	A	B	C	D	E	F
1					**Response to Public Comments on BTP 7-19 Revision 6**	Prepared by TWG#2 - October 27, 2010; minor adjustment of 02/22/2012 for response letter of 01/27/2012 (ML11319A108) to ACRS letter of 11/14/2011 (ML12006A106)
2					Comments from the following Documents (Nos. 1 - 4 below)	Legend for column headings:
3					1 = From Florida Power & Light Co. [ML101470419]	Comment No. = TWG#2 assigned comment number (No.)
4					2 = from Nuclear Energy Institute (NEI) [ML101520095]	Doc = TWG#2 assigned Public Comment Document No.
5					3 = from M T Lesar [ML101540531]	No = TWG#2 assigned comment No. in Doc
6					4 = from M. Waterman	Location = Section and/or paragraph from BTP 7-19 Rev 6
7					TWG#2 = Task Working Group #2, Ian Jung, Chairman	
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
9	1	3	1	A.1.7	BTP 7-9 Rev. 6 does not mention SRP Section -7.8, which contains acceptance criteria for diverse actuation systems; BTP 7-19 should mention SRP Section 7.8, Diverse Instrumentation and Control Systems," in Section A.1.7, "Diverse Backup Method."	Section B.1, "Introduction," provides a detailed introduction of several specific functions, diversity questions, and concepts. The purpose of Section B.1.7 (there is no A.1.7) is to briefly introduce the concept that if a D3 analysis has determine that there is a potential for a CCF, then a diverse means is needed that can be automated or manual. Mentioning SRP 7.8 does not fit. However, the staff agrees that SRP 7.8 should be added to the relevant guidance in Section A.2.
10	2	3	2	B.1.3	Regarding BTP 7-19 Section B. 1.3, "Combining RTS and ESFAS": The second sentence is not correct. "The traditional I&C in Westinghouse plants combined RTS and ESF function in the Foxboro H-Line, Westinghouse 7100 Series, Westinghouse 7300 Series, Eagle 21 and SSPS systems.	The staff agrees that there were early digital systems that combined RTS and ESFAS, but there were many early analog I&C architectures that consisted of discrete and separate analog components in each echelon of defense. The key point is that going from discrete and separate components to combining RTS and ESFAS functions into a single microprocessor or limited number of digital components per division introduces new effects from single failure as well as CCF. Revision 6 will be revised to Clarify these points.
11	3	3	3	A.1	BTP 7-19 does not mention NUREG/CR-6042 Rev. 2 Section 1.1.5, "Defense in Depth," in Section A.1, "Relevant Guidance;" BTP 7-19 should mention /CR-6042 Rev. 2 Section 1.1.5, Defense in Depth," in, Section A. 1, "Relevant Guidance."	NUREG/CR-6042, Revision 2, describes a one-week course in nuclear safety concepts (R800). Section 1.1.5, concerning "Defense in Depth," does not add sufficient information on CCF to justify including it in Section A.1.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
12	4	3	4	A.1	BTP, 7-19 does not explicitly mention IEEE 603 Clause 6.2, "Manual Control," in Section A.1, "Regulatory Basis;" BTP 7-19 should mention IEEE 603 Clause 6.2, "Manual Control. ," in Section A.1, Regulatory Basis."	IEEE Std. 603-1991, Clause 6.2, does not directly apply to addressing the potential for CCF and thus would not normally need to be in the regulatory basis. However, Revision 6, Section 1.5 discusses the potential need for two manual initiation systems and the minimum criteria to provide only one manual initiation system. Criterion 6.2 is referenced in this section. Revision 6 will include IEEE 603, Clause 6.2, in the regulatory basis, Section A.1.
13	5	3	5	A.1	BTP, 7-19 does explicitly mention IEEE 279 Clause 4.17, “Manual Initiation,” in Section A.1, “Regulatory Basis;" BTP 7-19 should mention IEEE 279 Clause 4.17, “Manual Initiation,” in Section A.1, “Regulatory Basis;"	IEEE 279, Clause 4.17, does not directly apply to addressing the potential for CCF and thus would not normally need to be in the regulatory basis. However, Revision 6, Section 1.5 discusses the potential need for two manual initiation systems and the minimum criteria to provide only one manual initiation system. For some plants, IEEE 279 applies instead of IEEE 603. Revision 6 will include IEEE 279, Clause 4.17, in the regulatory basis, Section A.1.
14	6	3	6	A.1	BTP 7-19 does not explicitly mention Regulatory Guide 1..62, "Manual Initiation of Protective Actions," in Section A. 1, "Relevant Guidance;" BTP 7-19 should mention Regulatory Guide 1.62, "Manual Initiation of Protective Actions," in Section A. 1, "Relevant Guidance."	Regulatory Guide 1.62, "Manual Initiation of Protective Actions," Revision 1, has issued in June 2010 and includes Position 7 and 8 that address diverse manual initiation of protective actions. Revision 6 will include Regulatory Guide 1.62 in Section A.2., "Relevant Guidance."
16	7					NOTE: Intentionally left blank due to a skipped number in column A

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
17	8	3	7	B.3.3	Regarding Section B.3.3, "Single Failure and CCF": The first clause of the first sentence is not correct. RG 1.53 Rev. 2 dated November 2003 endorses IEEE Std 379-2000. IEEE 379 Clause 5.5, "Common-cause failures," states: "Certain common cause failures shall be treated as single failures when conducting single-failure analysis..."	The staff disagrees. Section B.3.3 begins with, "Since CCF is not classified as a single failure (as defined in RG 1.53), ..." An issue with IEEE Std 379-2000 clause 5.5 is that later in the clause exceptions to CCF as single failures effectively excludes all CCFs from consideration 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.' This issue is being addressed by Subcommittee 6.3 in its revision to IEEE Std 379.
18	9	3	8	B.1.8	Regarding BTP 7-19 Section A.1, "Regulatory Basis," and BTP 7-19 Section B.1.8, "Potential Effects of CCF: Failure to Actuate and Spurious Actuation,": BTP 7-19 Section B. 1.8 states, "Software or software logic based CCF was declared a 'beyond-DBE' by the Commission in the SRM issued in response to SECY-93-087." This conflicts with the listing of design basis regulatory requirements. The design basis regulatory requirements listed in this section are applicable to certain **I&C s**ystems, but not to a D3 analysis. Listing a bunch of regulations that are not applicable only cause regulatory uncertainty.	In Revision 6, Section B.1.8, the sentence, "Software or software logic based CCF was declared a 'beyond-DBE' by the Commission in the SRM issued in response to SECY-93-087," will be removed from Revision 6 as not relevant to addressing failure to actuate and spurious actuations.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
19	10	1	1	Sec 1.5 Page BTP 7-19-7	Point 3 does <u>not</u> state there be a diverse backup means for the automated safety-related RPS. Page BTP 7- Point 3 is in regard to functions, not the entire system and allows for not necessarily the same 19-7 functions to achieve adequate protection. The linking of Point 3 for **CCF** and IEEE 603 requirements for manual actuation in this paragraph implies if not specifies that a diverse system be available doing all of the RPS actuation functions, and this should not be a requirement. It is possible that manual actuation at the division level be an input to a digital protection system, and In the event of a CCF in the protection system the manual actuation of components in circuits not subject to the CCF can be shown to achieve adequate protection. The manual actuation of a division that is input to a digital protection system bypasses field sensor and **I/O** failures, logic associated with coincidence of conditions to actuate, and allows the operator to take action in response to visual indications. A CCF that would disable both the automatic function and the manual division level actuation could be dealt with using manual actions at the component level, or at a level that would actuate multiple functions but a subset of the RPS functions.	The staff agrees that Point 3 is based on safety functions. The staff also agrees that all safety functions and actuation logic may not be disabled. What safety functions potentially could be affected are determined in the D3 analysis. However, a postulated worst case CCF should assume that all divisions of the actuation logic are disabled. If the automatic initiation of the safety system functions required by IEEE 603 (Clauses 6.2 and 7.2) is also affected by the same CCF, then the staff interprets that Point 3 directs that a diverse manual means be provided that may be non-safety, i.e. <u>two manual actuation means</u>. The key point is that if the IEEE 603 required manual actuation logic is sufficiently diverse, the D3 analysis should show a diverse manual means is not required. This assumes the ATWS rule is addressed. Sec. B.1.5 will be revised to bring more clarity to this section.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
20	11	1	2	Sec. 3.1 (4), Page BTP-19-11	This section attempts to and should not link **CCF** to control and protection system interaction (specifically ESFAS is targeted). Control and protection system interaction is a protection system design requirement based in single failure criteria. CCF is not a single failure. If shared sensors for protection and control cannot cause an event and disable the required protection function assuming a single failure, then there is no difference to a postulated CCF.	The assumption that control system interactions with the protection system is a protection system design requirement based on single failure criteria is not correct. Control system interactions with the protection system is a separation and independence issue (IEEE Std 384, not IEEE Std 379). Section B.3.1 (4) was intended to address a CCF that resulted in an effect on control and loss of protection. Sec B.3.1 (4) will be revised to improve clarity by removing first part of the sentence which sets a condition for common element or shared sources interactions. This would eliminate the system interaction qualifier and the CCF that affects both systems would still have to be addressed. *Reword*: "When a CCF results in a plant response that requires engineered safety features (ESF) and also impairs the ESF function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the ESF function."
21	12	1	3	Sec. 3.1 (8) a)	Division level actuation by independent and diverse means may not be required if in the event of CCF, adequate protection can be provided by functions not affected by the CCF or manual actions at the component level.	The staff agrees that all safety functions and actuation logic may not be disabled by a CCF. In some cases adequate protection may be provided by functions not affected by the specific CCF. What safety functions potentially could be affected are determined in the D3 analysis. If there is sufficient diversity in the design, the D3 analysis may show a diverse means is not required.
22	13	4	1		If digital I&C systems can be vulnerable to software CCFs to a degree that warrants a BTP, why are software CCFs considered beyond design basis? That is, why are failures that are not expected to occur over the lifetime of the plant given such weight?	With high quality software specification, design, development, and implementation backed by V&V and other testing, the probability of CCF is reduce significantly, but not eliminated. While the probability is low the consequence is high. Note, in the recent Gulf of Mexico oil well leak in the Spring of 2010, the probability for this occurence was very low, leading to less than adequate D3. Then note the high consequence when the leak did occur. Until there is a recision of the SRM 93-087 position, this BTP 7-19 states that CCF is beyond design basis.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
23	14	4	2		The definition of a design basis event is an event that is not expected to occur during the lifetime of the plant. Given that software CCFs have occurred (as opposed to a double-ended cold leg break LOCA), software CCFs should not be considered beyond design basis events. This is especially true for the nuclear industry given it's relatively immature digital system development capabilities.	Until there is a recision of the NRC four-point D3 position from SRM on SECY 93-087, this BTP 7-19 states that CCF is beyond design basis.
24	15	4	3		The SRM to SECY-93-087 did not state that software common mode failures were beyond design basis. Rather, the SRM (ML003708056) states that [all] common mode (cause) failures are beyond design basis events. Industry history with digital system failures reveals that at least one event resulted in a common cause failure; therefore, the design basis conclusion is not valid.	Until there is a recision of the NRC four-point D3 position from SRM on SECY 93-087, this BTP 7-19 states that CCF is beyond design basis.
25	16	2	1	A, Page 2 Par. 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.	The staff agrees that this statement regarding combining echelons of defence is not relevant to the purpose of BTP 7-19 and can be removed without impact to the guidance. The sentence will be deleted from Revision 6. A finer point is that echelons of defense that are not in the same safety-grade category (safety vs non-safety) shall not be combined. The basis for this position is the separation and independence requirements of IEEE Std 603, and by reference, IEEE Std 384.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
26	17	2	2	A, Pg. 2 Par. 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.'	The staff accepts the comment in part and Revision 6 will be modified as recommended.
27	18	2	3	A.2, Pg. 3 Last Par.	"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.'	The staff agrees with the comment, but not the solution. This section of the BTP is intended to point out relevant guidance and not to restate or interpret that guidance. Revision 6 will be revised as follows: "IEEE Std. 379 2000, Clause 5.5, establishes the relationship between common cause failures and single failures by defining criteria for CCFs that are not subject to single-failure analysis. This clause also identifies D3 as a technique for addressing CCF. Revision 6 will eliminate reference to clause 6.1"

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
28	19	2	4	A.3, Pg. 4, Par. 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 software logic-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.	SRP 7.3 differentiates between the Engineered Safety Features Actuation System (ESFAS) and "ESF control systems." This BTP is applicable to the "sense and command features" (from Figure 3, IEEE Std. 603 - 1991) that include RTS and ESF, auxiliary supporting features, and other auxilary features. Revision 6 will be modified to improve clarity. Reword: " … the NRC position on D3 for I&C systems incorporating digital, software-based or software logic-based sense and command features of RTS and ESF, auxiliary supporting features, and other auxilary features as appropriate."
29	20	2	5	B.1.1, Pg. 5, Par. 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:'	The staff agrees and Revision 6 will be modified as recommended.
30	21	2	6	B.1.1, Pg. 5, Par. 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.	The staff agrees. NUREG/CR-6303 labeled this echelon as the "ESFAS echelon", but then defined this echelon to include the safety equipment, actuation, and controls. Revision 6 will be modified to clarify this point.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
31	22	2	7	B.1.3, Pg. 5, Last Par.	"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.'	The staff agrees that there were early digital systems, but there were traditional analog systems with discrete and separate components. Revision 6 will be revised to change "traditional" to "analog." Further, the main issue in this introduction to combining echelons of defense is the potential effects of CCF when the RTS and ESFAS functions are combined compared to discrete component systems, rather than the effect on a single failure in a division. If RTS and ESFAS are combined in one microcomputer or controller, a random single failure of that microcomputer could defeat both RTS and ESFAS for that division alone. A CCF caused by a hidden flaw tiggered by some event could in theory defeat both RTS and ESFAS in all divisions. Revision 6 will be revised to provide further clarification and also mention the single failure effect in a division.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
32	23	2	8	Sec 1.4, Pg. 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.	The staff does not agree. Point 2 of the NRC four point policy on D3 used the term "best-estimate." A similar, but more accurate and frequently used term is "realistic assumptions." The staff provided a clarifying example to emphasize that the analysis could be performed for normal or nominal power level conditions rather than typical FSAR Chapter 15 analysis methods, i.e. 102% power. The use of normal or nominal power does not exclude the analysis of events where the worst case is at a power level of less than 100% rated thermal power where needed for some design base accidents.
33	24	2	9	B.1.4, Point 2, Pg. 6, Par. 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 ... '	The staff agrees with the intent of the comment. Some design basis accidents may occur at other than normal power operating levels (e.g., low-temperature over pressure events occur at zero power levels). Revision 6 will add a definition of "realistic assumptions" in Section B.1.4 and not repeat the definition later. The phrase " corresponding to the event" will be included in "Concerning Point 2" after "normal power operation" in the recommended rewording to clarify that the use of "normal power" does not exclude the analysis of events where the worst case is at a power level less than 100% of rated thermal power.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
25 34		2	10	B.1.4, Point 4, Pg. 6, Par. 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.	The Staff agrees with the comment in that Point 4 directs a set of displays and controls in the MCR for manual actuation of the (plant) critical safety functions at the system or division level (depending on the design.) Once actuation has occurred, there may be a need for the use of controls outside of the MCR to maintain these (plant) critical safety functions when supported by suitable Human Factors Engineering (HFE) and procedures and instructions. Revision 6, Section B.1.4, will be revised with a specific paragraph to reflect this recommendation.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
35	26	2	11	B.1.4, Point 4, Pg. 6, Par. 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.	The staff finds the comments helpful, but disagrees that the words "safety systems" in Point 4 add ambiguity, since Point 4 specifically directs inclusion of displays and manual controls that, "… shall be independent and diverse from the safety computer system in items 1 and 3 above." The "safety computer system" refers to the (sense and command features) safety-related automated reactor trip systems and safety-related automated ESF actuation systems. Point 3 also addresses manual initiation methods of RTS and ESFAS, if subject to a postulated CCF. Point 3 directs inclusion of a diverse means, if needed, to protect against a postulated CCF. However, some of the Point 4 displays and controls may be credited as a part of or all of the diverse means. The Independence requirements of a diverse protection system from the safety protection system (i.e., physical, electrical, and communication separation) are defined in IEEE Std. 603. The diverse means could be safety-related and part of a safety division, and would then be subject to meeting divisional independence requirements. The diverse means could also be non-safety-related in which case, the independence from safety system requirements would need to be met. In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system. Revision 6, Section B.1.4, will be revised to provide further clarification.
36	27	2	12	Sec. 1.4, Pg. 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.'	The staff agrees. Revision 6 will be modified as recommended.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
37	28	2	13	B.1.4, Pg. 7, Par. 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".	The staff accepts this recommendation and Revision 6 will be revised as suggested.
38	29	2	14	B.1.4, Pg. 7, Par. 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.	The staff disagrees that these statements imply new requirements. These statements are simply part of the background and provide helpful information. Current protective trip systems employ diverse trip functions to address the same events. For example, both a Departure from Nuclei Boiling Ratio (DNBR) trip and a low pressure trip are design to protect fuel rod cladding. A high temperature trip and a high flux trip are designed to prevent fuel damage. A containment high pressure trip and a reactor low pressure trip are design to protect containment integrity (low reactor pressure implies a Large Break Loss of Coolant Accident (LBLOCA), which could overpressurize the containment).
39	30	2	15	B.1.5, Pg. 7, Par. 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.	Section B.1.5 provides important awareness that there may be a need for two manual initiation means: one to meet the regulatory requirements of IEEE 603-1991 and one to satisfy Point 3 (not point 4) for a diverse means. Some of the displays and controls of Point 4 may be credited as some or all of the diverse means needed to satisfy Point 3. The purpose of this section is to state that if the diverse means is safety related and meets other relevant criteria, then only one manual initiation means is needed. Revision 6, Section B.1.5, will be revised to provide additional clarification to avoid confusion.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
40	31	2	16	B.1.5, Pg. 7, Par. 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.'	The staff agrees and will reword based on the comment.
41	32	2	17	B.1.5, Pg. 7, Par. 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.'	The purpose of Section B.1.5 is to emphasize that two different manual initiation means may be required and present the criteria that would allow only one manual initiation means. Section B.1.5 will be adjusted to simplify presentation of the section purpose and reflect the comments the staff is in agreement with. Comment (1); the staff agrees, but notes: Revision 6 states that safety functions that were normally performed manually could still be performed manually in the presents of a postulated CCF (even if applied to different equipment.) Point 4 implies that the main focus of Point 3 is on the automatic safety functions when reference is made to "safety computer system identified in items 1 and 3 above". Comment (2): the staff agrees. Coment (3); the diverse means directed by Point 3 is to provide an alternate for accomplishing a safety function subject to a postulated CCF. Some of the displays and controls of Point 4 may be credited as the diverse means directed by Point 3.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
42	33	2	18	B.1.5, Pg. 7, Par. 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.'	The purpose of Section B.1.5 is to emphasize that two different manual initiation means may be required and present the criteria that would allow only one manual initiation means. Section B.1.5 will be adjusted to simplify presentation of the section purpose and reflect the comments the staff is in agreement with. The staff disagress that there should be no contingency. Point 3 specifically directs the inclusion of a diverse means to perform a safety function that may be disabled by a postulated CCF. The manual controls of Point 4 may be able to provide part of or all of the diverse means directed by Point 3.
43	34	2	19	B.1.5, Pg. 7, Par. 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.'	The staff agrees with the four points in the comments and Section B.1.5 will be revised to provide more clarity including using the first sentence recommended. However, the key point made by Section B.1.5 is whether or not two different manual initiation means are required and emphasizing criteria for having only one manual initiation means. [Begin adjustment of 02/22/2012, based on response of 01/27/2012 to ACRS letter of 11/14/2011] The ACRS liked a figure in the slide presentation by the NRC I&C staff and recommended it be included in Revision 6] The staff will add Figure 1 to BTP 7-19, Revision 6, in Section B.1.5. The acceptance criteria in Section B.3.1, Item (6) will reference the figure. Figure 1 illustrates the concept of a need for two different manual means for initiating the automated protection system functions verses criteria for having only one manual initiation means [end update].

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
44	35	2	20	B.1.6, Pg. 7, Par. 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.'	The key point of Section B.1.6 is to introduce the D3 analysis and establish that if the D3 analysis determines there is a potential for a CCF, then a diverse means needs to be provided. The purpose of Section B.1.7 is only to briefly state that the diverse means may be automated or manual, but automated is generally preferred. The suggested rewording applies to Section B.1.7 and is already included in the guidance part in Section 3.4.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
45	36	2	21	B.1.7, Pg. 8, Par. 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.'	Revision 6, will be edited to reflect the staff evaluation of these comments including additional paragraphs in Sections B.1.4, and B.1.7. Comment (1); if the diverse means is non-safety, then the IEEE 603 Clause 5.6, "Independent," directs the separation or independence requirement. Comment (2); the primary focus of BTP 7-19 is a diverse means available due to an automated safety system function being subject to a postulated CCF. BTP 7-19 states that if a function was performed manually prior to a postulated CCF, then it may still be performed manually if the safety system is adversely affected by a CCF (even if applied to different equipment.) The staff agrees that If manual action actuates a function on safety systems that are credited in the safety analysis, but this manual actuation method could be adversely affected by a potential CCF, then again a diverse means is needed to manually perform the safety function or an acceptable alternate function. Comment (3); the staff agrees. Comment (4): the staff agrees and will included a statement in Section B.1.5.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
46	37	2	22	Sec. 1.8, Pg. 8, 2nd Par. , 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.	The staff will accept the comment and Revision 6 will be modified as recommended.
47	38	2	23	B.1.8, Pg. 9, Par. 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 ... '	The staff accepts the comment and Revision 6 will be modified as recommended.
48	39	2	24	B.1.9, Pg. 9, Par. 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?	Section B.1.9 revised to clarify that either diversity OR testability is sufficient to eliminate consideration of CCF.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
49	40	2	25	B.1.8, Pg. 9, Par. 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.'	The staff disagrees it can be concluded that simply because spurious trips and actuations are self-announcing, that the software defect can be detected and corrected prior to a CCF. However, Revision 6, Section 1.8 will be revised [Begin adjustment of 02/22/2012, based on response of 01/27/2012 to ACRS letter of 11/14/2011 to be consistent with ISG-02] to provide guidance that: Failures of the automated protection system stemming from a software CCF can cause spurious actuations. The plant design basis addresses the effects of certain software CCF-caused spurious actuations. The overall defense in depth strategy of a plant should prevent or mitigate the effects of credible spurious actuations caused by a software CCF that have the potential to place a plant in a configuration that is not bounded by the plant's design basis. If existing coping strategies (e.g., emergency, normal, and diverse equipment and systems, controls, displays, procedures, and the reactor operations team) are not effective for responding to credible postulated spurious actuations that result in the plant exceeding its design basis, the licensee should develop additional coping strategies [end update]. Note that a spurious actuation may not annuciate if the CCF affects primary annunciation signals, causing a dependence and need for a diverse means.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
50	41	2	26	Sec. 1.9 (1), Pg. 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.	This is an illustrative example of an approach and not intended to provide detail instructions. The staff will incorporate the main elements of the suggested rewording, but disagrees with the full discussion. While the staff recognizes that dual systems may increase O&M procedures, training, spare parts, etc. and thus increased cost, it should be noted that similar, offsetting cost would be incurred by retaining one digital platform for the four divisions and adding a diverse system. Even if the most likely cause of CCF results from human errors and a high quality software or logic development by software is achieved, there still exist the possibility of a CCF. Even if the potential for a CCF is low, the consequence could be significant, unless the possibility of a CCF is adequately addressed.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
51	42	2	27	B.1.9 (2), Pg. 9, Par. 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;'	The staff agrees with the comment concerning "external" states. Revision 6 will be revised to be consistent with the definition of 100% testing from DI&C-ISG-04, Section 2, Item 6.
52	43	2	28	B.2, Pg. 10, Par. 1	"...HFE analysis associated with manual operator actions as an independent and diverse an 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.'	Staff accepts the comment and Revision 6 will be revised as recommended.
53	44	2	29	B.3.1, Pg. 10, Par. 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.	Disagree with *reword*. The term "postulated accidents" is not used in licensing terminology such as in 10CFR50.36, Technical Specifications.
54	45	2	30	B.3.1 (1), Pg. 10, Par. 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 ..."	The staff agrees with the intent of the comment. Some design basis accidents may occur at other than normal power operating levels (e.g., low-temperature over pressure events occur at zero power levels). Revision 6 will define "realistic assumptions" in Section B.1.4 and not repeat the definition by deleting the "(e.g., plant operating at normal power levels, temperature, pressure, flows, normal alignment of equipment,etc)" from Section B.3.1 (1).

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
55	46	2	31	B.3.1 (2), Pg. 10, Par. 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 ... '	The staff agrees with the intent of the comment. Some design basis accidents may occur at other than normal power operating levels (e.g., low-temperature over pressure events occur at zero power levels). Revision 6 will define "realistic assumptions" in Section B.1.4 and not repeat the definition later.
56	47	2	32	B.3.1 (6), Pg. 11, Par. 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".	The staff accepts the comment and Revision 6 changes "division level" to "system or division level (depending on the design)"
57	48	2	33	B.3.1 (6), Pg. 11, Par. 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.'	The staff agrees. Revision 6 will delete the sentence of concern as part of adjusting Section B.3.1 (6) to be consistent with the modifications to Section B.1.5. If the diverse means is non-safety, then the IEEE 603 - 1991, Clause 5.6, "Independent," directs the separation or independence requirement between the safety systems and the diverse means.
58	49	2	34	B.3.1 (7), Pg. 11, Par. 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 ... '	The staff agrees and Revision 6 will be revised as recommended. If the diverse means is non-safety, then the IEEE 603 - 1991, Clause 5.6, "Independent," directs the separation or independence requirement between the safety systems and the diverse means.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
59	50	2	35	B.3.1 (8), Pg. 11, Par. 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..'	The staff agrees and Revision 6 will be revised as recommended.
60	51	2	36	B.3.1 (8) a), Pg. 11, Par. 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".	The staff accepts the comment and Revision 6 changes "division level" to "system or division level (depending on the design)"
61	52	2	37	B.3.1 (8) c), Pg. 11, Par. 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 ...'	The staff agrees with rewording suggested. Revision 6 will be revised as recommended.
62	53	2	38	B.3.1 (8) e), Pg. 12, Par. 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.'	The staff agrees that malfunctions are limited to those affected by the CCF. However, these malfunctions may include the normally used displays that support the safety systems. Therefore the diverse means needs to include diverse displays that will not be affected by the CCF and support the operator in determining the important plant status from B.3.1 (8) e).

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
63	54	2	39	B.3.1 (9) e), Pg. 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.	The staff agrees. Revision 6 will be revised to state, "Use of design techniques (e.g., redundancy, conservative setpoint selection, coincidence logic, and use of quality components) to mitigate these concerns is recommended."
64	55	2	40	B.3.1 (9) , Pg. 12, Par. 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. "Use of design techniques (e.g., redundancy, conservative setpoint selection, coincident logic, and use of quality components) to mitigate these concerns is recommended."	Point 4 clearly states that the set of displays and controls used to support the (plant) critical safety functions are independent and diverse. However, Point 3 only indicates the need for a diverse means not subject to the postulated CCF. The staff accepts the comment and Revision 6 will be revised as recommended. If the diverse means is non-safety, then the IEEE 603 - 1991, Clause 5.6, "Independent," directs the separation or independence requirement between the safety systems and the diverse means.
65	56	2	41	B.3.1 (9) , Pg. 12, Par. 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".	The staff disagrees. Redundancy does not imply the need for single failure compliance. Redundancy is implied by use of 2-out-of-2, 2-out-of-3, etc.. Guidance should not suggest the amount of coincidence needed.
66	57	2	42	B.3.2, Pg. 12, Par. 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.'	The staff agrees with the comment. Revision 6 will be revised as recommended.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
67	58	2	43	B.3.3, Pg. 12, Par. 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...'	The staff agrees with the intent of the comment. Some design basis accidents may occur at other than normal power operating levels. Revision 6 will add the definition for "realistic assumptions" to the discussion in "Concerning Point 2" of the four-point NRC position in Section B.1.4 and not repeat the definition by deleting the "(e.g., plant operating at normal power levels, temperature, pressure, flows, normal alignment of equipment,etc)" from Section B.3.3.
68	59	2	44	B.3.5, Pg. 13, Par. 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 I.A and SRP 18-A Section 1.A. This paragraph should be deleted from BTP 7-19.	The staff agrees that the required time margin between time available and time required to accommodate uncertainties in the estimate of time required is a Human Factors Engineering (HFE) issue to be justified (as noted in Revision 6) using SRP Appendix 18-A. However, this note has the purpose of emphasising factors to consider before selecting either an automated or operator action as the diverse means. No change is needed, except for some minor word editing. [Begin adjustment of 02/22/2012, based on response of 01/27/2012 to ACRS letter of 11/14/2011 to address ACRS recommendation on the "note"] The "note" will be adjusted based on the ACRS recommendation and input from human factors branch, reactor systems branch, and I&C NRC staff. See comments concerning Section B.4.6 below for final wording of the "note" [end update].

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
69	60	2	45	B.3.5, Pg. 13, Par. 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.	The staff accepts the comment. See next comment below (comment on B.3.5, Pg 13, Paragraph 3, for suggested wording. The wording of Revision 6 will be changed to, "Diverse system manual initiation of a safety system function should be performed on a system level or division level basis (depending on the design)."
70	61	2	46	B.3.5, Pg. 13, Par. 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.'	The staff agrees with the comment and Revision 6 will be revised using the recommendation. Revision will be changed as follows: "Diverse system manual initiation of a safety system function should be performed on a system level or division level basis (depending on the design). 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. " Note, the suggested word "backup" was not included in the revision.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
71	62	2	47	B.3.5, Pg. 13, Par. 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.'	The staff agrees with the comment and Revision 6 will be revised using the recommendation. "Diverse manual initiation of safety functions should be performed on a system level or division level basis (depending on the design). Since single failures concurrent with a CCF are not required to be postulated and normal alignment of equipment is assumed, the capability for manual actuation of a single division is sufficient. For plants licensed to allow one division to be continuously out of service, the diverse manual actuation must apply to at least one division that is in service (see section B.3.1, item 9). A CCF that affects normal displays or controls shall not prevent the operator from manually initiating safety functions. Prioritization between safety and diverse 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."
72	63	2	48	B.3.6, Pg 15, Par. 1	"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.	It is not the intent of Point 4 to exclude ESF digital equipment. The term "ESFAS" will be changed to simply "ESF" to provide clarity and to be consistent with the discussion of the echelons of defense in Section B.1.1.

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
73	64	2	49	B.3.9, Pg. 14, Par. 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.'	The staff agrees with the comment and Revision 6 will be revised using the recommendation which is the definition used in DI&C-ISG-04 Section 2 item 6.
74	65	2	50	B.3.10, Pg. 15, Par. 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.	The staff agrees with the comment and Revision 6 will be revised as recommended.
75	66	2	51	B.3.10, Pg. 15, Par. 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.'	The staff agrees with the comment and Revision 6 will be revised as, "The point at which the manual controls are connected to safety equipment should be downstream of equipment that can be adversely affected by a CCF.
76	67	2	52	B.3.10, Pg. 15, Par. 3	"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.'	The staff agrees with the comment and Revision 6 will be revised as follows: "The displays may include digital components that are not adversely affected by a CCF of the safety functions credited in the accident analysis."

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
77	68	2	53	B.4.3, Pg. 16, Par. 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: **1.0)** * ASIC qualification was done with COTS process. There was no review of the software/firmware lifecycle documents documented by NRC." **2.0)** * 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 staff recognizes the comments as having merit, but disagrees that the 100% testing as discussed in the guidance in Section B.1.9 and B.3.9 above goes beyond the regulatory acceptance for testing coverage in the explicit reference to the WCAP 15413 SER. Again, this is guidance and an applicant can present alternate methods. The staff agrees that the Westinghouse example may not be appropriate. Section B.4.3 has been revised as follows: "4.3 Exclusion of Components from D3 Analysis "A software-based component may be sufficiently simple and deterministic in performance such that the component is not a significant source of a CCF. Such components need not be considered in a D3 analysis. When a basis is given that a component is not susceptible to CCF, the NRC staff should examine the justification carefully."

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
78	69	2	53	B.4.3, Pg. 16, Par. 4	(Item 53 Continued) **2.1)** *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. **2.2) *** 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. **2.3)** * 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.	(Reserved for continuation of response to comment above above, Comment 68, from Doc. 2, Item 53)
79	70	2	54	B.4.5, Pg. 16, Par. 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...'	The definition of realistic assumptions has been added to Section B.1.1. Section B.4.5 has been changed as follows: "Thermal-hydraulic analyses, using realistic assumptions of the sequence of events that would occur if the primary trip channel failed to trip the reactor or actuate ESF are included in the assessment. (Coordination with the organization responsible for the review of reactor systems is necessary in reviewing these analyses.)"

	A	B	C	D	E	F
8	**Comment No.**	**Doc**	**No**	**Location**	**Public Comment**	**NRC Response**
80	71	2	55	B.4.6, Pg. 17, Par. 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 I.A. This paragraph should be deleted from BTP 7-19.	The staff disagrees with deleting the note, but agrees that the required time margin between time available and time required to accommodate uncertainties in the estimate of time required is a Human Factors Engineering (HFE) issue to be justified (as noted in Revision 6) using SRP Appendix 18-A. However, this note has the purpose of emphasising factors to consider before selecting either an automated or operator action as the diverse means. [Begin adjustment of 02/22/2012, based on response of 01/27/2012 to ACRS letter of 11/14/2011 to address ACRS recommendation on the "note"] The "note" will be adjusted based on the ACRS recommendation and input from human factors branch, reactor systems branch, and I&C NRC staff and presented as follows: "Note: As the difference between Time Available and Time Required for operator action is a measure of the safety margin and as it decreases, uncertainty in the estimate of the difference between these times should be appropriately considered. This uncertainty could reduce the level of assurance and potentially invalidate a conclusion that operators can perform the action reliably within the time available. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed." [end update]
81					END PUBLIC COMMENTS	END NRC RESPONSE