



James H. Riley  
DIRECTOR  
ENGINEERING  
NUCLEAR GENERATION DIVISION

6/11/09  
74 FR 27831

July 10, 2009

(3)

Rulemaking, Directives, and Editing Branch  
Office of Administration  
U.S. Nuclear Regulatory Commission  
Washington, DC 20555-0001

RECEIVED

JUL 10 10 11:46

RULES AND DIRECTIVES  
BRANCH  
UNAS

**Subject:** Diversity NUREG/CR, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems," Request for Comment

**Project Number: 689**

The Nuclear Energy Institute (NEI)<sup>1</sup>, on behalf of the nuclear industry, is submitting the attached response to the June 11, 2009, Federal Register Notice (74 FR 27832) which invited written comments on the Diversity NUREG/CR, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems".

NEI's primary comment is that much of the material is for reference only as related to US nuclear plants. This material could be moved to the appendices. Additionally, there is a need for a clarification of the intended purpose of the document. A spreadsheet containing all our comments is included as an enclosure.

We appreciate the opportunity to comment on the draft document, and we look forward to continued meetings with the Staff where we can address diversity strategies and means to address their adequacy. If you have any questions regarding this matter, please contact me at (202) 739-8137; [jhr@nei.org](mailto:jhr@nei.org) or Gordon Clefton at (202) 739-8086; [gac@nei.org](mailto:gac@nei.org).

<sup>1</sup> NEI is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, nuclear material licensees, and other organizations and individuals involved in the nuclear energy industry.

SUNSI Review Complete

ERIDS = ADM-03

Template = ADM-013

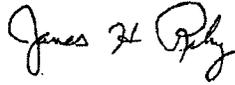
add = m-Waterman (mew)

Rulemaking, Directives, and Editing Branch

July 10, 2009

Page 2

Sincerely,

A handwritten signature in black ink, appearing to read "James H. Riley". The signature is written in a cursive style with a large initial "J" and "R".

James H. Riley

Enclosure

c: Mr. Michael E. Waterman, RES/DE/DICB, NRC  
Mr. Ian C. Jung, NRO/DE/ICE2, NRC  
NRC Document Control Desk

NEI Comment Matrix

Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
1		General	<u>General</u> The purpose and use of the document is not clear. Is it intended to measure the diversity inherent in an overall plant design? Or, is it intended to measure the diversity inherent between a safety-related digital protection system and a diverse system design to satisfy BTP 7-19?	NRC-Clarify purpose of document, explain what type of inherent diversity the document is intended to measure	O	
2		General	<u>General</u> The inclusion of function and signal diversity attributes in the methodology is not on point if the purpose of the document is to support decision-making in the context of BTP 7-19. These attributes are part of any safety-related design 'to the extent practical' and serve no direct purpose for mitigating software common mode failures. As such, they are not relevant to any BTP 7-19 decision.	NRC-Edit function and signal diversity attributes section to fit the purpose of the document (support decision-making in the context of BTP 7-19).	O	
3		General	<u>General</u> The application of function and signal diversity attributes in the methodology is not well defined for use on operating plants. The credit for these attributes is not clearly defined, is not rigorously applied, and appears to be based on anecdotal examples. How does one credit these attributes when the underlying regulation only requires use 'to the extent practical'? There is more signal diversity in reactor trip system designs than in the engineered safety feature system designs (e.g., much less signal diversity for Condition IV events). There are significant differences in NSSS designs with respect functional diversity in reactor trip systems (e.g., diverse scram systems not required for all NSSS designs). No functional diversity for the actuation of ESF equipment. These system characteristics will likely not be affected by the replacement of analog protection systems with digital systems. As such, they are not useful to any BTP 7-19 decision for retrofit designs.	NRC-Specifically define the application of function and signal diversity attributes in the methodology and edit text to show importance in BTP 7-19 decision making.	O	
4		General	<u>General</u> The application of function and signal diversity attributes in the methodology is not well defined for use on new plant designs. It is not clear from the discussion of examples of the three strategies	NRC-Explain whether credit for function and signal diversity is based on characteristics of the safety-related protection	O	

NEI Comment Matrix

Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			<p>whether the credit for function and signal diversity is based on characteristics of the safety-related protection system (independent of the use of a digital platform) or between the safety-related digital system and the diverse protection system (creating additional design expectations for the diverse protection system). If the intent is to assess differences between the safety-related digital system and the diverse protection system, the diversity expectations are not consistent the expectations outlined for diverse protection systems are described in SRP 7.8, which states:</p> <ul style="list-style-type: none"> <li>• Equipment diversity is required from the sensors/transmitters to and including the components used to interrupt control rod power or vent the scram air header.</li> <li>• For interruption of control rod power, obtaining circuit breakers from different manufacturers is not, in and of itself, sufficient to provide the required diversity.</li> <li>• For mitigating systems other than diverse RTSs (e.g., auxiliary feedwater), diversity is required from the sensors to, but not including, the final actuation device.</li> <li>• Sensors need not be of a diverse design or manufacturer.</li> </ul> <p>This inconsistency should be reconciled.</p>	<p>system (independent of the use of a digital platform) or between the safety-related digital system and the diverse protection system (creating additional design expectations for the diverse protection system); If it is based on characteristics between the safety-related digital system and the diverse protection system, lean text to be consistent with the expectations outlined for diverse protection systems are described in SRP 7.8</p>		
5		Executive Summary - Implementation	<p><u>Executive Summary</u>                      Defining the three example strategies as baselines will create confusion regarding what is considered acceptable in a retrofit project. Specifically, the statement that 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</p>	<p>NRC – Edit text of three example strategies to prevent confusion about what is acceptable in a retrofit project</p>	O	

\* = High NEI Priority

### NEI Comment Matrix

Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			(i.e., an acceptable rationale is provided to support mitigation claims)" (emphasis added). This statement can be interpreted as expecting retrofits to existing plants to achieve the same degree of function and signal diversity (i.e., attributes unrelated to the use of a digital platform for the protection system) as new plant designs. The conformance language is used a several points throughout the report.			
6		2.2 ¶ 2	<u>COMMON-CAUSE FAILURE VULNERABILITIES AND DIGITAL SAFETY SYSTEMS AT NUCLEAR POWER PLANTS</u> On page 2-1, how is the discussion of module or component meant to be applied (e.g., for an analog board or a well defined and tested software function block)?	NRC-Clarify how discussion of module or component is meant to be applied	O	
7		2.2 ¶ 4	<u>COMMON-CAUSE FAILURE VULNERABILITIES AND DIGITAL SAFETY SYSTEMS AT NUCLEAR POWER PLANTS</u> On page 2-2, the extension of the discussion to non-software based system clouds the purpose of the document.	NRC-Edit text of non-software based systems in order to prevent it from drifting away from the purpose of the document	O	
8		2.3	<u>COMMON-CAUSE FAILURE VULNERABILITIES AND DIGITAL SAFETY SYSTEMS AT NUCLEAR POWER PLANTS</u> In Section 2.3, the extensive discussion involving NUREG/CR-6303 and BTP 7-19 implies that the purpose of the document is to support decision making for diverse protection systems requirement to mitigate software common mode failures.	NRC-Edit text of discussion involving NUREG/CR-6303 and BTP 7-19 to strictly follow purpose of document	O	
9		3.1.1 ¶ 4	<u>DIVERSITY IN NONNUCLEAR INDUSTRIES</u> On page 3-2, the statement "Clearly, the absence of expected action is much more discernable than that of an unusual action" is not supported or reasonable.	NRC-Support given statement	O	
10		4 (page 4-1)	<u>DIVERSITY USAGE IN INTERNATIONAL NUCLEAR POWER INDUSTRY</u> On page 4-1, the discussion to non-software based system clouds the purpose of the document. It should also be noted that the ATWS rule established diverse protection for a limited set of higher probability transients coupled with a failure of the protection system. It did not establish any broader treatment of common cause failures.	NRC-Edit text to strictly follow purpose of the document; Correct wording of ATWS rule	O	

\* = High NEI Priority

NEI Comment Matrix  
Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C  
Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
11		4.1.1	<u>DIVERSITY USAGE IN INTERNATIONAL NUCLEAR POWER INDUSTRY</u> On page 4-2, the discussion on the traditional use of signal and equipment diversity overstates the implementation. For example, there is much less signal diversity for Condition IV events). There are significant differences in NSSS designs with respect functional diversity in reactor trip systems (e.g., diverse scram systems not required for all NSSS designs). No functional diversity for the actuation of ESF equipment.	NRC-Edit text to correctly explain, not exaggerate, content of the discussion on the traditional use of signal and equipment diversity	O	
12		4.2.2 ¶ 1	<u>DIVERSITY USAGE IN INTERNATIONAL NUCLEAR POWER INDUSTRY</u> On page 4-9, it should be noted that the Sizewell example of implementation of the Eagle digital technology (and used as baseline strategy example A) is not representative of the use of that technology in the US operating fleet.	NRC-Include given detail in description of Sizewell Nuclear Power Station	O	
13		4.2.8	<u>DIVERSITY USAGE IN INTERNATIONAL NUCLEAR POWER INDUSTRY</u> On page 4-32, the EPR designation should be used without the European or evolutionary descriptors.	NRC-Remove European and evolutionary descriptors from EPR designation	O	
14		5.1.1 ¶ 4	<u>INTERNATIONAL CONTRIBUTIONS TO DIVERSITY</u> On page 5-1, is it correct to refer to the FPGA-based system as a hardwired system?	NRC-Defend decision to refer to the FPGA-based system as a hardwired system or correct statement	O	
15		5.1.1 ¶ 5	<u>INTERNATIONAL CONTRIBUTIONS TO DIVERSITY</u> On page 5-2, the use of diversity at the Sizewell B NPP in the United Kingdom is described as "the most extensive example available from presently operating international NPPs." Sizewell is used as example strategy A. Is it an appropriate standard to measure conformance when assessing the acceptability of a diverse protection system?	NRC-Defend given statement or edit it if it is not an appropriate standard to measure conformance when assessing the acceptability of a diverse protection system	O	
16		6.1.2.1 ¶ 3	<u>DIVERSITY STRATEGIES</u> On page 6-2, the report notes that 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	NRC-Remove given excerpt from document or connect it to a BTP 7-19 decision; Make text consistent with NRC Digital I&C lessons learned workshop	O	

\* = High NEI Priority

NEI Comment Matrix  
Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C  
Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			considerations related to the accommodation of the unique characteristics of digital technology." This statement seems to imply that these attributes are measured for the existing safety-related system. As such, they are not relevant to any BTP 7-19 decision. Comment 3 above discusses the difficulty is assessing this attribute for existing design. It should be noted that in the recent NRC Digital I&C lessons learned workshop, two NRC members discussed the application of the NUREG methodology to the Oconee project; neither person credited signal diversity in their assessment. This point underscores the difficulty in understanding and applying the methodology, since signal diversity is an element of the existing reactor protection system design.			
17		6.2 (page 6-5); 6.3.2 (6.15-6.18)	<u>DIVERSITY STRATEGIES</u> On pages 6-5 and 6-15 through 6-18, the conclusion that both CPU and FPGA-based technologies different approaches within a technology is not appropriate. The significant differences in (fundamentally different chips, uses of firmware or software, different development processes, different development tools, etc.) more readily supports a conclusion that they are different technologies. CPU-based systems developed by different vendors with different tools and different operating systems and function block libraries are a better example of different approaches within a technology. Similarly, FPGA-based systems developed by different vendors with different tools are a better example of different approaches within a technology.	NRC-Correct conclusion concerning relationship between CPU-based systems and FPGA-based systems	O	
18		6.3.1 ¶ 2	<u>DIVERSITY STRATEGIES</u> On page 6-6, the statement "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 ..." is incorrect. The use of function and signal diversity addresses common cause failure concerns related to specifications and analytical knowledge, not hardwired system vulnerabilities. Similarly, the ATWS rule established diverse protection for a limited set of higher probability transients coupled with a failure of the protection	NRC-Correct given statement	O	

\* = High NEI Priority

NEI Comment Matrix  
Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C  
Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			system; it did not establish any broader treatment of common cause failures for hardwired systems.			
19		6.3.2.2.2 ¶ 3	<p><u>DIVERSITY STRATEGIES</u> On page 6-18, the statement below is not correct:</p> <p>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.</p> <p>CPU-based software cannot be used to generate a FPGA-based solution. Common functional requirement specifications may be used; however, that is not a unique digital technology attribute.</p>	NRC-Correct given statement	O	
20		6.4.2 ¶ 4	<p><u>DIVERSITY STRATEGIES</u> On page 6-41, the particular use of 'common personnel involved in one or more phases of each platform's lifecycle' creates confusion as to the expectations for implementation of different design teams. Consider the following scenarios:</p>	NRC-Prevent confusion in section by integrating given scenarios into content	O	

\* = High NEI Priority

NEI Comment Matrix

Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			<ul style="list-style-type: none"> <li>Is every person who ever worked on a software module for a generic platform, with many software modules and an ongoing maintenance lifecycle, forever excluded from working on a companion diverse protection system?</li> <li>Is an electrical engineer who worked on the physical wiring of a digital protection system excluded from working on the physical wiring of the diverse protection system?</li> <li>Is a software engineer who worked for one vendor of the safety related protection system later excluded from working on a diverse digital protection system with another vendor?</li> </ul> <p>The expectations for the implementation and verification of different design teams should be clarified.</p>			
21		8 (page 8-2)	<p><u>References</u> On page 8-2 – The reference to www.nasa.gov is not specific or useful.</p>	NRC-Remove reference or edit it to reference a specific article or section	O	
22		8 (page 8-3)	<p><u>References</u> On page 8-3 – Wikipedia is not an appropriate source of information, since it can be continually modified.</p>	NRC-Remove reference and ensure that any information in the document obtained from Wikipedia is supported by a more reliable source	O	
23		A.3.2 ¶ 2	<p><u>Appendix A</u> On page A-9, the first assumption “that the frequency of diversity attribute usage represents consensus on the effectiveness of a diversity attribute to address observed or potential CCFs” is not valid. The report ignores an important contributor to the selection of diverse protection system designs: the availability of useful and accepted technology. The dated nature of the diversity examples considered introduces a bias against newer technologies. As a consequence, the weighting factor show in Table A.3 indicates a preference for non-digital technology (weight of</p>	NRC-Lean text to point to specific section of SRP Appendix 7.1-C, rather than duplicating words.	O	

\* = High NEI Priority

NEI Comment Matrix

Reference: NUREG/CR-XXXX, Diversity Strategies for Nuclear Power Plant I&C Systems

#	COMMENT DATE	ISG SECTION	COMMENT	ACTION	STATUS	DISPOSITION
			0.500) over alternate digital technologies (weight of 0.333). This preference is not consistent with the position taken by the Commission in the SRM to SECY-93-087 to not favor non-digital solution.			
24		A.5.1.2 (page A-18)	<u>Appendix A</u> Figure A.1 -- Lungmen is shown twice on the chart.	NRC-Remove one instance of Lungmen	O	
25		Sections 3,4,5	<u>General</u> Sections 3, 4, and 5 amount to about 40% of the document volume and pertain to diversities in non-nuclear industries or to international diversity usage and contributions. Due to the general nature of this added material, it is recommended that these sections be moved to an appendix.	NRC-Move sections 3,4, and 5 to an appendix	O	
26	26 Jun 09	Foreword	<u>Foreword</u> It is recommended that the NUREG Foreword be amended to clarify upfront the intended purpose of each section or group of sections.	NRC-Amend Foreword to specify what each section is about	O	