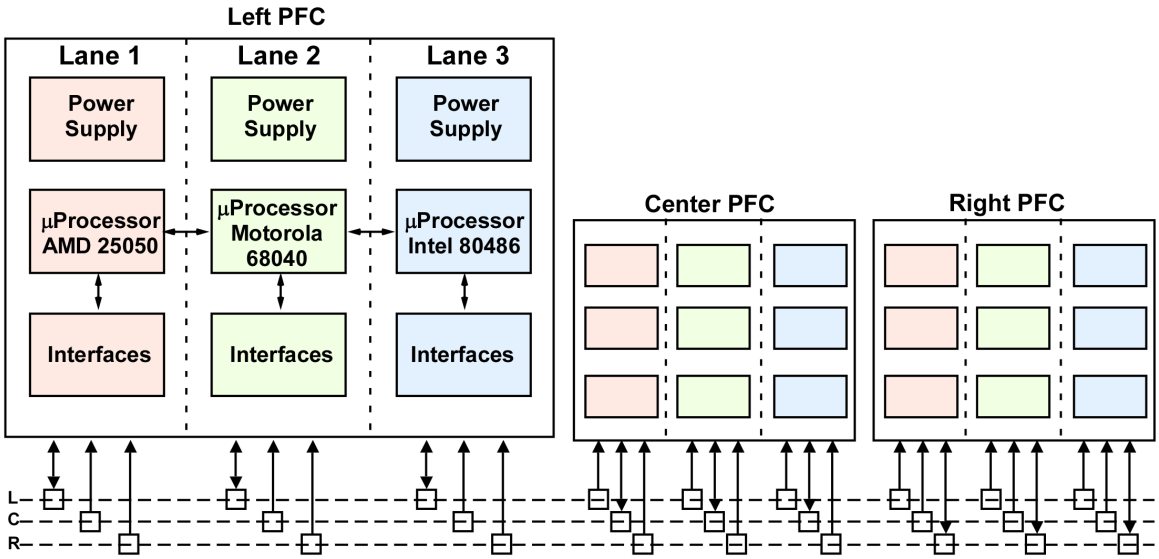

Figure 3.3. Triple-triple redundancy architecture of the primary flight computer. (Adapted from Ref. 58.)

The functionality of each lane is the same, but each is assigned a separate operational role. The three modes of operation are command, monitor, and standby. The command lane is the active controller for the channel. The monitor lane performs the same calculation as the command lane and shares its output for comparison. The standby lane is effectively in hot standby mode as it also performs the same calculations. However, the standby lane does not transmit its output unless it is activated due to a failure of the command lane. The cross-lane comparisons involve transmissions across the same bus (e.g., the left [L] bus for the Left PFC).[59]

The initial design approach proposed for the B-777 PFCS was to implement significant diversity among the lanes of each PFC through the use of different design teams and different software implementations.[60] However, Boeing decided against such extensive diversity due to concerns that (1) the management of multiple development teams would be onerous and prone to error,[53] (2) effort to maintain independence among the development teams would restrict communication among software and system engineers and prevent correction of requirements errors,[61] and (3) adoption of N-version programming would not be effective in avoiding common programming errors.[58] Thus, a single development team for the software application was used to generate the control software as common Ada source code. To enhance software quality, formal methods (e.g., static and dynamic analyses) were applied to PFCS algorithms.[53] Nevertheless, a different Ada compiler for the software implementation in each lane was used to enhance the triple dissimilarity.[58] Table 3.6 provides a summary of diversity usage for the Boeing 777.

Table 3.6. Summary of diversity usage for Boeing 777

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Three flight control channels composed of three lanes that are based on three different microprocessors

Table 3.6 (continued)

Diversity attribute	Usage[a]	Details
Equipment (Manufacturer)		
Same manufacturer—different version	x	GEC-Marconi Avionics developed the flight control system
Equipment (Processing)		
Different logic processing architecture	x	Motorola 68040 vs Intel 80486 vs AMD 29050
Different data flow architecture	–	ARINC 629 data bus in all cases
Functional		
Different purpose, function, control logic, or actuation means	–	Same for all PFC; zone controls (left, center, right) with median select for commands among controllers; Pilot-assist mode for degraded operation (very limited functionality, common to all channels); Diverse manual controls also available (mechanical linkage)
Life-cycle		
Different management teams within same company	–	Separate teams for diverse software development rejected over concerns that (1) management of multiple teams would add excessive complexity, (2) interactions (requirements clarifications) would "corrupt" independence, and (3) N-version programming would be ineffective
Logic (Software)		
Different algorithms, logic, and program architecture	–	Common to all channels; Degraded mode (reduced functionality + pilot assist) provides minimal automatic control or simple support of manual control
Different functional representation	x	Same source code for all channels and lanes (programmed in Ada); different compilers used for each lane
Signal		
Same parameter sensed by a different redundant set of similar sensors	–	Shared cross-equalized signals for each zone
Other Diversity Considerations		
Parallel Redundant (zone separation) architecture with embedded diverse Redundant Self-Checking computers; Formal methods applied to minimize requirement specification errors; Size and weight constraints	Diverse computers (lanes) within each control channel for internal comparison; Redundant triplets (lanes for command, monitor, standby) implemented with same software using different compilers	

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

3.3 Chemical Process Industry

3.3.1 Overview

The chemical process industry transforms the raw materials of the earth, sea, and air into industrial and commercial products. Within the U.S., the chemical process industry employs almost 900,000 workers and generates over $660 billion in products and assets. While volatile chemical reactions and toxic constituents are frequently involved in the product stream, the domestic chemical process industry maintains injury and illness rates half of the U.S. manufacturing average.[62]

The Occupational Safety and Health Administration (OSHA) under the U.S. Department of Labor enforces health and safety regulations for industrial processes and has regulatory oversight responsibility for workplace safety and worker health. Additionally, the American Institute of Chemical Engineers (AIChE) established the Center for Chemical Process Safety (CCPS) to develop and disseminate voluntary guidance for use in the prevention of chemical accidents.

The U.S. chemical process industry regularly produces, stores, transforms, and consumes highly toxic, explosive, highly flammable, and carcinogenic materials in large quantities. Moreover, it employs physically (e.g., temperature, pressure) and chemically aggressive environments to perform its basic functions. Hazardous material processing takes place in plants that share many features with NPPs. Modern chemical plants feature a main control room that presents information about the plant and process status to the operator. Local control loops may also be employed to control particular aspects of the process operation. Plants may be spatially extensive with many distributed process steps, possibly implemented in parallel branches, or compact with the primary reaction occurring in a small set of tanks. Plants may produce large volumes of bulk products (e.g., fertilizer or polyethylene) or relatively small quantities of high-value products (e.g., pharmaceuticals or nuclear fuel). The quality of the product (e.g., tires, pharmaceuticals) may have as large a safety implication as the operation of the plant. In general, the breadth and diversity of the processes and products of the chemical industry require a higher degree of abstraction than the nuclear power industry in the evaluation of plant control and safety architectures.

While chemical processing plants have many features similar to those of NPPs they can be significantly more complicated to safely and effectively operate and maintain. A notable difference between chemical processing plants and NPPs is the fact that feedstocks enter and products exit during operation of the former. The required ingress and egress of materials during process operation makes the concept of containment of those input and output materials inherently less rigorous than for an NPP. While some chemical plants operate in purely batch mode, where feedstock chemicals are loaded prior to processing and products are unloaded following processing, this is not common for high-volume production that involves more continuous real-time control.

Another important difference between chemical processing and NPPs is the potential storage of large volumes of hazardous materials on-site in the case of the former. In chemical plants accidents can occur outside of the processing steps with the feedstock or product materials as well as during active processing. Further, the intermediate products in chemical processing plants can be hazardous and reactive with the environment, potentially having violent reactions with air or water, making control of small leaks potentially more important in chemical than in nuclear plants. Finally, nuclear power plants have a deenergized safe shutdown condition. Chemical plants do not necessarily have a rapidly accessible, deenergized shutdown condition. Plant shutdown in chemical plants can be a multistep, time-consuming process. For example, polymerization resulting in a line blockage can occur in the process piping if the process temperature is lowered, potentially allowing hazardous pressure buildups.

In spite of the aforementioned differences in application context, there still remains significant similarity between control and protection systems at chemical processing plants and NPPs. Within a chemical process plant, the primary control functions are performed by the basic process control system (BPCS) while protective functions are provided by separate, high-integrity safety instrumented systems

(SISs). An SIS is "composed of sensors, logic solvers, and final control elements whose purpose is to take the process to a safe state when predetermined conditions are violated."[63] Typical SISs include emergency shutdown systems (ESD or ESS), safety interlock systems, protective logic systems, and safety shutdown systems (SSD). Although SISs traditionally involve physical (e.g., pneumatic and hydraulic) and electrical (e.g., direct wired, electromechanical, and solid-state relay) systems, programmable electronic systems (PESs) are becoming prevalent. Common PES platforms include programmable logic controllers (PLCs), distributed control systems (DCSs), or application-specific stand-alone microcontrollers.

3.3.2 Guidance on Diversity Usage

The 1992 OSHA rule on Process Safety Management of Highly Hazardous Chemicals[64] is the federal regulation for the chemical processing industry most directly comparable to Chapter 7 of the NRC's Standard Review Plan (NUREG-0800). The OSHA rule was developed to prevent and mitigate hazardous releases of the regulated chemicals. The rule was adopted following several catastrophic chemical and petrochemical incidents causing multiple deaths and extensive property damage. In particular, a toxic gas leak at a chemical process plant in Bhopal, India, directly caused the death of over 2000 people. Inadequate safety design and nonfunctioning safety systems due to poor maintenance were identified as contributing factors.[65]

The OSHA rule addresses process hazard assessment, risk control measures, and consequence evaluation for system failures, as well as documentation and maintenance requirements. The central OSHA requirements are founded on a process hazard analysis that identifies, evaluates, and specifies the controls for the hazards of a particular process. Of note, the rule requires "that equipment complies with recognized and generally accepted good engineering practices" as opposed to prescriptively specifying particular equipment design and performance requirements. There are no specific requirements regarding consideration of the potential for CCF vulnerability or the use of diversity.

Following the 1985 Bhopal disaster, the AIChE/CCPS developed a series of guidelines providing technical information and recommendations for chemical process safety. In particular, the CCPS Guidelines for Safe Automation of Chemical Processes[66] provides the most extensive guidance on design practices for SISs. Most of the information presented in this section is drawn from the guidance in this document. Additional guidance and standards considered include the CCPS guide, "Guidelines for Safe and Reliable Instrumented Protective Systems;"[67] the Instrument, System, and Automation Society (ISA) standard S84.01-1996, "Application of Safety Instrumented Systems;"[68] and IEC 61511, "Functional Safety: Safety Instrumented Systems for the Process Industry Sector."[69]

Starting with the safe design, defense-in-depth is generally employed for chemical processes through provision of successive independent protection layers (IPLs). As a result, thorough separation between BPCS and SIS layers and among individual systems is encouraged to promote independence. Depending on the risk, each SIS is assigned an integrity level (IL) from among three distinct safety performance levels. Redundancy of components and signal paths, along with the extensive use of active diagnostics, provides degrees of fault tolerance associated with each IL level. Specific techniques to minimize faults include software quality assurance practices, use of watchdog timers, pulsed outputs to detect failures, and fault-tolerant configurations (e.g., triple modular redundant with two-out-of-three voting). Additionally, SIS interlocks are designed to be failsafe.

Nevertheless, recognizing CCF to be a significant concern for control and safety systems (especially those employing PESs), the CCPS recommends diversity in protective systems for hazardous processes. Diversity is identified as referring to "factors that make two components (e.g., devices, subsystems, systems, software systems, communications systems, sensors, or final control elements) different in a way that minimizes common mode fault."[66] The CCPS further states that diversity "may include the use of

different physical methods, technology, manufacturers, installation, maintenance personnel and/or environment."[67]

Identifying the degree of risk in the chemical process, and thereby determining the SIS diversity needs, begins with a detailed process analysis. After process hazards have been identified, process modifications to reduce the overall risks are then considered. Next a basic process control strategy is identified. Process risks are then assessed, through probabilistic risk assessment, by considering accident likelihood and consequences coupled with predicted safety equipment performance probabilities. A minimum safety performance integrity level is then associated with a particular process based upon the identified risk and the available IPL. Higher risks are associated with higher ILs and increase the required amount of engineering rigor in the process control and safety system design. For the highest integrity level, the CCPS recommends that "Diversity should be considered and used where appropriate."[66]

The CCPS safety evaluation model, relatively speaking, maintains a considerable degree of correspondence with that of the nuclear power industry. The CCPS safety evaluation model employs independent protection layers—roughly in accord with the "echelons of defense" of the nuclear industry. The CCPS endorses separation (lack of direct communication), independence (no common components or collocation), and diversity of each layer of the control and protection system(s). The CCPS also provides guidelines for necessary exchange of information among separate safety channels (e.g., for voting) and for buffered intercommunication to other components. Employing multiple, independent protection layers is also provided as an example of increasing safety system diversity.

Acknowledging the significant functional difference between the process control and safety systems, most of the CCPS diversity recommendations adopt that difference as a basic diversity attribute. Essentially, the chemical industry notes that the functions of the control system and the safety system are different. Consequently significant diversity is thus inherently obtained by having independent safety and control systems.

The CCPS does not provide detailed guidance on how much diversity is required for a particular process risk. In fact, the CCPS specifically places the responsibility for determining the appropriate amount of safety engineering on the plant owners. The minimum number of Independent Protection Layers required to address a process risk can be derived from the user company's safety policy.

However, the CCPS guidance does provide high-level recommendations on the use of diversity, depending on the IL associated with each SIS. Diversity usage recommendations include the use of different technologies, different manufacturers (or products from different vendors), and different application programming teams. For hardware diversity, different sensors and logic equipment are identified as options. For system software diversity, different controller/logic platforms and smart sensor devices are recommended. For application software diversity, development of different programs is recommended. It is explicitly noted in the guidance that diversity "can cause serious problems when reliability is sacrificed to achieve diversity."[66] Therefore, diversity is recommended only where reliable components are available.

Finally, the CCPS does provide cautionary guidance about the difficulties in eliminating CCF throughout the system life-cycle. The CCPS indicates that CCFs are frequently of human origin with system maintenance, testing, and design being prime common failure sources. The elimination of these vulnerabilities is thus difficult to achieve in SIS. Further, while the CCPS does endorse both passive and active diagnostics of the plant control and safety systems (e.g., internal and external watchdog timers) at the same time the guidance notes that the additional complexity engendered by the diagnostics increases the possibility for system failure from a separate source. Thus, a balance between adequate diagnostic coverage and minimizing system complexity is required.

3.3.3 Diversity Usage Examples

Specific applications and particular company guidelines based on the principles established by the CCPS are proprietary and not generally available. Thus, this discussion of diversity usage in the chemical process industry focuses on the guiding practices found in the CCPS documents.

In its guidance, the CCPS states the design of an SIS must address failsafe characteristics, fault prevention and mitigation, separation between control and protection, diversity, software quality and performance, diagnostics, and communications. The CCPS recognizes and advocates types of diversity that are consistent with the diversity attributes identified in NUREG/CR-6303.

The diversity type most definitively advocated in chemical plant process safety design is functional diversity. The CCPS recognizes that the goals of the process control and safety systems are different (one, to produce product, the other, to bring to the plant to a safe shutdown condition) and that considerable diversity inherently derives from this difference of purpose.

The CCPS also advocates signal diversity as a powerful technique for minimizing the potential for CCF. The central identifying characteristic of the signal diversity principle is to provide a diverse measurement of the same process measurement point. The CCPS indicates that signal diversity is preferentially obtained through measuring diverse system attributes and then applying a system model to correlate the measurements. Transducer diversity within a single measured variable (e.g., a resistance temperature detector vs a thermocouple) is also recommended.

Further, the CCPS does recognize that the use of diverse hardware, computer operating and system services software, compiler, programming language, and application programs can combine to minimize the potential for CCF vulnerabilities. Additionally, the CCPS recognizes that increased diversity and improved safety can result from diverse design and maintenance teams. In particular, the CCPS notes that diverse application software between the control and safety or among separate safety systems provides protection against CCF. The CCPS also provides a cautionary note that having a common set of functional requirements inherently limits the diversity achievable in application software. However, the CCPS does not provide guidance on quantifying the particular risk reduction associated with employing any particular form of design, equipment, software, or human diversity.

Table 3.7 provides a summary of diversity usage recommended by the CCPS. Specific diversities related to hardware, system software, and application software is recommended for SIS at the highest IL (IL 3). Hardware and system software diversity is recommended between SIS controllers and SIS smart field devices. This diversity usage is considered optional between SIS and BPCS controllers. Application software diversity is recommended between SIS controllers and smart field devices and between BPCS and SIS controllers. Additional software application considerations identify different logic between SIS and BPCS controllers as well as the use of dedicated, user-approved engineer's workstations and programming utility software (from the SIS hardware vendor).

Table 3.7. Summary of diversity usage for chemical process plants

Diversity attribute	Usage[a]	Details
Design		
Different technologies	–	Identified as an option (e.g., relays vs PLCs); hardware diversity of this type minimizes need for additional diversities
Different architectures	x	Different PES (e.g., different PLCs) promotes hardware/software diversity (e.g., different implementation and behavior)

Table 3.7 (continued)

Diversity attribute	Usage[a]	Details
Equipment (Manufacturer)		
Different manufacturer—same design	x	Different hardware to avoid common vulnerabilities or manufacturing defects
Same manufacturer—different version	–	Noted as an option (different products)
Equipment (Processing)		
Different logic processing architecture	x	Different PLCs to promote different implementation and execution of functions
Functional		
Different purpose, function, control logic, or actuation means	x	Different purpose and function between control and safety systems; Safety interlock vs control or different interlocks (i.e., different activation indicator or protection means)
Life-cycle		
Different design organizations/companies	–	Identified as option if supplier configures application
Different management teams within same company	–	Not addressed in guidance
Different design/development teams (designers, engineers, programmers)	x	Helps avoid common development errors
Different implementation/validation teams (testers, installers, or certification personnel)	x	Helps avoid common implementation and interaction errors
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different algorithms and logic (i.e., batch/continuous control vs interlocks or different input/output relationships for interlocks)
Different runtime environment	x	Different system services and runtime management to avoid common faults
Different functional representation	x	Different programming languages and methods to avoid common errors
Signal		
Different parameters sensed by different physical effects	x	Employed wherever feasible for critical measurements
Different parameters sensed by same physical effects	x	Employed wherever feasible for critical measurements
Same parameter sensed by a different redundant set of similar sensors	x	Employed to ensure separation between safety and control

Draft

Table 3.7 (continued)

Diversity attribute	Usage[a]	Details
Other Diversity Considerations		
Diverse Redundant architecture for Integrity Level 3 safety interlock systems; Emphasis on use of hardware, system software, and application software diversity; Separation of safety and control; Recommends communication isolation	Design and equipment diversity to promote hardware and system software differences; Functional, life-cycle, and software diversity to promote application software differences; Signal diversity to promote separation and input diversity; Separation among safety devices recommended as well as separation between control and safety; Any communications with high-integrity devices should be "read-only" (i.e., data or demands but no change commands such as reprogramming)	

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

3.4 Rail Transportation Industry

3.4.1 Overview

The Federal Railroad Administration (FRA) under the U.S. Department of Transportation promulgates and enforces rail safety regulations as a central element of its mission to oversee domestic rail transportation. The U.S. rail transport is subdivided into three categories: freight, intercity passenger service (Amtrak), and local commuter service. The most sophisticated rail switching and control systems are in the densely interconnected local commuter rail networks. Freight railroads currently have a mix of purely manual and remotely operated manual controls with little system automation.

In Europe, the European Railway Agency (ERA) was established in 2004 to facilitate an integrated railway system by reinforcing safety and interoperability. The primary activities of the ERA involve the development of economically viable common technical standards and approaches to safety and serving as the system authority for the European Rail Traffic Management System.

Collision avoidance is a key operational safety concern for railway and train control. Signaling, interlocks, and train speed control are critical functions for ensuring railway safety. Ensuring unobstructed routes and track circuits while controlling train traffic requires a distributed system of sensing and control elements, both embedded on the trains and stationed along the tracks. By stopping or slowing trains to inhibit access to occupied tracks, railways have a readily accessible safe state. Thus, systems can be designed to fail to a local de-energized "stop" configuration. Essentially, a failsafe condition can be achieved in which all trains stop.[70] This failsafe approach results in a practical emphasis for rail safety system on identifying faulted conditions and stopping the affected trains until the hazard can be cleared or the system can be fixed. Because of the distributed nature of the rail network, the widely varying track loads (e.g., demand profile), and the localized action for interlocks and train control, safety-critical functions for railway management have some different characteristics and implementation approaches compared to NPP protection functions that respond to more inherently interrelated processes with more global (i.e., plant-wide) actions. Nevertheless, insights into approaches to mitigate the potential for CCF vulnerabilities can be drawn from diversity usage by the rail transportation industry.

3.4.2 Guidance on Diversity Usage

The FRA safety regulations are found in Title 49 of the Code of Federal Regulations. The *Signal and Train Compliance Manual* is formed by Parts 233–236 of Title 49. Of particular relevance is Subpart H, "Standards for Processor-Based Signal and Train Control Systems," of Part 236, "Rules, Standards, and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances,"[71] which establishes regulations addressing the use of microprocessors in signal and train control systems. Other subparts address requirements for interlocking systems, traffic control systems, and automatic train stop, train control, and cab signal systems.

The regulations in 49 CFR 236 Subpart H require the establishment of a Railroad Safety Program Plan (RSPP) based on product safety plans (PSPs). The RSPP must address system requirements and concepts, design for V&V, design for human factors, and configuration management controls. In particular, a safety analysis must be included which describes the critical behavioral characteristics, risk assessment procedures, any safety precedence applied, and the safety assessment process. In addition to containing the aforementioned risk assessment, the PSP must also provide a hazard mitigation analysis and V&V plan as part of a complete description of the safety assessment. Within the regulations, practices developed by the American Railway Engineering and Maintenance of Way Association (AREMA) for the application of vital electronic/software-based equipment are adopted. Coded processors represent a high-integrity implementation approach that contributes to addressing the potential for CCF vulnerabilities. This approach will be described in the subsequent examples of diversity usage.

As indicated previously, the ERA began in 2004 through publication of the European Rail Safety Directive (2004/49/EC),[*] which forms the basis of the European rail safety scheme. However, this directive is at a high level, emphasizing overall system quality and not focused on implementation methodologies. Subsequently, the ERA issued the initial Common Safety Methods and guidance on the development of Common Safety Targets. The Common Safety Methods, developed as recommendations in late 2007, primarily address the use of risk assessment, based on hazard identification and consensus assessment principles, as a means of establishing safety requirements.[72] In April of 2008, the first recommendations on a framework of methods to be used for calculation, assessment, and enforcement of Common Safety Targets were issued. Generation of the first set of Common Safety Targets is anticipated in 2009.

The principal European railway standard that addresses digital safety-critical systems is the CENELEC (European Committee for Electrotechnical Standardization) European Norm (EN) 50128 "Railway applications—Communications, signaling and processing systems—Software for railway control and protection systems,"[73] which draws heavily from IEC 61508.[74] The norm provides guidance on software safety integrity levels, personnel and responsibilities within the software life-cycle, life-cycle documentation, requirements specifications, architectures, design and implementation, verification and testing, software/hardware integration, validation, assessment, quality assurance, and maintenance.

Within EN 50128, the guidance on software assessment highly recommends a Common Cause Failure Analysis. The informative Annex B describes methods of CCF Analysis as "general quality control, design reviews, verification and testing by an independent team, and analysis of real incidents with feedback of experience from similar systems."[73] The norm also contains specific guidance regarding software architectures that addresses means to mitigate CCF. These include defensive programming, safety bag techniques, and diverse programming. Defensive programming techniques include approaches to check for control or data anomalies, such as plausibility checks for data or control flow sequence checking for code execution. The safety bag approach is based on the concept of a safety envelope (or "bag") surrounding the application to ensure only safe actions are authorized (see Annex B of Ref. 73). Safety bag techniques involve an external monitoring application on an independent computer with the

[*] http://www.era.europa.eu/PUBLIC/CORE/SAFETY/Pages/default.aspx

application based on a different specification from the safety-critical application. The purpose of the safety bag processor is to confirm that the actions/commands of the safety-critical application are "safe, not necessarily correct, actions."[73] Given detection of a potentially hazardous state for the safety-critical application, the safety bag processor enforces a safe state. Diverse programming involves N-version programming with arbitration based on either complete agreement or majority voting. For software of the highest safety integrity level (SIL 4), defensive and diverse programming techniques are highly recommended while safety bag techniques are recommended.

3.4.3 Diversity Usage Examples

Deployed automatic train control and traffic management systems, as described in the literature, employ varying amounts of system diversity, which is generally achieved through software. However, an early example of computerized train control relies on fault tolerance through hardware rather than diversity. The Computer Aided Traffic Control (COMTRAC) system is used by the Japanese National Railways (JNR) to provide high-speed train control for its Shinkansen trains.[75] The system was inaugurated in 1964 and was upgraded using digital technology 8 years later. The fault tolerant approach employed is based on hardware redundancy. For the COMTRAC system, dual or triple symmetric computers, each of which operate on equalized data using the same software, are continuously monitored by a failsafe comparator that enforces a safe state upon detection of a discrepancy. As is the case for the Japanese nuclear power industry, the Japanese rail transportation industry accepts well-proven programming techniques and experience with digital systems in non-safety applications.

An automatic train control system employing software diversity was implemented by Ericsson in the commuter train system of Gothenburg, Sweden, in 1978.[76] The Gothenburg system underwent a formalized, high-quality software development process similar to that described in BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems."[77] The system also employed component-level redundancy. The Gothenburg system invoked software diversity by using two independent design teams provided different design rules.

An Italian train control system has also been implemented using software diversity through sequentially running diverse programs and comparing their results for error detection.[78] A more recent example is the Computer-Based Interlocking system designed by Ansaldo Trasporti. This system employs identical computers and computing environments within a triple modular redundant architecture to form a Safety Nucleus for vital processing. However, each of the three interlocking-logic application programs is different (i.e., N-version programming). A logic exclusion comparator enforces failsafe conditions upon any detected disagreement.[79]

A different means of achieving software diversity is reported to have been implemented for licensing purposes in Germany in 1984. In this case the final program object code was reverse engineered to obtain the requirement specifications, which were then cross compared with the originals to verify lack of translation errors.[80]

Even more recent examples of railway control system design focus on the use of redundant hardware, high-quality software, and stopping trains in case of system failures.[81] Control systems with a fully diverse means to both decide that the rail system is in an unsafe state and bring the system to safe shutdown are not yet available.

Three examples of unique diversity usage in safety-critical rail transportation application involve either the safety bag approach or vital coded processors. These techniques are illustrated in the following examples.

3.4.3.1 Austrian Federal Railways

The Elektra railway interlocking control system was designed by Alcatel Austria for the Austrian Federal Railways. The Elektra system was first implemented in 1989. The architecture employs diversity through its dual channel checking system:[82,83] One channel, designated as the interlocking processor (ILP), executes the interlocking control software (i.e., functional computation), while the other channel, designated as the safety bag processor (SBP), executes the monitoring software (i.e., checking computation). Intercommunication between the processors is implemented via the Votrics communication layer to provide a fault-tolerant message passing architecture for functional monitoring and communications monitoring.[84] Both channels employ redundancy and active replication with identical triple-redundant hardware and software internal to a channel. The replicated, redundant modules perform synchronized computations and require complete agreement to support failure detection. Any faulty component that is detected is reset and resynchronized. The monitoring channel's purpose is to check whether each interlocking control function places the system in a safe state. Actions are only performed if the second channel agrees that the results proposed by the first channel do not violate any safety conditions. If this is not the case, a transition to a safe state is invoked.

For the Elecktra interlocking system, the safety bag implementation employed diverse development teams within Alcatel. Additionally, diverse functional requirements were the basis for the channels, with different functions programmed using different tools in each channel.[85] Specifically, the software specifications for the monitoring channel were derived from the railway authority's operating regulations, while the software specifications for the interlocking control channel were based on functional requirements. Additionally, the monitoring channel was programmed according to a rule-based paradigm, while the interlocking control channel was programmed according to a procedural paradigm. Thus, different languages (i.e., Pamela for SBP and CHILL for ILP) and compilers were used. Table 3.8 provides a summary of diversity usage for the Austrian Federal Railway implementation of the Elektra system.

Table 3.8. Summary of diversity usage for Austrian Federal Railways (Alcatel Austria)

Diversity attribute	Usage[a]	Details
Design		
Different architectures	–	Control and monitor channels implemented on identical platforms
Equipment (Manufacturer)		
Equipment (Processing)		
Different logic processing architecture	–	Intel 80286 or 80486 CPUs used (no intentional diversity specified)
Functional		
Different purpose, function, control logic, or actuation means	x	Control vs safety purpose; Diverse requirements; Control vs checking functions; Execution by functional computation vs rule-based comparison; Dual permissive needed for action (SBP must authorize IPL action)
Life-cycle		
Different management teams within same company	–	No information provided
Different design/development teams (designers, engineers, programmers)	x	Different teams established within Alcatel
Different implementation/validation teams (testers, installers, or certification personnel)	x	Different teams established within Alcatel

Table 3.8 (continued)

Diversity attribute	Usage[a]	Details
Logic (Software)		
Different algorithms, logic, and program architecture	x	Difference in algorithms/logic (functions vs rules) and architecture (procedural vs rule based)
Different functional representation	x	Different software language (CHILL vs Pamela); Different compilers used
Signal		
Different parameters sensed by different physical effects	x	Measurement of process (train speed/location) vs communication of system status (controller operations and variables)
Other Diversity Considerations		
Parallel primary-checker architecture; Fundamentally diverse functional requirements; Formal verification of controller software	Safety bag processor for verification of safe action; Checker performs concurrent validation with failsafe response	

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

3.4.3.2 Paris Rail

In 1988, the Paris Public Transportation Authority (Régie Autonome des Transports Parisiens—RATP) and the Société Nationale des Chemins de fer Français (French National Railway Company—SNCF) engaged a consortium of railway equipment manufacturing companies (GEC Alstom Transport, MATRA Transport, and CSEE Transport, now part of Ansaldo Transporti) to develop a microprocessor-based automatic train control system. The resulting Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance (SACEM) fault-tolerant train speed control system was first implemented on the Paris Rail line A (RER A or Réseau Express Régional A). SACEM was characterized by development of the vital coded processor (VCP) approach.[86] In 1998, an application of the VCP for the unmanned automatic subway, Météor, enhanced the use of a formal development process to reduce the potential for design errors. The VCP approach is currently supported by manufacturers such as Siemens and Alstom for applications that include the Canarsie Line in New York and the North East Line in Singapore.

The basic premise behind the VCP is to provide a hardwired comparator to confirm the proper execution of the safety or control function in the computer system by comparing expected (i.e., pre-determined) properties of the code against observed or generated properties of the code. The principle of encoding is based on expressing information about the application program and its execution using an arithmetical code, an operational signature, and a dynamic or temporal code (i.e., "technique of dynamisation").[87] The process for implementing the VCP proceeds as follows.[88] Using a formal process (based on the B formal language for the examples cited), an implementation (i.e., abstract model) is first developed from the software specification in the formal language and is subsequently translated into code. As part of this process, the implementation undergoes formal proof during the development process. The translation of the implementation into code is based on two diversely developed translators (i.e., different teams, designs, and programming languages)[88] to yield two distinct versions of the code. One version is compiled to become the safety application object code. The other version is processed to create reference signatures of the code execution. The VCP is implemented with a hardwired checker that compares precomputed signatures against the actual signatures corresponding to the runtime values. If a discrepancy is detected, an error has occurred and a failsafe condition is enforced.

For the SACEM example, formal methods were used at a later stage of the development effort than for the Météor example. Essentially, the code (written in Modula 2) was developed, inspected, tested, subjected to formal proof, and then processed through formal re-expression (i.e., a formal specification was generated after the fact). Separate teams were used at each stage of the process: design, safety assessment, validation, and formal re-expression. Additionally, separate sub-teams were used for validation.[89] In the case of the Météor application, a formal specification was developed up front.[88] In this case, the concept of separate teams at different life-cycle stages persisted with separate formal support, development, testing, and validation teams. It should be noted that this use of separate teams at different stages of the life-cycle does not necessarily provide life-cycle diversity at the latter stages because the final system is an individual integrated system rather than two separate systems. Thus, there are not two separate, parallel developments by teams that can remain separated, as would be customary usage for life-cycle diversity. Table 3.9 summarizes the diversity usage for the Paris Rail applications.

Table 3.9. Summary of diversity usage for Paris Rail (RATF)

Diversity attribute	Usage[a]	Details
Design		
Different approach—same technology	x	CPU + hardware checker (FPGA/PLD)
Different architectures	i	Same (integrated) system architecture but different microarchitecture
Equipment (Manufacturer)		
Same manufacturer—different design	x	Integrated applications developed by same consortium/company on interconnected platforms supplied by different manufacturers
Equipment (Processing)		
Different logic processing architecture	i	CPU vs gate arrays (result of design diversity)
Different component integration architecture	–	Integrated implementation (no inherent diversity)
Different data flow architecture	–	Shared bus (no inherent diversity)
Functional		
Different underlying mechanisms	i	Encoded data processing vs signature comparison (result of intentional functional diversity); Different execution mechanisms (result of design diversity)
Different purpose, function, control logic, or actuation means	x	Control vs safety purpose; Control vs checking functions; Execution and dynamic generation of coded signatures vs comparative logic for signatures
Different response time scale	i	Sequence of operations vs comparison of intermediate states against correctness criteria (result of intentional functional diversity)

Table 3.9. (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different design organizations/companies	–	Application development by same consortium/company
Different management teams within same company	–	Integrated product (No intentional diversity specified)
Different design/development teams (designers, engineers, programmers)	x	Different designers/programmers for control function vs checking function (related to expertise); Different teams providing different expertise for parallel application development
Different implementation/validation teams (testers, installers, or certification personnel)	x	Different validation teams for different codes; Integrated final system (no intentional diversity specified)
Logic (Software)		
Different algorithms, logic, and program architecture	x	Difference in algorithms/logic and architecture (related to technology and function)
Different timing or order of execution	–	Synchronized execution
Different runtime environment	i	Arises from technology difference (result of design diversity)
Different functional representation	x	Diverse code translators for generation of code from formal implementation; Software language vs hardware description language are inherently diverse (result of design diversity)
Signal		
Different parameters sensed by different physical effects	x	Measurement of process (train speed/location) vs communication of system status (controller operations and variables)
Other Diversity Considerations		
Embedded Primary-Checker architecture; Fundamentally diversity functional requirements; Formal verification of controller software	Coded processor for end-to-end control; Checker performs concurrent validation with failsafe response	

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

3.4.3.3 Los Angeles Metro Green Line

In the mid-1990s, the Center for Semicustom Integrated Systems (CSIS) at the University of Virginia (UVa) teamed with the Advanced Technology Group of Union Switch and Signal (now a part of Ansaldo Trasporti) to develop the Vital Framework (V_Frame).[90] The V-Frame is a fault-tolerant safety-critical platform to support the use of COTS hardware and software. The V-Frame can be seen related to the VCP approach except that it does not depend on formal development of the initial code or application-specific implementation of dedicated hardware.

The V_Frame embodies the safety-critical algorithm-based fault tolerance (SC-ABFT) approach developed at UVa.[91] SC-ABFT provides a method for verifying whether applications are executed correctly within a certain probability. In this approach, an application or algorithm is decomposed to its fundamental operations or primitive blocks so that the sequence of execution for those operations can be verified though the generation and confirmation of a check-stream. To avoid the paradox of a self-referencing system, a separate checking device accomplishes the verification of the check-stream.[90]

The decomposed algorithm can be represented in terms of a data flow graph that captures key attributes of the set of equations. In particular, the data flow graph uniquely identifies each operator, each input and output object, and the temporal relationship among operators in the execution sequence. Based on this deconstruction, code words can be generated to construct the check-stream representing the correct execution of the algorithm. Subsequently, the correct operation of each primitive block can be precomputed and stored in a look-up table. The blocks themselves are simple enough to allow proof of correctness. Having precomputed, proven blocks enables checking the correct execution of each block in real time by comparing the results of the look-up table versus those of the code calculation. Additionally, corresponding check-streams can be established to enable verification of correct execution in the field. This checking capability is implemented either in "a redundant processor executing software or a low-complexity custom hardware device."[91] This type of system relies on having primarily discrete, as opposed to continuous, variables to allow the control system to be decomposed into a finite set of states.

The V_Frame implementation of the SC-ABFT was demonstrated in prototype form simulating the Los Angles Metro Green Line. The first demonstration at UVa involved a COTS-based test system using a Motorola 68040 processor card with supporting I/O implemented in a VME-based chassis.[91] Also, the check process was performed via a check algorithm that executed on a Motorola 68040 processor card. Later prototypes involved the use of FPGAs, and a commercial platform was subsequently developed by Ansaldo.[92] Table 3.10 summarizes the diversity usage for the Los Angeles Metro Green Line prototype.

Table 3.10. Summary of diversity usage for LA Metro Green Line (Ansaldo/UVa)

Diversity attribute	Usage[a]	Details
Design		
Different approach—same technology	x	CPU + hardware checker (FPGA/PLD)
Different architectures	i	Same (integrated) system architecture but different microarchitecture
Equipment (Manufacturer)		
Different manufacturer—different design	x	Application development by different organizations; Different processing equipment manufacturer
Equipment (Processing)		
Different logic processing architecture	i	CPU vs gate arrays (result of design diversity)
Different component integration architecture	–	Integrated implementation (no inherent diversity)
Different data flow architecture	–	Shared bus (no inherent diversity)

Table 3.10. (continued)

Diversity attribute	Usage[a]	Details
Functional		
Different underlying mechanisms	i	Encoded data processing vs criteria comparison (result of intentional functional diversity); Different execution mechanisms (result of design diversity)
Different purpose, function, control logic, or actuation means	x	Control vs safety purpose; Control vs checking functions; Execution by lookup of precomputed results based on encoded data vs comparative logic for signatures; Actuate track switches (or train controls) vs interrupt power for failsafe configuration
Different response time scale	i	Sequence of operations vs comparison of intermediate states against correctness criteria (result of intentional functional diversity)
Life-cycle		
Different design organizations/companies	x	Application development by different organizations (Ansaldo and UVa)
Different design/development teams (designers, engineers, programmers)	i	Inherent different in control designers/programmers for control function vs checking function (related to organization and expertise)
Different implementation/validation teams (testers, installers, or certification personnel)	–	Integrated system (no intentional diversity specified)
Logic (Software)		
Different algorithms, logic, and program architecture	x	Difference in algorithms/logic and architecture (related to technology and function)
Different timing or order of execution	–	Synchronized execution
Different runtime environment	i	Arises from technology difference (result of design diversity)
Different functional representation	i	Software language vs hardware description language (result of design diversity)
Signal		
Different parameters sensed by different physical effects	x	Measurement of process (train speed/location) vs communication of system status (controller operations and variables)
Other Diversity Considerations		
Embedded Primary-Checker architecture; Fundamentally diverse functional requirements; Formal verification of controller software	Coded processor for end-to-end control; Checker performs concurrent validation with failsafe response	

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

3.5 Summary of Nonnuclear Industry Diversity Usage

Table 3.11 summaries the diversity usage identified through the investigation of the nonnuclear industries. While specific examples may not be easily translated into the nuclear power application domain, key insights from each industry can help to inform the development of a basis for guidance on diversity usage at NPPs.

The aerospace industry tends to rely on high-quality processes to minimize the potential for CCF vulnerabilities. The use of failsafe design practices with reduced functionality backups characterizes the prime examples of safety-critical applications for manned space systems.

The aviation industry provided several examples of diversity usage, with two prominent approaches. 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. The nature of the application domain favors much different architectural approaches from what is generally employed within the nuclear power industry as well.

The chemical process industry provides guidance that is similar in nature to the nuclear power industry. However, no definitive metrics or specific diversity usage template is provided. 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 safety bag technique is seen as a key example of that approach. A more hardware-oriented approach based on encoded processors for parallel checking architectures was also seen in key examples. These diversity usage examples suggest different approaches to the system architecture approach that may warrant consideration. However, based on current architectural configurations at NPPs, careful consideration would be needed to evaluate an appropriate implementation strategy.

Table 3.11. Summary of diversity usage for nonnuclear industries[a]

Diversity attribute	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	–	–	–	–
Equipment (Processing)										
Different logic processing architecture	–	–	x	–	x	x	x	–	i	i
Different logic processing versions in same architecture	–	–	–	x	–	–	–	–	–	–
Different component integration architecture	–	–	–	–	–	–	–	–	–	–
Different data flow architecture	–	–	–	–	–	–	–	–	–	–

Table 3.11 (continued)

Diversity attribute	SS	IS	20	40	80	77	C	A	PR	LA
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 (Software)										
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 a different redundant set of similar sensors	x	–	x	x	x	–	x	–	–	–

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

Draft

4. DIVERSITY USAGE IN INTERNATIONAL NUCLEAR POWER INDUSTRY

From its inception, the commercial nuclear power industry has included layers of defense to mitigate the potential effects of failures within the structures, systems, and components of a plant, including I&C systems. The defense-in-depth concept involves echelons of defense composed of independent systems that serve as successive barriers and must fail coincidentally to result in an unsafe condition. The application of this approach encompasses all I&C systems, both safety and nonsafety, with the objective of managing the risk of core damage or radiation release beyond allowable limits. Echelons (or lines) of defense have been identified in terms of control (and limitation) systems, reactor trip systems, engineered safety feature actuation systems, and monitoring and indication systems.[7] These barriers provide prevention, termination, and mitigation capabilities through either automatic or manual means.

Nuclear safety systems provide the automatic systems for termination and mitigation. These safety systems typically employ parallel redundancy of channels or divisions with voting logic that requires majority agreement (e.g., two out of three or two out of four) to actuate the protection function in response to detection of a design basis event (DBE). Although high-quality design and implementation practices for safety systems are promoted through quality assurance regulations and Class 1E equipment requirements, the use of redundancy is maintained so that a single random failure in the safety system neither trips the plant unnecessarily nor prevents a protective action when the plant conditions require it.

By itself, the redundancy of identical channels or divisions in conventional analog-based safety systems offers no protection against a systematic fault that is common to all instances of the replicated implementation. Thus, even for well-established analog-based system designs, the potential for CCF vulnerabilities is present and is typically addressed through provision of different I&C systems to mitigate consequences if an automatic trip fails to occur (e.g., manual scram initiation and ATWS systems). These considerations have resulted in traditional usage of intentional diversity within the nuclear power industry. In fact, diversity is defined by the international nuclear power industry as the "existence of two or more different ways or means of achieving a specified objective"[11] where its usage is generally provided specifically as a defense against CCF.

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 concern is that a latent, systematic fault in the design or implementation could be present in all identical systems and result in the concurrent failure of essential safety or compensating systems during a demand. While diversity and other design measures have been traditionally coupled with high-quality practices for conventional safety systems to mitigate the potential for common design errors or defects in common components, the complexity of digital I&C components (e.g., microprocessors) and the less predictable nature of software behavior lead to greater uncertainty in demonstrating that undetected systematic faults are avoided in the design, implementation, and operation of digital safety systems. Specifically, although a great deal of effort has been applied to develop highly reliable software with extremely low failure rates, current software engineering practice has not achieved the capability to *prove* quality and reliability (i.e., "error-free" software) through testing and analysis under all credible conditions. Thus, it is accepted that the added potential for CCF vulnerabilities posed by digital I&C systems is not negligible and requires additional consideration.

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 described in Chapter 2 were developed concurrently with the first extensive applications of digital technology for international evolutionary reactors. This discussion presents the findings of the investigation into diversity usage at international NPPs through several key example cases. The context for the nuclear power application domain is established through an overview of traditional practices for the application of

diversity and a discussion of general architectural approaches for incorporating diversity in I&C systems at NPPs.

4.1 Context for Diversity in Nuclear Power I&C Systems

4.1.1 Traditional Application of Diversity for Nuclear Power Plants

Separation and redundancy, as well as physical barriers and electrical isolation, are generally employed as design measures to address potential vulnerabilities related to a single failure of equipment and the propagation of its effect. These measures tend to minimize shared components or equipment and nonessential interconnections within I&C system architectures. However, common components or functional interrelationships can also pose potential failure vulnerabilities that may challenge safety assurance. As stated in NUREG/CR-6303, "[p]hysical and electrical independence is the beginning, not the end, of common-[cause] failure concerns" since "[r]elated and almost-coincident failures of supposedly separate systems can occur because of functional interactions, shared signals, common design errors, common environmental effects, and human actions."

While design criteria primarily embody principles such as high quality, integrity, reliability, independence, and qualification, NPPs in general, and protection systems in particular, have traditionally employed diversity as a contributing factor in satisfying safety requirements. From the outset of nuclear power development, functional diversity through diverse shutdown mechanisms has been employed. For Chicago Pile #1 (CP-1), three reactor trip capabilities were provided: (1) automatic control rods, (2) a manually initiated, gravity-driven shutdown rod, and (3) manual liquid control (i.e., reactivity control by flooding the pile with a cadmium-salt solution). This form of functional diversity relates to different actuation means and different underlying methods. The use of this approach to functional diversity is incorporated within requirements concerning provision of diverse reactivity control mechanisms [cf., GDC 26].

The existence of additional requirements addressing diversity makes it clear that potential vulnerability to CCF is not specific to digital technology. In particular, the design criterion on protection system independence (GDC 22) identifies "functional diversity or diversity in component design and principles of operation" as design techniques to "be used to the extent practical to prevent loss of the protection function." Consequently, traditional application of diversity for protection and reactivity control systems has been well established for conventional hardwired I&C systems and components. The primary instances of this traditional diversity usage involve signal, functional, and equipment (e.g., sensor or actuator) diversities. Examples of technology-neutral CCF concerns include requirement flaws, hardware design errors, equipment qualification deficiencies, installation or maintenance errors, instrument loop scaling and setpoint mistakes, and so forth.

The potential for requirement flaws provides a primary motivation for the use of functional diversity. Basically, uncertainties in defining postulated initiating events (PIEs) or deficiencies in accident modeling or analysis have the potential to result in inadequate coverage of the full range of prospective safety challenges. The use of diverse functional relationships between sensed or calculated parameters (e.g., high neutron flux and overpower ΔT) and the plant conditions that correspond to specific PIEs provides alternate criteria for initiating a safety response. As noted in Chapter 2, the IEC definition of functional diversity emphasizes this aspect of the CCF coping characteristics for this diversity attribute by citing an example of diverse actuation initiation criteria (i.e., "trip activation on both pressure and temperature limit"[11]). Thus, traditional usage and international consensus recognize that functional diversity can help mitigate the potential for CCF vulnerabilities that may arise from requirement deficiencies or uncertainties regarding detection and response actuation for PIEs.

Functional diversity of this type is feasible where diverse measurements are available to support establishment of more than one actuation initiation criterion corresponding to a specific PIE. Consequently, signal diversity supports functional diversity through measurement of different parameters

with correlated physical relationships (e.g., pressure and level measurements for confirming coolant system integrity). Signal diversity also minimizes commonalities in signal sources to mitigate the potential impact associated with either the loss of shared sensors or common failure of a measurement type. The use of signal diversity includes (1) measurement of different parameters by different physical effects, (2) measurement of different parameters by the same physical effect, and (3) measurement of the same parameter by redundant, physically separate similar sensors. The first two of these signal diversity criteria involve the interrelation of physical processes to provide diverse indication of plant conditions (particularly PIEs) and to provide alternate measurements of vital parameters. The feasibility of specific signal diversities is dependent on the plant design and available measurement technologies. The third criterion primarily relates to separation of equipment to avoid potential CCF vulnerabilities from shared components or environments, although there can be some diversification benefit to the modest differences in signal trajectory that can be gained through the variations present in separate measurements of stochastic phenomena (i.e., data diversity).

This use of a parametric diversification approach is common within the nuclear power industry. In the United States, the combination of functional and signal diversities has traditionally been used as a contributing approach to satisfy the requirements of GDC 22. As the findings presented in this chapter confirm, this CCF mitigation approach is also prevalent in the application of diversity at international NPPs. The transition to digital I&C systems, in particular for the implementation of safety systems, does not obviate the importance nor minimize the value of the traditional usage of diversity. Specifically, the capability to provide a diverse means for accomplishing similar or compensating functions is facilitated by application of signal and functional diversity to enable diverse measurements and different initiation criteria. As discussed above, this diversity approach is an effective means for addressing long-standing concerns about the potential for CCF vulnerabilities that are not limited to software-based safety systems.

At the system level, functional diversity contributes to reducing the potential for common mistakes, misinterpretations, and errors by the designers and implementers of each system by providing some diversification of functional requirements and differences in the functions (e.g., relationships, algorithms, logic) to be implemented. In effect, diverse safety function initiation criteria correspond to diversified requirements that are captured through different functional expressions, thereby facilitating differences in the functions and control logic assigned to each diverse system. The impact of this diversification is to minimize the potential for common systematic faults. In addition to enabling functional diversity, signal diversity reduces commonalities between systems. Regarding potential CCF vulnerabilities associated with digital technology, an additional benefit from the combined use of these diversities (i.e., functional and signal) arises through the reduced likelihood of common signal trajectories. This effect results from the different input patterns presented to diverse systems that implement different combinations of functional or logical relationships. Thus, the prospect of concurrent execution profiles is minimized.

4.1.2 Architectural Approaches

The investigation of diversity usage in the nuclear power industry primarily focused on the use of diversity at the system level, with an emphasis on approaches to address the potential for CCF vulnerabilities associated with digital safety systems. As discussed above, CCF vulnerability is not unique to a particular technology and diversity usage practices have been developed in an effort to address technology-neutral concerns. These practices are consistent with the architectural conventions that have developed within the nuclear industry. Although different architectures are seen in other industries (e.g., the primary-checker architectures of the aviation and rail transportation industries), the differences in the nature of the application domains (e.g., range of demands, frequency of action, implementation and operational constraints, regulatory requirements, etc.) complicate any direct translation of those approaches to nuclear power usage. Additionally, the architectural approach for I&C systems at NPPs most strongly relates to defense in depth and thus is treated here as a context for diversity rather than a consequence of diversity.

As seen in the NPP examples cited below, the application of diversity in the nuclear power industry involves some systematic subdivision of protection or compensating functions into versions A and B that represent different systems, redundancies, subsystems, or modules (including software). Some means of implementing compensating functionality through diversification is provided for each digital safety system cited in the examples, but there are differences in overall approach. The architectural context for diversity usage can be grouped into three general categories: coequal diverse safety systems, primary and secondary diverse systems, and functionally diverse subsystems.

4.1.2.1 Coequal Diverse Safety Systems

In this architectural approach, diversity is achieved between two separate safety systems that provide equivalent protective action. This approach is illustrated in Figure 4.1. 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 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, etc.).

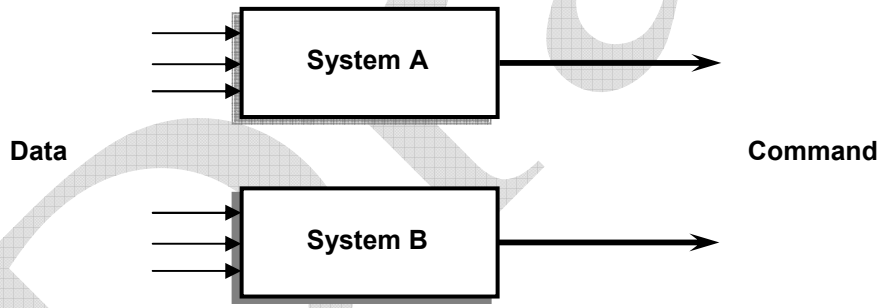

Figure 4.1. Coequal diverse safety systems.

4.1.2.2 Primary and Secondary Diverse Systems

This architectural approach 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 4.2 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 (e.g., 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

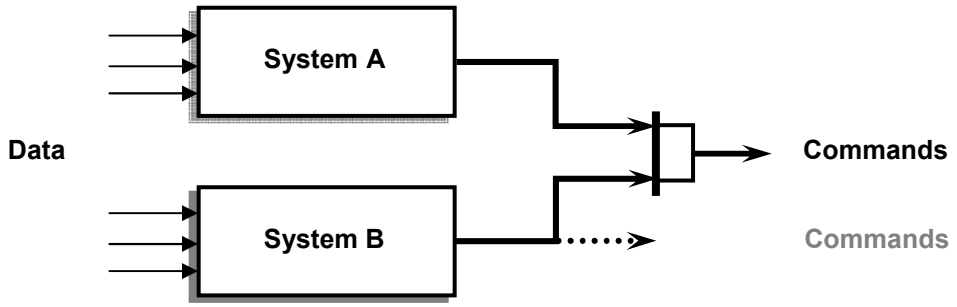

Figure 4.2. Primary and secondary diverse systems.

PIEs and/or the safety classification. Specifically, the secondary system may only provide backup safety or compensating functions for high-frequency DBEs, such as anticipated operational occurrences (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 non-safety 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.

4.1.2.3 Functionally Diverse Subsystems

The prior discussion on traditional diversity usage described the strategic use of functional diversity combined with signal diversity. This usage is recognized as a particularly effective coping strategy for CCF vulnerabilities attributed to sources such as requirements deficiencies. This diversification can be applied alone within a single safety system or in conjunction with the other architectural approaches presented previously. The unique characteristic of functionally diverse subsystems is that two diverse versions are implemented as subsystems rather than separate systems. Thus, although the diverse versions may be separated on different modules, chassis, or even cabinets, they will retain some commonality by the nature of the approach. For example, it is likely that the subsystems will be supplied by the same development organization using the same platform. Even where different development teams are intentionally used for the implementation of the subsystems, there will be commonality of the platform developers and likely some commonality of the system implementers, testers, and installers of the integrated system.

Figure 4.3 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 subsystems type (i.e., A1, A2, etc., or B1, B2, etc.) are voted to determine the resultant safety decision for the individual line of protection (e.g., 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.

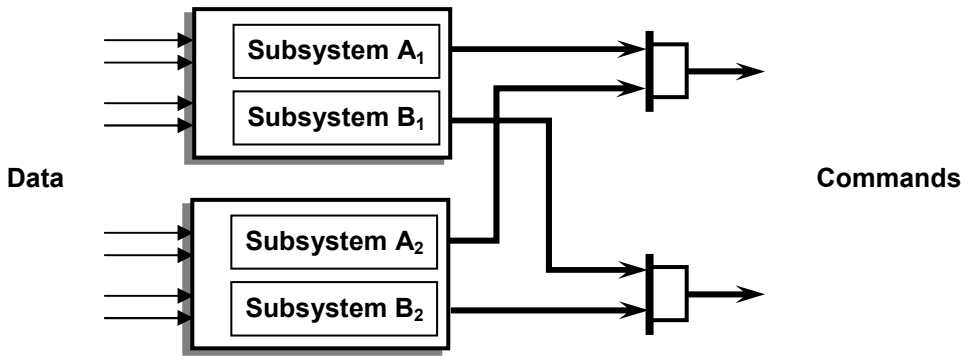

Figure 4.3. Functionally diverse subsystems.

4.2 International Nuclear Power Diversity Strategies

This section presents the specific findings from the investigation into diversity usage at selected international NPPs. The examples that are described represent a sampling of evolutionary reactors and modernized plants that employ digital technology extensively. In particular, five 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, and Temelín. 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.

The information presented in this section is derived from available published information and discussions with cognizant sources. The main references are reviews of digital safety systems that discuss the implementations in general but do not necessarily emphasize the diversity aspect of those I&C architectures in detail. It is recognized that more extensive information on the designs and more detailed descriptions of the licensing assessments of these diverse systems could be gleaned from proprietary sources on the designs and internal licensing reviews by the national and international regulatory agencies. However, restrictions on reporting such information compromise its value for this report. Thus, efforts to enhance the information extracted from the published sources included follow-up inquiries where points of contact could be identified and discussions with technical experts at international meetings. One objective of this report is to assemble this information from the variety of public sources and capture it in a summary record.

4.2.1 Darlington (Canada)[93,94]

The Darlington Nuclear Generating Station is the site of four Canada deuterium-uranium (CANDU) reactors supplied by Atomic Energy of Canada, Ltd. (AECL). Units 1 and 2 were commissioned in 1990 as the first CANDU plants to employ “fully” digital I&C systems. There are two diverse digital shutdown systems within each unit at Darlington, with each capable of independently shutting down the reactor in response to detection of any PIE. Thus, the Darlington architectural approach for diversity usage corresponds to coequal diverse safety systems.

The two shutdown systems, designated as Shutdown System Number 1 (SDS1) and Shutdown System Number 2 (SDS2), are functionally independent and physically separate from each other, and from the plant control systems that support normal operation. Specifically, functional independence between the shutdown systems is provided through the use of different means for safety actuation based on diverse physical principles: mechanical (solid) shutoff rods for SDS1 and direct liquid poison injection into the moderator for SDS2. Where feasible, each shutdown system has two diverse trip parameters corresponding to each PIE. Thus, additional functional diversity is provided internally within each

system through diverse actuation initiation criteria as well as between shutdown systems through the diverse actuation mechanisms. Diverse trip parameters are available between shutdown systems in a few cases (e.g., low flow and low Δp for loss of flow events). Separate sensors are used for each shutdown system, and where feasible, diverse measurements are employed for the same parameter (e.g., in-core neutron flux).

Figure 4.4 shows the architectural arrangement of computers for SDS1 and SDS2. Each shutdown system contains three physically separate but identical divisions composed of trip computers. The inputs to each trip computer consist of measured parameters and test signals/commands, while the outputs are trip signals and display data. Communication links shown as dotted lines are normally disabled by hardware interlocks. The human-system interfaces and monitoring computers are also shown on the figure, including the Display/Test computers for each division with their associated video display units.

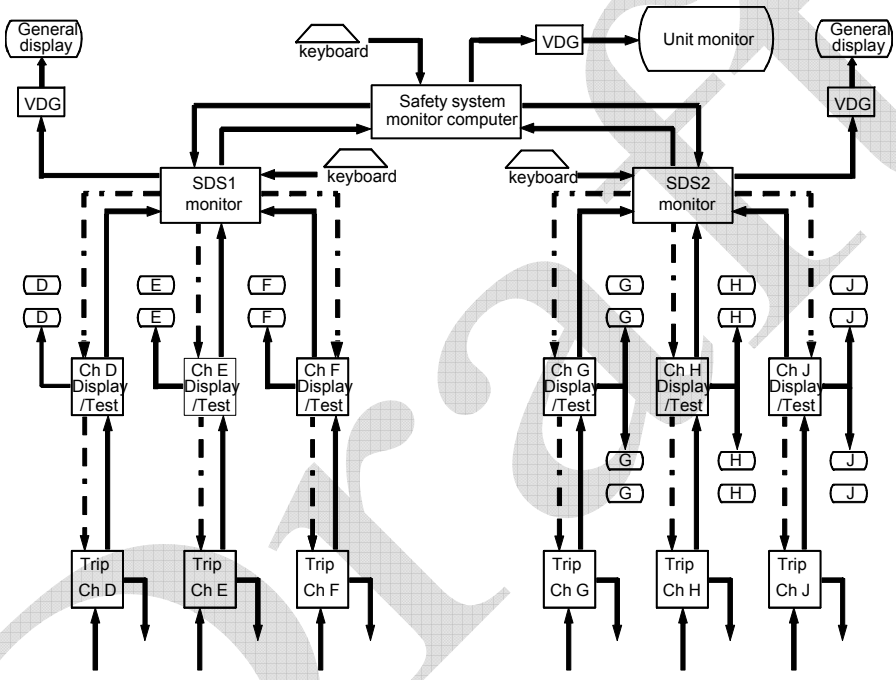

Figure 4.4. Fully computerized shutdown system.

Redundancy in the form of duplication, triplication, and division voting are used to address single failures. Initiation of shutdown action is based on two-out-of-three coincidence among division trip decisions within a shutdown system. SDS1 depends on general coincidence among divisions for trip voting (i.e., two divisions indicating trip without regard to correspondence between the particular actuation initiation criterion), while SDS2 employs local coincidence among divisions for software-based division trip voting (i.e., two divisions indicating trip for the same actuation trip criterion). Final system trip voting is performed with relay logic.

The diversity established between SDS1 and SDS2 begins with the use of computers from different manufacturers as the base platform for each system. The two platforms are based on different computer chip families and have different board layouts. Additionally, development of each system employed separate compilers, computer languages, and development software and was accomplished by different development teams. Specifically, SDS1 uses General Automation (GA) Model 220 machines (based on the GA-16/220 microprocessor) with the application software programmed in FORTRAN and GA assembler. The trip computers for SDS2 are Digital Equipment Corporation (DEC) Programmed Data Processor (PDP) computers based on the LSI-11/23 microprocessor, and the application software is programmed in Pascal and MACRO assembler. All three divisions within a shutdown system contain

identical software (except for division identification), but as noted, the software for each shutdown system is different. Table 4.1 provides a summary of diversity usage for Darlington.

Table 4.1. Summary of diversity usage for Darlington

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two shutdown systems based on different microprocessors
Equipment (Manufacturer)		
Different manufacturer—same design	x	General Automation for SDS1, DEC for SDS2
Equipment (Processing)		
Different logic processing architecture	x	GA-16/220 CPU for SDS1 and LSI-11/23 CPU for SDS2
Different component integration architecture	x	Different circuit board designs for GA Model 220 and DEC PDP-11/23
Functional		
Different underlying mechanisms	x	CANDU reactors have two separate, diverse mechanisms for shutting down the reactor [absorber rods vs borated water]
Different purpose, function, control logic, or actuation means	x	Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used to the extent possible within each shutdown system and, in limited cases where feasible, between shutdown systems; Different coincidence logic is used for voting (general vs local); Different actuation means are provided [spring-assisted rod insertion vs pressurized liquid poison injection]
Different response time scale	x	Differences in mechanisms provide distinction in response time; Either system can shutdown reactor in less than 2 seconds
Life-cycle		
Different management teams within same company	x	Separate teams established within AECL to develop diverse systems based on different platforms using different tools
Different design/development teams (designers, engineers, programmers)	x	Different personnel for each team
Different implementation/validation teams (testers, installers, or certification personnel)	x	Different personnel for each team

Draft

Table 4.1 (continued)

Diversity attribute	Usage[a]	Details
Logic (Software)		
Different algorithms, logic, and program architecture	x	Some algorithmic differences due to limited functional diversity between shutdown systems; Program architecture differences arising from different developers and development tools; Software-based local coincidence voting provided for SDS2 divisions
Different runtime environment	x	Platform-specific runtime environment
Different functional representation	x	SDS1 programmed in FORTRAN and GA assembler while SDS2 programmed in Pascal and MACRO assembler; Different compilers were also used
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within each shutdown system
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within each shutdown system and, in limited cases, between shutdown systems (e.g., for loss of flow events)
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between shutdown systems and between divisions within each shutdown system
Other Diversity Considerations		
Coequal diverse safety systems	SDS1 and SDS2 provide protection against all DBEs and have separate, diverse actuation means based on diverse shutdown mechanisms	

[a]Intentional diversity (x).

4.2.2 Sizewell (United Kingdom)[95–99]

The Sizewell B Nuclear Power Station is the only pressurized-water reactor (PWR) in the United Kingdom (UK). The Sizewell PWR, supplied by Westinghouse, began commercial service in 1995. The characteristic that distinguished Sizewell from most other PWRs at the time was its extensive use of digital I&C technology. In fact, Sizewell is the first plant at which the Westinghouse Integrated Protection System (IPS) was installed. The IPS architectural approach provides an integrated structure of microprocessor-based subsystems using the Westinghouse Eagle series platform. Features such as the safety functions that are supported, the configuration of safety divisions into quadruple redundancies (designated as guardlines), and the provision of two-out-of-four voting logic are generally the same as those found in conventional analog safety systems at other Westinghouse PWRs. The primary distinction for Sizewell is that it was commissioned with control and safety system implementations based on microprocessor technology and digital data links (e.g., networks or optical fiber links). Thus, the Sizewell B plant serves as a pioneering example of the continuing trend toward more highly integrated digital I&C systems.

Sizewell represents the use of primary and secondary diverse systems to address CCF concerns. However, as described below, functionally diverse subsystems are also employed within the digital

primary protection system (PPS). The PPS implements the reactor trip and engineered safety feature (ESF) functionality needed to respond to the full range of DBEs. A diverse secondary protection system (SPS) based on hardwired modules is also provided. As is the case for the PPS, the SPS is arranged in quadruple-redundant guardlines to enable two-out-of-four voting. Both systems are assigned to the highest safety class, and no communication interconnection is permitted between them.

At the time Sizewell was designed and the licensing process was initiated, concern over CCF vulnerability attributed to software was emerging in the international nuclear power industry. As a result, several design measures, including diversity, and various regulatory review approaches were actively discussed to resolve the potential threat posed by digital CCF. To resolve the outstanding issues, the Nuclear Installations Inspectorate (NII) within the UK Health and Safety Executive (HSE) employed a special case procedure using a risk-based safety analysis for software-based systems. A principal outcome of the risk-based regulatory assessment was the requirement for a SPS to provide alternate protection for high-frequency events (i.e., greater than 10^{-3} events per year). Thus, the SPS is only credited in the safety case for the licensing of Sizewell as a diverse backup for safety functions corresponding to a reduced set of PIEs (i.e., high-frequency events).

An additional determination of the risk-based regulatory assessment was that the SPS must employ thoroughly diverse protection technology to sufficiently reduce the risk contribution associated with a common fault in the system requirements or software design and thereby achieve the required safety goals. To satisfy this requirement, Laddic technology, which had been developed for use in protection systems at British gas reactors, was selected as the basis for the Sizewell SPS. Basically, a SPS guardline is composed of analog trip units for signal processing and Laddic modules for safety actuation voting.

Laddic devices perform logic calculations using pulsed currents through magnetic cores. The underlying physical mechanism for Laddic logic processing is clearly fundamentally diverse from logic processing based on integrated circuit electronics. Additionally, given the long history of operation for these devices in Magnox and advanced gas-cooled reactors (AGRs), Laddic hardware had a well-documented reliability record in nuclear applications in contrast to the very limited experience with digital technology at the time.

Other factors that favored the selection of Laddic logic as the basis for the Sizewell SPS relate to the inherent diversities that arise from the difference in the nature of the technologies. Essentially, the design methods and implementation tools for Laddic and microprocessors are very dissimilar, and the necessary expertise and skill sets lead to significant differences in the personnel that are appropriate for either development team. In particular, British Energy and GEC [General Electric Company plc, now Babcock Nuclear Services (BNS)] developed the SPS while Westinghouse supplied the remainder of the I&C systems for the Sizewell nuclear steam supply system (NSSS), including the PPS.

Several aspects of the traditional diversity usage that are described earlier in this chapter were also incorporated into the Sizewell protection systems. For example, Westinghouse implemented functionally diverse subsystems as part of the digital PPS at Sizewell. Specifically, more than one parameter measured by different types of sensors was identified to cover each PIE. Two alternate groupings of these actuation initiation criteria were assigned to separate subsystems, each of which consists of dedicated computing resources and input/output electronics.

In each of the four guardlines (i.e., divisions), two sets of functionally diverse subsystems were established, with one set corresponding to the two diverse groupings of termination functions (i.e., reactor trip) and the other set providing the two diverse grouping of mitigation functions (i.e., ESF). Keeping termination and mitigation functions separate is intended to ensure that the echelons of defense remain distinct. Figure 4.5 illustrates the separation of functionally diverse subsystems for the reactor trip and ESF within one guardline.

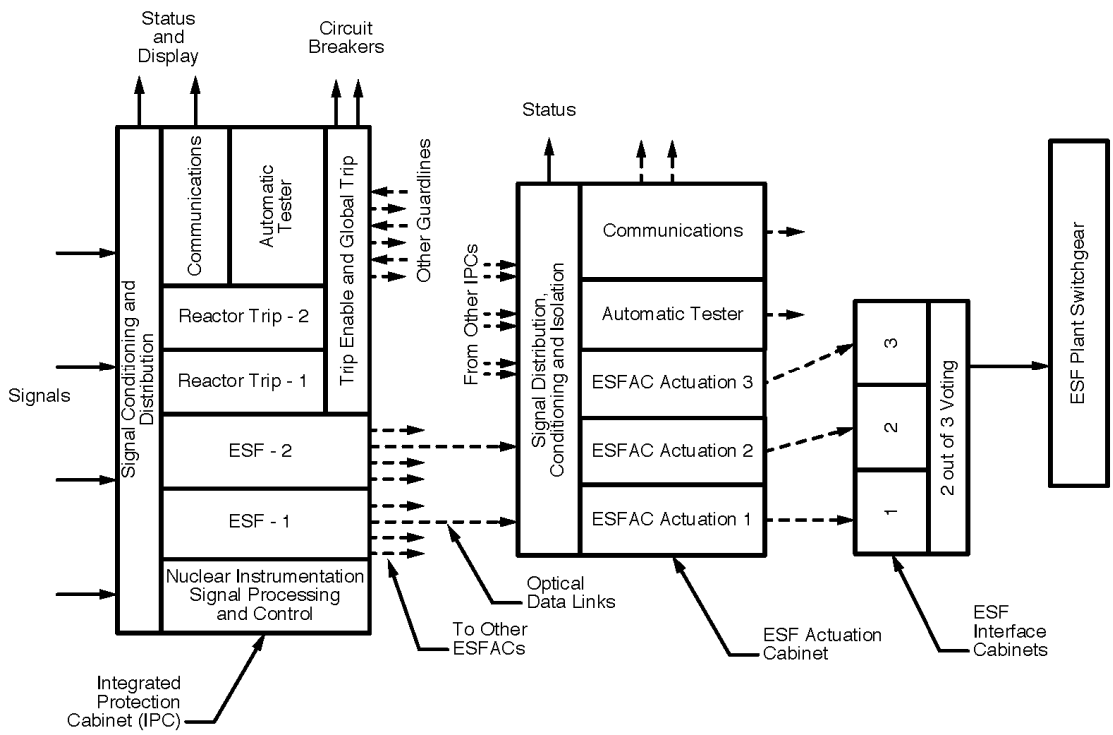

Figure 4.5. Functionally diverse subsystems for Sizewell PPS. (Adapted from Ref. 97.)

Correspondingly, diverse sensors are provided in the plant design to enable the functional diversity. Additional signal diversity is provided between the PPS and SPS with the selection of sensors from different vendors for each system. Similarly, different vendors were used to supply the reactor trip breakers associated with each protection system. In addition to the eight breakers that are configured in pairs to give two-out-of-four general coincidence logic for reactor trip, the SPS can also remove power from the rod control system bus as a backup means of tripping the reactor. Table 4.2 provides a summary of diversity usage for Sizewell.

Other features of interest for the Sizewell I&C architecture include command prioritization, application of failsafe principles, signal selection for shared measurements, and digital platform differences for protection and control. Sizewell contains some safety actuation equipment (e.g., valves) that can receive control commands from the PPS, the SPS, and the High-Integrity Control System (HICS). As a result, relay-based "priority" interfaces to safety components are employed to arbitrate among commands that originate in the different systems. The logic is based on achieving a safe state in the presence of conflicts.

To better cope with component failures at the system level, the Laddic logic modules can be configured to fail to a preferred state on loss of power. Thus, a failsafe design was implemented for the SPS in which a known safe "failed" state is established by design. For the PPS, watchdog timers and self-diagnostics are included to detect faulted states and enforce a known state as the fault recovery action. Determining the efficacy of this digital failsafe solution depends on the confidence that can be achieved through a systematic assessment of whether the self-diagnostics are comprehensive and without faults of their own.

Table 4.2. Summary of diversity usage for Sizewell

Diversity attribute	Usage[a]	Details
Design		
Different technologies	x	Two protection systems based on diverse technologies [Microprocessor vs Laddic (magnetic-core-based logic)]
Different architectures	i	Inherent difference in system architectures due to technology diversity
Equipment (Manufacturer)		
Different manufacturer—different design	x	Westinghouse supplied IPS/Eagle for PPS, while British Energy/GEC provided Laddic-based SPS
Equipment (Processing)		
Different logic processing architecture	i	Inherent architectural difference in processing elements due to technology diversity; PPS based on Intel 80286 CPUs and SPS based on Laddic logic modules
Different component integration architecture	i	Inherent difference in component integration resulting from different technologies for PPS and SPS
Different data-flow architecture	i	Inherent difference in data-flow architecture resulting from different technologies for PPS and SPS
Functional		
Different underlying mechanisms	i	Inherent difference in mechanisms for accomplishing function due to technology diversity
Different purpose, function, control logic, or actuation means	x	Purpose of SPS is to protect against high-frequency events (10^{-3} events/year), so SPS provides reduced functional coverage of DBEs vs PPS; Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used in subsystems of PPS; Diverse actuation means provided by SPS (i.e., remove power from rod control system bus)

Draft

Table 4.2 (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different design organizations/companies	x	Different companies developed and supplied the diverse systems (Westinghouse vs British Energy/GEC)
Different design/development teams (designers, engineers, programmers)	i	Different personnel for each company
Different implementation/validation teams (testers, installers, or certification personnel)	i	Different personnel for each company
Logic (Software)		
Different algorithms, logic, and program architecture	i	Inherent difference in logic/function instantiation (e.g., structure of logic) due to technology diversity
Different timing or order of execution	i	Inherent difference in logic/function execution due to technology diversity
Different runtime environment	i	Inherent difference in logic/function execution due to technology diversity
Different functional representation	i	Inherent difference in logic/function instantiation due to technology diversity
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within each protection system
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within each protection system
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between protection systems and between divisions (guardlines) within each protection system
Other Diversity Considerations		
Primary and secondary diverse safety systems with functionally diverse subsystems within the primary safety system; Diverse actuation and measurement equipment for each protection system; Priority module to arbitrate between commands from different to the same safety equipment; Failsafe state implemented for secondary system	Both systems are quadruple redundant and safety grade, but SPS has reduced functionality (i.e., covers limited set of PIEs); Trip breakers and sensors for each protection system are separate and supplied by different manufacturers; Relay logic prioritization at device-level among some commands from PPS, SPS, and control system; Laddic logic configured for safe state on failure/loss of power	

[a]Intentional diversity (x), inherent diversity (i).

Draft

To promote a failsafe reactor trip interface, a dynamic trip bus was developed to provide dynamic logic units corresponding to each trip parameter. The bus is designed to fail to a safe state if a continuous stimulus is removed due to failure (i.e., the breakers trip unless they remain actively energized).

Westinghouse practice is to utilize protection system measurements to support reactor controls. Sharing of these signals is achieved through unidirectional optical serial data links to ensure direct electrical and functional isolation of the protection system from effects propagating back through the data link. Functional filtering of the data to guard against propagation of failures from the protection system to the control system is provided by dual redundant signal selector subsystems that perform data validation/rejection.

The PPS for Sizewell is implemented on the Westinghouse Eagle 2000 platform, while the HICS is implemented on IPS and Integrated Control System (ICS) hardware. HICS provides automatic control for the NSSS, manual control of safety components, and data management for safety displays. The PPS is based on the Intel 80286 microprocessor, while the HICS CPUs are Intel 80386 microprocessors. Balance-of-plant control is implemented using the Westinghouse Distributed Processing Family (WDPF) platform, which also is based on the Intel 80286 microprocessor. The hardware architecture for each computer subsystem uses the Multibus I internal data bus. The PPS application software was primarily implemented using a high-level structured program language. Use of assembly language was avoided except where required by timing or hardware interface constraints. For the Sizewell PPS, PL/M-86 was the software language employed.

4.2.3 Chooz B (France)[95,100–102]

The Chooz B Nuclear Plant Unit 1, commissioned in 1996, is the prototype of the standardized N4-class PWRs supplied by Framatome (now AREVA NP). The microprocessor-based safety system for N4 reactors was jointly developed by Framatome, Electricité de France (EdF), and Schneider Electric/Merlin Gerin (now Data Systems and Solutions—DS&S) and is designated as version two of the Système de protection intégré numérique (Integrated Digital Protection System—SPIN). Diverse compensating functions to back up the safety system for a limited set of PIEs are provided by the Class 2E (i.e., safety-related) ATWS system. Thus, Chooz employs a primary and secondary diverse system architectural approach for CCF mitigation. Additionally, functionally diverse subsystems are employed within the primary safety system.

At the system level for automatic control and protection, the reactor protection system (SPIN) is grouped within the Class 1E CO3 system (COntrôle-COmmande COuer or I&C system for the reactor core), which also contains the nuclear instrumentation system and the control rod drive system. The safety support systems are provided by the Class 1E CS3 system (Contrôle des Systèmes Support de Sauvegarde or safeguards control system) and SCAP system (Système de Contournement à l'AtmosPhère or containment atmospheric control system). General automation is provided by SCAT (Systèmes de Commande des Auxiliaires de Tranche or reactor auxiliary systems control), which is implemented on the Contronic-E platform supplied by Hartmann and Braun (H&B). The Class 2E ATWS functions are incorporated into SCAT.

As noted, the SPIN system is the primary safety system that provides the reactor trip and emergency cooling functions. It consists of four divisions of measurement and calculation equipment and two trains of redundant logic equipment. Figure 4.6 illustrates the configuration of the system. Each division contains multiple processors. In particular, the ensemble of two acquisition units (UA) and five functional units (UF) constitutes the Acquisition and Processing Unit for Protection (UATP). In general, the measurements are quadruple redundant with each sensor set being connected to one of the four divisions. Within each of the divisions, two acquisition unit processors (UA1 and UA2) acquire the signals. Signals are distributed from the acquisition units to five functional unit processors (UF1 through

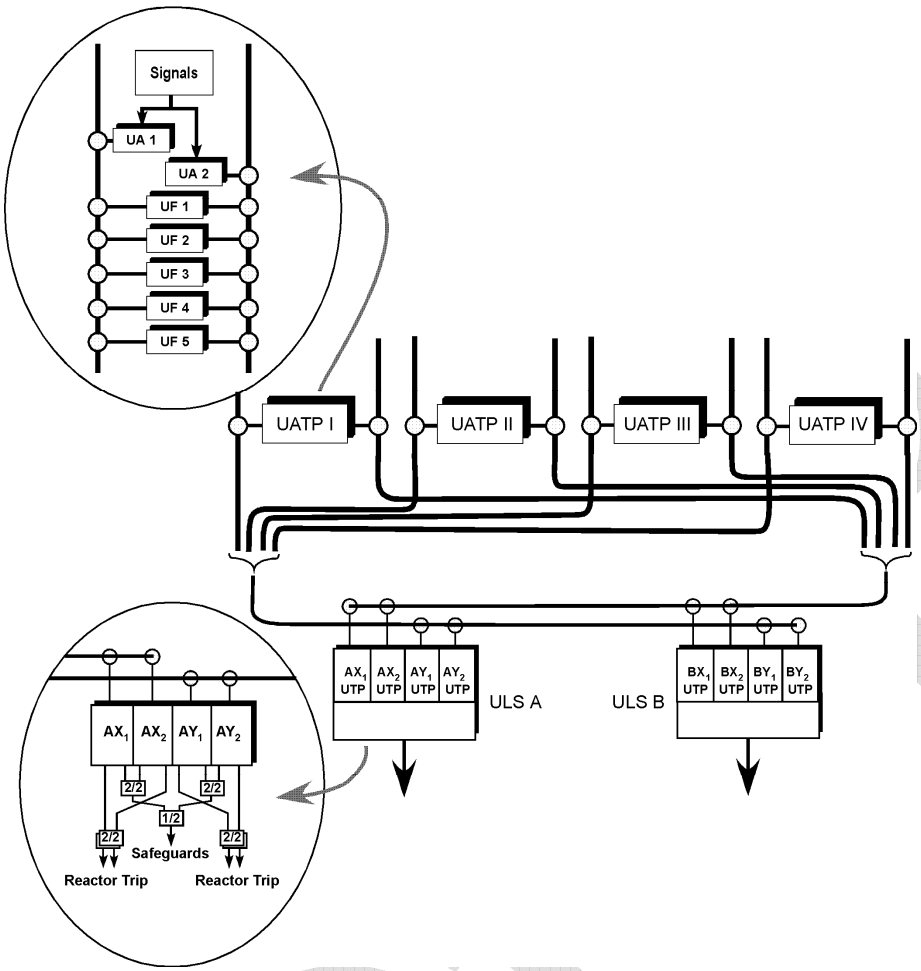

Figure 4.6. SPIN architecture. (Adapted from Ref. 101.)

UF5) using two separate, redundant protection data networks (called NERVIA). The functional units perform the required "partial trip" determinations.

Trip data from the UATP of each division are transmitted across redundant, isolated branches of the protection data network for distribution to the two trains. These data from each division are collected and retransmitted on two separate protection networks supporting the Logic Safeguard Unit (ULS) associated with each train. Thus, there are ten protection data networks consisting of eight UATP networks (two per division) feeding into two ULS networks (each collecting data from one set of four divisional UATP networks).

Each ULS train (A or B) contains four logic processors (UTPs) that are divided into two pairs (X or Y). Each pair is connected to a different ULS protection network. Based on the trip data from the UATPs, the ULS performs two-out-of-four specific coincidence logic and safety features system level logic. Basically, the SPIN system provides two-out-of-four voting for reactor trip. For emergency core cooling actuation, a logical operation is included that provides an "OR" operation between dual two-out-of-two voters. In both cases, the SPIN design provides protection against a single failure.

Table 4.3 provides a summary of diversity usage for Chooz. As noted above, the N4 design provides ATWS functions in the SCAT system to provide protection against high-frequency events should the SPIN system fail. The ATWS functions are treated as Class 2E, so the system adheres to enhanced quality requirements. The probabilistic safety analysis for the N4 plant showed that loss of secondary

Table 4.3. Summary of diversity usage for Chooz

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two systems (safety and ATWS) based on different microprocessors
Equipment (Manufacturer)		
Different manufacturer—same design	x	SPIN by DS&S vs Contronic-E by H&B
Equipment (Processing)		
Different logic processing architecture	x	Motorola 68000 for SPIN vs Intel 80286 (with an Intel 80287 co-processor) for Contronic-E
Functional		
Different purpose, function, control logic, or actuation means	x	Purpose of ATWS with SCAT is to protect against high -frequency events (10^{-3} events/year), so the diverse Class 2E backup system provides very reduced functional coverage of DBEs than that provided by the primary Class 1E safety system; Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used in subsystems of SPIN; Redundant trains with separate communication paths are provided for safety component actuation
Life-cycle		
Different design organizations/companies	x	Different companies developed and supplied the diverse systems (DS&S vs H&B)
Different design/development teams (designers, engineers, programmers)	i	Different personnel for each company
Different implementation/validation teams (testers, installers, or certification personnel)	i	Different personnel for each company
Logic (Software)		
Different algorithms, logic, and program architecture	x	Algorithmic and logic differences between diverse systems due to limited scope of ATWS (i.e., reduced functionality with some use of different relationships); Functionally diverse subsystems within primary safety system provide algorithmic and architectural differences as well as logic differences between trains

Draft

Table 4.3 (continued)

Diversity attribute	Usage[a]	Details
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within SPIN subsystems
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within SPIN subsystems
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between diverse systems and between divisions within SPIN
Other Diversity Considerations		
Primary and secondary diverse systems with functionally diverse subsystems within the primary safety system; Diverse measurement equipment for each system; Priority module to arbitrate between systems commanding safety equipment	Primary system is quadruple redundant safety system, while secondary (backup) system is lower-safety-class ATWS system that provides reduced functionality (i.e., covers very limited set of PIEs); Separate signals for primary and backup systems; Separate signals among divisions of safety system but common redundant network links for diverse sensor and trip signals associated with functionally diverse subsystems within division; Relay logic prioritization at device level among some commands from safety and control systems	

[a]Intentional diversity (x), inherent diversity (i).

feedwater is particularly important in the event of SPIN failure, so an ATWS protection signal based on low-steam-generator level was implemented. Thus, the ATWS scope offers very limited coverage against the full range of PIEs addressed by the safety system. Consequently, the ATWS system constitutes a reduced functionality backup system where the ATWS and safety systems have a different purpose and utilize different functions and logic. Since SCAT, specifically ATWS, and SPIN command some common actuation equipment, priority logic is implemented to arbitrate among these signals, including manual actuation initiation signals. The priority logic is implemented using relays.

Regarding the implementation of the two diverse systems, the DS&S SPIN platform, which is based on the Motorola 68000 microprocessor, serves as the Chooz safety system. The H&B Contronic-E platform used for the ATWS system employs the Intel 80286 microprocessor with an Intel 80287 co-processor. The software for SPIN was written in C, while a proprietary graphical programming language was used for ATWS. It is not known whether this language involved function blocks that may have been written in C or generated C code, so this form of diversity cannot be confirmed.

Finally, additional diversity is provided within the Chooz safety system through the traditional application of functional and signal diversity to provide diverse actuation initiation criteria corresponding to each DBE. The diverse functions are distributed within each division by function among the five UF microprocessors within each divisional UATP, with each unit responsible for one or more protection functions. Consequently, the algorithms and program architecture among these units incorporate some differences.

4.2.4 Kashiwazaki-Kariwa 6 and 7 (Japan)[100,103,104]

Units 6 and 7 of the Kashiwazaki-Kariwa Nuclear Power Station (KK-6/KK-7) are the first operating advanced boiling-water reactors (ABWRs). The units were constructed by Hitachi, Toshiba, and General Electric (GE). GE supplied the turbine/generators for both units, while Hitachi and Toshiba alternated by unit as the lead contractors for either the NSSS or the balance-of-plant (BOP) systems. Toshiba supplied the control and safety systems for the KK-6 NSSS, while Hitachi supplied those I&C systems for KK-7. Commercial operation of KK-6 began in 1996 and KK-7 connected to the electric grid in 1997.

The I&C systems for NSSS control and protection throughout either KK-6 or KK-7 are implemented on a common microprocessor-based platform using a similar software development environment (e.g., design methods, implementation tools, symbolic language). The protection and control systems of KK-6 were implemented on Toshiba Microprocessor Aided Power System Control (TOSMAP) platforms, which are based on Intel microprocessor-family CPUs, while the KK-7 systems were implemented on Hitachi Integrated Autonomic Control System (HIACS) platforms, which are based on Motorola microprocessor-family CPUs. The application of diversity at KK-6/KK-7 most closely corresponds to an architectural approach based on a primary safety system and secondary backup system. In this case, the backup capabilities are provided by ATWS functionality and manual controls.

Figure 4.7 shows an overview schematic of the I&C systems at KK-6/KK-7. Safety functions are implemented in the reactor protection system (RPS) and emergency core cooling system (ECCS). Each safety system consists of four redundant divisions and employs two-out-of-four voting. Anticipated transient without scram mitigation logic drives the automatic Reactor Pump Trip (RPT) and Alternate Rod Injection (ARI) system as an alternate shutdown means using analog circuits. Automatic control for NSSS systems is provided by I&C systems such as the rod control and information system (RC&IS), recirculation flow control system (RFC), feedwater flow control system (FWC), and automatic power

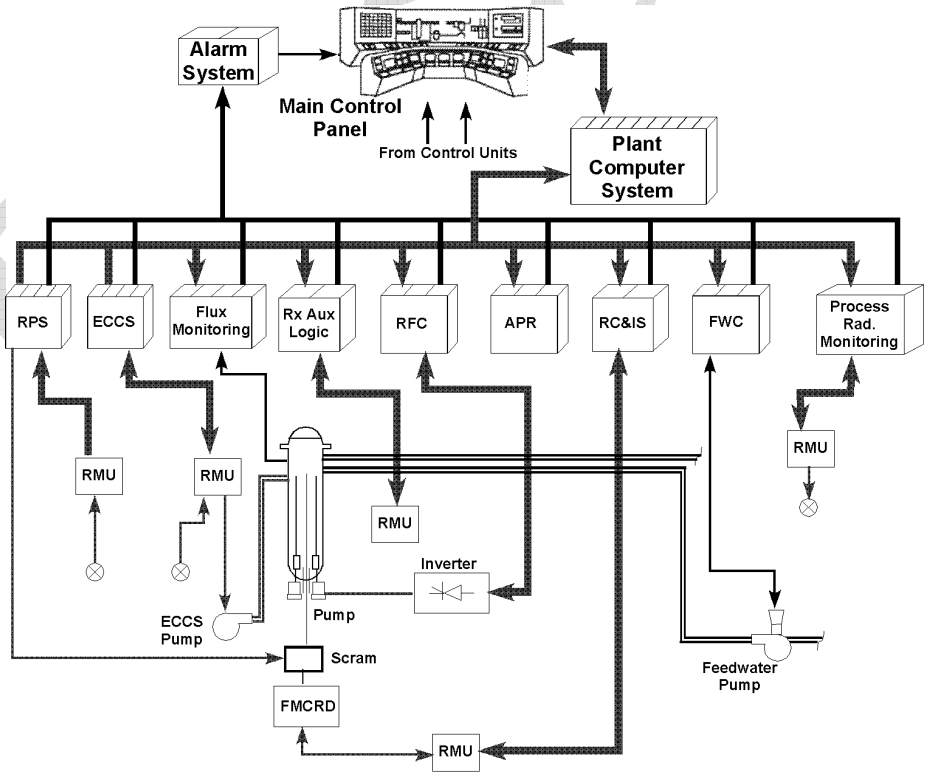

Figure 4.7. Overview of Kashiwazaki-Kariwa I&C systems. (Adapted from Refs. 100 and 103.)

regulator (APR). In the figure, communication links correspond to multiplexed connections (thick lines) or hardwired cables (thin lines) where optical multiplexing of field data is performed by remote multiplexing units (RMUs).

In Japan, the application of digital technology in NPPs progressed systematically from auxiliary systems, dedicated control loops, and monitoring systems in the 1980s to non-safety control systems and then safety systems in the 1990s. The long-term experience gained by the Japanese nuclear power industry from this phased introduction of digital technology is credited through confidence in the efficacy of consensus practices (e.g., design measures and software qualification)[105] to reduce the potential for software CCF vulnerability. In particular, a symbolic language (Problem Oriented Language—POL) is used to provide an intuitive structured representation of the software specifications (interlock block diagrams) that is implemented through graphically driven coding tools. Additionally, simplicity of software structure is promoted through simple logic, periodic execution, static resource usage, and avoidance of external interrupts. Thus, the Japanese nuclear power industry emphasizes consensus software development practices that are intended to facilitate software verification and validation as a primary means for minimizing the potential for systematic software faults.

As noted above, traditional diversity approaches are incorporated in Japanese NPPs. In KK-6/KK-7, diversity across lines of defense (RPS, ECCS, automatic control) results from the different purpose and functional relationships that are the bases of each system. Functional diversity is also provided through diverse means for safety actuation. Specifically, the RPS has three reactor shutdown initiation mechanisms (i.e., two ways to depressurize scram accumulators and a fast actuation mode for electric control rod drive mechanism) and the ECCS has two high-pressure injection systems (i.e., the high-pressure core flood system and the reactor core isolation cooling system) as well as one low-pressure flooding system. An automatic depressurization system is also provided to transition to low pressure should a small break event occur.

To cope with any remaining potential for digital CCF vulnerability, manual safety function initiation capabilities are provided in the main control room to serve as a diverse backup. Manual safety action is initiated through hardware switches and hardwired logic circuits, which bypass the digital automatic safety systems. These manual actions include scram, main steam isolation valve actuation, and high-pressure core flood system initiation. Diverse displays of essential parameters are also provided. These essential measurements consist of reactor-pressure-vessel water level, reactor pressure, main steam isolation valve (MSIV) status, reactor water cleanup system (CUW) isolation valve status, reactor core isolation cooling (RCIC) valve status, and high-pressure core flood system status. The manual trip signal de-energizes the power to every divisional trip relay so reactor scram is initiated by a diverse mechanism from that used for automatic trip actuation. Table 4.4 provides a summary of diversity usage at KK-6/KK-7.

Table 4.4. Summary of diversity usage for Kashiwazaki-Kariwa Units 6 and 7

Diversity attribute	Usage[a]	Details
Design		
Different technologies	x	Protection system and limited backup system based on diverse technologies [Microprocessor vs Analog circuit]
Different architectures	i	Inherent difference in system architectures due to technology diversity

Table 4.4 (continued)

Diversity attribute	Usage[a]	Details
Equipment (Manufacturer)		
Same manufacturer—different version	–	I&C systems for a unit are implemented on the same dedicated digital platform; KK-6 I&C systems are provided by Toshiba (TOSMAP); KK-7 I&C systems are provided by Hitachi (HIACS)
Equipment (Processing)		
Different logic processing architecture	i	Inherent diversity between digital platform for safety system and analog circuits for ATWS; No diverse digital hardware for automatic functions; Manual actuation is hardwired to provide diverse capability
Functional		
Different underlying mechanisms	i	Inherent difference in mechanisms for accomplishing function due to technology diversity
Different purpose, function, control logic, or actuation means	x	Reduced functionality backup provided through ATWS; RPS provides three shutdown mechanisms (Two ways to depressurize scram accumulators and a fast actuation mode for the electric control rod drive mechanism); ECCS has three diverse coolant injection systems (High pressure core flood system, reactor core isolation cooling system, and low pressure flooding system); Automatic depressurization system to transition a small break event to low pressure
Life-cycle		
Different design organizations/companies	–	Design, implementation, and quality assurance departments have separate management
Different design/development teams (designers, engineers, programmers)	x	Safety systems (RPS, ECCS, etc.) and control systems (FWC, RFC, etc.) were designed by separate teams
Different implementation/validation teams (testers, installers, or certification personnel)	x	Separate V&V team conducted IV&V based on requirements of JEAG 4609)

Draft

Table 4.4 (continued)

Diversity attribute	Usage[a]	Details
Logic (Software)		
Different algorithms, logic, and program architecture	i	Inherent difference in logic/function instantiation (e.g., structure of logic) due to technology diversity; All digital safety divisions have identical software
Different timing or order of execution	i	Inherent difference in logic/function execution due to technology diversity; No difference for digital safety divisions; As is common, asynchronous execution among divisions and systems
Different runtime environment	i	Inherent difference in logic/function execution due to technology diversity; No difference for digital safety divisions
Different functional representation	i	Inherent difference in logic/function instantiation due to technology diversity; For all digital safety systems, symbolic language (POL) used to express software specification and graphical tools used for implementation and validation
Signal		
Different parameters sensed by different physical effects	x	Diverse parameters used (e.g., flux vs pressure)
Different parameters sensed by same physical effects	x	Diverse parameters used (e.g., pressure vs water level or flow)
Same parameter sensed by a different redundant set of similar sensors	x	Different redundant sensors for important parameters (e.g., water level or reactor pressure) used for separate systems;
Other Diversity Considerations		
Primary and backup diverse systems with very limited functionality analog backup; Hardwired manual actuation also provided to protect against digital CCF in automatic safety system; Little digital equipment diversity provided	Primary system is quadruple redundant safety system, while secondary (backup) system is lower-safety-class analog-based ATWS system that provides reduced functionality (i.e., covers very limited set of PIEs); All major I&C systems are implemented using the same digital platform; Hardwired Manual scram, MSIV closure, CUW isolation, and RCIC steamline isolation; Hardwired manual divisional trip via diverse non-microprocessor-based logic; Hardwired manual high pressure injection initiation	

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

4.2.5 Temelín (Czech Republic)[95,106–108]

The Temelín Nuclear Power Plant is a two-unit Russian-designed water-cooled water-moderated power reactor (VVER) generating station. Construction based on the VVER-1000/320 design began in 1982 but was suspended at the end of the decade. Following resumption of construction, a modernization program was initiated to replace the original I&C systems with digital technology. The modernized Unit 1 was commissioned in 2002.

The Sizewell protection system design was adopted as a reference, and the Westinghouse IPS was chosen as the basis for the modernization of the primary reactor protection system (PRPS) at Temelín. The Temelín architectural design adhered to the Sizewell example of providing a diverse protection system. However, instead of a secondary system based on the fundamentally diverse Laddic technology, it was decided to use a microprocessor-based system based on a different platform for the Temelín diverse protection system (DPS). The Westinghouse Ovation digital control modules were selected as the platform for the Temelín DPS. The principal requirement driving the incorporation of a diverse system is that the overall plant safety system must be capable of mitigating an event concurrent with a postulated CCF in either PRPS or DPS, but not both simultaneously.

As is the case for Sizewell, diversity usage at Temelín can be characterized as a primary and secondary diverse system architecture. Both systems are essentially equivalent in safety classification with the PRPS being fully Class 1E and the DPS consisting of Class 1E and dedicated equipment. The Temelín DPS assumes the same role as the SPS at Sizewell by serving as a backup safety system for AOOs that are estimated to occur with frequency greater than 10^{-3} events per year. Other than the use of digital technology for the DPS, the primary difference between the I&C system architecture at Temelín and that at Sizewell is the constraint of three rather than four divisional sensor sets to conform to the original Russian-designed configuration of the VVER I&C systems. Thus, both the PRPS and DPS are implemented as triple redundant systems and each employs two-out-of-three voting logic for actuation. An additional feature of the I&C system at Temelín is the availability of an additional line of defense through the presence of a separate reactor limitation system, which was also modernized.

As noted, the PRPS is divided into three identical, redundant divisions. Each division communicates its partial trip status to the other divisions for two-out-of-three specific coincidence voting by the microprocessor systems. Subsequent general coincidence voting logic is implemented at the circuit breakers, which are configured into three trains of actuation logic. The PRPS is implemented using the Westinghouse Eagle 2000 platform. As with Sizewell, separate functionally diverse subsystems based on alternate actuation initiation criteria (e.g., parametric diversity arising from signal diversity) are provided within each division. Each subsystem incorporates a “host” (or main) processor and a number of supporting processors for communication, input/output, and auxiliary processes. The Eagle processors are implemented using Intel 80486 microprocessors and supporting integrated circuits. The PRPS application software is written in a combination of PL/M 86 and ASM86 assembler.

The DPS provides a secondary automatic means to shut down and cool the plant should the PRPS fail to take appropriate action in response to a reduced set of events (i.e., frequently occurring PIEs). The system also uses two levels of two-out-of-three voting (by the microprocessors and relays). In addition, a second set of breakers is provided for the DPS. These breakers are separate from the breakers used by the PRPS and are supplied by a different vendor. As stated above, the three divisions for the DPS are implemented on Ovation equipment, which is based on Motorola 68000 microprocessors. The DPS application software is written in Ada.

The Ovation platform provides a compact design in which the processor module, as well as the I/O modules, resides on the same VME (VERSAbus-E) bus. Thus, the functionally diverse subsystems within the DPS are not as distinctly separate as for the PRPS using the IPS/Eagle platform.

Other differences between the Eagle and Ovation platforms include different bus architectures (Multibus vs VME, respectively), different network communication technology (proprietary token bus vs reflective memory bus), and different I/O handling (proprietary vs VME-based). Finally, different development teams, development processes, development platforms, and tools were used for each system while different verification and validation (V&V) teams were established as well.

The integration of the primary and diverse safety systems at the actuated device level for Temelín required a more complicated priority logic module than the relay-based logic at Sizewell. While the presence of multiple systems (PRPS, DPS, limitation, control, and manual initiation) issuing commands that must be arbitrated has an impact, the previously identified requirement, in which either safety system must compensate for loss of the other due to CCF, drives the need for a robust prioritization capability. Thus, Westinghouse developed non-programmable logic (NPL) equipment to implement command priority logic for safety valves and pumps that are affected by multiple systems. Additionally, a portion of the diesel generator sequencing logic is also implemented in NPL equipment. The equipment performing prioritization of safety commands is qualified as Class 1E. Nevertheless, the priority module is a common point at which both the primary and secondary diverse protection systems connect to the final actuated device. Because actuation signals from both systems must pass through a common device, the potential for CCF vulnerability must be considered. Consequently, the NPL design is intended to provide a very simple, highly reliable component that is more fully testable than a software-based module. Table 4.5 summarizes the diversity usage at Temelín.

Table 4.5. Summary of diversity usage for Temelín

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two systems (primary and diverse) based on different microprocessors
Equipment (Manufacturer)		
Same manufacturer—different version	x	Westinghouse supplied IPS/Eagle for PRPS and Ovation (from the Westinghouse Process Control Division, now Emerson) for DPS
Equipment (Processing)		
Different logic processing architecture	x	Intel 80486 vs Motorola 68000
Different component integration architecture	x	Different chipsets on different board designs
Different data-flow architecture	x	Multibus vs VME bus
Functional		
Different purpose, function, control logic, or actuation means	x	Purpose of DPS is to protect against high-frequency events (10^{-3} events/year), so DPS provides reduced functional coverage of DBEs vs PRPS; Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used within subsystems of PRPS and DPS (i.e., internal functional diversity); Different trip breakers (from different suppliers) for DPS and PRPS

Table 4.5 (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different management teams within same company	x	PRPS and DPS supplied by separate divisions within Westinghouse
Different design/development teams (designers, engineers, programmers)	x	Different personnel for each team
Different implementation/validation teams (testers, installers, or certification personnel)	x	Different personnel for each team
Logic (Software)		
Different algorithms, logic, and program architecture	x	Algorithmic and logic differences between diverse systems due to reduced scope of DPS (i.e., reduced functionality); Functionally diverse subsystems within each system provide algorithmic and architectural differences
Different functional representation	x	PL/M-86 and ASM86 assembler vs Ada
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within subsystems of each diverse system
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within subsystems of each diverse system
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between protection systems and between divisions within each diverse system
Other Diversity Considerations		
Primary and secondary diverse systems with functionally diverse subsystems within the each diverse system; Diverse measurement equipment for each system; Priority module to arbitrate between systems commanding safety equipment	Primary safety system is triple redundant safety system, while secondary diverse system is also triple redundant safety system (also of high safety class) that provides reduced functionality (i.e., covers a limited set of PIEs); Functionally diverse subsystems within each division of each safety system; Separate signals for primary and diverse systems as well as separate signals among divisions of safety systems; Non-programmable logic equipment provides prioritization at device-level among commands from the two safety systems as well as among safety and control systems	

[a]Intentional diversity (x).

4.2.6 Dukovany (Czech Republic)[109]

The Dukovany Nuclear Power Plant is a four-unit power station based on the VVER-440/213 Russian design. A modernization program for each unit was initiated in 2002 with phased

implementation spanning several outages. In 2005, Unit 3, which began operation in 1986, was the first to have its main upgrade projects completed. The modernization was accomplished using *SPINLINE 3*, which was developed jointly by Schneider Electric and Framatome (now DS&S and AREVA NP, respectively). *SPINLINE 3* was used to upgrade the RTS, ESF actuation system (ESFAS), emergency load sequencer, reactor limitation system, and reactor control system. For Dukovany, the digital reactor protection system (DRPS) fulfills the roles of the RTS, ESFAS, and reactor limitation system. Within the DRPS, separate Lines of Protection (LOP) are established based on functionally diverse subsystems employing diverse signals and separate trains of actuation equipment.

The Dukovany plant, like other VVERs, is only able to support instrumentation for three divisions of protection logic. The voting is consequently two out of three. Within each of the three divisions, the *SPINLINE 3* design implements the functionally diverse subsystem approach in a manner similar to that accomplished at Chooz using the SPIN system. As previously described, at least two parameters are identified as event indicators associated with each PIE. These diverse actuation initiation criteria are grouped and processed by separate subsystems, LOP A and LOP B (as shown in Figure 4.8). The digital instrumentation system (DIS) performs the data acquisition and safety comparison processing for each division. The diverse parameters are distributed to separate pairs of processors corresponding to the two LOP. Partial trip results are transmitted across separate NERVIA networks to each division of the DRPS where the two-out-of-three voting is accomplished in two trains corresponding to the two LOP. The voting logic implementation is similar to that described above for the ULS in SPIN at Chooz (see Figure 4.6). Both LOP trains control the ESFAS actuators associated with the division, while each LOP train drives separate diverse trip breakers based on two-out-of-three general coincidence logic. The diverse trip breakers are supplied by different manufacturers.

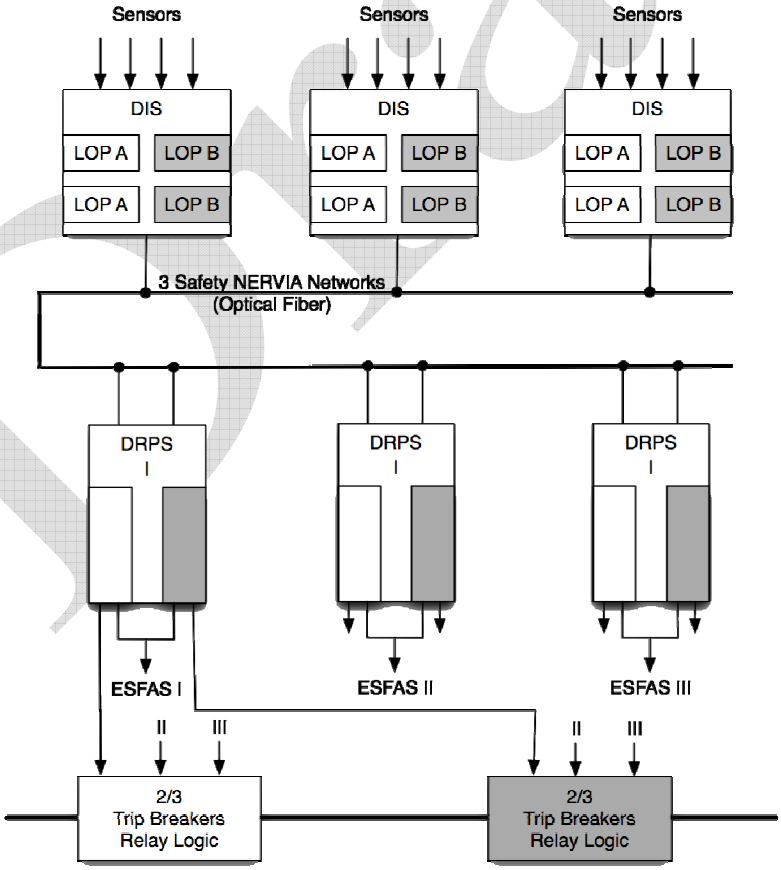

Figure 4.8. Digital safety system at Dukovany Nuclear Power. (Adapted from Ref. 109.)

While the subsystems utilize separate processing units, the platform and communication network (*SPINLINE 3* and NERVIA, respectively) associated with each subsystem are identical. The *SPINLINE 3* platform is based on the Motorola 68040 microprocessor. NERVIA is a high-bandwidth token ring network that utilizes broadcast messaging for data transfer. The application software is designed based on formal programming language techniques using a graphical data-flow-oriented development environment called CLARISSE. The CLARISSE system and software development environment (SSDE) provides automatic C code generation for analysis or compilation into binary code for direct implementation.

No diverse backup system is provided at Dukovany. In fact, the safety (RTS and ESFAS), limitation, and control lines (i.e., echelons) of defense are all implemented on the *SPINLINE 3* platform. The principal diversity argument for functionally diverse subsystems arises from the diversification of input profiles and execution of different software applications (i.e., different signal trajectories) such that the diverse subsystems of the RTS and ESFAS should not share any common stimuli other than the initiating event. Cyclic, invariant execution of functions is used to avoid common demand dependencies. Consequently, coincident triggering of common faults to cause a CCF would be unlikely. The impact of time dependency is addressed as a potential common stimulus by requiring asynchronous operation, static memory and program configuration, no external interrupts, and no operations requiring accumulation or functions of time. Table 4.6 summarizes the diversity usage at Dukovany.

Table 4.6. Summary of diversity usage for Dukovany

Diversity attribute	Usage[a]	Details
Design		
Equipment (Manufacturer)		
Equipment (Processing)		
Functional		
Different purpose, function, control logic, or actuation means	x	Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used in subsystems (LOP) of DRPS; Redundant trains with separate communication paths are provided for safety component actuation; Diverse trip breakers (from different suppliers) between LOP
Life-cycle		
Different design/development teams (designers, engineers, programmers)	–	No information on whether separate teams were established for application development at the LOP level or for system development at the echelon (line) of defense level
Logic (Software)		
Different algorithms, logic, and program architecture	x	Functionally diverse subsystems within DRPS provide algorithmic and architectural differences as well as logic difference between LOP

+Table 4.6 (continued)

Diversity attribute	Usage[a]	Details
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within SPINLINE 3 subsystems
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within SPINLINE 3 subsystems
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between divisions within SPINLINE 3
Other Diversity Considerations		
Functionally diverse subsystems within the safety system; Diverse measurement equipment supporting functional diversity; Little equipment diversity provided (especially for digital systems)	Safety system is triple redundant system with functional diversity provided by diverse groupings of actuation initiation criteria between subsystems (LOP); Diverse sensors in each divisional set to facilitate functional diversity; ESFAS and RTS integrated and share signals; Safety, limitation, and control echelons implemented on same platform	

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

4.2.7 Lungmen (Taiwan)[110,111]

The Lungmen Nuclear Power Station is a two-unit ABWR plant currently under construction by the by GE for the Taiwan Power Company (Taipower). The control, information, and safety systems are all implemented digitally for Lungmen. Figure 4.9 illustrates the principal control and safety systems. The

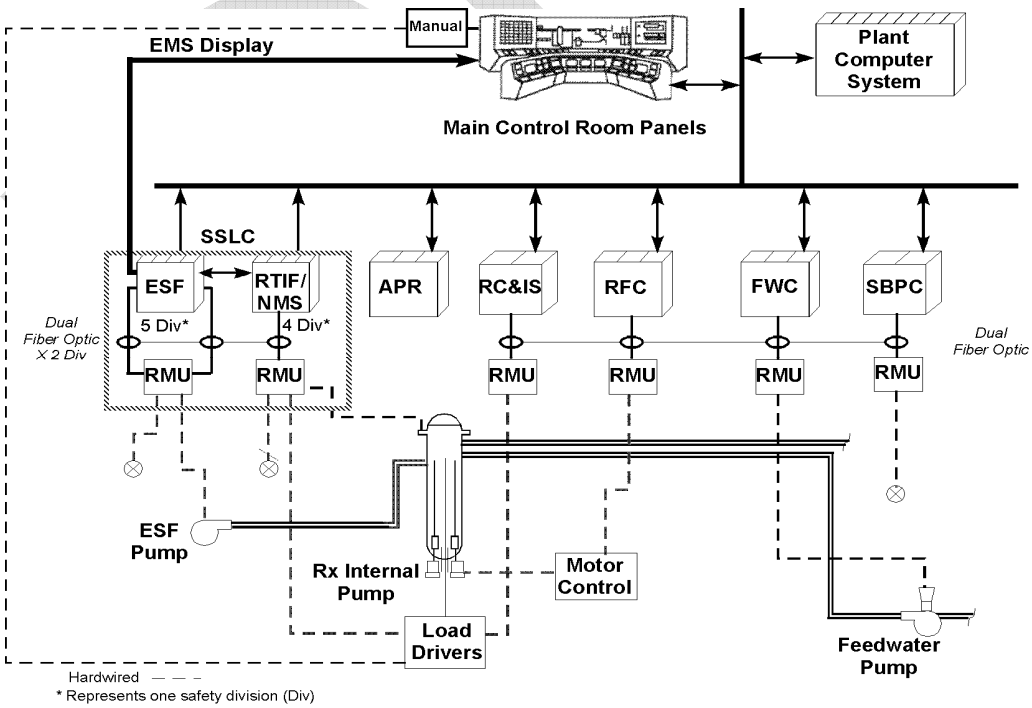

Figure 4.9. Overall architecture of Lungmen I&C systems. (Adapted from Ref. 110**.)**

plant employs six main vendors with several subcontractors to provide the integrated systems. The primary system suppliers are GE, DRS Technologies (formerly Eaton Corporation), GE Industrial Systems (GEIS), Invensys Process Systems, Hitachi, and Mitsubishi Heavy Industries (MHI). The use of multiple vendors and digital platforms results in significant system diversity among the echelons of defense. The systems that constitute these echelons utilize different platforms and perform different functions that provide some level of backup or complementary mitigation for the primary safety functions. Thus, the backup and compensating functions introduced across lines of defense provide significant diversity across the board.

In particular, ATWS mitigation logic is provided to serve as the principal backup in the event of a CCF in the safety system. This backup functionality utilizes several diverse systems within the Lungmen I&C architecture. Consequently, Lungmen can be characterized in terms of a primary and secondary diverse system architectural approach.

The main Class 1E safety systems for the plant constitute the System Safety Logic Control (SSLC). These systems include the reactor protection system (RPS), ESF system, and neutron monitoring system (NMS). These safety systems within the SSLC are supplied primarily by two vendors, GE and DRS Technologies. DRS supplies the ESF system and GE supplies the RPS, NMS, and associated isolation function systems.

The RPS combines functions for the reactor shutdown via rod scram and the isolation of the reactor system by closing the main steam isolation valves. It is sometimes identified as the Reactor Trip and Isolation Function (RTIF) system.

The ESF system operates the emergency core cooling system (ECCS) and other cooling and post-accident protective functions. The ECCS systems include the High-Pressure Core Flooder System (HPCF), the Automatic Depressurization System (ADS), the Reactor Core Isolation Cooling (RCIC) System, and the low-pressure flooder mode of the Residual Heat Removal System (RHRS). The ECCS provides a series of diverse and redundant systems to provide cooling to the fuel following a design basis accident.

The RPS is implemented using the GE NUMAC platform. It is configured as a quadruple redundant system that consists of distributed processing elements. The main modules that comprise a safety division are RMUs, digital trip modules (DTMs), and trip logic units (TLUs). These modules are configured in a logical pathway from measurement to actuation with downstream interfaces provided via optical communication links. The RMUs communicate multiplexed field data to the DTMs, which perform safety calculations. The partial safety actuation results from the DTMs are communicated to the TLUs in all four divisions. The TLUs perform two-out-of-four-voting to establish divisional trip results.

The ESF system is composed of five divisions with a distributed modular structure similar to that of the RPS. The ESF modules are implemented using the DRS Technologies Programmable Logic Microprocessor System (PLμS) based on the 32 bit PLμS 32 microprocessor. Four divisions constitute the dedicated ESF system for a reactor unit, while the fifth division serves as the unit interface to manage a spare swing set of emergency diesel generators that service both units of the plant. The four primary divisions communicate within the ESF system, with the RPS, and to ESF actuation devices across the essential multiplexing system (EMS). As is common, the digital safety actuation logic implements two-out-of-four voting.

The EMS provides five separate serial ring networks (i.e., four for the ESF system and one supporting the fifth division). Each division is connected to two EMS rings. The EMS is treated as two divisions consisting of two rings connected to two ESF divisions. The ring network is implemented based on the DRS Technologies performance-enhanced redundant fiber optic replicated memory network (PERFORM.NET). The two EMS divisions are linked to each other and the RPS through redundant communication interface modules (CIMs).

The main process control systems at Lungmen are implemented on fault-tolerant control platforms. In particular, the Feedwater Control (FWC) System, Steam Bypass and Pressure Control (SBPC) System, Recirculation Flow Control (RFC) System, and Automatic Power Regulator (APR) are implemented as triple modular redundant (TMR) controllers using the GEIS Mark VIe platform. This TMR platform is based on the Freescale 8349 (i.e., PowerPC) microprocessor. These systems act to maintain operating conditions in an acceptable range and also provide actuation mechanisms that serve to backup the safety systems.

To enable that backup capability, the Lungmen I&C architecture provides a separate system for ATWS mitigation logic as an alternate means for safe shutdown and cooling of the plant. The ATWS system is primarily a non-Class 1E backup that utilizes several control systems and alternate, diverse shutdown means, such as the Standby Liquid Control System (SLCS), ARI, and Fine Motion Control Rod Drive (FMCRD). However, some of the ATWS logic is implemented in diverse modules within the SSLC cabinets. The system provides diversity in its sensors, hardware, and software. The ATWS system is conceived as a simple, safe recovery system to protect the plant in the event that the safety systems should fail to function due to CCF. Table 4.7 summarizes the diversity usage in Lungmen.

Table 4.7. Summary of diversity usage for Lungmen

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Diverse systems are based on different microprocessors
Equipment (Manufacturer)		
Different manufacturer—same design	x	GE for RPS, DRS for ESFAS, GEIS for RFC, FWC, and Steam Bypass and Pressure Control (SBPC)
Equipment (Processing)		
Different logic processing architecture	x	Motorola 68000 for NUMAC, PLμS32 for DRS programmable logic controller (PLC), Freescale 8349 (PowerPC) for Mark VIe (provides ATWS logic in RFC); Processor for additional ATWS logic in SSLC not specified
Different component integration architecture	x	Not specified but diverse circuit board designs likely for ESF system based on PLC compared with RPS and other platforms based on Motorola CPU heritage
Different data-flow architecture	x	Not specified but diverse bus architecture likely for ESF system based on PLC compared with RPS and other platforms based on Motorola CPU heritage

Draft

Table 4.7 (continued)

Diversity attribute	Usage[a]	Details
Functional		
Different purpose, function, control logic, or actuation means	x	Different purposes for RPS, ESF system, control system and ATWS logic; ATWS system provides reduced functional coverage of DBEs vs SSLC; ATWS provides alternate means of shutdown (e.g., ARI, FMCRD, SLCS) and provides ECCS by independent systems (feedwater, control rod drive, and condensate systems); Different interlock logic provided in each ESF division
Life-cycle		
Different design organizations/companies	x	GE for RPS, DRS for ESF, GEIS for TMR control systems and some ATWS logic; No information was available on the developer of the ATWS logic processor modules
Different design/development teams (designers, engineers, programmers)	i	Different personnel for each company
Different implementation/validation teams (testers, installers, or certification personnel)	i	Different personnel for each company
Logic (Software)		
Different algorithms, logic, and program architecture	x	Algorithmic and logic differences between diverse systems due to different purposes/functions and because of reduced scope of ATWS (i.e., reduced functionality); Logic differences provided between ESF divisions
Different timing or order of execution	x	Different purpose and function between RPS/ESF and ATWS leads to execution differences; Parameter choice for PIE indication and expanded range of actuation initiation criteria (to avoid ATWS action unless warranted) contributes to timing differences
Different runtime environment	–	No specific information available
Different functional representation	–	No specific information available

Draft

Table 4.7 (continued)

Diversity attribute	Usage[a]	Details
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support different echelons (or lines) of defense; Different combined signal sets support ATWS, ESF, and RPS
Different parameters sensed same physical effects	x	Diverse measurements support different echelons (or lines) of defense; Different combined signal sets support ATWS, ESF, and RPS
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between diverse systems and between redundant divisions
Other Diversity Considerations		
Primary and secondary diverse systems; Diverse measurements and diverse equipment for each system	Quadruple redundant safety systems (RPS and ESF) are diverse; Reduced functionality ATWS provides additional diversity; Functional diversity among systems arising from different purpose, logic, and inputs	

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

The Lungmen ATWS system consists of redundant logic to initiate diverse automatic actuation of safety or compensating functions. The system contains a simple, reduced set of automatic actuations compared with either the RPS or ESF system. The system also provides analog displays and manual inputs that connect through a minimum set of equipment to the actuated equipment to give the operator a diverse means of manual control. The ATWS controls are available in the main control room and the Remote Shutdown System in the standby control room.

The protective actions provided by the ATWS system include backup scram of the safety rods, liquid poison injection, speed trip or runback of the recirculation pumps, and feedwater runback. The logic for these actions is implemented within the RFC and other systems and on ATWS logic modules in the SSLC. The logic for backup scram is implemented in the TMR RFC system. These actions include two-out-of-three logic for actuation of the safety rods, the FMCRD, and the ARI. Additional logic implemented in the RFC addresses internal pump runback and reactor pump trip. The logic utilizes measurement and status inputs from the FWC, SBPC, SSLC, and manual initiation to provide signal diversity. Mitigation logic to initiate SLCS injection and feedwater runback as well as inhibit ADS actuation is implemented on ATWS logic processor modules in the SSLC cabinets. Specific details on the ATWS logic processor was not addressed in available information resources.

Another aspect of the diversity usage at Lungmen involves the dissimilarity of the safety functions applied in each division of the ESF system. Basically, the software for the safety applications of the ESF is not identical in all divisions. Specifically, the ESF interlock logic is different in each division. The inputs and outputs vary in number and type. Redundant sensors have data messages with unique identifications and time-tags in each division. The intent is to promote differences in the software that may reduce the potential for CCF vulnerabilities that depend on coincident timing or execution. The system is designed so that modules operate asynchronously and thus a common clock or timing signal cannot be a source of CCF. Nevertheless, certain errors depend on the same operation occurring in all modules at the same or close to the same time. The differences in the division software are believed to reduce the likelihood of such errors from occurring or from occurring simultaneously in all divisions.

4.2.8 Olkiluoto-3 (Finland)[112,113]

The European or evolutionary pressurized reactor (EPR) is an advanced evolutionary PWR supplied by AREVA NP (formerly Framatome). It is currently under construction in Finland as Unit 3 of the Olkiluoto Nuclear Power Station (OL-3), with an expected commissioning in 2012.

The EPR provides an extensive, highly integrated digital I&C architecture based on the AREVA Teleperm XS (TXS) and Siemens Power Plant Automation (SPPA) T2000 (formerly Teleperm XP) platforms. The I&C architecture for OL-3 provides a reduced functionality digital backup for the primary safety system and a hardwired backup system (HBS), based on field-programmable gate arrays (FPGAs), to mitigate the potential for CCF vulnerabilities within the microprocessor-based systems. Thus, OL-3 conforms to a primary and secondary diverse system architectural approach.

Major I&C systems are shown in Figure 4.10. The I&C architecture includes the Safety Information and Control System (SICS), the Plant Information and Control System (PICS), the Protection System (PS), the Reactor Control, Surveillance and Limitation System (RCSL), the Severe Accidents Automation System (SAAS), the Safety Automation System (SAS), and the Process Automation System (PAS). Priority Actuator Control (PAC) modules are provided as interfaces to shared actuation devices. The reactor trip and ESF functions are contained within the quadruple-redundant PS system.

The PS is implemented on the TXS platform, which is based on the AMD K6-E2 microprocessor. The non-safety I&C systems are implemented using the SPPA-T2000 platform, which is based on dual SIMATIC S7-400H microprocessors. Of those non-safety systems, the dual-redundant SAS provides diverse digital backup of the PS safety function for high-frequency PIEs, such as AOOs. The HBS is a

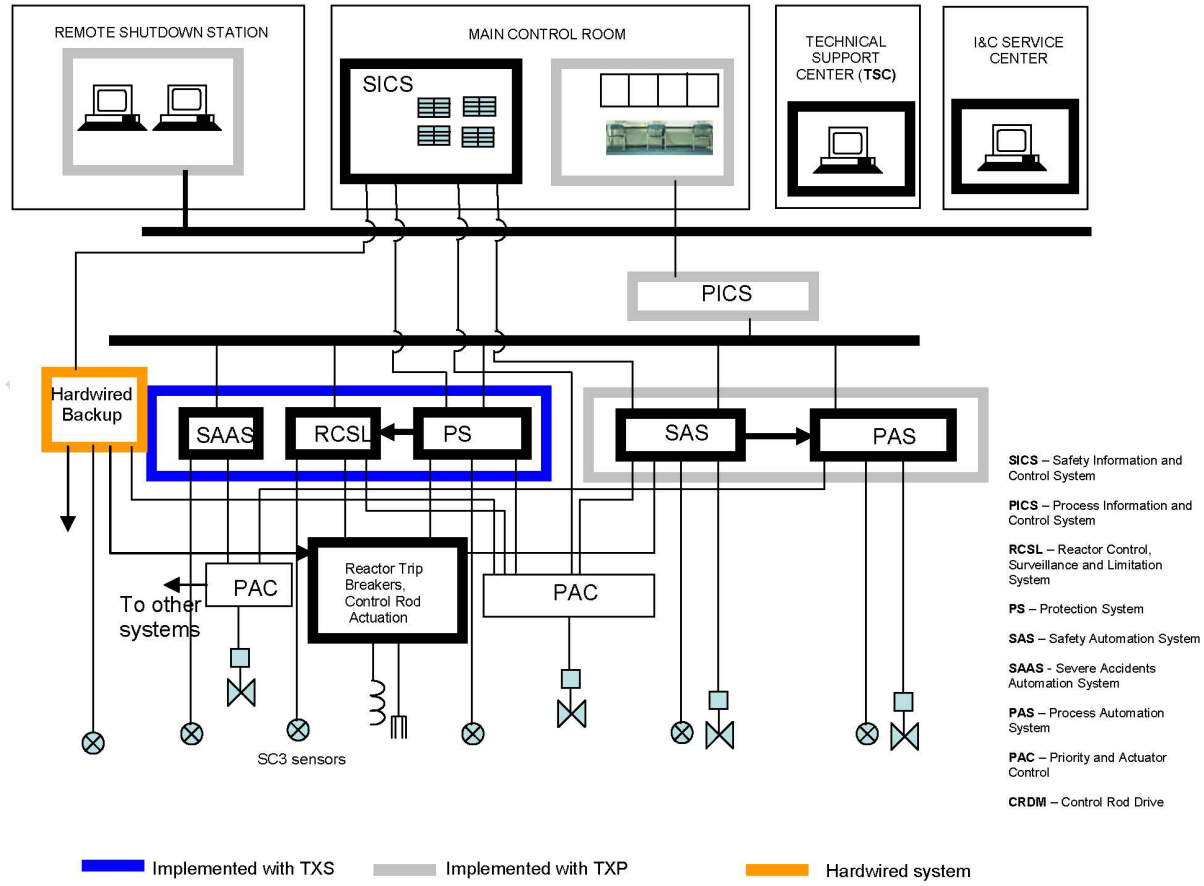

Figure 4.10. Olkiluoto-3 I&C architecture. (Adapted from Ref. 112.)

quadruple redundant system that provides automatic backup of all reactor trip functions. Although a final decision had not been determined at the time of this investigation, the expectation is that AREVA/ Siemens would develop the diverse FPGA-based HBS. Hardwired manual initiation capabilities are also provided as an additional backup.

In addition to the multiple layers of diverse backups to mitigate the potential impact of CCF vulnerability for the PS, the I&C architecture of OL-3 (and the EPR in general) also employs functionally diverse subsystems within each division of the PS. This strategic diversity usage, as for Sizewell, Chooz, Temelín, and Dukovany, assigns diverse safety parameters to different subsystem diversity groups, A and B, within each division. A high degree of functional diversity is achieved because diverse signals and some actuated devices are assigned to different subsystems. Table 4.8 summarizes the diversity usage at OL-3.

Table 4.8. Summary of diversity usage for Olkiluoto Unit 3

Diversity attribute	Usage[a]	Details
Design		
Different approach—same technology	x	Primary and backup systems based on different digital technology (microprocessor-based vs FPGA-based)
Different architectures	i	Inherent difference in system microarchitectures due to technology diversity; Digital backup for reactor trip and ESF is also provided based on a different microprocessor
Equipment (Manufacturer)		
Same manufacturer—different design	x	Primary and backup system to be supplied by same vendor (AREVA/Siemens); Digital backup provided by a different group within the AREVA/Siemens company; Base platforms (particularly different core processing equipment) of primary and backup systems manufactured by different companies
Equipment (Processing)		
Different logic processing architecture	i	General purpose microprocessor distinctly different from application-specific FPGA processor; AMD K6-E2 CPU vs customized gate arrays for logic processing; Digital backup uses SIMATIC S7-400H microprocessors
Different component integration architecture	i	Unspecified but likely inherently different circuit board layout anticipated arising from customized logic (FPGA) vs CPU with associated chipsets

Table 4.8 (continued)

Diversity attribute	Usage[a]	Details
Equipment (Processing) (continued)		
Different data-flow architecture	i	Unspecified but likely inherently different bus architecture anticipated arising from specialized circuitry vs generalized computer/peripheral bus interface
Functional		
Different underlying mechanisms	i	Inherent difference in mechanisms for accomplishing function due to technology diversity (PS vs HBS)
Different purpose, function, control logic, or actuation means	x	Purpose of PS is to provide reactor trip and ESF protection for all DBEs while HBS backs up trip functions and SAS protects against high-frequency events (10^{-3} events/year); SAS provides reduced functional coverage of DBEs vs PS; Different functional relationships (i.e., diverse actuation initiation criteria for responding to each PIE) are used in subsystems of PS; Functional diversity in the actuated device is present for several functions of PS, HBS, SAS, and RCSL as well as for functionally diverse subsystems of PS (e.g., different systems for ESF response to PIEs)
Life-cycle		
Different management teams within same company	x	It is anticipated by the Finnish regulator that different teams within AREVA/Siemens will be used to develop PS, SAS, and HBS; Different teams/companies supply the safety and non-safety system platforms (AREVA vs Siemens)
Different design/development teams (designers, engineers, programmers)	x	Anticipated life-cycle diversity through separate teams for primary and backup systems (expertise/skill sets are inherently different for HBS)
Different implementation/validation teams (testers, installers, or certification personnel)	x	Anticipated life-cycle diversity through separate teams for primary and backup systems

Draft

Table 4.8 (continued)

Diversity attribute	Usage[a]	Details
Logic (Software)		
Different algorithms, logic, and program architecture	x	Inherent difference in logic/function instantiation (e.g., structure of logic) due to technology diversity (PS vs HBS); Algorithmic and logic differences between diverse systems due to reduced scope of SAS (i.e., reduced functionality); Functionally diverse subsystems within PS provide algorithmic and architectural differences
Different timing or order of execution	i	Inherent difference in logic/function execution due to technology diversity (HBS vs PS); Primary and backup systems execute different logic within different architectures in which mechanisms of execution (e.g., sequential execution of op code vs parallel execution of configured arrays) are different
Different runtime environment	i	Inherent difference in logic/function execution due to technology diversity
Different functional representation	i	Inherent difference in logic/function instantiation due to technology diversity
Signal		
Different parameters sensed by different physical effects	x	Diverse measurements support alternate actuation criteria within PS subsystems
Different parameters sensed by same physical effects	x	Diverse measurements support alternate actuation criteria within PS subsystems
Same parameter sensed by a different redundant set of similar sensors	x	Separate sensors used between diverse systems and between divisions within PS

Draft

Table 4.8 (continued)

Diversity attribute	Usage[a]	Details
Other Diversity Considerations		
Primary and secondary diverse safety systems with functionally diverse subsystems within the primary safety system; Sharing of some signals and actuation equipment (through priority interface) among major systems (control and protection); Complex priority module to arbitrate between systems commanding safety equipment	Both PS and HBS are quadruple redundant, while SAS is dual redundant; PS has full functionality with functionally diverse subsystems, while SPS has reduced functionality (i.e., covers limited set of PIEs), and HBS covers only reactor trip conditions; Trip breakers and sensors for each protection system are separate, but signal are shared for cross-validation; FPGA-based logic prioritization at device level among some commands from PS, HBS, SAS, RCSL, and control system	

[a]Intentional diversity (x), inherent diversity (i).

The configuration of the PS involves four divisions, each consisting of five acquisition and processing units (APUs) and four actuator logic units (ALUs). Within a division, each APU is assigned to one of the two functionally diverse subsystem groupings. Each APU communicates its safety actuation results to the corresponding subsystem grouping of ALUs in each of the other three divisions. Each subsystem within a division also provides dual ALUs for redundant voting per subsystem using the shared safety actuation signals from across divisions. For the ESF logic, these redundant voters are connected via an "OR" operator. In comparison to a design with single voter, this architecture increases the division reliability by the capability to generate an ESF signal when a single voter fails. The reactor trip logic also contains redundant voters, but these voters are connected with an "AND" operator. This logic provides protection against a spurious reactor trip. The reactor trip signals from the voted subsystem groupings drive different trip breakers. The voted ESF actuation signals from the grouped subsystems are assigned to primary and alternate ESF mechanisms (e.g., emergency feedwater system and safety injection system, which can both provide core cooling) where feasible.

The potential for CCF vulnerabilities between the functionally diverse subsystem groupings (i.e., subsystems A and B) is expected to be minimized because the subsystems employ different parameters associated with each PIE based on diverse functional relationships. Essentially, the application software is diversified because the protection functions and parameter/sensor inputs are different. The subsystems do not share any common safety functions. The subsystems are electrically independent and are not connected by any communication links. Nevertheless, common equipment is used for the subsystems and software diversity is limited because the subsystems share the same system software and function block modules. Equipment and logic diversity are achieved in OL-3 by a reduced functionality mitigation capability in the form of the digital backup functions that are implemented as part of the SAS and through the hardwired backup functions provided by the HBS. The SAS is implemented via a diverse platform using the SPPA-T2000 equipment while the HBS provides additional, more technologically distinct, diversity through the FPGA-based backup trip functions. The SAS employs a limited set of measurements corresponding to the reduced set of PIEs in its scope. The HBS uses separate measurements of the same parameters for backup trip functions as those used by the PS. The SAS is a non-safety system with enhanced quality, while the HBS is a safety-related system of a lower safety class than the PS.

In addition to the functional diversity provided by the subsystems A and B within the PS as well as the mitigation arising from the diverse backup systems, there is additional defense in depth provided in the I&C architecture. Specifically, the RCSL system provides control, surveillance, and limitation functions to reduce reactor trips and safety system challenges. Basically, the RCSL supplies soft

protection by avoiding safety system challenges by limiting plant conditions. For example, actions such as a power runback are means by which it restores normal operating conditions in response to transients.

Finally, a potential source of CCF vulnerability for protection systems is commonality or sharing of the final actuation device. In the EPR design, PAC module serves as the interface to ESF actuators and pumps drivers. Its purpose is to manage the use of the actuation resource by arbitrating commands from different sources (e.g., safety, control, and manual commands) while also providing resource protection (i.e., limiting demands to saturated or failed equipment). Dual-use equipment, such as the ESF cooling systems, provides both safety and normal operating functions. Selecting between the input signals requires a final signal arbiter to enforce priority based on safety goals. In OL-3, the PAC is not a simple set of relays (e.g., Chooz or Sizewell) but it is a more complex device providing FPGA-based priority logic and communication interfaces to non-safety systems. The PAC prioritizes the various sense and command inputs and distributes an output that reflects the plant licensing requirements and operational preferences. In addition, it monitors checkback (or surveillance) signals from the actuators and other devices to protect those resources. The checkback feature limits actuation at the saturation limits. For example, the PAC inhibits demands to a valve to prevent driving it past the full in or full out position. The multi-use actuators are interfaced through a PAC module.

This final device is recognized as a potential site for a CCF vulnerability of the protective function. To address the CCF concern arising from the common usage of PAC modules, alternate designs of the PAC are being considered to provide diverse options. However, concerns about added complexity are also being factored into any final decision. For other plants that provide priority interface modules (e.g., Sizewell, Chooz, Temelín, and Dukovany), the argument that CCF vulnerabilities are sufficiently addressed rests on the simplicity and testability of the final control device.

4.3 Summary of Nuclear Power Plant Diversity Usage

Table 4.9 summaries the diversity usage identified through the investigation of the international evolutionary NPPs. The prevalent approach to implementing diversity is through a primary and secondary diverse system architecture 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.

Table 4.9. Summary of diversity usage for international NPPs[a]

Diversity attribute	Dr	S	C	K	T	Dk	L	O
Design								
Different technologies	–	x	–	x	–	–	–	–
Different approach—same technology	–	–	–	–	–	–	–	x
Different architectures	x	i	x	i	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	–	–	–
Equipment (Processing)								
Different logic processing architecture	x	i	x	i	x	–	x	i
Different logic processing versions in same architecture	–	–	–	–	–	–	–	–
Different component integration architecture	x	i	–	–	x	–	x	i
Different data-flow architecture	–	i	–	–	x	–	x	i

Table 4.9 (continued)

Diversity attribute	Dr	S	C	K	T	Dk	L	O
Functional								
Different underlying mechanisms	x	i	–	i	–	–	–	i
Different purpose, function, control logic, or actuation means	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
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 (Software)								
Different algorithms, logic, and program architecture	x	i	x	i	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
Different parameters sensed by same physical effects	x	x	x	x	x	x	x	x
Same parameter sensed by a different redundant set of similar sensors	x	x	x	x	x	x	x	x

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

Draft

5. INTERNATIONAL CONTRIBUTIONS TO DIVERSITY

The international nuclear power community has been active in efforts to resolve the challenge of what constitutes sufficient diversity usage to adequately address the potential for CCF vulnerabilities, especially for digital I&C systems. Key technical interactions and recent international meetings have focused on the diversity issue. In particular, the NRC cosponsored an IAEA meeting in 2007 to discuss approaches to cope with CCF, including diversity usage to mitigate its impact. In addition to the current investigation of diversity strategies, the international nuclear power industry has performed research for several years on the application of diversity as a means to avoid or mitigate CCF. Finally, the importance of properly addressing the potential for CCFs has resulted in the development of common positions on regulatory considerations and consensus standards. Specifically, IEC has recently issued a standard (IEC 62340) on coping with CCFs in I&C system designs at NPPs.

5.1 International Information Exchanges and Technical Meetings

5.1.1 Multinational Design Evaluation Program Interactions

NRC is a leading party to the Multinational Design Evaluation Program (MDEP), in which international regulatory agencies interact to share experience and collaborate on the development of multinational regulatory standards for NPPs. Through this program administered by the Organisation for Economic Cooperation and Development/Nuclear Energy Agency (OECD/NEA) with the cooperation with the IAEA, NRC staff meets with other international regulators to discuss key issues such as appropriate diversity to avoid CCF.

The investigation of CCF mitigation approaches and regulatory practice regarding diversity, which was performed under this research effort, leveraged these MDEP interactions by engaging international regulators and licensees to capture experience gained from the implementation of evolutionary reactors with primarily digital I&C systems. In the spring of 2007, NRC and ORNL personnel engaged in discussions with European regulators and regulatory researchers at the Institut de Radioprotection et de Sûreté Nucléaire (Institute for Radiological Protection and Nuclear Safety—IRSN) in France, the Säteilyturvakeskus (Radiation and Nuclear Safety Authority—STUK) of Finland, and the HSE in the United Kingdom. In addition, an associated meeting with EdF personnel allowed discussion of the use of diversity at N4 plants (e.g., Chooz B) as well as expected approaches for the planned EPR at Flammanville. Some relevant highlights of the discussions with each organization follow.

IRSN staff stated that France does not emphasize diversity as a primary response to the potential for digital CCF vulnerabilities but instead places great demands on quality and the establishment of a safety case. There is obvious similarity between the stated approach within the French nuclear power industry and the approaches employed by nonnuclear industries such as the aerospace and defense industries. As part of the discussion of regulatory practices in France, IRSN described the analysis tools they employ to assess quality and correctness for systems and applications. For the N4 plants, functional diversity (i.e., different compensating functions based on diverse parameters and initiation criteria) within subsystems of the protection system was employed along with equipment diversity between the safety systems and the limited-functionality ATWS system. This diversity approach is consistent with traditional diversity usage as described in Chapter 2. IRSN had considered whether diverse platforms should be required to further diversify the already functionally diverse subsystems of the safety systems, but it was decided that the complexity would not be warranted. EdF staff discussed the use of defensive measures (such as cyclic, uninterruptible, repetitive execution of safety system code) to mitigate potential vulnerability to CCF arising from the digital platform and provided additional information about diversity in the I&C systems at N4 plants.

At STUK, the discussion focused on issues being addressed in the license review for the new unit 3 under construction at the Olkiluoto NPP. The new unit at Olkiluoto will have a hardwired (i.e., based on field-programmable gate arrays [FPGAs]) diverse actuation backup system to mitigate vulnerability to

CCF. This system will also be quad redundant. According to the regulatory staff, the application of a hardwired backup system is licensee driven, not in response to any regulatory requirement. Regarding the use of priority actuation modules as an interface between actuators and multiple commanding systems (e.g., safety, control, manual), the EPR vendor had proposed using two different modules to address CCF concerns where multiple components are commanded through common interface type. The alternate module employs an additional programmable logic device (PLD) to provide diversity. The staff at STUK had not completed review of this approach but did express the opinion that this solution may add considerable complexity.

The use of diversity at the Sizewell B NPP in the United Kingdom is the most extensive example available from presently operating international NPPs. The HSE staff described how the "As Low As Reasonably Possible" (ALARP) principle in British law has driven their regulatory practices toward a "risk-based" approach. For Sizewell B, the risk-based considerations resulted in a reliability goal of 10^{-7} failure/demand. Given the inability to analytically demonstrate high reliability for software-based systems, conservative estimates of system reliability were used and two lines of protection proved necessary to achieve the desired reliability. The primary safety system is designed to address all design basis events (DBEs), while the secondary safety system addresses the more frequent events (e.g., anticipated operational occurrences). HSE engaged subject matter experts (SMEs) from noted universities in the United Kingdom to assess the design of the Sizewell safety systems. Ultimately, extensive analysis of the software-based primary safety system, coupled with the hardware-based secondary safety system to address higher-risk, higher-frequency events, provided acceptable proof of the necessary safety claims.

Under British law, the nuclear industry must fund safety research annually. Further research into digital system dependability and software diversity is being conducted under this program by the Centre for Software Reliability at City University London and the Safety Critical Systems Research Centre at Bristol University (see below). This research includes investigations into methods for characterizing software diversity and employing statistical testing approaches for validating software quality. At present, the prevailing approach in the United Kingdom is to first determine whether safety function reliability claims indicate a need for a second system to account for limitations/uncertainties in the reliability of the primary safety system for frequent events. If a secondary safety system is necessary, the high-level principles are employed to assess the diversity between the systems. These high-level principles are captured in a technical document on the common regulatory position by European regulators for software licensing (see below).[114]

5.1.2 International Technical Meetings on Common-Cause Failure

The IAEA initiated development of a technical report on avoiding CCF in digital I&C systems at NPPs through a consultancy meeting of international experts in March 2006. During this meeting, plans for a technical meeting on the topic were developed to facilitate the capture of international experience with CCF and engage additional technical experts in the determination of best-practice approaches for CCF avoidance and mitigation.

On June 19–21, the 2007 IAEA Technical Meeting on Avoiding Common-Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants was held in Bethesda, Maryland. The meeting was cohosted by the NRC, the U.S. Department of Energy (DOE), the Nuclear Energy Institute (NEI), and the Electric Power Research Institute (EPRI). The purpose of the meeting was to provide an expert forum to discuss the use of diversity as well as D3 principles to prevent CCFs in reactor protection and control systems. Practical aspects of the following areas were discussed:

- achieving functional, physical, and design diversity;
- defense-in-depth solutions;
- system robustness and fault tolerance;
- functional and physical separation;

- parallel systems supporting the same function;
- testing digital I&C systems for susceptibility to CCFs;
- possible CCFs triggered by maintenance activities and human errors;
- potential increase in CCF by the use of commercial-off-the-shelf (COTS) components;
- potential increase in CCF with increasing system complexity; and
- CCF-proof system design and requirement specification.

The importance and complexity of implementing and licensing digital I&C systems with the features of defense-in-depth, diversity, and independence in new NPP I&C designs were emphasized in several presentations.[115] Recent CCF events were highlighted as well as trends in the industry.

During the meeting, Arndt Lindner of the Institut für Sicherheitstechnologie (Institute for Safety Technology—ISTec) in Germany discussed the nature and consequences of software CCF. In particular, examples of effective mitigation approaches and diversity usage were presented. The conditions for CCF require the presence of one or more common faults and the occurrence of a triggering event to activate the faults coincidentally. Time and signal trajectories are considered to be the predominant triggering conditions. Taking a system-level view, ISTec recommendations for effective diversity usage were presented. A system model consisting of a parallel diverse redundant architecture with two coequal quad-redundant safety systems (see Figure 5.1) served as the sample case.

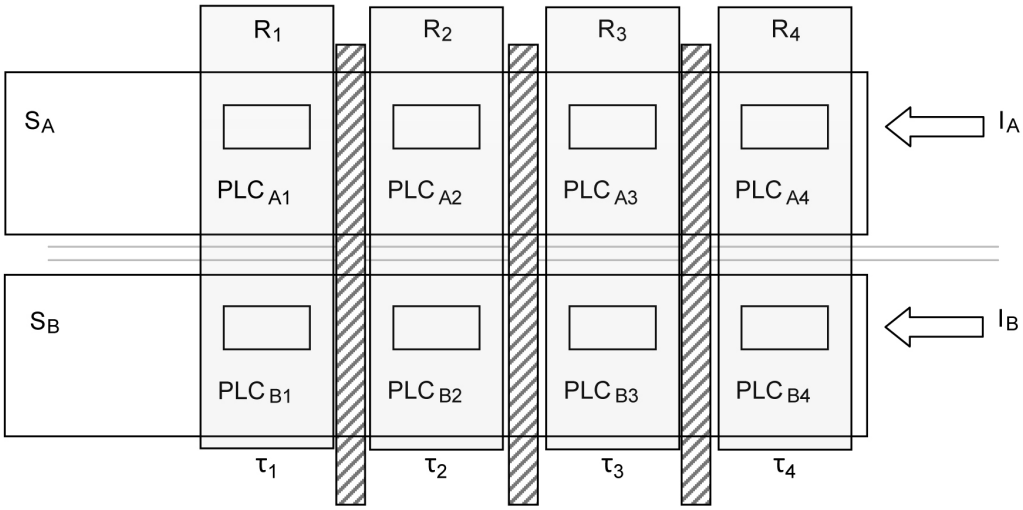

Figure 5.1. ISTec diversity usage approach for a parallel diverse redundant architecture. (Adapted from Ref. 18.)

The two systems or diversity groups, S_A and S_B, represented in Figure 5.1 are based on two different PLC-based platforms implemented in quad-redundant configurations (i.e., each system consists of four redundancies: R_1, R_2, R_3, and R_4). Additionally, different sets of measured parameters, I_A and I_B, provide diverse initiation criteria for each PIE covered by the parallel systems. An additional diversity (i.e., different internal time, τ) is invoked through staggered restarts/reboots of each redundancy (while in a bypassed condition) within a system to prevent coincident faulted internal states. This enforced internal time diversity is essentially a form of temporal or platform operational cycle (i.e., execution history) diversity.

The diversity usage in the ISTec case provides protection against common systematic faults due to specification flaws. In effect, the different requirements arising from the use of different functional relationships associated with diverse parameters and initiation criteria can reduce the prospect of common design deficiencies. Implementation of different functions in software can also help reduce the potential for common software faults between diverse systems. However, software CCF associated with execution history dependence can result from common platform usage (e.g., system software services) and system

integration (e.g., application/system software interfaces) faults. The introduction of temporal diversity through different internal times helps to resolve concerns about execution history dependence among redundancies executing the same software on the same platform. Specifically, it was noted that the use of different internal times between redundancies reduces commonality of signal trajectory in terms of internal states (and state transitions). Additionally, the use of different input sets between systems (i.e., signal and functional diversity) reduces commonality of signal trajectory in terms of input profile. Thus, the combination of enforced internal time diversity and input signal set diversity lessens the prospect of common triggering conditions related to time and signal trajectories. Essentially, any faults triggered by time (or execution) dependence would affect only one redundancy given the staggered restarts, while faults triggered by signal trajectory (arising from plant transients) would affect only one system or diversity group given the use of functional diversity.

Table 5.1 summarizes the diversity usage from the ISTec case. In some instances, inferences were made about specific criteria (e.g., equipment manufacturer diversity). Additionally, the recommended use of a form of temporal diversity (i.e., enforced internal time differences through staggered restarts) was

Table 5.1. Summary of diversity usage for the ISTec example case

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two coequal safety systems based on different PLCs
Equipment (Manufacturer)		
Different manufacturer—same design	x	Different PLC platforms from different suppliers
Equipment (Processing)		
Different logic processing architecture	x	Different microprocessor for each PLC platform
Different component integration architecture	x	Different platform bases (i.e., different board designs from different suppliers)
Functional		
Different purpose, function, control logic, or actuation means	x	Different functional relationships for diverse parameters and initiation criteria
Different response time scale	x	Intentionally different internal time for each redundancy within a system (i.e., different execution histories resulting from different start/restart times leading to different numbers of execution cycles) plus typical time response differences between systems from diverse parameter–PIE dynamic relationships

Table 5.1 (continued)

Diversity attribute	Usage[a]	Details
Life-cycle		
Different design organizations/companies	x	Separate companies supplying similar designs (i.e., PLC-based systems)
Different design/development teams (designers, engineers, programmers)	i	Inherent personnel differences between organizations involved
Different implementation/validation teams (testers, installers, or certification personnel)	i	Inherent personnel differences between organizations involved
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different algorithms and program architecture corresponding to different functional relationships between diverse parameters and initiation criteria
Different timing or order of execution	x	Impact of internal time differences due to staggered restarts of redundancies coupled with typical timing differences from asynchronous operation (between systems and redundancies) and different program architecture (between systems)
Signal		
Different parameters sensed by different physical effects	x	Different sensed parameters for each system (A and B) to enable implementation of diverse initiation criteria based on diverse parameters
Different parameters sensed by same physical effects	x	Different sensed parameters for each system (A and B) to enable implementation of diverse initiation criteria based on diverse parameters
Other Diversity Considerations		
Architecture consists of two coequal safety systems composed of different quad-redundant PLC-based systems (e.g., each system, A and B, composed of four redundancies based on PLC_A and PLC_B, respectively); Use of different input sets between systems reduces commonality of signal trajectory in terms of input profile, whereas the use of different internal times between redundancies reduces commonality of signal trajectory in terms of internal state; Note: Internal time diversity is captured above in terms of different response time scale and different timing, since there is no direct correspondence between the adapted NUREG/CR-6303 diversity criteria and this proposed diversity usage		Additional design measures to reduce common time trigger potential include no clock or calendar dependence and cyclical execution of application with no dependence on input values (plant status); Additional design measures to reduce combined temporal and signal trajectory trigger potential involves decoupling of application and system software

[a]Intentional diversity (x), inherent diversity (i).

treated as consisting of two time-related criteria: different time scale under functional diversity and different timing under logic diversity. However, the primary impact of the temporal diversity approach is to diversify the execution profiles of software-based systems by reducing the potential impact of platform usage deficiencies (e.g., buffer overwrites, stack overflows, pointer errors, race conditions).

Emil Ohlson of Forsmark Kraftgrupp AB discussed an event involving several CCF issues that occurred on July 2006 at Forsmark Unit 1 in Sweden. Human error during switchyard operations resulted in an electric arc and subsequent short circuit between two phases, which led to activation of the unit breaker and a turbine trip on overspeed. A CCF associated with the rectifiers in the uninterruptible power supply (UPS) units caused two of four subdivisions to be without power for a short time. A design weakness in the emergency diesel generator startup system resulted in a failure to initiate an automatic start of the diesel generators in two subdivisions. A CCF in the unit generator breakers for low-frequency protection delayed the switch from 400- to 70-kV off-site power. There was also a partial loss of information (two of four channels) in the main control room, which included control rod position, reactor pressure and level, and vital bus voltage. The unit operators followed written procedures to properly respond to the cascade of failures and achieve safe shutdown. Subsequently, modifications and design changes were implemented at Forsmark 1 regarding the UPS, low-frequency protection breakers, and power for the diesel generator startup system. Forsmark 2 and Oskarshamn 1 and 2 were also shut down for similar analysis and modifications. In another presentation on the followup to the Forsmark incident, Kristina Johansson of Statens Kärnkraftinspektion (Swedish Nuclear Power Inspectorate—SKI) noted that the modifications to Oskarshamn 1 proved to be the most challenging. Oskarshamn 1 has been in operation since 1972 but had recently completed plant updates (2002) to incorporate software-based I&C systems (i.e., a computer-based reactor protection system) and a hybrid digital main control room.

Other presentations at the technical meeting noted challenges and benefits of upgrading older plants to digital I&C systems. In particular, several presenters noted that adopting complete functional diversity in a modernization of older plants is extremely difficult. Steve Patterson of Diablo Canyon Nuclear Power Plant and John Hefler of Altran Associates described the plant's plans to upgrade its protection and control architecture to a digital platform to limit the effects of obsolescence and facilitate maintenance. The authors suggested that the biggest challenge in retrofitting a digital I&C system is that the diversity strategy must be developed up front before design, licensing, and equipment purchase can proceed.

In contrast to a plant retrofit, the I&C systems in Japanese advanced boiling-water reactor (ABWR) plants incorporated digital I&C technology from the initial design stage. Susumu Kunito of Tokyo Electric Power Company noted that Kashiwazaki-Kariwa units 6 and 7 (KK-6 and -7) have more than 10 years of commercial operation with no severe or common I&C failures. The simple software structure was credited with uncomplicated design, development, and validation of the digital platform. As discussed in Chapter 4, system diversity for KK-6 and -7 is provided by manual initiation of hardwired backup systems and traditional functional diversity through diverse actuation mechanisms.

Finally, there were several presentations given on risk insights for D3 assessments, classification approaches for CCF, and evaluation of available failure experience for software-based systems in the nuclear power industry. In particular, John Bickel of Evergreen Safety and Reliability Technologies reported on an investigation into experience with digital core protection calculators (CPCs). Observing that several combustion engineering (CE) plants in the United States and South Korea began using digital CPCs as early as the late 1970s, the experience with these systems can provide an extensive knowledge base for analysis. Mr. Bickel identified 141 license event reports representing over 140 reactor years in U.S. CE plants between 1984 and 2005. Of those reports analyzed, only one software CCF was noted out of 26 CCFs overall.

5.2 British Research on Diverse Software

As previously noted, the British nuclear power industry is funding safety research under the U.K. Nuclear Research Programme to address key issues.[116] Principally, this research is being conducted by the Centre for Software Reliability at City University London and the Critical Systems Research Centre at Bristol University under research contracts established for the DIverse Software PrOject (DISPO). The DISPO projects began in 1996 and were conducted initially over 3-year periods. Recent projects have been conducted on an annual basis with the latest project, DISPO5, covering 2006 and 2007.

The primary methodologies used in the DISPO research are

- detailed problem parsing,
- careful progression of research topics,
- cautious logic about overextending conclusions, and
- reliance upon probabilistic models to understand the effects of commonality or separation influences on producing diverse versions of a system for a diverse redundant configuration.

The DISPO research focuses on the use of diversity in digital systems. The basic application of diversity within an I&C architecture composed of software-based systems involves parallel redundant systems or subsystems (e.g., versions, channels, redundancies) that perform the same or equivalent functions and are arranged in a one-out-of-*N* or voted configuration. The simplest example is a diverse redundant pair of systems (or redundancy versions) that are implemented in a one-out-of-two (logical "OR") configuration.

The DISPO research emphasis involves the use of diversity as a means to achieve system dependability, with particular emphasis on accounting for the likely presence of faults in software. Dependability is defined as the "[t]rustworthiness of a delivered service (e.g., a safety function) such that reliance can justifiably be placed on this service." Attributes of dependability include reliability, availability, and safety. The findings of the research contribute to understanding the relationship between diversity and failure independence, determining life-cycle decisions that encourage diversity, and assessing the qualitative impact of diversity.

An additional consideration introduced recently to the DISPO research is the application of diversity in the assessment of dependability. Essentially, this aspect of the current investigation addresses the use of "diverse arguments." This study involves the consideration of diversity to address weaknesses in the arguments that are used to support dependability claims (i.e., "multi-legged" arguments). The findings suggest that the potential increase in confidence for a claim depends crucially on notions of dependence between arguments (e.g., between their assumptions).

5.2.1 General Findings of the DISPO Program

The relevant measure of interest for system dependability is the probability of failure on demand (*pfd*) for the system. A common erroneous assumption is that different versions resulting from "independent" (or, more accurately, separate) development processes result in independence of failure behavior.[117] Experimental studies by Knight and Leveson[118] showed that "independently" developed software versions did not necessarily fail independently. In essence, the failures identified in the investigation were not statistically independent but rather showed a strong positive correlation between the failure behaviors of the different versions solving the same problem. It is noted that even with separate development teams and processes, common influences, assumptions, understandings, and mistakes may be present and there may be only conditional independence of version failures. In effect, dependent failure sets (i.e., the set of demands that result in failure due to the presence of faults) may exist. Basically, there is often an erroneous assumption that the common *pfd* of two versions is zero and

that the *pfd* of the diverse redundant system (composed of the separately developed versions) is exactly equal to the product of the probabilities associated to each of the two failures sets. As this assumption does not always prove true, a conclusive mathematical basis often cannot be established to demonstrate that increasing diversity between versions will increase diversity against failure.

As a consequence of knowledge capture from system development experience and experiments conducted during the multiyear research program, a principal DISPO finding is that claims for statistical independence between failures of diverse versions have not been reasonably demonstrated, which limits the provability of dependability for a system based on design diversity. Essentially, independent development is not likely to be solely sufficient for the version failures to be independent for a randomly chosen demand. Nevertheless, it is observed that increasing diversity may increase reliability for separate developments where the reliability improvement can be enhanced by stronger diversity enforcement mechanisms. The research has shown that confidence in a dependability claim can be increased through the use of design diversity. The conclusion is that "forced diversity is a good thing," although individual or collective effects are difficult to quantify. The research has also shown that some forms of dependence or interaction (e.g., shared knowledge about requirement deficiencies) may bring substantial benefit not only to the development process but also to the resulting system reliability.

Two key technical issues investigated by the DISPO research team involve the achievement of dependability and the assessment of dependability. Regarding the former, the application of diversity in digital I&C systems can be encouraged by invoking decisions in the management of the system design process. These choices are described as diversity-seeking decisions (DSDs). The effect of such decisions is to promote a high degree of fault diversity. The remaining challenge arises because the effect of these decisions on failure diversity (i.e., achieving reduced correlation between failure behaviors of different versions) is indirect. Figure 5.2 illustrates the relationship. There is insufficient knowledge to definitively guide the choice among DSDs to effectively produce the desired failure diversity and thus, in turn, improve system dependability.

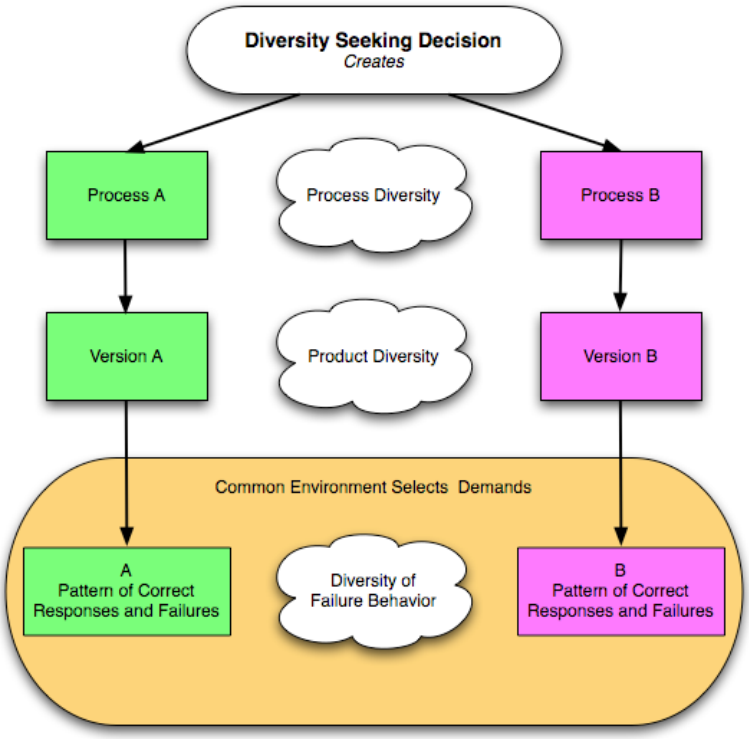

Figure 5.2. The different facets of diversity and their interdependence. (Adapted from Ref. 119.**)**

Regarding the latter issue, assessment of dependability involves establishing assurance that critical (or safety) functions are protected against CCF through diversity. Assessment involves both oversight of the development processes to ascertain that diversity is present and understanding of the impact on the *pfd* corresponding to each diverse system. The DISPO research has contributed to improved reliability assessment for diverse systems in terms of "independent fault" models. However, since there is not a known definitive relationship between the DSD-induced product/fault independence and the desired failure independence, dependencies are to be expected. Nevertheless, research findings indicate that if the separate development processes are managed to enforce diversity, then independence (or possibly negative correlation) between failures of design-diverse versions is promoted. The problem remains that even when the presence of diversity is established, there are no quantifiable measures to determine its efficacy. Thus, the DISPO research added a focused investigation on the use of arguments diversity as a means to resolve weaknesses in dependability claims.

5.2.2 Practices for Achieving Diversity

As a fundamental element of this research program, the DISPO research team investigated the effect of variation of difficulty in which the concept of "difficulty functions" was developed.[120] A difficulty function is described as the probability that a randomly chosen version would fail on a given demand, which indicates the difficulty in achieving the desired response (or conversely, the ease of making a mistake in implementing the desired response to that demand). The presumption is that mistakes correlate with the difficulty posed by demands or requirements. Essentially, the idea is that it is possible to develop dissimilar software versions by employing different processes (e.g., different software engineering practices and procedures), leading to different difficulty functions over the space of demands. The desired result is negative covariance between the difficulty functions for different versions, which means that demands that are "hard" to satisfy (or cause difficulty) for one version are not the same as those demands that are difficult for another version. Difficulty variation may be achieved by decoupling development activities that are essentially the same by substituting different influence factors for each version or by forcing diversity within development activities through the intentional use of different processes, methods, tools, etc.

Key findings have been published regarding practices that have the potential for increasing the extent of diversity between redundant implementations of software or software-based systems.[119] Limitations of existing knowledge preclude definitive diversity recommendations based on quantitative estimation of the combined effect of specific practices. However, useful indications of the qualitative effect have been observed and provide some measure of justification, beyond intuitive argument, for decisions that contribute to diversity. The presentation of DISPO research findings in Ref. 119 summarizes prospective means for achieving failure diversity with respect to design faults that induce failures, discusses expected advantages for each method, and identifies available anecdotal evidence.

A means of "forcing" diversity is to impose constraints on the software-based system development process to introduce development differences between two versions of a diverse redundant architecture. The desired benefit is that the difficulties presented to each development team will differ, leading to the credible prospect that common faults would be unlikely to occur in the two versions. Based on the research, examples of DSDs include the following: "using different development environments, different tools and languages at every level of specification, design and coding, implementing each function with different algorithms, applying different V&V methods, etc." Table 5.2 summarizes the identified DSDs that can contribute to achieving the goal of failure independence of software-based systems through data diversity, design diversity, and functional diversity. In this context, data diversity refers primarily to input differences achieved by measurement dissimilarity, stochastic signal behavior, analytical variation (reexpression), and loose coupling between functional instantiations (e.g., asynchronous execution of

function in separate systems). Design diversity embodies all of the design options that can engender diversity in the development of parallel systems that provide the same or similar input-to-output function.

Table 5.2. Overview of diversity-seeking decisions from U.K. DISPO research

Diversity-seeking decision	
DSD type	**Variant**
Data Diversity	
Diverse inputs	— Stochastic input variations — Reexpression of inputs — Different signal sources (with functional diversity)
Design Diversity	
Separate developments	
Diverse development teams	
Diverse descriptions, programming languages, and notations	
Diverse requirements or specifications	— Different expressions of identical requirements — Different required properties/constraints providing the same behavior — Different required behavior
Diverse development methods	
Diverse verification, validation, and/or testing	
Diverse code (automatic code transformation)	
Diverse development platforms	— Different tools — Different compilers
Diverse support platform (runtime platform)	— Separation and loose coupling — Different timing — Different (dissimilar) hardware — Different operating systems or runtime executives
Functional Diversity	
Diverse functionality	

This diversity includes differences in the system life-cycle process (e.g., resources, methods, tools) as well as different realizations of the functionality. Establishing "cognitive" diversity for the designers, implementers, testers, and so forth is central to minimizing the potential for common mistakes, errors, and misunderstandings that can lead to systematic faults. Functional diversity involves the establishment of different functional relationships (e.g., diverse parameter and initiation criteria to protect against the same PIE) as the basis for diversity. Signal diversity as discussed in this diversity research is necessary to enable functional diversity.

For many of the plausible DSDs, the mechanism by which dependability improvement can be achieved is not fully understood (i.e., "how" specifically they work and, as a result, "why" or "whether" they will work). Most of these DSDs address the likelihood of faults rather than failures, so the recommendations do not directly resolve CCF potential. However, given the current limitations in knowledge about the relationship between faults and failures, it is considered that taking action to reduce the potential common faults is a reasonable approach. Additionally, the research team notes that diverse runtime platforms are considered to be "the only form of diversity that is generally and absolutely necessary, as the system designers usually have no other effective defence against platform faults."

Some additional findings on achieving diversity between (among) two or more versions include the following:

- Combining diversity in design with diversity in fault removal can enable improved robustness against CCF while enhancing cost-effectiveness.
- The optimum combination of diversity attributes and diversity criteria is unknowable in general, given the inadequate understanding of the direct relationship between minimizing common faults with the goal of minimizing common failure.
- The prospective increase in reliability through the use of diverse separate development processes can only be characterized realistically as an expectation that the uncertainty associated with the system reliability will be greater if the introduction of diversity through DSDs is not carefully administered to encourage independence.

Two forms of forced diversity are discussed extensively in the DISPO research: (1) "normal" forced diversity and (2) functional diversity. The first approach to forced diversity involves imposed differences in development activities leading to different design versions that are based on the same underlying physical relationships that correspond to use of the same or similar inputs to indicate each specific event. The second approach to forced diversity involves employing alternate underlying physical relationships and results in different design versions utilizing different inputs to provide indication of each event. It is noted that claims of independence among functionally diverse systems are not absolutely justified, and there is a distinct possibility of correlated failures.[121] Thus, functional diversity, while very effective at addressing key CCF vulnerabilities, can benefit from application of other DSDs.

Table 5.3 translates the recommended DSDs into corresponding diversity usage in terms of the diversity criteria adapted from NUREG/CR-6303. Identification of the relevant DSDs is provided in the discussion of details for each diversity criterion. Where a DSD specifies diversity in design approach, method, expression, or tool, these DSDs have been attributed to the diversity criteria that are affected.

Table 5.3. Summary of diversity usage from the UK DISPO research findings

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Two coequal safety systems based on different microprocessors (diverse hardware)
Equipment (Manufacturer)		
Different manufacturer—same design	x	Different software-based platforms from different suppliers (separate developments, diverse runtime platform)
Equipment (Processing)		
Different logic processing architecture	x	Different microprocessor for each platform (diverse runtime platform)
Different component integration architecture	x	Different circuit board designs from different platform suppliers (diverse runtime platform—diverse hardware)

Table 5.3 (continued)

Diversity attribute	Usage[a]	Details
Different data-flow architecture	x	Different bus architectures from different platform suppliers (diverse runtime platform—diverse hardware)
Functional		
Different purpose, function, control logic, or actuation means	x	Different functional relationships for diverse parameters and initiation criteria or different scope/constraints through reduced functionality or different purpose such as protection vs checking (different requirements or specifications, different functionality)
Life-cycle		
Different design organizations/companies	x	Separate companies supplying similar designs (separate developments, diverse development teams)
Different design/development teams (designers, engineers, programmers)	i	Inherent personnel differences between organizations involved (diverse development teams, diverse development methods, diverse tools)
Different implementation/validation teams (testers, installers, or certification personnel)	i	Inherent personnel differences between organizations involved (diverse development teams, diverse verification, validation, and testing, diverse tools)
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different algorithms for the same or different functions/ logic, different program architectures, different expressions of requirements or function (different requirements or specifications, diversity in description and notations, automatic code transformation, diverse compilers, different functionality)
Different timing or order of execution	x	Different sequencing of operations, asynchronous execution, decoupling from time-dependent disturbances (separation and loose coupling, diverse timing)
Different runtime environment	x	Different operating systems or runtime executives (diverse runtime platform)
Different functional representation	x	Different software instantiation (diversity in programming

Table 5.3 (continued)

Diversity attribute	Usage[a]	Details
		languages, automatic code transformation, diverse compilers)
Signal		
Different parameters sensed by different physical effects	x	Different sensed parameters (data diversity, different functionality)
Different parameters sensed by same physical effects	x	Different sensed parameters (data diversity, different functionality)
Same parameter sensed by a different redundant set of similar sensors	x	Separate data sources with stochastic differences (data diversity, separation and loose coupling)
Other Diversity Considerations		
Parallel diverse architecture Diversity-seeking decisions are intended to diversify faults with the expectation that failure diversification will result consequently Design diversity in the DISPO context addresses numerous DSDs related to diversifying the inputs, methods, and tools employed within the life-cycle process for separate developments		The general architecture is presumed to consist of two or more coequal safety systems or subsystems (i.e., "diverse modular redundancy") An alternate architecture provides checked redundancies (i.e., "primary-checker")

[a]Intentional diversity (x), inherent diversity (i).

5.3 International Guidance for Coping with Common-Cause Failure

5.3.1 Common Regulatory Position in Europe

The Western European Nuclear Regulators' Association (WENRA) invited European safety authorities to contribute to the completion of a common position on the licensing of safety-critical software. The objectives of this effort were determination of best practices concerning key licensing issues posed by computer-based implementations of safety functions at NPPs and establishment of a consensus position. The work group assembled for this effort, which continued a collaborative exchange that began in the mid-1990s, consisted of a group of regulators and safety experts representing seven organizations from six countries. The participating organizations are Association Vinçotte Nuclear (AVN) of Belgium, STUK of Finland, Bundesamt für Strahlenschutz (Federal Office for Radiation Protection—BfS) and ISTec of Germany, Consejo de Seguridad Nuclear (Nuclear Safety Council—CSN) of Spain, SKI of Sweden, and HSE Nuclear Installations Inspectorate (NII) of the United Kingdom. The outcome of this collaborative interaction is a report documenting the common position of the participating safety authorities.[114] The report is directly available from any of the seven organizations.

The common position of the European regulators consists of consensus requirements (based on unanimous agreement) and recommended practices (based on general agreement) addressing key licensing considerations. The clauses that constitute the common position explicitly apply to safety systems and relate to issues arising from the use of digital and programmable technology. These issues address generic and life-cycle-phase aspects of licensing computer-based safety systems. The topics addressing specific stages of the design and development process for digital safety systems are computer-based system requirements, hazard analysis, safety demonstration, reliability targets, defense against CCF, communication system design, fault-tolerant architectures, software design and structure, coding and programming directives, diversification and testing (plans, coverage, and traceability), validation and commissioning, change control and configuration management, and operational requirements. The topics

with general or full life-cycle implications are safety demonstration, safety categories and graded software requirements, reference standards, use and validation of preexisting software, tools, organizational requirements, software quality assurance program and plan, security, use of formal methods, independent assessment, graded requirements for software of safety-related systems, software design diversity, software reliability, and data collection for operational experience. Clearly, the requirements for software design diversity are of particular relevance to this research effort.

For the design of computer-based safety systems, the common position requires that "principles of redundancy, diversity, physical isolation, segregation, and separation between safety functions, safety related functions and functions not important to safety" be applied to computer system architecture design. These principles address considerations such as reliability and independence while providing protection against CCF. Architectural and other design decisions influence the necessity and the nature of software design diversity employed. The adoption of a simple hardwired system as the diverse alternative to a computer-based safety system can resolve software-related CCF concerns. In fact, this approach is emphasized as a best-practice recommendation for this topic. The use of fundamentally diverse technologies for primary and secondary safety systems at the Sizewell NPP (see Chapter 4), coupled with enforced functional diversity, provides an example that adheres to this recommended practice. However, it is recognized that multiple computer-based diverse systems are more likely to be adopted given the increasing prominence of digital technology; therefore, specific requirements for ensuring software design diversity are provided.

The common position on software design diversity addresses design decisions (i.e., DSDs) that invoke methods, techniques, and measures to force software design diversity. The goal is to diversify failure behavior among diverse software-based systems. Functional diversity is the foremost DSD identified in the common position, and it is required to be implemented whenever possible for safety system elements that are intended to be diverse. Additionally, the functionally diverse systems are required to be associated with the same safety class and subject to the same graded requirements. Other DSDs specified for the design of computer-based systems are independence of development teams (with no direct communication between teams); different description languages (e.g., specification languages) and notations; different programming languages; different development methods; different development platforms, tools, and compilers; different hardware; and diverse verification and validation (e.g., back-to-back testing).

It is required that the safety demonstration provide an analysis of potential CCFs with justification of the impact of diversity usage on reliability and CCF potential arising from any commonalities in the product (e.g., systems, redundancies, and components) or process (e.g., life-cycle activities and resources). Simplicity of design and implementation is also emphasized to keep complexity of the system and software to a minimum that is commensurate with satisfying safety requirements. Thus, there is a reliance on sufficiently detailed analysis to determine the need for diversity, confirm the types of diversity providing the appropriate mitigation, and justify omissions of diversity where need is indicated.

Table 5.4 summarizes the common position on diversity usage in terms of the diversity criteria adapted from NUREG/CR-6303. The specific DSDs associated with each diversity criterion are identified in parenthesis. Where the common position specifies diversity in design approach, method, expression, or tool, these DSDs have been attributed to the diversity criteria that are affected.

Table 5.4. Summary of diversity usage for the European common position

Diversity attribute	Usage[a]	Details
Design		
Different architectures	x	Different computer-based systems based on different microprocessors (different hardware)
Equipment (Manufacturer)		
Same manufacturer—different version	x	Supplier/manufacturer choice unspecified
Equipment (Processing)		
Different logic processing architecture	x	Different microprocessors (different hardware)
Functional		
Different purpose, function, control logic, or actuation means	x	Use of different parameters to achieve same safety objective and different requirements representations (functional diversity, different description languages and notations)
Life-cycle		
Different management teams within same company	x	Fully separate development teams throughout system life-cycle (independent development teams with no direct communication)
Different design/development teams (designers, engineers, programmers)	x	Separate teams using different approaches and resources [e.g., forced diversity] (independent teams; different development methods; different development platforms, tools, and compilers)
Different implementation/validation teams (testers, installers, or certification personnel)	x	Separate teams using different approaches (independent development teams, diverse V&V)
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different functions and functional representations (functional diversity [simple vs more computationally complex], different description languages and notations)
Different functional representation	x	Different functional implementation (different programming languages, different compilers)
Signal		
Different parameters sensed by different physical effects	x	Different sensed parameters (functional diversity)
Different parameters sensed by same physical effects	x	Different sensed parameters (functional diversity)

Draft

Table 5.4. (continued)

Diversity attribute	Usage[a]	Details
Other Diversity Considerations		
Parallel diverse architecture Technology diversity (e.g., analog vs digital) is a recommended best practice Architectural independence required Complexity must be minimized CCF analysis required Digital (e.g., software-based) diversity must preserve plant-level functional diversity		Parallel coequal independent diverse computer-based systems are presumed; Determinations of the need for diversity, the type(s) of diversity to be used, and the omission of diversity must be justified; Where a diversity need is identified, functional diversity is required whenever feasible; CCF analysis must address reliability impact and risk posed by commonalities (e.g., modules, tools, development methods); design complexity must be minimized proportionate to the safety needs Note: Adoption of diverse systems based on fundamentally diverse technology (i.e., non-computer-based diverse system) results in substantially different diversity usage (equivalent to Sizewell example)

[a]Intentional diversity (x).

5.3.2 International Standards

The IEC issues and maintains international normative standards for all electrical, electronic, and related technologies. These standards are developed according to consensus procedures by technical experts supplied by the national committees of participating countries. Subcommittee (SC) 45A, Instrumentation and Control of Nuclear Facilities, of technical committee (TC) 45, Nuclear Instrumentation (TC45/SC45A), has responsibility for standards that apply to I&C systems important to safety in nuclear-energy-generation facilities (e.g., NPPs). These standards cover the entire life-cycle of I&C systems at these facilities, ranging from conception through design, manufacture, test, installation, commissioning, operation, maintenance, aging management, modernization, and decommissioning. Key standards relevant to this research investigation that address overall I&C architecture and system design and software for systems important to safety are discussed in Sects. 5.3.2.1 through 5.3.2.3 and are summarized in aggregate in Section 5.4.2.4. Of particular interest is a recently issued standard providing requirements to cope with CCF, IEC 62340 (see Section 5.3.2.3).

5.3.2.1 IEC 61513

The IEC standard that covers the system aspects of I&C systems important to safety, including computer-based systems, is IEC 61513, "Nuclear Power Plants—Instrumentation and control for systems important to safety—General requirements for systems."[122] This top-level standard for I&C systems important to safety at NPPs is the nuclear power industry derivative of the multipart parent document on functional safety of industrial process measurement and control systems (i.e., IEC 61508, "Functional

safety of electrical/electronic/programmable electronic safety related systems"). Comparable to the parent standard for general industrial-sector application, IEC 61513 defines a life-cycle process for I&C systems important to safety at NPPs and contains the top-level requirements on system functions, architecture, and I&C system design for application to those I&C systems. These requirements are intended to be independent of technology and apply to hardwired (i.e., analog) and software-based (i.e., digital) systems.

IEC 61513 requires analyses to verify the I&C architecture design at an NPP. A specified analysis that must be conducted is an "evaluation of the effectiveness of measures used to reduce the sensitivity of the safety groups to CCF" with an emphasis on Category A functions. As part of this analysis, common components, identical hardware, and identical software must be determined. Where such commonalities are identified, justification must be provided to demonstrate that the potential for CCF is low.

Correspondingly, IEC 61513 gives requirements for defense against CCF. As noted, the standard emphasizes I&C systems that perform Category A functions in addressing defense against CCF within I&C systems important to safety. Categorization of function is provided in IEC 61226, "Nuclear power plants—Instrumentation and control systems important for safety—Classification,"[123] based on the consequence of malfunction. Category A functions are safety functions that play a principal role in the safety of the NPP. These functions are implemented in Class 1 systems (i.e., protection systems, safety actuation systems, emergency power actuation systems).

In IEC 61513, the design goal for defending against CCF is specified as providing "measures against the occurrence of a CCF within I&C systems implementing different lines of defence against the same PIE." The identified measures include the following:

- design provisions promoting tolerance of hazardous plant events (e.g., external influences and internal hazards),
- design provisions resulting in insensitivity to plant demand design (e.g., decoupling execution from plant status to avoid common triggering conditions),
- design provision to minimize the use of common elements or support systems among lines of defense,
- quality assurance and fault tolerance to minimize the potential impact of systematic faults,
- strategic design decisions to manage complexity, and
- design differences through application of diverse features.

For each design measure, requirements and recommendations are given to guide the usage of these defensive approaches. This guidance is briefly reviewed below, with a subsequent focused treatment of the specific guidance on diversity usage as a CCF defense.

Design provisions enabling hazard tolerance include separation, independence, prevention, and compatibility (e.g., electromagnetic and environmental).

Minimizing the risk of common triggering conditions arising from demand profile involves analysis of I&C components to identify loadings (e.g., electrical, computational) that are demand dependent and reduction of the coupling between I&C system operation and plant conditions.

Avoidance of common elements involves architectural provisions such as independence across different lines of defense for I&C systems protecting against the same PIE, independent monitoring and control capabilities to ensure safety functions in the event of a failure, minimized potential for CCF within independent manual control capabilities that back up automatic safety functions, and arbitration or prioritization of commands for ESF actuation that may conflict during failure conditions.

Measures to reduce the risk due to systematic faults include application of high-quality planning for development and manufacturing life-cycle activities, provision of self-supervision capabilities (e.g., exception-handling routines, watchdog timer, plausibility-checking algorithms), and definition and annunciation of a safe state to be achieved upon detection of failures.

Analysis of the I&C system architecture and individual system designs contributes to managing complexity. Such an analysis involves consideration of the degree to which either computer-based or hardwired technologies are employed and the reliance on human action to ensure that safety functions are maintained.

The design measure of interest for this research is the provision of diversity as an effective means for defending against CCF. Diversities that are identified in IEC 61315 include human diversity, signal diversity, functional diversity, design and test diversity, software diversity, and equipment diversity.

Specific guidance on diversity usage involves recommended practices more than requirements per se. The standard recommends that diversity be used to achieve high reliability when uncertainties exist in the evaluation of a design. Combinations of signal and functional diversities are cited as "particularly effective methods to reduce risk of CCF due to errors in the requirements specifications or in the specification and implementation of application software." For complex I&C systems where there is a limited experience base, equipment diversity is identified as a means to address hardware CCF and contribute to defense against system software faults. Use of diverse methods or procedures for verification and validation is cited as a means to contribute to CCF avoidance without introducing design complexity. Examples of this approach include back-to-back testing with a simulator and use of different testing facilities. Finally, it is required that the effectiveness of any diversity usage that is claimed to minimize the potential for CCF be analyzed and documented with appropriate justification.

5.3.2.2 IEC 60880

IEC 60880, "Nuclear power plants—Instrumentation and control systems important to safety—Software aspects for computer-based systems performing Category A functions,"[124] supplements IEC 61513 by providing "requirements for the software of computer-based I&C systems of NPPs performing functions of safety Category A." The second edition of this standard encompasses both the first edition, issued in 1986, and the supplemental part 2, issued in 2000, along with updated requirements covering the software aspects of the I&C system life-cycle process (as defined in IEC 61513). Additionally, IEC 60800 includes an informative annex on defense against CCFs as well as other annexes on details for the safety software life-cycle process, software requirements and software development, tools for software qualification, and requirements on preexisting software.

In particular, IEC 60880 provides requirements for defense against "software design and coding faults" that can result in the potential for CCF in software-based implementations of Category A functions. The standard states that software "by itself does not have a CCF mode." Instead, CCF is a system failure issue that arises from "faults in the functional requirements, system design, or in the software." Thus, the standard recommends that the potential effects of software CCF be considered in the application of the defense-in-depth principle, with appropriate countermeasures employed throughout the development and evaluation processes. In particular, these countermeasures should be considered in the design, implementation, verification, and validation of each layer of defense and in the assessment of independence and diversity among redundant layers of defense. It is noted that diversity usage can not only reduce the potential for CCF but also enhance reliability of some I&C systems.

The nature of CCF, as described in IEC 60880, is that faults may exist undetected in software until challenged by a specific unanticipated or untested signal trajectory. Thus, the mechanism for CCF is the presence of at least one common latent fault within systems or redundancies that defend against the same

PIE and the coincident exposure to specific signal trajectories in a sensitive time frame. IEC 60880 specifically addresses faults arising from the software engineering process.

The standard states that high-quality software engineering practices are the most important defense against software CCF. It is also noted that the use of self-monitoring features can help to limit the potential impact of software CCF. However, since error-free software cannot be assured in general, IEC 60880 requires an analysis of the potential sources and consequences of software CCF as part of the I&C architecture design assessment. The guidance provided for the analysis is consistent with the guidance on D3 assessments given in NUREG/CR-6303.

Guidance regarding the use of diversity as a countermeasure to address software CCF is given as recommended practices. The primary implementation strategy identified is the use of functional diversity among independent systems. If functional diversity is not feasible, then consideration of system diversity, diverse software features, and diverse design approaches is advised. It is required that justification of the strategy employed be documented. Specific techniques to address the software implementation are identified as diversification of the operational conditions for the software, avoidance of failure propagation paths, mitigation of the impact of CCF, and use of different specifications for different software implementations of the same functional requirements. It is noted that N-version programming is not recommended.

Informative discussion of CCF considerations and diversity options is given in Annex G. This information is not considered part of the normative guidance of the standard. Commonalities that can result in CCF vulnerability are identified as including common software, architecture, algorithms, development methods, tools, implementation methods, staffing, and management. A discussion of the role of signal trajectories in triggering CCFs is provided. Also, the impact of abnormal hardware failures, plant conditions, and events that result from unforeseen signal trajectories, which include unexpected software states, is noted. The annex presents specific diversity features that can be considered for resolving software CCF. These features include the following:

- software diversity features (e.g., functional diversity, different design specifications, and different functional implementations);
- diversity at the system level (e.g., independent diverse actuation systems, different basic technology, different types of computers, hardware modules and major design concepts, a different classes of computers);
- diverse design approaches (e.g., algorithms, system data, hardware for inputs or interfaces, timing and sequencing);
- different design and implementation methods (e.g., languages, compilers, support libraries, software tools, programming techniques, system and application software, software structures, data);
- diverse testing; and
- diverse management approaches (e.g., separation of design teams, forced diversity between design teams, restricted communication between teams, different staff).

The potential benefit of functional or software diversity usage is derived from the increased protection against software CCF arising from adequately diverse versions. However, it is noted that potential disadvantages can include greater overall complexity, increased risk of spurious actuation, more complex specifications and design, modification problems (e.g., maintaining diversity during modification), cost, and potential lower quality of diverse versions. Thus, improvements in the reliability of safety functions should be considered in the justification of diversity usage.

5.3.2.3 IEC 62340

The IEC has recently issued a new standard addressing means to cope with CCFs in I&C systems that perform Category A functions (e.g., safety systems). The standard is IEC 62340, "Nuclear power plants—Instrumentation and control systems important to safety—Requirements for coping with common cause failure (CCF)."[11] Specifically, IEC 62340 gives requirements regarding the avoidance and mitigation of CCF and provides principles to ensure independence among the I&C systems that are implemented to overcome CCF vulnerabilities.

In providing a strategy to cope with CCF, IEC 62340 discusses the conditions that cause CCF. Basically, the standard adopts the position that a CCF can occur only when two factors are present concurrently:

- a latent systematic fault exists, <u>and</u>
- a corresponding triggering mechanism is activated by a signal trajectory.

The standard defines a "signal trajectory" as the "time histories of all equipment conditions, internal states, input signals and operator inputs which determine the outputs of a system." A "latent fault" presupposes that the fault is not identified by validation testing, self-supervision, or periodic testing in the field. Also, latent systematic faults may originate from any phase of the life-cycle (e.g., design phase, manufacturing phase, operational procedures).

Systematic faults within I&C systems may result from human errors in design or implementation (considered to be technology independent) or may arise from physical effects during the manufacturing process (considered to be technology dependent). Common sources of these faults include flaws in the safety function requirements or system specifications, inadequate determination of external (e.g., environmental) stress factors or hardware design limits, and design deficiencies. Systematic faults can also be introduced during maintenance, because of limited analysis and testing during modification. These faults can result from activities such as modification of setpoints, use of revised versions of spare parts, or modernization of I&C system components.

Triggering conditions may be caused by external factors such as common demand profiles (e.g., signal transients), environmental stress, or temporal dependencies (e.g., specific real time or calendar dates). Signal trajectory triggers can involve not only input signal transients but also internal states of digital systems and past execution history. Additionally, the existence of fault propagation mechanisms (e.g., communication interlinks) may propagate failure through mechanisms such as functional dependencies, corrupted data, or failed communication processes to cause consequential failure of other redundancies.

The strategic approach to coping with CCF involves reducing the likelihood of systematic faults being incorporated into independent systems or redundancies, minimizing the presence of failure propagation paths among systems, and reducing the possibility of concurrent exposure to triggering conditions. Accordingly, IEC 62340 provides requirements to establish a coping strategy for CCF. These requirements are grouped in terms of four areas of impact, which are characterized as follows:

- overcoming flaws in the requirements specification,
- preventing coincident failures through design measures,
- tolerating postulated latent software faults, and
- avoiding system failure due to maintenance during operation.

The requirements provided in each area are summarized in the following sections.

5.3.2.3.1 Overcoming Flaws in the Requirements Specification

It is noted that flawed requirements can lead to systematic faults that create the potential for CCF vulnerability. IEC 62340 states that functional diversity serves as an effective means of coping with the prospect of such faults through the provision of alternate requirements as the basis for diverse systems, subsystems, or redundancies. To enable this coping strategy, an analysis of design basis accidents (DBAs) and relevant DBEs that are affected by I&C system CCF must be performed. It is noted that most large transients influence nearly all safety parameters in parallel. Thus, the application of functional diversity requires a more detailed analysis of DBEs as a precondition. From this analysis, the subset of DBEs that could cause unacceptable consequences in the presence of I&C system CCF is determined and at least one alternate safety parameter must be identified for each event. On this basis, the specification of diverse safety functions is established and can be implemented through a selected design strategy, subject to demonstration that plant safety targets are achieved. Two prospective design strategies are noted: (1) to group diverse safety functions into independent systems to give full coverage by either system and (2) to implement the complete set of functions in a primary safety system with a reduced-scope set of functions covered by a lower safety class system based on diverse equipment.

The application of functional diversity in concert with the defense-in-depth principle requires "the identification of those specific safety I&C functions that can ensure independently that the main plant safety targets are met." These diverse safety functions must be allocated to independent I&C systems that are implemented in an architectural arrangement such that plant safety is maintained even in the presence of a postulated failure of one I&C system. Essentially, the failure of one I&C system must not affect the other I&C systems that provide compensating safety functions or lines of defense. The independent performance of the diverse safety functions must be validated and documented.

5.3.2.3.2 Preventing Coincident Failures Through Application of Design Measures

Independence is an essential element of any coping strategy because it enables the impact of CCF to be limited to a single I&C system. The principle of independence is satisfied if a postulated failure of one I&C system does not prevent the other I&C systems from performing their intended safety functions. Effective design principles to defend against CCF begin with requirements that ensure high-quality, high-integrity I&C systems. Adherence to the requirements of existing standards is reinforced in this standard. Specifically, the relevant requirements that must be fulfilled are cited as the following (with the referenced standard identified):

- system design: IEC 61513,
- software design: IEC 60880,
- physical separation: IEC 60709,[125] and
- component qualification: IEC 60780[126] (environmental) and IEC 60980[127] (seismic).

In addition to the requirements in the standards above, additional requirements are provided by IEC 62340 to ensure the independent performance of diverse safety functions. Some of these requirements involve analyses of potential CCF mechanisms present in the design. In particular, an analysis of the plant I&C architecture is required to determine whether there exist common mechanisms that could compromise the independence of the diverse I&C systems. It is required that any identified vulnerability be either eliminated or resolved through adequate mitigation. Additionally, an assessment of expected operating conditions for diverse I&C systems must be performed to identify any common triggering conditions to be addressed.

Other design requirements specified in IEC 62340 address particular design measures that are considered effective in promoting independence and coping with CCF. First, "system specific processing paths from sensing the plant status to the actuation of plant safety functions" must be provided without

employing any shared components. Second, support systems such as power supplies or heating, ventilation, and air conditioning (HVAC) must provide sufficiently redundant and separated subsystems. Third, self-supervision must be provided independently for each processing unit. Fourth, functionally diversity must be used wherever practical for diverse I&C systems.

In executing the design of independent diverse I&C systems, several design considerations must be addressed. First, the design of these systems must reduce the likelihood that the same input signal transient can initiate a CCF to a level that is not significant at any time during the life of the plant. Essentially, measures must be invoked to ensure that each system is subjected to different signal trajectories. Second, no shared components or services are permitted if their postulated failure can cause a CCF of the independent diverse I&C systems. Third, an analysis of the potential for CCF must be performed to assess the impact of identical hardware or software in independent diverse I&C systems. If the resulting potential for CCF is not negligible, then operation of the systems must be restricted such that they are (1) subjected to different service conditions and operational loads (e.g., input and/or processing demands) or (2) not operationally dependent on the demand profile of the plant process and the corresponding environmental conditions. Essentially, the diverse I&C systems must either be exposed to different signal trajectories and external influences or be insensitive to those factors. Fourth, if diversification of the demand profile as previously described is not feasible, then qualification for the intended application must be assured and periodically tested. Alternately, equipment diversity may be analyzed for consideration.

For software-based I&C systems, it is required that each software module of the application, as well as the associated signal trajectories, be assessed for potential CCF vulnerability. In particular, functional diversity is required to diversify the input signal component of the signal trajectories and introduction of other diversities to the system designs must be considered to diversify the internal state component of the signal trajectories. Additionally, independent diverse I&C systems must not perform identical application functions since the possibility exists that "coincidental, quasi-synchronized failure of these systems maybe triggered from the same input signal transient."

Regarding the treatment of system communications, requirements are given to ensure that failure propagation through communication paths is avoided. Specifically, communication is not permitted between independent I&C systems that are provided to protect against the impact of CCF. Additionally, requirements addressing internal propagation paths within safety systems are stated. These design measures include detection of data correctness on receipt, exclusion of faulty data from processing, physical separation of redundant subsystems, and protection of safety functions from the effects of communication failure (e.g., failure of the transaction or failure of the subsystem handling communications). In particular, system operation must not be jeopardized by failure of any central subsystems that require communication to more than one redundancy of a safety system to accomplish their information exchange function. For example, these subsystems "may provide information to the main control room for display or may support modification of parameters derived from the plant process." Furthermore, it is required that all software functions provided for the transfer of messages be implemented in a manner that ensures that the correct execution of these transfer mechanisms cannot be compromised by the information content (e.g., data values) being communicated.

The potential for system failure to be induced by maintenance activities must also be addressed in the design of independent I&C systems. Specifically, the safety system design must be analyzed to ensure that maintenance and test activities are properly accommodated by (1) means to prohibit spurious actuation due to maintenance and (2) provisions to limit the simultaneous impact of maintenance or testing on multiple safety functions.

Additional design measures addressed in IEC 62340 include system integrity, independence from external dates or messages, and assurance of physical separation and environmental robustness. Provisions to ensure system integrity through self-supervision (as required in this standard and

IEC 60880) must include determination of a predefined state to invoke on failure detection. This "failed" state must be based on failsafe principles. Requirements regarding avoidance of dependencies address precautions against dependence on external time and provisions for access security (which are referenced from IEC 60880). Finally, other standards are cited for requirements on separation and isolation (IEC 60709), equipment qualification (IEC 60780), and electromagnetic compatibility (IEC 61000-4).[128]

5.3.2.3.3 Tolerating Postulated Software Faults

It is noted that in accordance with IEC 61513, digital safety systems should be designed to "operate internally without dependence on the demand profile." The software-specific requirements given in IEC 60880 are supplemented by additional requirements in IEC 62340. These requirements, which are consistent with IEC 60880, are intended to "reduce the possibility that assumed latent software faults may be triggered from data which depend on transients of the plant process." In particular, it is required that application and system software be separated such that "the algorithmic processing of plant process data is entirely performed by the application software." Additionally, execution of system software functions "should not be influenced by any data which directly or indirectly depends on the plant status." To satisfy this requirement, IEC 60880 is cited along with the following design measures: "invariant cyclic processing of the application functions," "invariance of processing load and communication load," and "avoidance of interrupts triggered by process data."

Other software-related coping requirements address tolerance of invalid input signals and spurious signal transients, online identification of invalid or faulty input signals, protection of other safety functions in the presence of single function failure due to invalid input signals, and provision of a safe action in response to multiple CCF or input signal failures. It is cautioned that the signal validation by comparison of redundant information can introduce dependencies between redundancies that must be analyzed for CCF possibilities.

5.3.2.3.4 Avoiding System Failure Due to Maintenance During Operation

IEC 62340 addresses the prospect that CCF can be induced by maintenance activities during operation. Specifically, it is required that simultaneous activities are limited to "a single redundancy to avoid a resulting failure of more than one of the redundant trains, channels, or subsystems." Additionally, an analysis must confirm that the prospective impact of maintenance activity during power operation cannot induce failure of other nonrelated systems performing safety functions. Finally, it is required that the useful lifetime of components be determined to limit the potential effect of aging degradation and that replacement components be adequately qualified and their compatibility be sufficiently verified to avoid introduction of new failure modes or reduction of system reliability.

5.3.2.4 Aggregate IEC Guidance

The guidance provided in the three international standards discussed above constitutes an overall approach to coping with CCF in I&C systems important to safety. IEC 61513 represents the high-level guidance addressing I&C system architecture considerations. IEC 60880 supplements that guidance by specifically addressing software-based system considerations. IEC 62340 provides a framework for establishing a CCF coping strategy that is consistent with the high-level requirements in IEC 61513 and complementary to the software requirements in IEC 60880.

Table 5.5 provides a representation of the aggregate guidance on diversity usage extracted from the three standards. The primary emphasis of each standard is on the use of functional diversity (coupled with the enabling signal diversity) to diversify the functional requirements to be realized by diverse systems or redundancies and to minimize the likelihood that the diverse systems are presented coincidentally with common triggering conditions (i.e., common signal trajectories). Other diversities are

identified to address any remaining vulnerabilities that cannot be shown to be resolved solely by the use of functional diversity.

Table 5.5. Summary of diversity usage from IEC standards

Diversity attribute	Usage[a]	Details
Design		
Equipment (Manufacturer)		
Same manufacturer—different version	x	Different equipment addresses hardware CCF and contributes to defense against system software CCF (IEC 61513 cites this usage for complex systems where there is a limited experience base; IEC 60880 notes hardware diversity as an available diversity feature; IEC 62340 cites equipment diversity as an alternative if demand-profile diversification is not feasible)
Equipment (Processing)		
Functional		
Different purpose, function, control logic, or actuation means	x	Different functional relationships for diverse parameters and initiation criteria (all three standards cite this usage as the primary basis for CCF defense)
Life-cycle		
Different implementation/validation teams (testers, installers, or certification personnel)	x	Different V&V methods or procedures especially considering back-to-back testing (IEC 61513 notes the benefit afforded by enhanced opportunity for fault detection and removal)
Logic (Software)		
Different algorithms, logic, and program architecture	x	Different algorithms and program architecture corresponding to different functional relationships between diverse parameters and initiation criteria (all three standards cite functional diversity as the primary basis for CCF defense; algorithmic/logic differences are a consequence of functional diversity and contribute to diversifying the internal state component of signal trajectories)
Signal		
Different parameters sensed by different physical effects	x	Different sensed parameters (explicitly cited by IEC 61513 and implicitly included to enable functional diversity for IEC 60880 and IEC 62340; signal diversity provides diversification of the input signal component of signal trajectories)

Table 5.5 (continued)

Diversity attribute	Usage[a]	Details
Different parameters sensed by same physical effects	x	Different sensed parameters (same as above)
Other Diversity Considerations		
Parallel Diverse architecture in terms of systems or redundancies Other types of diversity addressed in guidance		Independence among diverse elements emphasized in IEC 62340; IEC 61513 invokes V&V testing diversity; IEC 60880 identifies system diversity, diverse software features, and diverse design approaches as alternatives if functional diversity is not feasible; IEC 62340 includes guidance on the use of design measures to minimize the potential for CCF, considerations arising from communication-enabled dependencies, and means to address the impact of maintenance

[a]Intentional diversity (x).

5.4 Diversity Considerations from the International Nuclear Power Community

The overview of current international interactions, research findings, and consensus guidance given in this chapter provides additional technical input to support development of diversity strategies that address the potential for CCF vulnerabilities in I&C systems at NPPs. Recent meetings among nuclear industry stakeholders have confirmed a collective awareness of the potential threat posed by CCF as the industry proceeds with more-extensive incorporation of digital technology in safety-related I&C systems. As previously discussed, the characteristics of modern I&C systems (e.g., complexity, limitations on testability) and the absence of quantitative metrics to assess the effectiveness of CCF coping strategies drive the need for more-definitive guidance on what constitutes sufficient diversity.

The elevated attention presently devoted to CCF concerns is reflected in the discussions among international regulators and the conduct of significant international meetings that are described in this chapter. Some key findings resulting from the investigation of international interactions on diversity usage involve the guidance provided in the common position of European regulators and insights drawn from a sample case of a CCF mitigation approach for a digital I&C architecture. Additionally, the extensive research program funded by the British nuclear power industry has expanded the fundamental understanding of the nature of diversity and its impact on the prospect of common systematic faults. That research has made possible identification of diversity-seeking decisions that can contribute to improved dependability for I&C systems and the safety functions they support. Finally, best practice for coping with CCF vulnerability in I&C architectures at NPPs has been captured in the consensus international standards that can be considered for adoption.

Table 5.6 summarizes the diversity usage derived from investigation of these international information sources. Specifically, the table presents diversity usage corresponding to the ISTec sample case, the U.K. DISPO research program, the European common position of software system diversity, and the IEC standards on I&C systems important to safety at NPPs. An alternate expression of the European common position guidance[114] captures the best-practice recommendation for the use of different technologies as the diversity usage basis (i.e., provision of a non-computer-based diverse system).

Table 5.6. Comparison of diversity usage from international sources[a]

Diversity attribute	ISTec sample case	U.K. research progress	European Comm. position	European Comm. position (tech.)	IEC Stds.
Design					
Different technologies	–	–	–	x	–
Different architectures	x	x	x	i	–
Equipment (manufacturer)					
Different manufacturer—different design	–			x	–
Different manufacturer—same design	x	x		–	–
Same manufacturer—different version	–	–	x	–	x
Equipment (Processing)					
Different logic processing architecture	x	x	x	i	–
Different component integration architecture	x	x	–	i	–
Different data flow architecture	–	x	–	i	–
Functional					
Different underlying mechanisms	–	–	–	i	–
Different purpose, function, control logic, or actuation means	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	–	–
Different design/development teams (designers, engineers, programmers)	i	i	x	i	–
Different implementation/validation teams (testers, installers, or certification personnel)	i	i	x	i	x
Logic (Software)					
Different algorithms, logic, and program architecture	x	x	x	i	x
Different timing or order of execution	x	x	–	i	–
Different runtime environment	–	x	–	i	–
Different functional representation	–	x	x	i	–
Signal					
Different parameters sensed by different physical effects	x	x	x	x	x
Different parameters sensed by same physical effects	x	x	x	x	x
Same parameter sensed by a different redundant set of similar sensors	–	x	–	–	–

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

It is observed that comprehensive application of the DSDs identified through the U.K. DISPO research provides the most-extensive usage of the diversity criteria derived from NUREG/CR-6303. Many of the DSDs relate to diversity of design in terms of design basis (including functional diversity), development approach, tools, validation approach (e.g., testing techniques), development teams, and

platforms. Each of these DSDs is related to mitigation of CCF through diversification of the purpose, process, and/or product. A key goal of many of the purpose- and process-related DSDs is to enhance the cognitive diversity (e.g., understanding, mental model for design) of the development teams. By doing so, the impact is expected to be reduced prospects for systematic faults being introduced throughout the I&C system life-cycle process by decreasing the likelihood of common misunderstandings, mistakes, and errors. Data diversity and functional diversity affect the performance aspect of CCF mitigation through diversification of execution profiles and, coupled with platform diversity, through different responses to external influences. Thus, diversity usage based on the DSDs identified through the U.K. DISPO research can be considered to provide a very thorough approach to resolving the potential for CCF vulnerabilities in software-based I&C systems.

The diversity usage derived from the European common position on software design diversity is closely related to the treatment represented by the DSDs covered in the U.K. DISPO research. Additionally, the foremost best-practice recommendation from the common position reflects the primary approach employed by the Sizewell NPP (see Chapter 4).

The diversity usage illustrated by the ISTec example employs a unique means of addressing vulnerabilities that may arise from temporal and platform (e.g., system support services) dependencies. The staggered restart (e.g., software rejuvenation) approach can minimize the potential for commonality in the internal state component of the signal trajectory presented coincidentally to diverse systems. Thus, through a form of operational diversity, the prospect of concurrent exposure to triggering conditions is minimized.

Finally, the guidance in the IEC standards represents a consensus basis from which to establish CCF coping strategies. The emphasis on functional diversity and independence captures best practices that have been traditionally employed within the nuclear power industry for addressing the potential for CCF vulnerabilities. However, caution is warranted in that functional diversity as a primary means of coping with CCF in digital systems may not adequately resolve the potential for systematic faults resulting from human errors in development or from the impact of platform-specific defects and/or system software deficiencies. In fact, IEC 61513 identifies equipment diversity (e.g., diverse platforms) as an effective approach for complex systems for which an extensive experience base is unavailable. The broad coverage of design considerations (e.g., flawed requirement specifications, independence) and implementation issues (e.g., dependencies from communication, impact of maintenance activities) suggests that IEC 62340 could provide a suitable framework for establishing a more comprehensive treatment of CCF mitigation. However, the diversity usage approaches identified from other information sources (such as those described in this and the preceding chapters) and the diversity strategies developed through this research based on those findings should be addressed via enhancements to the standard.

Draft

This page is intentionally left blank.

Draft

6. DIVERSITY STRATEGIES

The principal findings of this research are diversity strategies drawn from experience and best practices with safety-critical digital applications within the international nuclear power community and in other industries. The approach employed in establishing these strategies began with examples of diversity usage that were identified during the course of this investigation. The combinations of diversities from the referenced examples were then characterized in terms of the diversity attributes given in NUREG/CR-6303. The nature of potential CCF vulnerabilities was considered, and the prospective impact of each diversity in mitigating those vulnerabilities was assessed. Engineering judgment was then applied to derive strategies based on the cited examples and relevant technical considerations accounting for the nature of nuclear power safety systems and characteristics of available I&C technologies. The resulting baseline diversity strategies are presented in this chapter, along with the source examples and supporting rationale. It should be noted that these strategies do not constitute required approaches to diversity usage but rather represent acceptable means for achieving adequate diversity. Alternate diversity strategies are feasible and may be similarly justified.

6.1 Usage of Diversity

6.1.1 Considerations for Assessing 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, 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 baseline diversity strategies developed through this research provide guidance on acceptable combinations of diversity criteria. These strategies are drawn from best practices 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 are intended to 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. In the subsequent discussion of the rationale for each diversity strategy, these diversity effects are characterized in terms of impact on common systematic faults, concurrent execution profiles, or similar responses to external influences.

6.1.2 Crosscutting Diversity Usage

6.1.2.1 Functional and Signal Diversities

As seen in the Chapter 4 discussion of traditional diversity usage, the intentional use of functional and signal diversities is a common practice applied to I&C system architectures at NPPs. The approach was developed to address potential CCF vulnerabilities in hardwired systems that may arise from requirement flaws, systematic faults, and common or shared equipment. Furthermore, there are additional benefits specific to digital safety systems that arise from different signal trajectories, alternate functions, and diversified requirements. The impact of this diversification is to lessen both the prospect of common design mistakes that may result in systematic faults and the potential for concurrent execution profiles that may trigger common failures.

Based on survey findings, this diversity approach is typically implemented in either redundant subsystems of a digital safety system or between safety and diverse actuation systems being compared. As is the case in most of the international NPP examples cited, the main use of signal diversity may be focused on redundant subsystems within the primary digital safety system. This approach is consistent with GDC 22. However, in cases where parallel diverse systems are the primary means of achieving diversity, some intentional signal diversity (beyond simply using separate redundant sensors) between the system inputs is warranted to achieve the benefits of input diversification (and the associated functional diversity) in comparative systems. In those instances, providing some diverse measurements (i.e., diverse initiation criteria for the same or compensating function corresponding to the selected PIEs), along with coverage of a reduced set of PIEs (as needed, based on the D3 analysis for the plant), should provide adequate diversification of the input component of the signal trajectories seen by each system.

To help ensure that current regulations continue to be satisfied and that best practices are maintained, the combined application of functional and signal diversities is treated within each strategy as a baseline practice to be supplemented, not replaced, by additional considerations related to the accommodation of the unique characteristics of digital technology. The specific functional diversity criterion that is emphasized as an intentional diversity usage involves different purpose, function, control logic, or actuation means. The intentional use of each signal diversity criterion, to the extent practical, is also adopted in conjunction with the use of functional diversity. Thus, use of these diversity criteria applies to all of the diversity strategies developed through this research.

Finally, this position on the baseline use of functional and signal diversity not only contributes to satisfying current regulations (GDC 22) but also is consistent with current international guidance on approaches to address CCF vulnerabilities. The use of functional (and the supporting signal) diversity is central to the guidance provided by IEC 62340, which gives requirements for coping with CCF in NPP I&C systems.[11] Additionally, the common positions on software design diversity that were developed by European regulators emphasize the use of functional diversity "wherever possible" in the implementation of diverse digital systems.[114]

6.1.2.2 Equipment (Manufacturer) and Life-Cycle Diversities

Due to the cross-dependence of the life-cycle and equipment manufacturer diversity attributes, these diversities are considered together. Basically, the selection of different manufacturers for diverse systems is generally equivalent to the selection of different design organizations. It is expected that common teams or shared personnel between different companies would occur only in rare cases, such as in situations where the development of the diverse systems involves either a joint venture between separate manufacturers or comparable products from parent and subsidiary companies. Conversely, the selection of a common manufacturer suggests the need for intentional establishment of separate teams. This linkage between the diversities is addressed in the following discussion. Additionally, cross-cutting issues (i.e., those common to all strategies) are covered as well.

In instances where the same equipment manufacturer is used to supply diverse systems, there is the potential for common physical defects to be introduced by deficiencies in shared manufacturing processes or flaws in common source material or parts. Additionally, an adverse effect could arise as a consequence of common influences or shared resources (e.g., cultural factors, personnel, tool sets, corporate practices) affecting each diverse product. For example, the potential for systematic faults because of common design mistakes or implementation errors is of greater concern because of the prospect of common development and implementation teams. These considerations suggest that there is some CCF mitigation advantage in the selection of different manufacturers as the primary equipment suppliers for the diverse systems. In essence, the intentional selection of different equipment manufacturers (or system suppliers) can lessen the likelihood of potential CCF vulnerabilities that may be introduced through shared manufacturing processes, system integration approaches, source material/components, or deficient quality control.

Similarly, the likelihood of human-induced systematic faults due to misinterpretations of requirements, design mistakes, or implementation errors can be reduced via the use of different personnel. At the very least, employing human diversity in the life-cycle of each system minimizes the prospect of common faults being introduced by the same person or team. The use of different design organizations generally provides across-the-board life-cycle diversity. By default, the project management, design and development teams, and implementation and validation teams are likely to be different. Thus, when different organizations are engaged, it can be inferred that different design and implementation teams are inherently provided. The presumption is that both life-cycle criteria for personnel diversity (designers, engineers, and/or programmers in one case and testers, installers, or certifiers in the other case) are satisfied to some extent.

It is expected that systems supplied by different companies are more likely to provide some variation of design and contain several different components. One prospective consequence is that the diverse systems would be less likely to respond identically to common external influences (e.g., environmental stress). Of course, minimizing common triggering factors by separation and control of external influences is a key consideration in coping with CCF as well as diversity.

The bottom-line effect of selecting different manufacturers, and thus different design organizations, is that commonalities are likely to be reduced and the potential for common systematic faults (e.g., manufacturing defects, design mistakes, implementation errors) can be minimized.

While the prospect of fewer commonalities between diverse systems is a more reasonable expectation for different suppliers than for a common supplier, a comparable effect regarding the introduction of systematic faults can be achieved by a common manufacturer through the use of separate teams for each system, instead of a single development team. Additionally, strict quality control, such as that expected from an Appendix B supplier, can help to ensure that the potential for common defects or errors among product lines is minimized. Thus, a common equipment manufacturer (or system supplier) can be selected if measures are taken to compensate for potential communalities in the manufacturing or system integration processes and common components are minimized to the extent feasible.

If a common manufacturer (or system supplier) is selected, an equivalent life-cycle diversity can be achieved through the use of separate teams dedicated to each system, instead of using a single development team. Essentially, the life-cycle diversity under this scenario can be intentionally invoked in the form of separate teams (e.g., each involving design, development, testing, and installation disciplines but under separate management) within the company. There is value in providing a comparable level of expertise for the personnel on each team to ensure adequate quality for both systems. The basis for including the intentional use of different management teams is stated in NUREG/CR-6303. The motivating consideration is that "[m]anagement has the most significant effect on [life-cycle] diversity because management controls the resources applied and the corporate culture under which [design teams] work." In effect, management can significantly impact the potential for common systematic errors through the objectives, practices, and constraints it imposes.

The majority of the examples cited in this research involve use of different equipment and selection of different manufacturers to supply the diverse systems. Where the same supplier was used, separate teams and strict quality controls were applied to each diverse system in most cases. Likewise, the examples showed that it is common practice in almost all of the industries investigated (e.g., nuclear, aerospace, aviation, chemical process) to utilize life-cycle diversity. The intentional application of this diversity, whether for different or similar designs, was achieved either through separate teams within an organization or, more commonly, at different companies. Furthermore, the guidance for the chemical industry recommends the use of different equipment from different manufacturers as well as different personnel.[66] Guidance provided by IEC standards also notes the value of different equipment and different development teams in coping with potential CCF vulnerabilities.[124]

In keeping with common practice found in the survey, intentional selection of different equipment manufacturers (or system suppliers) is treated within each strategy as a baseline practice. Alternate diversity strategies within each classification can be based on the intentional selection of the same manufacturer for the diverse systems as a variation of the baseline combination of diversity criteria. Use of this alternate equipment manufacturer criterion is subject to the provision of evidence establishing reasonable assurance that the manufacturer has properly addressed the potential impact of common influences and shared resources. As indicated above, selection of an Appendix B supplier can resolve concerns about quality control. The intentional use of different teams assigned to each system is a normal practice for addressing concerns about the potential for common fault introduction by shared human resources. Thus, the intentional selection of diverse systems from the same equipment manufacturer is cross-dependent on compensatory intentional application of separate teams within that company.

Similarly, intentional selection of different design organizations to conduct life-cycle activities related to the application-specific system development is adopted within each strategy as a baseline practice. Specifically, the life-cycle diversity criteria baseline is the intentional use of different design organizations, with corresponding inherent life-cycle diversities in the form of different design and development teams (i.e., designers, engineers, and/or programmers) and different implementation and validation teams (i.e., testers, installers, and certifiers). Alternate diversity strategies within each classification may adopt the intentional selection of separate teams when the same manufacturer is used to supply the diverse systems. In particular, this alternate strategic approach involves the manufacturer's intentionally establishing, to the extent practical, the following teams for each system: different management teams; different design and development teams; and different implementation, validation, and installation teams. For this strategy variation, the intentional application of life-cycle (human) diversity within a company that is supplying both systems compensates for the increased prospect that systematic errors could be introduced through the use of common personnel or the influence of common corporate constraints or cultural practices.

The cross-dependent relationship for these diversity attributes results in the following linkage between the criteria associated with each diversity. If different manufacturers are selected for the diverse systems, then different design organizations are also effectively selected. Conversely, if the same

manufacturer is selected for the diverse systems, then different teams (i.e., management, design and development, and implementation and validation) are intentionally established to separately execute the full life-cycle activities for each system. The linkage between these diversity criteria applies to all of the diversity strategies developed through this research. This position on the relationship between the life-cycle and equipment manufacturer diversities is consistent with best practices drawn from the survey of diversity usage.

It should be noted that even with the selection of different manufacturers, there remains the potential for common parts or components. Therefore, some consideration should be given to the components and parts of diverse systems to ensure that any common items are sufficiently simple to be readily qualified for their intended usage. In considering the diversity of measurement equipment (i.e., sensors), the prospective introduction of smart sensors warrants awareness of the potential impact on CCF vulnerability posed by a common embedded microcontroller for otherwise fundamentally diverse sensing equipment.

6.2 Classification of Diversity Approaches

Considering the NUREG/CR-6303 diversity attributes, a framework is established for classifying strategic approaches to diversity usage. Technology is selected as the principal feature for characterizing each diversity strategy grouping or family. The technology choice for implementing diverse systems, redundancies, subsystems, modules, or components constitutes the type of design diversity that is intentionally applied. The rationale for this approach to classifying the strategies is based on two primary considerations. First, the selection of technology has a significant impact on both the process (e.g., design and implementation) and product (e.g., hardware, software, integrated system) involved with each diverse system being compared. In particular, many of the other diversity attributes identified in NUREG/CR-6303 are strongly affected by the choice of design for diverse systems. Second, differences provided by systems and equipment based on diverse technologies are often readily observable. NUREG/CR-6303 states that "the clearest distinction between two candidate subsystems would be design diversity."

Thus, the classification framework is derived from the NUREG/CR-6303 representations of the design diversity attribute: (1) different technologies, (2) different approaches within the same technology, and (3) different architectures within the same technology. Using this convention, the first grouping, designated as the Strategy A classification, is characterized by fundamentally diverse technologies. The Strategy A baseline, at the system or platform level, is illustrated by the example of analog and digital implementations providing design diversity. The second grouping, designated as the Strategy B classification, is achieved through the use of distinct technology approaches. The Strategy B baseline can be described in terms of different digital technologies, such as the distinct approaches represented by field programmable gate arrays (FPGAs) and general-purpose microprocessors (i.e., CPUs). The third grouping, designated as the Strategy C classification, involves the use of architectural variations within a technology. An example of the Strategy C baseline involves different digital architectures, such as the diverse microarchitectures provided by different CPUs (e.g., Intel Pentium and Apple-IBM-Motorola [AIM] Power PC).

Obviously, this classification framework implies a fourth diversity family. The fourth strategy classification (i.e., Strategy D) would consist of those strategies that are characterized by use of the same technology (e.g., the same platform) for the diverse systems being compared. Essentially, there is no design diversity and little or no equipment diversity provided by approaches within the Strategy D classification. Some relevant examples were identified in the survey of diversity usage. In particular, the flight control system (PASS and BFS) for the Space Shuttle and the railway interlocking system (ELEKTRA) for the Austrian Federal Railways provide nonnuclear industry examples that are based on diverse applications implemented on common platforms. For the international nuclear power industry, examples of common platform usage include Dukovany and Kashiwazaki-Kariwa. In each case,

thorough quality control processes and extensive design analysis contribute to the avoidance of systematic faults. It is noted that similar practices are commonplace throughout the nuclear power industry. The reduced functionality backup in the Space Shuttle example involves functional, life-cycle, and software diversities. The ELEKTRA railway example focuses on active replication complemented by extreme design specification diversity, which leads to significant diversification in terms of function (i.e., different purpose) and software (i.e., different program architectures and logic). The nuclear power industry examples employ the traditional diversities (i.e., functional and signal diversities) in response to CCF considerations. As described previously, this diversity combination also affects the potential for digital CCF vulnerabilities through diversification of the signal trajectories associated with each diverse system.

6.3 Diversity Strategies

The diversity strategies that are developed through this research represent baseline combinations of diversity criteria that are judged to provide adequate mitigation of potential CCF vulnerabilities that could compromise the successful execution of safety functions. As described above, three strategy families have been established. Each classification is presented below with detailed discussion of its basis. A key resource for the development of the strategies and establishment of the supporting technical basis arises from the diversity examples identified in the survey of nonnuclear and nuclear power industry experience. These examples are cited in the discussion of each strategy classification.

The description of each strategy grouping provides an overview of the diversity survey findings that are relevant for that classification, the rationale for the use of diversity within the strategy, and a description of the baseline strategy. In the discussion of the rationale for each strategy family, the impact of the technology differences that are central to the classification is described, the diversity characteristics that are inherently achieved are summarized, and the bases for specifying intentional diversities to address the unresolved potential for CCF vulnerabilities are detailed. In addition to defining baseline combinations of diversity criteria, variations on the baseline are presented for each strategy. These strategy variants provide alternate diversity combinations based on recognition of interrelationships among the diversities and consideration of the examples identified in the survey as well as NUREG/CR-6303.

Strategy A represents the extremes in diversity arising from technology differences and provides associated inherent diversities that are characteristic of fundamental dissimilarities posed by the diverse nature and behavior of those technologies. Inherent to varying degrees in this use of design diversity are processing equipment, functional, logic, and platform-specific life-cycle diversities. Intentional specification of traditional diversities (signal and functional), coupled with the cross-dependent choice of different manufacturers and different design organizations, provides an additional degree of diversification. For Strategy B, aspects of processing equipment, functional, logic, and platform-specific life-cycle diversities are inherent in this use of significant design diversity. The common practice of intentional use of functional and signal diversities applies to this classification, as does the cross-dependent choice of different manufacturers and different design organizations. Additionally, the intentional use of logic diversity (i.e., different algorithms and logic) in association with the specified functional diversity is also provided. The approach in Strategy C employs different architectures (specifically, CPU microarchitectures) within digital technology to provide platform-specific life-cycle diversity as an inherent consequence of the implementation. As for the other strategy families, intentional diversification is specified through the use of equipment manufacturer, functional, life-cycle, and signal diversities. Additional logic and processing equipment diversities are included to address commonalities in the platform and means for logic processing that are possible given potential macroarchitectural similarities.

For the prospective Strategy D classification, the principal feature characterizing each strategy is that the basic components (hardware parts, software blocks, system architectural structure) of diverse systems

are the same. Thus, the primary need to support any approach within the Strategy D classification is to acceptably demonstrate that the platform is not a credible source of CCF vulnerability. In considering the nonnuclear industry examples that are relevant for this classification, it is noted that considerations such as implementation constraints (e.g., size, weight, and power) or a preference for other design approaches (e.g., active redundancy or significant requirements diversity) may have a substantial impact on the acceptability of certain diversity combinations. For use in the nuclear industry, parallel diverse systems providing similar or compensating functionality represent the typical architecture for addressing CCF vulnerabilities in safety systems. The "parallel diverse" implementation may involve separate systems (i.e., coequal safety systems or primary and secondary systems) or separate redundancies (or subsystems within redundancies). Although the diversification of signal trajectories (i.e., inputs and internal states) can reduce the potential for concurrent execution profiles that could activate latent systematic faults in the platform, it does not preclude the prospect for common failures in response to unexpected, untested conditions that may arise from exception handling, system software deficiencies (e.g., software "aging"), or hardware defects/degradation. The justification that the potential for CCF vulnerabilities associated with a common platform is not significant necessarily relies on considerations other than diversity. Some of these factors that may contribute to an adequate basis for employing a common platform include operational experience, design measures, functional usage, platform quality assurance, and other prospective evidence. These considerations are beyond the scope of this research; therefore, a comprehensive treatment was not feasible. As a result, a baseline Strategy D is not provided in this report. It is noted that the absence of a baseline for the Strategy D classification does not mean that adequate justification for a form of this strategy cannot be generated. Nevertheless, development of the supporting technical basis for the Strategy D classification must be deferred.

6.3.1 Strategy A: Fundamentally Diverse Technologies

The Strategy A classification encompasses those diversity strategies that employ fundamentally diverse technologies as the basis for establishing diverse systems, redundancies, or subsystems. The use of such technologies at the system level is readily apparent and is most directly seen through the significantly different equipment associated with each technology (e.g., analog modules such as square-root extractor, summing, and comparator/bistable circuits vs a printed circuit board with an FPGA or CPU chip providing the necessary computational capabilities). Strategy A takes advantage of the significant differences in the nature of fundamentally diverse technologies to provide substantial inherent diversity to help mitigate potential CCF vulnerabilities. Intentional diversities are specified primarily to incorporate traditional diversities that have been developed to contribute to satisfying specific protection system requirements (e.g., GDC 22).

The inherent diversities that are a consequence of this design diversity are equipment manufacturer, processing equipment, functional, life-cycle, and logic diversities. Different heritages in terms of platforms/components account for inherent diversity regarding equipment manufacturer and life-cycle. The fundamental difference in the means of processing functions due to the nature of the technologies provides inherent diversity for the processing equipment. Similarly, inherent logic diversity is a consequence of significant dissimilarity in functional implementation and processing methods for digital and analog technologies. Inherent functional diversity results from different underlying mechanisms for the expression and execution of functions (e.g., different functional configurations and diverse execution of function). Additional intentional diversities are specified for the cross-dependent life-cycle and equipment manufacturer diversities to address potential commonalities in the application-specific system development. To maintain the traditional usage of diversity that was developed by the nuclear power industry in response to long-standing concerns about potential CCF vulnerabilities for hardwired systems, intentional functional and signal diversities are incorporated in the baseline strategy for this classification.

6.3.1.1 Survey Findings Related to Strategy A

The investigation of diversity practices for the nonnuclear industry did not identify any specific fielded examples that correspond to this strategy classification (i.e., no examples of the intentional use of fundamentally diverse technologies). There are instances of analog and digital equipment coexisting in distributed applications (cf., electric power distribution industry), but such use appears to be a consequence of phased replacement rather than intentional diversity through different technologies. Within the examples cited for the international nuclear community, Sizewell provides the sole example that corresponds to Strategy A. The use of this technology-focused approach is mentioned in a few of the articles, reports, and guidance documents referenced in this research. In particular, the use of a noncomputer-based technology to provide diversity is recommended in the common positions on software design diversity that were developed by European regulators.[114]

It should be noted that there are many other NPPs throughout the world that have undergone some modernization projects that have resulted in hybrid I&C architectures with some digital systems (including safety systems) and some analog systems. However, these cases are not cited as examples of diversity strategies because the mix of technologies seems to be driven more by economic and schedule considerations than by some intentional diversity strategy for any particular plant. It remains feasible for a plant to choose to retain some analog systems (i.e., maintained, refurbished, or replaced) to provide design diversity within or across lines of defense.

In the Sizewell example, diversity is implemented through provision of the computer-based primary protection system and the analog secondary protection system. In comparing the two parallel diverse systems, it is found that design, equipment (manufacturer), functional, life-cycle, and signal diversities are intentionally provided. Based on the technology usage, inherent diversities can be inferred for equipment (processing) diversity and logic (software) diversity. Traditional approaches to promote hardwired diversification, such as independent diverse power supplies and diverse actuation equipment, were also applied. At Sizewell, most of the intentional diversities were implemented to diversify the primary and secondary protection systems. However, the traditional practice of providing diverse parameters for initiation criteria (i.e., signal diversity and functional diversity) was implemented through separate, independent subsystems within the primary protection system. To promote independence, signal diversity was provided between the diverse systems by separate redundant sensors. Additionally, a measure of functional diversity between the diverse systems was provided via a somewhat reduced functional scope of the secondary protection system, which primarily addresses initiation criteria for high-frequency PIEs.

6.3.1.2 Rationale for Strategy A

6.3.1.2.1 Impact of Strategy A Technology Differences

Fundamentally diverse technologies are characterized by significant differences in their underlying physical nature and the mechanisms by which they process functions (i.e., representation and execution). As a result, systems based on fundamentally diverse technologies can be expected to provide differences in their functional capabilities, dynamic behavior, and means of realizing (i.e., implementing and executing) functions. Each of these characteristics contributes to mitigation of the potential for common systematic faults, concurrent execution profiles, or similar responses to external influences.

The diverse functional capabilities and processing mechanisms provided by fundamentally diverse technologies promote substantial differences in physical components and architectural conventions (e.g., physical layout, interconnections, distribution of function). The impact is reduction in the potential for common misinterpretation or mistakes in the translation of requirements (what function is needed) to design specifications (how the function is to be achieved). Similarly, the technology difference impacts the prospect of implementation faults through less potential for common hardware manufacturing defects

or software coding errors. Differences in the dynamic behavior and timing characteristics of systems based on diverse technologies can also lessen the prospect for concurrent failures in response to common external influences, such as environmental factors or human actions.

The differences between technologies also impact the prospect for common human mistakes in the design and implementation processes. The personnel (e.g., designers, developers, testers, installers) engaged in various life-cycle activities for either system are more likely to develop different cognitive models (i.e., mental representations or understanding) of the system specification and the way the functional requirements can be implemented and validated. This effect is likely to be further enhanced by typical differences in implementation approaches and methods associated with the diverse technologies such as unique development tools, different system integration techniques, and unique skill sets (or technical expertise).

The diversity combinations described below take advantage of the diverse technology basis to contribute to the mitigation of potential CCF vulnerabilities that primarily arise from the unique characteristics of digital technology. Other forms of diversity that have been traditionally employed at NPPs to address potential CCF vulnerabilities for hardwired systems are not replaced by this diversity strategy but are rather supplemented by it. As seen in the Sizewell example (and almost every other NPP example), both diversification of common sources (e.g., power, sensed parameters, etc.), and avoidance of common components or nonvital interconnections are key practices. Because of the recognition that the functional and signal diversities commonly employed in the nuclear power industry have an impact on reducing the potential for digital CCF vulnerabilities, they are explicitly included in this strategy to emphasize their value and to reflect best practice.

6.3.1.2.2 Inherent Diversities for Strategy A

As a consequence of extreme technology diversity, differences arise that provide some level of inherent diversification for several other attributes of the comparative systems (i.e., the parallel systems being compared for diversity). The impact of this design diversity basis is to provide inherent design, equipment, functional, life-cycle, and processing (i.e., logic, function structure) diversity to some degree.

There is generally a clear difference in equipment associated with the diverse technologies. Inherent equipment diversity clearly relates to processing equipment, which results from different underlying mechanisms for execution of functions. Basically, the equipment types on which the diverse systems are based inherently provide fundamentally different processing of functions, algorithms, and/or logic. A highly simplified comparison of digital processing vs analog processing in a safety channel illustrates some of the fundamental differences. A microprocessor-based trip system processes digitized data via functional algorithm(s) and voting logic through sequential execution of software instructions to compute a command that is communicated for further voting and/or actuation. Conversely, separate modules in an analog trip channel process electrical inputs in parallel based on the instantaneous response of their circuits to generate output that is transmitted for further processing along the instrumentation channel or ultimately to relays for voting. As a result of the substantial difference in processing elements, architectures, and mechanisms, the processing equipment diversity criteria represent inherent differences, rather than prospective equipment selection options, in the context of the Strategy A classification.

Additionally, the equipment difference associated with this technology usage likely involves factors such as development heritage and manufacturer while the likelihood of common components is almost certainly less. Manufacturer differences also reduce the potential for common defects introduced by process deficiencies or source material defects. Additionally, different equipment with diverse capabilities, components, and configurations reduces the potential of common responses to common influences (e.g., environmental stress).

The intentional application of fundamentally diverse technologies as the primary design diversity results in an inherent functional diversity involving different underlying mechanisms to accomplish the safety function. This additional inherent diversity relates specifically to the digital aspects of this criterion for functional diversity that arise from the different functional execution mechanisms for the safety functions implemented on the diverse technologies. This inherent functional diversity is also observed in the findings regarding Sizewell.

Differences in development heritage reduce the prospect of common human contributors to the potential residual fault space for I&C platforms, modules, or components based on each technology. However, inherent life-cycle diversity may be limited to the base platform or key modules, components, or parts. In such cases, action would be needed to address the prospect of common human contributors who could increase the potential for system design mistakes or implementation errors.

The commonality of skill sets employed and the similarity of cognitive modeling achieved by personnel involved at various phases of the system life-cycle phases are profoundly affected by the technology employed. In the context of the Strategy A classification, the use of fundamentally diverse technologies represents an extreme in dissimilarity for functional capabilities, processing mechanisms, dynamic behavior, equipment types, and implementation approaches. Each of these factors contributes to minimizing the similarity of design products, implementation activities, testing practices, and integration/installation interconnections. As a result, some degree of diversity in the system concept, design development, and implementation techniques is achieved inherently. Nevertheless, full life-cycle diversity was employed at Sizewell with different teams responsible for the primary reactor protection system and the secondary reactor protection system.

Because of the nature of the processing mechanisms for fundamentally diverse technologies, each aspect of the logic diversity attribute is inherently present. The criterion providing different algorithms, logic, and logic (program) structure is inherently achieved through diverse logic structures because of the significant difference in the mechanisms by which functional relationships are processed. Additional diversity through this criterion would arise as a consequence of any intentional functional diversity since the algorithms and/or logic would also be affected by the specification of different functional relationships. The criterion providing different timing or order of execution is inherently satisfied through the fundamentally different means by which functions are executed (e.g., sequential computations manipulating digital data images in contrast to instantaneous parallel response of analog circuits to electrical input). The criteria on different execution environments (e.g., operating systems for microprocessor-based technologies) and different functional representations (e.g., languages for software-based systems, electrical circuits for analog systems) are also inherently satisfied because of the fundamental difference in the way the diverse technologies represent and execute functions.

Finally, a prominent consequence of employing this technology diversity is that some additional design diversity is achieved inherently. From both the micro- and macroarchitectural viewpoints, the system architectures are likely to be substantially different due to the nature of the technologies (e.g., concentrated software-instantiated functionality executed sequentially in highly complex, compact components operating on digitized data vs distributed hardware–based functionality executed in parallel on separate modules responding to continuous or discrete inputs).

6.3.1.2.3 Basis for Diversity Usage in Strategy A

The intentional use of fundamentally diverse technologies constitutes the principal design diversity that is characteristic of this diversity strategy classification. Applying analog and digital technologies as the basis for diverse designs provides inherent diversities that result in a substantial effect on the potential for CCF vulnerabilities related to systematic faults, execution commonalities, or responses to common external influences. Nevertheless, diversity usage found in the primary example of a Strategy A approach (Sizewell) involved intentional application of design, equipment (manufacturer), functional, life-cycle,

and signal diversities. Coupling findings from the Sizewell example with an evaluation of the prospective mitigation impact of each diversity attribute provides a basis for grouping the diversity criteria to establish a baseline for Strategy A.

Equipment (Manufacturer) Diversity. Within the Strategy A classification, diversity strategies inherently involve fundamentally different designs in the context of the equipment manufacturer diversity attribute. In particular, the basic components of the diverse systems (if not the base platforms themselves) are generally composed of recognizably different equipment. Typically, equipment types with substantially different technology bases have different development heritages, provide notable architectural differences, and are often supplied by different manufacturers. The Sizewell example involved different equipment manufacturers.

In spite of the expectation that equipment based on fundamentally diverse technology will be significantly different, it is noted that such equipment can be manufactured by the same provider or may be integrated at the system level by a single supplier of both diverse systems. In cases where it is feasible and a common supplier is selected, action is warranted to minimize the potential for common systematic faults arising from manufacturing defects (e.g., from process deficiencies or flawed source components) or implementation errors (e.g., system integration errors). Ensuring rigorous quality control and establishing separate development teams are common actions.

Equipment (Processing) Diversity. As previously described, this diversity attribute is inherently satisfied as a consequence of the fundamental diversity between the nature of analog and digital technology. In the context of the Strategy A classification, the processing equipment architecture relates to the structure or organization of processing elements, which is substantially different for fundamentally diverse technologies. For a microprocessor-based system, the primary processing element structure is provided by the CPU microarchitecture. For analog modules, the primary processing element structure is provided by the analog circuits themselves, which may consist individually of several miniature circuits involving transistors and passive devices implemented in analog chips. The processing equipment component integration architecture generally involves the printed circuit board assembly. It is expected that technology differences will continue to result in notably different board layouts that should minimize the potential for common design errors and provide some difference in the responses to common external influences. The data-flow architecture basically represents the internal communication architecture for the processing equipment. Again, the fundamental technology differences drive different internal interconnection structures and communication conventions. Thus, the potential for common undetected systematic faults in platform-, board-, or chip-level communication should be minimal.

Functional Diversity—As discussed above, the intentional use of functional diversity, in combination with signal diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research. The relevant diversity criterion involves different purpose, function, control logic, or actuation means. Basically, different functional expressions capture the diverse safety function initiation criteria, with the result being differences in the functions and control logic assigned to each diverse system. As discussed above, inherent functional diversity is also achieved as a result of the differences in the nature of the technologies, which leads to diversification of the underlying mechanisms for processing functions.

Findings from the investigation of diversity practices at international NPPs confirm the prevalence of this diversity approach as an intentional diversity. For Sizewell, functional diversity and signal diversity were intentionally applied in combination. The different functionality corresponding to diverse initiation criteria was primarily implemented within subsystems of the digital safety system. The secondary protection system provides backup safety action for a reduced set of high-frequency PIEs, thus providing some further diversification of function between the parallel diverse systems.

Life-Cycle Diversity. Fundamentally diverse technologies are likely to have diverse manufacturers or suppliers for key modules, components, and parts, if not the base platforms themselves. If the

equipment differences are such that no common manufacturer or system supplier exists, then life-cycle diversity is achieved by default via the different design organizations in each company. If a common manufacturer (or system supplier) is selected, a comparable life-cycle diversity can be achieved through the use of separate teams dedicated to each system, instead of a single development team. The nature of fundamentally diverse technologies generally implies demands for different expertise, which may result in establishment of separate teams for diverse systems as a natural consequence. For the Sizewell example, different design organizations from different companies were used.

Logic (Software) Diversity. Strategy A provides inherent logic diversity due to the fundamentally diverse means of processing functions that result from the diverse technologies. The benefit is significant difference in the execution profile (e.g., computational states and state transitions) of the functions implemented in the diverse systems. Coupled with intentional signal diversity, this inherent logic diversity provides significant difference in signal trajectories for the diverse systems. Thus, common triggers related to input patterns and/or internal states are extremely unlikely.

Signal Diversity. The selection of fundamentally diverse technologies as the basis for parallel diverse systems, redundancies, or subsystems has no direct impact on signal diversity. As discussed above, the intentional use of signal diversity, in combination with functional diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research.

This usage is consistent with the examples identified from the nuclear power industry survey. For the Sizewell example, diverse signals were provided to separate subsystems within the primary protection system to support diverse initiation criteria based on different parameters. The secondary protection system primarily addressed backup action for a reduced set of high-frequency PIEs, which led to a reduced set of inputs compared with those for the primary protection system.

6.3.1.3 Description of Strategy A

6.3.1.3.1 Design Diversity

Intentional diversity is provided through the selection of fundamentally diverse technologies. Specifically, the principal example of strategies in this classification involves the use of analog and digital technology as the basis for diverse systems, redundancies, or subsystems. The purpose of this diversity usage is to address potential CCF vulnerabilities that may arise from common systematic faults, concurrent execution profiles, and similar response to common external influences.

It should be noted that embedded microcontrollers are becoming more common for electrical and instrumentation components, such as power supplies and sensors. This trend warrants awareness by the designer and assessor to reasonably ensure that the safety-related functionality of ostensibly analog components is not compromised by potential CCF vulnerabilities of embedded digital elements.

6.3.1.3.2 Equipment (Manufacturer) Diversity

Intentional diversity is provided through the selection of different manufacturers (or system suppliers) for different equipment designs. The purpose of this diversity usage is to minimize the potential for common systematic faults arising from manufacturing defects or implementation errors.

Alternate diversity strategies within the Strategy A classification may adopt the intentional selection of the same manufacturer of different designs as a variation of the baseline combination of diversity criteria. Use of the alternate equipment manufacturer criterion is linked to the compensatory intentional application of life-cycle (human) diversity.

6.3.1.3.3 Equipment (Processing) Diversity

The inherent processing equipment diversity criteria that are relevant for Strategy A are different processing equipment architectures, different processing equipment component integration architectures, and different data-flow architectures. No intentional diversity is necessary.

6.3.1.3.4 Functional Diversity

Intentional diversity is provided in the form of different functions or control logic associated with coverage of a reduced set of PIEs (as needed based on the D3 analysis for the plant) and the use of diverse safety function initiation criteria (cf., GDC 22 and signal diversity). The purpose of this diversity usage is to provide differences in functional requirements and design specification as well as to diversify the signal trajectories seen by each system.

6.3.1.3.5 Life-Cycle Diversity

Intentional diversity is provided through the use of different design organizations to conduct life-cycle activities related to the application-specific system development. This baseline criterion is linked to the intentional selection of the equipment manufacturer diversity criterion for different manufacturers of different designs. The purpose of this life-cycle diversity usage is to avoid the introduction of systematic faults during design and implementation of the diverse systems due to common mistakes or misunderstandings by shared human resources.

Alternate diversity strategies within the Strategy A classification may adopt the intentional selection of separate teams when the same manufacturer is used to supply the diverse systems. In particular, this alternate strategic approach involves the manufacturer intentionally establishing, to the extent practical, the following teams for each system: different management teams; different design and development teams; and different implementation, validation, and installation teams.

6.3.1.3.6 Logic (Software) Diversity

Logic diversity is inherently realized for Strategy A. The criteria that are inherent are different algorithms, logic, and logic structure; different timing or order of execution; different execution environment; and different functional representations. No intentional logic diversity is necessary.

6.3.1.3.7 Signal Diversity

Intentional diversity is provided through the use of separate and/or diverse measurements of plant parameters. The purpose of this intentional diversity usage involves minimization of commonalities, support of functional diversity (cf., GDC 22), and diversification of concurrent execution profiles. Each of the three signal diversity criteria is appropriate for application as intentional diversities to the extent practical.

6.3.1.4 Strategy A Summary

Strategies that involve the use of fundamentally diverse technologies as the basis for diverse systems, redundancies, or subsystems are classified as examples of Strategy A. The combinations of diversity criteria that characterize Strategy A, in conjunction with traditional diversity strategies for hardwired systems, provide adequate mitigation of potential CCF vulnerabilities. In particular, implementation of the Strategy A diversity grouping serves to minimize the opportunities for common systematic faults,

concurrent execution profile, or similar responses to external influences. The use of a microprocessor-based primary protection system and an analog (Laddic logic) secondary protection system at the Sizewell NPP represents the principal example of Strategy A drawn from the survey findings. Table 6.1 provides a summary of the baseline example of Strategy A, along with one variant. Strategy A1 represents the baseline grouping of diversity criteria. Strategy A2 corresponds to the alternative where the same manufacturer provides the equipment while separate teams within the organization are specified for the diverse systems. Figure 6.1 illustrates the baseline combination of diversity criteria.

Table 6.1. Overview of diversities comprising Strategy A

Diversity attribute	Strategy[a]	
	A1	A2
Design		
Different technologies	x	x
Different architectures	i	i
Equipment (Manufacturer)		
Different manufacturer—different design	x	–
Same manufacturer—different design	–	x
Equipment (Processing)		
Different logic processing architecture	i	i
Different component integration architecture	i	i
Different data-flow architecture	i	i
Functional		
Different underlying mechanisms	i	i
Different purpose, function, control, logic, or actuation means	x	x
Life-cycle		
Different design organizations/companies	x	–
Different management teams within same company	–	x
Different design/development teams (designers, engineers, programmers)	i	x
Different implementation/validation teams (testers, installers, or certification personnel)	i	x
Logic (Software)		
Different algorithms, logic, and program architecture	i	i
Different timing or order of execution	i	i
Different runtime environment	i	i
Different functional representation	i	i
Signal		
Different parameters sensed by different physical effects	x	x
Different parameters sensed by same physical effects	x	x
Same parameter sensed by a different redundant set of similar sensors	x	x

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

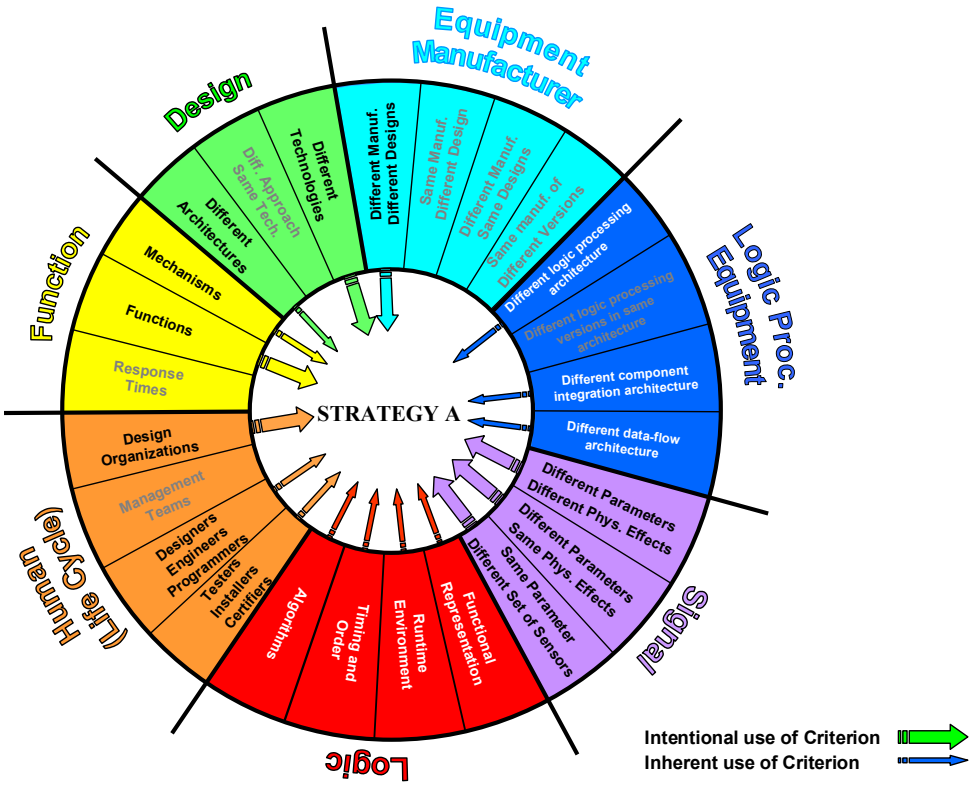

Figure 6.1. Baseline diversity strategies: ORNL Strategy A.

6.3.2 Strategy B: Distinct Technology Approaches

The Strategy B classification is comprised of those diversity strategies that use distinctly different technology approaches as a central element in forming diverse systems, redundancies, or subsystems. Distinct approaches within a broad technology class (i.e., digital) generally provide some intrinsic dissimilarity in the mechanisms by which functions are executed, as well as notable differences in the methods and tools for system implementation. However, in spite of such differences, diverse systems based on different digital technologies, such as FPGAs and microprocessors, may not assume substantially different physical forms at the system level. In fact, implementations using either technology approach will likely consist of the logic processing equipment (i.e., CPU or FPGA) installed on printed circuit boards that are housed within a rack-mounted chassis or card cage. Nevertheless, differences in the nature of these technological approaches contribute to the mitigation of potential CCF vulnerabilities that may arise in design, implementation, or execution of safety systems.

The design diversity provided by use of different digital technologies results in inherent diversities arising from distinctive differences in application-specific FPGAs and general-purpose microprocessors. These inherent diversities involve equipment manufacturer (in terms of processing equipment heritage), processing equipment (reflecting the distinct difference in the mechanisms for processing functions), functional, life-cycle (also in terms of processing equipment heritage), and logic (related to functional implementation and processing characteristics) diversities. A measure of inherent functional diversity results from different underlying mechanisms for the representation of functions (i.e., complex logic hardwired within programmable arrays vs software instructions executed sequentially on a general-purpose CPU). Complementary intentional diversities are established for the logic processing equipment

diversity and also for the cross-dependent life-cycle and equipment manufacturer diversities. The first intentional diversity usage addresses potential commonalities regarding board-level design and equipment, while the second usage relates to potential commonalities in the application-specific system development. Additionally, intentional functional and signal diversities are specified as part of the baseline for this strategy classification. This diversity usage adheres to the traditional CCF mitigation approach that was developed for hardwired systems in response to specific protection system requirements (e.g., GDC 22). The use of intentional functional diversity also implies corresponding intentional logic diversity resulting from the different algorithms associated with the different functional relationships between PIEs and diverse initiation criteria.

6.3.2.1 Survey Findings Related to Strategy B

Of the nonnuclear industries investigated, only the rail industry provided any specific examples of diversity practices that correspond to Strategy B. The primary instances of the use of different digital technologies involve railway control systems. In particular, the SACEM system has been implemented for speed control in rail lines of the Paris RER and the V-Frame system was demonstrated for a wayside switching and signaling application of the Los Angeles Metro Green Line. Each Strategy B example is based on the coded processor approach to provide fault-tolerant control for railway systems. A coded processor involves encoding of data and the software program (i.e., functions) coupled with signature comparison by a hardwired checker. The use of encoding provides information redundancy, while concurrent checking confirms correct performance of the logic processor at each execution step. The safety action taken by the checker on detection of faulted conditions is to remove power and force a safe state to be assumed. This approach is effective in a dedicated hardware environment and is most appropriate for limited-functionality applications. However, it is not readily adaptable to the typical architectural approach employed in the nuclear power industry to provide diverse actuation in response to demands.

Within the international nuclear industry, Olkiluoto provides the only specific example of a Strategy B approach. The primary safety system is microprocessor based, while the hardwired backup system for diverse protection functions is being implemented using FPGAs. Based on discussions with regulatory staff from STUK and representatives from the system supplier, several intentional diversities are being explicitly applied to diversify safety and compensating functions (e.g., diverse reactor trip and ESF functions as well as ATWS mitigation logic) in addition to providing the diverse backup safety system. Specifically, design, equipment (manufacturer), functional, life-cycle, logic (in terms of different algorithms based on different functional relationships), and signal diversities are specified. Additionally, the technology usage provides inherent diversification of the logic processing equipment, with some degree of functional and logic (software) diversities arising as a related consequence. This example is directly relevant for consideration in this classification since it involves parallel diverse systems that implement similar or equivalent functions to respond to safety initiation criteria.

6.3.2.2 Rationale for Strategy B

6.3.2.2.1 Impact of Strategy B Technology Differences

Distinctly different technology approaches are generally characterized by significant differences in the underlying mechanisms by which they process functions (i.e., representation and execution) and the methods for implementing functions. As a result, systems based on different digital technologies typically can be expected to provide differences in their dynamic behavior, microarchitectural configuration, and methods for realizing (i.e., implementing and executing) functions. Each of these characteristics contributes to mitigation of the potential for common systematic faults, concurrent execution profiles, or similar responses to external influences.

FPGAs and complex programmable logic devices (CPLDs) are basically digital computational platforms that enable field-programmable application-specific integrated circuits (ASICs). In contrast, microprocessors are commercial off-the-shelf (COTS) computational platforms that can be adapted for specific applications through software-configured usage of their general-purpose instruction sets (i.e., operation codes, data management). While each technology approach processes digitized data, the specific method of processing provided by each technology results in significant differences in the execution of functions. Thus, the likelihood that either concurrent execution states or common external influences will lead to a CCF should be minimized.

The nature of design and mechanisms of implementation for these digital technologies are significantly different. Although applications developed based on either technology ultimately are translated to fundamental forms (i.e., machine language for CPUs or array configurations for FPGAs) and the implementation techniques of each technology can utilize high-level abstraction (e.g., graphical configuration of basic block modules, descriptive language representations) and automatic generation tools, the design concepts are distinctive. For example, FPGA usage typically involves some form of digital microcircuit design (i.e., configuring gate arrays) to achieve a hardwired logic structure that corresponds to specific functions. Conversely, microprocessor usage generally involves development of a software program representing the sequence of computations needed to execute a function. Both design approaches can address highly complex functionality but the cognitive models that are constructed by the designer/implementer in either case are likely to be significantly different. This consequence of the technology difference, along with differences in tool sets, addresses some of the most likely sources of design mistakes and implementation errors. Thus, the prospect of common systematic faults arising from the design and implementation of diverse systems based on different digital technologies is less than that for those based on similar digital technologies.

Finally, it is important to recognize that different digital technology approaches also present some similarities in behavior that arise from the nature of digital computations (i.e., input → operation → output). These similarities allow programmable logic devices to be used to emulate general-purpose microprocessors. Essentially, the intellectual property (IP) core of a CPU can be implemented in a CPLD. Thus, FPGAs can be adapted to provide equivalent capabilities and can be used as central processing cores to execute software-based functions. In such instances, significantly greater similarity between the FPGA-based system and the CPU-based system is provided in terms of the representation of functions and their execution. Although differences in microarchitecture will arise due to the nature of the processor implementations, the execution commonalities that are likely if this implementation approach is taken would make this strategy grouping more appropriate for consideration in the Strategy C classification.

6.3.2.2.2 Inherent Diversities for Strategy B

Distinctly different technology approaches typically provide significant dissimilarity in the means of physically realizing functions and notable differences in the mechanisms of execution. As a result, some level of inherent diversification is achieved for several other attributes of the comparative systems. The consequence of employing this technology difference as a basis for design diversity is to provide some measure of inherent equipment, functional, life-cycle, and logic diversity.

The equipment associated with the different digital technologies provides some basic identifiable diversity. Inherent equipment diversity clearly relates primarily to the logic processing equipment, and it arises from different underlying mechanisms for accomplishing functions (i.e., software statement execution vs hardwired digital logic). Basically, the primary logic processing equipment, which embodies the characteristic design diversity within this classification, generally provides some inherent differences in the processing of functions, algorithms, and/or logic. Typically, FPGA-based implementation of functions involves application-specific design, representation, and fabrication of

hardwired logic to enable functional processing of digital inputs within a preconfigured gate array framework. In contrast, a microprocessor-based trip system processes digitized data through sequential execution of instructions based on software statements that instantiate functional algorithm(s) and voting logic. As a result of the difference in processing elements, microarchitectures, and computational mechanisms, the processing equipment diversity criterion is generally satisfied inherently for this technology difference.

Caution is warranted regarding the treatment of FPGAs and CPUs as inherently different logic processing equipment representing distinct technology approaches. The effect of this diversity criterion, which arises from the distinctive characteristics of the different digital technology approaches, can be compromised if the FPGA platform is used to emulate the base CPU of the diverse system (i.e., the IP core of the CPU is implemented in an FPGA form). Essentially, the FPGA serves as an equivalent CPU that can execute common software functions. Thus, the manner in which FPGAs are employed must be considered before assigning credit for this inherent diversity. Additionally, inherent diversity in logic (software) may be similarly compromised.

The equipment difference associated with this technology usage likely involves factors such as development heritage and manufacturer. However, similarities in the nature of digital technology can present some equipment commonalities such as component integration architectures (i.e., circuit board design) or data-flow architectures (i.e., internal bus structure). The potential impact of these commonalities warrants further consideration in determining what intentional diversities need to be specified. While the potential for common components is generally limited to the board level or higher, manufacturer differences reduce the potential for common defects introduced by process deficiencies or source material defects.

As described above, the intentional application of different digital technologies as the primary design diversity results in an inherent functional diversity involving different underlying mechanisms to accomplish the safety function. This additional inherent diversity relates specifically to the digital aspects of this criterion for functional diversity that arise from the different functional execution mechanisms for the safety functions implemented on the diverse technologies. This inherent functional diversity is also observed in the findings regarding Olkiluoto.

Differences in development heritage reduce the prospect of common human contributors to the potential residual fault space for I&C platforms, modules, or components based on each technology. However, inherent life-cycle diversity may be limited to the base platform or, specifically, to the logic processing component (i.e., FPGA or CPLD vs CPU). In such cases, action would be needed to address the prospect of common human contributors for the system and application development. The effect is to control the potential for common system design mistakes or application implementation errors.

Because of the nature of the processing mechanisms for distinctly different digital technologies, each criterion of the logic diversity attribute is inherently present. The criterion providing different algorithms, logic, and logic (program) structure is inherently achieved through diverse functional configurations. Essentially, dedicated preconfigured arrays provide the program structure and functional representation in a programmable logic device while software statements calling general-purpose instructions in a predefined sequence provide the program architecture for microprocessor-based systems.

The criterion providing different timing or order of execution is inherently satisfied through the distinctly different means by which functions are executed (e.g., sequential computations manipulating digital data in contrast to parallel processing through hardwired gate array interconnections in response to digitized inputs). The criteria on different execution environments (e.g., operating systems for microprocessor-based technologies) and different functional representations (e.g., computer languages for software-based systems, hardware description languages for hardwired-logic-based systems) are also inherently satisfied because of the significant difference in the way the diverse technologies represent and execute functions.

6.3.2.2.3 Basis for Diversity Usage in Strategy B

The intentional use of distinctly different technology approaches constitutes the principal design diversity that is characteristic of this diversity strategy classification. Applying different digital technologies as the basis for diverse designs provides inherent diversities that result in a significant effect on the potential for CCF vulnerabilities related to systematic faults, execution commonalities, or responses to common external influences. Nevertheless, the diversity usage found in the primary example of a Strategy B approach (Olkiluoto) involves intentional application of design, equipment (manufacturer), functional, life-cycle, logic (in correspondence with functional diversity), and signal diversities. Coupling findings from the Olkiluoto example with an evaluation of the prospective contribution of each diversity attribute provides a basis for grouping the diversity criteria to establish a baseline for Strategy B.

Equipment (Manufacturer) Diversity. Within the Strategy B classification, diversity strategies generally involve different designs in the context of the equipment manufacturer diversity attribute. However, it is noted that the nature of digital technologies and the commonality of platform-level architectures (i.e., circuit boards within card cages) suggest that different designs can present some similarities and may be available from the same manufacturer. In cases where a common supplier is selected, action is warranted to minimize the potential for common systematic faults arising from manufacturing defects (e.g., from process deficiencies or flawed source components) or implementation errors (e.g., system integration errors). Ensuring rigorous quality control and establishing separate development teams are common actions.

For the Olkiluoto example cited in this research, the equipment manufacturer for the hardwired backup system had not yet been confirmed although it is anticipated that AREVA would serve as system supplier. However, the clear expectation expressed in discussions with STUK[112] was that different teams are to be engaged for each diverse system should a common manufacturer prove to be the case. The rail industry examples that are relevant to the Strategy B classification involved selection of the same manufacturer because the hardwired checker is part of an integrated system approach for the rail control applications. This is due to the nature of the checking functionality (i.e., involving signature comparison for intermediate states) and the architectural approach employed.

Equipment (Processing) Diversity. Logic processing equipment diversity can also contribute to resolving vulnerabilities that may arise from any significant common components, such as processing unit, system services, board architecture, bus structure, and peripherals. Because of the design diversity selection, different logic processing architectures (i.e., FPGA and CPU microarchitectures) are provided. As discussed above, the basic impact of different logic processing architectures relates to a reduced likelihood of common systematic faults and differences in the execution profile (i.e., the internal states of the processor).

Given the nature of digital technologies, it is reasonable to anticipate the prospect of commonalities in the circuit board design for diverse implementations based on FPGAs and CPUs. The use of different component integration architectures (i.e., circuit board designs) addresses potential commonalities in the equipment and prospective common design errors. One result of invoking this diversity can be a contribution to diversifying each system's response to external influences such as environmental effects (e.g., temperature/humidity, radiated electromagnetic interference) or aging (e.g., metallic whiskers or electromigration). Additionally, employing circuit boards of different design can help minimize the prospect for common systematic faults at the platform level. This can include component defects, resource integration deficiencies, or board design errors.

The acquisition of diverse systems from different manufacturers may result in circuit board design differences as a direct consequence. Additionally, differences in chipsets associated with each

microprocessor also diversify the board components and may influence design difference as well. As a result, it may not be necessary to intentionally specify circuit board differences. Nevertheless, it is prudent to identify differences to the degree that such information is available for the platform. While simple parts that are common can be treated through source determination and qualification, complex components need to be considered to fully address CCF vulnerability associated with the logic processing equipment.

It is possible to justify the use of alternate means to address concerns about potential CCF vulnerabilities arising from common circuit boards. Supporting evidence can involve confirmation that the circuit board uses a very simple design, employs parts of high quality, and has been thoroughly tested and qualified. In addition, control of external influences can also be used to demonstrate that measures are provided to ensure that common stress factors (e.g., power quality, environmental conditions) are not applied concurrently to each system.

The use of different data-flow architectures (i.e., bus architectures) is similar to consideration of different component integration architectures. However, management of data flow throughout the system and the topologies for bus structures are generally well established and these architectures have been standardized in many instances. Use of diverse bus architectures seems unnecessary. Little specific information was provided on bus architectures for the diversity examples cited in this research.

The Olkiluoto example cited in the Strategy B discussion of survey findings does not specify circuit board design or bus architecture differences. The rail examples that are identified with this strategy classification employed common data buses and similar circuit boards. In all of these cases, different logic processing architectures are inherently provided due to the choice of technology and design concept (i.e., no CPU emulation).

Functional Diversity. As discussed above, the intentional use of functional diversity, in combination with signal diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research. The relevant diversity criterion involves different purpose, function, control logic, or actuation means. Basically, different functional expressions capture the diverse safety function initiation criteria with the result being differences in the functions and control logic assigned to each diverse system. As discussed above, inherent functional diversity is also achieved due to the differences in the nature of the technologies, which leads to diversification of the underlying mechanisms for processing functions.

Findings from the investigation of diversity practices at international NPPs confirm the prevalence of this diversity approach as an intentional diversity. For the Olkiluoto example, functional diversity and signal diversity are intentionally applied in combination. From the survey of nonnuclear industries, significant functional diversity was achieved for the rail examples based on the extreme difference in the purpose of each system (i.e., active control vs real-time checking using performance signatures).

Life-Cycle Diversity. As noted above, the technology difference for Strategy B approaches affects the commonality of skill sets employed and similarity of cognitive modeling achieved by personnel involved at various phases of the system life-cycle phases. Although there are high-level similarities in the life-cycle activities (e.g., representation of a functional application in high-level languages using software-based design tools), the nature of the design is different for software-based systems and hardwired-logic-based systems. Thus, the use of distinctly different digital technologies provides dissimilarity for functional representation, processing mechanisms, dynamic behavior, equipment types, and implementation approaches. Each of these factors contributes toward minimizing the similarity of design products, implementation tool sets, and testing practices. As a result, some degree of diversity in the system concept, design development, and implementation techniques is achieved inherently. Nevertheless, life-cycle diversity is expected to be practiced at Olkiluoto by having different teams responsible for the primary reactor protection system and the hardwired backup system.

As previously described, the use of different design organizations generally provides across-the-board life-cycle diversity to minimize the potential for common systematic faults to be introduced by human contributors. This diversity is generally achieved by default through the use of different design organizations. If a common manufacturer (or system supplier) is selected, comparable life-cycle diversity can be achieved through the use of separate teams for each system. Most of the examples identified in the survey of diversity usages involved the intentional application of life-cycle diversity either through separate teams within an organization or, more commonly, at different companies.

Logic (Software) Diversity. As previously discussed, the logic diversity attribute is inherently satisfied because of the nature of the processing mechanisms for distinctly different digital technologies. In association with the traditional use of intentional functional diversity, the criterion providing different algorithms, logic, and logic (program) structure is also intentionally achieved because of the different functional relationships that are represented in digital form for each diverse system. Each of the differences in logic (either intentional or inherent) provides some diversification of the transition mechanisms between internal states, resulting in differences in the execution profile of the system.

Again, it is noted that use of FPGAs to emulate the processing core of a CPU may compromise the logic diversification benefits generally associated with this technology difference. In those instances, the function is executed through software in each system. The result is that the logic diversity may be limited to that achieved through microarchitectural differences in the representation of the code at the machine level and the resulting execution differences. Thus, confirmation of the nature of the FPGA implementation is warranted before crediting the inherent diversities discussed for this attribute.

Signal Diversity. The selection of distinct technology approaches as the basis for parallel diverse systems, redundancies, or subsystems has no direct impact on signal diversity. As discussed above, the intentional use of signal diversity, in combination with functional diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research.

This usage is consistent with the examples identified from the nuclear power industry survey. For the Olkiluoto example, signal diversity is employed within the safety system and, to a lesser extent, between the safety and backup systems. In addition, signal diversity is applied to enhance diversity between redundancies performing trip and engineered safety feature functions.

6.3.2.3 Description of Strategy B

6.3.2.3.1 Design Diversity

Intentional diversity is provided through the selection of distinct technology approaches. The specific form of technology difference employed in this classification involves the use of different digital technologies (e.g., FPGA or CPLD vs general-purpose CPU) as the basis for different systems, redundancies, or subsystems. The purpose of this diversity usage is to address the potential CCF vulnerabilities by minimizing the prospect for common systematic faults, concurrent execution profiles, and similar response to common external influences.

The acceptability of diversity usage within this strategy classification relies upon the assumption that the FPGA-based processing equipment provides direct implementation of the functional logic rather than emulation of a general-purpose microprocessor. The nature of the FPGA-based system should be confirmed to determine whether a strategy involving different digital technologies is appropriate for treatment within the Strategy B grouping.

6.3.2.3.2 Equipment (Manufacturer) Diversity

Intentional diversity is provided through the selection of different manufacturers (or system suppliers) for different equipment designs. The purpose of this diversity usage is to minimize the potential for common systematic faults arising from manufacturing defects or implementation errors.

Alternate diversity strategies within the Strategy B classification may adopt the intentional selection of the same manufacturer of different designs as a variation of the baseline combination of diversity criteria. Use of the alternate equipment manufacturer criterion is linked to the compensatory intentional application of life-cycle (human) diversity.

6.3.2.3.3 Equipment (Processing) Diversity

Inherent processing equipment diversity for different digital technologies is generally provided through different processing equipment architectures. As noted in the discussions of the impact of the technology difference and the inherent diversities resulting from use of this design diversity, confirmation of the nature of the FPGA implementation is warranted. Diversity strategies involving FPGA-based emulation of a general-purpose CPU may be more appropriately treated within the Strategy C classification.

Within the Strategy B classification, intentional diversity is provided through the selection of different circuit board designs. The application of the component integration architecture diversity criterion can contribute to minimizing the potential for common systematic faults at the platform level (e.g., component defects, integration deficiencies, or board design errors) as well as common susceptibility to external influences such as environmental stress (e.g., temperature/humidity, radiated electromagnetic interference) or aging (e.g., metallic whiskers or electromigration).

Recognizing that comparable benefits may be achieved through alternate means such as simplification of board design, thorough qualification and testing, and control of external influences, this diversity criterion is a reasonable candidate for optional treatment. The justifying basis for omitting the intentional application of this criterion should address considerations such as the complexity of the platform designs, minimal use of common components, and limited commonality of stress factors. For strategic approaches in which component integration architecture commonalities are justifiably treated as minor, coupling that strategy variation with the use of different equipment manufacturers can provide added (potentially compensatory) assurance that the potential for common board design errors or component defects is reasonably addressed.

6.3.2.3.4 Functional Diversity

Intentional diversity is provided in the form of different functions or control logic associated with coverage of a reduced set of PIEs (as needed based on the D3 analysis for the plant) and the use of diverse safety function initiation criteria (cf., GDC 22 and signal diversity). The purpose of this diversity usage is to provide differences in functional requirements and design specification as well as to diversify the signal trajectories seen by each system.

6.3.2.3.5 Life-Cycle Diversity

Intentional diversity is provided through the use of different design organizations to conduct life-cycle activities related to the application-specific system development. This baseline criterion is linked to the intentional selection of the equipment manufacturer diversity criterion for different manufacturers of different designs. The purpose of this life-cycle diversity usage is to avoid the introduction of systematic

faults during design and implementation of the diverse systems due to common mistakes or misunderstandings by shared human resources.

Alternate diversity strategies within the Strategy B classification may adopt the intentional selection of separate teams when the same manufacturer is used to supply the diverse systems. In particular, this alternate strategic approach involves the manufacturer intentionally establishing, to the extent practical, the following teams for each system: different management teams; different design and development teams; and different implementation, validation, and installation teams.

6.3.2.3.6 Logic (Software) Diversity

Intentional diversity is provided in the form of different algorithms, logic, and program architectures that are implemented in digital form. This diversity is associated with the intentional use of functional diversity. The purpose of this diversity usage is to contribute to the diversification of execution profiles (i.e., internal states and state transitions) and to help in avoiding potential systematic faults due to common mistakes or misunderstandings in the design process or common errors in the implementation process.

6.3.2.3.7 Signal Diversity

Intentional diversity is provided through the use of separate and/or diverse measurements of plant parameters. The purpose of this intentional diversity usage involves minimization of commonalities, support of functional diversity (cf., GDC 22), and diversification of concurrent execution profiles. Each of the three signal diversity criteria is appropriate for application as intentional diversities to the extent practical.

6.3.2.4 Strategy B Summary

Strategies that involve the use of distinctly different technology approaches as the basis for diverse systems, redundancies, or subsystems are classified as examples of Strategy B. The combinations of diversity criteria that characterize Strategy B, in conjunction with traditional diversity strategies for hardwired systems, provide adequate mitigation of potential CCF vulnerabilities. In particular, implementation of the Strategy B diversity grouping serves to minimize the opportunities for common systematic faults, concurrent execution profiles, or similar responses to external influences. 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 a significantly different architectural approach through which to implement strategic use of this technology difference. Table 6.2 provides a summary of the baseline example of Strategy B, along with two variants. Strategy B1 represents the baseline grouping of diversity criteria. Strategy B2 corresponds to the alternative in which the same manufacturer provides different equipment but separate teams within the organization are specified for the diverse systems. Strategy B3 corresponds to the alternative in which circuit board diversity can be shown to be unnecessary. Figure 6.2 illustrates the baseline combination of diversity criteria.

Table 6.2. Overview of diversities comprising Strategy B

Diversity attribute	Strategy[a]		
	B1	B2	B3
Design			
Different approach—same technology	x	x	x
Equipment (Manufacturer)			
Different manufacturer—different design	x	–	x
Same manufacturer—different design	–	x	–
Equipment (Processing)			
Different logic processing architecture	i	i	i
Different component integration architecture	x	x	–
Functional			
Different underlying mechanisms	i	i	i
Different purpose, function, control, logic, or actuation means	x	x	x
Life-cycle			
Different design organizations/companies	x	–	x
Different management teams within same company	–	x	–
Different design/development teams (designers, engineers, programmers)	i	x	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	x	i
Logic (Software)			
Different algorithms, logic, and program architecture	x	x	x
Different timing or order of execution	i	i	i
Different runtime environment	i	i	i
Different functional representation	i	i	i
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 (–).

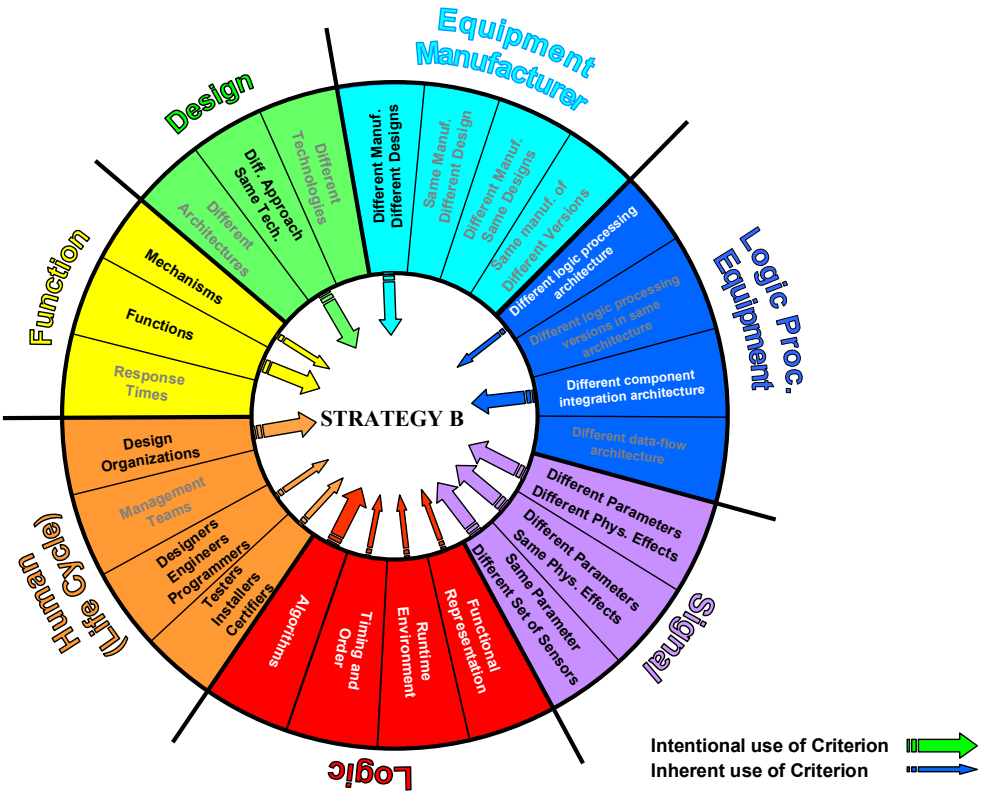

Figure 6.2. Baseline diversity strategies: ORNL Strategy B.

6.3.3 Strategy C: Architectural Variations within a Technology

The Strategy C classification consists of those diversity strategies that adopt architectural variations within a particular technology as a contributing factor in providing diverse systems, redundancies, or subsystems. Application of architectural variations within digital technology is achieved primarily through the use of different microprocessors as the basis for diverse systems. This type of technology difference at the system level is not often readily discernible (e.g., few obvious differences between two computer-based systems of similar composition and configuration providing similar functionality). The nature of design diversity within this strategy classification arises primarily at the microarchitecture level (i.e., CPU or processing element), although macroarchitectural differences at the board or module level may also have an effect. Essentially, the microarchitectural differences at the core of the logic processing equipment provide the principal design diversity for systems being compared and result in some degree of hardware and software dissimilarity. The primary impact of this design diversity is that microarchitectural differences between microprocessors affect the implementation of functions for each system (e.g., translation of source code to executables) and provide some differences in execution (i.e., different physical realization of basic computational operations).

The inherent diversities that arise to some degree from this design diversity relate to equipment manufacturer, life-cycle, and logic diversities. Regarding equipment manufacturer and life-cycle consideration, inherent diversity is achieved in terms of the heritage of the diverse microprocessors. Inherent logic diversity results from the difference in fundamental execution mechanisms. The inherent diversities for this technology difference provide only modest contributions to minimizing the potential

for CCF vulnerabilities. As a result, criteria from the other diversity attributes are intentionally employed to supplement the effect of the design diversity provided by this technology difference. In association with the use of diverse microprocessors, the intentional diversities that are established in the baseline strategy for this classification are equipment manufacturer (system supplier), logic processing equipment, life-cycle, and logic (software) diversity. As with the other strategy classifications, the traditional approach of intentionally applying functional and signal diversities is also adopted as part of the baseline for this strategy classification. In addition to emphasizing well-established best practices, the usage of these latter diversities provides some particular benefits for addressing CCF concerns related to digital systems.

6.3.3.1 Survey Findings Related to Strategy C

The investigation of diversity practices for the nonnuclear industry identified several examples that can be classified as Strategy C approaches. These examples involved the use of different microprocessor-based systems as a means of addressing potential CCF vulnerabilities. The most prominent examples are found in the aviation industry and the chemical industry. In both industries, the approach to diversity can be classified based on the selection of architectural variations within digital technology.

For the aviation industry, diversity usage based on different microprocessors is found in implementations of fly-by-wire flight control. The Airbus flight control systems for the A320, A340, and A380 aircraft make use of diverse microprocessors in parallel diverse control systems. This design diversity (with the associated equipment diversity) is supplemented by intentional functional, life-cycle, and logic (software) diversity. These diversities are introduced through the use of a reduced-functionality flight control provided by the diverse system, different organizations or system development teams, different algorithms (arising from the reduced set of control laws and alternate control surfaces), and different software implementation (i.e., different languages and coding methods). The Boeing 777 flight control system also employs diverse microprocessors. However, the approach chosen by Boeing implements the technology difference as redundancies (i.e., lanes) embedded within parallel redundant flight control systems (i.e., channels). The reduced-functionality flight control capability for the B777 is implemented in the common software for all three channels, so no functional or software diversity is intentionally employed. The modest exception for software diversity is the use of different Ada compilers to translate the code for each lane. Based on the expectation that requirements/specification errors would be the most likely source of software faults, Boeing focused on fault avoidance through the use of formal methods and quality processes in developing the design specification. Thus, the cost and complexity of managing separate design teams were considered to be unnecessary and life-cycle diversity was not employed. The differences in approaches used by Airbus and Boeing to mitigate potential CCF vulnerabilities in their flight control systems arise from different concerns by each company. Airbus focused on software design faults, while Boeing emphasized design faults for very complex COTS hardware and implementation faults arising from code translation (compilers).[129] Essentially, Boeing relied on its quality processes for the design items it controlled and employed diversity for COTS components and tools. Nevertheless, in each example, design diversity is employed through the use of different microprocessors (i.e., architectural variations within a technology) within redundancies. This practice is especially significant given the constraints on aircraft equipment and the burden of maintaining separate designs.

The chemical industry guidance on chemical process safety also corresponds to the Strategy C classification. In particular, the guidelines issued by the CCPS provide recommendations on the use of diversity to achieve a high integrity level. As is the case for the nuclear power industry, separation (e.g., physical, electrical, and communication isolation) is cited as a key consideration in avoiding potential CCF vulnerabilities. Also, diverse redundant hardware is recommended to avoid a common hardware fault. In addition to these traditional approaches to addressing potential CCF vulnerabilities, the "software" aspect of CCF is addressed through guidance on the use of programmable electronic systems

(PES). The stated goal is to address potential CCF vulnerabilities related to hardware, system software, and application software.[66] Recommended practices involve different equipment (e.g., differences in devices and manufacturers), different functions, different software, and different signals. The impact of common designers, programmers, testers, installers, and maintainers is noted, and the use of different personnel is recommended. Thus, the composite diversity strategy for the chemical industry employs equipment (both manufacturer and logic processing), functional, life-cycle, logic (software), and signal diversities. It is also noted that selection of a nonprogrammable device (i.e., Strategy A) can mitigate concerns about software faults.

Use of different architectures within a technology (i.e., different microprocessor microarchitectures) is the most common design diversity observed in the examples cited from the international nuclear power community. In particular, Chooz, Darlington, and Temelin illustrate various means by which groupings of diversity criteria that are characteristic of the Strategy C classification have been used. Additionally, the I&C system architecture being implemented at Lungmen provides another example of this strategic approach.

The application of diversity in these nuclear power examples involves different architectural schemes. For Chooz, the diversity occurs across lines of defense through the use of a qualified reduced-functionality system (providing ATWS functions) within the control line of defense to back up the safety systems. Darlington implements diversity in coequal protection systems (i.e., SDS1 and SDS2) that drive diverse actuation mechanisms. The Temelin example involves primary and secondary safety systems with the nonsafety-grade diverse (secondary) actuation system providing reduced functionality through a limited set of safety function initiation criteria. The I&C system architecture for Lungmen also provides reduced-functionality backup of safety functions. Additionally, Lungmen employs significant diversity among systems within and across lines of defense.

In each of these examples, the traditional uses of diversity (e.g., signal and functional diversity) are employed. Traditional approaches to promote hardwired diversification, such as independence, diverse power supplies, and diverse actuation equipment, were also applied. At Chooz, the different functions (i.e., reduced function set and different initiation criteria) are implemented on different microprocessor-based equipment of similar designs that were provided by different manufacturers. The Temelin example is similar to that of Chooz, with the principal exceptions arising from the architectural application of diversity (standalone DAS vs embedded ATWS) and the source of the equipment. For Temelin, the different microprocessor-based equipment was provided by the same supplier (Westinghouse) rather than by separate suppliers. The designs of the safety (Eagle) and process control (Ovation) equipment are similar, but different microprocessors are used and different software implementations provided. Additionally, different teams developed the platforms and applications. In both of these cases (Chooz and Temelin), functional diversity is implemented primarily within the safety system while the functional and signal diversity for the diverse actuation system results mainly from a reduced set of function initiation criteria and separate redundant sensors.

In the case of Lungmen, functional and signal diversity is employed both within and between systems. Additionally, a diversity of system suppliers for Lungmen provides an extensive use of equipment diversity throughout the I&C system architecture. Different functions are provided within the same redundancies of the safety systems and between different systems providing diverse safety responses through similar or compensating functions. Focusing on the diversity provided by the ATWS system, the application of diversity is similar in approach to that used at Chooz.

Because of the nature of CANDU reactors and the requirements for diverse shutdown mechanisms, Darlington provides equivalent safety coverage of PIEs through the two shutdown systems. The diverse systems at Darlington were provided by different suppliers and consist of different equipment with limited design similarity. Functional and signal diversities are implemented to the full extent feasible within and between the systems. Additionally, software diversity is promoted not only through different

algorithms and software program architectures but also through the use of different software development tools and languages. The nature of the phenomena monitored for safety function initiation and the difference in actuation means provide additional functional diversity related to time scale and underlying mechanism for safety response. However, these considerations relate more to traditional diversity usage than to diversities specific to potential CCF vulnerabilities arising from the unique characteristics of digital technology.

Each of the nuclear power examples involves application of intentional diversities in addition to the design diversity associated with the use of different architectures within digital technology. The diversity in processing equipment is related to the technology employed (i.e., different CPUs). Life-cycle diversity is used in each case, and the particular criteria applied are related to the choice of equipment manufacturer. The specification of functional and signal diversity in response to regulatory design criteria is common and contributes to logic diversity in terms of the algorithms that relate to diverse initiation criteria. In some of the examples, additional logic diversity is provided through the choice to implement reduced functionality and/or through other criteria to diversify software (e.g., language, operating system).

Finally, approaches to diversity based on the use of the different microprocessors are addressed in a several articles, reports, and guidance documents referenced in this research. In particular, recommendations on the use of diversity to support nuclear plant safety applications that employ computer-based technology are given in the common positions on software design diversity that were developed by European regulators.[114] Additionally, consideration of diversity-seeking decisions during the development of diverse software-based systems is discussed at great length in research on software diversity.[119] The volume of information provided by these resources is also considered in the development of the baseline strategy for this classification.

6.3.3.2 Rationale for Strategy C

6.3.3.2.1 Impact of Strategy C Technology Differences

In contrast to fundamentally diverse technologies or distinctly different technologies, architectural variations within a technology do not provide significant differences in their underlying physical nature or the mechanisms by which they process functions. As a result, the associated characteristics of this design diversity do not substantially contribute to mitigation of the potential for common systematic faults, concurrent execution profile, or similar responses to external influences. To illustrate, the design and implementation of functions for computer-based systems have many commonalities (e.g., high-level language instantiation of the functions, similar cognitive models of design realization) that are unaffected by microprocessor differences. Additionally, execution of software from common source code on different computers is similar from a macroperspective (i.e., program level). Nevertheless, use of this design diversity can lessen the prospect for some common design faults by differences in the fundamental architecture of highly complex electronics and can affect the execution of functions on diverse platforms through differences in the internal conditions of state-machine processing cores.

Architectural variations within a technology provide differences in the way processing elements are interconnected and how those elements interoperate. Basically, the organization of fundamental processing units affects how functions are executed, often at the lowest (i.e., machine) level. In terms of different microprocessors, differences in microarchitecture result in dissimilarity in the way the higher-level abstraction of the represented integrated circuit operation is accomplished. This abstraction for the structure of a microprocessor is called an instruction set architecture (ISA). An ISA specifies the machine language (or opcodes) that represents the native commands for the execution units and data paths implemented in the microarchitecture. The ISA describes fundamental processing elements such as data types, instructions, addressing, modes, registers, and so forth, to facilitate programming. Even for CPUs

sharing a common ISA, the internal designs can be substantially different. Different efficiency enhancements (e.g., instruction pipelining, memory caching, and multithreading) can result in very different execution of ISA operations at the microcode level.

As another consequence of differences in machine instructions, pipelining, and other computational mechanisms that exist between diverse microarchitectures, differences in the machine-level representation of software and execution of the constituent opcodes provide some diversity in the performance of software programs. Additionally, diverse microprocessors also provide some measure of diversity in the system software (i.e., operating system and system services), translation of application software to the machine level (e.g., compilers, assemblers), and runtime execution of software operations. This diversity does not address software design or programming faults introduced during design and coding of an application. However, it does provide for some degree of diversity in software execution (i.e., the basic mechanisms for state transition).

The use of different microprocessors generally provides some difference in heritage, depending on the manufacturer, processor family, and/or family generation. Given a choice of microprocessors, the commonality of human-introduced design and implementation errors can be minimized for the main processing components (i.e., microprocessors, chipsets) of different system platforms, especially as microarchitecture differences are more pronounced. Chip manufacturers do publish current errata sheets to document known flaws so that these can be compared to give further indication of differences. Additionally, diverse microprocessors from different manufacturers are likely to be fabricated using different process lines, thus minimizing the prospect of common manufacturing defects. However, this assumption warrants some caution. Quality assurance processes for Appendix B suppliers can address the issue of component source commonalities. Nevertheless, the microarchitecture differences, coupled with the likely heritage difference, decrease the prospect of common faults (e.g., flaws in the implementation of an ISA, fabrication defects) between diverse microprocessors.

Many microprocessor families have associated chipsets (i.e., memory controller hub, I/O controller hub) that are specific to that family. These specialized components are generally designed to work with particular microprocessor families to provide optimum performance. The selection of diverse microprocessors can contribute to diversifying the main circuit board design for different platforms through differences arising from the associated chipsets. In this way, the potential for systematic faults in board design and common response to external influences can be reduced.

Additionally, some understanding of the architectural differences between microprocessors/chipsets facilitates consideration of the degree of diversity provided. Fortunately, the nuclear power and nonnuclear industry cases of diversity usage, which are cited in this research, provide examples of diverse microprocessors that have been judged to be adequately diverse to address concerns about potential CCF vulnerabilities arising from computer-based platforms.

The fundamental impact of using diverse microprocessors is to reduce the potential for common faults in the processing core of computer-based systems and to enforce some diversity in the internal states of diverse microprocessor-based systems. As a result, some modest benefit arises through reduced potential CCF vulnerabilities due to implementation faults (i.e., translation of a program into machine language) or execution commonalities. These considerations appear to be the driver for the use of different microprocessors and compilers in the Boeing 777 flight control system.

6.3.3.2.2 Inherent Diversities for Strategy C

The use of different microprocessors as the selected design diversity approach contributes little inherent diversification to the systems being compared in regard to other diversity attributes. At the platform level, there is likely to be some inherent equipment manufacturer diversity for the different microprocessors and, possibly, the associated chipsets. Likewise, inherent life-cycle diversity would

result from the different development heritage of diverse microprocessors. Some degree of inherent processing equipment diversity for the component integration architecture (i.e., circuit board) is likely if the chipsets are specific to the chosen microprocessors. As discussed above, some modest logic diversity may arise from the effect of diverse microarchitectures and chipsets on the runtime environments (operating system and system services).

Finally, diversity of the processing equipment is intentionally specified in correspondence with the design diversity selection. In effect, the choice of different architectures within a technology implies selection of different processing equipment (i.e., microprocessors) and the converse is also true.

6.3.3.2.3 Basis for Diversity Usage in Strategy C

The design diversity that is characteristic of the Strategy C classification corresponds to the intentional selection of different architectures within a technology. This diversity, in the form of different microprocessors, provides some reduction in the potential for CCF vulnerabilities related to systematic faults and concurrent execution profiles. However, this impact is very limited. Additionally, the modest technology diversity provided results in little inherent diversification for other application-specific aspects of comparative systems. As a result, use of intentional diversity is needed to contribute to resolving concerns about remaining potential CCF vulnerabilities related to systematic faults, execution commonalities, or responses to common external influences. Diversity usage in the cited examples corresponding to Strategy C involved intentional application of equipment manufacturer diversity, processing equipment diversity, functional diversity, life-cycle diversity, signal diversity, and logic (software) diversity. Based on these examples and consideration of the prospective impact of each diversity attribute and its associated criteria, the basis for a strategic grouping of diversity criteria can be derived to establish a baseline for Strategy C.

Equipment (Manufacturer) Diversity. As indicated in the discussion above, equipment differences for platforms based on different microprocessors can be subtle. Microarchitecture differences are not readily apparent when comparing two systems. Generally, processing equipment differences must be stated or directly observed to confirm that two microprocessor-based platforms are different. The review guidance in BTP 7-19 cautions against assuming diversity based solely on “name-plate” differences.

The majority of the examples cited in this research that correspond to Strategy C involve use of different equipment and selection of different manufacturers to supply the diverse systems. Where the same supplier was used, separate teams and strict quality controls were applied to each diverse system in most cases. In cases where a common supplier is selected, adopting these practices is prudent to minimize the potential for common systematic faults arising from manufacturing defects (e.g., from process deficiencies or flawed source components) or implementation errors (e.g., system integration errors).

Equipment (Processing) Diversity. Logic processing equipment diversity can also contribute to resolving vulnerabilities that may arise from any significant common components, such as processing unit, system services, board architecture, bus structure, and peripherals. Because of the design diversity selection, different logic processing architectures (i.e., CPU microarchitectures) are provided. As discussed above, the basic impact of different logic processing architectures relates to a reduced likelihood of common systematic faults and differences in the execution profile (i.e., the internal states of the processor). Different microprocessor families from different manufacturers can be expected to provide significant differences in microarchitecture. Caution is warranted if the microprocessor difference is limited to different generations from the same manufacturer. Some effort may be needed to ensure that significant differences in microarchitecture are present. Information such as descriptions of the architectural enhancements implemented in the evolution of the CPU family, errata differences for the reported chip flaws, associated development of new supporting chipsets, and so forth may give evidence of the degree of difference between the CPUs.

In many cases, diverse microprocessors also have differences in the associated chipsets, which are often supplied by different manufacturers as well. These diverse processing components contribute to differences in the circuit board (or component integration architecture). The result of diversity in chipsets increases the diversity of components at the board level, minimizes the prospect for embedded residual faults in complex processing components, and slightly reduces the commonality of the board design.

The use of different component integration architectures (i.e., circuit board designs) addresses potential commonalities in the equipment and prospective common design errors. One result of invoking this diversity can be a contribution to diversifying each system's response to external influences such as environmental effects (e.g., temperature/humidity, radiated electromagnetic interference) or aging (e.g., metallic whiskers or electromigration). Additionally, employing circuit boards of different design can help minimize the prospect for common systematic faults at the platform level. This can include component defects, resource integration deficiencies, or board design errors.

The acquisition of diverse systems from different manufacturers may result in circuit board design differences as a direct consequence. Additionally, differences in chipsets associated with each microprocessor also diversify the board components and may influence design difference as well. As a result, it may not be necessary to intentionally specify circuit board differences. Nevertheless, it is prudent to identify differences to the degree that such information is available for the platform. While simple parts that are common can be treated through source determination and qualification, complex components need to be considered to fully address CCF vulnerability associated with the logic processing equipment.

It is possible to justify the use of alternate means to address concerns about potential CCF vulnerabilities arising from common circuit boards. Supporting evidence can involve confirmation that the circuit board uses a very simple design, employs parts of high quality, and has been thoroughly tested and qualified. In addition, control of external influences can also be used to demonstrate that measures are provided to ensure that common stress factors (e.g., power quality, environmental conditions) are not applied concurrently to each system.

The use of different data-flow architectures (i.e., bus architectures) is similar to consideration of different component integration architectures. However, management of data flow throughout the system and the topologies for bus structures are generally well established and these architectures have been standardized in many instances. Use of diverse bus architectures seems unnecessary. No specific information was provided on bus architectures for the diversity examples cited in this research.

Each example cited in the Strategy C discussion of survey findings employed intentional use of different microprocessors. There was one example (A340) in which the different microprocessors were from different generations of the same family from the same manufacturer. The investigation of nonnuclear industries did not reveal any specific information on the use of different circuit boards. In the NPP examples, it was reported that Darlington used different circuit board layouts for SDS1 and SDS2. As stated above, little use of different bus architectures was reported.

<u>Functional Diversity</u>. The notable similarity in the functional capabilities and processing mechanisms provided by microprocessors (i.e., architectural variations of digital technology) does little to promote differences in system specifications and implementation conventions (e.g., coding practices, testing approaches, installation procedures). As a result, the potential for common misinterpretation or mistakes in the translation of requirements (what function is needed) to design specifications (how the function is to be achieved) is significant. Additionally, the modest differences provided by this technology variation do not contribute much to reducing the prospect for common human mistakes in the design and implementation processes. The personnel (e.g., designers, developers, testers, installers) engaged in various life-cycle activities for either system are likely to develop common cognitive models of the system specification and the way the functional requirements can be implemented and validated. This commonality can be further attributed to similar development tools, common system integration

techniques, and comparable skill sets (or technical expertise). These conditions increase the importance of functional diversity for this strategy as a means of addressing common systematic faults.

As discussed above, the intentional use of functional diversity, in combination with signal diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research. The relevant diversity criterion involves different purpose, function, control logic, or actuation means. Basically, different functional expressions capture the diverse safety function initiation criteria, with the result being differences in the functions and control logic assigned to each diverse system. As discussed above, inherent functional diversity is also achieved due to the differences in the nature of the technologies, which leads to diversification of the underlying mechanisms for processing functions.

Findings from the investigation of diversity practices at international NPPs confirm the prevalence of this diversity approach as an intentional diversity. Functional diversity and signal diversity were applied in combination in each example cited in the Strategy C discussion of survey findings. In the examples from nonnuclear industries, functional diversity is recommended for the chemical industry in the form of different functional relationships to initiate a safety response. Additionally, the flight control systems for the Airbus aircraft utilize functional diversity in the form of a reduced-functionality alternate system for automatic flight control. The reduced functionality corresponds to a minimal set of control laws (similar to the reduced coverage of nuclear plant PIEs through ATWS or DAS).

Life-Cycle Diversity. As stated in the discussion above on functional diversity, the selection of architectural variations within a particular technology (e.g., different microprocessors) as the design diversity has little impact on the prospect for common human mistakes in the design and implementation processes. As a result, the intentional use of functional diversity is also employed to provide diversification of the functional requirements and functions to be implemented. The result is that the designers, developers, implementers, testers, and installers achieve some degree of cognitive diversification. Additionally, the different functionality promotes some variation in the system designs and software instantiation of the safety functions.

As previously described, the use of different design organizations generally provides across-the-board life-cycle diversity to minimize the potential for common systematic faults to be introduced by human contributors. This diversity is generally achieved by default through the use of different design organizations. If a common manufacturer (or system supplier) is selected, comparable life-cycle diversity can be achieved through the use of separate teams for each system. Most of the examples identified in the survey of diversity usages involved the intentional application of life-cycle diversity either through separate teams within an organization or, more commonly, at different companies.

Logic (Software) Diversity. The design diversity based on use of different microprocessors does provide some impact on software diversity. As noted above, differences in microarchitecture cause some difference in the fundamental execution of software instructions. A similar effect is present for operating systems, application program interfaces, and runtime environments, especially given differences in on-chip resources (e.g., multicore processors, system on a chip) or associated chipsets for management and access of onboard resources. Each of these differences provides some diversification of the transition mechanisms between internal states, resulting in some difference in the execution of software-based functions.

Differences in microarchitecture also led to some diversity in the methods for translating application software into machine code. Thus, the compilers, interpreters, and assemblers provide some diversity in the back-end translation to account for differences in the machine-level representation of the software as opcodes and operands that are machine specific. There is some value in using different compilers to diversify the generation of executable code and minimize the potential for common errors in the translation process.

The differences noted above provide some diversification in the machine-language representation of the software for the diverse systems and the runtime support provided by the platform. Coupling the dissimilarity in native language representation and runtime environment with the difference in hardware mechanisms for performing the basic operations and the resource management involved in executing each safety function results in diversification of the execution profiles at a fundamental level. Thus, it is unlikely that logic processor flaws or system software faults for diverse microprocessor-based platforms would result in concurrent failure of the diverse systems. The conclusion is that intentional application of diverse runtime environments and diverse code generation (i.e., compilers, assemblers), in conjunction with diverse microprocessors, can minimize the prospect of common platform-specific systematic faults while reducing the potential for concurrent execution profiles.

The diversity achieved through the combination of different microprocessors, runtime environments, and software compilers (which provides a form of different functional representation or, essentially, computer language) relates to the coupling of software and hardware into an integrated computational machine and does not address the prospect of software design or coding errors, which constitute systematic faults at the application level.

Sources of potential CCF vulnerabilities at the application level are more directly related to mistakes or misunderstandings in the design of the system and its application software or to errors in implementation of the software design (e.g., programming, V&V). Although flaws in design and programming tools have the potential to introduce systematic faults, a greater source of potential CCF vulnerabilities arises from the human developers themselves. As described above, life-cycle and functional diversity each contribute to establishing cognitive diversity between the different development teams for each diverse system. Intentional software diversity can also contribute to this diversification and reduce the prospects for common systematic faults in design and implementation.

The use of functional diversity, as previously described, corresponds to the intentional use of different algorithms and logic. As a result of these differences in functional relationships, the software designs will be different in terms of the number and types of computational operations, the sequence in which those operations are arranged, the data sets to be manipulated, and so forth. The program architectures for the diverse systems will consequently show some differences as well. In addition to affecting the prospect for introduction of common design and implementation faults, this software diversity also contributes to diversifying the execution of the software in the diverse systems. Thus, the prospect of concurrent execution profiles can be minimized and the potential for CCF vulnerability triggered by a common signal trajectory (i.e., common internal states and inputs) can be reduced.

In contrast to the representation diversity achieved through the use of different compilers to translate software into machine code, the use of different programming languages can affect the cognitive diversity of the different programmers assigned to each diverse system. This is particularly true for language choices that require substantially different programming paradigms. The use of a high-level language (e.g., ADA, Pascal, PL/M) for one implementation and a low-level language (e.g., assembler) for another was seen in several examples identified in the diversity usage survey. Airbus, Temelin, and Darlington provide specific examples. The guidance for the chemical industry, the common positions of European regulators, and several IEC standards[122,124] identify different languages as a recommended means of contributing to the mitigation of potential CCF vulnerabilities. NUREG/CR-6303 also identified different computer languages as a criterion under the software diversity attribute. However, it notes that high-level languages are converging and may be intermixed. Therefore, the effectiveness of this criterion may be limited depending on the language choices. Thus, careful consideration should be given to the type of languages selected and the associated programming conventions. It should be noted that NUREG/CR-6463, *Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems*,[130] provides guidance on safety characteristics and acceptable programming conventions for ten high-level languages.

The Boeing example provides a striking case in which measures other than different computer languages were taken to address the potential for human-induced systematic faults. For the B777, formal methods were employed to reduce the prospect of mistakes in formulating the software design specification. The reliance on extensive software quality assurance processes is also common in other nonnuclear industries (e.g., aerospace, defense). Additionally, the use of significant functional diversity (e.g., requirements associated with different-purpose functions, such as active control or performance checking) may also provide sufficient diversity to provide a comparable effect on the potential for common systematic faults in design. The bottom line is that compensatory approaches that can provide effective alternatives to the use of different computer languages have been demonstrated in other application domains and may be considered in assessing the need for this diversity criterion.

Regarding other criteria under this diversity attribute, most examples that were cited from the nuclear power and nonnuclear industries used logic diversity in the form of different algorithms, logic, or program architectures. The primary use of that criterion related to functional diversity based on reduced functionality backups or different functional relationships for initiation criteria. The use of different compilers, which is treated here as a programming language (or functional representation) diversity criterion, was employed in several cases. Boeing used different compilers associated with each of the three diverse microprocessors within the B777 flight control system. Airbus used different software development tools (e.g., compilers, code generators) for each diverse computer/software language combination. Additionally, Darlington employed different compilers and software languages for its diverse shutdown systems. Of particular significance in considering the value of using diverse compilers is the Boeing experience. Comparing the processing of the same source code with three different compilers (i.e., a separate compiler corresponding to each microprocessor in the three diverse lanes), Boeing found ten compiler errors.[53] Although there were no common errors detected, the experience highlights the potential significance of compilers/assemblers and illustrates the prospect for embedded faults from common tools leading to common systematic faults within system implementations.

The other logic diversity criteria involve different timing or order of execution and different runtime environment. No examples were found in which the former criterion was identified as an intentional or inherent diversity. The use of timing differences or execution order to achieve some level of diversification in signal trajectory would seem to be most appropriate in cases where there is no program architecture or algorithm diversity related to functional diversity (i.e., the software is the same or would be without order shifts). Since the combination of functional and signal diversity provide different signal trajectories (along with the differences in internal states provided by the design diversity that is characteristic of this strategy grouping), the use of this diversity criterion does not appear to be necessary.

The impact of the latter criterion on runtime environments is discussed above. No specific information was identified regarding operating systems in the examples cited in the survey. However, the diversity of microprocessors indicated that some inherent, if not intentional, diversity was achieved in many of the cases. Additionally, the guidelines for the chemical industry specifically identify system software as a potential source of CCF vulnerability. Also, system services are identified as a candidate for diversification in information on CCF mitigation provided by IEC 60880.[124] It is noted that NUREG/CR-6303 gives examples in which the operating system was omitted from D3 analyses on the basis of its simplicity. Obviously, this approach is appropriate where the claim is justified.

<u>Signal Diversity</u>. The selection of architectural variations within a technology as the basis for parallel diverse systems, redundancies, or subsystems has no direct impact on signal diversity. As discussed above, the intentional use of signal diversity, in combination with functional diversity, is adopted as part of the baseline for all of the strategy classifications developed through this research.

This usage is consistent with the examples identified from the nuclear power industry survey. For the examples drawn from Chooz, Temelin, and the other plants, the ATWS system or diverse (secondary)

actuation system primarily addresses backup action for a reduced set of high-frequency PIEs, which leads to a reduced set of inputs compared with the primary protection system.

6.3.3.3 Description of Strategy C

6.3.3.3.1 Design Diversity

Intentional diversity is provided through the selection of different architectures within a technology. Specifically, the use of diverse microprocessors as the basis for different systems, redundancies, or subsystems constitutes the primary example of strategies in this classification. The purpose of this diversity usage is to address the potential CCF vulnerabilities arising from common systematic faults at the platform level (i.e., the base processing components and the interface of application software to the processing capabilities provided by the platform) and from concurrent execution profiles (i.e., internal states and state-transition mechanisms).

Equipment (Manufacturer) Diversity. Intentional diversity is provided through the selection of different manufacturers (or system suppliers) for different equipment designs. The purpose of this diversity usage is to minimize the potential for common systematic faults arising from manufacturing defects or implementation errors.

Alternate diversity strategies within the Strategy C classification may adopt the intentional selection of the same manufacturer of different designs as a variation of the baseline combination of diversity criteria. Use of the alternate equipment manufacturer criterion is linked to the compensatory intentional application of life-cycle (human) diversity.

Equipment (Processing) Diversity. Intentional diversity is provided through the selection of different logic processing equipment. This diversity is closely tied to the selection of design diversity that is characteristic of the Strategy C classification. Basically, the primary architecture difference is provided through the selection of diverse microprocessors. The purpose of this diversity usage is to minimize common components while minimizing the potential for CCF vulnerabilities arising from common systematic faults at the platform level and from concurrent execution profiles.

The review of diversity usage cases from the nonnuclear (e.g., aviation) industry, as well as for international NPPs, establishes examples of diverse CPUs. These examples of accepted microprocessor diversity include Intel 80186 vs Motorola M68010, AMD 29050 vs Motorola 68040 vs Intel 80486, and Intel 80386 vs Intel 80186.

The third example of diverse microprocessors, which was used in the flight control systems of the A340, represents the only cited case where microprocessors from the same manufacturer were specified as diverse. While this example employs different generations of the same family, the CPUs are not from successive generations. Caution is warranted if the microprocessor difference is limited to different generations from the same manufacturer to ensure that significant differences in microarchitecture are present. The alternate use of different logic processing versions using the same architecture as the base logic processing equipment diversity criterion should be justified by evidence of structural differences (e.g., what microarchitectural changes were implemented), flaw diversification (based on the errata sheets), and/or chipset differences.

Intentional use of component integration architecture (i.e., circuit board design) diversity criterion can contribute to minimizing the potential for common systematic faults at the platform level (e.g., component defects, integration deficiencies, or board design errors) as well as common susceptibility to external influences such as environmental stress (e.g., temperature/humidity and radiated electromagnetic interference) or aging (e.g., metallic whiskers and electromigration). However, these benefits may be achieved through alternate means such as simplification of board design, thorough qualification and testing, and control of external influences. Therefore, this diversity criterion may be treated as optional

based on considerations such as the complexity of the platform designs, minimal use of common components, and limited commonality of stress factors. If the decision to omit intentional application of this logic processing equipment criterion is justified, coupling that strategy variation with the use of different equipment manufacturers can provide added (potentially compensatory) assurance that the potential for common board design errors or component defects is minimized.

Functional Diversity. Intentional diversity is provided in the form of different functions or control logic associated with coverage of a reduced set of PIEs (as needed based on the D3 analysis for the plant) and the use of diverse safety function initiation criteria (cf., GDC 22 and signal diversity). The purpose of this diversity usage is to provide differences in functional requirements and design specification as well as to diversify the signal trajectories seen by each system.

Life-Cycle Diversity. Intentional diversity is provided through the use of different design organizations to conduct life-cycle activities related to the application-specific system development. This baseline criterion is linked to the intentional selection of the equipment manufacturer diversity criterion for different manufacturers of the same (or similar) design. The purpose of this life-cycle diversity usage is to avoid the introduction of systematic faults during design and implementation of the diverse systems due to common mistakes or misunderstandings by shared human resources.

Alternate diversity strategies within the Strategy C classification may adopt the intentional selection of separate teams when the same manufacturer is used to supply the diverse systems. In particular, this alternate strategic approach involves the manufacturer intentionally establishing, to the extent practical, the following teams for each system: different management teams; different design and development teams; and different implementation, validation, and installation teams.

Logic (Software) Diversity. Intentional diversity is provided in the form of different algorithms, logic, and program architectures. This diversity is associated with the intentional use of functional diversity. Additionally, intentional diversity is also provided through use of different operating systems, different compilers, and different computer languages. The specific diversity criteria are different runtime environments (i.e., operating systems) and different functional representations (i.e., compilers and computer languages). The purpose of this diversity usage is twofold. First, use of different operating systems and different compilers can contribute to avoiding potential CCF vulnerabilities arising from common systematic faults at the platform level (i.e., the interface of application software to the processing capabilities provided by the platform) and from concurrent execution profiles (i.e., internal states and state transitions). Second, use of different computer languages can help to avoid the introduction of systematic faults due to common mistakes or misunderstandings in the design process or common errors in the implementation process.

Alternate diversity strategies within the Strategy C classification may arise if it can be established that the simplicity of the operating system minimizes the contribution of the runtime environments to the potential for CCF vulnerability.

Signal Diversity. Intentional diversity is provided through the use of separate and/or diverse measurements of plant parameters. The purpose of this intentional diversity usage involves minimization of commonalities, support of functional diversity (cf., GDC 22), and diversification of concurrent execution profiles. Each of the three signal diversity criteria is appropriate for application as intentional diversities to the extent practical.

6.3.3.4 Strategy C Summary

Strategies that involve the use of architectural variations within a technology as the basis for diverse systems, redundancies, or subsystems are classified as examples of Strategy C. The combinations of diversity criteria that characterize Strategy C, in conjunction with traditional diversity strategies for hardwired systems, provide adequate mitigation of potential CCF vulnerabilities. In particular,

implementation of the Strategy C diversity grouping serves to minimize the opportunities for common systematic faults, concurrent execution profiles, or similar responses to external influences. 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.
Table 6.3 provides a summary of the baseline example of Strategy C, along with four variants. Strategy C1 represents the baseline grouping of diversity criteria. Strategy C2 corresponds to the alternative where the same manufacturer provides the diverse equipment while separate teams within the organization are specified for the diverse systems. Strategy C3 arises when the diverse microprocessors are based on suitably different generations within a manufacturer's microprocessor family. Strategy C4 corresponds to the alternative in which circuit board diversity can be shown to be unnecessary. Strategy C5 involves the determination that a common operating system is sufficiently simple that it does not credibly contribute potential CCF vulnerabilities. F igure 6.3 illustrates the baseline combination of diversity criteria.

Table 6.3. Overview of diversities comprising Strategy C

Diversity attribute	Strategy[a]				
	C1	C2	C3	C4	C5
Design					
Different architectures	x	x	x	x	x
Equipment (Manufacturer)					
Different manufacturer—same design	x	–	x	x	x
Same manufacturer—different version	–	x	–	–	–
Equipment (Processing)					
Different logic processing architecture	x	x	–	x	x
Different logic processing versions in same architecture	–	–	x	–	–
Different component integration architecture	x	x	x	–	x
Functional					
Different purpose, function, control, logic, or actuation means	x	x	x	x	x
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	x	i	i	i
Different implementation/validation teams (testers, installers, or certification personnel)	i	x	i	i	i
Logic (Software)					
Different algorithms, logic, and program architecture	x	x	x	x	x
Different runtime environment	x	x	x	x	–
Different functional representation	x	x	x	x	x
Signal					
Different parameters sensed by different physical effects	x	x	x	x	x
Different parameters sensed by same physical effects	x	x	x	x	x
Same parameter sensed by a different redundant set of similar sensors	x	x	x	x	x

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

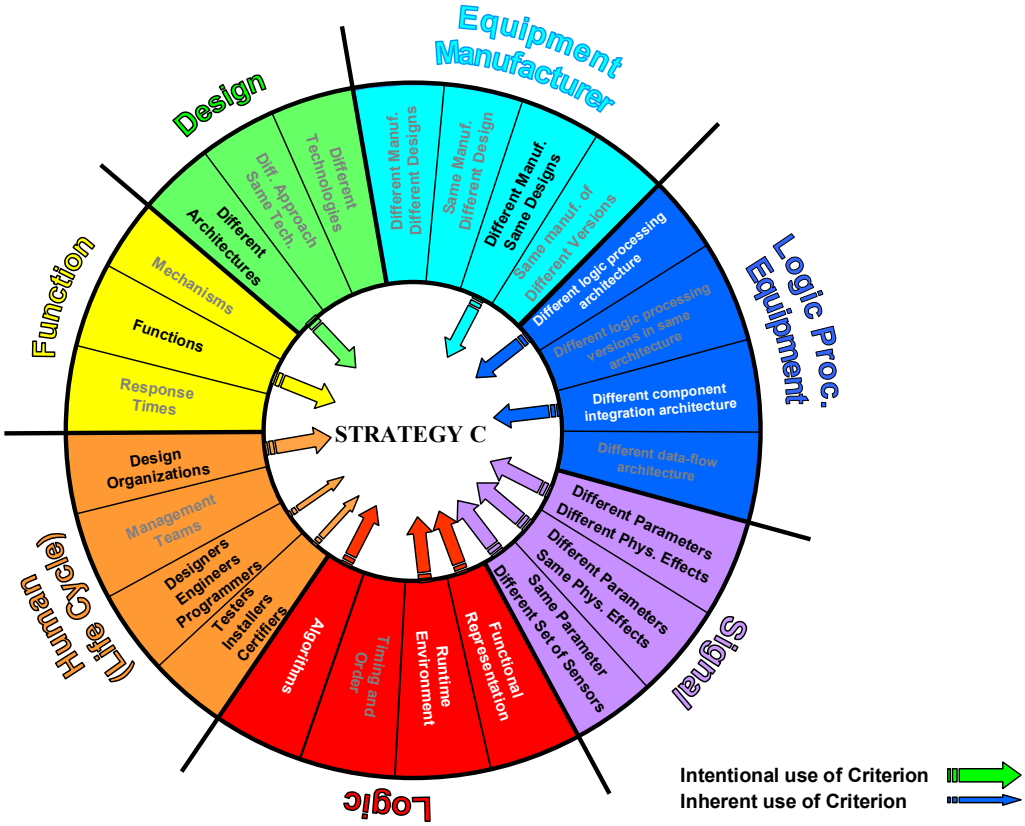

Figure 6.3. Baseline diversity strategies: ORNL Strategy C.

6.4 Application of Diversity Strategies

6.4.1 Strategy Development Summary

The diversity strategies presented in this chapter represent baseline approaches to providing adequate mitigation of potential CCF vulnerabilities. The strategies and their variants are composed of combinations of diversity criteria, which are adapted from the attributes and criteria defined in NUREG/CR-6303. These strategies are based on best practices derived from examples of diversity usage by the international nuclear power industry and several nonnuclear industries. The strategies established through this research accommodate factors such as the effect of technology choices, the nature of CCF vulnerabilities, and the prospective impact of each diversity type.

The context of these diversity strategies arises from a focus on addressing CCF vulnerabilities that can inhibit the timely performance of a safety function by a safety system (effectively disabling redundancies within the system). The results of a D3 analysis establish the need for diversity by determining where diversity is needed to satisfy safety regulations. Based on these results, diversity is typically applied to mitigate the unacceptable consequences associated with the identified CCF vulnerabilities. The assumption for the use of the diversity strategies developed through this research is that they would either be applied to add diversity to the affected safety system(s) or to provide an automatic diverse actuation system. In the former case, the diversities relate to differences between redundancies, subsystems, modules, and components within a safety system. In the latter case, the diversities relate to differences between the affected safety system and a parallel diverse system that accomplishes either the same function or a compensating function providing adequate protection.

The technical basis for the strategies developed through this research, as described in this chapter, can be summarized as follows. First, several considerations regarding the usage of diversity are described. In particular, the impact and benefits of diversity are identified in terms of common fault sources (purpose and process), location of vulnerabilities (product), and common triggering conditions (performance). Effectively, these contributions of the diversity criteria for coping with CCF vulnerabilities are characterized in terms of their capability to effect common systematic faults, concurrent execution profiles, or similar responses to external influences.

Additionally, the starting point for diversity strategies in the nuclear power application domain is established. Specifically, traditional approaches to diversity usage within I&C systems at NPPs are captured as baseline practices to be adopted in each diversity strategy. These diversity approaches were developed by the nuclear power industry prior to concerns about CCF vulnerabilities associated with digital technology, and they have served to ensure that conventional analog systems addressed system-level CCF vulnerabilities. The primary focus of these traditional diversity approaches relates to commonalities and design-basis uncertainties. The diversity strategies developed through this research build on those approaches by adding coping measures to address the unique characteristics associated with digital technology.

As additional considerations for the development of baseline strategies, some fundamental technology-independent relationships among key diversity attributes are also described. The nature of these relationships involves complementary characteristics and cross-dependence. The first consideration is illustrated by the traditional use of functional and signal diversity to provide diverse input/output relationships and initiation criteria corresponding to a PIE. The second consideration involves dependencies such as the almost-default provision of personnel diversity that arises from the selection of different companies to serve as manufacturers or suppliers for diverse systems.

Next, the diversity strategy classification scheme is presented. The grouping of diversity combinations was established to facilitate a systematic organization of strategies into families that are readily amenable to review. The classification of strategies enables a consistent representation of the comparative use of diversity between systems, redundancies, subsystems, modules, or components. The technology employed was chosen as the basis for the strategy classifications, given that this fundamental difference between systems provides an identifiable, easily recognizable diversity characteristic of system design. Additionally, the design diversity attribute that arises from the use of technology differences generally has a significant, consequential impact on other diversity attributes.

The diversity usage considerations and the findings of the survey of nonnuclear industries and international NPPs are tied together in the context of the diversity classification scheme to document the basis for baseline diversity strategies. The discussion of rationale for each strategy classification provides clear ties to best practices through cited examples from the nuclear and nonnuclear industries and addresses the prospective impact of the diversity criteria on fault sources, vulnerability sites, and triggering mechanisms for CCF. Additionally, the identification of inherent diversity characteristics that arise from technology usage acknowledges the nature of diverse technologies and indicates areas in which credit can be given for intrinsically providing some coping capability for potential CCF vulnerabilities.

Each strategy classification presented in this chapter provides a baseline combination of diversity criteria that in conjunction with traditional diversity usage for hardwired systems provides adequate mitigation of potential CCF vulnerabilities. In particular, implementation between diverse systems of the combination of diversity criteria that constitutes one of the three baseline strategies provides adequate diversity to mitigate potential CCF vulnerabilities that have been identified through a D3 analysis as being unacceptable. Alternatively, adherence to one of the diversity strategy variants that are identified in the discussion of each classification can also provide sufficient coping capabilities, where specified conditions are satisfied. Table 6.4 provides a comparative summary of the baseline diversity strategies

for the three classifications. Figures 6.1, 6.2, and 6.3 illustrate the baseline combination of diversity criteria for Strategy A, Strategy B, and Strategy C, respectively.

Table 6.4. Overview of baseline diversity strategies

Diversity attribute	Strategy[a]		
	A	B	C
Design			
Different technologies	x	–	–
Different approach—same technology	–	x	–
Different architectures	i	–	x
Equipment (Manufacturer)			
Different manufacturer—different design	x	x	–
Same manufacturer—different design	–	–	–
Different manufacturer—same design	–	–	x
Same manufacturer—different version	–	–	–
Equipment (Processing)			
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 (Software)			
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 (–).

6.4.2 Strategy Evaluation Approach

A systematic evaluation process can be established to review the application of the diversity strategies developed through this research. For usage that adopts a baseline strategy, the process is a straightforward confirmation of conformance to the combination of diversity criteria. On the other hand, application of an alternate means for mitigating potential CCF vulnerabilities leads to a more complex

evaluation approach to ascertain that the proposed alternate method provides sufficient coping capability with reasonable assurance. The conclusions drawn from an evaluation of diversity usage support the determination of whether safety regulations and regulatory requirements are satisfied. In particular, application of the traditional diversity usage, explicitly addressed in these strategies through the inclusion of functional and signal diversities in the baseline combination of diversity criteria, addresses the design criteria embodied in the GDC of 10 CFR 50, Appendix A (in particular, GDC 22), and fulfills the requirements of 10 CFR 50.62 and 10 CFR 50.55a(h). The application of the full set of diversity criteria specified in any of the strategy baselines to ensure a diverse means to accomplish the same or different function is an integral element of providing reasonable assurance that Point 3 of the Commission's positions on D3 is satisfied.[6]

The evaluation process associated with the diversity strategies developed under this research consists of multiple steps. The review method addresses various aspects of diversity usage related to identification of the diversities claimed, confirmation of adherence to a specified combination of diversity criteria, determination of the impact of any deviations, and/or assessment of the suitability of an alternate strategy. The steps of the evaluation process are as follows:

Classify the diversity strategy—This step involves recognition of the technology employed in the diverse systems based on the design descriptions or, if explicitly referenced, identification of the specific diversity strategy selected.

Confirm inherent diversity credit—This step relates to the determination of technology usage and the impact of technology difference. The importance of this step arises from the prospect that some intrinsic benefits derived from technology differences can be compromised based on factors such as the design concepts adopted or the degree of commonality feasible. Examples of these factors include the use of one technology (or technology approach) to emulate another (e.g., use of an FPGA to emulate a CPU) and commonalities in platform heritage (e.g., mixed-mode electronics using common parts, boards, and/or design methods, as well as common personnel involved in one or more phases of each platform's life-cycle). If the documentation of the proposed diversity strategy does not provide a discussion of the nature of the technology difference (e.g., digitized vs continuous data, sequential vs parallel execution of function, software logic vs hardwired logic), the design concepts employed, and any commonalities (e.g., parts or components, interfaces, processing mechanisms, heritage), then a more detailed review of (or inquiries about) the designs may be warranted.

Identify intentional diversity usage—This step consists of identification of the diversity criteria that are intentionally applied. The documentation of the proposed diversity strategy should explicitly describe the intentional diversities on which it is based.

Categorize diversity usage in relation to the corresponding strategy classification—This step involves capture of the combination of diversity criteria in either tabular form (see Tables 6.1 through 6.4) or a spreadsheet (see Appendix A) followed by classification in terms of a corresponding strategy and subsequent determination of the degree of adherence to one of the strategies established through this research. The categorization options are (1) baseline strategy (either A, B, or C), (2) variant of baseline strategy (i.e., A2, B2, B3, C2–C5), or (3) alternate strategy. The determination of which strategy classification applies is based on the compiled diversity usage or, if provided, an explicit claim in the diversity strategy documentation.

Assess the adequacy of the diversity strategy—The activity associated with this step depends on the categorization of the proposed diversity strategy determined in Step 4.

Baseline strategy. This category consists of proposed diversity usage that appears consistent with one of the baseline combinations of diversity criteria defined for any of the three strategy classifications. The associated actions are to confirm that the diverse systems provide the specified technology difference

(Step 1), the system designs do not compromise the related credit for inherent diversity (Step 2), and the explicit diversity usage employs the full set of intentional diversities (Step 3).

Variant of baseline strategy. This category involves proposed diversity usage that appears consistent with one of the alternate combinations of diversity criteria described for any of the three strategy classifications. The associated actions are to perform a assessment comparable to that described for the baseline strategy category (Step 5a) with the supplemental determination of whether the conditions associated with suitability of the variant are present (e.g., confirm that an Appendix B supplier is used when the same manufacturer is selected for the diverse systems or evaluate the justification that a common operating system or runtime executive is sufficiently simple to acceptably minimize the potential for CCF vulnerabilities from that platform element).

Alternate strategy. This category concerns proposed alternate means for addressing potential CCF vulnerabilities. Essentially, proposed strategies of this type do not fully correspond to any of the diversity strategies established through this research. The associated actions begin with a determination of the type and extent of deviations from the most closely related baseline strategy. If the deviations are not substantial, then the assessment can proceed similarly to the prior approaches (Step 5a or 5b) with an additional review of the technical justification for the deviations. If the deviations are numerous and substantial in nature or the proposed diversity strategy does not conform to any of the strategy classifications, then a detailed assessment of the technical basis for the proposed mitigation approach is warranted.

The review approach in this category can proceed based on some combination of technical review and comparative assessment. A diversity assessment tool is described in Appendix A. This tool was independently developed and was used to confirm the adequacy of the three strategy classifications established through this research. The diversity assessment tool can also be employed for comparative analysis to assess the relative standing of a proposed alternate diversity strategy against the baseline strategies as well as best practices and common usage of the nuclear power and nonnuclear industries, as reflected in the survey findings on diversity usage. This tool provides a systematic approach to evaluate proposed combinations of diversity criteria.

Regardless of the review approach chosen, there are two important considerations that should be addressed in the review. First, the assessment should consider whether the alternate combination of diversities provides an equivalent effect on capability to mitigate the CCF vulnerabilities of concern. Essentially, the impact of the alternate approach on fault sources, vulnerability sites, and triggering mechanisms for CCF should be comparable to an accepted strategy. Second, the assessment should address the rationale that constitutes the basis for each diversity criterion applied (e.g., see Section 6.3).

Conclude whether the diversity strategy is adequate—An affirmative conclusion that the diversity strategy adequately resolves the diversity needs identified in the D3 analysis can be based on either (1) confirmation that the strategy conforms to a baseline strategy (or a cited variant with the accompanying qualifying conditions) or (2) determination that the strategy is an acceptable alternate approach providing reasonable assurance of sufficient mitigation for potential CCF vulnerabilities.

7. CONCLUSIONS

Although the potential for CCF vulnerability in I&C systems has long been recognized, the increasing use of highly complex digital technologies in modern I&C system designs poses additional concern that common systematic faults may persist undetected in spite of rigorous, high-quality life-cycle processes. The use of diversity as a mitigating strategy to resolve CCF concerns supplements the quality assurance practices employed to satisfy safety requirements. In particular, diversity usage is cited in the design criteria for NPP safety systems as well as being required by regulation for NPPs. Traditional diversity strategies have been commonly employed for hardwired safety systems, with an emphasis on addressing commonalities and design-basis uncertainties. However, consideration of additional diversity usage is warranted to accommodate the unique characteristics of digital technology. The diversity strategies developed through this research build on the more traditional diversity approaches by adding coping measures to address potential CCF vulnerabilities associated with digital technology.

The research basis for establishing diversity strategies involved investigation of available documentation on D3 methods and experience from nuclear power and other industries, capture of expert knowledge and lessons learned, determination of best practices, and assessment of the nature of CCFs and compensating diversity attributes. The resulting diversity strategies represent baseline approaches for providing adequate mitigation of potential CCF vulnerabilities. The strategies and their variants are composed of combinations of diversity criteria, which are adapted from the attributes and criteria defined in NUREG/CR-6303. The basis for these strategies centers on best 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 strategies established through this research address considerations such as the effect of technology choices, the nature of CCF vulnerabilities, and the prospective impact of each diversity type.

This research establishes a framework for classifying strategic approaches to diversity usage. 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.

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 (Laddic logic) 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 employ a significantly different architectural approach through which to implement strategic use of this technology difference.

- **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 profile, and similar responses to external influences that can contribute to the potential for CCF vulnerabilities in digital I&C systems.

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. For usage that adopts a baseline strategy, the process is a straightforward confirmation of conformance to the associated combination of diversity criteria. Conversely, application of an alternate means for mitigating potential CCF vulnerabilities leads to a more complex evaluation approach to ascertain that the proposed alternate method provides sufficient coping capability with reasonable assurance. The conclusions drawn from an evaluation of diversity usage support the determination of whether adequate CCF mitigation is provided and regulatory requirements are satisfied. The evaluation process associated with the diversity strategies consists of multiple steps. The methodology addresses various aspects of diversity usage related to identification of the diversities claimed, confirmation of adherence to a specified combination of diversity criteria, determination of the impact of any deviations, and/or assessment of the suitability of an alternate strategy. 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 (see Section 6.4.2.for a more detailed discussion of the process):

- Classify the diversity strategy—identify what technology is employed.
- Confirm inherent diversity credit—ensure that intrinsic benefits of technology differences are not compromised.
- Identify use of intentional diversities explicitly employed to address CCF.

- 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.

    Diversity usage tables and the diversity assessment tool (described in Appendix A) were developed to aid in the evaluation of proposed diversity strategies. The diversity assessment tool can also be employed for comparative analyses to assess the relative standing of a proposed alternate diversity strategy against the baseline strategies as well as best practices and common usage of the nuclear power and nonnuclear industries. This tool provides a systematic approach to evaluate proposed combinations of diversity criteria.

    While reviewing a proposed alternate strategy, it should be noted that there are two important questions to consider in this step of the evaluation process:

    1. Does the combination of diversities provide an equivalent effect on mitigating the CCF vulnerabilities of concern?
    2. Is the rationale for the applied diversities provided in the strategy, and is it supportive?
- Determine if the diversity strategy is adequate. A conclusion that a proposed diversity strategy adequately addresses CCF mitigation needs, as identified by 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 prospects for common systematic faults, reducing the occurrence of concurrent execution profiles, and lessening the likelihood of similar responses to external influences.

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.

Finally, the diversity usage investigation showed that the international nuclear power community has focused significant attention on the means for avoidance and mitigation of digital CCF. In particular, IEC 60340 provides specific guidance on the topic. This international consensus standard warrants consideration as a base guidance document on which to establish more general guidance on methods for addressing CCF. However, the findings of this research on acceptable diversity strategies should be addressed to enhance the guidance provided by the standard.

This page is intentionally left blank.

Draft

8. REFERENCES

1. Institute of Electrical and Electronics Engineers, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std 603-1991, Piscataway, New Jersey, 1991.
2. Institute of Electrical and Electronics Engineers, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," IEEE Std. 379-2000, Piscataway, New Jersey, 2000.
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, "Digital Computer Systems for Advanced Light-Water Reactors," SECY 91-292, Washington, DC, September 26, 1991.
5. U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," SECY-93-087, Washington, DC, April 2, 1993 (ADAMS Accession No. ML003708021).
6. U.S. Nuclear Regulatory Commission, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Staff Requirements Memorandum on SECY-93-087, Washington, DC, July 21, 1993 (ADAMS Accession No. ML003708056).
7. U.S. Nuclear Regulatory Commission, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, December 1994.
8. 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.
9. 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 (ADAMS Accession No. ML070550072).
10. International Atomic Energy Agency, "Radiation Aspects of Design for Nuclear Power Plants," IAEA S-G-1.3, Vienna, Austria, 2005.
11. International Electrotechnical Commission, "Instrumentation and Control Systems Important to Safety—Requirements to Cope with Common Cause Failure (CCF)," IEC 62340, Geneva, Switzerland, 2008.
12. 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.
13. Y. Huang, C. Kintala, N. Kolettis, and N. D. Fulton, "Software Rejuvenation: Analysis, Module and Applications," *Twenty-Fifth International Symposium on Fault-Tolerant Computing (FTCS-25)*, Pasadena, California, June 1995, p. 381.
14. V. Castelli et al., "Proactive management of software aging," *IBM Journal of Research and Development*, **45**(2), March 2001.
15. K. J. Cassidy, K. C. Gross, and A. Malekpour, "Advanced pattern recognition for detection of complex software aging phenomena in online transaction processing servers," *Proc. of Int'l Conf. on Dependable Systems and Networks (DSN 2002)*, June 2002.

Draft

16. A. Avritzer and E. J. Weyuker, "Monitoring Smoothly Degrading Systems for Increased Dependability," *Empirical Software Engineering*, **2**(1), March 1997.

17. M. Grottke et al., "Analysis of Software Aging in a Web Server," *IEEE Transactions on Reliability*, 55(3), September 2006.

18. A. Lindner, "CCF due to Software—A Contribution to the Actual Discussion," International Atomic Energy Agency Technical Meeting on Avoiding Common-Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, Bethesda, Maryland, June 2007.

19. International Atomic Energy Agency, *IAEA Safety Glossary*, Ed. 2.0, Vienna, Austria, 2006.

20. International Atomic Energy Agency, *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook*, IAEA Technical Report Series No. 387, 1999.

21. Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations," IEEE Std. 279-1971, Piscataway, New Jersey, 1971.

22. Institute of Electrical and Electronics Engineers, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std. 7-4.3.2-2003, Piscataway, New Jersey, 2003.

23. U.S. Nuclear Regulatory Commission, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Regulatory Guide 1.152, rev.2, Washington, DC, 2006 (ADAMS Accession No. ML053070150).

24. http://www.nasa/gov

25. National Aeronautics and Space Administration*, NASA General Safety Program Requirements*, NPR 8715.3, April 2007.

26. National Aeronautics and Space Administration, *Software Safety Standard*, NASA-STD-8719.13B, Change No. 1, July 2004.

27. National Aeronautics and Space Administration, *Safety Policy and Requirements For Payloads Using the Space Transportation System*, NSTS 1700.7B, Change No. 17, June 2004.

28. National Aeronautics and Space Administration, *Human-Rating Requirements for Space Systems*, NPR 8705.2A, February 2005.

29. National Aeronautics and Space Administration, *NASA Software Safety Guidebook*, NASA-GB-8719.13, March 2004.

30. J. E. Tomayko, *Computers in Spaceflight: The NASA Experience*, NASA CR 182505, March 1988.

31. J. E. Tomayko, *Computers Take Flight: A History of NASA's Pioneering Digital Fly-By-Wire Project*, NASA SP-2000-4224, April 2000.

32. J. F. Hanaway and R. W. Moorehead, *Space Shuttle Avionics System*, NASA SP-504, January 1989.

33. J. E. Tomayko, *Computers Take Flight: A History of NASA's Pioneering Digital Fly-By-Wire Project*, NASA SP-2000-4224, April 2000.

34. J. F. Hanaway and R. W. Moorehead, *Space Shuttle Avionics System*, NASA SP-504, January 1989.

35. P. Ladkin, "Excerpt from the Case Study of the Space Shuttle Primary Control System," http://www.rvs.uni-bielefeld.de/publications/Incidents/DOCS/ComAndRep/Ariane/shuttle.html

Draft

36. National Aeronautics and Space Administration, *International Space Station Familiarization*, NASA TD9702A, Houston Texas, July 1998.

37. P. Robinson et al., "Applying Model-Based Reasoning to the FDIR of the Command & Data Handling Subsystem of the International Space Station," *Proceedings of the 7th International Symposium on Artificial Intelligence, Robotics and Automation in Space* (ISAIRAS03), Detroit, Michigan, May 19–23, 2003.

38. "ISS Status Report: ISS 01-11," May 2001, http://www.astronautix.com/details/iss52449.htm

39. "Ailing Computers Critical to ISS," May 2001, http://www.space.com/news/spacestation/sts100_iss_computers_010501.html

40. http://www.faa.gov

41. Wikipedia, "Air Safety," http://en.wikipedia.org/wiki/Air_safety

42. Radio Technical Commission for Aeronautics, "Software Considerations in Airborne Systems and Equipment Certification," DO-178B, RTCA, Inc., 1992.

43. Society of Automotive Engineers, "Certification Considerations for Highly-Integrated or Complex Aircraft Systems," SAE ARP 4754, SAE International, Warrendale, Pennsylvania, 1996.

44. Radio Technical Commission for Aeronautics, "Design Assurance Guidance for Airborne Electronic Hardware," DO-254, RTCA, Inc., 2000.

45. I. Moir and A. Seabridge, Aircraft Systems: Mechanical, electrical, and avionics subsystems integration, 3rd Edition, John Wiley & Sons, Ltd., 2008.

46. J. Voas, A. Ghosh, F. Charron, and L. Kassab, "Reducing uncertainty about common-mode failures," *Proc. of Eighth International Symposium on Software Reliability Engineering*, Albuquerque, New Mexico, November 2–5, 1997, pp. 308–319.

47. P. Traverse, "Dependability of Digital Computers on Board Airplanes," *Dependable Computing for Critical Applications*, Vol. 4, A. Avizienis and J. C. Laprie, eds., 1991, pp. 134–152.

48. J. E. Tomayko, "Computers Take Flight: A History of NASA's Pioneering Digital Fly-By-Wire Project," NASA SP-2000-4224, Washington, DC, 2000.

49. G. Mauri, "Integrating Safety Analysis Techniques, Supporting Identification of Common Cause Failure," Ph.D. Dissertation, The University of York, September 2000.

50. P. Traverse, I. Lacaze and J. Souyris, "Airbus fly-by-wire: A total approach to dependability," *IFIP World Computer Congress*, Toulouse, France, August 2004.

51. D. Briere and P. Traverse, "AIRBUS A320/A330/A340 Electrical Flight Controls: A Family of Fault-Tolerant Systems," *Digest of Papers FTCS-23: The Twenty-Third International Symposium on Fault-Tolerant Computing*, June 1993, pp. 616–623.

52. D. P. Siewiorek and P. Narasimhan, "Fault-Tolerant Architectures for Space and Avionics Applications," http://ic-www.arc.nasa.gov/projects/ishem/Papers/Siewiorek_Fault_Tol.pdf

53. Health and Safety Commission, "The Use of Computers in Safety-Critical Applications - Final Report of the Study Group on the Safety of Operational Computer Systems," London, UK, November 1998.

54. W. Torres-Pomales, "Software fault tolerance: A tutorial," *NASA Technical Report NASA/TM-2000-210616*, October 2000.

Draft

55. L. Lamport, R. Shostak, and M. Peace, "The Byzantine Generals Problem," *ACM Trans. on Programming Languages and Systems*, Vol. 4, No. 3, July 1982.

56. Y. C. Yeh, "Safety critical avionics for the 777 primary flight controls system," *IEEE Conference on Digital Avionics Systems*, Vol. 1, Daytona Beach, Florida, October 2001, pp. 1–11.

57. Y. C. Yeh, "Dependability of the 777 Primary Flight Control System," *Proc. of the 5th IFIP Int'l Working Conf. on Dependable Computing for Critical Applications (DCCA-5)*, Urbana-Champaign, Illinois, September 1995.

58. Y. C. Yeh, "Triple-Triple Redundant 777 Primary Flight Computer," *Proc. of the 1996 IEEE Aerospace Applications Conference*, Vol. 1, Aspen, Colorado, February, 1996, pp. 293–307.

59. R. W. Pratt, *Flight Control Systems - Practical Issues in Design and Implementation*. Institution of Engineering and Technology, 2000.

60. J. H. Lala and R. E. Harper, "Architectural Principles for Safety-Critical Real-Time Applications," *Proceedings of the IEEE*, **82**(1), January 1994, pp. 25–40.

61. Y. C. Yeh, "Design Considerations in Boeing 777 Fly-By-Wire Computers," *3rd IEEE High-Assurance Systems Engineering Symposium (HASE),* Washington, DC, IEEE Computer Society Press, 1998, pp. 64–73.

62. Americanchemistry, "Industry Profile," http://www.americanchemistry.com/s_acc/sec_statistics.asp?CID=289&DID=744

63. *The Automation Systems and Instrumentation Dictionary*, 4th edition, ISA—The Instrumentation Systems and Automation Society, Research Triangle Park, North Carolina, 2003, p. 433.

64. OSHA, "Process safety management of highly hazardous chemicals," 29 CFR Part 1910.119, Washington, DC (1992).

65. I. Eckerman, *The Bhopal Saga. Causes and consequences of the world's largest industrial disaster*, Universities Press (India) Private Ltd., Hyderabad, 2004.

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

67. Center for Chemical Process Safety, *Guidelines for Safe and Reliable Instrumented Protective Systems*, American Institute of Chemical Engineers, New York, New York, 2007.

68. Instrumentation, Systems and Automation Society, "Application of Safety Instrumented Systems (SIS) for the Process Industry," ANSI/ISA S84.01-1996, Research Triangle Park, North Carolina, 1996.

69. International Electrotechnical Commission, "Functional Safety: Safety Instrumented Systems for the Process Sector," IEC 61511, Geneva, Switzerland, 2003.

70. W. L. Heimerdinger and C. B. Weinstock, *A Conceptual Framework for System Fault Tolerance*, Technical Report CMU/SEI-92-TR-033 (ESC-TR-92-033), October 1992.

71. FRA, "Standards for Processor-Based Signal and Train Control Systems," 49 CFR Part 236, Subpart H, Washington, DC (2005).

72. European Railway Agency, "European Railway Agency Recommendation on the 1st set of Common Safety Methods," ERA-REC-02-2007-SAF, http://www.era.europa.eu/public/core/Safety/Documents/our%20products/cst-csm/ERA-REC-02-2007-SAF.pdf

Draft

73. European Committee for Electrotechnical Standardization, "Railway applications—Communications, signaling and processing systems—Software for railway control and protection systems," EN 50128, Brussels, Netherlands, 2001.

74. International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety-related systems," IEC 60508, Geneva, Switzerland, 1999.

75. A. Hachiga, K. Akita, and Y. Hasegawa, "The Design Concepts and Operational Results of Fault-tolerant Computer Systems for the Shinkansen Train Control," *Twenty-Third International Symposium on Fault-Tolerant Computing (FTCS-23)*, Toulouse, France, June 22–24, 1993, pp. 78–87.

76. G. Hagelin, "Ericsson Safety System for Railway Control," Chapter 2, p. 12, Railway Applications, in *Dependable Computing and Fault-Tolerant Systems Vol. 2 Software Diversity in Computerized Control Systems*, U. Voges (ed.), Springer-Verlag Wien, New York, 1988.

77. U.S. Nuclear Regulatory Commission, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position 7-14, Washington, DC, 2007.

78. R. Frullini and A. Lazzari, "Use of Microprocessor in Rail-Safe on Board Equipment," *Proc. Intern. Conf. on Railway Safety Control and Automation Towards the 21st Century*, London, UK, September 25–27, 1984, pp. 292–299.

79. A. M. Amendola et al., "Architecture and Safety Requirements of the ACC Railway Interlocking System," *Proceedings of IEEE International Computer Performance and Dependability Symposium*, Urbana-Champaign, Illinois, September 4–6, 1996, pp. 21–29.

80. G. Hagelin, "Railway Applications," in Chapter 2, p. 9, *Dependable Computing and Fault-Tolerant Systems Vol. 2 Software Diversity in Computerized Control Systems*, U. Voges (ed.), Springer-Verlag Wien, New York, 1988.

81. A. Pataricza, I. Majzik, G. Huszerl, and G. Várnai, "UML-based Design and Formal analysis of a Safety-Critical Railway Control Software Module," in *Proc. Formal Methods for Railway Operation and Control Systems (FORMS 2003)*, l'Harmattan, Budapest, 2003.

82 H. Kantz and C. Koza, "The ELEKTRA Railway Signalling-System: Field Experience with an Actively Replicated System with Diversity," *Twenty-Fifth International Symposium Fault-Tolerant Computing (FTCS-25)*, Pasadena, California, June 27–30, 1995, pp. 453–458.

83. A. Denault, "Fault Tolerance in Railway Signalling System: A study of the Elektra Interlocking Systems," http://www.adinfo.qc.ca/alex/wp-content/Elektra/elektra.pdf

84. G. Wirthumer, "Votrics—Fault Tolerance Realised in Software," *IFAC Proceedings SAFECOMP 89*, Vienna, Austria, December 1989, pp. 135–140.

85. D. Powell et al., "Architectural Approaches for using COTS Components in Critical Applications," www.laas.fr/~dpowell/slides/0005%20EWDC11.pdf

86. P. Forin, "Vital Coded Microprocessor: Principles and Application for Various Transit Systems," *Proc. IFAC-GCCT*, Paris, France, September 1989, pp. 79–84.

87. C. Hennebert and G. Guiho, "SACEM: a fault tolerant system for train speed control," *Twenty-Third International Conf. on Fault-Tolerant Computing (FTCS-23)*, Toulouse, France, 1993.

88. D. Dollé, "Vital software: Formal method and coded processor," Third Embedded Real Time Conference (ERTS 2006), Toulouse, France, January 25–27, 2006.

Draft

89. G. Guiho and C. Hennebert, "SACEM Software Validation," 12th ICSE, IEEE Computer Society Press, Mars 1990, pp. 186–191.

90. J. A. Profeta III et al., "Safety-Critical Systems Built with COTS," *Computer*, **29(**11), 54–60 (November 1996).

91. D. T. Smith et al., "An Algorithm Based Fault Tolerance Technique for Safety-Critical Applications," *1997 Proceedings of the Annual Reliability and Maintainability Symposium*, Philadelphia, Pennsylvania, January 1997.

92. B. Johnson, University of Virginia, private communication with R. T. Wood, October 2007.

93. J. R. Popovic and G. J. Hinton, "CANDU Computerized Safety System," presented at the *Advanced Computer Technology for the Power Industry*, Scottsdale, Arizona, EPRI, December 4–6, 1989.

94. *ACR-1000 Technical Summary: An Evolution of CANDU*, Atomic Energy of Canada Limited, Mississauga, Ontario, Canada.

95. R. T. Wood et al., *Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants*, NUREG/CR-6842, April 2004.

96. G. W. Remley, B. M. Cook, and P. A. Loftus, "Sizewell B Integrated Control and Instrumentation System: A Vision Becomes Reality," Conference Record of the 1992 IEEE Nuclear Science Symposium and Medical Imaging Conference, Vol. 2, Orlando, Florida, Oct. 25–31, 1992, pp. 736–738.

97. A. Johnson, "The implementation of Sizewell B automatic control systems," International Conference on Electrical and Control Aspects of the Sizewell B PWR, London, UK, Sept. 14–15, 1992, pp. 143–148.

98. C. Percival and D. Bradbury, "The engineering specification, design and implementation of the Sizewell B reactor secondary protection system," International Conference on Electrical and Control Aspects of the Sizewell B PWR, London, UK, Sept. 14–15, 1992, pp. 232–244.

99. G. B. Moutrey and G. Remley, "Sizewell B power station primary protection system design application overview," International Conference on Electrical and Control Aspects of the Sizewell B PWR, London, UK, Sept. 14–15, 1992, pp. 221–231.

100. International Atomic Energy Agency, *Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook*, IAEA Technical Report Series No. 387, 1999.

101. J. D. White et al., *WTEC Panel Report on European Nuclear Instrumentation and Controls*, Loyola College, Baltimore, Maryland, 1991.

102. B. Fride, J. Y. Henry, and S. Manners, "Safety Assessment of Computerized Instrumentation and Control for Nuclear Power Plants," International Conference on Probabilistic Safety Assessment Methodology and Applications (PSA-95), November 26–30, 1995, Seoul, Korea.

103. S. Kunito, "Construction and Operation Experience of Digitalized Safety Systems of Japanese ABWR," IAEA Technical Meeting on Common-Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, June 20, 2006, Bethesda, Maryland.

104. S. Makino, "Operating Experience of Digital Safety Related System of Kashiwazaki-Kariwa Unit Nos. 6 and 7," CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems Workshop Proceedings, NEA/CSNI/R(2002)1/Vol. 2, Hluboka nad Vltavou, Czech Republic.

Draft

105. Japan Electric Association Guideline, "Application Criteria for Programmable Digital Computer System in Safety–Related System of Nuclear Power Plants," JEAG 4609, 1999.

106. W. C. Gangloff and C. L. Werner, "I&C Modernization for VVER Reactors," *IEEE Transactions on Nuclear Science*, **40**(4), 819–825 (August 1993).

107. P. Závodsky, "Independent Assessment of the Temelín Safety System Software," *CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems Workshop Proceedings*, NEA/CSNI/R(2002)1/Vol. 1, September 2001, Hluboka nad Vltavou, Czech Republic.

108. R. G. Orendi, "Human Factors Experience in Designing a Modern Control Room for a VVER-1000 Nuclear Plant," IEEE Sixth Annual Human Factors Meeting, 1997, Orlando, Florida.

109. J.-P. Burel, F. Dalik, K. Wagner, Miroslav RIS, and J.-P. Mauduit, "Modernization of I&C systems for the ANP Dukovany by the use of computer-based equipment," *CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems Workshop Proceedings*, NEA/CSNI/R(2002)1/Vol. 2, September 2001, Hluboka nad Vltavou, Czech Republic.

110. C-F. Chuang and Y-B. Chen, "Regulatory Overview of Digital I&C in Taiwan Lungmen Project," NRC 19th Annual Regulatory Information Conference, March 13–15, 2007, Rockville, Maryland.

111. C-K. Lee, "The Network Architecture and Site Test of DCIS in Lungmen Nuclear Power Station," 5th International Topical Meeting on Nuclear Plant Instrumentation Control and Human Machine Interface Technology (NPIC & HMIT 2006), November 12–16, 2006, Albuquerque, New Mexico.

112. J. Hyvärinen, "Presentation Slides: OL3 I&C Review Status," ASN/IRSN-NRC-STUK Meeting, March 22, 2007, Paris, France.

113. U.S. EPR Pre-Application Review Meeting: U.S. EPR Digital Protection System Topical Report, presentation by AREVA NP, Inc., to the NRC, March 1, 2007, Rockville, Maryland.

114. Licensing of safety critical software for nuclear reactors. Common position of seven European nuclear regulators and authorized technical support organizations, HSE, 2007, http://www.hse.gov.uk/nuclear

115. International Atomic Energy Agency Technical Meeting on Avoiding Common-Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, Bethesda, Maryland, June 2007.

116. B. Littlewood et al., "DISPO project: A summary of CSR work on modelling of diversity," Centre for Software Reliability, City University, London, 2006.

117. B. Littlewood, P. Popov, and L. Strigini, "DISPO project: A summary of CSR work on modelling of diversity," Centre for Software Reliability, City University, London, UK, 2006.

118. J. C. Knight and N. G. Leveson, "Experimental evaluation of the assumption of independence in multiversion software," *IEEE Trans Software Engineering*, **12**(1), 96–109 (1986).

119. B. Littlewood and L. Strigini, "A discussion of practices for enhancing diversity in software designs," DISPO LS-DI-TR-04, Centre for Software Reliability, City University, London, 2000.

120. B. Littlewood and D. R. Miller, "Conceptual Modelling of Coincident Failures in Multi-Version Software," *IEEE Transactions on Software Engineering*, **15**(12), 1596–1614 (1989).

121. B. Littlewood, P. Popov, and L. Strigini, "A note on modelling functional diversity," *Reliability Engineering and System Safety*, vol. 66, no. 1, pp. 93–95, 1999.

Draft

122. International Electrotechnical Commission, "Nuclear power plants—Instrumentation and control for systems important to safety—General requirements for systems," IEC 61513, March 2001.

123. International Electrotechnical Commission, "Nuclear power plants—Instrumentation and control systems important for safety—Classification," IEC 61226, ed. 2.0, February 2005.

124. 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, May 2006.

125. International Electrotechnical Commission, "Nuclear power plants—Instrumentation and control systems important to safety—Separation," IEC 60709, November 2004.

126. International Electrotechnical Commission, "Nuclear power plants—Electrical equipment of the safety system—Qualification," IEC 60780, October 1998.

127. International Electrotechnical Commission, "Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations," IEC 60980, June 1989.

128. International Electrotechnical Commission, "Electromagnetic compatibility (EMC)—Part 4-1: Testing and measurement techniques—Overview of IEC 61000-4 series," IEC 61000-4-1, October 2006.

129. Y. C. Yeh, "Unique dependability issues for commercial airplane fly-by-wire systems," *IFIP World Computer Congress*, Toulouse, France, August 2004.

130. U.S. Nuclear Regulatory Commission, *Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems*, NUREG/CR-6463, June 1996.

Draft

APPENDIX A EVALUATING DIVERSITY IN SYSTEM DESIGNS

Draft

APPENDIX A
EVALUATING DIVERSITY IN SYSTEM DESIGNS

Licensees and applicants perform diversity and defense-in-depth (D3) analyses to determine whether diversity should be added or incorporated into proposed safety system designs as a means of mitigating the consequences of potential common cause failures (CCFs) in safety systems. If an analysis identifies the need for diversity to address a potential CCF, the licensee or applicant addresses the potential CCF vulnerability either by incorporating diverse features into the safety system design or by adding an additional diverse actuation system to the safety system design. The NRC determines the adequacy of proposed diverse designs as part of its review of licensee applications. The acceptance criteria for this determination have been subjective, generally depending upon the experience and engineering judgment of the NRC staff. This subjectivity has led to licensing uncertainty in the nuclear power industry. Specifically, the question that has arisen is, "If diversity is required to avoid or mitigate a potential CCF, how much diversity is sufficient for addressing the CCF in accordance with NRC regulations?"

This appendix describes a process for translating the diversity design information provided in the body of this report into a method the NRC staff and the nuclear industry can apply to consistently confirm that the amount of diversity in a safety system design is sufficient relative to a predetermined acceptance threshold. In the following discussions, diversity criteria comprise a diversity attribute. There are seven diversity attributes consisting of a total of 25 diversity criteria; four attributes consist of four related criteria and three attributes consist of three related criteria.

Diversity attribute usage information obtained from the sources of information was collated in a table format consistent with modified NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (ML071790509), diversity attributes and criteria to identify common trends in diversity attributes and related criteria usage. The diversity attributes and criteria are summarized in Section A.1. The sources of information used to develop a process for evaluating diversity in safety system designs are listed in Section A.2. The process for weighting the data obtained from the sources listed in Section A.2 is described in Section A.3. The development of the table format for evaluating the diversity information is described within the context of the discussions in these sections. The process for combining the weights to evaluate diversity strategies quantitatively is described in Section A.4. Results of the data analysis also will be summarized in this section. An assessment tool using the results of the data evaluation and the structure defined in the table is described in Section A.5.

A.1 Diversity Attributes and Criteria

NUREG/CR-6303 provides a method for determining uncompensated CCFs in safety system designs. Section 2.6, "Diversity," defines six diversity attributes and related diversity criteria. These attributes and related criteria are

- Design
  - Different technologies
  - Different approaches within a technology
  - Different architectures, same technology
- Equipment
  - Different manufacturers of fundamentally different designs
  - Same manufacturer of fundamentally different designs
  - Different manufacturers of same design
  - Different versions of the same design

- Different CPU architectures
- Different CPU versions
- Different printed circuit board designs
- Different bus architectures

- Function
  - Different underlying mechanisms
  - Different purpose, function, control logic, or actuation means
  - Different response time scale
- Human (renamed Life-cycle)
  - Different design organizations/companies
  - Different management teams within the same company
  - Different designers, engineers, and/or programmers
  - Different testers, installers, or certification personnel
- Signal
  - Different reactor or process parameters sensed by different physical effects
  - Different reactor or process parameters sensed by the same physical effect
  - Same process parameter sensed by a different redundant set of similar sensors
- Software
  - Different algorithms, logic, and program architecture
  - Different timing or order of execution
  - Different operating system
  - Different computer languages

At the time NUREG/CR-6303 was published (December 1994), microprocessor-based digital systems were assumed to comprise the next generation of safety systems. This assumption has been disproved with proposed safety system designs using programmable logic devices, field programmable gate arrays, application-specific integrated circuits, and multi-aperture magnetic ladder-like logic structures (Laddic). Consequently, to assure the diversity criteria could be applied independent of the technology used to implement a safety system design, this report subdivided the Equipment diversity attribute defined in NUREG/CR-6303 into two attributes, Equipment Manufacturer and Logic Processing Equipment. The Logic Processing Equipment diversity criteria were renamed to accommodate different technologies. Additionally, the Software diversity attribute was renamed the Logic diversity attribute to better reflect differences in logical representations of system functions. The resulting Equipment-related and Logic-related attributes and criteria are

- Equipment Manufacturer
  - Different manufacturers of fundamentally different designs
  - Same manufacturer of fundamentally different designs
  - Different manufacturers of same design
  - Same manufacturer of different versions of the same design
- Logic Processing Equipment
  - Different logic processing architectures
  - Different logic processing versions in same architecture
  - Different component integration architectures
  - Different data flow architectures
- Logic
  - Different algorithms, logic, and program architecture
  - Different timing or order of execution
  - Different runtime environments (e.g., operating systems)

— Different functional representation (e.g., logic languages)

NUREG/CR-6303 listed the diversity criteria above in the order representing the effectiveness of one diversity criterion relative to the other criteria in the same diversity attribute. For example, in the Design diversity attribute, using different technologies (e.g., analog and digital technologies) to add diversity to a design was determined to be more effective than using different approaches within a technology (e.g., computer-based digital technology and ASIC-based digital technology), which in turn was considered to be more effective than using different architectures (i.e., the arrangement and connection of components within a design). Table A.1 shows the resulting diversity attributes and associated ranked criteria.

Table A.1. Diversity attributes and criteria

Attribute criteria
Design
Different technologies
Different approaches within a technology
Different architectures
Equipment (Manufacturer)
Different manufacturers of fundamentally different equipment designs
Same manufacturer of fundamentally different equipment designs
Different manufacturers of same equipment design
Same manufacturer of different versions of the same equipment design
Logic Processing Equipment
Different logic processing architectures
Different logic processing versions in same architecture
Different component integration architectures
Different data flow architectures
Function
Different underlying mechanisms to accomplish safety function
Different purpose, function, control logic, or actuation means of same underlying mechanism
Different response time scale
Life-cycle
Different design organizations/companies
Different management teams within the same company
Different designers, engineers, and/or programmers
Different implementation/validation teams (testers, installers, or certification personnel)
Signal
Different parameters sensed by different physical effects
Different parameters sensed by the same physical effects
Same parameter sensed by a different redundant set of similar sensors
Logic
Different algorithms, logic, and program architecture
Different timing or order of execution
Different runtime environments
Different functional representations

Draft

In the development of the analysis process described in this appendix, additional columns and rows were added to Table A.1 to allow weights and calculations of diversity evaluation parameters. In the following discussion these additional columns and rows will be shown only for the Design, Equipment Manufacturer, and Logic Processing Equipment diversity attributes to illustrate development of the diversity strategy evaluation method.

A.2 Information Sources

As stated in the body of the report, design information for diverse systems and functions was obtained from the following sources:

- NASA
- Aviation industry
- Industrial applications
- International positions on diversity
- International nuclear power plants using diversity in safety systems

Additionally, two international plants using digital technology but no automated diverse actuation systems a generic ATWS system description for typical Westinghouse designed pressurized water reactors in the United States were included in the data base for contrast with the above sources of information. The information obtained from the first five above sources was collated in a table format to identify common trends in diversity attribute and criteria usage. Each set of diversity information from the above sources was added to the table in sets of three columns for each diversity strategy under the title of the corresponding diversity strategy. The table format with diversity attributes and diversity strategy columns is shown in Table A.2 for the first three of the seven diversity attributes for illustration purposes.

Separate columns for intentional use (INT) and inherent use (INH) of diversity criteria differentiate diversity criteria usage in the diversity strategies. The difference between intentional uses and inherent uses of criteria is described in the body of this report. The first column for each diversity strategy (INT) was used to indicate with an “X” the intentional use of a criterion in that strategy. The second column (INH) was used to indicate with an “i” the inherent use of a criterion. The third column was used to provide the corresponding criterion ranking weight if the criterion was used, regardless of whether the use was intentional or inherent. The default value in this column was set to 0.000.

Table categories consistent with the modified NUREG/CR-6303 diversity attributes described above were selected to enable comparisons between different diversity strategies. The data was then weighted and combined to obtain quantitative values for each diversity design. The development of the weights is described in section A.3, Weighting. The use of the weights and the data is described in Section A.4, Diversity Strategy Evaluation.

Draft

Table A.2. Diversity attributes, criteria, ranks, and a diversity strategy examples

Attribute criteria	Example design		
	Design 1		
Design	INT	INH	Score
Different technologies			0.000
Different approaches within a technology			0.000
Different architectures			0.000
Equipment Manufacturer	INT	INH	Score
Different manufacturers of fundamentally different equipment designs			0.000
Same manufacturer of fundamentally different equipment designs			0.000
Different manufacturers of same equipment design			0.000
Same manufacturer of different versions of the same equipment design			0.000
Logic Processing Equipment	INT	INH	Score
Different logic processing architectures			0.000
Different logic processing versions in same architecture			0.000
Different component integration architectures			0.000
Different data flow architectures			0.000

A.3 Weighting

This section describes the process used to apply weights to the data described in the report to enable quantitative comparisons of diversity strategies on the basis of the guidance in NUREG/CR-6303, the experience gained by other industries and countries, and diversity positions developed by other agencies and countries. The information gathered from the sources listed in Section A.2 above was combined by weighting the diversity criteria used in each diversity strategy in two weight categories to address guidance and experience. The guidance and experience weights for each attribute were combined by applying the experience weight to the guidance-based weights.

Diversity Criterion Effectiveness (DCE) weights were developed from NUREG/CR-6303 guidance on the effectiveness of one criterion in an attribute relative to the other criteria in the same attribute. Diversity Attribute Effectiveness (DAE) weights were developed by collating information gathered from other industry, agency, and country evaluations and experience with applying diversity to address CCFs and potential CCFs in safety system designs. The development of the algorithms for these two weights and the underlying assumptions and bases for these algorithms are described in the following sections.

A.3.1 Diversity Criterion Effectiveness Weights

The algorithm to determine the DCE (guidance-based) weights was based on the discussions of relative effectiveness provided in NUREG/CR-6303. Other factors influencing the selection of specific diversity criteria by other industries, agencies, and countries were excluded from the DCE weight algorithm because these factors were included in the DAE weight algorithm (the experience-based weights). The assumptions and underlying bases for the DCE weight algorithm are described in this section.

The first assumption is that the criteria within a diversity attribute can be weighted according to the ordering of the criteria within that diversity attribute, with the highest and lowest DCE weights assigned to the first and last criterion in a diversity attribute, respectively. The underlying basis for this assumption is that NUREG/CR-6303 qualitatively ranked the relative effectiveness of the criteria to determine the order in which the criteria are listed. The ordering by relative effectiveness has been accepted by the

NRC and the nuclear power industry since NUREG/CR-6303 was published (December 1994). Further, the use of the rankings for over a decade has not resulted in revisions to the order of the criteria. Consequently, the relative effectiveness of each criterion within a diversity attribute has been shown by consensus and experience to be appropriate.

The second assumption is that the criteria weights within a diversity attribute should be different for each criterion within the attribute. The underlying basis for this assumption is that NUREG/CR-6303 did not equate any two adjacent criteria within a diversity attribute as equally effective; therefore, the weights should be different.

The third assumption is that the DCE weights within a diversity attribute can be uniformly distributed according to the order and number of criteria within a diversity attribute absent other quantitative measures of relative effectiveness. The underlying basis for this assumption is that the weights are applied uniformly to every diversity strategy for the purpose of comparing diversity strategies. Further, since the diversity attributes are relatively independent, differences in weights between diversity attributes with different numbers of criteria can be different, as long as the weighting process is applied consistently.

The diversity criteria in each category were given relative effectiveness values from one to either three or four, depending on the number of criteria within the corresponding diversity attribute, with one being the most effective criterion, and three or four being the least effective criterion. The ranked criteria were then converted to DCE weights, W_{Cij}, using Eq. (1).

$$W_{Cij} = \frac{(N_{cj} - M_{cij} + 1)}{\sum_{i=1}^{N_{cj}} M_{cij}} \tag{1}$$

where

W_{cij} = DCE weight of criterion i in attribute j
N_{cj} = number of criteria in attribute j
M_{cij} = rank of criterion i in attribute j

Columns indicating the ranking of the diversity criteria and associated DCE weights are shown in Table A.3, DCE Weights.

Table A.3. DCE weights

Attribute criteria	Rank	Weights (DCE WT)
Design		
Different technologies	1	0.500
Different approaches within a technology	2	0.333
Different architectures	3	0.167
Equipment Manufacturer		
Different manufacturers of fundamentally different equipment designs	1	0.400
Same manufacturer of fundamentally different equipment designs	2	0.300
Different manufacturers of same equipment design	3	0.200
Same manufacturer of different versions of the same equipment design	4	0.100
Logic Processing Equipment		
Different logic processing architectures	1	0.400
Different logic processing versions in same equipment architecture	2	0.300
Different component integration architectures	3	0.200
Different data flow architectures	4	0.100
Function		
Different underlying mechanisms to accomplish safety function	1	0.500
Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333
Different response time scale	3	0.167
Life-cycle		
Different design companies	1	0.400
Different management teams within the same company	2	0.300
Different designers, engineers, and/or programmers	3	0.200
Different implementation/validation teams	4	0.100
Signal		
Different reactor or process parameters sensed by different physical effect	1	0.500
Different reactor or process parameters sensed by the same physical effect	2	0.333
The same process parameter sensed by a different redundant set of similar sensors	3	0.167
Logic		
Different algorithms, logic, and program architecture	1	0.400
Different timing or order of execution	2	0.300
Different runtime environments	3	0.200
Different languages	4	0.100

A.3.2 Diversity Attribute Effectiveness Weights (Experience)

This section describes the assumptions and underlying bases for the DAE algorithm. The algorithm to determine the DAE weights was based on the experience of other industries, agencies, and countries with the use of diversity criteria in applications and the development of research and regulatory positions by other countries. Four assumptions and underlying bases were applied to develop the DAE algorithm.

The first assumption is that the frequency of diversity attribute usage represents consensus on the effectiveness of a diversity attribute to address observed or potential CCFs. The underlying basis for this assumption is that diversity strategies developed by industries, agencies and countries to address specific CCF vulnerabilities reflect experience with failures that have occurred and engineering judgment regarding potential failures that should be addressed. Additionally, current versions of diversity strategies reflect the efficacy of certain combinations of diversity attributes over time.

The second assumption is that consensus on diversity attribute usage accounts for application constraints on the diverse designs used to establish consensus. The underlying basis for this assumption is that to determine consensus on the use of a diversity attribute, each diverse design used in the consensus determination should have had the option to use the diversity attribute. Physical or functional restrictions on the use of specific diversity attributes in a diverse design would inappropriately bias consensus on diversity attribute effectiveness. For example, if functional diversity could not be used to mitigate CCFs in a specific application, the exclusion of the Function diversity criteria from the diverse design would appear to reflect a decision that the Function diversity attribute was not effective for any other application.

The third assumption is that consensus on the use of a diversity attribute is independent of the consensus on use of other diversity attributes (i.e., the diversity attributes represent relative degrees of freedom in a diversity strategy). The underlying basis for this assumption is that each diversity attribute addresses specific types of failures that generally cannot be addressed as effectively by other diversity attributes. As a result, the sum of the seven DAE weights is not required to be 1.0 because the diversity attributes are relatively independent.

The fourth assumption is that DAE weights should account for the number of criteria in an attribute that are available for use in a diverse design (i.e., use of one criterion in an attribute that excludes use of one or more other criteria in the diversity attribute reduces the number of available options in that attribute). The underlying basis for this assumption is that, since DAE weights (as opposed to DCE weights) represent consensus on the use of the criteria comprising the attributes, and all criteria may not be available for use in a diversity strategy, the weights must be adjusted to account for the limitations on selection of diversity criteria in a strategy. For example, three intentionally mutually exclusive diversity criteria comprise the Design diversity attribute. Assume 16 diverse designs used a total of 16 Design attribute criteria. If the Design DAE weight was determined by dividing the number of Design diversity criteria used in the set of diverse designs comprising consensus by the total number of Design diversity criteria multiplied by the number of applications, the resulting weight would imply only a 33.3% consensus on use of the Design attribute. However, since there were actually only 16 opportunities to intentionally use Design diversity criteria in the 16 diversity strategies, the actual consensus would be that the diversity strategies had used 100% of Design diversity opportunities, which would reflect the consensus opinion on Design diversity.

The diversity attributes consist of the following number of criteria that could be used in the same diverse system or function:

- Design, 1 out of 3 intentionally selected
- Equipment Manufacturer, 4 out of 4 either intentionally or inherently selected
- Logic Processing Equipment, 1 out of first 2 and remaining 2 out of 4 either intentionally or inherently selected
- Function, 3 out of 3 either intentionally or inherently selected
- Life-cycle, 4 out of 4 either intentionally or inherently selected
- Logic, 4 out of 4 either intentionally or inherently selected
- Signal, 3 out of 3 either intentionally or inherently selected

To address differences in the number of diversity criteria available for use in each diversity attribute, the ratio of the number of diversity criteria used to the number of designs comprising consensus was normalized by the number of diversity criteria in the same diversity attribute that could be used together in a system design. Using this normalization process assured that higher DAE weights would be assigned to diversity attributes that are used most frequently, which coincides with the first assumption that frequency of usage correlates to effectiveness.

The diversity attribute weights were calculated using Eq. (2).

$$W_{Aj} = \frac{\sum_{i=1}^{N_{Cj}} N_{Cij}}{N_S \times N_{Cj}} \tag{2}$$

where

W_{Aj} = DAE weight for attribute j
N_{Cj} = number of criteria in attribute j
N_{Cij} = number of criterion i used in attribute j by the N_s systems
N_S = number of system designs evaluated
N_{Cj} = number of criteria that could be used together in attribute j

Alternate approaches to Eq. (2) were necessary for the Design DAE weight (***W_{A1}***) and the Logic Processing Equipment DAE weight (***W_{A3}***). The Design attribute criterion for different architectures (criterion rank 3) can be inherently included in a design by selecting either of the higher ranked Design attribute criteria. To avoid double counting the number of Design attribute criteria selected by other industries and countries, the inherent use of this criterion was not included in the determination of the Design DAE weight. Consequently, the number of Design diversity criteria that could be used together was set to 1. The resulting equation for the Design DAE weight is given by Eq. (3),

$$W_{A1} = \frac{\sum_{i=1}^{3} N_{Ci1}}{N_S} \tag{3}$$

where

W_{A1} = design DAE weight
N_{Ci1} = number of system designs using criterion i in attribute 1
N_S = number of system designs evaluated

For the Logic Processing Equipment DAE weight (***W_{A3}***), the two most effective criteria are mutually exclusive, and the remaining criterion/criteria may be used in conjunction with either of the first two criteria. These combinations of criteria required a separate DAE weighting function, which is given by Eq. (4).

$$W_{A3} = \frac{\sum_{i=1}^{4} N_{Ci3}}{N_S \times (N_{C3} - 1)} \tag{4}$$

where

W_{A3} = Logic Processing Equipment DAE weight
N_{Cij} = number of system designs using criterion i, attribute 3
N_S = number of system designs evaluated
N_{Cj} = number of criteria in attribute 3 (4)

To calculate the DAE weights, an extra column was added to Table A.3 above to record the number of strategies using each diversity criterion. Additionally, another row was added for each diversity attribute to record the number of criteria used and the DAE weight for each diversity attribute. The DAE weights for the seven diversity attributes and the data used to calculate the DAE weights are shown in Table A.4. The number of diversity criteria used by the 16 strategies in the evaluation is shown in the "$\boldsymbol{N_{Cij}}$," column. The DAE weight for each attribute, $\boldsymbol{W_{Aj}}$, is immediately below the diversity attribute DCE weights, $\boldsymbol{W_{Cij}}$, in the same column.

The process for using the DCE weights and the DAE weights to quantitatively evaluate the diversity strategies obtained from the sources listed in Section A.2 is described in the next section. An assessment tool using the results of the data evaluation is described in Section A.5.

Table A.4. Diversity criteria usage and DAE weights

Attribute criteria	Weights		
Design (attribute = 1, i = 1 to 3)	M_{Ci1}	W_{Ci1}	N_{Ci1}
Different technologies	1	0.500	4
Different approaches within a technology	2	0.333	3
Different architectures	$N_{C1} = 3$	0.167	9
DAE WT. and subtotals	$\sum_{i=1}^{N_{C1}} M_{Ci1} = 6$	$W_{A1} = 1.000$	$\sum_{i=1}^{N_{C1}} N_{Ci1} = 16$
Equipment Manufacturer (attribute 2, i = 1 to 4)	M_{Ci2}	W_{Ci2}	N_{Ci2}
Different manufacturers of fundamentally different equipment designs	1	0.400	5
Same manufacturer of fundamentally different equipment designs	2	0.300	2
Different manufacturers of same equipment design	3	0.200	5
Same manufacturer of different versions of the same equipment design	$N_{C2} = 4$	0.100	2
DAE WT. and subtotals	$\sum_{i=1}^{N_{C2}} M_{Ci2} = 10$	$W_{A2} = 0.219$	$\sum_{i=1}^{N_{C2}} N_{Ci2} = 14$
Logic Processing Equipment (attribute 3, i = 1 to 4)	M_{Ci3}	W_{Ci3}	N_{Ci3}
Different logic processing equipment architectures	1	0.400	14
Different logic processing versions in same equipment architecture	2	0.300	0
Different component integration architectures	3	0.200	9
Different data flow architectures	$N_{C3} = 4$	0.100	7

Table A.4. Diversity criteria usage and DAE weights (continued)

Attribute criteria	Weights

DAE WT. and subtotals	$\sum_{i=1}^{N_{C3}} M_{Ci3} = 10$	$W_{A3} = 0.625$	$\sum_{i=1}^{N_{C3}} N_{Ci3} = 30$
Function (attribute 4, i = 1 to 3)	M_{Ci4}	W_{Ci4}	N_{Ci4}
Different underlying mechanisms to accomplish safety function	1	0.500	7
Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	16
Different response time scale	3	0.167	4
DAE WT. and SUBTOTALS	$\sum_{i=1}^{N_{C4}} M_{Ci4} = 6$	$W_{A4} = 0.563$	$\sum_{i=1}^{N_{C4}} N_{Ci4} = 27$
Life Cycle (attribute 5, i=1 to 4)	M_{Ci5}	W_{Ci5}	N_{Ci5}
Different design companies	1	0.400	8
Different management teams within the same company	2	0.300	4
Different designers, engineers, and/or programmers	3	0.200	16
Different implementation/validation teams	$N_{C5} = 4$	0.100	14
DAE WT. and subtotals	$\sum_{i=1}^{N_{C5}} M_{Ci5} = 10$	$W_{A5} = 0.656$	$\sum_{i=1}^{N_{C5}} N_{Ci5} = 42$
Signal (attribute 6, i = 1 to 3)	M_{Ci6}	W_{Ci6}	N_{Ci6}
Different reactor or process parameters sensed by different physical effect	1	0.500	19
Different reactor or process parameters sensed by the same physical effect	2	0.333	13
The same process parameter sensed by a different redundant set of similar sensors	$N_{C6} = 3$	0.167	9
DAE WT. and subtotals	$\sum_{i=1}^{N_{C6}} M_{Ci6} = 6$	$W_{A6} = 0.792$	$\sum_{i=1}^{N_{C6}} N_{Ci6} = 38$
Logic (attribute 7, i = 1 to 4)	M_{Ci7}	W_{Ci7}	N_{Ci7}
Different algorithms, logic, and program architecture	1	0.400	16
Different timing or order of execution	2	0.300	6
Different runtime environments	3	0.200	9
Different languages	$N_{C7} = 4$	0.100	12
DAE WT. and subtotals	$\sum_{i=1}^{N_{C7}} M_{Ci7} = 10$	$W_{A7} = 0.672$	$\sum_{i=1}^{N_{C7}} N_{Ci7} = 42$

A.4 Diversity Strategy Evaluation

The process used to evaluate the diversity strategies obtained from the sources listed in Section A.2 above using the weights developed in Section A.3 is described in this section. The DCE weight variables and the DAE weight variables for the seven diversity attributes are listed in Table A.4, and are repeated in Table A.5.

Sixteen diversity strategies were used to develop the data shown in Table A.4. The NASA and Aircraft diversity strategies were excluded from the DCE and DAE weight evaluations because these applications were limited in their diversity options by size, weight, and functional diversity limitations.

One of the nuclear power plants (Dukovany) was excluded bcause the plant did not incorporate diverse systems in its design. Four diversity strategies were obtained from non-nuclear industrial applications. Five diversity strategies were obtained from positions developed thru research activities in other countries and regulatory positions developed by other countries. Seven diversity strategies were obtained from nuclear power plants in other countries. An example strategy was obtained from design information for a typical Westinghouse design U.S. nuclear power plant anticipated transient without scram (ATWS) system to use as a comparison point for the development of the tool.

The number of strategies using each criterion is listed in the **CRIT. USAGE** column in Table A.5. The total number of diversity criteria used by the 16 diversity strategies is listed in the **DAE WT. and subtotals** row as the sum of the N_{Cij} for each diversity attribute. The resulting DAE weights are listed in "**DAE WT. and subtotals"** row in the **Weights** column.

A set of worksheet columns was completed for each diversity strategy identified in the body of this report. A sample worksheet illustrating the structure of the worksheet is shown in Table A.5. The dotted line delimiting the two diversity strategies shown in Table A.5 starting at the fifth column of the worksheet signifies other diversity strategies could be in the actual worksheet but are not shown here.

The relationship between intentional diversity criteria and inherent diversity criteria described in Chapter 6 of the report was applied to the worksheet to assure appropriate credit for diverse attributes and related criteria. Intentionally used criteria are indicated in the Intentional criteria column (INT) cells with an "X." Criteria inherently included in the strategy are indicated with an "i" in the corresponding Inherent criterion (INH) column cells.

Diversity strategies were scored using the Eq. (5) below. The scores of each diversity strategy were scaled by 100 to facilitate qualitative comparisons of diversity strategy scores.

$$S_n = \left(\sum_{j=1}^{7} W_{Aj} \times \sum_{i=1}^{N_{Cj}} (W_{Cij} \times k) \right) \times 100^{*}/264 \qquad (5)$$

where

S_n = normalized diversity strategy score for strategy n
W_{Aj} = DAE weight for attribute j
N_{Cj} = number of criteria in attribute j
W_{Cij} = DCE weight of criterion i in attribute j
k = 1 if criterion i in attribute j is used
k = 0 if criterion i in attribute j is not used

The 16 diversity strategy scores used in the analysis were averaged to develop a normalizing constant for later use in the evaluation tool described in Section A.5. The mean value of the 16 diversity strategies used in the analysis was 264 ± 66. Each score was normalized by the mean to facilitate comparison of scores to the mean. The mean score was used as the normalizing constant on the basis that the mean score represents a consensus on adequate diversity by the organizations responsible for developing the 16 diversity strategies. An example ATWS system score determined from the weights was 272, which compares favorably with the average score of diversity strategies used in other applications. The evaluation tool described in Section A.5 uses the above equations and the normalizing constant (264) to enable licensees, applicants, and the NRC staff to evaluate potential diversity strategies quantitatively.

*Scaled by 100 for readability.

Table A.5. Diversity evaluation worksheet structure

Attribute criteria	Rank	DCE WT	Crit. usage	Strategies					
				Strategy 1			Strategy 2		
				INT	INH	Score	INT	INH	Score
Design									
Different technologies	1	0.500	4			0.000	X		0.500
Different approaches within a technology	2	0.333	3			0.000			0.000
Different architectures	3	0.167	9	X		0.167		i	0.167
DAE WT. and subtotals		1.000	16		0.167	0.167		0.667	0.667
Equipment Manufacturer									
Different manufacturers of fundamentally different equipment designs	1	0.400	5			0.000	X		0.400
Same manufacturer of fundamentally different equipment designs	2	0.300	2			0.000			0.000
Different manufacturers of same equipment design	3	0.200	5			0.000			0.000
Same manufacturer of different versions of the same equipment design	4	0.100	2	X		0.100			0.000
DAE WT. and subtotals		0.219	14		0.022	0.100		0.088	0.400
Logic Processing Equipment									
Different logic processing equipment architectures	1	0.400	14	X		0.400		i	0.400
Different logic processing versions in same equipment architecture	2	0.300	0			0.000			0.000
Different component integration architectures	3	0.200	9			0.000		i	0.200
Different data flow architectures	4	0.100	7			0.000		i	0.100
DAE WT. and subtotals		0.625	30		0.250	0.400		0.438	0.700

Draft

Table A.5 (continued)

Attribute criteria	Rank	DCE WT	Crit. usage	Strategies					
				Strategy 1			Strategy 2		
				INT	INH	Score	INT	INH	Score
Function									
Different underlying mechanisms to accomplish safety function	1	0.500	7			0.000	X		0.500
Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	16	X		0.333	X		0.333
Different response time scale	3	0.167	4			0.000			0.000
DAE WT. and subtotals		0.563	27		0.187	0.333		0.469	0.833
Life-cycle									
Different design companies	1	0.400	8			0.000	X		0.400
Different management teams within the same company	2	0.300	4	X		0.300			0.000
Different designers, engineers, and/or programmers	3	0.200	16	X		0.200		i	0.200
Different implementation/validation teams	4	0.100	14	X		0.100		i	0.100
DAE WT. and subtotals		0.656	42		0.394	0.600		0.459	0.700
Signal									
Different reactor or process parameters sensed by different physical effects	1	0.500	16	X		0.500	X		0.500
Different reactor or process parameters sensed by the same physical effect	2	0.333	13	X		0.333	X		0.333
The same process parameter sensed by a different redundant set of similar sensors	3	0.167	9			0.000			0.000
DAE WT. and subtotals		0.792	38		0.660	0.833		0.660	0.833

Draft

Table A.5 (continued)

Attribute criteria	Rank	DCE WT	Crit. usage	Strategies					
				Strategy 1			Strategy 2		
				INT	INH	Score	INT	INH	Score
Logic									
Different algorithms, logic, and program architecture	1	0.400	16	X		0.400		i	0.400
Different timing or order of execution	2	0.300	6			0.000		i	0.300
Different runtime environments	3	0.200	9			0.000		i	0.200
Different languages	4	0.100	12	X		0.100		i	0.100
DAE WT. and subtotals		0.672	42		0.356	0.500		0.672	1.000
Mean and standard deviation/scores			264 ± 66	204			345		
Number of strategies/Normalized scores	16		287	0.77			1.31		

Draft

Figure A.1 compares the diversity strategy evaluations graphically, and compares the results of the evaluations to the mean value of the 16 strategies used to develop the DCE and DAE weights. The ORNL strategies and the example ATWS strategy are also presented.

A.5 Evaluation Tool for Proposed Diversity Strategies

Section A.1 above described the diversity attributes and criteria used to evaluate diversity strategies obtained from the sources of information listed in Section A.2. The process for weighting the data obtained from these sources in a worksheet format was described in Section A.3. The process for combining the weights to evaluate diversity strategies quantitatively was described in Section A.4. These processes were formalized in a worksheet format for evaluating other diversity strategies using a standardized approach. The evaluation tool is described in this section. Section A.5.1 provides guidelines for using the evaluation tool to define a diversity strategy. Section A.5.2 provides the formulas for automatically crediting inherent diversities on the basis of selecting intentional diversities. Section A.5.3 provides an example calculation.

Table A.6 below provides the basic structure of the worksheet table. The letters across the top of the table and the numbers down the left side of the table provide a coordinate system for referencing specific elements (cells) of the table using a letter-number format. For example, cell D5 in Table A.6 lists the DCE weight (0.500) for the "Different technologies" criterion in the "Design" attribute. This cell designation system will be used to describe the formulas used in the table for determining credit for inherent criteria on the basis of selected intentional criteria. The other formulas used in the table for calculating scores will not be described in this section because these formulas were defined in Section A.4 above.

A.5.1 Guidelines

Using a tool for evaluating diversity strategies provides the NRC staff, licensees and applicants a process for consistently concluding sufficient diversity has been incorporated into a safety system design. However, this process cannot be used consistently without first providing a framework for the use of the tool. This section briefly outlines constraints on the use of the tool. These constraints are relatively high level common sense recommendations that should be addressed when developing a diverse system or function for a safety system.

A.5.1.1 Scope of System or Function

The set of diversity attributes in the diverse system design should address the postulated CCF mechanisms. The underlying basis for incorporating diversity into a system design is to address specific, postulated or expected CCFs that should be avoided or mitigated. Consequently, the user of the tool should provide justifications for each diversity attribute and criterion used in the modeled diverse system. For example, if a Software CCF, a Function CCF, and a Logic Processing CCF are postulated by a licensee as failures that could defeat a safety system, criteria from these attributes should be included in the diverse system design.

A.5.1.2 Credit for Inherent Diversities

Intentional selection of some diversity criteria for a diversity strategy will result in the tool crediting other diversity criteria as inherent features in a specific design. This feature of automatically crediting inherent diversity criteria was incorporated into the tool design to provide consistency in the application of inherent criteria. The rules for crediting inherent criteria are typically applicable; however, the system

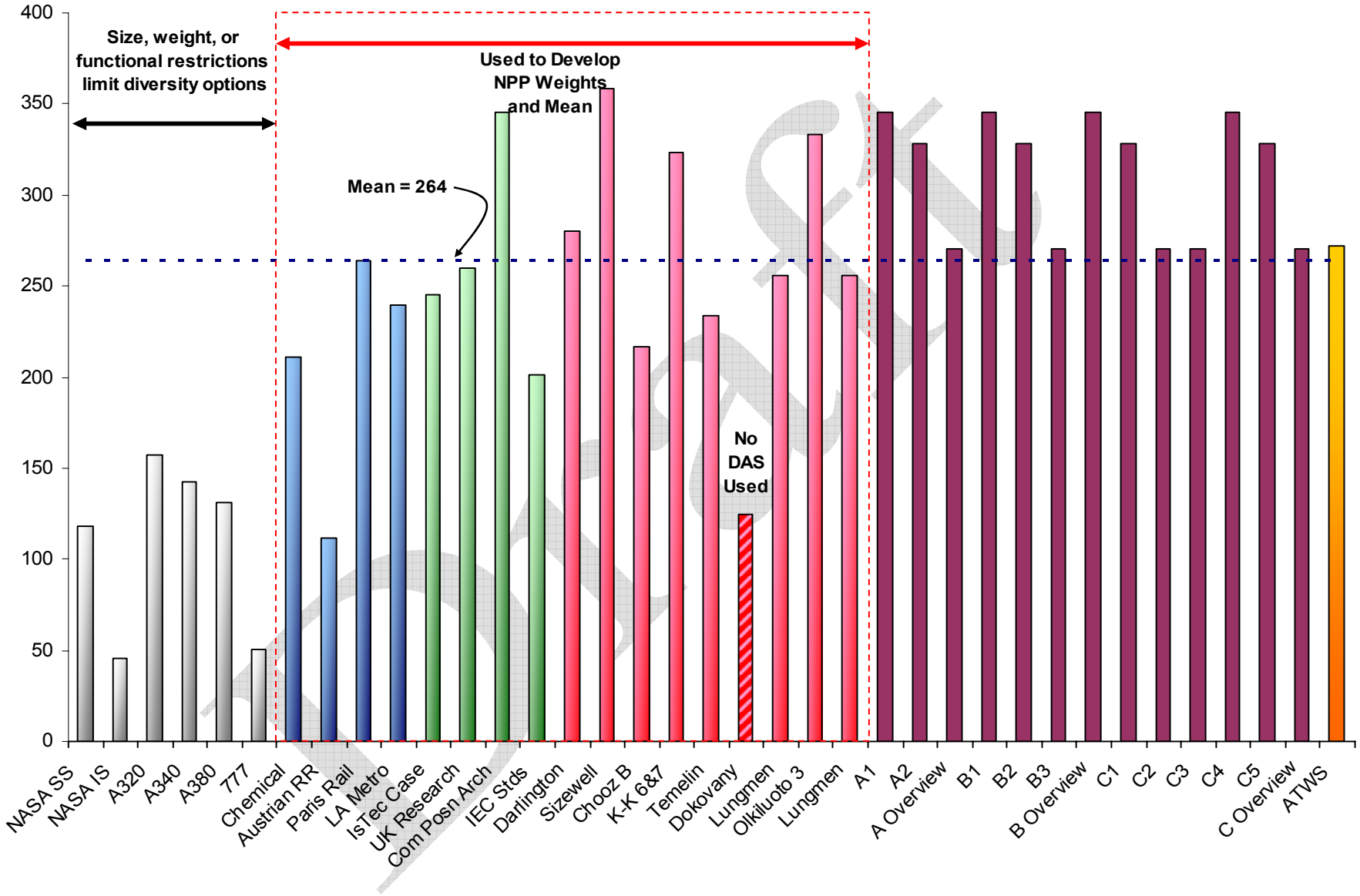

Figure A.1. Comparison of diversity strategies

Table A.6. Diversity evaluation worksheet

	A	B	C	D	E	F	G
1	**Attribute criteria**				**Facility**		
2					**Application**		
3			**Rank**	**DCE WT**	**INT**	**INH**	**Score**
4	DESIGN	Design					
5		Different technologies	1	0.500			0.000
6		Different approaches within a technology	2	0.333			0.000
7		Different architectures	3	0.167			0.000
8		DAE WT. and Subtotals		1.000		0.000	0.000
9	EQUIP. MANUF.	Equipment Manufacturer					
10		Different manufacturers of fundamentally different equipment designs	1	0.400			0.000
11		Same manufacturer of fundamentally different equipment designs	2	0.300			0.000
12		Different manufacturers of same equipment design	3	0.200			0.000
13		Same manufacturer of different versions of the same equipment design	4	0.100			0.000
14		DAE WT. and Subtotals		0.219		0.000	0.000
15	LOGIC PROC. EQUIP.	Logic Processing Equipment					
16		Different logic processing equipment architectures	1	0.400			0.000
17		Different logic processing versions in same equipment architecture	2	0.300			0.000
18		Different component integration architectures	3	0.200			0.000
19		Different data flow architectures	4	0.100			0.000
20		DAE WT. and Subtotals		0.625		0.000	0.000
21	FUNCTION	Function					
22		Different underlying mechanisms to accomplish safety function	1	0.500			0.000
23		Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333			0.000
24		Different response time scale	3	0.167			0.000
25		DAE WT. and Subtotals		0.563		0.000	0.000

Draft

Table A.6 (continued)

	A	B	C	D	E	F	G
26	LIFE-CYCLE	Life-cycle					
27		Different design companies	1	0.400			0.000
28		Different management teams within the same company	2	0.300			0.000
29		Different designers, engineers, and/or programmers	3	0.200			0.000
30		Different implementation/validation teams	4	0.100			0.000
31		DAE WT. and Subtotals		0.656		0.000	0.000
32	SIGNAL	Signal					
33		Different reactor or process parameters sensed by different physical effects	1	0.500			0.000
34		Different reactor or process parameters sensed by the same physical effect	2	0.333			0.000
35		The same process parameter sensed by a different redundant set of similar sensors	3	0.167			0.000
36		DAE WT. and Subtotals		0.792		0.000	0.000
37	LOGIC	Logic					
38		Different algorithms, logic, and program architecture	1	0.400			0.000
39		Different timing or order of execution	2	0.300			0.000
40		Different runtime environments	3	0.200			0.000
41		Different logic languages	4	0.100			0.000
42		DAE WT. and Subtotals		0.672		0.000	0.000
43							
44		Score (×100)			0		
45		Normalized score			0.00		
46		Basis for normalizing	264				

designer should ensure that the credited diversity criteria have been addressed in the design. For example, if a system design consists of two fundamentally different technologies (cell G5 in Table A.6), the tool automatically credits the Design attribute criterion, "Different architectures, same approach," (cell F7), the Equipment Manufacture attribute criterion, "Different manufacturers of fundamentally different equipment designs" (cell F10 in Table A.6), and other diversity attribute criteria. If the diverse equipment

is produced by the same manufacturer, however, the designer should not credit this inherent criterion in the evaluation. (The process by which credit for an inherent diversity can be removed from the worksheet is explained in Section A.5.2).

A.5.1.3 Guidance Constraints

The constraints and guidance provided in the body of this report should be followed to the extent practical. For example, the intentional selection of diverse systems from the same equipment manufacturer should be compensated with intentional application of separate teams within that company. Further guidance is available in Chapter 6 of the report.

A.5.1.4 Acceptance Threshold

Acceptance of a diversity strategy on the basis of a quantitative evaluation implies that a threshold value has been established for determining that sufficient diversity exists in the design. As stated in the preceding sections, 16 diversity strategies were used to define an average score using the worksheet and algorithms described in Section A.4 above. The average score represents a consensus on appropriate combinations of diversity attributes and related criteria. The average score was then used as a normalizing constant for diversity strategies such that, when a strategy was found to be above 1.0, the analyst could conclude with reasonable assurance that the strategy would be acceptable to the body of engineers who comprised the consensus. Consequently, in using the tool to define a specific diversity strategy or to determine whether sufficient diversity is present in a design (consistent with the guidelines in this appendix) a score of 1.0 was set as the acceptance threshold.

A.5.2 Worksheet Logic

This section describes the logic used in the worksheet to identify intentional and inherent diversity criteria selected for a diverse system or function, to apply the weights described in section A.3, and to combine the weights using the process described in Section A.4 to determine a quantitative value for a diverse system or function. The worksheet logic is presented in a format that allows a user to cut-and-paste the logic into a spreadsheet that uses Microsoft Excel logic syntax. Additional features not required for evaluating a diversity strategy are available in a spreadsheet developed by the NRC and available in the NRC document management system (ADAMS Access Number ML083440387).

Table A.7 consists of four columns. The first column identifies the cell address for each logic statement. These cells are identified in Table A.6. The second column provides a pseudo-language representation of the logic for each cell that contains logic. The third column translates the pseudo-language representation into an Excel-like logical statement that can be transferred by cut-and-paste into cells in an Excel spreadsheet. The fourth column briefly describes the purpose of the logic. The format of the Excel spreadsheet and cell values such as DCE weights, DAE weights, diversity attribute titles, and cell labels are provided in Table A.6.

A.5.3 Example Evaluation of Diversity

This section provides an example of how the worksheet can be used to develop a diverse actuation system to avoid or mitigate specific CCFs. The example system is based upon a pressurized water reactor (PWR) design using a microprocessor-based reactor protection system (RPS)

In this example the licensee performed a CCF analysis of the RPS and determined from best estimate analyses of a design basis large break loss of coolant accident (LBLOCA) that if a CCF occurred in the RPS logic during a design basis LBLOCA there was some potential for exceeding safety limits. As a first step, the licensee evaluated the existing microprocessor-based RPS and filled in the worksheet "PWR

Example" column below to determine a numerical value for the diversity in the RPS. The RPS was typical of most PWR RPS designs, relying on:

- Different underlying mechanisms;
- Different purpose, function, control logic, or actuation means of same underlying mechanism;
- Different reactor or process parameters sensed by different physical effects; and
- Different reactor or process parameters sensed by the same physical effect.

Additionally, because of the difference in underlying mechanisms; purpose, function, etc.; different algorithms, logic, and program architecture were inherently credited for the safety functions. The resulting worksheet and calculation of a diversity score (0.52) for the PWR Example RPS is shown in Table A.8 below.

As shown in Table A.8, the safety system diversity score (0.53) is substantially less than the 1.0 threshold. The licensee, therefore, developed a diverse system design using analog-based technology with components manufactured by a company different from the company supplying the RPS. The licensee also chose different underlying mechanisms to initiate the backup trip function for the RPS and selected the pressurizer level instrumentation to indicate a loss of coolant accident caused by a LBLOCA.

As a result of selecting the above features intentionally, the licensee achieved additional inherent diversities from the following diversity criteria:

- Different architectures (Design);
- Different manufacturers of fundamentally different equipment designs (Equipment Manufacturer);
- Different logic processing equipment architectures (Logic Processing Equipment);
- Different component integration architectures (Logic Processing Equipment);
- Different data flow architectures (Logic Processing Equipment);
- Different design organizations/companies (Life-cycle);
- Different designers, engineers, and/or programmers (Life-cycle);
- Different implementation/validation teams (Life-cycle);
- Different algorithms, logic, and logic architecture (Logic);
- Different timing or order of execution (Logic);
- Different runtime environments (Logic); and
- Different logic languages (Logic).

The licensee concluded that the diversity in the RPS was not sufficient to address CCFs in the RPS occurring coincident with a LBLOCA. Additionally, as a result of the analysis, the licensee concluded, on the basis of the 1.24 score, that some diversity could be eliminated from the DAS while still retaining sufficient diversity, as long as the features removed from the design left a system capable of responding to the CCFs assumed in the initial analysis, and the resulting score was at least 1.0. The effect of removing a diverse feature could be determined by removing the corresponding intentional diversity criterion from the worksheet and observing the effect on the diversity score. As long as the diversity score remained greater than the threshold value of 1.0, and the resulting design addressed the postulated CCFs, the design would be adequate for its intended purpose.

A.6 Conclusions

Diversity attribute usage information obtained from the sources of information was collated in a table format consistent with the modified NUREG/CR-6303 diversity attributes and criteria to identify common trends in diversity attributes and related criteria usage. The diversity attributes and criteria summarized in Section A.1 were weighted using the information gathered from the sources listed in Section A.2. The weights and supporting algorithms were translated into a worksheet format to allow a

user to evaluate the amount of diversity in a system design, independent of the technology used in the design. The algorithms were presented in Section A.5, and an example of using the resulting worksheet was presented.

The use of a worksheet format allows the user flexibility in developing diverse systems that address specific CCFs identified in a diversity assessment. A process was described for translating the diversity design information provided in the body of this report into a method the NRC staff and the nuclear industry can apply to consistently confirm that the amount of diversity in a safety system design is sufficient relative to a predetermined acceptance threshold.

Draft

Table A.7. Worksheet logic

Cell	Pseudo-language logic	Logic	Comments
E2	**System name**	Text format cell	Use cell **E2** to designate the name of the system being evaluated
G5	**IF** "**Different technologies**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in cell **D5** into cell **G5** **OTHERWISE** Set cell **G5** to **0**	=IF(E5="X",$D5,0)	Sets cell **G5** to the DCE weight if an "**x**" is in cell **E5**. Otherwise, sets cell **G5** to 0 for subsequent calculations.
G6	**IF** "**Different approaches within a technology**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in cell **D6** into cell **G6** **OTHERWISE** Set cell **G6** to **0**	=IF(E6="X",$D6,0)	Sets cell **G6** to the DCE weight if an "**x**" is in cell **E6**. Otherwise, sets cell **G6** to **0** for subsequent calculations.
F7	**IF** "**Different technologies"** is criterion selected **OR** **"Different approaches within a technology"** is selected **AND** "**Different architectures**" criterion is BLANK **THEN** Insert "**i"** in cell **F7** **OTHERWISE** Set cell **F7** to **BLANK**	=IF(AND(OR(E$5="X",E$6="X"),E$7=""),"i", "")	Sets Inherent flag, "i", for cell **F7** if an "**X**" or "**x**" is in cells **E5** or **E6** and cell **E7** is **BLANK**. If any other character is in cell **E7**, cell **F7** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G7	**IF** "**Different architectures**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D7** into cell **G7** **OTHERWISE** Set cell **G7** to **0**	=IF(OR(E7="X",F7="i"),$D7,0)	Sets cell **G7** to the DCE weight if an "**x**" is in cell **E7** or an "i" is in cell **F7**. Otherwise, sets cell **G7** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F10	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **AND** "**Different manufacturers of fundamentally different equipment designs**" criterion is BLANK **THEN** Insert **"i"** in cell **F10** **OTHERWISE** Set cell **F10** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X"),E$10=""), "i", "")	Sets Inherent flag, "i", for cell **F10** if an "**X**" or "**x**" is in cell **E5** or cell **E6,** and cell **E10** is **BLANK**. If any other character is in cell **E7**, cell **F7** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
F8	Cell **F8** = cell **G8** * cell **D8**	=G8*$D8	Multiply the sum of the **Design** attribute criteria values in cell **G8** by the **Design DAE** weight in cell **D8** and place the result in cell **F8**
G8	Cell **G8** = **G5** + **G6** + **G7**	=SUM(G5:G7)	**ADD** the **Design** attribute criteria values in cells **G5, G6,** and **G7** and places result in cell **G8**
G10	**IF** "**Different manufacturers of fundamentally different equipment designs**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D10** into cell **G10** **OTHERWISE** Set cell **G10** to **0**	=IF(OR(E10="X",F10="i"),$D10,0)	Sets cell **G10** to the DCE weight if an "**x**" is in cell **E10** or an "**i**" is in cell **F10**. Otherwise, sets cell **G10** to **0** for subsequent calculations.
G11	**IF** "**Same manufacturer of fundamentally different equipment designs**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in cell **D11** into cell **G11** **OTHERWISE** Set cell **G11** to **0**	=IF(E11="X",$D11,0)	Sets cell **G11** to the DCE weight if an "**x**" is in cell **E11**. Otherwise, sets cell **G11** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G12	**IF** "**Different manufacturers of same equipment design**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D12** into **G12** **OTHERWISE** Set cell **G12** to **0**	=IF(E12="X",$D12,0)	Sets cell **G12** to the DCE weight if an "**x**" is in cell **E12**. Otherwise, sets cell **G12** to **0** for subsequent calculations.
G13	**IF** "**Same manufacturer of different versions of the same equipment design**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D13** into **G13** **OTHERWISE** Set cell **G13** to **0**	=IF(E13="X",$D13,0)	Sets cell **G13** to the DCE weight if an "**x**" is in cell **E13**. Otherwise, sets cell **G13** to **0** for subsequent calculations.
F14	Cell **F14** = cell **G14** * cell **D14**	=G14*$D14	Multiply the sum of the **Equipment Manufacturer** attribute criteria values in cell **G14** by the **Equipment Manufacturer DAE** weight in cell **D14** and place the result in cell **F14**
G14	Cell **G14** = cell **G10** + cell **G11** + cell **G12** + cell **G13**	=SUM(G10:G13)	**ADD** the **Equipment Manufacturer** attribute criteria values in cells **G10, G11, G12,** and **G13** and place result in cell **G14**

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F16	**IF** "**Different technologies**" criterion is selected **OR** "**Different approaches within a technology**" criterion is selected **OR** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **OR BOTH** "**Same approach, different architectures**" criterion is selected **AND** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **AND** "**Different logic processing equipment architectures**" criterion is BLANK **THEN** Insert **"i"** in cell **F16** **OTHERWISE** Set cell **F16** to **BLANK**	=IF(AND(OR(E$5="X",E$6="X", E$10="X", AND(E$7="X", E$10="X")),E$16=""),"i", "")	Sets Inherent flag, "i", for cell **F16** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or both cells **E7** and **E10** have an "**X**", and cell **E16** is **BLANK**. If any other character is in cell **E16**, cell **F16** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G16	**IF** "**Different logic processing equipment architectures**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D16** into cell **G16** **OTHERWISE** Set cell **G16** to **0**	=IF(OR(E16="X",F16="I"),$D16,0)	Sets cell **G16** to the DCE weight if an "**x**" is in cell **E16** or an "i" is in cell **F16**. Otherwise, sets cell **G16** to **0** for subsequent calculations.
G17	**IF** "**Different logic processing versions in same equipment architecture**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D17** into **G17** **OTHERWISE** Set cell **G17** to **0**	=IF(E17="X",$D17,0)	Sets cell **G17** to the DCE weight if an "**x**" is in cell **E17**. Otherwise, sets cell **G17** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F18	**IF** "**Different technologies**" criterion is selected **OR** "**Different approaches within a technology**" criterion is selected **OR** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **OR BOTH** "**Different architectures**" criterion is selected **AND** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **AND** "**Different component integration architectures**" criterion is BLANK **THEN** Insert **"i"** in cell **F18** **OTHERWISE** Set cell **F18** to **BLANK**	=IF(AND(OR(E$5="X",E$6="X", E$10="X", AND(E$7="X", E$10="X")),E$18=""),"i", "")	Sets Inherent flag, "i", for cell **F18** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or both cells **E7** and **E10** have an "**X**", and cell **E18** is **BLANK**. If any other character is in cell **E18**, cell **F18** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G18	**IF** "**Different component integration architectures**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D18** into cell **G18** **OTHERWISE** Set cell **G18** to **0**	=IF(OR(E18="X",F18="I"),$D18,0)	Sets cell **G18** to the DCE weight if an "**x**" is in cell **E18** or an "i" is in cell **F18**. Otherwise, sets cell **G18** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F19	**IF** "**Different technologies**" criterion is selected **OR** "**Different approaches within a technology**" criterion is selected **OR** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **OR BOTH** "**Different architectures**" criterion is selected **AND** "**Different manufacturers of fundamentally different equipment designs**" criterion is selected **AND** "**Different data flow architectures**" criterion is BLANK **THEN** Insert **"i"** in cell **F19** **OTHERWISE** Set cell **F19** to **BLANK**	=IF(AND(OR(E$5="X",E$6="X", E$10="X", AND(E$7="X", E$10="X")),E$19=""),"i", "")	Sets Inherent flag, "i", for cell **F19** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or both cells **E7** and **E10** have an "**X**", and cell **E18** is **BLANK**. If any other character is in cell **E19**, cell **F19** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G19	**IF** "**Different data flow architectures**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D19** into cell **G19** **OTHERWISE** Set cell **G19** to **0**	=IF(OR(E19="X",F19="i"),$D19,0)	Sets cell **G19** to the DCE weight if an "**x**" is in cell **E19** or an "i" is in cell **F18**. Otherwise, sets cell **G19** to **0** for subsequent calculations.
F20	Cell **F20** = cell **G20** * cell **D20**	=G20*$D20	Multiply the sum of the **Logic Processing Equipment** attribute criteria values in cell **G20** by the **Logic Processing Equipment DAE** weight in cell **D20** and place the result in cell **F20**

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G20	Cell **G20** = cell **G16** + cell **G17** + cell **G18** + cell **G19**	=SUM(G16:G19)	**ADD** the **Logic Processing Equipment** attribute criteria values in cells **G16, G17, G18,** and **G19** and place result in cell **G20**
G22	**IF** "**Different underlying mechanisms to accomplish safety function**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D22** into **G22** **OTHERWISE** Set cell **G22** to **0**	=IF(E22="X",$D22,0)	Sets cell **G22** to the DCE weight if an "**x**" is in cell **E22**. Otherwise, sets cell **G22** to **0** for subsequent calculations.
G23	**IF** "**Different purpose, function, control logic, or actuation means of same underlying mechanism**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D23** into **G23** **OTHERWISE** Set cell **G23** to **0**	=IF(E23="X",$D23,0)	Sets cell **G23** to the DCE weight if an "**x**" is in cell **E23**. Otherwise, sets cell **G23** to **0** for subsequent calculations.
G24	**IF** "**Different response time scale**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D24** into **G24** **OTHERWISE** Set cell **G24** to **0**	=IF(E24="X",$D24,0)	Sets cell **G24** to the DCE weight if an "**x**" is in cell **E24**. Otherwise, sets cell **G24** to **0** for subsequent calculations.
F25	Cell **F25** = cell **G25** * cell **D25**	=G25*$D25	Multiply the sum of the **Function** attribute criteria values in cell **G25** by the **Function DAE** weight in cell **D25** and place the result in cell **F25**
G25	Cell **G25** = cell **G22** + cell **G23** + cell **G24**	=SUM(G22:G24)	**ADD** the **Function** attribute criteria values in cells **G22, G23,** and **G24** and place result in cell **G25**

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F27	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **AND** "**Different design organizations/companies**" criterion is BLANK **THEN** Insert **"i"** in cell **F27** **OTHERWISE** Set cell **F27** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X"),E$27=""), "i", "")	Sets Inherent flag, "i", for cell **F27** if an "**X**" or "**x**" is in cell **E5** or cell **E6,** and cell **E27** is **BLANK**. If any other character is in cell **E27**, cell **F27** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G27	**IF** "**Different design organizations/companies**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D27** into cell **G27** **OTHERWISE** Set cell **G27** to **0**	=IF(OR(E27="X",F27="i"),$D27,0)	Sets cell **G27** to the DCE weight if an "**x**" is in cell **E27** or an "i" is in cell **F27**. Otherwise, sets cell **G27** to **0** for subsequent calculations.
G28	**IF** "**Different management teams within the same company**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D28** into **G28** **OTHERWISE** Set cell **G28** to **0**	=IF(E28="X",$D28,0)	Sets cell **G28** to the DCE weight if an "**x**" is in cell **E28**. Otherwise, sets cell **G28** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F29	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **OR** "**Different design organizations/companies**" criterion is selected **AND** "**Different designers, engineers, and/or programmers**" criterion is BLANK **THEN** Insert **"i"** in cell **F29** **OTHERWISE** Set cell **F29** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X",E$27="X"),E$29=""), "i", "")	Sets Inherent flag, "i", for cell **F29** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or cell **E27**, and cell **E29** is **BLANK**. If any other character is in cell **E29**, cell **F29** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G29	**IF** "**Different designers, engineers, and/or programmer**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D29** into cell **G29** **OTHERWISE** Set cell **G29** to **0**	=IF(OR(E29="X",F29="i"),$D27,0)	Sets cell **G29** to the DCE weight if an "**x**" is in cell **E29** or an "i" is in cell **F29**. Otherwise, sets cell **G29** to **0** for subsequent calculations.
F30	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **OR** "**Different design organizations/companies**" criterion is selected **AND** "**Different implementation/validation teams**" criterion is BLANK **THEN** Insert **"i"** in cell **F30** **OTHERWISE** Set cell **F30** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X",E$27="X"),E$30=""), "i", "")	Sets Inherent flag, "i", for cell **F30** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or cell **E27**, and cell **E30** is **BLANK**. If any other character is in cell **E30**, cell **F30** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G30	**IF** "**Different implementation/validation teams**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D30** into cell **G30** **OTHERWISE** Set cell **G30** to **0**	=IF(OR(E30="X",F30="i"),$D30,0)	Sets cell **G30** to the DCE weight if an "**x**" is in cell **E30** or an "i" is in cell **F30**. Otherwise, sets cell **G30** to **0** for subsequent calculations.
F31	Cell **F31** = cell **G31** * cell **D31**	=G31*$D31	Multiply the sum of the **Life-cycle** attribute criteria values in cell **G31** by the **Life-cycle DAE** weight in cell **D31** and place the result in cell **F31.**
G31	Cell **G31** = cell **G27** + cell **G28** + cell **G29**+ cell **G30**	=SUM(G27:G30)	**ADD** the **Life-cycle** attribute criteria values in cells **G27, G28, G29,** and **G30** and place result in cell **G31.**
G33	**IF** "**Different reactor or process parameters sensed by different physical effects**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D33** into G**33** **OTHERWISE** Set cell **G33** to **0**	=IF(E33="X",$D33,0)	Sets cell **G33** to the DCE weight if an "**x**" is in cell **E33**. Otherwise, sets cell **G33** to **0** for subsequent calculations.
G34	**IF** "**Different reactor or process parameters sensed by the same physical effect**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D34** into **G34** **OTHERWISE** Set cell **G34** to **0**	=IF(E34="X",$D34,0)	Sets cell **G34** to the DCE weight if an "**x**" is in cell **E34**. Otherwise, sets cell **G34** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G35	**IF** "**The same process parameter sensed by a different redundant set of similar sensors**" criterion is intentionally selected **THEN** Insert corresponding DCE weight in **D35** into **G35** **OTHERWISE** Set cell **G35** to **0**	=IF(E35="X",$D35,0)	Sets cell **G35** to the DCE weight if an "**x**" is in cell **E35**. Otherwise, sets cell **G35** to **0** for subsequent calculations.
F36	Cell **F36** = cell **G36** * cell **D36**	=G36*$D36	Multiply the sum of the **Signal** attribute criteria values in cell **G36** by the **Signal DAE** weight in cell **D36** and place the result in cell **F36**
G36	Cell **G36** = **G33** + **G34** + **G35**	=SUM(G33:G35)	**ADD** the **Signal** attribute criteria values in cells **G33, G34,** and **G35** and places result in cell **G36**
F38	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **OR** "**Different underlying mechanisms to accomplish safety function**" criterion is selected **OR** "**Different purpose, function, control logic, or actuation means of same underlying mechanism**" criterion is selected **AND** "**Different algorithms, logic, and logic architecture**" criterion is BLANK **THEN** Insert **"i"** in cell **F38** **OTHERWISE** Set cell **F38** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X",E$22="X", E$23="X"),E$38=""), "i", "")	Sets Inherent flag, "i", for cell **F38** if an "**X**" or "**x**" is in cell **E5** or cell **E6** or cell **E22** or cell **E23**, and cell **E38** is **BLANK**. If any other character is in cell **E38**, cell **F38** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G38	**IF** "**Different algorithms, logic, and logic architecture**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D38** into cell **G38** **OTHERWISE** Set cell **G38** to **0**	=IF(OR(E38="X",F38="i"),$D38,0)	Sets cell **G38** to the DCE weight if an "**x**" is in cell **E38** or an "i" is in cell **F38**. Otherwise, sets cell **G38** to **0** for subsequent calculations.
F39	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **AND** "**Different timing or order of execution**" criterion is BLANK **THEN** Insert **"i"** in cell **F39** **OTHERWISE** Set cell **F39** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X"),E$39=""), "i", "")	Sets Inherent flag, "i", for cell **F39** if an "**X**" or "**x**" is in cell **E5** or cell **E6**, and cell **E39** is **BLANK**. If any other character is in cell **E39**, cell **F39** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G39	**IF** "**Different timing or order of execution**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D39** into cell **G39** **OTHERWISE** Set cell **G39** to **0**	=IF(OR(E39="X",F39="I"),$D39,0)	Sets cell **G39** to the DCE weight if an "**x**" is in cell **E39** or an "i" is in cell **F39**. Otherwise, sets cell **G39** to **0** for subsequent calculations.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
F40	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **AND** "**Different runtime environments**" criterion is BLANK **THEN** Insert **"i"** in cell **F40** **OTHERWISE** Set cell **F40** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X"),E$40=""), "i", "")	Sets Inherent flag, "i", for cell **F40** if an "**X**" or "**x**" is in cell **E5** or cell **E6**, and cell **E40** is **BLANK**. If any other character is in cell **E40**, cell **F40** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.
G40	**IF** "**Different runtime environments**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D40** into cell **G40** **OTHERWISE** Set cell **G40** to **0**	=IF(OR(E40="X",F40="i"),$D40,0)	Sets cell **G40** to the DCE weight if an "**x**" is in cell **E40** or an "i" is in cell **F40**. Otherwise, sets cell **G40** to **0** for subsequent calculations.
F41	**IF** "**Different technologies"** criterion is selected **OR** **"Different approaches within a technology"** criterion is selected **AND** "**Different logic languages**" criterion is BLANK **THEN** Insert **"i"** in cell **F41** **OTHERWISE** Set cell **F41** to **BLANK**	=IF(AND(OR(E$5="X", E$6="X"),E$41=""), "i", "")	Sets Inherent flag, "i", for cell **F41** if an "**X**" or "**x**" is in cell **E5** or cell **E6**, and cell **E41** is **BLANK**. If any other character is in cell **E41**, cell **F41** will be set to **BLANK**. This allows the Inherent flag to be cleared if this criterion is not used in the design.

Draft

Table A.7 (continued)

Cell	Pseudo-language logic	Logic	Comments
G41	**IF** "**Different logic languages**" criterion is intentionally or inherently selected **THEN** Insert corresponding DCE weight in cell **D41** into cell **G41** **OTHERWISE** Set cell **G41** to **0**	=IF(OR(E41="X",F41="i"),$D41,0)	Sets cell **G41** to the DCE weight if an "**x**" is in cell **E41** or an "i" is in cell **F41**. Otherwise, sets cell **G41** to **0** for subsequent calculations.
F42	Cell **F42** = cell **G42** * cell **D42**	=G42*$D42	Multiply the sum of the **Logic** attribute criteria values in cell **G42** by the **Life-cycle DAE** weight in cell **D42** and place the result in cell **F42.**
G42	Cell **G31** = cell **G27** + cell **G28** + cell **G29**+ cell **G30**	=SUM(G27:G30)	**ADD** the **Life-cycle** attribute criteria values in cells **G38, G39, G40,** and **G41** and place result in cell **G42.**
E44	Cell **E44** = (cell **F8** + cell **F14** + cell **F20** + cell **F25** + cell **F31**+ cell **F36**+ cell **F42**) * 100	=(F8+F14 +F20+F25+F31+F36+F42) * 100	Calculate the **Score** by adding the **Design** attribute score (cell **F8**), the **Equipment Manufacturer** attribute score (cell **F14**), the **Logic Processing Equipment** attribute score (cell **F20**), the **Function** attribute score (cell **F25**), the **Life-cycle** attribute score (cell **F31**), the **Signal** attribute score (cell **F36**), and the **Logic** attribute score (cell **F42**), scaling the sum by 100 and placing the result into cell **E44**.
E45	Cell **E5** = cell **E44**/cell **G46**	=E44/C46	Normalize the **Score** in cell **E44** by the Mean value (264) determined from the evaluation of the diversity strategies and place the result in cell C**46.**
C46	Place the Mean score from the diversity strategy evaluation in cell **C46**	264	This cell contains the Mean value (264) determined from the evaluation of the diversity strategies.

Draft

Table A.8. Diversity evaluation worksheet example

	Attribute criteria			Category					
				PWR Example			DAS		
		Rank	DCE WT	INT	INH	Score	INT	INH	Score
DESIGN	Design								
	Different technologies	1	0.500			0.000	X		0.500
	Different approaches within a technology	2	0.333			0.000			0.000
	Different architectures	3	0.167			0.000		i	0.167
	DAE WT. and Subtotals		1.000		0.000	0.000		0.667	0.667
EQUIP. MANUF.	Equipment Manufacturer								
	Different manufacturers of fundamentally different equipment designs	1	0.400			0.000		i	0.400
	Same manufacturer of fundamentally different equipment designs	2	0.300			0.000			0.000
	Different manufacturers of same equipment design	3	0.200			0.000			0.000
	Same manufacturer of different versions of the same equipment design	4	0.100			0.000			0.000
	DAE WT. and Subtotals		0.219		0.000	0.000		0.088	0.400

Draft

Table A.8 (continued)

	Attribute criteria			Category					
				PWR Example			DAS		
		Rank	DCE WT	INT	INH	Score	INT	INH	Score
LOGIC PROC. EQUIP.	Logic Processing Equipment								
	Different logic processing equipment architectures	1	0.400			0.000		i	0.400
	Different logic processing versions in same equipment architecture	2	0.300			0.000			0.000
	Different component integration architectures	3	0.200			0.000		i	0.200
	Different data flow architectures	4	0.100			0.000		i	0.100
	DAE WT. and Subtotals		0.625		0.000	0.000		0.438	0.700
FUNCTION	Function								
	Different underlying mechanisms to accomplish safety function	1	0.500	X		0.500	X		0.500
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	X		0.333	X		0.333
	Different response time scale	3	0.167			0.000	X		0.167
	DAE WT. and Subtotals		0.563		0.469	0.833		0.563	1.000

Draft

Table A.8 (continued)

Attribute criteria				Category					
				PWR Example			DAS		
		Rank	DCE WT	INT	INH	Score	INT	INH	Score
LIFE-CYCLE	Life-cycle								
	Different design organizations/companies	1	0.400			0.000		i	0.400
	Different management teams within the same company	2	0.300			0.000			0.000
	Different designers, engineers, and/or programmers	3	0.200			0.000		i	0.200
	Different testers, installers, or certification personnel	4	0.100			0.000		i	0.100
	DAE WT. and Subtotals		0.656		0.000	0.000		0.459	0.700
SIGNAL	Signal								
	Different reactor or process parameters sensed by different physical effects	1	0.500	X		0.500	X		0.500
	Different reactor or process parameters sensed by the same physical effect	2	0.333	X		0.333			0.000
	The same process parameter sensed by a different redundant set of similar sensors	3	0.167			0.000			0.000
	DAE WT. and Subtotals		0.792		0.660	0.833		0.396	0.500

Draft

Table A.8 (continued)

Attribute criteria			Category					
			PWR Example			DAS		
	Rank	DCE WT	INT	INH	Score	INT	INH	Score
LOGIC								
Logic								
Different algorithms, logic, and logic architecture	1	0.400		i	0.400		i	0.400
Different timing or order of execution	2	0.300			0.000		i	0.300
Different runtime environments	3	0.200			0.000		i	0.200
Different logic languages	4	0.100			0.000		i	0.100
DAE WT. and Subtotals		0.672		0.269	0.400		0.672	1.000
Score (x100)			140			328		
Normalized score			0.53			1.24		
Basis for normalizing	264							

Draft