NUCLEAR ENERGY INSTITUTE

6/22/2010

75 FR 35508

2

John C. Butler
DIRECTOR
ENGINEERING & OPERATIONS SUPPORT
NUCLEAR GENERATION DIVISION

August 20, 2010

Ms. Cynthia K. Bladey
Chief, Rules, Announcements, and Directives Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Comments on Draft Regulatory Guide, DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants" (*Federal Register* of June 22, 2010, 75 FR 35508) Docket ID NRC–2010–0216.

Project Number: 689

Dear Ms. Bladey:

On behalf of the nuclear energy industry, the Nuclear Energy Institute (NEI)[1] submits comments on the subject Draft Regulatory Guide (DG). These comments represent both operating power reactor and new plant perspectives. The industry appreciates the opportunity to review and comment on the draft guide. Based upon the complexity of separating the provisions of this regulatory guide and 10CFR73.54, we encourage the staff to consider a public workshop to assist in refining the content.

Industry agrees that DG-1249 should address a secure development environment to protect against undocumented, unneeded, and unwanted modifications, as well as design features to protect against a predictable set of undesirable acts. It should not address the physical environment or operation and maintenance of digital safety systems, as this is covered by 10CFR73.54, NEI 08-09, and Regulatory Guide (RG) 5.71. The use of the attached comments is expected to further this separation between computer security and cyber security.

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

SUNSI Review Complete

E-RIDS = ADM-03

1776 I Street, NW | Suite 400 | Washington, DC | 20006-3708 | P: 202.739.8108 | F: 202.533.0113 | jcb@nei.org | www.nei.org

Template = ADM-013

Add = T. Goodman (TXM7)
M. Case (MJC)
S. Aggarwal (SKA)

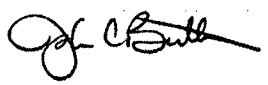
Typically, in regulatory guides that endorse IEEE standards, the regulatory positions are linked directly to specific clauses of the standard to which the staff position is providing additions, exceptions or clarifications. Such linkage is missing in DG-1249.

- RG 5.71 and NEI 08-09 describe how to protect critical digital assets (and data) in the operating plant, including an aggressive treatment of access controls. DG-1249 should reference RG 5.71 Appendix B, Section B.1 for control of access to digital safety systems as an acceptable method for meeting clause 5.9 of IEEE-603.
- DI&C-ISG-04 describes how to demonstrate communications independence. DG-1249 should reference DI&C-ISG-04 as an acceptable method for meeting clause 5.6.3 of IEEE-603.

Additional comments on the draft regulatory guide are attached.

If you have any questions, please feel free to contact me at (202) 739-8108; jcb@nei.org or Gordon Clefton at (202) 739-8086; gac@nei.org.

Sincerely,



John C. Butler

Attachment

DG-1249 Comments

ID	Section, Page, and Line #	Comment	Proposed Resolution
1	Section B Page 3 of 11 Paragraph 2	"The justification for equipment diversity or for the diversity of related system software, such as a real-time operating system, must extend to equipment components to ensure that actual diversity exists. For example, different manufacturers might use the same processor or license the same operating system, thereby introducing the possibility of common failure modes." As written, this implies a requirement for hardware diversity. It should be clear that hardware diversity is only needed as necessary to achieve software diversity.	Revise to read as follows: "The justification for diversity of system software, such as a real-time operating system, must extend to equipment components to ensure that actual diversity exists. ....'
2	Section B Page 3 of 11 Paragraph 5	"For this reason, any software providing nonsafety functions that resides on a computer providing a safety function must be classified as a part of the safety system. If a licensee wants a safety-related computer system to perform a nonsafety function, it must classify the software that performs the nonsafety function as safety-related software with all the attendant regulatory requirements for safety software, including communications independence from other nonsafety software." IEEE-603 requires non-safety functions residing on a safety computer to be considered Class 1E, only if the software also performs a safety function. For example, the bidirectional software for non-safety functions, which resides in a separate communication processor for compliance to	Revise to read as follows: 'For this reason, any software that resides on a computer providing a safety function, that performs a non-safety function and is also credited to function correctly to protect the safety function, must be classified as a part of the safety system, with all the attendant regulatory requirements for safety software. If a licensee wants a safety-related computer system to perform a non-safety function and classify that software as non-safety, it must demonstrate that the safety function protects itself against any failure in that software that could adversely affect the safety function.'

ID	Section, Page, and Line #	Comment	Proposed Resolution
		DI&C-ISG-04, must be Class 1E because the communication error detection functions within those processors credited to protect the safety function. However, if the safety processor protects the safety function by only providing deterministic outbound communication and the communication processor only provides communication handshaking for unidirectional outbound communication, the communication processor would not be credited to protect the safety function; therefore it would not need to be Class 1E. Similarly, functions within protection processors that are used only for status information and alarming are not considered Class 1E as long as there is no credit for their correct operation to not interfere with the safety function (i.e., the safety function must protect itself).	
3	Section B Page 4 of 11 Paragraph 1	"Consequently, the NRC modified Regulatory Guide 1.152, Revision 2, to include regulatory positions that provide specific guidance concerning the protection of the design and development phases of computer-based safety systems, which is intended to address the criteria within these clauses." There is no clear connection to show that "protection of design and development phases" will address the criteria within clauses 5.6.3 (independence) and 5.9 (access control) of IEEE-603.	RG 5.71 and NEI 08-09 describe how to protect critical digital assets (and data) in the operating plant, including an aggressive treatment of access controls. DG-1249 should simply reference RG 5.71 Appendix B, Section B.1 for control of access to digital safety systems as an acceptable method for meeting clause 5.9 of IEEE-603. DI&C-ISG-04 describes how to demonstrate communications independence. DG-1249 should simply reference DI&C-ISG-04 (or the final durable guidance) as an acceptable method for meeting clause 5.6.3 of IEEE-603.

ID	Section, Page, and Line #	Comment	Proposed Resolution
4	Section B Page 4 of 11 Paragraph 1	"Consequently, the NRC modified Regulatory Guide 1.152, Revision 2, to include regulatory positions that provide specific guidance concerning the protection of the design and development phases of computer-based safety systems, which is intended to address the criteria within these clauses." The term "phase" is meaningless in the context of security and protection. Security is about protecting data and assets.	Revise to read as follows: 'Consequently, the NRC modified Regulatory Guide 1.152, Revision 2, to include regulatory positions that provide specific guidance concerning the protection of the assets and data in the design and development phases of computer-based safety systems, which is intended to address the criteria within these clauses."
5	Section B Page 4 Paragraph 1 fourth sentence	"DG-1249 clarifies that these regulatory positions are specifically concerned with the access controls and protective measures applied to the development of digital safety systems and with the ability of protective features within the system to provide a secure operating environment such that system integrity and reliability are maintained in the event of inadvertent operator actions and undesirable behavior of connected equipment. This guide is not intended to address the ability of those protective features to thwart malicious cyber attacks." It is not possible for designers to protect against unbounded inadvertent operator actions or incredible concurrent failures of connected equipment.	Revise to read as follows: 'These regulatory positions are specifically concerned with the access controls and protective measures applied to the development of digital safety systems and with the ability of protective features within the system to provide a secure operating environment such that system integrity and reliability are maintained in the event of a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems). This guide is not intended to address the ability of those protective features to thwart malicious cyber attacks.'
6	Section B Page 4 of 11 Paragraph 1	"The requirements of 10 CFR 73.54 address cyber security of digital safety systems." 10CFR73.54 addresses more than the	Rewrite this sentence to more clearly describe the scope of 10CFR73.54 and that the scope of DG-1249 is limited to addressing a secure development environment to protect against undocumented, unneeded, and unwanted modifications, as well as features to protect against a

ID	Section, Page, and Line #	Comment	Proposed Resolution
		"cyber security of safety systems." It addresses cyber security of all critical digital assets in Safety, Security, and Emergency Planning (SSEP) systems.	predictable set of undesirable acts.
7	Section B Page 4 of 11 Paragraph 2	"Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 3), provides guidance to meet the requirements of 10 CFR 73.54." 10CFR73.54 does not identify the nature of a cyber attack. It does not distinguish "malicious" from any other form of attack. It does require protection of critical assets in SSEP systems; RG 5.71 and NEI 08-09 provide an approved method for meeting 10CFR73.54. RG 5.71 and NEI 08-09 provide thorough, aggressive, and prescriptive methods for protecting critical assets and data in the O&M phase. 10CFR73.54, RG 5.71, and NEI 08-09 provide all of the necessary rules and guidance for protecting SSEP systems in the O&M phase, regardless of the nature of an intended or unintended act by a human being.	Revise to read as follows: 'Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities" (Ref. 3) and NEI 08-09 rev 6, provide guidance to meet the requirements of 10 CFR 73.54.'
8	Section B Page 4 of 11 Bullet 1	DG-1249 has not clearly explained how its Regulatory Positions 2.1 through 2.5 achieve the SDOE and why requirements contained in IEEE Std 7-4.3.2 and other IEEE Standards do not achieve the same performance objectives.	With DG-1249 endorsing IEEE Standard 7-4.3.2 , the regulatory positions linked directly to specific clauses of the Standard would show how Regulatory Positions 2.1 through 2.5 achieve the SDOE.
9	Section B Page 4 of 11	"These SDOE actions may include adoption of protective design features into the digital	Revise to read as follows:

ID	Section, Page, and Line #	Comment	Proposed Resolution
	Bullet 1	safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational." Physical access controls are already addressed in NEI 08-09 and RG 5.71 Appendix B Section B.1. They not distinguish "inadvertent access" from advertent access. Access controls per RG 5.71 and NEI 08-09 are adequate for any form of physical access. "Undesirable behavior from connected systems" is addressed in DI&C-ISG-04.	'These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent electronic access to the system and/or protection against undesirable behavior from connected systems as addressed in DI&C-ISG-04.'
10	Section B Page 4 of 11 Bullet 2	""Cyber security" refers to those measures and controls, implemented to comply with 10 CFR 73.54, to protect digital systems against the malicious acts of an intelligent adversary up to and including the design basis threat, as defined by 10 CFR 73.1." 10CFR73.54 does not distinguish "malicious" attacks from other attack forms and it does not attempt to define attack vectors. Nor does it use the term "intelligent adversary." The problem is that using terms like "malicious" and "intelligent adversary" to distinguish the applicability of DG-1249 from the applicability of 10CFR73.54 (and RG 5.71) will require carefully developed definitions of these terms. Who is to say if an act is malicious? What is an intelligent adversary?	Remove the words "...the malicious acts of an intelligent adversary..." from Bullet 2. Also, replace the phrase "digital systems" with the phrase 'Critical Digital Assets in SSEP systems' to more clearly describe the scope of 10CFR73.54.

ID	Section, Page, and Line #	Comment	Proposed Resolution
		Attempting to distinguish the applicability of DG-1249 from 10CFR73.54 also borders on redefining the scope of 10CFR73.54 as applicable only to malicious attacks by intelligent adversaries.	
11	Section B Page 4 of 11 Paragraph 4	"The NRC's intention is that the combination of this regulatory guide and the programmatic provisions under 10 CFR 73.54 should seamlessly address the secure design, development, and operation of digital safety systems." Industry agrees DG-1249 should address a secure development environment to protect against undocumented, unneeded, and unwanted modifications, as well as design features to protect against a predictable set of undesirable acts. It should not address the physical environment or operation and maintenance of digital safety systems, as this is covered by 10CFR73.54, NEI 08-09, and RG 5.71. Sentence 1 is not clear on this point.	Add to this sentence to clarify that • DG-1249 applies to the secure development environment to protect against undocumented, unneeded, and unwanted modifications, as well as design features to protect against a predictable set of undesirable acts and • 10CFR73.54, NEI 08-09, and RG 5.71 address the physical environment or operation and maintenance of digital safety systems.
12	Section B Page 5 of 11 Paragraph 2	"The regulatory guide provides guidance for designing digital systems (hardware and software) such that they are free from vulnerabilities…"	Revise to read as follows: 'The regulatory guide provides guidance for designing digital systems (hardware and software) such that they are free from known vulnerabilities…"
13	Section B Page 5 of 11 Paragraph 2	"In the context of this regulatory guide, vulnerabilities are considered to be 1) deficiencies in the design that may allow inadvertent, unintended, or unauthorized	Revise to read as follows: 'In the context of this regulatory guide, vulnerabilities are considered to be 1) deficiencies in the design that may allow inadvertent, unintended,

ID	Section, Page, and Line #	Comment	Proposed Resolution
		access or modifications to the safety system that may degrade the reliability, integrity or functionality of the safety system during operations or 2) an inability of the system to sustain the safety function in the presence of undesired behavior of connected systems." DG-1249 says that vulnerabilities are considered to be those that may allow inappropriate access or an inability to sustain a safety function in the presence of undesired behavior of connected systems. These topics are already addressed in RG 5.71, NEI 08-09, and DI&C-ISG-04, by prescribing methods and features that are necessary to preclude inappropriate physical access.	or unauthorized electronic access or modifications to the safety system…'
14	Section B Page 5 of 11 Paragraph 2	"The considerations for hardware access control should include physical access control, configuration of modems, connectivity to external networks, data links, and open ports." Access control and other features necessary to eliminate security vulnerabilities are already addressed in RG 5.71 and NEI 08-09.	Revise to read as follows: 'In accordance with the guidance of RG 5.71 and NEI 08-09, the considerations for hardware access control should include physical access control, configuration of modems, connectivity to external networks, data links, and open ports.'
15	Section B Page 5 of 11 Paragraph 2	"The licensee can provide a secure development and operational environment for digital systems…" Rewording would reflect the reality that the licensee is rarely the developer.	Revise to read as follows: 'The licensee should ensure that a secure development environment is used and the licensee must provide a secure operational environment for digital systems…'

ID	Section, Page, and Line #	Comment	Proposed Resolution
16	Section B Page 5 of 11 Paragraph 2	"... (1) by designing features that will meet the licensee's secure operational environment requirements for the systems..." It is important to also meet the NRC's requirements for a secure operational environment.	Revise to read as follows: '... (1) by designing features that will meet the secure operational environment requirements for the systems...'
17	Section B Page 5 of 11 Paragraph 2	"...(3) by maintaining a secure operational environment for digital safety systems in accordance with the station administrative procedures and other licensee's programs to protect against unwanted and unauthorized access or changes to these systems." Item (3) discusses the Operations and Maintenance phases which are out of the scope of DG-1249.	Revise to read as follows: '... (3) by maintaining a secure development environment for digital safety systems in accordance with the developer's administrative procedures and other developer's programs to protect against unwanted and unauthorized access or changes to the development environment.'

18	Section C Pages 6-10 of 11	There is no nexus between the DG-1249 regulatory positions provided and any clauses within IEEE Std 7-4.3.2. Typically, in NRC Regulatory Guides that endorse IEEE standards, the regulatory positions are linked directly to specific clauses of the standard to which the staff position is providing additions, exceptions or clarifications. Examples of such regulatory guides are as follows: • RG 1.8, "Qualification and Training of Personnel for Nuclear Power Plants • RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" • RG 1.172, "Software requirements Specifications for Digital Computer Software Use in Safety Systems of Nuclear Power Plants" • RG 1.205, "Risk-Informed, Performance-Based Fire Protection for Existing Light-Water Nuclear Power Plants" • RG 1.210, "Qualification of Safety-Related Battery Chargers and Inverters for Nuclear Power Plants" • RG 1.211, "Qualification of Safety-Related Cables and Field Splices for Nuclear Power Plants"	The DG-1249 regulatory positions should be revised such that there is a clearly stated link between each position and a clause of IEEE Std 7-4.3.2. There are three possible clauses that these regulatory positions may pertain to: 5.3 Quality, 5.6 Independence, and 5.9 Control of Access. Additionally, the regulatory position section should be revised to provide specific additions, exceptions, or clarifications to these specific clauses. 5.3. Quality • System integrity – no undocumented code, unwanted functions or applications • No dead code • Validation of code • Testing/Scanning • COTS 5.6 Independence • Connected systems • No undesirable behavior from connected systems 5.9 Control of Access • Physical and Logical Access • No remote access • No inadvertent access
19	Section C Pages 6-10 of 11	Eliminate all references to assessments. Guidance for assessments, verification, validation, reviews, and audits is contained in RG 1.168 which endorses IEEE Std 1012-1998.	Revise RG 1.152 to reference RG 1.168 in lieu of additional assessments. Provide additions, exceptions, or clarifications to the existing clauses of IEEE Std 7-4.3.2 that relate to the specific Regulatory Position.

20	Section C Page 6 of 11 *Paragraph 1*	DG-1249 provides no guidance regarding implementation if the digital safety system's *design occurred prior to the effective date of* RG 1.152. This is particularly of concern where the regulatory position includes the provision of performing an assessment when one may not have been done in prior years.	Provide guidance on acceptable measures as alternatives to stated regulatory provisions. In the alternatives, delete references to life cycle phases in favor of simply providing additions, exceptions, or clarifications to the existing clauses of IEEE Std 7-4.3.2.
21	Section C Page 6 of 11 Paragraph 2	Item 5 should reference DI&C-ISG-04 for guidance on communication independence.	Add the reference to DI&C-ISG-04.
22	Section C Page 7 of 11 Paragraph 1	"The NRC will evaluate the secure development environment controls applied to safety system development through the test phase and any secure operational environment design features intended to ensure reliable system operation included in a submittal as part of its review of a license amendment request, design certification, or combined license application." There is nothing in DG-1249 that states what controls and features are acceptable.	Identify examples of controls and features that are acceptable to staff for protecting assets and data used in the design and development of qualified products and safety systems.
23	Section C Page 7 of 11 Paragraph 2	The guidance in sections 2.1 - 2.5 can be followed for new software and new products. An additional section should be added to explain the guidance the NRC will use to evaluate legacy products that were developed prior to the issuance of this Regulatory Guide.	Add new Regulatory Position section(s) for legacy products.
24	Section C Page 7 of 11 Item 2.1 & Item 2.2	Since these may have separate responsibilities, care must be taken to use these terms appropriately: "licensee and developer".	Eliminate references to "licensee and developer" when tasks should be separated, by referring to the task to be accomplished by either or both. For example: 'An assessment should be performed by the licensee or developer to identify the digital safety system's . . . .'

		The content of an application is covered by DI&C-ISG-06.	Eliminate reference to content of an application as this is covered by DI&C-ISG-06.
25	Section C Page 7 of 11 Item 2.1	"Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems."	The documents associated with these NRC positions and guidance should be listed.
26	Section C Page 7 of 11 Item 2.2.1	The term "secure operating environment" is not used the same in this section as the "secure operational environment" term used elsewhere in the document.	Replace with 'secure development and operational environment (SDOE)', if that is what is intended.
27	Section C Page 7 of 11 Item 2.2.1	"Therefore, the verification and validation process of the overall system should ensure the correctness, completeness, accuracy, testability, and consistency of the system secure operational environment design feature requirements." This sentence should only discuss the verification activities conducted during this phase. Validation is conducted during the testing phase.	Revise to read as follows: 'Therefore, the verification process of the requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system secure development and operational environment feature requirements.'
28	Section C Page 8 of 11 Item 2.2.2	"During the development of requirements, measures should be taken to ensure that the requirements development processes and documentation are secure such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system." It makes no sense to discuss coding during the requirements phase. There is no code development or code review.	Revise to read as follows: 'During the development of requirements, measures should be taken to ensure that the requirements development processes and documentation are secure such that the system does not contain unwanted functions or applications that could adversely impact the integrity or reliability of the digital safety system.'

29	Section C Page 8 of 11 Item 2.3.1	"Design configuration items that incorporate predeveloped software into the safety system should address how the predeveloped software will not challenge the secure operational environment for the safety system." This sentence implies that designers must assume predeveloped software contains malicious code; therefore, the rest of the system must protect itself. This is not practical.	Revise to read as follows: 'Design configuration items that incorporate predeveloped software into the safety system should address how the predeveloped software will be demonstrated to be free of malicious code and therefore does not challenge the secure operational environment for the safety system. Predeveloped software can be demonstrated to be free of malicious code by evaluation of its development environment to ensure adequate security or by code inspection. Demonstration by evaluation of operating history may also be acceptable, with strong consideration of configuration controls and application similarity. After predeveloped software is accepted into the secure development environment, it should be controlled to the same extent as newly developed software.'
30	Section C Page 8 of 11 Item 2.3.2	"The developer should delineate the standards and procedures that will conform with applicable design controls to ensure that the system design products (hardware and software) do not contain undocumented code (e.g., backdoor coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital safety system." It makes no sense to discuss coding during the design phase. There is no code development or code review.	Revise to read as follows: ' During the development of requirements, measures should be taken to ensure that the system design products (hardware and software) do not contain unwanted functions or applications that could adversely impact the reliable operation of the digital safety system.'
31	Section C Page 9 of 11 Item 2.4.2	"In such cases, unless the application developer can modify such systems, the development activity should ensure that the features within the operating system do not compromise the required secure operational environment design features of the system in such a manner that the reliability of the digital safety system would be degraded."	Add as follows: 'Proprietary Commercial Off the Shelf (COT) software can be demonstrated to be free of malicious code by evaluation of its development environment to ensure adequate security. Demonstration by evaluation of operating history may also be acceptable, with strong consideration of configuration controls and application similarity.'

		The NRC should clarify their expectations. What is expected of the developer to ensure proprietary Commercial Off the Shelf (COT) systems are free of malicious code?	
32	Section C Page 9 of 11 Item 2.4.2	"... the development activity should ensure that the features within the operating system..." It is suggested that the word 'known' be inserted in front of "features within the operating system" to produce a requirement that can be implemented.	Revise to read as follows: "... the development activity should ensure that the known features within the operating system..."
33	Section References Page 11 of 11 Reference	Reference Section does not mention DI&C-ISG-04.	Revise to add reference DI&C-ISG-04, "Highly-Integrated Control Rooms—Communications Issues (HICRc)"