Public Comments and NRC Responses for Draft Regulatory Guide (DG) -1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Revision 1 of Regulatory Guide (RG) 1.170

A Federal Register Notice was published on August 22, 2012 (77 FR 50720) announcing the availability of Draft Regulatory Guide (DG) -1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" for public comment. DG-1207 is Revision 1 of Regulatory Guide (RG) 1.170 dated September 1997. The following table contains the public comments received and the NRC staff responses.

Comments were received from the following individuals:

1. David Herrell
   MPR Associates, Inc.
   320 King St.
   Alexandria, VA 22314
   (ADAMS – ML12346A034)
2. Matt Gibson
   Duke Energy
   Matt.Gibson@Duke-Energy.Com
   (ADAMS – ML12321A011)
3. Mark Burzynski,
   New Clear Day, Inc.
   2036 Marina Cove Dr.
   Hixson, TX 37343
   (ADAMS – ML122910763)
   (ADAMS – ML122910764)
   (ADAMS – ML122910778)
   (ADAMS – ML12286A386)

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
David Herrell	DG-1207 (RG 1.170) General	With the current emphasis on FPGAs, one would have thought that the topic would have at least been mentioned in this draft. Incorporate sufficient guidance on software lifecycle techniques to support FPGA VHDL code development.	Thank you for your comment. No changes have been made as a result of this comment. The information on software can be applied to the software of field-programmable gate arrays (FPGAs). For more direct information on FPGAs see NUREG/CR-7006, "Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems" (ADAMS Accession No. ML100880142)
David Herrell	DG-1207 (RG 1.170) General	This regulatory guide clearly defines the roles and responsibilities of licensees, applicants, and NRC staff for software processes. However, this reviewer's experience shows that most, if not almost all, safety software is not written by licensees or	Thank you for your comment. No changes have been made as a result of this comment. The NRC is responsible for regulating commercial nuclear power plants and other uses of nuclear material, such as in nuclear medicine, through its licensing, inspection

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		applicants. Rather, safety software and safety systems are designed and developed by various vendors. This regulatory guide does not define how software and system vendors are to apply the regulatory guidance. This regulatory guide does not define which version of the regulatory guide is to be applied by a software vendor, or the requirements for software vendors to maintain their programs current with regulatory guidance, which seems to be the NRC requirement, based on topical report submittals. Consistently define the application of RGs 1.168 through 1.173 for software and system vendors, throughout all sections of each of the regulatory guides. Define the expectations for use of current regulatory guides, since software and system vendors do not have the capability to commit to a given version of the regulatory guides and industry standards in a license. Define the expectations for use of current or older regulatory guides in topical report submissions, or point to other NRC documents that define these requirements.	and enforcement of its regulations and requirements. The NRC issues regulatory guidance documents, such as regulatory guides, standard review plans, and the NRC's Inspection Manual to aid licensees in meeting the agency's safety requirements. The NRC has no authority to regulate or direct the activities of software developers or software and system vendors. The NRC promulgates its regulatory guidance documents to the NRC's licensees and applicants and it is the responsibility of the licensee and applicant to define software and software system requirements to their vendors as needed to demonstrate compliance with the NRC regulations.
David Herrell	DG-1207 (RG 1.170) General	DG-1207 now covers all aspects of testing, from unit through system validation/Factory Acceptance Test. DG-1208 only provides guidance for Unit Test. Please provide guidance equivalent to DG-1208 that covers all aspects of testing to be consistent with the guidance provided in this document.	Thank you for your comment. No changes have been made as a result of this comment. DG-1207 (RG 1.170) provides an overview of the testing program whereas DG-1208 (RG 1.171) describes a specific part of the overall testing program. The "unit test" described in DG-1208 is one of the building blocks needed to develop the details and requirements for testing of specific software functions. The direction of these details of how DG-

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
			1207 provides this planning can also be found under topics and regulation, such as: configuration management (DG-1206) and verification and validation (DG-1267).
David Herrell	DG-1207 (RG 1.170) Section B	Page 2, third paragraph, third line from end - Please clarify the version of NUREG-0800 used in reviews. After the phrase "*The NRC staff uses the*" add the phrase "latest version of" to provide guidance to industry.	Thank you for your comment. No changes have been made as a result of this comment. The NRC staff does not identify specific revisions for some guidance documents. This type of dynamic referencing is done because different licensees and applicants may have committed to different versions of the guidance documents and it would be inappropriate to always use the "latest version" of the guidance document if the applicant or licensee has committed to follow an earlier version.
David Herrell	DG-1207 (RG 1.170) Section B	Page 3, third paragraph, second sentence - In the paragraph beginning "*Several criteria in Appendix B...*" the word "Criterions" is used. The plural form of criterion is criteria. While "criterions" shows up in several informal dictionaries, it should not be used in formal writing. Suggest rephrasing the start of the second sentence to either "The listed criteria are only part…" or "Each criterion listed below is only part…" to use correct grammar.	Thank you for your comment. As a result of the comment the term "Criterions" was revised to "criteria."
David Herrell	DG-1207 (RG 1.170) Section B	Page 4, first bullet on the page (last in the list), 2nd and 3rd lines - The sentence does not clearly state what must be "identifiable and retrievable." Replace *"...specific itemized records for test documentation and controlled by the SCM as the software evolves with development and maintenance are identifiable*	Thank you for your comment. No changes have been made as a result of this comment. The suggested sentence does not enhance understanding. It adds more complexity unnecessarily.

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		and retrievable..." with "…specific itemized records for test documentation are identifiable and retrievable, and that the records are controlled by the SCM as the software is developed and as the software evolves…"	
David Herrell	DG-1207 (RG 1.170) Section B	Page 4, 4th paragraph - The paragraph starting "*The IEEE Std. 829-2008*…" requires interim status reporting, without defining the purpose or content of the "status reports" required. There are additional problems in the first four lines. If the intent is to require phase summary test reports, then so state. Testing requirements should include test reports which provide results of testing, which are not clearly required by this section. Replace: "*The IEEE Std. 829-2008 test reporting category consists of an interim status report, an anomaly report, more test logs, along with the final test summary reports that allow the licensee to record and summarize test events and that follow the integrity scheme needed within the life-cycle and serve as the basis for evaluating test results*." With something more like: "The test documentation shall include phase summary test reports, anomaly report or reports, test reports, test logs, and the test summary reports. This test documentation will support the licensee by recording and summarizing test events. The test documentation shall follow the integrity scheme documented within the life-cycle. The test documentation shall serve as the basis for evaluating test results."	Thank you for your comment. No changes have been made as a result of this comment. Section B of the regulatory guide is the discussion section. The discussion section provides an overview on how the specific IEEE standard relates to the test reporting criterion. Specific requirements for test documentation and status reporting are provided in Section C.

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
David Herrell	DG-1207 (RG 1.170) Section B	Page 5, 3rd paragraph, 6th line - The word "associated" has specific meanings in IEEE standards and in regulatory space, which is not the meaning intended in this section. Replace the word "associated" with another word, or, preferably, delete "associated" from the draft sentence.	Thank you for your comment. No changes have been made as a result of this comment. The word "**associated**" as used in the sentence "The licensee should formally test all **associated** features in the safety system and follow the recommended testing activity process outlined under Clause 5 in IEEE Std. 829-2008" is a common usage word and does not require modification or additional explanation or definition.
Matt Gibson	DG-1207 (RG 1.170) Section B, page 5, paragraph 4	This wording makes it sound like Integrity Level 4 is brand new in the standard. Integrity Level schemes are new 829 not just for level 4 but all levels. Not sure what is trying to be conveyed by the wording of this sentence. In relation to Position 6 discussion, I would suggest clarification that integrity level schemes are new in the standard and that the NRC considers Level 4 to be an adequate classification of software used in safety systems of nuclear power plants.	Thank you for your comment. No changes have been made as a result of this comment. The paragraph identifies a change in this revision to Regulatory Guide 1.170. The Staff Regulatory Guidance in Section "C" of RG 1.170 has been expanded to include the four-level integrity scheme method of quantifying software integrity. This was not part of the earlier version of this RG and is identified as part of the "Description of Change" section of the RG. The language in Section C of this RG describes the NRC staff position on the use of integrity scheme level 4.
David Herrell	DG-1207 (RG 1.170) Section B	Page 5, 6th paragraph, 3rd line - For consistency, refer to IEEE standards in a consistent manner. Replace "IEEE 829-2008" with "IEEE Std. 829-2008"	Thank you for your comment. As a result of the comment the word "Std." was added.
David Herrell	DG-1207 (RG 1.170)	Page 6, 1st partial paragraph, last line - The phrasing makes it appear that there is a single "the SDOE."	Thank you for your comment. No changes have been made as a result of the comment. The existing

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
	Section B	Replace the phrase "*the SDOE*" with "an SDOE" to provide indication that SDOE is not a one-size-fits-all proposition.	sentence already makes that point that SDOE is not a one-size-fits-all proposition.
David Herrell	DG-1207 (RG 1.170) Section B and Section C	Page 6, 1st paragraph, 3rd line and C page 7, 1st partial paragraph, 2nd line - Break the existing sentence into two separate sentences. Replace ", however" with ". However"	Thank you for your comment. No changes have been made as a result of the comment. The existing sentence is designed to eliminate the "choppy sentence" transition issue. See Diana Hacker's "A Writer's Reference," Page 112. The use of "; however, will be revised.
Matt Gibson	DG-1207 (RG 1.170) Section C.1	Page 7, section 1, paragraph 2: - It is not clear in the second statement if the minimum acceptable information for the MTP is all of Clause 8 in 829. As long as we have items a - g in the regulatory guide, are parts of the Clause 8 MTP details omissible?	Thank you for your comment. As a result of the comment the paragraph has been changed to improve the NRC staff's intent that items "a" through "g" should be added to the Master Test Plan.
Matt Gibson	DG-1207 (RG 1.170) Section C.1	Page 7, Section la: - Only Clause 9.3.6 [of IEEE Std. 829-2008] mentions necessary skills and test training. There are no qualifications or skills identified in Clause 8. What additional training, skills and qualifications would be required other than what is identified in Clause 9.3.6?	Thank you for your comment. No changes have been made as a result of the comment. Clause 8 of IEEE Std. 829-2008 outlines the need for a resource summary as well as responsibility, training and support. Additionally, it is the responsibility of the licensee or applicant to define training, skills, and qualifications for working with software and software system requirements for themselves and for their vendors as needed to demonstrate compliance with the NRC regulations.
David Herrell	DG-1207 (RG 1.170) Section C.1, page 7, item d	Item d extends the testing boundary for this regulatory guide well past the "Software" in the title, to include system, software, and hardware. It is not clear whether this item applies to all hardware or just	Thank you for your comment. No changes have been made as a result of the comment. All aspects of the system and hardware should be considered when designing software.

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		hardware containing digital devices. If this item is retained, then the title of the regulatory guide should be updated to include hardware to make it possible to identify this regulatory guide as applying to hardware.	
David Herrell	DG-1207 (RG 1.170) Section C.2, page 8, first paragraph, last sentence	The sentence clearly defines the requirements for the licensee. The applicant's and the software vendor's responsibilities are not defined. In many cases, the licensee will not be provided with complete software records, making this statement difficult to meet. Please revise the statement to one where the licensee or applicant is responsible for ensuring that software and system records are retained, including at a vendor's location.	Thank you for your comment. No changes have been made as a result of the comment. The NRC is responsible for regulating commercial nuclear power plants and other uses of nuclear material through its licensing, inspection, and enforcement of its regulations and requirements. The NRC issues regulatory guidance documents, such as regulatory guides, standard review plans, and the NRC's Inspection Manual to aid licensees in meeting the agency's safety requirements. The NRC has no authority to regulate or direct the activities of software developers or software system vendors. The NRC promulgates its regulatory guidance documents to the NRC's licensees and applicants and it is the responsibility of the licensee and applicant to define software and software system requirements to their vendors as needed to demonstrate compliance with the NRC regulations.
David Herrell	DG-1207 (RG 1.170) Section C.3 first paragraph, last sentence	The timing required by the phrase "prior to implementation" is not clear, and can be interpreted in a manner that makes it impossible to write code in the Implementation Phase of the software life cycle, which is different from installation in the plant.	Thank you for your comment. No changes have been made as a result of the comment. It is suggested that the originator review RG 1.171 and the cited reference Boris Beizer. The implementation phase of any software project is when the system design is transformed into code, database structures, and

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		Change "prior to implementation" to "prior to being credited with performing one or more safety functions in a plant" for more appropriate guidance.	related machine executable representations. The suggested change would leave the test documentation as an end discussion after the safety system is installed as per the software lifecycle. This is not acceptable and would defeat the purpose of designing the software unit tests before coding.
Matt Gibson	DG-1207 (RG 1.170) Section C.3	Page 8, Section 3, Paragraph 1: - Consider moving this discussion to an earlier section to better align with the order of 829. The previous section discusses items from Clause 8 & 9 whereas this section is discussing Clauses & 7.	Thank you for your comment. No changes have been made as a result of the comment. Though this is a good suggestion, however, the NRC considers Clause 8 and then 9 as the most important aspects of building a test documentation plan. The discussion in regulatory position #3 adds further value.
Matt Gibson	DG-1207 (RG 1.170) Section C.3	Page 8, Section 3, Paragraph 2: This section discusses the allowance of combining testing documents. It omits the allowance of eliminating testing documents. Clause 6.4 allows both combination and elimination without distinction. Is it implied, then, because the NRC only discusses combining documents that elimination is not allowable? Why is only the lowering of level of integrity discussed as to what is not acceptable? This paragraph is not clear on what is acceptable and what is not acceptable within Clause 6.4. Interpretation could be made that since only lowering the integrity level is identified, fast tracking a project allows elimination of documents. Please clarify specifically what is acceptable and what is not.	Thank you for your comment. No changes have been made as a result of the comment. The combining of documentation allows for improving the document management process. The documentation elimination by lowering the integrity level is not acceptable as stated in regulatory position #3. Regulatory guides describe one method the licensee may use to demonstrate compliance with the regulations. They may not be the only method and the licensee is free to propose alternatives.
Matt Gibson	DG-1207 (RG 1.170)	Page 9, section 6, paragraph 1:	Thank you for your comment. No changes have been made as a result of the comment. Though the IEEE

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
	Section C.6	The standard specifically states that it does NOT mandate the use of integrity level schemes (Page 14, first sentence of second paragraph: "This standard does not mandate the use of the integrity level schemes.") It further states in the paragraph, "The use of integrity level scheme is a recommended best practice..." Since the standard does not mandate it, the NRC needs to clarify if the regulatory guide will mandate it.	standard doesn't mandate an integrity level scheme it also states "This standard uses integrity level to determine the test tasks to be performed." This regulatory guide describes one method the licensee may use to demonstrate compliance with the regulations. It may not be the only method and the licensee is free to propose alternatives.
David Herrell	DG-1207 (RG 1.170) Section C.6	2nd paragraph, last sentence - There is a grammar issue with this sentence. We believe that replacing "… integrity level 4 and defined…" with "… integrity level 4 as defined…" conveys the intent.	Thank you for your comment. As a result of your comment "as" was inserted in place of "and."
David Herrell	DG-1207 (RG 1.170) Section C.6 page 9, 1st paragraph, last sentence	It is not clear what should/shall be done based on "should consider" in the last sentence. Considering and implementing lead to two very different outcomes. We believe that the implementation is more important than consideration. Replace "should consider" with "should implement" and replace "this annex" with "Annex C" for clarity.	Thank you for your comment. No changes have been made as a result of the comment. The paragraph in question is under Section C.7. The "Annex C" is mentioned in the 1st paragraph and can be considered without being restated. This regulatory guide describes one method the licensee may use to demonstrate compliance with the regulations. It may not be the only method and the licensee is free to propose alternatives.
Mark Burzynski	DG-1207 (RG 1.170) Section C.6 and DG-1267 (RG 1.168) Section C.8	DG-1207 Regulatory Position C.6 states: *"The NRC staff takes exception to the Table B.3, "Risk assessment scheme" in Annex B. The IEEE Std. 829-2008 statement about the Table B.3 illustration for determining the likelihood and evaluating software integrity level lower than Level 4 is not acceptable. The likelihood of occurrence is likely to cause catastrophic consequence and*	Thank you for your comment. As a result of your comment, he regulatory position 1 in DG-1267 was updated with the following paragraph: "The NRC staff takes exception to the Table B.1, 'Assignment of software integrity levels' and Table B.3 'Graphic illustration of the assignment of the

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		thus the breadth or depth of testing and documentation should adhere to the proper activities for a nuclear software safety system product. The licensee or applicant should assign integrity level 4 or the equivalent to software used in nuclear power plant safety systems, as demonstrated by a mapping between its approach and integrity level 4 and defined in IEEE Std. 829-2008." DG-1267 Regulatory Position C.8 states: *"Annex B (of IEEE 1012-2004), "A Risk-based Software Integrity Level Scheme," describes the four software integrity levels and associated consequences. This regulatory guide endorses this annex, as described in Staff Regulatory Guidance position 1."* The NRC positions in the two DGs are contradictory, since the Annex B information in IEEE Std. 829-2008 and IEEE Std 1012-2004 are essentially equivalent. The contradictory NRC positions should be reconciled.	software integrity levels' in Annex B. In Table B.1 critical consequences in the system description is not acceptable as a task description for level 4. The IEEE Std. 1012-2004 statement about the Table B.3 illustration for determining the likelihood and evaluating software integrity level lower than Level 4 is not acceptable. The likelihood of occurrence is likely to cause catastrophic consequence with no mitigation possible and thus the breadth or depth of testing and documentation should adhere to the proper activities for a nuclear software safety system product to prevent such an occurrence. The licensee or applicant should assign integrity level 4 or the equivalent to software used in nuclear power plant safety systems, as demonstrated by a mapping between its approach and integrity level 4."
Mark Burzynski	DG-1207 (RG 1.170) Section C.7	It would be better to revise the discussion in C.7 (Testing Tasks) and the endorsement of Annex C in DG-1207 to ensure consistency with the treatment of test-related tasks in DG-1267, which endorse IEEE Std. 1012-2004. The proposed approach when coupled with DG-1267 would require the use of two task schemes for the test-related tasks.	Thank you for your comment. No changes have been made as a result of the comment. Annex C is endorsed. Thus DG-1207 discusses the project documentation, which includes the test documentation for life cycle of the software. The DG-1267 provides guidance for V&V activities, which are addressed by a separate independent group.
David Herrell	DG-1207 (RG 1.170) Section C.10 page 10	Please correct the last sentence to reflect the endorsement of annexes. Replace "*These annexes are listed here as sources of information; they have not…*" with "Annexes B and	Thank you for your comment. No changes have been made as a result of the comment. The summarization is not necessary, as the intent is for reading through each annex.

Comments on DG-1207, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" DG-1207 is Rev. 1 of RG 1.170			
Originator	**Draft Guide**	**Comment**	**NRC Response**
		C have been endorsed by this regulatory guide. Annexes A, D, E, F, G, and H are listed here as sources of information, which have not…" and remove "unless otherwise noted"	
David Herrell	DG-1207 (RG 1.170) Section C.10 page 10	Items 1, 4, 5, and 6 - Rather than limiting the scope of applicability, provide guidance for software vendors as well. Replace "applicants and licensees may find it useful" with "users of this regulatory guidance may find this annex useful"	Thank you for your comment. No changes have been made as a result of the comment. The pronoun "it" refers to the annex in the paragraph.