NUCLEAR ENERGY INSTITUTE

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

3/26/2010
75FR 14643
(2)

May 25, 2010

Mr. Michael T. Lesar
Chief, Rulemaking and Directives Branch
Division of Administrative Services
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

Subject: Comments on Branch Technical Position (BTP) 7–19, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-based Instrumentation and Control Systems (*Federal Register* of March 26, 2010, 75 FR 14643)

Project Number: 689

Dear Mr. Lesar:

On behalf of the nuclear energy industry, the Nuclear Energy Institute (NEI)[1] submits the attached comments for your consideration as you finalize the subject draft Branch Technical Position.

This revised BTP should be internally consistent and also consistent with issued DI&C ISGs that the NRC and industry developed over the past three years. The Human Factors Engineering (HFE) guidance in this BTP conflicts with the more comprehensive treatment of these issues in DI&C-ISG-05 and SRP Section 18-A, including the ability to credit local controls based on HFE analysis. This BTP also confuses the requirements of IEEE-603 for 'manual initiation' of RPS and ESFAS with the SECY-93-087 Point 4 requirements for manual system level 'actuation and control' of critical safety functions. These points are addressed in more detail in the attached comments. Incorporating the recommendations and the suggested rewording will help achieve the desired BTP consistency.

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

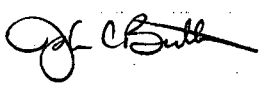
SUNSI Review Complete E-RIDS=ADM-03

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

Template=ADM-013 Add = S. Burrows (sab)

We thank you for the opportunity to comment and trust you will find these comments helpful. If you have any questions, please feel free to contact me at (202) 739-8108; jcb@nei.org or Gordon Clefton at (202) 739-8086; gac@nei.org.

Sincerely,



John C. Butler

Attachment

ATTACHMENT

Comments on BTP 7-19 Rev 6

ID	Section, Page, and Line #	Comment
1	A, Page 2 Paragraph 1	"SECY-91-292 and SECY-93-087 did not address the consolidation of the four echelons of D3 (echelons described in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems") into one digital system, nor did the Commission address combining echelons of defense at the time it established policy on CCF." Comment: This statement implies that these are new features of recent Design Certification applications; however, CE plants have combined RPS and ESFAS in analog protection systems since the mid-1970's, and in the digital protection system for System 80+, which was certified in accordance with these SECYs. The reason combining echelons of defense was not addressed in these SECYs may have been simply that it was not considered new. This sentence should be completely deleted for several reasons: (1) The purpose of this statement is not clear, (2) Its implication is not true, (3) The combining of echelons of defense does not change the original intent of BTP-19, nor does it result in any changes to the current guidance.
2	A, Page 2 Paragraph 3	"In summary, while the NRC considers (software) CCF in digital systems to be beyond design basis, digital safety systems should be protected against the effects of CCF." Comment: The intent of BTP-19 is not to protect the digital safety systems; it is to protect the plant. Reword as follows: 'In summary, while the NRC considers (software) CCF in digital systems to be beyond design basis, plants should be protected against the effects of AOOs and Postulated Accidents with a concurrent CCF in the digital protection system.'

3	A.2, Page 3 Last Paragraph	"Regulatory Guide (RG) 1.53, "Application of the Single-Failure Criterion to Safety Systems," clarifies the application of the single-failure criterion (GDC 21) and endorses IEEE Std. 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," providing supplements and an interpretation. IEEE Std. 379-2000, Clause 5.5, identifies D3 as a technique for addressing CCF, and Clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion." Comment: This paragraph incorrectly implies that CCF should be treated as a single failure. This has lead to significant industry and NRC confusion. DI&C-ISG-02 has now clarified that CCF is not a single failure. Thus, for clarity of this point this paragraph should be revised as follows: 'IEEE Std. 379-2000, Clause 5.5, distinguishes single failures that can lead to cascaded failures, and are therefore subject to single failure analysis, from defects that are not treated as single failures. This Clause states that design qualification and quality assurance programs afford protection against external environmental effects, design deficiencies, and manufacturing errors that can lead to CCFs. Thus, these types of CCFs are not subject to single failure analysis. Instead Clause 5.5 identifies D3 as a technique for addressing CCF.'
4	A.3, Page 4 Paragraph 6	"The purpose of this BTP is to provide guidance for evaluating an applicant/licensee's D3 assessment, design, and the design of manual controls and displays to ensure conformance with the NRC position on D3 for I&C systems incorporating digital, software-based or softwarelogic- based RTS or ESFAS." Comment: As written this BTP is only applicable to the ESFAS and not the ESF Control Systems, which are also covered in SRP Section 7.3, and may also have digital implementations. If this is the NRC's intent that should be more clearly stated.
5	B.1.1, Page 5 Paragraph 1	"The NRC staff identified four echelons of defense against CCFs in NUREG/CR-6303:" Comment: NUREG/CR-6303 identifies these only as "echelons of defense", not "echelons of defense against CCFs". NUREG/CR-6303 describes these as echelons of defense against plant accidents, not defense against CCF. Defense against CCF only results from diversity within these echelons. Even diversity between the echelons is insufficient to provide adequate defense for plant accidents, with a concurrent CCF that disables all divisions of the same echelon, since plant accident analysis demonstrates that the echelons do not always provide sufficient backup for one another. Incorrectly stating that different echelons of defense results in defense against CCF has lead to considerable regulatory confusion. Therefore, delete "against CCFs".\ Thus reword as follows: 'The NRC staff identified four echelons of defense in NUREG/CR-6303:'
6	B.1.1, Page 5 Paragraph 1	"ESFAS - The ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release... Comment: More correctly, this is the ESF echelon, since the ESFAS by itself cannot perform the safety functions described.

7	B.1.3, Page 5 Last Paragraph	"Earlier traditional I&C echelons of defense architectures consisted of discrete and separate components in four echelons of defense. In digital systems, formerly discrete systems (e.g., the RTS and the ESFAS) could be combined into a single DI&C system. Digital systems that combine most, if not all RTS and ESFAS functions within a single digital system in both new NPP designs and upgrades to current operating plant systems could introduce new CCF mechanisms that do not exist in systems that use separate discrete components." Comment: (1) RTS and ESFAS echelons have been combined in CE analog Plant Protection Systems since the mid-1970s. (2) Combining echelons only extends the effects of single failures. It does not introduce new CCF mechanisms, since even when echelons are combined independence is still maintained between divisions. Thus reword as follows: 'In addition to divisional independence, some earlier traditional I&C architectures consisted of discrete and separate components for each echelon of defense. In digital systems, formerly discrete systems (e.g., the RTS and the ESFAS) could be combined into a single DI&C system. Digital systems that combine most, if not all, RTS and ESFAS functions within a single digital system in both new NPP designs and upgrades to current operating plant systems could introduce new effects from single failures (i.e., effects on multiple echelons of a single division) that do not exist in systems that use separate discrete components.'
8	Section 1.4, page 6, point 2, line 4	Examples cited for realistic assumptions form an ultra conservative threshold that could be used (during future NRC reviews) to limit more effective assumptions, serve no real guidance, and should therefore be deleted. These same examples are also cited in Sections 1.6, 3.1(1), 3.3, and 4.5.
9	B.1.4 Point 2, Page 6 Paragraph 3	"In performing the assessment, the vendor or applicant/licensee should analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using either realistic assumptions (e.g., plant operating at normal power levels ..." Comment: The addition of "plant operating at normal power levels" is an important clarification. For consistency, reword the first part of this sentence as follows: 'In performing the assessment, the vendor or applicant/licensee should analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) relevant to normal power operation using either realistic assumptions (e.g., plant operating at nominal power levels ...'

10	B.1.4 Point 4, Page 6 Paragraph 4	"... a set of displays and controls (safety or non-safety) should be provided in the main control room (MCR) for manual system level actuation and control of safety equipment to manage plant critical safety functions..." Comment: After manual actuation from the MCR, local control actions should be permitted to maintain control of critical safety functions. Thus reword as follows: '... a set of displays and controls (safety or non-safety) should be provided in the main control room (MCR) for manual system level actuation of safety equipment to initiate control of plant critical safety functions...' When supported by a suitable HFE analysis, in accordance with SRP 18-A, diverse local controls may be used to maintain control of critical safety functions.
11	B.1.4 Point 4, Page 6 Paragraph 4	"The displays and controls should be independent and diverse from the safety systems in Points 1-3 discussed above." Comment: The displays and controls need to be diverse, but not independent (i.e., no physical or electrical separation), since they could be part of the same safety system and the same safety division. Independence from the safety system is needed only if they are non-safety. Thus reword as follows: 'The displays and controls should be diverse from any CCF vulnerability identified within the safety systems in Points 1-3 discussed above and meet divisional independence requirements as applicable for the specific design implementation.' Reading Point 4 in isolation seems to imply that additional diverse manual controls are required beyond any diverse means provided in response to Point 3. The words "safety systems" in that sentence add to the ambiguity. Section 1.5 is better than Section 1.4 and seems to be generally in line with common industry understanding on this subject. There are probably a number of ways to deal with this (break Point 4 up into more tractable pieces, Integrate Point 4 and section 1.5 & streamline, etc.) but the potential for misunderstanding between the NRC and an applicant/vendor is very high as written.
12	Section 1.4, page 6, point 4, last sentence	"However, if existing displays and controls are digital and/or the same platform is used this point may not be satisfied." Comment: The last sentence should safeguard against analog display devices whose signals are provided by digital safety-systems. Thus reword as follows: 'However, if existing displays and controls are digital and/or the same platform is used to provide signals to the analog displays, this point may not be satisfied.'
13	B.1.4, Page 7, Paragraph 1	"... because identical copies of the software based logic and architecture are present in redundant channels of safety-related systems." Comment: Channels do not require redundancy; therefore, for consistency with IEEE-603, "channels" should be changed to "divisions".

14	B.1.4, Page 7, Paragraph 1	"Also, some errors labeled as "software errors" (for example) actually result from errors in the higher level requirements specifications used to direct the system development that fail in some way to represent the actual process. Such errors further place emphasis on the use of diversity to avoid or mitigate CCF." Comment: This implies a new requirement for diverse functionality (i.e., diverse trip algorithms and diverse ESF actuation algorithms), which goes well beyond the current requirement for diversity to address potential errors in digital software based implementation. Requirements errors are not software errors since they can equally affect any implementation method, including hardware implementation. These two sentences should be deleted.
15	B.1.5, Page 7 Paragraph 2	"Two types. . . . would not be needed." Comment: This paragraph is very confusing because the IEEE-603 requirement for "manual initiation at the division level of the automatically initiated protective actions" is different than the Point 4 guidance for manual system level actuation and control of critical safety functions. Diverse manual initiation of all automatically initiated protective actions may not be necessary or may not be sufficient to control the critical safety functions. Thus this paragraph should be deleted. If the paragraph is retained it should be corrected as commented below.
16	B.1.5, Page 7 Paragraph 2	"... a safety-related means shall be provided in the control room to implement manual initiation at the division level of the RPS functions." Comment: ACRS letter March 29, 2010 regarding RG 1.62 revision states "system level actuation of all divisions which meets the requirements of IEEE 603-1991 is acceptable". Thus reword as follows: '... a safety-related means shall be provided in the control room to implement manual initiation at the system or division level of the RPS functions.'
17	B.1.5, Page 7 Paragraph 2	"Point 3 states that not only should there be a diverse backup means for the automated safety-related RPS subject to a potential CCF, but if the required safety-related RPS manual actuation system (required per IEEE Std. 603 – 1991) is also subject to the same CCF as the automated safety-related actuation system, then a diverse manual backup actuation (safety or non-safety) should also be provided." Comment: (1) Point 3 does not distinguish automated or manual means. Point 3 is only referring to the safety functions, automated or manual, credited in the accident analysis of Point 2; the analysis for some accidents credit only manual safety functions. (2) There is no requirement in IEEE-603 for a "manual actuation system"; the requirement is for manual initiation of the automated functions. (3) Diverse manual backup is only needed to the extent necessary to control critical safety functions. Thus reword as follows: 'Point 4 states that manual actuation (safety or non-safety) should also be provided to control all critical safety functions. This function should be diverse from the CCF that affects the safety functions credited in the accident analysis.'

18	B.1.5, Page 7 Paragraph 2	"The indicators and controls described in Point 4 may be able to address the need for this independent and diverse manual actuation backup." Comment: (1) There should be no contingency in this sentence. (2) There is no requirement for independence. Thus reword as follows: 'The indicators and controls described in Point 4 address the need for this diverse manual actuation backup.'
19	B.1.5, Page 7 Paragraph 2	"If an IEEE Std. 603 -1991 required safety-related manual actuation system is independent and sufficiently diverse from the automated safety-related RPS actuation system, then a second diverse non-safety related manual actuation system would not be needed." Comment: (1) There is no requirement for a "manual actuation system"; the requirement in IEEE-603 is for manual initiation of the automated functions. (2) There is no requirement in IEEE-603 that the manual initiation be independent from the automated actuation. This BTP should not impose an additional independence requirement, since diversity from the CCF is sufficient. (3) Point 4 requires diversity from all safety functions credited in the safety analysis, automated or manual. (4) Manual initiation of the automated protective actions may not be sufficient to control all critical safety functions. Thus reword as follows: 'If the system/division level manual initiation required by IEEE Std. 603 -1991 is not vulnerable to the same CCF that affects the safety functions credited in the accident analysis, then a second diverse manual system level actuation would not be needed for those automated protective actions. An addition manual system level actuation would only be needed for control of critical safety functions that are not controlled by those automated protective actions.'
20	B.1.6, Page 7 Paragraph 3	Deleted sentence. Comment: The following sentence, which was deleted from Revision 5, should be retained, since it clarifies the ability to credit manual means and non-safety equipment: "The diverse means may be an automatic or manual non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time." However, for consistency with DI&C-ISG-05 "required time" should be changed to "time available". Thus reword as follows: 'The diverse means may be an automatic or manual non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the time available.'

21	B.1.7, Page 8 Paragraph 2	"When an independent and diverse method is needed as a backup to an automated system used to accomplish a required safety function as a result of the D3 assessment identifying a potential CCF, the backup function can be accomplished via either an automated system, or manual operator actions performed from the MCR. The preferred independent and diverse backup method is generally an automated system." Comment: (1) Independence is only needed if the backup is not part of the same safety division. (2) A backup may also be needed for manual functions if a manual function is credited in the safety analysis and that function is adversely affected by the CCF. (3) Point 4 requires controls in the MCR only for system level actuation of critical safety functions. Controls for other manual actions credited for accident mitigation or longer term management of critical functions can be from outside the MCR, if suitably supported by the HFE analysis. (4) It is important to state that the backup can be non-safety. Thus reword as follows: 'When a diverse method is needed as a backup to a required safety function as a result of the D3 assessment identifying a potential CCF, the backup function can be accomplished via either an automated system or manual operator actions. The preferred backup for an automated safety function is generally a diverse backup automated function. The backup function may be a safety function or a non-safety function. Appropriate divisional independence shall be maintained. Backup manual operator actions, credited from either the MCR or local controls, shall be supported by a suitable HFE analysis.'
22	Section 1.8, page 8, second paragraph, lines 6-8	"For this reason, the evaluation of failure modes as a result of CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate." Comment: The evaluation of failure modes should be in accordance with NUREG-6303 which provides a sufficient level of detail to formulate/postulate failure modes. Thus reword as follows: 'For this reason, the evaluation of failure modes as a result of CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate in accordance with Section 3 of NUREG-6303.' This same statement is also contained in Section 4.1.
23	B.1.8, Page 9 Paragraph 1	"Software or software logic based CCF was declared a "beyond-DBE" by the Commission in the SRM issued in response to SECY-93-087. Such a CCF that causes an undesired trip ..." Comment: The Commission's determination that CCF is a beyond DBE is irrelevant to the point of this section. Delete the first sentence. Reword the second sentence as follows: 'A CCF that causes an undesired trip ...'
24	B.1.8, Page 9 Paragraph 1	"....there are two design attributes listed that are sufficient to eliminate the consideration of CCF." Comment: Are these two attributes considered to both be required or is one sufficient?

25	B.1.8, Page 9 Paragraph 2	"The effects of spurious trips and actuations should be evaluated by the applicant/licensee." Comment: The key point of DI&C-ISG-02 is missing. Add the following: 'Since spurious trips or actuations are self-announcing, the software defect can be corrected prior to causing a CCF in multiple safety divisions. Therefore, spurious trips or actuations of safety-related digital protection systems do not need to be addressed beyond what is already set forth in plant design basis evaluations.'
26	Section 1.9 (1), page 9	"Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 determines that the two diverse digital systems are not subject to a CCF. In this case, no additional diversity would be necessary in the safety system." Comment: This example does not consider the significant increase in O&M procedures, training, spare parts, etc. Industry research on digital operating experience (EPRI TR 1016731) demonstrates that the most likely cause of CCF is human error. To reduce the extent of human interaction, system designs should limit the parts and procedures and thereby minimize the potential for these errors. Overall, the practicality of this approach has not been adequately evaluated by industry or the NRC. The example cited needs to address a failure mode where one of the channels in one of the diversities is bypassed for maintenance/testing and a SW CCF occurs in the other two (diverse) channels. Under this postulated event, the plant protection system could not perform its intended safety function as only one channel would be available. Thus, this example should be deleted. If it is retained it should be revised. (1) For consistency with IEEE-603, channels should be replaced by divisions. (2) This example does not consider the impact on Technical Specifications that allow continuous bypass of one safety channel. Reword as follows: 'Example: An RPS design in which each safety function is implemented in two divisions that use one type of digital system and another two divisions that use a diverse digital system. However, consideration must be given to increased restrictions in plant Technical Specifications which may currently allow one division to be out of service continuously.
27	B.1.9 (2), Page 9 Paragraph 6	"Testability - A system is sufficiently simple such that every possible combination of inputs, internal and external states, and every signal path can be tested;" Comments: "External states" are irrelevant, since they are the result of the test or they are covered by every combination of inputs. Using the criterion "every possible combination" goes beyond the regulatory acceptance for testing coverage in the explicit reference to the WCAP 15413 SER (B.4.3, Page 16, Paragraph 4). Thus reword as follows: 'Testability - A system is sufficiently simple such that every possible combination of inputs, internal states, and every signal path can be tested;'

28	B.2, Page 10 Paragraph 1	"...HFE analysis associated with manual operator actions as an independent and diverse backup method." Comment: Independence is not required (see comments above). Thus reword as follows: '...HFE analysis associated with manual operator actions as a diverse backup method.'
29	B.3.1, Page 10 Paragraph 2	"Since the acceptance criteria address confirmation that anticipated operational occurrences and design-basis accidents (DBAs) are mitigated in the presence of CCF..." Comment: The accident analysis section of the SRP uses "postulated accidents" not "DBA". "DBA" should be replaced with "postulated accidents" throughout this BTP.
30	B.3.1(1), Page 10 Paragraph 3	"For each anticipated operational occurrence in the design basis ...(e.g., plant operating at normal power levels ..." Comment: The addition of "plant operating at normal power levels" is an important clarification; therefore, for consistency the first part of this sentence should be revised. Thus reword as follows: 'For each anticipated operational occurrence in the design basis relevant to normal power operation ...(e.g., plant operating at normal nominal power levels ...'
31	B.3.1(2), Page 10 Paragraph 4	"For each postulated accident in the design basis ..." Comment: See comment regarding 3.1 Item 1. Thus reword as follows: 'For each postulated accident in the design basis relevant to normal power operation ...'
32	B.3.1 (6), Page 11 Paragraph 3	"For safety systems to satisfy IEEE Std. 603–1991 ... implement manual initiation at the division level of the RTS and ESFAS functions." Comment: Per previous comment (i.e., ACRS letter in B.1.5, Page 7 Paragraph 2) change "division level" to "system or division level".
33	B.3.1 (6), Page 11 Paragraph 3	"If the means is independent and diverse from the safety-related automatically initiated RTS and ESFAS functions, the design meets the system-level actuation criterion in Point 4 of this BTP." Comment: There is no requirement in IEEE-603 for independence between automatic and manual functions. There is no need for independence to cope with CCF; therefore, delete "independent and". Reword as follows: 'If the means is diverse from the safety-related automatically initiated RTS and ESFAS functions, the design meets the system-level actuation criterion in Point 4 of this BTP.'

34	B.3.1 (7), Page 11 Paragraph 4	"If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the independent and diverse means ..." Comment: There is no need for independence to cope with CCF; therefore, delete "independent and". Reword as follows: 'If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means ...'
35	B.3.1 (8), Page 11 Paragraph 5	"If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the independent and diverse means of actuating the protective safety functions should meet the following criteria: The independent and diverse means should be..:" Comment: There is no need for independence to cope with CCF; therefore, delete "independent and" in two places in this sentence. Reword as follows: 'If the D3 assessment reveals a potential for a CCF, then the method for accomplishing the diverse means of actuating the protective safety functions should meet the following criteria: The diverse means should be..'
36	B.3.1 (8) a), Page 11 Paragraph 5	"a) at the division level;" Comment: Per previous comment (i.e., ACRS letter in B.1.5, Page 7 Paragraph 2) change "division level" to "system or division level".
37	B.3.1 (8) c), Page 11 Paragraph 5	"c) capable of responding with sufficient time available for the operators to determine the need for protective actions even with malfunctioning indicators..." Comment: Malfunctions are limited to those affected by the CCF. There are no additional independent failures postulated concurrent with the CCF, either in the safety equipment or in diverse backup equipment. Thus reword as follows: '... even with indicators that may be malfunctioning due to the CCF ...'
38	B.3.1 (8) e), Page 12 Paragraph 1	"e) supported by sufficient instrumentation that indicates .... 3. the automated backup or manual action is successful in performing the safety function." Comment: Malfunctions are limited to those affected by the CCF. There are no additional independent failures postulated concurrent with the CCF, either in the safety equipment or in diverse backup equipment. Thus reword as follows: '3. the automated backup or manual action's affect on the critical safety function.'

39	B.3.1, (9) page 12, lines 5&6	"Use of design techniques (for example: redundancy, conservative setpoint selection, and use of quality components) to mitigate these concerns is recommended." Comment Include 'increased coincidence logic required for actuation' to the example. This will provide one of the better avenues to avoid inadvertent (spurious) actuations. Thus reword as follows: 'Use of design techniques (for example: redundancy, conservative setpoint selection, increased coincidence logic required for actuation, and use of quality components) to mitigate these concerns is recommended.'
40	B.3.1 (9), Page 12 Paragraph 2	"(9) If the D3 assessment reveals a potential for a CCF, then, in accordance with the augmented quality guidance for the independent and diverse backup system used to cope with a CCF..." Comment: There is no need for independence to cope with CCF; therefore, delete "independent and" in this sentence. Reword as follows: '(9) If the D3 assessment reveals a potential for a CCF, then, in accordance with the augmented quality guidance for the diverse backup system used to cope with a CCF...'
41	B.3.1 (9), Page 12 Paragraph 2	"Use of design techniques (for example: redundancy, conservative setpoint selection, and use of quality components) to mitigate these concerns is recommended." Comment: "Redundancy" implies the need for single failure compliance for actuation. Change "redundancy" to "a two-out-of-two configuration for actuation".
42	B.3.2, Page 12 Paragraph 4	"Further, RTS and ESFAS could be combined into a single DI&C platform provided D3 is adequately addressed to protect against CCF." Comment: The issue addressed by DI&C-ISG-02 is not the use of a single platform but rather the use of a single CPU. Thus reword as follows: 'Further, RTS and ESFAS could be combined into a single controller or single central processing unit provided D3 is adequately addressed to protect against CCF.'
43	B.3.3, Page 12 Paragraph 5	"Consequently, realistic assumptions (e.g., plant operating at normal power levels, temperatures..." Comment: The addition of "plant operating at normal power levels" is an important clarification. Reword as follows: 'Consequently, realistic assumptions (e.g., plant operating at normal nominal power levels, temperatures...'

44	B.3.5, Page 13 Paragraph 2	"Note: As the difference between time available and time required for operator action decreases, there is increasing potential that uncertainties in the estimate of time required will invalidate a conclusion that operators can perform the action reliably within the time available (e.g., less than 30 minutes between the time available and the time required for operators to perform the protective action)." Comment: The required time margin between time available and time required to accommodate uncertainties in the estimate of time required is an HFE issue which is addressed in DI&C-ISG-05 Section 1.A and SRP 18-A Section 1.A. This paragraph should be deleted from BTP 7-19.
45	B.3.5, Page 13 Paragraph 3	"Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division. This recommendation does not prohibit the use of manual controls for operating individual safety system components after the corresponding safety system functions have been actuated. The design and normal operation of any such non-safety displays and controls shall not prevent any safety systems from performing the intended protective safety function when actually required to be actuated." Comment: This says that manual initiation should be done for each division. This assumes that the diverse backup system will be implemented with the same division boundaries as the primary system. Not all diverse systems will be implemented along the safety division boundaries.
46	B.3.5, Page 13 Paragraph 3	"Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division." Comment: There is no requirement to assume additional single failures concurrent with the postulated CCF. In addition, the analysis assumes "normal alignments of equipment" (i.e., no equipment abnormally out of service). Therefore, it is sufficient to actuate a single division. Thus reword as follows: 'Diverse backup manual initiations of safety systems should be performed on a system-level or division-level basis. Since additional independent single failures are not postulated concurrent with the CCF, and normal alignment of equipment is assumed, actuation of a single division is sufficient. For plants licensed to allow one division to be continuously out of service, the actuation must apply to at least one division that is in service.'

47	B.3.5, Page 13 Paragraph 3	"Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division...The design and normal operation of any such non-safety displays and controls shall not prevent any safety systems from performing the intended protective safety function when actually required to be actuated." Comment: (1) The second sentence is unrelated to the first. (2) "Such" is not needed in this sentence. (3) Failures in non-safety controls must also be considered, not just normal operation. (4) This paragraph needs to address accomplishment of the safety function not just actuation of the safety system. Therefore put the second sentence in a new paragraph Reword as follows: 'The normal operation or failure of any non-safety displays or controls shall not prevent any safety systems from performing the intended safety function when actually required to be actuated. Prioritization between safety and backup non-safety systems to ensure the required safety function can be accomplished by either system is addressed in DI&C-ISG-04 Section 2.3.'
48	B.3.6, Page 13 Paragraph 4	"Therefore, Point 4 applies to new plants and to existing plants installing digital equipment in RTS or ESFAS." Comment: If it is the NRC's intent that Point 4 is not applicable if digital equipment is installed in ESF control systems, then this policy should be more clearly stated.
49	B.3.9, Page 14 Paragraph 5	"Fully tested or 100% testing means testing every possible combination of inputs, internal and external states, and every signal path." Comment: If it is the NRC's intent that Point 4 is not applicable if digital equipment is installed in ESF control systems, then this policy should be more clearly stated. Using the criterion "Fully tested" goes beyond the regulatory acceptance for testing coverage in the explicit reference to the WCAP 15413 SER (B.4.3, Page 16, Paragraph 4). This is already defined in DI&C-ISG-04, Section 2. BTP 7-19 should be internally consistent and consistent with DI&C-ISG-04. Reword as follows: '100% testing means that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case.'
50	B.3.10, Page 15, Paragraph 2	"This additional manual capability is necessary in new NPP designs because all of the protection and control systems are expected to be digital-based and thus vulnerable to CCF." Comment: Point 4 of the NRC position on D3 is applicable to all plants not just new plants, so this sentence should be deleted.

51	B.3.10, Page 15, Paragraph 3	"The point at which the manual controls are connected to safety equipment should be downstream of DI&C safety system outputs." Comment: In new plant designs, it is common for the DI&C safety system outputs to connect directly to the plant's electromechanical equipment (e.g., motor starters, solenoids, breakers). Thus reword as follows: 'The point at which the manual controls are connected to safety equipment should be downstream of equipment that can be adversely affected by a software CCF.'
52	B.3.10, Page 15, Paragraph 4	"The displays may include digital components that are dedicated exclusively to the display function." Comment: This sentence misses the key point which is to preclude susceptibility to the postulated CCF. Thus reword as follows: 'The displays may include digital components that are not adversely affected by the CCF that affects the safety functions credited in the accident analysis.'

53	B.4.3, Page 16, Paragraph 4	"In certain cases, the NRC staff has concluded that software-based components may be sufficiently simple and deterministic in performance that measures such as, for example, online error checking and exhaustive testing can provide adequate assurance that a component is not a significant source of CCF. CCF of such components need not be considered in the course of a D3 analysis. When a basis is given that a block is not susceptible to CCF, the NRC staff should examine the justification carefully. The safety evaluation of Westinghouse WCAP-15413, Westinghouse 7300a ASIC-Based Replacement Module Licensing Summary Report," provides an example of the basis for such a determination."
		
		Comment: The staff reviewed the design, operation, and error detection mechanism of the ASIC chip, the controller PROM, the 01 and RAMLogic PROMs, and the Hi-Memory PROM. On the basis of that review, the staff concluded that the testing conducted on the ABRMs provides adequate assurance that the ABRMs are not a significant source of common-cause failure resulting from software errors and, therefore, are acceptable.
		
		This new criterion (Section B.1.9(2) "every possible combination") now goes beyond the regulatory acceptance for testing coverage in the explicit reference to the WCAP 15413 SER.
		
		The SER for WCAP-15413 has the following relevant points:
		
		• ASIC qualification was done with COTS process. There was no review of the software/firmware lifecycle documents documented by NRC.
		
		• Founded on the premise that the ASIC is thoroughly testable because the ASIC performs basic mathematical operations using its eight independent circuits. Therefore, Westinghouse conducted its qualification and validation test programs to demonstrate that the ASIC will perform its intended safety-related functions.
		
		  • The ABRM ASIC is assembled from logic blocks, such as a 2-bit adder. Before assembling these blocks, ORNL tests the logic blocks to confirm that they perform as required. The logic blocks are then added one at a time. Each time a block is added, tests are performed to confirm that the new block performs as required. After all of the circuits in the ASIC were assembled, Westinghouse performed functional testing and design testing to verify that the ASIC design and fabrication are both correct.
		
		  • For functional testing, Westinghouse used a set of test vectors to test whether each of the eight independent circuits in the ASIC is operating properly to show that each of the circuits is correctly designed. Fabrication testing exercised nodes in the ASIC to determine whether the manufacturing process resulted in any faulty components in the ASIC. For these tests, Westinghouse used two sets of test vectors, totaling 225,000 test vectors. These tested 100 percent of the functions and exercised 99.8 percent of the nodes.
		
		  • Westinghouse addressed common-mode failure issues associated with the ABRMs by performing the following activities to ensure that the ASIC, the controller PROM, the 01 and RAMLogic PROMs, and the Hi-Memory PROM operate as intended.

54	B.4.5, Page 16, Paragraph 6	"Thermal-hydraulic analyses, using realistic assumptions (e.g., plant operating at normal power levels, temperatures..." Comment: The addition of "plant operating at normal power levels" is an important clarification. Reword as follows: 'Thermal-hydraulic analyses, using realistic assumptions (e.g., plant operating at normal nominal power levels, temperatures...'
55	B.4.6, Page 17, Paragraph 3	"Note: As the difference between time available and time required for operator action decreases, there is increasing potential that uncertainties in the estimate of time required will invalidate a conclusion that operators can perform the action reliably within the time available (e.g., less than 30 minutes between the time available and the time required for operators to perform a protective action)." Comment: The required time margin between time available and time required to accommodate uncertainties in the estimate of time required is an HFE issue which is addressed in DI&C-ISG-05 Section 1.A and SRP 18-A Section 1.A. This paragraph should be deleted from BTP 7-19.