

Resolution of Public Comments Received on Draft Regulatory Guide DG-1190, “Manual Initiation of Protective Actions”

During the public comment period for Draft Regulatory Guide DG-1190, which ended on February 20, 2009, the NRC received comments from AREVA NP, Inc., General Electric-Hitachi (GEH), Nuclear Energy Institute (NEI), Data Systems and Solutions (DSS), South Texas Project (STP), Hurst Technologies, and Westinghouse. The NRC staff has carefully reviewed the draft and addressed the comments as appropriate. The following table summarizes the comments and staff’s response to them.

AREVA NP, Inc. Comments (ML0901401201)		
Section of DG-1190	Comment	Resolution
<p>Section B 1st paragraph page 3</p>	<p><u>Comment 1:</u> This paragraph portrays digital instrumentation and control (I&C) systems in a negative way only. For balance, the positive capabilities of digital I&C should be included. The following modifications are suggested:</p> <p style="padding-left: 40px;">“Existing instrumentation and control (I&C) equipment in nuclear power plants is currently being replaced with computer-based digital I&C systems or advanced analog systems <u>to increase reliability and plant safety</u>. However, <u>if designed or operated improperly</u>, these technologies may pose new vulnerabilities for the nuclear power plant in a number of aspects compared to existing I&C systems.”</p>	<p>The staff partially agrees. The affected paragraph will be revised to clarify the digital I&C failure vulnerabilities. However, it is not the NRC’s role to promote a technology that is still evolving and facing challenges. The wording in this paragraph will be revised to read:</p> <p style="padding-left: 40px;">“Existing instrumentation and control (I&C) equipment in nuclear power plants is being replaced with computer-based digital I&C systems or advanced analog systems. However, if designed, installed, operated, or maintained improperly, these technologies may pose new vulnerabilities for the nuclear power plant compared to existing I&C systems.”</p>
<p>Section B 3rd paragraph page 3</p>	<p><u>Comment 2:</u> This paragraph is confusing and does not provide any useful guidance. It is suggested that this entire paragraph be removed from the Draft Regulatory Guide (RG) for the following reasons:</p> <ul style="list-style-type: none"> • The need for manual component-level control cannot be stated in a blanket manner. Instead, this need is dictated by the functional requirements and operating procedures for each plant design on a component-by-component basis. • This guidance expands manual control requirements in an unbounded manner. Is component-level control only suggested 	<p>The staff partially agrees. Although some language in the draft Regulatory Guide (RG) may have caused confusion, there is no blanket or unbounded statement in the draft. The scope of the draft is confined within protective systems. The purpose of revising the RG is to update the reference to the most recent IEEE standard endorsed by NRC and to interpret existing regulations and guidance with respect to the use of manual initiation of protective actions in digital systems to reduce the licensing uncertainties in the light of aging analog I&C systems being replaced by digital systems. However, to eliminate confusion the staff agrees to delete the affected paragraph.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>for those components that take part in a protective action, or does this suggestion extend beyond that? The language "...each appropriate plant system component" is ambiguous.</p> <ul style="list-style-type: none"> • It is not clear whether the staff expects these manual component-level controls to be part of the safety system. It is not clear if there is overlap between these component-level manual controls and those specified by item (3) in the previous paragraph. • It is not accurate to state that component-level controls are required to achieve completion of the safety function. For example, many components of the auxiliary supporting systems (e.g., heating, ventilation and air conditioning, diesel generators, and component cooling water) would not require manipulation, following actuation at the system level, to complete the safety function. • It is not clear how "high functional reliability of the protective system" constitutes a basis for requiring extensive manual component-level controls. 	<p>This response also applies to comments 4 and 8.</p>
<p>Section B 4th paragraph page 3</p>	<p><u>Comment 3:</u> The provision of manual, system level control of protective actions is required by IEEE Std 603-1991 Clause 6.2. Clause 6.2 does not provide any requirements that manual controls be provided to cope with failures of the automatic protective actions. Therefore, the use of the term "backup" in describing the manual controls is not consistent with Clause 6.2.</p> <p>The use of the term "backup" is more appropriate in describing the diverse I&C provided specifically to cope with postulated software common cause failure (CCF) of the automatic protective actions. Diverse I&C is not the subject of IEEE Std 603-1991 Clause 6.2, and should not be the subject of RG 1.62.</p> <p>The following modification is suggested:</p> <p>"The protective actions can involve automatic controls with backup manual controls be initiated automatically, or, in certain cases, can be</p>	<p>The staff agrees. The affected paragraph will be revised as proposed.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>accomplished solely by manual controls. Protective actions selected to be controlled <u>initiated solely by manually controls</u> are subject to consideration of..."</p>	
<p>Section B 6th paragraph page 4</p>	<p><u>Comment 4:</u> This paragraph is confusing and does not provide any useful guidance. It is suggested that this entire paragraph be removed from the Draft RG for the following reasons:</p> <ul style="list-style-type: none"> • The reference to IEEE Std 603-1991 Clause 5.6.3.1 seems inappropriate. When would system-level manual initiation of protective actions be used as a non-safety function? • It is not clear if the safety related classification is intended to apply to the system level manual functions, or the component level manual functions, or both. • This paragraph specifies that the manual controls and indications must contain safety related software (i.e., they are part of a digital safety system). However, Regulatory Position 4 states: "In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs." How can the manual controls only be connected to safety equipment downstream of the digital I&C safety system outputs if the manual controls themselves are part digital I&C safety systems? <p>A better discussion is proposed as follows:</p> <p>IEEE Std 603-1991, Section 5.6.3.1, specifies that equipment "... that is used for both safety and nonsafety functions shall be classified as part of the safety systems..." Therefore equipment that is not classified as part of a safety system must not be credited for performing safety functions, if it is the only equipment that supports those safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform functions needed to support plant safety, if there is also safety-related equipment available to perform the same plant safety function. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being</p>	<p>The staff partially agrees. While some language in the draft may have caused confusion, the reference to Section 5.6.3.1 of IEEE Std 603-1991 is a necessary discussion. However, to eliminate the confusion the affected paragraph will be revised to read:</p> <p>“Section 5.6.3.1 of IEEE Std 603-1991 specifies that interconnected “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.” Therefore, equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform functions that support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant safety analyses.”</p> <p>Also see response for comment 2 with regard to component-level manual control and response for comment 10 with regard to Position 4.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>performed utilizing only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety related control and display equipment that is credited in the plant safety analyses.</p> <p>When using non-safety multidivisional control and display stations to perform safety-related actions, plant operators are expected to confirm that appropriate responses have been achieved for the actions taken. If the operator observes or suspects that the non safety multidivisional control and display station is not responding as expected, or that the nonsafety indications may be inaccurate, or that the plant is not responding as expected, then the operator must utilize the safety-related controls and indications to perform the necessary actions and to assess plant conditions and responses.</p>	
<p>Section B 8th paragraph page 4</p>	<p><u>Comment 5:</u> This paragraph states: "Credible common-mode failures should be compensated either by diversity or defense in depth." The use of the word "or" is incorrect. Diversity can not be separated from defense in depth in the context of coping with software CCF. Instead, diversity must be incorporated into the lines of defense.</p> <p>The following modification is suggested: "Credible common-mode failures should be compensated either by diversity <u>and</u> or defense in depth."</p>	<p>The staff agrees. The statement will be revised as proposed. However, in an effort to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions, the discussion on common-mode failures and diversity will be removed from the affected paragraph and will be included in the paragraph that addresses Point 4 of BTP 7-19.</p>
<p>Section B 11th paragraph page 5</p>	<p><u>Comment 6:</u> This paragraph makes reference to NRC's Branch Technical Position (BTP) 7-19: "Guidance provided to NRC staff in BTP 7-19 asserts that manual controls for safety equipment should be connected downstream of the plant's digital I&C safety system outputs." This paragraph incorrectly interprets the guidance in BTP 7-19 to apply to all manual controls for safety equipment; it should be removed from this RG.</p> <p>In many I&C designs, the manual controls used to address BTP 7-19 Point 4 are not the same as those used to address IEEE Std 603-1991 Clause 6.2 (i.e., diverse controls). Combining the two issues in this</p>	<p>The staff partially agrees. Although some language in the draft RG may have caused confusion, combining manual controls used to address BTP 7-19 Point 4 and those used to address IEEE Std 603-1991 is not the intent of the draft.</p> <p>The purpose of RG 1.62 is to provide guidance/acceptable methods for use in complying with the NRC regulations with respect to the means for manual initiation of protective actions. BTP 7-19 provides "guidance for evaluating an applicant/licensee's diversity and defense-in-depth (D3) assessment and the design of manual controls and displays to ensure conformance with the NRC positions on D3 for I&C</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>guidance is confusing and not useful. The purpose of RG 1.62 is to provide guidance on compliance with IEEE Std 603-1991 Clause 6.2, not BTP 7-19 Point 4.</p> <p>Comment 11 also applies to this paragraph.</p>	<p>systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS).” Both IEEE Std 603-1991 and BTP 7-19 address manual control for protective systems. Thus, (1) there is no conflict between the two, and (2) with more and more nuclear power plants participating in digitalization of I&C systems and with the potential for common-cause failure becoming important as the complexity of digital and advanced analog protection systems has increased, addressing BTP 7-19 with respect to diverse manual control for computer-based protective systems is appropriate and necessary. However, to eliminate the confusion, the draft will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions. The Discussion section will include the following:</p> <p>“This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation, as incorporated in 10CFR50.55a(h) and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet guidance specified in Point 4 of BTP 7-19.”</p> <p>And the affected paragraph will be revised to read:</p> <p>“2. <u>Meeting BTP 7-19 guidance:</u></p> <p>The potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed for D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of diverse non-safety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
		<p>failures in computer-based safety systems. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems to identify design vulnerabilities to common-cause failure. The fourth point of the Commission's diversity position listed in BTP 7-19 states in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or non-safety. Guidance provided to NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of NRC position on D3 should be connected downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic. 3. <u>Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance:</u></p> <p>As an alternative to two different manual controls discussed above, applicants or licensees may also propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies criteria of both IEEE Std 603-1991 and Point 4 of NRC position on D3."</p> <p>This response also applies to comment 11.</p>
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 7:</u> Section C, Regulatory Position 1, page 5 - The phrase, "on a system-level basis for each division" is very confusing. IEEE Std 279-1971 uses "system-level" and IEEE Std 603-1991 uses "division level" and certainly the difference in terminology should be addressed. However, simply combining the two provides no clarity on what is meant by</p>	<p>The staff agrees. The phrase "on a system-level basis for each division" will be revised to read: "on a division-level basis" to be consistent with IEEE Std 603-1991.</p> <p>This response also applies to comment 8.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>either concept.</p> <p>The Discussion section of this Draft RG should define "system-level" and "division level" specifically in terms that relate directly to manual initiation of protective functions.</p>	
<p>Section C</p> <p>Regulatory Position 1 page 5</p>	<p><u>Comment 8:</u></p> <p>It is suggested that the following statement be removed, as it cannot be meaningfully applied:</p> <p>"Individual means should also be provided for manual initiation of each plant system component required for... providing functional reliability for protective systems as set forth in GDC 13 and GDC 21."</p> <p>The wording is ambiguous and no applicant will be able to provide a meaningful list of "components required for providing functional reliability for protective systems" short of all components.</p> <p>This requirement is a significant expansion of the requirement in the existing RG 1.62. The unbounded scope of additional of controls required in the main control room has significant negative aspects associated with the-added system design-and human factors complexity. These negatives effects are not justified, since the added complexity has no clear and defined safety benefit.</p> <p>The requirement should be modified to focus on safety-related component-level controls for required manual actions to provide safety functions for accident and transient mitigation and to achieve safe-shutdown (in accordance with BTP 5-4).</p> <p>Comment 2 also applies to this Regulatory Position.</p>	<p>The staff agrees. Regulatory Position 1 will be revised to read:</p> <p>"Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve)."</p> <p>Also see response for comments 2 and 7.</p>
<p>Section C</p> <p>Regulatory Position 2 page 6</p>	<p><u>Comment 9:</u></p> <p>The Regulatory Position contains the following statement: "Multiple initiations of safety systems (autosequencing) by distinct manual control manipulations are not precluded. It is not clear what type of functionality is being discussed in this sentence. The use of the term "autosequencing" is confusing. Is it different than "action-sequencing" as used in the previous sentence? The use of "multiple initiations"</p>	<p>The staff agrees. The affected statement will be deleted as proposed.</p> <p>This response also applies to comment 10.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>combined with "distinct manual control manipulations" is ambiguous.</p> <p>The intent to allow a series of non-complex component-level actions in lieu of certain providing system-level manual controls should be clearly stated.</p>	
<p>Section C</p> <p>Regulatory Position 4 page 6</p>	<p><u>Comment 10:</u></p> <p>The following statement from RG 1.62 was deleted from between the first two sentences on Regulatory Position 4 :</p> <p>"However, action-sequencing functions and interlocks (of position 2) associated with the final actuation devices and actuated equipment may be common if individual manual initiation at the component or channel level is provided in the control room."</p> <p>This statement should be reinstated.</p> <p>It should be noted that Regulatory Position 2 recognizes the existence (and need) for this additional control logic between the actuation system and the actuated devices.</p> <p>"The Manual initiation of a protective action on a system-level basis for each division should perform all actions performed by automatic initiation such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the required action-sequencing functions and interlocks."</p> <p>In modern plants, this logic layer will be provided using software on safety function digital I&C processors. The net effect of the deletion of the noted sentence would be to preclude design using software logic for-this functionality. Instead, new plant designs would be required to use conventional hardware equipment (e.g., relays and current-carrying wires) between the digital safety system and the final actuation device, with all related negative safety and reliability issues associated with this dated technology. This approach directly contradicts the "minimum of equipment" statement in Regulatory Position 4, unreasonably increases maintenance burden, decreases reliability of the protection functions, and therefore reduces plant safety.</p>	<p>The staff partially agrees. The original Regulatory Position 4 (Revision 0 of RG 1.62) included the following guidance for manual initiation of protective actions: "<i>The amount of equipment common to both manual and automatic initiation should be kept to a minimum. It is preferable to limit such common equipment to the final actuation devices and the actuated equipment.</i>" This guidance provided a measure of diversity between the automatic and manual initiation in analog based systems. The affected statement excluded action-sequencing functions and interlocks from this guidance so that manual initiation would not be unnecessarily burdened with sequencing or interlock functions.</p> <p>Since (1) IEEE Std 603-1991 does not require that equipment common to both manual and automatic initiation be minimized and (2) with diversity guidance for digital computer-based I&C systems (BTP 7-19) being addressed under new Position 7, Position 4 (subject to IEEE Std 603-1991 requirements) will be revised to delete "<i>The amount of equipment common to both manual and automatic initiation should be kept to a minimum. It is preferable to limit such common equipment to the final actuation devices and the actuated equipment</i>". Therefore, the affected statement (served as an exception for the above statement) is therefore no longer needed.</p> <p>This response also applies to comments 9 and 11.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Comment 11:</u> The following statement is a new requirement added to the Draft RG: "In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment." This passage incorrectly extends guidance in BTP 7-19 to cover all manual controls for safety equipment and should be removed from this RG. BTP 7-19 suggests that: "displays and manual controls provided for compliance with Point 4 of the NRC position on diversity and defense in depth (D3)..." should be connected downstream of the plant's digital I&C safety system outputs. BTP 7-19 is silent on manual controls that are not credited for compliance with Point 4. Manual controls that exist to cope with software CCF of a digital safety system (those discussed in BTP 7-19) must be independent of the digital safety system, and therefore connected downstream of the digital safety system outputs. There is no requirement for manual controls (component-level or system-level) of safety equipment to be independent of the digital safety system if they are not credited to cope with failure of the digital safety system. In many I&C designs, the manual controls used to address BTP 7-19 Point 4 are not the same as those used to address IEEE 603 Clause 6.2. Combining the two issues in this guidance is confusing and not useful. The purpose of RG 1.62 is to provide guidance on compliance with IEEE Std 603-1991 Clause 6.2, not BTP 7-19 Point 4. Therefore, it is suggested that this paragraph and the entire discussion section on D3 be removed from this RG. This passage also invokes the "downstream of digital system" requirement on individual component controls as well as the system level controls. Implementing this guidance for all component level controls of safety equipment would result in extensive addition of</p>	<p>The staff partially agrees. The draft RG may have caused confusion by not distinguishing between guidance for manual controls that are subject to IEEE Std 603-1991 and diverse manual controls that are subject to BTP 7-19. However, as more and more nuclear power plants participate in digitalization of I&C systems and the complexity of digital and advanced analog protection systems has increased, the potential for software common-cause (CCF) failure has become increasingly important and needs to be addressed. In an effort to eliminate the confusion, the draft will be revised to distinguish between IEEE Std 603-1991 requirements and the guidance of BTP 7-19 with respect to manual initiation of protective actions. The diversity guidance subject to BTP 7-19 will be removed from Position 4 and will be addressed under a new regulatory position (Position 7). Also, new Position 8 will provide applicant/licensees an optional method for a safety-related diverse manual control that meets both IEEE Std 603-1991 requirements and the guidance of BTP 7-19. The opening statement of Section C will be revised to read: "Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to manual initiation of protective actions. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance." The new Position 7 will Read: "In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	<p>hardware between the digital safety system and the final actuation device, which unreasonably increases maintenance burden, decreases reliability of the I&C systems and therefore reduces plant safety.</p>	<p>or electronic cabinets and the plant's electromechanical equipment."</p> <p>The new Position 8 will Read:</p> <p>"An optional acceptable method that satisfies both requirements of IEEE Std 603-1991 and guidance on Point 4 of NRC position on D3, a single safety-related manual initiation of protective actions that satisfies Positions 1, 2, 3, 4, 5, 6, and 7 above can be provided."</p> <p>See response for comments 2 and 8 with regard to component-level manual control concern. Also see response for comments 6 and 10.</p>
<p>Regulatory Analysis Section 3.2, page 8; Section 4, page 8 Section D page 6</p>	<p>Comment 12: Regulatory Analysis Section 3.2, page 8 - The following statement is made about the cost impact of the changes proposed in the Draft RG: "Applicants would incur little or no cost and may, in fact, achieve cost savings." Regulatory Analysis Section 4,- page 8 - The following statement is made about the cost impact of the changes proposed in the Draft RG: "It could also lead to cost savings for the industry, especially with regard to applications for standard plant design certifications and combined licenses." These statements are only true if the new requirements proposed in the Draft RG are not applied to the existing fleet or any certified design or any design current submitted for design certification. Section D of the Draft RG supports this perspective in the following statement: "The NRC does not intend or approve any imposition or backfit in connection with its issuance." However, the third request for additional information issued against ANP-1 0281 P, <i>U.S. EPR Digital Protection System Topical Report</i>, indicates that NRC is already applying these new requirements to</p>	<p>The staff partially agrees. As stated in Section D of the draft RG the NRC does not intend or approve any imposition or backfit in connection with its issuance. Therefore, there is no cost impact for existing NPPs that do not involve digital upgrades. One of the benefits of revising the RG is that the new revision may result in cost saving for most (not all) applicants/licensees due to the reduction of licensing uncertainty with regard to digital upgrades. Although some language in the draft may have caused confusion with regard to component-level manual control and diversity guidance (BTP 7-19), adding new requirements is not the intent of the draft. The draft will be revised to remove guidance associated with component-level manual controls and to distinguish the existing requirements of IEEE 603-1991 and the guidance of BTP 7-19 (see above responses). There is no significant cost incurred as the result of the revision of the RG since no new regulatory requirement/guidance is introduced in the revision.</p> <p>The NRC, of course, has not issued a license for any plant based on the USEPR design, nor is the design currently certified. Therefore neither the backfit protection of the 10CFR52.63 apply to the USEPR. The staff might consider acknowledging that it could cost AREVA to conform to this revised RG.</p>

AREVA NP, Inc. Comments (ML0901401201)

Section of DG-1190	Comment	Resolution
	designs certification applications even though the guidance post dates the guidance applicable for the U.S. EPR based on 10 CFR 52.47 (a)(9). Significant design modifications would be required to bring these designs into alignment with this guidance. Significant cost would be incurred, both in the design and licensing areas. This new guidance would certainly not result in cost savings for AREVA NP.	

General Electric-Hitachi (GEH) Comments (ML090650474)		
Section of DG-1190	Comment	Resolution
<p>Section C Regulatory Positions 4 & 5</p>	<p>In general, GEH found the document to establish acceptable and useful guidance regarding certain aspects of control systems. However, there are certain areas where GEH suggests changes to the wording in order that the guidance does not preclude a vendor from designing a digital control system that minimizes the potential for some of the failure modes of concern. Specifically, GEH disagrees with the regulatory positions presented in paragraphs C.4 and C.5 of DG-1190 which conflate the requirements for manually initiated protective actions with those for diverse initiation of protective actions. Specifically, paragraph C.4 should be limited to the following requirement: "No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means." Paragraph C.5 should also be deleted as it places constraints on the design of the manual initiation systems and may have a negative impact on plant safety. The suggested wording and the basis for GEH's comments are provided below.</p> <p><u>Recommended Modifications to Paragraphs C.4 and C.5</u></p> <p>4. The amount of equipment common to manual and automatic initiation should be kept to a minimum. It is preferable to limit such common equipment to the final actuation devices and the actuated. No single failure within manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means. In case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment.</p> <p>5. Manual initiation of protective actions should depend on the operation of a minimum of equipment, consistent with Positions 1, 2, 3, and 4 above.</p> <p><u>Basis for Comments</u></p> <p>In order to conform with the guidance in paragraph C.2 of DG-1190,</p>	<p>The staff partially agrees. Although some language in the draft RG may have caused confusion, conflating the requirements for manually initiation of protective actions with those for diverse initiation of protective action is not the intent of the draft. However, with more and more nuclear power plants participating in digitalization of I&C systems and the potential for common-cause failure becoming increasingly important as the complexity of digital and advanced analog protection systems has increased, addressing diverse manual control for computer-based protective systems is appropriate and necessary. In an effort to eliminate the confusion, the draft will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions. The Discussion section will include the following:</p> <p>"This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation, as incorporated in 10CFR50.55a(h) and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet guidance specified in Point 4 of BTP 7-19."</p> <p>Guidance subject to diversity will be removed from Position 4 and will be addressed under new Position 7 as an effort to distinguish the difference between guidance for manual controls that are subject to IEEE Std 603-1991 and diverse manual controls that are subject to BTP 7-19.</p> <p>Position 4 will be revised to read:</p> <p>"No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means."</p> <p>The new Position 7 will Read:</p>

General Electric-Hitachi (GEH) Comments (ML090650474)

Section of DG-1190	Comment	Resolution
	<p>the position presented in paragraph C.4 would imply complete, parallel hardwiring from the Main Control Room to the “safety equipment,” bypassing the Digital I&C System (DCIS). This imposes an additional level of diversity beyond that required by regulation or previous regulatory guidance. In addition and importantly, such a design requirement could significantly increase costs without enhancing reactor safety, as well as introducing additional risk, as discussed further below.</p> <p>Imposing limits on the degree of common equipment between automated and manual functions is not appropriate because the primary function of manual controls for protective actions is not to mitigate the effects of a failure in the automated controls; rather manual controls provide additional capabilities to plant operators. The first sentence of paragraph C.4 may represent a design solution specific to one vendor, but it does not provide flexibility to those vendors using other DCIS concepts. That is, a DCIS with a design approach inconsistent with the regulatory position proposed in paragraph C.4 could provide equivalent protection. For example, a design that has a diversity of platforms to address the protective actions can provide a high degree of safety. The guidance should not be so specific to preclude other design solutions that may use a different approach.</p> <p>More specifically, the second sentence of paragraph C.4 would preclude the use of standard DCIS designs since it would recommend wiring around DCIS. The direct connection of some plant components to manual controls in the Main Control Room, bypassing the DCIS logic and interlocks, would not – in all cases – enhance plant safety because such a design may increase the probability of inadvertent actuation of components. In fact, such a design also may increase the potential for component damage by operating components without proper process interlocks. For example, manual controls that bypass the DCIS could allow the plant operator to manually start a pump with the pump’s suction valve closed.</p> <p>The last two sentences of C.4 should be deleted since they repeat and expand on the material in the second sentence for the reasons described above.</p> <p>Finally, item C.5 should be deleted since the minimization of the</p>	<p>“In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant’s electromechanical equipment.”</p> <p>The staff disagrees with the proposed deletion of Position 5. Section 6.2.1 of IEEE Std 603-1991 requires, in part, that the means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment.” Position 5 neither imposes the limitation of the amount of equipment nor addresses common cause failure as the concern. Position 5 is consistent with IEEE Std 603-1991 and not a new regulatory position, and therefore will be retained.</p>

General Electric-Hitachi (GEH) Comments (ML090650474)		
Section of DG-1190	Comment	Resolution
	<p>equipment does not necessarily result in improved safety for the same reasons specified above. Alternately, if the intent of this paragraph is to address manual protective actions implemented specifically to address potential common mode failure of the primary controls for automated and manual protective actions, the paragraph could be modified to limit the scope of the position to a diverse manual approach (although GEH recommends deletion of regulatory position C.5).</p> <p>In considering risk perspectives, probabilistic risk assessment (PRA) insights also support the conclusion that, without the above-suggested modifications, the proposed guidance in paragraphs C.4 and C.5 could result in designing a plant that is actually less safe. When the pros and cons of this design configuration are combined, the net effect could be a significant reduction in safety. For one plant design, the resulting increased probability of fire-induced shorting alone could significantly increase the Fire PRA core damage frequency, making it the dominant contributor to risk. Moreover, the risk of bypassing the logic and protection interlocks by improper operation of manual controls could result in an increased core damage frequency in all risk models (e.g., internal, fire, flood). These risk insights support the above-suggested changes to the proposed guidance in DG-1190.</p>	

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
<p>Section B 3rd paragraph page 3</p>	<p><u>Current text:</u> "... individual means should also be provided to implement manual initiation at the plant component level since manual initiation for each appropriate plant system component (e.g., start pump, open or close valve) is subsequently required to provide (1) the completion of the safety function and (2) high functional reliability for the protective system as set forth in GDC 13 and GDC 21 of Appendix A to 10 CFR Part 50."</p> <p><u>Comment 1:</u></p> <p>Component level manual control is a new requirement that goes beyond IEEE-279/603 and beyond the scope of this Regulatory Guide. IEEE-279/603 requires only system level controls, not component level controls. It is for the initiation of each protective action, not for completion of the protective action. The title and scope of this Regulatory Guide also pertain only to manual initiation of the protective action, not completion of the protective action.</p> <p>High functional reliability, as set forth in GDC 13 and 21, is achieved through safety functions that comply with the requirements of IEEE-279/603, including compliance to quality, qualification and single failure criteria. Manual controls are not required to achieve high reliability for safety functions.</p> <p><u>Recommendation:</u></p> <p>The requirement for component level manual control should be eliminated or revised. This paragraph should be replaced with the requirements found in Section 6.2 of IEEE Std 603.</p>	<p>The staff agrees to remove the third paragraph of Section B from the draft.</p>
<p>Section B 4th paragraph page 3</p>	<p><u>Current text:</u></p> <p>"Protective actions selected to be controlled manually are subject to consideration of (1) the time available to the operator to analyze and manually respond to an adverse condition, normally 30 minutes unless specifically justified..."</p> <p><u>Comment 2:</u></p> <p>A 30 minute prerequisite for manual control is a new requirement that goes beyond IEEE-279/603. The determination of whether a protective</p>	<p>The staff agrees to remove the 30-minute reference from the draft.</p>

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
	<p>action should be controlled manually or automatically is the result of the human factors engineering process. The function allocation process considers numerous factors including time available based on the safety analysis and time required based on numerous HFE factors such as available indications and alarms, task complexity, task frequency, other concurrent tasks and control room staffing.</p> <p><u>Recommendation:</u> The 30 minute reference should be eliminated.</p>	
<p>Section B 6th paragraph page 4</p>	<p><u>Current text:</u> “these manual controls and indications must consist of safety-related devices ... dedicated to specific safety divisions.”</p> <p>Comment 3: Manual controls dedicated to specific safety division is a new requirement that goes beyond IEEE-279/603. There is considerable industry precedence for system level manual initiation pushbuttons that actuate reactor trip and ESF functions for all divisions concurrently; these exist at both CE and Westinghouse plants. In addition, ISG-04 (Digital I&C Interim Staff Guidance on communications) allows multi-division safety related workstations. As long as the manual controls meet the single failure criteria (i.e. no single failure shall prevent credited manual control of the safety function), there is no reason to restrict controls to a single division. Compliance to the single failure criteria can be assured with redundant multi-division safety related pushbuttons or redundant multi-division safety related workstations, where each redundant device is independently powered, physically separated and electrically isolated from the other.</p> <p><u>Recommendation:</u> Rewrite the text to comply with existing guidance.</p>	<p>The staff partially agrees. The draft RG updates the “system level” term used in IEEE Std 279-1971 to “division level” term used in IEEE Std 603-1991. However, to eliminate the confusion, the 6th paragraph will be revised to read:</p> <p>“Section 5.6.3.1 of IEEE Std 603-1991 specifies that interconnected “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.” Therefore, equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, nonsafety multidivisional control and display stations may be used to perform functions that support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Nonsafety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant’s safety analyses.”</p> <p>This response also applies to comment 5.</p>
<p>Section B 11th paragraph</p>	<p><u>Current text:</u> “This Regulatory Guide focuses on criteria for safety-related equipment or systems and does not address diverse manual-initiation</p>	<p>The staff partially agrees. The purpose of RG 1.62 is to provide guidance/acceptable methods for use in complying with the NRC regulations with respect to the means for manual initiation of protective actions. BTP 7-19 provides “guidance for evaluating an</p>

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
<p>page 5</p>	<p>equipment that is not classified as part of a safety system.”</p> <p><u>Comment 4:</u></p> <p>It is more appropriate to state that this Regulatory Guide focuses on criteria for compliance with the credited manual control requirements defined in IEEE-279/603, rather than manual controls that are part of the safety system. This is because a supplier/licensee may elect to provide safety related controls for compliance with position 4 of BTP 7-19 or safety related controls for other functions not required by IEEE-279/603. If those controls are not credited for compliance with IEEE-279/603, it would not be appropriate to extend this regulatory guidance to those controls.</p> <p><u>Recommendation:</u></p> <p>Rewrite the text to comply appropriately limit the scope.</p>	<p>applicant/licensee’s diversity and defense-in-depth (D3) assessment and the design of manual controls and displays to ensure conformance with the NRC positions on D3 for I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS).” Both IEEE Std 603-1991 and BTP 7-19 address manual control for protective systems. Thus, (1) there is no conflict between the two, and (2) with more and more nuclear power plants participating in digitalization of I&C systems and the potential for common-cause failure becoming important as the complexity of digital and advanced analog protection systems has increased, addressing diverse manual control for computer-based protective systems is necessary. However, to eliminate the confusion it may have caused, the draft will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions. The Discussion section will include the following:</p> <p>“This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation as incorporated in 10CFR50.55a(h) and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet the guidance specified in Point 4 of BTP 7-19.”</p> <p>And the affected paragraph will be revised to read:</p> <p>“2. <u>Meeting BTP 7-19 guidance:</u></p> <p>The potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed for D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of</p>

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
		<p>diverse non-safety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause failures in computer-based safety systems. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems to identify design vulnerabilities to common-cause failure. The fourth point of the Commission's diversity position listed in BTP 7-19 states in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or non-safety. Guidance provided to NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of NRC position on D3 should be connected downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic. 3. <u>Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance:</u></p> <p>As an alternative to two different manual controls discussed above, applicants or licensees may also propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies criteria of both IEEE Std 603-1991 and Point 4 of NRC position on D3."</p>
<p>Section B 6th paragraph page 4</p>	<p><u>Comment 5:</u> The paragraph should be expanded to reflect the context of the referenced section of IEEE Std 603. <u>Recommendation:</u> Reword the second sentence adding the following (additions are in</p>	<p>See response for comment 3.</p>

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
	<p>italics) - Clause 5.6.3.1 of IEEE Std 603-1991 specifies that interconnected “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems” <i>up to isolation devices provided to effect the safety system boundary.</i></p>	
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Current text:</u> “Individual means should also be provided for manual initiation of each plant system component ...”</p> <p>Comment 6: Component level manual control is a new requirement that goes beyond IEEE-279/603 and beyond the scope of this Regulatory Guide. IEEE-279/603 requires only system level controls, not component level controls. It is for the initiation of each protective action, not for completion of the protective action. The title and scope of this Regulatory Guide also pertain only to manual initiation of the protective action, not completion of the protective action.</p> <p><u>Recommendation:</u> This requirement should be deleted.</p>	<p>The staff agrees. The guidance associated with component-level controls will be removed. Position 1 will be revised to read:</p> <p>“Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).”</p>
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Current text:</u> “In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant’s digital I&C safety system outputs.”</p> <p>Comment 7: This requirement is applicable to the diverse automated and manual controls credited for accident mitigation with a concurrent CCF in the digital safety systems, per BTP-19. The manual controls credited for compliance with IEEE-279/603 are not required to be downstream of the plant’s digital safety system outputs, as long as a CCF of these manual controls is considered in the BTP-19 analysis. Position 5 is sufficient to ensure manual controls are implemented with sufficient simplicity.</p> <p><u>Recommendation:</u> The last two sentences of Section C, Position 4 should be deleted.</p>	<p>The staff agrees. Position 4 of the draft RG may have caused confusion by not distinguishing between guidance for manual controls that are subject to IEEE Std 603-1991 and diverse manual controls that are subject to BTP 7-19. In an effort to eliminate the confusion, the diversity guidance will be removed from Position 4 and will be addressed in new Position 7. Also, to make the distinction between requirements of IEEE Std 603-1991 and the guidance of BTP 7-19, the opening statement of Section C will be revised to read:</p> <p>“Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to manual initiation of protective actions. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance.”</p>

Nuclear Energy Institute (NEI) Comments (ML090650470)

Section of DG-1190	Comment	Resolutions
		<p>Position 4 will be revised to read:</p> <p>“No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means.”</p> <p>The new Position 7 will Read:</p> <p>“In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant’s electromechanical equipment.”</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
<p>Section B 3rd paragraph page 3</p>	<p><u>Comment 1</u> IEEE 603, clause 6.2.3, states “Means shall be provided to implement manual actions necessary to maintain safe conditions after protective actions are completed as specified in 4.10”. IEEE 603 does not require that each Class 1E component have individual component controls in the control room if they are not required to maintain the plant in a safe shutdown condition.</p>	<p>The staff agrees. The 3rd paragraph will be removed from the draft RG.</p>
<p>Section B 2nd paragraph page 3</p>	<p><u>Comment 2</u> IEEE 603, clause 7.2 states “If manual control of any actuated component in the execute features is provided, the additional design features necessary to accomplish such manual control shall not defeat the requirements of 5.1 and 6.2”. It does not state the manual controls “be subject to the single-failure criterion”. The wording must be changed for a Class 1E component is associated with a division or train, and the manual controls associated with that component will only be associated with the respective division or train and will not meet the single-failure criterion.</p>	<p>The staff agrees. The affected sentence will be revised to reflect the content of Section 7.2 of IEEE Std 603-1991. The revised sentence will read:</p> <p>“Section 7.2 requires, in part, that additional design features in the execute features necessary to accomplish manual control of actuated component shall not defeat the requirements of single-failure criterion.”</p>
<p>Section B 1st paragraph page 3</p>	<p><u>Comment 3</u> A definition should be provided for the term “advanced analog systems.” What types of platforms are encompassed by this term and what are new vulnerabilities associated with their use?</p>	<p>The staff partially agrees. The affected statement presents a fact in which existing I&C equipment in NPPs has been replaced by digital or advanced analog equipment. Advanced analog technology is generally known as a wide range of integrated/semiconductor circuits. There is no need to define a well known technology. However, to address the reason why digital I&C and advance analog technologies are subject to new vulnerabilities, the affected paragraph will be revised to read:</p> <p>“Existing instrumentation and control (I&C) equipment in nuclear power plants is being replaced with computer-based digital I&C systems or advanced analog systems. However, if designed, installed, operated, or maintained improperly, these technologies may pose new vulnerabilities for the nuclear power plant, compared to existing I&C systems.”</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
<p>Section B 4th paragraph page 3</p>	<p><u>Comment 4</u> ANSI/ANS 58.8 has always been used as a guideline for allowable operator action times following an anticipated operational occurrence (AOO) or design basis event (DBE), i.e., 5 to 10 minutes for an AOO and 20 to 30 minutes for a DBE. Is this regulatory guide essentially stating that 30 minutes must be assumed for all operator action times in the future? Why is the standard revising the existing guidance that has been used for many years?</p>	<p>The staff agrees to remove the 30-minutes reference from the draft.</p>
<p>Section B 7th paragraph page 4</p>	<p><u>Comment 5</u> It would be better if the regulatory guide only referred to Regulatory Guide 1.97, and not to a specific revision. There are no operating plants licensed to revision 4 which endorses IEEE 497-2002. Most operating plants are licensed to Regulatory Guide 1.97, revision 3.</p>	<p>The staff agrees to remove the specific version and issue date associated with referenced regulatory guides.</p>
<p>Section B 8th paragraph page 4</p>	<p><u>Comment 6</u> Why is this regulatory guide even addressing software common cause failure (CCF) since scenarios resulting from an initiating event concurrent with a postulated software CCF are beyond design basis events? The last four sentences of this paragraph should be removed beginning with "IEEE Std 7-4.3.2-2003 ..."</p>	<p>The staff partially agrees. As more and more nuclear power plants participate in digitalization of I&C systems and the complexity of digital and advanced analog protection systems has increased, the potential for software common-cause (CCF) failure has become increasingly important and needs to be addressed. However, to distinguish the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions, the discussion on CCF and diversity will be moved to the end of the discussion section, where it addresses the need of Diversity and Defense-in-Depth (D3) for manual initiation of protective actions that is subject to BTP 7-19.</p> <p>This response also applies to comment 7.</p>
<p>Section B 11th paragraph page 5</p>	<p><u>Comment 7</u> Again, this paragraph is discussing requirements following an initiating event concurrent with a postulated software CCF which is beyond a design basis event. IEEE 603 is only applicable to AOOs and DBEs. This paragraph should be removed and addressed in a D3 document, e.g, DI&C-ISG-02.</p>	<p>The staff disagrees. As stated in the response for comment 6 above, it is important and necessary to address the need of D3 for manual initiation of protective actions that are not subject to IEEE Std 603-1991 requirements. The affected paragraph will be revised to address this need and also to clarify the scope of the draft, which covers IEEE Std 603-1991 requirements separately from the guidance of BTP 7-19 in regards to manual initiation for protective actions. The opening statement of the Discussion</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
		<p>section includes the following:</p> <p>“This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation, as incorporated in 10CFR50.55a(h) and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet the guidance specified in Point 4 of BTP 7-19.”</p> <p>And the affected paragraph will be revised to read:</p> <p>“2. <u>Meeting BTP 7-19 guidance:</u></p> <p>The potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed for D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of diverse non-safety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause failures in computer-based safety systems. In addition, NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems to identify design vulnerabilities to common-cause failure. The fourth point of the Commission’s diversity position listed in BTP 7-19 states in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or non-safety. Guidance provided to NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of NRC position on D3 should be connected downstream of</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
		<p>the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.</p> <p>3. <u>Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance:</u></p> <p>As an alternative to two different manual controls discussed above, applicants or licensees may also propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies criteria of both IEEE Std 603-1991 and Point 4 of NRC position on D3."</p> <p>Also see response for comment 6.</p>
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 8</u> Refer to comment 2 above</p>	<p>The staff agrees to remove the guidance associated with component level manual control. Regulatory Position 1 will be revised to read:</p> <p>"Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve)."</p> <p>Also see response for comment 1.</p>
<p>Section C Regulatory Position 3 page 6</p>	<p><u>Comment 9</u> The first sentence should be modified to state the following: "The control interfaces for manual initiation of protective actions on a plant system component basis (required to maintain safe plant conditions) and on a system-level basis for each division should be located in the control room".</p>	<p>The staff agrees to remove guidance associated with component level. Position 3 will be revised to read:</p> <p>"The control interfaces for manual initiation of protective actions on a division-level basis should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the plant conditions for which the protective actions of the</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
		<p>safety system shall be initiated as required in Section 4.10.1 of IEEE Std 603-1991. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.”</p>
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Comment 10</u> This paragraph essentially requires that the component manual controls not be implemented through a software path for a digital protection system implementation. In other words, the signal prioritization between automatic and manual command signals from the protection system must be performed in the priority module (as is implemented in the relay logic of most operating plants). This requirement increases the complexity of the priority module which makes it more difficult to use FPGAs upon which to implement the logic (100% testability). I recommend that additional discussion be added to this paragraph discussing the conflicting requirements if the manual component controls are excluded from the protection system software and the increased complexity in the protection system priority logic.</p>	<p>The staff partially agrees. Although Position 4 of the draft may have caused confusion by not distinguishing between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with respect to manual initiation of protective actions, this position does not imply the stated concern. However, as an effort to eliminate the confusion, the diversity guidance will be removed from Position 4 and will be addressed in new Position 7. Also, to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19, the opening statement of Section C will be revised to read:</p> <p>“Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to manual initiation of protective actions. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance.”</p> <p>Position 4 will be revised to read:</p> <p>“No single failure within the manual, automatic, or common portions of the protection system should prevent initiation of a protective action by manual or automatic means.”</p> <p>The new Position 7 will Read:</p> <p>“In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These</p>

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
		connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment."
Section A 4 th paragraph page 2	<u>Comment 11</u> The author should note that IEEE 603 is written for Design Basis Events and not Beyond Design Basis Events, which later in this draft guide becomes a dominant issue (SWCMFs).	See response for comments 6 and 7.
Section A 6 th paragraph page 2	<u>Comment 12</u> In this area, IEEE 603 is referring to divisional level manual switches and not component level switches. Component control is only discussed if necessary for safe shutdown.	See response for comment 1 with regard to component-level manual control.
Section B 10 th paragraph pages 4 & 5	<u>Comment 13</u> Why is the draft RG referencing a computer-based Equipment Qualification RG? Most of this paragraph deals with computer based qualification such as IEEE 7-4.3.2 and RG 1.209. These areas should be removed from the draft RG.	The staff disagrees. Section 5.4 of IEEE 603-1991 requires that safety system equipment be environmentally qualified. Reference to regulatory guides and IEEE standards in regard to environment qualification for Class 1E equipment is appropriate.
Regulatory Analysis Sections 1 & 2 pages 6 & 7	<u>Comment 14</u> This draft RG has included more than the referencing of IEEE 603 and digital capabilities. It has included Beyond Design Basis Event guidance for manual initiation, actual guidance for allowed times (30 minutes), computer qualification criteria, and increased guidance for component controls.	See response for comments 1, 4, 6, 7, 8, 10, and 13.
Regulatory Analysis Section 4 page 8	<u>Comment 15</u> The NRC should identify where the cost savings will be for a plant to implement this draft RG.	The staff partially agrees. As stated in Section D of the draft RG the NRC does not intend or approve any imposition or backfit in connection with its issuance. Therefore, there is no cost impact for existing NPPs that do not involve digital upgrades. One of the benefits of revising the RG is that the new revision may result in

Data Systems and Solutions (DSS) Comments (ML090650473)

Section of DG-1190	Comment	Resolution
		<p>cost saving for most (not all) of applicants/licensees due to reduction of licensing uncertainty with regard to digital upgrade. Although some language in the draft may have caused confusion with regard to component-level manual control and diversity guidance (BTP 7-19), adding new requirements is not the intent of the draft. The draft will be revised to remove guidance associated with component-level manual controls and to distinguish the existing requirements of IEEE 603-1991 and the guidance of BTP 7-19 (see above responses). There is no significant cost incurred as the result of the revision of the RG since no new regulatory requirement/guidance is introduced in the revision.</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
<p>Section A 6th paragraph page 2</p>	<p><u>Comment 1</u> Clause 6.2 (.3) of IEEE 603 requires (in part) that means be provided to implement manual actions necessary to maintain safe conditions ...these controls shall be located in areas that are accessible. It does not state specifically in the control room.</p>	<p>The staff agrees. The affected sentence will be revised to read: "Section 6.2 of IEEE Std 603-1991 requires, in part, that means be provided in the control room to implement the manual actions necessary to maintain safe controls after the protective actions are completed."</p>
<p>Section B 1st paragraph page 3</p>	<p><u>Comment 2</u> A definition should be provided for advanced analog controls and why they are subject to new vulnerabilities.</p>	<p>The staff partially agrees. The affected statement presents a fact in which existing I&C equipment in NPPs has been replaced by digital or advanced analog equipment. Advanced analog technology is generally known as a wide range of integrated/semiconductor circuits. There is no need to define a well known technology. However to address the reason why digital I&C and advance analog technologies are subject to new vulnerabilities, the affected paragraph will be revised to read: "Existing instrumentation and control (I&C) equipment in nuclear power plants is being replaced with computer-based digital I&C systems or advanced analog systems. However, if designed, installed, operated, or maintained improperly, these technologies may pose new vulnerabilities for the nuclear power plant compared to existing I&C systems."</p>
<p>Section B 2nd paragraph page 3</p>	<p><u>Comment 3</u> Clause 7.2 actually states in part that manual control should not defeat the single failure criterion. Component controls are part of a division/train and as such are not required to separately or individually meet the SF criterion.</p>	<p>The staff agrees. The affected sentence will be revised to reflect the content of IEEE Std 603-1991, Section 7.2. The revised sentence will read: "Section 7.2 requires, in part, that additional design features in the execute features necessary to accomplish manual control of the actuated component shall not defeat the requirements of single-failure criterion."</p>
<p>Section B 3rd paragraph page 3</p>	<p><u>Comment 4</u> Not all component controls are required for completion of the safety function and the claim of increased reliability is questionable. IEEE 603 does not require this nor did the previous RG 1.62</p>	<p>The staff agrees to remove the guidance associated with component-level manual control. As the result, the affected paragraph will be deleted. This response also applies to comment 12.</p>

South Texas Project (STP) Comments (ML090650472)		
Section of DG-1190	Comment	Resolution
<p>Section B 4th paragraph page 3</p>	<p><u>Comment 5</u> What is the reason for requiring a specific manual action time of 30 minutes. It is recognized that this is used for the D3 ISG and the reasoning was the unknowns associated with a SWCMF. The ANS standard is written differently with two distinct times for AOOs and DBAs.</p>	<p>The staff agrees to remove the 30-minutes reference from the draft.</p>
<p>Section B 6th paragraph page 4</p>	<p><u>Comment 6</u> The statement is made that manual controls and indications consist of safety-related devices with safety-related software. Why is the NRC requiring this (software) for manual controls and indications.</p>	<p>The staff agrees. Also, to incorporate other public comments the paragraph will be revised to read:</p> <p>“Section 5.6.3.1 of IEEE Std 603-1991 specifies that “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.” Therefore, equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform functions that support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety related control and display equipment that is credited in the plant safety analyses.”</p>
<p>Section B 7th paragraph page 4</p>	<p><u>Comment 7</u> The RG should not reference a RG with a particular revision. Most operating plants use Revision 3 of RG 1.97. IEEE 603 references an earlier version of IEEE 497. Operating plants are not licensed to the 2002 version.</p>	<p>The staff agrees to remove the specific version or issue date associated with referenced regulatory guides.</p>
<p>Section B 8th paragraph page 4</p>	<p><u>Comment 8</u> Why is this RG discussing beyond design basis events since IEEE 603 does not (1st comment). The last four sentences of this paragraph should be removed.</p>	<p>The staff partially agrees. Although the affected paragraph may have caused confusion by not distinguishing between requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions, addressing diversity (BTP 7-19) with respect to manual control for computer-based protective systems to reduce licensing uncertainties is</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
		<p>appropriate and necessary.</p> <p>The purpose of RG 1.62 is to provide guidance/acceptable methods for use in complying with the NRC regulations with respect to the means for manual initiation of protective actions. BTP 7-19 provides “guidance for evaluating an applicant/licensee’s diversity and defense-in-depth (D3) assessment and the design of manual controls and displays to ensure conformance with the NRC positions on D3 for I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS).” Both IEEE Std 603-1991 and BTP 7-19 address manual control for protective systems. Thus, (1) there is no conflict between the two and (2) as more nuclear power plants participate in digitalization of I&C systems and the potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased, addressing diversity for manual control is appropriate and necessary. However, to eliminate the confusion it may have caused, the draft will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 in regard to manual initiation of protective actions. The diversity guidance will be removed from the affected paragraph and will be addressed at the end of the Discussion section.</p> <p>This response also applies to comment 11.</p>
<p>Section B 9th paragraph page 4</p>	<p><u>Comment 9</u> This comment is the same as above. The remainder of the paragraph starting with “Regulatory Guide 1.152” should be deleted.</p>	<p>The staff disagrees. Maintaining independence between redundant portions of the safety system is essential to the effective use of the single-failure criterion. Reference to regulatory guide and IEEE standard within regard to independent guidance for safety-related equipment is appropriate.</p>
<p>Section B 10th paragraph pages 4 & 5</p>	<p><u>Comment 10</u> Discussing computer qualification and harsh environment is questionable for this RG. The qualification effort should be restricted unless the manual components are part of a computer-based system, which is usually not the case for simplicity and automatic failure</p>	<p>The staff disagrees. Section 5.4 of IEEE 603-1991 requires that safety system equipment be environmentally qualified. Reference to regulatory guides and IEEE standards in regard to environment qualification for Class 1E equipment is appropriate.</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
	reasons.	
<p>Section B 11th paragraph page 5</p>	<p><u>Comment 11</u> Same as comment 10. This entire paragraph should be deleted. It is already covered in BTP 7-19 and the ISG.</p>	<p>The staff disagrees. As stated in the response for comment 8 above, addressing diversity (BTP 7-19) with respect to manual control for computer-based protective systems to reduce licensing uncertainties is appropriate and necessary. However, to eliminate the confusion it may have caused, the draft RG will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with regard to manual initiation of protective actions. The opening statement of the Discussion section includes the following:</p> <p>“This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet the guidance specified in Point 4 of BTP 7-19.”</p> <p>And the affected paragraph will be revised to read:</p> <p>“2. <u>Meeting BTP 7-19 guidance:</u></p> <p>The potential for common-cause failure has become increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed for D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of diverse non-safety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause failures in computer-based safety systems. In addition, NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
		<p>to identify design vulnerabilities to common-cause failure. The fourth point of the Commission’s diversity position, listed in BTP 7-19 states, in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or non-safety. Guidance provided to NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of NRC position on D3 should be connected downstream of the plant’s digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant’s electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic. 3. <u>Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance:</u></p> <p>As an alternative to two different manual controls discussed above, applicants or licensees may also propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies criteria of both IEEE Std 603-1991 and Point 4 of NRC position on D3.”</p>
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 12</u> The requirement for manual component controls needs to be rewritten. It seems that NRC is requiring plant system component level controls for the completion of all safety functions and to increase reliability. This is beyond IEEE 603.</p>	<p>The staff agrees to remove the guidance associated with component level manual control. Regulatory Position 1 will be revised to read:</p> <p>“Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).”</p> <p>This response also applies to comments 3, 4, 13, 15, 16, and 17.</p>
<p>Section C</p>	<p><u>Comment 13</u></p>	<p>The staff agrees to remove the guidance associated with</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
<p>Regulatory Position 3 page 6</p>	<p>The requirement for all component controls being in the control room is new and needs to be justified. IEEE 603 only requires those component controls necessary for safe shutdown action to be in the control room.</p>	<p>component-level manual control from Regulatory Position 3. The revised Regulatory Position 3 will read:</p> <p>“The control interfaces for manual initiation of protective actions on a division-level basis should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the plant conditions for which the protective actions of the safety system shall be initiated as required in Section 4.10.1 of IEEE Std 603-1991. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.”</p> <p>This response also applies to comments 15, 16, and 17.</p>
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Comment 14</u> Item 4 seems to require a priority logic module such as a FPGA. This needs to be justified and explained. How is the manual actuation to be kept simple?</p>	<p>The staff partially agrees. Although Position 4 of the draft may have caused confusion by not distinguishing between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with respect to manual initiation of protective actions, this position does not imply the stated concern. However, as an effort to eliminate the confusion, the diversity guidance will be removed from Position 4 and will be addressed in new Position 7. Also, to make the distinction between requirements of IEEE Std 603-1991 and the guidance of BTP 7-19, the opening statement of Section C will be revised to read:</p> <p>“Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to manual initiation of protective actions. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying regulatory requirements for both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance.”</p> <p>Position 4 will be revised to read:</p> <p>“No single failure within the manual, automatic, or common</p>

South Texas Project (STP) Comments (ML090650472)

Section of DG-1190	Comment	Resolution
		<p>portions of the protection system should prevent initiation of a protective action by manual or automatic means.”</p> <p>The new Position 7 will Read:</p> <p>“In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant’s electromechanical equipment.”</p>
<p>Regulatory Analysis Sections 1 & 2 pages 6 &7</p>	<p><u>Comment 15</u> The draft RG content goes beyond the purpose stated and formulates new positions not based on IEEE 603.</p>	<p>See response for comments 12 and 13.</p>
<p>Regulatory Analysis Sections 3.2 2nd paragraph page 8</p>	<p><u>Comment 16</u> The draft RG cites the benefit of enhancing reactor safety by endorsing the most current IEEE on safety systems endorsed by the NRC. The Draft RG goes beyond this endorsement.</p>	<p>See response for comments 12 and 13.</p>
<p>Regulatory Analysis 2nd paragraph of Section 3.2 (page 7) & Section 4 page 8</p>	<p><u>Comment 17</u> Does the NRC have actual numbers for the cost savings and where does the draft RG actually achieve this? Based on the high cost of any safety related system/equipment, the impact of this RG will be extremely high and not “cost affective”.</p>	<p>The staff partially agrees. As stated in Section D of the draft RG the NRC does not intend or approve any imposition or backfit in connection with its issuance. Therefore, there is no cost impact for existing NPPs that do not involve digital upgrades. One of the benefits of revising the RG is that the new revision may result in cost saving for most (not all) of applicants/licensees due to reduction of licensing uncertainty with regard to digital upgrade. Although some language in the draft may have caused confusion with regard to component-level manual control and diversity guidance (BTP 7-19), adding new guidance is not the intent of the draft. The draft will be revised to remove guidance associated</p>

South Texas Project (STP) Comments (ML090650472)		
Section of DG-1190	Comment	Resolution
		with component-level manual controls and to distinguish the existing requirements of IEEE 603-1991 and the guidance of BTP 7-19 (see above responses). There is no significant cost incurred as the result of the revision of the RG since no new regulatory requirement/guidance is introduced in the revision.

Hurst Technologies Comments (ML090650469)

Section of DG-1190	Comment	Resolution
<p>General</p>	<p><u>Comment 1:</u> The requirements as stipulated in the draft RG appear to be an attempt to move, what is currently a beyond design bases event (software common cause failure; SWCMF), to the level of a DBE and require full implementation of codes and standards previously not required for manual initiation. The issue of SCMF is already addressed in existing regulatory guidance and should not be included in this issue.</p>	<p>The staff disagrees. As more and more nuclear power plants participate in digitalization of I&C systems and the complexity of digital and advanced analog protection systems has been increased, the potential for software common-cause (CCF) failure has become increasingly important and needs to be addressed. However, to eliminate the confusion, the draft RG will be revised to make the distinction between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with regard to manual initiation of protective actions.</p>
<p>Section B</p>	<p><u>Comment 2:</u> Interpretation of IEEE-603 Requirements: In Section B. Discussion, the descriptions of IEEE-603 requirements go beyond the specific requirements of the standard and add additional requirements with no real bases. Example, the requirement that manual control must meet the single failure criterion.</p>	<p>The staff disagrees. As stated in 8th paragraph of Section B: “The single-failure criterion of IEEE Std 603-1991, Section 5.1, applies to safety systems whether control is by automatic or manual means.” Therefore, addressing single failure criterion is not beyond IEEE Std 603-1991 requirements.</p>
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 3:</u> This is a significant expansion of the current requirements and designs with no defined benefit or bases. The need is to have manual capability to support safety functions defined and not just because a piece of equipment is part of a system performing a safety function.</p>	<p>The staff agrees to remove the guidance associated with component-level manual control from Regulatory Position 1. The revised Regulatory Position 1 will read: “Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).”</p>
<p>Section C Regulatory Position 3 page 6</p>	<p><u>Comment 4:</u> The requirement to have individual manual controls in the main control room far exceeds the safety need. The need for what and where manual controls should be part of the design and safety evaluation as generally defined by IEEE-603.</p>	<p>The staff agrees to remove the guidance associated with component-level manual control from Regulatory Position 3. The revised Regulatory Position 3 will read: “The control interfaces for manual initiation of protective actions on a division-level basis should be located in the control room. They should be easily accessible to the operator so that action can be taken in an expeditious manner at the point in time or under the plant conditions for which the protective actions of the safety system shall be initiated as required in Section 4.10.1 of</p>

Hurst Technologies Comments (ML090650469)

Section of DG-1190	Comment	Resolution
		IEEE Std 603-1991. Information displays associated with manual controls should (i) be readily present during the time that manual actuation is necessary, (ii) be visible from the location of the manual controls, and (iii) provide unambiguous indications that will not confuse the operator.”
<p>Section C Regulatory Position 5 page 6</p>	<p><u>Comment 5:</u> To meet the requirements of system level actuation beyond the digital I&C requires an additional automatic type control system (either conventional or digital) this leads to then having a third level of individual controls and an even more complex design. Once again, the prescriptive requirements should not be added as IEEE-603 addresses this issue appropriately.</p>	<p>The staff disagrees. Position 5 does not imply the stated concern. Section 6.2.1 of IEEE Std 603-1991 requires, in part, that the means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment. Position 5 is consistent with IEEE Std 603-1991 and not a new regulatory position.</p>
<p>Regulatory Analysis pages 6, 7, & 8</p>	<p><u>Comment 6:</u> The statement that this RG could lead to cost savings has no bases and based on our experience it will be a significant cost adder to current and new plants.</p>	<p>The staff partially agrees. As stated in Section D of the draft RG the NRC does not intend or approve any imposition or backfit in connection with its issuance. Therefore, there is no cost impact for existing NPPs that do not involve digital upgrades. One of the benefits of revising the RG is that the new revision may result in cost saving for most (not all) of applicants/licensees due to reduction of licensing uncertainty with regard to digital upgrade. Although some language in the draft may have caused confusion with regard to component-level manual control and diversity guidance (BTP 7-19), adding new guidance is not the intent of the draft. The draft will be revised to remove guidance associated with component-level manual controls and to distinguish the existing requirements of IEEE 603-1991 and the guidance of BTP 7-19 (see above responses). There is no significant cost incurred as the result of the revision of the RG since no new regulatory requirement/guidance is introduced in the revision.</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
<p>Section B 3rd paragraph page 3</p>	<p><u>Comment 1:</u> There appears to be a significantly expanded expectation for safety-related controls at the component level. The expectation and basis are not clear. For example, the third paragraph in Section B states "..., individual means should also be provided to implement manual initiation at the plant component level..." This appears to be a new Regulatory Position; however, it does not appear in Section C. If this is a new Regulatory Position, Westinghouse believes it is a significant expansion of the existing guidance in Regulatory Guide 1.62, Revision 0, beyond the scope of any requirement in IEEE Std 603. Moreover, it is not clear whether these additional controls are expected to be safety-related. If so, the single failure criteria should be applied at the protective action level (e.g., SI, Containment Spray, etc.), not at the individual component level within each division. If the intent is to add additional controls, added equipment complexity with no clear safety benefit may result.</p>	<p>The staff agrees to remove guidance associated with component-level for manual controls. As the result, 3rd paragraph of Section B will be deleted and Regulatory Position 1 (Section C) will be revised to read:</p> <p>“Means should be provided for manual initiation of each protective action (e.g., reactor trip, containment isolation) on a division-level basis, regardless of whether means are also provided to initiate the protective action at the component or channel level (e.g., individual control rod, individual isolation valve).”</p> <p>This response also applies to comments 9 and 10.</p>
<p>Section B 11th paragraph page 5</p>	<p><u>Comment 2:</u> The last sentence of Section B states, “.... this regulatory guide focuses on criteria for safety-related equipment of systems and does not address diverse manual-initiation equipment that is not classified as part of a safety system.” However, there is a relationship between IEEE Std 603, BTP 7-19, this regulatory guide and the concept of manual initiation of protective actions to cope with software common cause failure. Therefore, it is suggested that the last sentence in Section B be deleted and additional clarification be added.</p>	<p>The staff agrees. Also to eliminate the confusion between IEEE Std 603-1991 requirements and the guidance of BTP 7-19 with respect to manual initiation of protective actions, the opening statement of the Discussion section includes the following:</p> <p>“This regulatory guide provides an acceptable method for establishing the design criteria for existing I&C systems and for establishing the design criteria for digital and advanced analog systems for the manual initiation of protective actions. To meet these objectives, (1) manual initiation of protective actions provided by otherwise automatically initiated safety systems must meet requirements in IEEE Std 603-1991 in regard to manual initiation, as incorporated in 10CFR50.55a(h) and (2) manual initiation of protective actions provided as a diverse method for automatic initiation should meet the guidance specified in Point 4 of BTP 7-19.”</p> <p>And the affected paragraph will be revised to read:</p> <p>“2. <u>Meeting BTP 7-19 guidance:</u> The potential for common-cause failure has become</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
		<p>increasingly important as the complexity of digital and advanced analog protection systems has increased. Credible common-cause failures should be addressed for D3 in the system design. Approaches to address D3 considerations for automatically initiated protective actions may include the use of diverse non-safety manual controls. IEEE Std 7-4.3.2-2003 provides guidance on using diversity to address common-cause failures in computer-based safety systems. In addition, NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," issued December 1994 (Ref. 19), describes a method for analyzing computer-based nuclear reactor protection systems to identify design vulnerabilities to common-cause failure. The fourth point of the Commission's diversity position, listed in BTP 7-19 states, in part, that independent and diverse displays and manual controls should be available in the main control room so that operators can initiate a system-level actuation of critical safety functions. These displays and controls may be safety or non-safety. Guidance provided to NRC staff in BTP 7-19 asserts that manual controls provided for compliance with Point 4 of NRC position on D3 should be connected downstream of the plant's digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant's electromechanical equipment. The manual controls may be connected either to discrete hardwired components or to simple, dedicated, and diverse, software-based digital equipment that performs the coordinated actuation logic.</p> <p>3. <u>Meeting both IEEE Std 603-1991 requirements and BTP 7-19 guidance :</u></p> <p>As an alternative to two different manual controls discussed above, applicants or licensees may also propose, as an optional acceptable method, a single safety-related means of manual initiation of protective actions that satisfies criteria of both IEEE Std 603-1991 and Point 4 of NRC position on D3."</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Comment 3:</u></p> <p>The proposed Regulatory Position C.4 is a misapplication of the principle of diversity as described in Branch Technical Position (BTP) 7-19. The manual controls used to address Point 4 of BTP 7-19 and IEEE Std 603 only confuses the complicated and controversial topic of defense-in-depth and diversity. There is no provision in IEEE Std 603, and its companion standard IEEE Std 7-4.3.2, that precludes the use of digital circuitry in the manual actuation path. Westinghouse believes that the manual system-level actuation path can, and generally should, include digital circuitry. Digital circuitry is more reliable than the alternative discrete analog logic (relays, timers, etc.) Furthermore, Westinghouse believes that requiring the manual and automatic actuation paths to be separate is not the best method to achieve the goal of high reliability.</p> <p>Section B eleventh paragraph states that, "BTP 7-19 asserts that manual controls for safety equipment should be connected downstream of the plant's digital I&C safety system outputs." This paragraph (C.4) incorrectly interprets the guidance in BTP 7-19 to apply to all manual controls for safety equipment. Therefore, the sentence, "In the case of automated digital protection systems, the point at which the manual controls are connected to safety equipment should be downstream of the plant's digital I&C safety system outputs," should be deleted.</p> <p>Manual controls that exist to cope with software common cause failure (CCF) of a digital safety system (those addressed in BTP 7-19) must not be susceptible to the same CCF as the digital safety system, and therefore are generally connected downstream of the digital safety system outputs. There is no requirement for manual controls of safety equipment to be independent of, or separate from, the digital safety system if they are not credited for coping with a failure of the digital safety system.</p>	<p>The staff partially agrees. Position 4 of the draft may have caused confusion by not distinguishing between the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with respect to manual initiation of protective actions. To eliminate the confusion, guidance subject to BTP 7-19 will be removed from Position 4 and will be addressed under a new regulatory position (Position 7). Also, as an effort to make the distinction between requirements of IEEE Std 603-1991 and the guidance of BTP 7-19 with respect to manual initiation of protective actions, the opening statement of Section C will be revised to read:</p> <p>“Regulatory Positions 1, 2, 3, 4, 5, and 6 below provide an acceptable method for complying with IEEE Std 603-1991 in regard to manual initiation of protective actions. Position 7 is an acceptable method for diverse manual initiations of protective actions that satisfies Point 4 of BTP 7-19. Position 8 is an optional acceptable method for satisfying regulatory requirements for both IEEE Std 603-1991 requirements and Point 4 of BTP 7-19 guidance.”</p> <p>The new Position 7 will Read:</p> <p>“In providing diverse manual initiation of protective actions, a set of independent and diverse displays and manual controls should be provided in main control room. These displays and controls may be safety or non-safety. The point at which the manual controls are connected to safety equipment should be downstream of the digital I&C safety system outputs. These connections should not compromise the integrity of interconnecting cables and interfaces between local electrical or electronic cabinets and the plant’s electromechanical equipment.”</p> <p>New Position 8 will provide applicant/licensees an optional guidance for a safety-related diverse manual control that meets the requirements of IEEE Std 603-1991 and the guidance of BTP 7-19. Position 8 will Read:</p> <p>“An optional acceptable method that satisfies both requirements of IEEE Std 603-1991 and guidance on Point 4 of NRC position</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
		<p>on D3, a single safety-related manual initiation of protective actions that satisfies Positions 1, 2, 3, 4, 5, 6, and 7 above can be provided.”</p> <p>This response also applies to comments 4, 5 and 7.</p>
<p>Section C Regulatory Position 4 page 6</p>	<p><u>Comment 4:</u> The existing guidance in Regulatory Guide 1.62, Revision 0, Regulatory Position 4 allows that "...action-sequencing functions ... may be common if individual manual initiation at the component or channel level is provided in the control room." This provision is removed in DG-1 190. The removal of this provision is not justified.</p>	<p>The staff partially agrees. The original Regulatory Position 4 (Revision 0 of RG 1.62) included the following guidance for manual initiation of protective actions: <i>“The amount of equipment common to both manual and automatic initiation should be kept to a minimum. It is preferable to limit such common equipment to the final actuation devices and the actuated equipment.”</i> This guidance provided a measure of diversity between the automatic and manual initiation in analog based systems. The affected provision excludes action-sequencing functions and interlocks from this guidance so that manual initiation would not be unnecessarily burdened with sequencing or interlock functions.</p> <p>Since (1) IEEE Std 603-1991 does not require that equipment common to both manual and automatic initiation be minimized and (2) with diversity guidance for digital computer-based I&C systems (BTP 7-19) being addressed under new Position 7, Position 4 (subject to IEEE Std 603-1991 requirements) will be revised to delete <i>“The amount of equipment common to both manual and automatic initiation should be kept to a minimum. It is preferable to limit such common equipment to the final actuation devices and the actuated equipment.”</i> Therefore, the affected provision (served as an exception for the above statement) is therefore no longer needed.</p>
<p>Section B 4th paragraph page 3</p>	<p><u>Comment 5:</u> Section B, fourth paragraph, indicates that manual actuation is a backup to automatic actuation. IEEE Std 603 does not require the manual controls to cope with a failure of the automatic actuation. They are simply another method to achieve the actuation. The use of the term "backup" is not appropriate. The term "backup" would be appropriate if describing the manual controls addressed in BTP 7-19. As stated in Item 3 above, DG-1190 is confusing the requirements</p>	<p>The staff agrees. The affected paragraph will be revised to read:</p> <p>“Design analyses determine the appropriate safety functions and corresponding protective actions for each plant design. The protective actions can be initiated automatically, or, in certain cases, can be accomplished solely by manual controls. Protective actions initiated solely by manual controls are subject to consideration of (1) the time for the operator to analyze and manually respond to an adverse plant condition,</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
	of IEEE Std 603 and the diversity issues of BTP 7-19.	<p>(2) the time available for actions to be taken to mitigate adverse plant conditions, (3) the plant conditions expected at the time manual controls is credited, (4) the range of conditions over which the manual controls are expected to be in effect, and (5) the display variables necessary to provide for effective manual control.</p> <p>Also see response for comment 3.</p>
<p>Section B 6th paragraph page 4</p>	<p><u>Comment 6:</u> Section B, sixth paragraph, states that "Safety-related controls and displays should be provided." Although it is true that these controls and displays must be provided, this entire paragraph is confusing, adds no value, and thus should be deleted.</p>	<p>The staff partially agrees. While some language in the draft may have caused confusion, the reference to Section 5.6.3.1 of IEEE Std 603-1991 is appropriate and necessary. However, to eliminate the confusion it may have caused, the affected paragraph will be revised to read:</p> <p>“Section 5.6.3.1 of IEEE Std 603-1991 specifies that interconnected “equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems.” Therefore, equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform functions that support plant safety. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant safety analyses.”</p>
<p>Section B 8th paragraph page 4</p>	<p><u>Comment 7:</u> Section B, eighth paragraph, addresses CCF and Regulatory Guide 1.53. It is recommended that this paragraph be replaced with a simple reference to Regulatory Guide 1.53. This entire discussion on how to address single failures and software CCF is not unique to manual actuation.</p>	<p>The staff partially agrees. As more and more nuclear power plants participate in digitalization of I&C systems and the complexity of digital and advanced analog protection systems has been increased, the potential for software common-cause (CCF) failure has become increasingly important and needs to be addressed. However, the draft RG may have caused confusion by not distinguishing between requirements of IEEE Std 603-1991 and the guidance of BTP 7-19. To eliminate the confusion the draft RG will be revised to distinguish the requirements of IEEE Std-1991 and the guidance of BTP 7-19 in regards to manual initiation</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
		of protective actions. The discussion on CCF and diversity will be moved to the end of the discussion section, where it addresses the need of Diversity and Defense-in-Depth (D3) for manual initiation of protective actions that are not subject to IEEE Std 603-1991 requirements.
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 8:</u> The words "for each division" have been added to Regulatory Position C.1 (second line) and C.2 (first line). The intent of this addition is not clear. Westinghouse has traditionally provided actuation switches on the control board for engineered safety feature (ESF) actuations and reactor trip. One switch actuates the function in all divisions, minimizing discrete operator manipulations as required by IEEE Std 603, Clause 6.2.1. It appears that these switches should now be designed such that each switch only communicates with one division, thus requiring an operator manipulation for each division for each function. The intent of this change should be clarified; or, the words "for each division" should be deleted.</p>	<p>The staff agrees. The phrase "on a system-level basis for each division" will be replaced with "on a division-level" to be consistent with IEEE Std 603-1991.</p>
<p>Section C Regulatory Position 1 page 5</p>	<p><u>Comment 9:</u> Proposed Regulatory Position C.1 includes the words "..., regardless of whether means are also provided to initiate the protective action at the component or channel level..." These words seem to indicate that component-level control is not necessarily required, further confusing the issue raised in Item 1 above.</p>	<p>See response for comment 1.</p>
<p>Section B 3rd paragraph page 3</p>	<p><u>Comment 10:</u> Section B, third paragraph, states that "manual initiation for each appropriate plant system component (e.g., start pump, open or close valve) is subsequently required..." It is not clear how "appropriate plant system components" are identified. The AP1000 is a passive plant. ESF actuations are automatic and require no further component-level manipulations. Therefore, Westinghouse would conclude that AP1000 has none of these components. Clarify the criteria for identifying "appropriate plant system components." Westinghouse agrees that high functional reliability is needed. There</p>	<p>See response for comment 1.</p>

Westinghouse Comments (ML0905404451)

Section of DG-1190	Comment	Resolution
	<p>are many methods to achieve high reliability. Many of these alternate methods provide higher reliability than simply adding circuitry for manual actuation. Alternative methods to achieve high reliability should be allowed and encouraged.</p>	
<p>Section C Regulatory Position 2 pages 5 & 6</p>	<p><u>Comment 11:</u> Proposed Regulatory Position C.2 has added the sentence "Multiple initiations of safety systems (autosequencing) by distinct manual control manipulations are not precluded." This sentence is confusing. For example, is "autosequencing" the same thing as "actionsequencing" in the previous sentence? If there is intent to soften the requirement that manual initiation perform all actions performed by the automatic means, then this should be clearly explained.</p>	<p>The staff agrees. Position 2 will be revised to read: "Manual initiation of a protective action on a division-level basis should perform all actions performed by automatic initiation such as starting auxiliary or supporting systems, sending signals to appropriate valve-actuating mechanisms to ensure correct valve position, and providing the credited action-sequencing functions and interlocks."</p>
<p>Regulatory Analysis Section 3.2 3rd paragraph page 8</p>	<p><u>Comment 12:</u> Regulatory Analysis Section 3.2 states "Applicants would incur little or no cost and may, in fact, achieve cost savings." Westinghouse does not agree. If the suggestions in this draft regulatory guide were incorporated into the AP1000 design, specifically the added circuitry for separate non-digital circuits for all manual controls, many additional cabinets for the analog circuitry and their associated costs would be required. The AP1000 is a compact plant design. It is not apparent that the currently-designed buildings can hold these additional cabinets. The added circuitry must also be designed, purchased and installed. In addition, periodic surveillance and corrective maintenance on this additional analog circuitry will be a significant recurring operations/maintenance cost.</p>	<p>The staff partially agrees. Although some language in the draft may have caused confusion with regard to component-level manual control and diversity guidance (BTP 7-19), adding new requirements that results in high cost to applicants/licensees is not the intent of the draft. The draft will be revised to remove guidance associated with component-level manual controls and to distinguish the existing requirements of IEEE 603-1991 and the guidance of BTP 7-19 (see above responses). There is no significant cost incurred as the result of the revision of the RG since no new regulatory requirement is introduced in the revision. This response also applies to comment 13.</p>
<p>Regulatory Analysis Section 4 page 8</p>	<p><u>Comment 13:</u> Section 4, Conclusion, indicates that the primary benefit to the proposed regulatory guide is reference to the modern standards. This proposed revision does much more than update the standards references. There is also a statement that alludes to cost savings. No cost savings have been identified in the draft regulatory guide and Westinghouse can only identify cost increases for these added requirements and added circuitry as indicated above.</p>	<p>See response for comment 12.</p>