

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
1	NEI	General	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.		<p>Disagree.</p> <p>The NRC staff recognizes that design features that are credited for establishing independence of the safety system from connected systems and/or precluding inadvertent access to the safety system may also serve cyber security functions as well. Such features, when submitted as part of a Part 50 review, would only be reviewed for their ability to meet the provisions of Regulatory Guide 1.152. No judgments regarding a design features' ability to thwart a cyber attack will be made as part of the Part 50 licensing action.</p> <p>Although RG 5.71 provides guidance on technical controls that should be applied to meet the requirements of 10 CFR 73.54 against cyber threats, meeting 10 CFR 73.54 does not automatically equate to meeting 10 CFR 50.55a(h). 10 CFR 50.55a(h), which incorporates by reference IEEE Std. 603-1991, has specific requirements for providing protective measures against non-malicious acts, such as unintended access or modification to the system or unexpected behavior of connected systems. Clause 5.9 of IEEE Std. 603-1991 requires licensees to have administrative control of access to safety system equipment that are supported by provisions in the generating station design. Clause 5.6.3 of IEEE Std. 603-1991 requires</p>	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
					independence between safety and non-safety systems. The staff recognizes that these administrative controls and provisions in the system design do not have to address malicious intent, but they do have to account for unintentional acts by personnel associated with facility operation that may impact safety functions. As such, any operational vulnerability that may allow personnel or connected non-safety systems to degrade or prevent the performance of safety functions should be identified and addressed by administrative controls that are supported by design features in or around the safety system.	
2	NEI	General	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.		Partially agree; however, no changes are warranted. While DI&C-ISG-04 does contain useful guidance to establish system independence from connected systems, the staff did not specifically reference any ISGs since these guidance documents are "interim" (i.e., the staff expects to incorporate these provisions and criteria into other formal documents). Consideration would be given to referencing non-interim documents containing the ISG-04 guidance in future revisions to RG 1.152.	No change.
3	NEI	Section B, Page 3, 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.	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	Disagree; this comment is beyond the scope of this revision. The language in DG-1249 is equivalent to the wording in RG 1.152, Rev 2. Component diversity	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			<p>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.</p>	<p>actual diversity exists . . . "</p>	<p>was not within the intended scope of this revision.</p> <p>IEEE Std. 7-4.3.2-2010 provides additional guidance regarding component diversity. The NRC staff intends to develop another revision to RG 1.152 to endorse appropriate sections of IEEE Std. 7-4.3.2-2010.</p>	
4	NEI	Section B, Page 3, Paragraph 5	<p>"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, against any failure in that software that could adversely affect the safety including communications independence from other nonsafety software." IEEE-603 requires non-safety functions residing on a safety computer to be considered Class 1 E, only if the software also performs a safety function. For example, the bidirectional software for nonsafety functions, which resides in a separate communication processor for compliance to DI&C-ISG-04, must be Class 1 E because the communication error detection functions within those processors credited to protect the safety</p>	<p>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.'</p>	<p>Disagree; this comment is beyond the scope of this revision.</p> <p>The language in DG-1249 is equivalent to the wording in RG 1.152, Rev 2. Minor edits were made to make the language more consistent with IEEE 603. Modifying this IEEE 603 guidance was not within the intended scope of this revision.</p> <p>Classification of non-safety functions that reside on safety systems as part of the safety system is rooted in the requirement of IEEE Std. 603-1991. Per the requirements of Clause 5.6.3 of IEEE Std. 603-1991, equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.</p> <p>IEEE Std. 7-4.3.2-2010 further specifies that for digital systems, software performing safety functions and software performing non-safety functions may reside on the same computer and use the</p>	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			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 1 E 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).		same computer resources. The non-safety software functions shall be developed in accordance with the safety-related requirements of this standard. The NRC staff intends to develop another revision to RG 1.152 to endorse appropriate sections of IEEE Std. 7-4.3.2-2010.	
5	NEI	Section B, Page 4, 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.	Disagree. See Response to Comment #1 Also, note that RG 1.152 states that it provides guidance on implementation of Criterion III, "Design Control," of Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," which does address design and development.	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
6	NEI	Section B, Page 4, 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.'	Agree in part. The intent of this sentence is to discuss the protection of the development process throughout the lifecycle of the safety system. It is not only restricted to protecting the assets and data, but also includes the development environment and activities as well as protection from unexpected behavior of connected equipment. By protecting the development lifecycle, the assets and data should also be protected. In addition, definitions for assets and data have not been included in this revision.	No change.
7	NEI	Section B, Page 4, Paragraph 1	"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 undesirable acts (e.g., inadvertent operator actions or the undesirable 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.'	Disagree. The discussion in Section B, Page 4, 1 st bullet clarifies that this addresses "protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations". The vulnerability assessment stipulated in Section C.2.1 should identify with reasonable assurance a rational, predictable set of non-malicious acts.	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
8	NEI	Section B, Page 4, Paragraph 1	"The requirements of 10 CFR 73.54 address cyber security of digital safety systems." 10 CFR 73.54 addresses more than the "cyber security of safety systems." It addresses cyber security of all critical digital assets in Safety, Security, and Emergency Planning (SSEP) systems.	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 predictable set of undesirable acts.	Agree	Sentence revised to read: "The requirements of 10 CFR 73.54 address cyber security of digital assets, which include those systems used to perform safety and important to safety, security, and emergency preparedness functions."
9	NEI	Section B, Page 4, 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.'	Disagree. See Response to Comment #1 Please note: this guide is intended to provide guidance for meeting the regulations of 10 CFR 50 and 52; therefore, it would be inappropriate to provide any endorsement of guidance relative to 10 CFR 73.	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
10	NEI	Section B, Page 4, 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.	Disagree. In the Introduction section to IEEE Std. 7-4.3.2-2003, it states "During the NPEC preview of this revision of the standard, the topic of safety system software security was discussed. Specifically, the ability of the software system to fulfill its safety related functions in the presence of attacks. Recommendations were made that a future revision of the standard address software risks associated with attacks by insiders and from outside." The current endorsement of IEEE Std. 7-4.3.2 is of the 2003 version. Currently, 10 CFR 73.54 addressed protection from attacks. However, the non-malicious portion still needs to address as part of the licensing process. Therefore, the staff revised RG 1.152, Rev 2 to focus on this aspect. IEEE Std. 7-4.3.2-2010 has taken steps to address security, and the staff will initiate another version of RG 1.152 to endorse appropriate provisions of the new (2010) revision to IEEE Std. 7-4.3.2.	No change.
11	NEI	Section B, Page 4, Bullet 1	"These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behavior from connected systems when operational." Physical access	Revise to read as follows: '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	Disagree. See Response to Comments #1 and #2	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			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.	systems as addressed in DI&C-ISG-04.'		
12	NEI	Section B, Page 4, Bullet 2	<p>"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."</p> <p>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."</p> <p>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? 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.</p>	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.	<p>Agree in part.</p> <p>See Response to Comment #1</p> <p>The clarifying definitions within DG-1249 were developed jointly by NRR, NRO and NSIR. The term "malicious" has been retained to clearly distinguish from the coverage of DG-1249.</p>	Replaced the term "digital systems" with "Critical Digital Assets" to be consistent with 10 CFR 73.54. Removed the term "intelligent" to be consistent with the definition of "Adversary" found in RG 5.71.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
13	NEI	Section B, Page 4, 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 1) DG-1 249 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 2) 10CFR73.54, NEI 08-09, and RG 5.71 address the physical environment or operation and maintenance of digital safety systems.	Agree in part. The consideration of the physical environment and the access controls associated with the physical location of the equipment is key to determining whether sufficient controls exist within the design of the system in its installed environment to protect the safety systems from unintended access or modification during operation.	The staff did remove Sections C.2.6 - C2.9 of RG 1.152, Rev 2, which addressed maintenance, operation, and retirement.
14	NEI	Section B, Page 5, 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..."	Agree in part. The discussion in Section B, Page 4, 1 st bullet clarifies that this guidance addresses "protective actions taken against a predictable set of undesirable acts (e.g., inadvertent operator actions or the undesirable behavior of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations". This wording limits the types of vulnerabilities that should be considered.	No change.
15	NEI	Section B, Page 5, 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 access or modifications to the safety	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,	Agree in part. See Response to Comment #1 IEEE 603-1991, Clause 5.9, "Control of Access" states: "The	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			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.	unintended, or unauthorized electronic access or modifications to the safety system...'	design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provisions in the generating station design, or by a combination thereof." While electronic (logical) access is clearly a component of "access" for digital systems, IEEE 603-1991 also applies to physical access. As was stated above, licensees may adopt provisions that serve to address the requirements of both Part 50 and Part 73; however, in the context of the Part 50 licensing review, the NRC would only make a conclusion on those provisions' ability to meet Part 50 requirements (i.e., IEEE 603-1991)	
16	NEI	Section B, Page 5, 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.'	Disagree. See Response to Comment #1	No change.
17	NEI	Section B, Page 5, 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...'	Agree	Language revised to read: "(2) by ensuring that the system is developed without undocumented codes . . ."

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
18	NEI	Section B, Page 5, 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...'	Disagree. The staff expects that licensees will comply with 10 CFR73.54, as appropriate. The focus of this guidance is establishing design features and controls that address operational environment needs identified by the licensee.	No change.
19	NEI	Section B, Page 5, 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.'	Disagree. This point is only discussed in the discussion section, and not part of the actual regulatory position. The regulatory position section states, "Cyber-security and other security controls applied to the latter phases of the lifecycle that occur at a licensee's site (i.e., site installation, operation, maintenance, and retirement) are not part of the 10 CFR 50 licensing process and fall under the purview of other licensee programs."	No change.
20	NEI	Section C, Pages 6-10	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" *	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,	Disagree. See Response to Comment #10 IEEE 7-4.3.2 – 2003 specifically recognized the need for security provisions, but deferred their adoption in the standard. Therefore, as was the intent with RG 1.152, Rev 2, these regulatory positions address this identified need.	No change.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			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"	<ul style="list-style-type: none"> 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 		
21	NEI	Section C, Pages 6-10	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.	Disagree. RG 1.168 is not specific on the establishment of a secure development and operational environment. In addition, although RG 1.168 specifies that a security assessment should be performed as part of the V&V activities, RG 1.168 does not specify that the results of the security assessment should drive requirements specifications for the system.	No change.
22	NEI	Section C, Page 6, 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.	Agree in part. The staff intends to provide additional detailed guidance such as this. However, this effort will be undertaken in Rev 4 of RG 1.152.	No change.
23	NEI	Section C, Page 6, Paragraph 2	Item 5 should reference DI&C-ISG-04 for guidance on communication independence.	Add the reference to DI&C-ISG-04.	Agree in part; however, no changes are warranted. See Response to Comment #2	No changes.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
24	NEI	Section C, Page 7, 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.	Agree in part. The staff intends to provide additional detailed guidance such as this. However, this effort will be undertaken in Rev 4 of RG 1.152.	No changes.
25	NEI	Section C, Page 7, Paragraph 1	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.	Agree in part. The staff intends to provide additional detailed guidance such as this. However, this effort will be undertaken in Rev 4 of RG 1.152.	No changes.
26	NEI	Section C, Page 7, Item 2.1 & 2.2	Since these may have separate responsibilities, care must be taken to use these terms appropriately: "licensee and developer". The content of an application is covered by DI&C-ISG-06.	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' Eliminate reference to content of an application as this is covered by DI&C-ISG-06.	Agree	Revised to reflect that these are licensee responsibilities.
27	NEI	Section C, Page 7, 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.	Agree in part; however, no changes are warranted. See Response to Comment #2	No changes.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
28	NEI	Section C, Page 7, 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.	Agree	Changed as recommended
29	NEI	Section C, Page 7, 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.'	Agree	Changed as recommended
30	NEI	Section C, Page 7, Item 2.2.2	"During the development of requirements, measures should be taken to ensure that therequirements 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.'	Agree	Revised wording to state: "During the requirements phase, measures should be taken to prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code."
31	NEI	Section C, Page 7, 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	Revise to read as follows: 'Design configuration items that incorporate predeveloped software into the safety system	Disagree. This point is to ensure that pre-developed software does not include extraneous or unused code	No changes.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
			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.	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.'	that could negatively affect the reliable performance of the safety function. If not properly identified, considered and addressed, extraneous code and functions could impede the reliable operation of a safety system. Simply ensuring that there is no malicious code is not sufficient.	
32	NEI	Section C, Page 7, 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.'	Agree	Revised wording to state: "During the design phase, measures should be taken to prevent the introduction of unnecessary design features or functions that may result in inclusion of unwanted or unnecessary code."

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
33	NEI	Section C, Page 7, 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." 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?	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.'	Agree in part. The staff intends to provide additional detailed guidance such as this. However, this effort will be undertaken in Rev 4 of RG 1.152.	No changes.
34	NEI	Section C, Page 7, 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..."	Agree in part. The staff intends to provide additional detailed guidance such as this. However, this effort will be undertaken in Rev 4 of RG 1.152.	No changes.
35	NEI	Page 11, References Section	Reference Section does not mention DI&C-ISG-04.	Revise to add reference DI&C-ISG-04, "Highly-Integrated Control Rooms-Communications Issues (HICRc)"	Agree in part; however, no changes are warranted. See Response to Comment #2	No changes.
36	VC Summer (wmartin@scana.com)		The draft DG relies heavily on the Vendor having a secure development environment. The draft regulatory guide should recommend developing a procurement specification for Digital Safety Systems that meet the regulatory guide.		Agree This guidance provides regulatory criteria for establishing a secure development and operational environment for safety systems. The licensee has the responsibility of ensuring the procured safety systems meet NRC regulations. If development of a digital safety system is performed by a vendor, a	Language added to Section 2 to state: "Licensees who have vendors develop their digital safety systems should include provisions in

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
					licensee should consider imposing requirements for secure development as part of the procurement.	their procurement specification to ensure that the vendor takes appropriate measures to establish a secure development environment and that the vendor includes any features in the system design the licensee requires to support a secure operational environment for the digital safety system."
37	VC Summer (wmartin@scana.com)	Section 2.1 Concepts Phase, last sentence	Section 2.1 Concepts Phase, last sentence states that the NRC has positions and guidance on data communication between non-safety and safety digital systems. The documents associated with these NRC positions and guidance should be listed.		Agree in part; however, no changes are warranted. See Response to Comment #2	No changes.
38	VC Summer (wmartin@scana.com)		RG 5.71 Security Control, C.12.5 Developer Security Testing, provides criteria for system developers and integrators of acquired CDAs to create, implement, and document a security test and evaluation plan. DG-1249 should align with the criteria in RG 5.71.		Disagree. See Response to Comment #1 As is noted in the response, the staff anticipates that features and controls adopted by licensees will serve the needs of both Part 50 and Part 73. However, the licensing review will not make any	No changes.

**Comment and Responses on DG-1249, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"
Proposed Revision 3 of Regulatory Guide 1.152**

Comment #	Commenter	Section	Comment	Commenter Recommendation	NRC Response	Document Changes
					judgments on the effectiveness of cyber security controls to thwart cyber threats.	