Table of Public Comments and NRC Staff Response on the Draft Revised REGULATORY ISSUE SUMMARY 2014-XX EMBEDDED DIGITAL DEVICES IN SAFETY- RELATED SYSTEMS (ML12248A065) Issued June 05, 2014

Special Note Number (SN#)	Special Notes concerning this Table of Public Comments and NRC Staff Response document
SN1	The revised RIS Title is now, "REGULATORY ISSUE SUMMARY 2015-XX, EMBEDDED DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS" (see ADAMS Accession No. ML15118A015).
SN2	This Table of Public Comments and NRC Staff Responses has an ADAMS Accession No. of ML15118A012.
SN3	For simplicity the term "staff" will be used hereafter in place of using the term "NRC staff."
SN4	For simplicity the acronym "EDD" or "EDDs" will be used in place of repeating "embedded digital device(s)."
SN5	When commenters reference or quote a specific section, page, sentence, or paragraph, they are referring to a location in the draft revised EDD Regulatory Issue Summary (RIS) issued June 05, 2014 (ML13338A769). When the staff states a change has been made, it means text from the issued draft RIS of June 5, 2014 has been changed and the revised sentence, wording, or paragraph will appear in the final RIS.

Table List of Commenters (Cmntr)				
Cmntr ID Code	**Commenter Organization**	**Organization Type**	ADAMS Accession Number	NRC Public Comment Set Number
N	Nuclear Energy Institute (NEI)	Nuclear Industry Institute	ML14191A013	3
E	Electric Power Research Institute (EPRI)	Nuclear Industry Institute	ML14175A247	1
F	Florida Power & Light Company	Utility	ML14192A010	4
A	Nuclear Automation Engineering, LLC	Consultant	ML14190A008	2
M	MIT Nuclear Reactor Laboratory	University	ML14198A063	6
D	NewClear Day, Inc.	Consultant	ML14198A062	5
P	The Pennsylvania State University	University	ML14198A064	7
U	University of Florida	University	ML14198A065	8
S	STARS Alliance, LLC	Utility	ML14198A075	9
I	Individual e--mail	Consultant	ML15112A179	10

Public Comment and NRC Staff Response Table Header Legend	
Symbol	**Definition**
MstrCmnt #	Master Comment Number (unique to each comment)
Cmntr ID & #	Commenter Identification Code (Cmntr ID Code) plus an NRC assigned commenter comment number (alphabetic letter + number)
Ch	Change; comment resulted in a change to the draft RIS; Y= Yes , N= No
Comment and Proposed Change	Public Comment submitted by commenter identified by "Cmntr ID" and Commenter's proposed change to the draft revised EDD RIS (ML13338A769) issued June 5, 2014
NRC Staff Response	NRC staff response to the public comment and proposed change

Table of Acronyms	
Acronym	**Definition**
ADAMS	Agencywide Documents Access and Management System
BTP	Branch Technical Position
BWR	Boiling Water Reactor
10 CFR	Title 10 of the *Code of Federal Regulations*
CDA	Critical Digital Asset
CCF	Common cause failure as a result of a EDD defect concurrently triggered to cause a failure of multiple equipment units within a division or in redundant, but otherwise independent divisions
CGD	Commercial Grade Dedication
CGID	Commercial Grade Item Dedication
CRGR	Committee to Review Generic Requirements
D3	Diversity and Defense-in-Depth
EDD	Embedded digital device
DI&C	Digital Instrumentation and Controls
I&C	Instrumentation and Controls
IEEE	Institute of Electrical and Electronic Engineers
IROFS	Items Relied On For Safety
ISG	Interim Staff Guidance
NPR	Non-power reactors
NRC	United States Nuclear Regulatory Commission
OE	Operating Experience
OGC	Office of General Counsel
PWR	Pressurized Water Reactor
QA	Quality Assurance
RG	Regulatory Guide
RIS	Regulatory Issue Summary
SRP	Standard Review Plan (NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition”)
Std	Standard

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
1	N1	**Comment:** [General] One area where the resolution of public comments on the earlier version has introduced a new issue for new plants or retrofits is the strong discussion of diversity with respect to simple devices that contain embedded digital components. The issue is of importance to the industry as design and procurement strategies are developed for the new plants regarding the use of 'smart' components or other devices that may contain embedded digital components. This ambiguity may adversely affect project decisions (in) the selection of plant equipment. **Proposed Change:** Address the perceived ambiguity directly such that project decisions can be made with full understanding.	Y	The staff, in part, agrees with the comment that simple verses complex and diversity in equipment with EDDs are important issues, and some further clarification has been made to remove perceived ambiguities. Since it is difficult to define a "simple" component, the use of the term "simple" has been removed. The RIS has been revised to emphasize that while the staff does not automatically exclude any equipment with EDDs from consideration in CCF vulnerability assessments, justification can be supplied as appropriate for the specific nuclear facility and application. Nevertheless, simplicity remains an important design consideration. The safety-related I&C in general can be grouped into three categories: (1) the protection systems and control systems (sense and command features), (2) data communications, and (3) certain other nuclear facility equipment (actuated equipment or execute features). The application software and programmable logic in these protection systems and control systems are usually designed, reviewed, and regulated specifically in accordance with regulations and guidance applicable for the specific type of nuclear facility. In general, the data communication systems and certain other nuclear facility equipment (e.g., motor control centers) and commonly used unit components from the sense and command features (e.g., transmitters, meters, and other indicating units) may be designed as non-nuclear industry commercial products. This may be the situation in many units of commercial equipment with EDDs where the development process is either not of the same quality as required by the NRC regulations or recommended by guidance, if applicable, different but equivalent, or unknown. Some of these components may be relatively simple and easily tested, while others are complex. However, these commercial products may have a successful operating history outside the nuclear industry that may be useful in helping justify these equipment units for use in nuclear facilities. A key concern with equipment with EDDs is the possibility that an undetected EDD defect (e.g., such as a software defect) may be triggered to cause the component to fail to function as intended. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF). Depending on certain factors as complexity, the risk significance of the system the components are in, knowledge of quality development, thorough testing, and a successful operational history, a licensee may be able to supply sufficient justification for a reasonable assurance of safety. This may be the case with those non-nuclear industry developed commercial products even with EDDs.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				In “very low probability of CCF, but very high damage consequence” systems as nuclear power reactor protection systems, complexity may prevent software or logic from being reasonably assured to have “no hidden defect.” In such cases, diversity and defense in depth help to reach a determination of reasonable assurance of safety.
2	N2	**Comment:** [General] Branch Technical Position BTP 7-19 was written as an NRC internal document. **Proposed Change:** References to Regulatory Guides would seem more appropriate.	N	The staff agrees in part with the comment that BTP 7-19 was written as part of the SRP as an internal document to establish criteria that the NRC staff intends to use in evaluating whether an applicant/licensee meets the NRC regulations. The staff disagrees with the implication that BTP 7-19 is not an appropriate reference in this RIS. In practice, applicants usually use the BTPs to understand what would be one acceptable way of meeting the regulations. Note that the regulations for construction permits [10 CFR 50.34(h)(1)(i)] and new design certifications [10 CFR 52.47(a)(9)] require, in part, applicants to indicate how their application conforms with or differs from the SRP acceptance criteria. The SRP is not a substitute for the regulations, and compliance is not a requirement. Applicants can propose alternative methods to the SRP criteria. It is possible a proposed design employing equipment with EDDs in safety-related systems may meet the intent of the regulations and yet differ from the SRP criteria.
3	N3	**Comment:** [General] Public comments from the earlier revision indicate that the RIS is attempting to define as "digital devices" a range of components not already defined by IEEE standards as digital devices. The public comments also state that this attempt to redefine the scope of what is a "digital device" could lead the licensee to scope more components as Critical Digital Assets pursuant to 10 CFR 73.54. The NRC disagreed with these comments, and in part of their dissent made this statement: "Therefore, merely classifying components as "digital" would not likely force licensees to classify components as CDAs." As further support to this concern, it has been announced that NEI has submitted a petition for rulemaking related to Cyber Security Digital Assets. On June 12, 2014, NEI submitted a petition to the NRC to amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks." The petition for rulemaking	Y	The staff disagrees with the comment that classifying components as "digital devices" would likely force licensees to classify components as CDAs. The cyber security paragraph in the INTENT Section of the RIS has been simplified to state, “Regulatory issues associated with equipment with EDDs related to common defense and security under 10 CFR Part 73, ’Physical Protection of Plants and Materials,’ and 10 CFR Part 74, ’Material Control and Accounting of Special Nuclear Material’ are beyond the scope of this RIS.” The Background Section of the RIS states the following: “For the purposes of this RIS, an embedded digital device is a component consisting of one or more electronic parts that requires the use of software, software developed firmware, or software developed programmable logic and that is integrated into equipment to implement one or more system safety functions.” Therefore, if a licensee determines that equipment with EDDs is a CDA, the EDDs are components of a CDA under the cyber security regulation. As explained in the response (ML13351A204) to the public comments on the

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		specifically requests the NRC to revise the scope of § 73.54(a)(1), which has resulted in licensees having to implement cyber security controls on hundreds to thousands of digital assets, most of which have no direct relationship to radiological sabotage. Among the suggested changes in the petition for rulemaking is a revision to § 73.54(a)(1) that would insert "structures, systems, or components." The revision would read: *"10 CFR 73.54 provides the programmatic requirements to defend against the design basis threat of radiological sabotage cyber-attack. As an integrated component of the physical protection program, the cyber security program is designed to prevent significant core damage and spent fuel sabotage.* *To prevent significant core damage and spent fuel sabotage, licensees may rely on plant structures, systems, or components to perform certain functions. Through the analysis required by 10 CFR 73.54(b)(1), the cyber security rule must be implemented to identify those digital computer and communication systems and networks that, if subject to the cyber-attack described in 10 CFR 73.54(a)(2), would adversely impact the capability for systems and equipment to perform their intended function to prevent significant core damage and spent fuel sabotage".* The NRC should acknowledge that by redefining the scope of "digital devices" in this RIS, cyber-security analysis and scoping of CDAs will be impacted. The incorporation of these comments should be coordinated with the NRC's Office of Nuclear Security and Incident Response (NSIR) to determine if the impact indicated is warranted. Redefining more basic components as "digital devices" will indeed cause the licensee to consider these newly defined digital devices when analyzing critical systems and will result in the scoping of more CDAs. In addition, it should be noted that NRC is considering cyber security requirements for fuel cycle facilities that would need to be reflected in and consistent with this RIS.		initial draft RIS, "Embedded Digital Devices in Safety- Related Systems, Systems Important to Safety, and Items Relied On For Safety" (ML12248A065), which was issued on May 20, 2013, this comment is not consistent with cyber security regulation 10 CFR 73.54(b)(1); Section 3.1.3, "Identification of Critical Digital Assets" of Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities;" or Section 3.3 of the licensees' NRC-approved cyber security plans. Specifically, the regulation, the regulatory guide, and the cyber security plans state that a licensee can determine, through analysis, if a digital asset within the scope of 10 CFR 73.54(a) qualifies as a CDA. If the analysis shows that a compromise of the digital asset could lead to adverse impact to safety, important-to-safety, emergency preparedness, or security functions, the digital asset is a CDA. Through these analyses, the licensee can identify a minimum set of CDAs within the digital assets that are within the scope of the cyber security regulation. Therefore, since an EDD is just a component of the equipment/asset in which it is incorporated, the EDD itself does not automatically cause licensees to scope more components as CDAs nor does it make the equipment/asset a CDA. A digital asset is determined to be a CDA by following the analysis process specified in the previous paragraph. Based on the above, the staff finds that merely classifying components of equipment/assets as "digital devices" would not require the licensees to scope such components or equipment/assets as CDAs. The comment goes on to state that this concern is shared by NEI in its petition for rulemaking related to cyber security digital assets submitted on June 12, 2014. The NRC acknowledges the receipt of NEI's petition to the NRC to amend 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: The NRC should acknowledge that by redefining the scope of "digital devices" in this RIS, cyber-security analysis and scoping of CDAs will be impacted. The incorporation of these comments should be coordinated with NSIR to determine if the impact indicated is warranted.		
4	N4a	**Comment:** [General] The broad scoping language associated with the definition and use of the term "safety related" (page 8) as it applies to Fuel Cycle Facilities (FCFs) versus power reactors (page 4) is problematic. Identification of clearly defined consequences of concern for FCFs is needed to risk inform the identification of components and systems that need adequate protection from cyber-attacks. **Proposed Change:** NRC has a decision-making framework (SECY-04-0222) which could be used to establish consequences of concern to assure public health and safety as well as common defense and security.	N	The staff disagrees with the comment. The "Fuel Cycle Facility Sector" section of the RIS explains the use of the term "safety-related" as it applies to FCFs by stating, "For the purpose of this RIS, the term 'safety-related' as applicable to FCFs applies to systems, structures, components, procedures and controls (of a facility or a process) that are relied upon to protect the health and safety of workers, the public and the environment." NRC is issuing this RIS to clarify the NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with EDDs. Common defense and security applications are excluded from the scope of this RIS. Therefore protection from cyber-attacks on components and systems is not considered. As a result of other comments, the "Intent" section of the RIS now states: "Regulatory issues associated with equipment with EDDs related to common defense and security under 10 CFR Part 73, 'Physical Protection of Plants and Materials,' and 10 CFR Part 74, 'Material Control and Accounting of Special Nuclear Material,' are beyond the scope of this RIS."
5	N4b	**Comment:** [Page 1, Second Paragraph of Intent Section] The discussion in this paragraph narrows the scope of the RIS to safety-related equipment and then broadens the underlying concern to non-safety equipment. As a result, the message is made ambiguous. The remaining discussion does not answer the question on how NRC expects the industry to treat requirement for non-safety equipment that contain embedded digital components. **Proposed Change:** NRC should clarify the scope regarding non-safety components with embedded digital devices. The discussion of non-safety equipment should be deleted, since it is not governed by any specific	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems." Also, the staff has deleted the third Paragraph in Item 2 in the Summary of Issue Section on Page 7 of the draft RIS that stated: "Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		regulation. In addition, the direction from the Commission in the Staff Requirements Memorandum to SECY-93-087 does not address non-safety digital components that are neither connected to nor can disable a safety system.		create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)."
6	N4c	**Comment:** [Page 1, line 36] The RIS does not provide a definition for "Important to Safety" system. "Important to Safety" system: "Those I&C systems that prevent anticipated operational occurrences from leading to an unacceptable consequence, or an unanalyzed initial condition assumed for Chapter 15 events." **Proposed Change:** The RIS should be updated to include the following definition for "Important to Safety" system: "Those I&C systems that prevent anticipated operational occurrences from leading to an unacceptable consequence, or an unanalyzed initial condition assumed for Chapter 15 events."	N	The staff disagrees with the proposed recommended definition for "important to safety." The term "important to safety" has been used in current NRC regulations (e.g., 10 CFR Part 50 Appendix A) without the need for a precise definition. Whether a system or component is considered important to safety depends on the plant specific design and use. These considerations include the design of the overall plant, the role of that system or component in supporting plant safety, and whether the system or component is considered risk significant. It is therefore up to the applicant/licensee to determine whether a system or component is important to safety and provide information to justify the decision. The applicant/licensee should make the determination of whether a system is important to safety based on their available processes, whether that is the maintenance rule, the 50.59 process, or other processes. Further, systems that are "important to safety" may not be limited to only those that prevent anticipated operational occurrences from leading to an unacceptable consequence, or an unanalyzed initial condition assumed for Chapter 15 events. For example, with the regulatory treatment of non-safety systems (RTNSS) for passive advanced light water reactors, certain systems may be classified as RTNSS but these systems may not be used to prevent anticipated operational occurrences from leading to an unacceptable consequence, or an unanalyzed initial condition assumed for Chapter 15 events. However, to help avoid any ambiguity that the scope is limited to safety related systems, the second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems."
7	N4d	**Comment:** [Page 1, Second Paragraph of Intent Section] On page 1, the second paragraph under "INTENT" reads:	Y	The staff agrees in part with the comment. The staff agrees that the RIS does not define what the term "important to safety" means. However, whether a system or component is considered

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		"The scope of this RIS is limited to equipment, including instrumentation and controls (/&C), in safety-related systems. Although this RIS excludes systems that are not safety-related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a non-safety system that, if inadequately addressed, could adversely affect safety. For example, a software common cause failure (CCF) in redundant non-safety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses." To a degree, this paragraph places appropriate focus on Safety Related components but continues to rely on the concept of "important to safety". While there are some resources to draw upon (i.e. Generic Letter 84-01), the available guidance is somewhat dated and does not provide a clear definition of what would be considered within the purview of this language. **Proposed Change:** There may be opportunities to more clearly define the scope of the RIS within the context of existing processes that would be beneficial (Maintenance Rule, 10 CFR 50.59 or Standard Review Plan Chapter 7 for example).		important to safety is dependent on the design of the overall plant and the role of that system or component in supporting plant safety or if the system or component is considered risk significant in the overall plant. The applicant/licensee should make the determination of whether a system is important to safety based on their available processes whether that is the maintenance rule, the 50.59 process, or other processes. In order to clarify that the scope of the RIS is limited to safety systems and equipment, the second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems."
8	N4e	**Comment:** [Page 1, Second Paragraph of Intent Section] Page 1, Intent, Second paragraph: *"The scope of this RIS is limited to equipment, including instrumentation and controls (/&C), in safety-related systems. Although this RIS excludes systems that are not safety-related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a non-safety system that, if inadequately addressed, could adversely affect safety."* To a degree, this paragraph places appropriate focus on Safety Related components but continues to rely on the concept of "important to safety". While there are some	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		resources to draw upon (i.e. Generic Letter 84-01), the available guidance is somewhat dated and does not provide a clear definition of what would be considered within the purview of this language. **Proposed Change:** This RIS identifies considerations for both safety and non-safety systems. While this comment only corrects this one sentence, there are many throughout the document that should be changed to address both safety and non-safety systems, as applicable. Alternately, delete all discussion of non-safety applications, and address them in a separate RIS.		
9	N4f	**Comment:** [Page 1, Second Paragraph of Intent Section] Page 1, Intent, Second paragraph: *"For example, a software common cause failure (CCF) in redundant non-safety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses."* **Proposed Change:** For example, a software defect in one or more non-safety controllers might create a common cause failure (CCF) of multiple non-safety control functions that has not been analyzed in the nuclear facility's transient and accident analyses. This concern is pertinent to non-safety systems that can directly initiate plant transients. These systems are often referred to as control systems "important to safety"; they are the systems described in Chapter 7 of the plant's UFSAR.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."
10	N4g	**Comment:** [Page 1, Line 31- 37] The RIS states: "*Although this RIS excludes systems that are not safety-related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a non-safety system that, if inadequately addressed, could adversely affect safety. For example, a software common*	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows:

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		cause failure (CCF) in redundant non-safety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses." In this one statement the RIS both excludes and then includes non-safety equipment consideration. **Proposed Change:** A clear position should be stated on whether embedded digital devices in non-safety system are or are not to be considered for software common cause failure. As stated, the RIS position is unclear and left to interpretation.		"The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."
11	N5	**Comment:** [Background Information, Page 3, Lines 14-19] The RIS states that: "NRC staff guidance does not automatically exclude these (so-called "simple") devices from consideration within the assessment of diversity to address vulnerabilities to potential CCF. Nevertheless, simplicity, diversity, design documentation, quality development, and operational history are some important functions to be considered within analyses to evaluate the suitability for use in an embedded digital device." This guidance does not provide definitive direction for safety equipment developers to adequately plan for what would be required for approval of the suitability for use of such devices. Safety equipment developers need reasonable assurance that the use of such "simple" devices can be approved based on supplying specific documentation and showing compliance with specific regulations. Leaving it up to the developers to determine which guidelines and regulations may be applicable to "simple" logic device introduces financial risk as the developer does not have reasonable assurance that at the end of the development the system can be approved. **Proposed Change:** Clarify the definition of "simple" by stating that simple systems are those that meet the	Y	The staff agrees in part with comment that safety equipment developers need reasonable assurance that supplying specific documentation and showing compliance with specific regulations can lead to a high probability of NRC licensing certainty of DI&C. While this RIS outlines the current applicable regulations and certain guidance documents, the function of a RIS is not the development of new guidance. The NRC staff met with industry representatives in several recent public meetings (e.g., the EDD issue workshop of October 9, 2014) to encourage the development of more specific guidance in the use of DI&C by industry through NEI and EPRI. The paragraph referenced in the comment has been revised for improved clarity by emphasizing that while the staff does not automatically exclude any equipment with EDDs from consideration in CCF vulnerability assessments, justification can be provided as appropriate for the specific nuclear facility and application. While the RIS will not address a definition of "simple," it does reference BTP 7-19. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs in systems with equipment with EDDs located in safety-related systems. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		testability attribute of BTP 7-19 such that they are not considered to have a potential for software-based CCF.		significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety.
12	N6	**Comment:** [Page 2, First Paragraph On page 2, the first paragraph includes the following language: "The scope of this RIS excludes embedded digital devices in systems related to common defense and security under 10 CFR Part 73, "Physical Protection of Plants and Materials," The paragraph goes on to read: "This RIS does not address the cyber security regulation provided in 10 CFR Part 73.54, "Protection of Digital Computer and Communication Systems." This language introduces several logical contradictions. From the perspective of 10 CFR 73.54, "digital" components associated with Physical Security must be considered and evaluated as Critical Digital Assets(CDA's) yet this paragraph seems to exclude them for consideration as digital components at all. Furthermore, the exclusion of Cyber Security implications places licensees in a situation where components outside of Physical Protection that would not normally be considered as "digital" in the conventional sense would now have to be considered as digital components and therefore likely to become CDA's under 10 CFR 73.54. As an illustration of the issue, consider the example of the CPLD based devices installed by several licensees in the Solid State Protection System (the Harris 10 CFR 50.59 inspection finding). These components would now clearly fall within the purview of the RIS as "digital" components yet they lack the attributes common to components within the scope of 10 CFR 73.54. For example, these devices	Y	The staff agrees with the comment that the language in the first paragraph of Page 2 appears to introduce some contradictions with the cyber security rule, 10 CFR 73.54. The intent of the second paragraph was to provide a clarification that the issues associated with cyber security rule are beyond the scope of this RIS, which addresses safety regulations associated with the EDDs in the safety related systems. An additional intent was to remind the readers of the RIS that the licensees' NRC-approved cyber security plans are required to comply with 10 CFR 73.54 as applicable. The NRC-approved cyber security plans are part of licensing bases for the power reactor licensees. The cyber security plans describe how licensees will implement cyber security programs at their facilities to comply with the cyber security rule. The cyber security plans describe how licensees will determine a minimum set of digital assets that need to be protected under 10 CFR 73.54. Additionally, Regulatory Guide 5.71 "Cyber Security Program for Nuclear Facilities," provides a method that licensees can use to comply with 10 CFR 73.54, including a method that licensees can use to determine whether a digital asset within a nuclear power plant is a CDA or not. Based on the above, the staff has revised the language in the Intent Section of Page 2 to the following: "Regulatory issues associated with equipment with EDDs related to common defense and security under 10 CFR Part 73, 'Physical Protection of Plants and Materials,' and 10 CFR Part 74, 'Material Control and Accounting of Special Nuclear Material' are beyond the scope of this RIS."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		have no microprocessor, do not execute sequential instructions (software or firmware), are not vulnerable to conventional malware, operate asynchronously, do not support the use of portable media and are not networked. The language of the RIS appears to make it necessary to classify these components as CDA's despite the fact none of the NEI 08-09 controls can be applied. For a typical dual unit PWR, this alone would force licensees to add several hundred components into the Cyber Security program. This increases the scope and complexity of the Cyber Security program substantially without producing a tangible benefit. The second paragraph on Page 3 seems to exacerbate the issue described above further by defining "embedded digital" component as devices that contains "software developed logic that is permanent". Nearly all fixed logic devices (a conventional "AND" gate for example) would meet this definition. **Proposed Change:** The NRC should acknowledge that by redefining the scope of "digital devices" in this RIS, cyber-security analysis and scoping of CDAs will be impacted. The incorporation of these comments should be coordinated with NSIR to determine if the impact indicated is warranted.		
13	N7	**Comment:** [Page 2, Third paragraph] Page 2, Third paragraph states in part: "Addressees should be aware of any potential vulnerability that could result from a postulated software common-cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices, which includes components implementing safety-related execute features (e.g., motor control centers, actuated equipment)". The use of CCF is incorrect. We postulate a defect, which may cause a CCF if triggered concurrently in multiple systems. We do not postulate a CCF. The concern is not	Y	The staff agrees, in part, with the comment. The RIS has been revised to reflect the concept that an EDD defect is postulated which may cause a CCF if triggered concurrently in multiple systems. A key concern with equipment with EDDs is the possibility that an undetected EDD defect may be triggered to cause the equipment to fail to function as intended. This RIS identifies regulations and guidance for identifying and eliminating defects. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		limited to execute features, it applies also to sense and command features (e.g., digital transmitters). Diversity is not the only defense against CCF. Other defenses are addressed below (e.g. simplicity, non-concurrent triggers). **Proposed Change:** Recommend sentence be revised to read: "Addressees should be aware of any potential CCF of redundant safety related equipment that could result from a postulated software defect within embedded digital devices, which includes component s implementing safety-related sense and command or execute features		such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This may be the situation in many units of commercial equipment with EDDs where the development process is either not of the same quality as required by the NRC regulations or recommended by guidance, different but equivalent, or unknown.
14	N8	**Comment:** [Page 2, fourth paragraph] Page 2, fourth paragraph: "Inadequate consideration of these devices in diversity assessments to address potential software CCFs could lead to an adverse safety consequence." We don't do diversity assessments. In accordance with BTP 7-19 we do CCF vulnerability assessments. Diversity is just one defense against CCF; it is not the only defense. **Proposed Change:** Inadequate consideration of these devices in CCF vulnerability assessments could lead to an adverse safety consequence. "Assessment of diversity" should be changed to "CCF vulnerability assessment" throughout this document.	Y	The staff agrees with the comment that the phrase “CCF vulnerability assessments” is more accurate than “diversity assessments.” The RIS has been modified to provide further clarification and reflect the proposed change. While diversity is not the only defense against the potential for a CCF caused by an EDD defect being concurrently triggered to cause equipment with that EDD to fail in redundant systems, diversity may become a primary strategy to prevent CCFs and support reaching a reasonable assurance of safety.
15	N9a	**Comment:** [Page 2, Fifth and Sixth Paragraphs of Intent Section] The discussion of postulated software common cause failures (CCFs) stemming from the use of non-diverse embedded digital devices coupled with the concern about inadequate diversity assessments strongly implies that diversity is a necessary mitigation strategy for the use of embedded digital devices, **Proposed Change:** NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support	Y	The staff agrees, in part, with the comment that further clarification is needed. This RIS identifies existing regulations and guidance applicable to safety-related equipment with EDDs. For example, while not applicable to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs in systems with equipment with EDDs located in safety-related systems. The BTP 7-19 strategy does not impose a requirement for diverse actuation systems for all safety functions. Rather, the requirement for diverse actuation systems is a last-resort requirement when all other mitigating strategies for one or more specific events have been determined by the licensee to be insufficient.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		obsolescence management strategies or new plant design and procurement strategies. IAEA NP-T-1.5 and EPRI TR-1002835 list are preventative set of fault voidance, fault detection and removal defensive measures that are often useful in developing mitigation strategies against faults and resulting CCFs.		An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This RIS cannot provide details on how to support obsolescence management strategies or new plant design and procurement strategies concerning equipment with EDDs, because it is not the function of a RIS to issue new regulations or guidance.
16	N9b	**Comment:** [Page 2, Fifth and Sixth Paragraphs of Intent Section] There are no bounds on postulated software CCFs and there is no mention of other design approaches that can reasonably minimize the potential for software CCFs as an alternative to component diversity, the ongoing discussions and resulting revision to NEI 01-01. **Proposed Change:** This issue is currently a topic of discussion between the industry and the NRC regarding plans to update NEI 01-01. The proposed RIS for embedded digital devices presents concepts that are not aligned with the ongoing discussions and resulting revision to NEI 01-01.	Y	The staff agrees, in part, with the comment and additional clarification has been added to help remove any perceived ambiguity concerning the use of diversity. Diversity is not usually addressed within the individual EDD level but is associated with equipment with EDDs and the system level. It is possible to apply and take credit for diversity at the EDD level as part of an overall D3 strategy. A key concern with equipment with EDDs is the possibility that an undetected EDD defect may be concurrently triggered to cause the equipment to fail to function as intended in redundant, but otherwise independent systems potentially resulting in a CCF. This RIS identifies regulations and guidance for identifying and eliminating defects. For example, while not applicable to all nuclear facilities, BTP 7-19 provides helpful strategies for dealing with postulated CCFs in digital devices. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. As stated in the 6th paragraph of the Intent Section of the June 2014 draft RIS, the intent of this RIS is to heighten awareness of the existence of embedded digital devices and associated potential hazards. It is not the function of a RIS to provide solutions and/or new guidance for addressing the hazards that may be created by use of EDDs. The need for additional guidance for safe use of EDDs in critical applications is being addressed separately. The staff agrees that updates to NEI 01-01 or a substitute document may provide some of the needed guidance on dealing with EDDs. EPRI is working to develop digital CCF guidance that will apply to EDDs.
17	N9c	***Comment:*** [Page 2, Fifth and Sixth Paragraphs of Intent Section] The implications of this section can extend to needing diversity in non-safety equipment. As stated in these paragraphs, the scope of the RIS is first narrowed to safety-related equipment and then broadens the underlying concern to non-safety equipment. As a result, the message is made ambiguous. **Proposed Change**: NRC should clarify the scope regarding non-safety components with embedded digital devices. The discussion of non-safety equipment should be deleted, since it is not governed by any specific regulation. In addition, the direction from the Commission in the Staff Requirements Memorandum to SECY-93-087 does not address non-safety digital components that are neither connected to nor can disable a safety system.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.”
18	N10	**Comment:** [Page 2, Last Paragraph] Page 2, last paragraph: "... that requires the use of software, software-developed firmware, or software-developed logic and that is integrated into equipment to implement one or more system safety functions" All logic is developed using software, even conventional logic. Clarify applicability to "programmable logic."	Y	The staff agrees with the proposed change. The RIS has been revised, as recommended, to use the term “programmable logic” in place of “logic” at appropriate locations.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: Suggest that the wording be revised as follows: "... that requires the use of software, software-developed firmware, or software-developed programmable logic that is integrated into equipment to implement one or more system safety functions." "logic" should be changed to "programmable logic" throughout this document.		
19	N11	**Comment:** [Page 3, Second Paragraph] Page 3, Second paragraph: The firmware of an embedded digital device may provide limited functionality with a well-documented design basis such that the embedded digital device could be characterized as "simple." Defining "simple" as "limited functionality with a well-documented design basis" is quite different than BTP 7-19 which defines "simple" as 100% testable including all combinations of input states and internal states. This will cause confusion in the industry. Add "concurrent triggers" are another consideration. These are all defenses against CCF. **Proposed Change:** The NRC staff provides guidance applicable to components containing software, firmware, and programmable logic developed from software-based development systems. NRC staff guidance does not automatically exclude the application of these embedded digital devices from consideration within CCF vulnerability assessments. Simplicity, diversity, design documentation, quality development, testing, operational history and the potential for concurrent defect triggers are some of the important factors to be considered within CCF vulnerability analyses to evaluate the suitability for use of an embedded digital device.	Y	The staff agrees in part with the concepts of the comment and proposed change. Since it is difficult to define what is a "simple" component, the paragraph referenced in the comment has been revised to remove the use of the term "simple" and emphasize that while the NRC staff does not automatically exclude any equipment with EDD from consideration in CCF vulnerability assessments; instead justification should be supplied by the licensee as appropriate for the specific nuclear facility and application. While the RIS will not address a definition of "simple," it does reference BTP 7-19. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs in systems with equipment with EDDs located in safety-related systems. BTP 7-19 (Revision 6), Section B.1.9, explains that the application of many system design and testing attributes, procedures, and practices can help significantly reduce the probability of CCF. Two design attributes, either of which is sufficient to eliminate consideration of software based or software programmable logic based CCF are: sufficient diversity and (100%) testability. Depending on the risk significance of the system the components are located in and the type of nuclear facility, knowledge of a quality development process and thorough testing may be sufficient to justify a reasonable assurance of safety. In "very low probability of CCF, but very high damage consequence" systems such as nuclear power reactor protection systems, complexity may prevent software or logic from being reasonably assured to have "no hidden defect." In such cases, diversity and defense-in-depth may help to reach a determination of reasonable assurance of safety.
20	N12	**Comment:** [Page 3, Paragraphs 3 & 4.] As a strictly editorial comment, the 3rd and 4th paragraphs on page 3	N	The staff agrees, in part, with this comment.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		referencing information notices 1994-020 and 2007-015 and the failure mechanisms that underlie. **Proposed Change:** These references do not appear to be directly applicable to the RIS.		Although the events identified in these two references are not directly related to failures of EDDs, these events highlight the need for licensees and applicants to understand that digital systems may have different failure modes than analog systems or even older digital systems. Therefore, licensees and applicants should consider the unique failure modes that EDDs present. For example, in a recent situation a vendor replaced an obsolete integrated circuit (IC) chip on a component using a small circuit board holding an EDD. This small board used the same holes for mounting on the component as the IC. The vendor did not change the part number of the modified component. This revised component was susceptible to an electromagnetic interface failure in certain nuclear facility applications not experienced by the original component.
21	N13	**Comment:** [Page 3, Fourth Paragraph of Background Information Section] This discussion seems to reinforce the expectation that diversity is a necessary mitigation strategy for the use of components with simple embedded devices can be applied to support embedded digital devices, since not even 'simple' devices can be excluded from a diversity analysis. **Proposed Change**: NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support obsolescence management strategies or new plant design and procurement strategies.	Y	The staff disagrees, in part, with the comment, but further clarification has been provided in the EDD RIS to remove any ambiguity. The RIS did not state that even simple devices can be excluded from a diversity analysis, only that it was not automatically excluded. Licensee should justify why the device is considered “simple” enough to exclude. Since it is difficult to define a “simple” component, the term has been removed in a revision of the referenced paragraph in the comment. Nevertheless, simplicity is still an important design measure. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This RIS cannot provide details on how to support obsolescence management strategies or new plant design and procurement strategies concerning equipment with EDDs, because it is not the function of a RIS to issue new regulations or guidance.
22	N14a	**Comment:** [Page 4, First Paragraph] The failure mode of excessive data rates, which could exceed the capacity of a communications link or the ability of nodes to handle	Y	The staff agrees with this comment. The additional proposed sentence has been added to the RIS.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		excessive traffic, has also been identified by the NRC staff in Digital Instrumentation and Controls DI&C-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms- communications Issues (HICRc), Interim Staff Guidance [ISG]." DI&C-ISG-04 should be referenced not just to identify the failure mode but to provide guidance for defenses against that failure mode. **Proposed Change:** The failure mode ... DI&C-ISG-04, "Task Working Group #4: Highly- Integrated Control Rooms-Communications Issues (HICRc), Interim Staff Guidance [ISG]." DI&C-ISG-04 provided guidance for defensive measures, such as separate communication processors and shared memory that prevent nodes on the communication network from being adversely effected by excessive data rates.		
23	N14b	**Comment:** [Page 4, Background Information Section] The Background on Page 4 (same statement in last year's draft) states in part: *"The regulations identified in each nuclear facility sector provide requirements for the process by which changes to a facility, procedure, or other controlling document may be made without prior NRC approval, except for 10 CFR Part 40 facilities (further discussed in the Fuel Cycle Facility Sector). Records of changes to the facility must be maintained. These records must include a written evaluation that provides the bases for the determination that the change, test, or experiment does not require prior NRC approval. The records of changes to the facility should show that <u>any potential safety issue from the use of embedded digital devices has been adequately addressed."</u>* **Proposed Change:** We are concerned that the highlighted statement represents a new NRC expectation under 10 CFR 70.72, "Facility Change and Change Process" and as such it should be deleted or clarified to the point of indicating that there is no new expectation.	N	The staff acknowledges the concern indicated in the "Proposed Change" and has provided clarification as follows. NRC is not setting any new expectations. This RIS reminds addressees of the need to identify, review, document, and control equipment with EDDs in safety-related systems to comply with applicable regulations for the nuclear facility. In the fuel facility sector, 10 CFR 70.72, "Facility change and change process" can be used to make changes to the site, structures, processes, systems, equipment, components, computer programs and activities of personnel without prior NRC approval when certain requirements are met. The RIS is making addressees aware that they may use the 10 CFR 70.72 process to make changes that involve EDDs contained in components in safety-related equipment in a facility while addressing and documenting the potential safety issues adequately.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
24	N15	**Comment:** [Page 5, Bullet List in Item 1 in Summary of Issue Section] Regulatory Guide 1.53, Revision 2, is missing from the list. The Regulatory Guide endorses IEEE Std 379-2000 without exception. The IEEE standard has relevant guidance for the treatment of CCFs. **Proposed Change:** NRC should add Regulatory Guide 1.53, Revision 2, to the list of applicable regulatory guidance.	Y	The staff agrees with the proposed change, and Regulatory Guide 1.53, Revision 2, has been added to the list of applicable regulatory guidance.
25	N16	**Comment:** [Page 6, Item 2] Title: *"The need to address potential vulnerabilities to CCFs"* This title implies the CCF will occur; therefore the emphasis is on coping. The emphasis should be on the assessment of the potential for the CCF to occur at all. **Proposed Change:** Change sentence to read as follows: "The need to conduct a CCF vulnerability assessment."	N	The staff disagrees that Item 2 implies the CCF will occur. The phrase mentions addressing potential vulnerabilities. The need to conduct a CCF vulnerability assessment is a part of the process to determine if there is a potential for a CCF in the DI&C design.
26	N17a	**Comment:** [Page 6, Last Paragraph] "It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function." Again, software CCF is being used incorrectly. This issue is not limited to execute features. **Proposed Change:** Suggested sentence change: "It may be possible that the intended safety protection could be defeated by a CCF of redundant safety divisions caused by a software defect within an embedded digital device, when the same device issued within those redundant divisions and the defect is triggered in multiple divisions. Such a software defect could prevent more than	Y	The staff agrees, in part, with the comment and the RIS has been revised similar to the proposed change as follows: The last two sentences in the last paragraph on Page 6 have been adjusted to read: “Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF).”

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e. a CCF)."		
27	N17b	**Comment:** [Page 6, Last paragraph] "It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function." "Software CCF" is used incorrectly. Not limited to execute features. Also, it is not clear what licensees are expected to do. The expectation needs to be well defined. **Proposed Change:** Another example of a suggested sentence change: "It may be possible that the intended safety protection could be defeated by a software defect within an embedded digital device when the same device is used within redundant safety system sense and command or execute features. Such a software defect could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e. a CCF)." "Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered in redundant divisions concurrently (i.e., causing a CCF). The CCF vulnerability assessment should also consider defects that may be triggered non-concurrently but remain undetectable; therefore allowing non-concurrent triggering to accumulate in multiple redundant divisions during that same time duration (i.e. again, causing a CCF). If a CCF vulnerability is concluded, then licensees should conduct a CCF coping analysis to demonstrate how plant safety is maintained during design basis accidents with the safety system CCF."	Y	The staff disagrees, in part, with the comment that "software CCF" is used incorrectly. The first sentence in the referenced paragraph in the comment discusses how the application of the regulations and guidance are relied on to assure the safety system sense and command features supply the logic signals to the execute features (assure no software CCF within redundant divisions of the sense and command features). The referenced sentence then discusses how the success of the protection against CCF, provided in the sense and command features, could still be defeated in the execute features. However, the RIS text of the reference sentence has been adjusted for clarification to avoid any ambiguity as follows: "Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD, when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF)." The referenced sentence in the comment is located under Item (2), "The need to address potential vulnerabilities to CCFs." This is followed by a list of applicable regulations and guidance that effectively provide the guidance suggested by the comment. Therefore, the staff did not follow the adjusted referenced sentence with further discussion.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
28	N18	**Comment:** [Pages 6 and 7, Second Paragraph in Item 2 in Summary of Issue Section] The pointer to BTP 7-19 for the treatment of potential CCFs reinforces the expectation that diversity is a necessary mitigation strategy for the use of embedded digital devices. BTP 7-19 describes "two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: Diversity or Testability." The Testability approach, where a "system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested)," is not a practical option for the types of equipment addressed in the RIS (i.e., such as motor controllers, sequencers, pumps, valve actuators, breakers, uninterruptable power supplies, emergency diesel generator controls, etc.), especially when the test cases must address internal states of the digital components, as has been the case for the more recent new plant reviews. ***Proposed Change:*** NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support obsolescence management strategies or new plant design and procurement strategies.	Y	The staff disagrees, in part, with the proposed change, but the RIS has been revised to further clarify how other preliminary options can be used to reduce the likelihood of EDD defects. A key concern with equipment with EDDs is the possibility that an undetected EDD defect may be concurrently triggered to cause the equipment to fail to function as intended in redundant, but otherwise independent systems potentially resulting in a CCF. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs in systems with equipment with EDDs located in safety-related systems, especially the sense and command functions. BTP 7-19 (Revision 6), Section B.1.9, explains that the application of many system design and testing attributes, procedures, and practices can help significantly reduce the probability of CCF. Two design attributes, either of which is sufficient to eliminate consideration of software based or software programmable logic based CCF are: sufficient diversity and (100%) testability. For testability, a system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested). Attempting to achieve 100% testing of equipment with EDDs is a high test bar, but there may be digital components now or in the future, that may be that simple, either with a reasonable number of inputs AND no intermediate states, perhaps a type of Field Programmable Gate Array (FPGA). Depending on certain factors as complexity, the risk significance of the system the components are in, knowledge of quality development, thorough testing, and a successful operational history, a licensee may be able to supply sufficient justification for a reasonable assurance of safety. This may be the case with non-nuclear industry developed commercial products even with EDDs. In “very low probability of CCF, but very high damage consequence” systems as nuclear power reactor protection systems, complexity may prevent software or logic from being reasonably assured to have “no hidden defect.” In such cases, diversity and defense-in-depth help reach a determination of reasonable assurance of safety. It is not the function of a RIS to provide solutions and/or new guidance for addressing the obsolescence management strategies or new plant design and procurement strategies.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
29	N19	**Comment:** [Pages 6 and 7, Third Paragraph in Item 2 in Summary of Issue Section] The discussion again broadens the underlying concern to non-safety equipment (see comment 2 above). As a result, the message is made ambiguous. The overall discussion does not answer the question on how NRC expects the industry needs to treat requirements for non-safety equipment that contain embedded digital components. **Proposed Change:** NRC should clarify the scope regarding non-safety components with embedded digital devices. The discussion of non-safety equipment should be deleted, since it is not governed by any specific regulation. In addition, the direction from the Commission in the Staff Requirements Memorandum to SECY-93-087 does not address non-safety digital components that are neither connected to nor can disable a safety system.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.” Also, the staff has deleted the first paragraph on Page 7 of the draft RIS that stated: "Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)."
30	N20	**Comment:** [Pages 6 and 7, Fourth Paragraph in Item 2 in Summary of Issue Section] The discussion of BTP 7-19 is limited to equipment performing safety-related system execute features; however, the guidance in BTP 7-19 is also relevant (to) equipment performing safety-related monitoring and display functions. **Proposed Change:** NRC should clarify expectations for the application of BTP 7-19 to monitoring and display functions.	Y	The staff agrees, in part, with this comment that further clarification would be helpful. On page 6 in Item 2 in Summary of Issue Section of the draft RIS for the Nuclear Reactor Sector, in a paragraph above the one mentioning BTP 7-19, it states, “Applicable regulations, guidance, and industry standards are relied on to assure the safety system sense and command features provide the logic signals to the safety system execute features. ”Figure 3” in IEEE Std. 603-1991 (incorporated by reference in 10 CFR 50.55a(a)(2) with the requirements statements in 10 CFR 50.55a(h)) indicates that the sense and command features include I&C equipment performing safety-related monitoring and display functions. While BTP 7-19 does not apply to all nuclear facilities, BTP 7-19 is one example of a guidance document that is relied upon to assure the safety system sense and command features provide the logic signals to the safety system execute features. However, to avoid any ambiguity in the RIS, the last paragraph in Item 2 in the Summary of Issues Section, Nuclear Reactor Sector, on Page 7 of the draft RIS has been revised to state, “In addition to the safety-related sense and command features, the guidance in BTP 7-19 is helpful when considering postulated CCFs in systems with components containing EDDs located in equipment performing safety-related system execute features.”

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
31	N21	***Comment:*** [Page 7, First Paragraph] *"Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)"* "beyond design basis of safety-related equipment" is confusing and irrelevant. Again, it is not clear what licensees are expected to do. The expectation needs to be well defined. **Proposed Change:** Revise to read as follows: "Consideration of CCF applies to equipment that is not safety-related to the extent that a software defect could create a transient that is unanalyzed in the plant's accident analysis. Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered for multiple control functions concurrently. For control functions that are in continuous use, the analysis should consider that a triggered defect may be self-announcing. Therefore, the defect may be correctable before it is triggered for multiple control functions (i.e. before it causes a CCF of multiple control functions). Therefore, the software defect may be correctable before it causes an unanalyzed transient."	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.” Also the staff has deleted the first paragraph on Page 7 of the draft RIS that stated: "Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)."
32	N22	**Comment:** [Fuel Cycle Facility Sector, Page 8, Line 3] The broad scoping language associated with the definition of safety related as it applies to Fuel Cycle Facilities is problematic. Identification of clearly defined consequences of concern for Fuel Cycle Facilities is needed to risk-inform the identification of the components and systems that need adequate protection from cyber-attacks.	N	The staff disagrees with the comment. The definition of the term “safety related” on page 8 of the draft RIS applies only to safety applications in fuel cycle facilities for systems and components with EDDs. NRC is issuing this RIS to clarify the NRC’s technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with EDDs. Common defense and security applications are excluded from the scope of this RIS. Therefore, systems and components for protection from cyber-attacks are not considered.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: NRC has a decision-making framework (SECY-04-0222) which could be used to establish these consequences of concern to assure public health and safety as well as common defense and security.		As a result of other comments, the "Intent" section of the RIS now states: "Regulatory issues associated with equipment with EDDs related to common defense and security under 10 CFR Part 73, 'Physical Protection of Plants and Materials,' and 10 CFR Part 74, 'Material Control and Accounting of Special Nuclear Material,' are beyond the scope of this RIS."
33	N23	**Comment:** [Page 9, Fuel Cycle Section] The fuel cycle section on Page 9 states in part: (1) The need to ensure adequate quality and reliability of embedded digital devices that exist in **actuation equipment** Regulations and review guidance focus on safety-related system control and protection logic rather than the actuated device; Digital technology is being introduced into actuation and actuated equipment. Examples include motor controllers, pumps, valve actuators, breakers, Uninterruptible power supplies, and emergency diesel generator controls (if applicable). In many instances, equipment consisting of older non-digital technology is being replaced with commercially procured products containing embedded digital devices that include software, software-developed firmware, or software- developed logic that may not have been developed in accordance with guidance and acceptable industry standards. **Proposed Change:** The term "actuation equipment" is not used at or relevant to FCFs thus it appears to be reactor-centric. NRC should delete this section or clarify its intent.	N	The staff disagrees with the comment. The term "actuation equipment" is used in the FCFs industry, and is not unique to reactors only. FCFs may incorporate in their design and operation actuation equipment such as motor controllers, circuit breakers, emergency diesel generator controls, etc. The actuation equipment provides actuating signals to the actuated equipment such as motors, valves, diesel generators, etc. This RIS reminds licensees to ensure adequate quality and reliability of embedded digital devices that may exist in actuation equipment as well as the actuated equipment.
34	N24	**Comment:** [Page 10, Fuel Cycle Section] The fuel cycle section on Page 10 states in part: (3) The need to ensure sufficient procurement planning and material control to identify, review, test, and control embedded digital devices	N	The staff disagrees with the comment. The highlighted concepts are not new expectations or regulatory requirements. The NRC's intent in issuing this RIS is to heighten awareness about EDDs that may exist in procured equipment used in safety-related systems without the devices having been explicitly identified in procurement documentation. FCFs may implement control systems that make use of digital technology with EDDs. Identification, review, documentation, and control of safety-related equipment with EDDs are

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Licensees should include, as part of their specifications for vendors supplying commercial products, requirements to identify the use of embedded digital devices and to sufficiently document the quality of the embedded digital devices to support the licensee's specific quality verification process (e.g., commercial grade dedication, management measures). In the early stages of design, vendors, licensees, and applicants should fully understand the challenges that embedded digital devices may pose. Procurement activities, including commercial grade item dedication processes and product testing and inspection, should be sufficient to ensure adequate quality and to prevent the introduction of components that could degrade system reliability. Where there is a strong reliance on functional testing to verify component quality, performance, and reliability, such testing should enable identification of product deficiencies. Licensee monitoring of components with embedded digital devices should support the documentation of item failures in order to aid in the identification of specific devices and vendors of suspect quality. **Proposed Change:** Several of the highlighted concepts appear to be new NRC expectations that warrant, at minimum, discussion with industry to better understand NRC's basis and intent.		necessary to demonstrate quality and reliability. The demonstration should address material control, development process, and equipment qualification.
35	A1	**Comment:** [Page 1, Intent, Second paragraph] "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems. Although this RIS excludes systems that are not safety- related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a non-safety system that, if inadequately addressed, could adversely affect safety." Saying this RIS excludes systems that are not safety related and then saying this RIS identifies considerations for non-safety is very ambiguous. The RIS provides	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		information only, and that information is pertinent to both safety and non-safety. **Proposed Change:** This RIS identifies considerations for both safety and non-safety systems. I have only corrected this one sentence. Sentences throughout the document should be changed to address both safety and non-safety systems, as applicable. Alternately, delete all discussion of non-safety applications, and address them in a separate RIS.		
36	A2	**Comment:** [Page 1, Intent, Second paragraph] "For example, a software common cause failure (CCF) in redundant non-safety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses." The words "software common cause failure" are being used incorrectly. Software defects may result in CCF. "Redundant" is an irrelevant attribute. The more important concern is that a design defect may effect multiple non-safety systems. "Important to safety" is an undefined term. "Beyond the design basis of safety related systems" is confusing when discussing no safety systems and is irrelevant; the key point is that the condition is not analyzed. **Proposed Change:** For example, a software defect in one or more non-safety controllers might create a common cause failure (CCF) of multiple non-safety control functions that has not been analyzed in the nuclear facility's transient and accident analyses. This concern is pertinent to non-safety systems that can directly initiate plant transients. These systems are often referred to as control systems "important to safety"; they are the systems described in Chapter 7 of the plant's UFSAR.	Y	The staff agrees, in part, with the comment. The RIS is being revised to avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems." The RIS has been adjusted to reflect the proper context of the term CCF. The staff disagrees that "redundant" is an irrelevant term. It is a term well understood and used in guidance documents. It is commonly used to describe identical equipment executing the same software in otherwise independent trains or divisions. It can also be used to describe duplicate channels within a division used to avoid a spurious trip signal. It can apply to both safety-related as well as non-safety systems. Yes, it is also possible that a defect in a specific EDD used in a similar component in multiple pieces of equipment in different systems within the same division or various equipment using the same EDD in different non-safety trains could be affected. However, the NRC would expect that the probability of the defect being triggered concurrently in diverse equipment performing different functions is significantly less than in the case of redundant or identical systems because of the increased diversity.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
37	A3	**Comment:** [Page 2, Third Paragraph] "Addressees should be aware of any potential vulnerability that could result from a postulated software common-cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices, which includes components implementing safety-related execute features (e.g., motor control centers, actuated equipment)." The use of CCF is incorrect. We postulate a defect, which may cause a CCF triggered concurrently in multiple systems. We do not postulate a CCF. The concern is not limited to execute features, it applies also to sense and command features (e.g., digital transmitters). Diversity is not the only defense against CCF. Other defenses are addressed below (e.g., simplicity, non-concurrent triggers). **Proposed Change:** Addressees should be aware of any potential CCF of redundant safety related equipment that could result from a postulated software defect within embedded digital devices, which includes components implementing safety-related sense and command or execute features (e.g., instrumentation, motor control centers, actuated equipment)	Y	The staff agrees, in part, with the comment. The RIS text has been revised in several places to reflect that it is a postulated undetected EDD defect that may cause the equipment with this EDD to fail to accomplish its safety function and when triggered concurrently in redundant equipment may result in a potential CCF. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices and a thorough test program to prevent EDD defects and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This may be the situation in many commercial equipment units and components containing EDDs where the development process is either not of the same quality as required by the NRC regulations and recommended by guidance, if applicable, different but equivalent, or unknown.
38	A4	**Comment:** [Page 2, fourth paragraph]: "Inadequate consideration of these devices in diversity assessments to address potential software CCFs could lead to an adverse safety consequence." We don't do diversity assessments. In accordance with BTP 7-19 we do CCF vulnerability assessments. Diversity is just one defense against CCF; it is not the only defense. Other defenses are addressed below. **Proposed Change:** Inadequate consideration of these devices in CCF vulnerability assessments could lead to an adverse safety consequence.	Y	The staff agrees, in part, with the comment and has adjusted the RIS to use the term "CCF vulnerability assessments" instead of "diversity assessments" as recommended. The staff also agrees that diversity is not the only defense against CCF. For designs that use DI&C in safety systems, the NRC has established a four point position on D3 for new reactor designs and for digital system modifications to operating plants in the SRM to SECY 93-087. Point 1 states, "The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to CCF have been adequately addressed." Diversity is usually considered one of the final and most important defensive barriers to preventing a CCF.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		"Assessment of diversity" should be changed to "CCF vulnerability assessment" throughout this document.		Despite many good design measures and practices, quality software development, and testing, a significant increase in complexity and a decrease in favorable measures that detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. Where that is the case, there is still a concern that an undetected EDD design error combined with an initiating event (concurrently triggered) could disable significant portions of the multi-division automated safety systems. Thus, diversity is usually considered one of the final and most important defensive barriers to preventing a potential CCF.
39	A5	**Comment:** [Page 2, last paragraph]: " ...that requires the use of software, software-developed firmware, or software-developed logic and that is integrated into equipment to implement one or more system safety functions." All logic is developed using software, even conventional logic. Clarify applicability to "programmable logic". **Proposed Change: "**... that requires the use of software, software- developed firmware, or software-developed programmable logic that is integrated into equipment to implement one or more system safety functions." "logic" should be changed to "programmable logic" throughout this document.	Y	The staff agrees with this comment. The proposed change now states, "... that requires the use of software, software-developed firmware, or software-developed programmable logic that is integrated into equipment to implement one or more system safety functions."
40	A6	**Comment:** [Page 3**,** Second paragraph]: The firmware of an embedded digital device may provide limited functionality with a well-documented design basis such that the embedded digital device could be characterized as "simple." Defining "simple" as "limited functionality with a well-documented design basis" is quite different than BTP 7-19 which defines "simple" as 100% testable including all combinations of input states and internal states. This will cause confusion in the industry. Add "concurrent triggers" as another consideration. These are all defenses against CCF.	Y	The staff agrees, in part, with the comment. Since it is difficult to define a "simple" component, the RIS has been revised to remove the use of the term "simple" and adjust the RIS to reflect the concepts of the comment and proposed change. However, simplicity is an important defensive design measure. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering potential postulated CCFs in systems with equipment with EDDs located in safety-related system. BTP 7-19 (Revision 6), Section B.1.9, explains that the application of many system design and testing attributes, procedures, and practices can help significantly reduce the probability of CCF. Two design attributes, either of which is sufficient to eliminate consideration of software based or software programmable logic based CCF are: sufficient diversity and (100%) testability. For testability, a system is sufficiently simple such that every possible

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: The NRC staff provides guidance applicable to components containing software, firmware, and programmable logic developed from software-based development systems. NRC staff guidance does not automatically exclude the application of these embedded digital devices from consideration within CCF vulnerability assessments. Simplicity, diversity, design documentation, quality development, testing, operational history and the potential for concurrent defect triggers are some of the important factors to be considered within CCF vulnerability analyses to evaluate the suitability for use of an embedded digital device.		combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested). Generally, it is thought this is not achievable either due to the internal memory states or too many input combinations to be tested in a reasonable period of time. It is a high test bar, but there may be digital components now or in the future, that may be that simple, either with a reasonable number of inputs AND no intermediate states, perhaps a type of FPGA. The RIS now states: "This RIS identifies regulations and guidance for identifying and eliminating defects. The NRC does not automatically exclude any equipment with EDD, even those of limited functionality with a well-documented design, from consideration in CCF vulnerability assessments; instead, justification should be supplied by the licensee as applicable for the specific nuclear facility and application."
41	A7	**Comment:** [Page 4, Paragraph 1] "The failure mode of excessive data rates, which could exceed the capacity of a communications link or the ability of nodes to handle excessive traffic, has also been identified by the NRC staff in Digital Instrumentation and Controls (DI&C)-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc), Interim Staff Guidance [ISG]." ISG-04 should be referenced not just to identify the failure mode but to provide guidance for defenses against that failure mode. **Proposed Change:** The failure mode ... (DI&C)-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc), Interim Staff Guidance [ISG]." ISG-04 provides guidance for defensive measures, such as separate communication processors and shared memory, that prevent nodes on the communication network from being adversely effected by excessive data rates.	Y	The NRC staff agrees with this comment. The additional proposed sentence has been added to the RIS.
42	A8	**Comment:** [Page 6, last paragraph] "It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within	Y	The staff agrees, in part, with the comment and further clarification is needed. The last two sentences in the last paragraph on Page 6 have been adjusted to read:

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function." Again, software CCF is being used incorrectly. This issue is not limited to execute features. **Proposed Change:** It may be possible that the intended safety protection could be defeated by a CCF of redundant safety divisions caused by a software defect within an embedded digital device, when the same device is used within those redundant divisions and the defect is triggered in multiple divisions. Such a software defect could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e. a CCF).		"Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD, when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF)."
43	A9	**Comment:** [Page 6, Item 2 Title] "The need to address potential vulnerabilities to CCFs" This title implies the CCF will occur, therefore the emphasis is on coping. The emphasis should be on the assessment of the potential for the CCF to occur at all. **Proposed Change:** The need to conduct a CCF vulnerability assessment.	N	The staff disagrees with this comment that the title implies the CCF will occur. The referenced sentence states, "The need to address potential vulnerabilities to CCFs." For designs that use digital I&C in safety systems, the NRC has established a four point position on D3 for new reactor designs and for digital system modifications to operating plants in the SRM to SECY 93-087. Point 1 states, "The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to CCF have been adequately addressed."
44	A10	**Comment:** [Page 6,Last paragraph] "It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function." "Software CCF" is used incorrectly. Not limited to execute features.	Y	The staff agrees, in part, with the comment and that further clarification is needed in the text. The last two sentences in the last paragraph on Page 6 have been adjusted to read: "Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD, when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF)."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Also, it is not clear what licensees are expected to do. The expectation needs to be well defined. **Proposed Change:** It may be possible that the intended safety protection could be defeated by a software defect within an embedded digital device when the same device is used within redundant safety system sense and command or execute features. Such a software defect could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF). Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered in redundant divisions concurrently (i.e., causing a CCF). The CCF vulnerability assessment should also consider defects that may be triggered non-concurrently but remain undetectable; therefore allowing non- concurrent triggering to accumulate in multiple redundant divisions during that same time duration (i.e., again, causing a CCF). If a CCF vulnerability is concluded, then licensees should conduct a CCF coping analysis to demonstrate how plant safety is maintained during design basis accidents with the safety system CCF.		
45	A11	**Comment:** [Page 7, First paragraph]: “Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design- basis accident analysis and a safety vulnerability results with respect to a radiological release).” "beyond design basis of safety-related equipment" is confusing and irrelevant. Again, it is not clear what licensees are expected to do. The expectation needs to be well defined.	Y	The staff agrees, in part, with the comment. However, as a result of other comments concerning avoiding any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment, the second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.” Also the referenced paragraph (first paragraph on Page 7) has been deleted.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: Consideration of CCF applies to equipment that is not safety-related to the extent that a software defect could create a transient that is unanalyzed in the plant's accident analysis. Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered for multiple control functions concurrently. For control functions that are in continuous use, the analysis should consider that a triggered defect may be self-announcing. Therefore, the defect may be correctable before it is triggered for multiple control functions (i.e. before it causes a CCF of multiple control functions). Therefore, the software defect may be correctable before it causes an unanalyzed transient.		
46	E1	**Comment:** [General] The draft RIS seems appropriate and helpful in calling attention to embedded digital devices in plant equipment and their potential for creating undesired behaviors, including common-cause failures (CCF). However, it seems to be overly reliant on diversity as a protective measure against CCF. It does not mention other protective measures that may be more appropriate and effective for embedded digital devices. As written, the guidance could lead to greater use of less-than-optimal approaches for protecting against CCF in embedded devices, with attendant adverse effects on safety. However, relatively minor changes could help remedy the situation. **Proposed Change:** However, relatively minor changes could help remedy the situation.	Y	The staff disagrees, in part, with the comment that the RIS is overly reliant on diversity as a protective measure against CCF. However, the staff agrees additional clarification would be helpful. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy, is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety.
47	E2	**Comment:** [Page 2, third paragraph, third sentence] The statement seems to assume that non-diverse components have a significant likelihood of CCF and diverse components do not. Neither is necessarily true. There is no guarantee that diverse components performing the same function won't both be vulnerable to potential triggers of software faults (for example, Y2K, out	Y	The staff agrees, in part, with this comment that emphasis should be on reasonable assurance of adequate protection against CCF. It is not a matter of components being diverse or non-diverse, but are the systems sufficiently diverse to still accomplish their intended safety function considering a credible postulated CCF resulting from an undetected EDD defect concurrently triggered to cause the failure of redundant, but otherwise independent equipment. While there may be a potential for non-hardware related and

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		of range inputs, invalid timing signals, network communication disturbances, etc.). The emphasis should not be on ensuring diversity, but on ensuring reasonable assurance of adequate protection against CCF. CCF protection would probably consist of some combination of preventive design measures (possibly including internal diversity), that preclude certain types of CCFs by avoiding triggers that might activate them, and mitigation measures that enable the plant to cope with such failures. **Proposed Change:** An alternative statement that might be better is: Addressees should be aware that embedded digital devices in redundant safety-related components (including components implementing safety-related execute features such as motor control centers and actuated equipment) could introduce potential for common-cause failure (CCF) due to designed-in software faults or defects.		non-software related faults that may lead to a common cause failure, this RIS is associated with potential CCF due to EDDs defects such as software defects. EDD defects include failures of the specifications to properly represent the process and environment (e.g., would include faults as Y2K, out of range inputs, etc.) not just errors the programmer made in the code. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. Since the phrase “components using non-diverse embedded digital devices” may give a misimpression, the sentence referred to in the comment has been revised for clarity. The suggested adjective “designed-in” is not included, because it could be misinterpreted as defects deliberately added.
48	E3	**Comment:** [Page 2, fourth paragraph, second sentence] This statement appears to assume that diversity is the one and only way to protect against CCF. Again, the assessment should be about protection against CCF - not just diversity. **Proposed Change:** An alternative statement that might be better is: Inadequate consideration of these devices in assessing susceptibility to potential software CCFs could lead to an adverse safety consequence.	Y	The staff agrees, in part, with the comment that protection should be against CCF. While BTP 7-19 does not apply to all nuclear facilities, it does provide helpful guidance. The foundation of BTP 7-19, Revision 6, is the four point “NRC position on D3” quoted in BTP 7-19. Point 1 (Item 1) states, “The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.” The referenced sentence in the comment has been revised to reflect the comment and state: “Inadequate consideration of these devices in the use of digital technology in system upgrades, component replacements, and new equipment applications could lead to an adverse safety consequence.” An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety.
49	E4	**Comment:** [Page 3, second full paragraph, third sentence] Again, the RIS seems to assume that diversity is the one and only way to protect against CCF. **Proposed Change:** An alternative statement that might be better is: However, NRC staff guidance does not automatically exclude the application of these (so-called "simple') devices containing the firmware from consideration within an assessment of vulnerabilities to potential CCF.	Y	The staff disagrees, in part, with the comment that the RIS assumes that diversity is the one and only way to protect against CCF. The staff does agree further clarification is needed to remove any ambiguity and will adjust the RIS accordingly. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. The referenced sentence in the RIS text has been revised to reflect this and similar comments as follows: “NRC staff guidance does not automatically exclude any equipment with EDDs, even those of limited functionality with a well-documented design, from consideration in CCF vulnerability assessments; instead justification should be provided by the licensee as applicable for the specific nuclear facility and application.”
50	E5	**Comment:** Page 3, second full paragraph, fourth sentence] Design measures that preclude or reduce the likelihood of various types of failures and CCFs should be added to this	Y	The staff agrees, in part, with the comment that the first defense against postulated EDD defects that potentially could result in various failures and CCFs is a quality design development process with appropriate defensive

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		list. Good process attributes (e.g., design documentation, quality development, testing, etc.) do not ensure a good design. Simplicity is good in that it makes it easier to anticipate undesired behaviors and failure modes and achieve more complete test coverage. Diversity can be helpful in either preventing or mitigating certain types of CCFs, but it increases complexity, and is not always appropriate. For example, diversity among redundant divisions that all have the same functional requirements does not protect against CCFs that originate in requirements specification faults (which various researchers have concluded is the most likely place to introduce a fault in a high integrity system). And there is no guarantee that such diverse systems will not be susceptible to the same stressors (for example, Y2K or out of range data or an invalid timing signal). Diversity should be encouraged where it makes sense, but not mandated, and the RIS should also encourage use of good design features (for example, data validation, watchdog timers, cyclic software architecture with no branching, invariance with respect to plant transients, etc.), which greatly reduce the likelihood of software-related failures and arguably can provide simpler solutions and greater assurance of adequate protection against failures and CCFs. **Proposed Change:** An alternative statement that might be better is: Nevertheless, several potentially important factors may be considered within a CCF assessment to evaluate the suitability for use of an embedded digital device, including: • simplicity • design features and measures that preclude or reduce the likelihood of failures and CCFs • diversity • design documentation • quality development • testing • operational history		design measures and thorough testing that can preclude or reduce the likelihood of the occurrence of EDD defects such as latent software defects. However, EDD defects include more than just programmer errors. They also include specifications errors and omissions that cause the hardware and software in some way to not accurately reflect the environment and process. The RIS has been adjusted to further clarify this point and reflect the proposed additions. Several potentially important factors provided by NRC regulations and guidance and industry standards should be considered in CCF assessments to evaluate the suitability for use of equipment with EDDs. These include: defense-in-depth and diversity, determinism, redundancy, independence, design documentation, a quality development process, thorough testing, failure mode and hazards analysis, operational history, and defensive design features and measures that preclude or reduce the likelihood of failures and CCFs, and achieve a degree of immunity from potential concurrent defect triggers. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors, may mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This may be the situation in many commercial units of equipment with EDDs where the development process is either not of the same quality required by the NRC regulations and recommended by guidance, as applicable, different but equivalent, or unknown.
51	E6	**Comment:** [Page 3, last paragraph]	N	The NRC staff agrees, in part, with this comment.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		The example of IN 2007-015 seems out of place in this RIS. While this is a good example of a CCF vulnerability introduced by digital equipment, it really is about the use of shared resources, not embedded digital devices. It is also a good example of a case where design measures that protect against broadcast storms, or segmentation of the I&C architecture to limit the extent of a **failure,** are the appropriate protective measures for CCF- not diversity. **Proposed Change:** One alternative is to simply delete this example. Another is to leave it in and use it to explain that diversity is not the only way to protect against CCF and that preventive measures against CCF can be implemented outside the digital components that might be affected by the CCF.		Although the broadcast storm described in IN 2007-15 is not directly related to failures of EDDs, these events highlight the need for licensees and applicants to understand that digital systems may have different failure modes than analog systems. The staff agrees that diversity is not the only way to prevent CCF. However, the root cause of this event was not due to a CCF failure of redundant components. This event was caused by a single component failing and sending excessive data to a network.
52	E7	**Comment:** [Page 6, Section (2)] If BTP 7-19 is applied to embedded devices as written, it might force the use of diversity as the only practicable way to meet the guidance (100% testability is rarely a viable option for digital devices, and demonstrating CCF coping capability per the BTP might not always be possible). This could effectively force the use of diversity in the components that contain the embedded devices, which would further complicate training and maintenance concerns. It is not clear whether the net effect on safety would be positive. Perhaps a supporting analysis, including cost-benefit considerations would be helpful. **Proposed Change:** If BTP-19 is not going to be revised, and its guidance is intended to be applied to embedded systems, then some additional guidance should be provided on the need to consider cost-benefit and the net effect on safety of using diverse components rather than simplicity and other preventive design measures to address CCF concerns.	N	The staff disagrees, in part, with this comment. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs. BTP 7-19 (Revision 6), Section B.1.9, explains that the application of many system design and testing attributes, procedures, and practices can help significantly reduce the probability of CCF. Two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF are: diversity and testability. For testability, a system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case (100% tested). Generally, with regard to 100% testing of all inputs and system states, this option, in effect, may or may not be a viable or attainable option depending on the component design. It is a high test bar, but there may be digital components now or in the future, that may be that simple, either with a reasonable number of inputs AND no intermediate states, perhaps a type of FPGA. However, in most cases it may be easier to achieve sufficient diversity. Crediting operator responses to design basis events when sufficient time is available to the operator is an option, as is the use of non-safety systems to mitigate events. Experience has shown that there are only a few design basis accidents that could require an automated diverse actuation system to mitigate (e.g., large break loss of coolant accidents requiring a low pressure injection system actuation). Consequently, the need for automated diverse actuation systems is thought to be relatively minor and infrequent.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				Simplicity and other preventative design measures may not be an option when components are already embedded in systems, as simplicity and defensive measures are implemented in the life cycle development phases; whereas the scope of this RIS applies to the operations and maintenance life cycle phase. It is at this point that diversity may become a primary defensive measure against a CCF. A cost/benefit analysis criterion addressing potential common cause failures currently is not available in BTP 7-19, and might not be considered for implementation in future revisions of BTP 7-19, as the acceptance criteria for simplicity, while feasible, may be unattainable for nuclear industry digital systems. For example, the goal value for one complexity metric that evaluates paths and junctions in code suggests, as a rule of thumb, that a value of 10 is the maximum value that should be allowed; whereas some function blocks in an embedded device's logic may have metric values exceeding 100. A simplicity acceptance criterion could prove to be more of a hindrance than a help in these cases.
53	E8	**Comment:** [Page 7, second paragraph] BTP-19 is limited in that it recognizes only 100% testability and diversity as evidence of adequate preventive measures for CCF. (It also allows for a demonstration of coping capability as evidence of adequate CCF protection). However, it does not consider defensive design measures and other metrics for simplicity, which may be more appropriate and effective CCF protection solutions for embedded equipment. **Proposed Change:** This endorsement of BTP-19 should probably be tempered until BTP-19 is revised. An alternative statement that might be better is: The guidance in BTP 7-19 describes some approaches for addressing potential CCFs of embedded digital devices located in equipment performing safety-related system execute features.	N	The staff disagrees with the proposed changed. While incorporating criteria for defensive design measures and metrics for simplicity in BTP 7-19 is laudable, specific, objective criteria have yet to be accepted by the NRC. Therefore, the suggested alternative statement would not be accurate in that it implies alternative NRC acceptance criteria for common cause failure mitigation are presently available. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering potential postulated CCFs in systems with equipment with EDDs located in safety-related system. Further, BTP 7-19 acknowledges system design attributes, complete testing, good procedures and practices can contribute to significantly reducing the probability of CCF. System design attributes, good procedures, and practices include defensive design measures and other metrics as simplicity. BTP 7-19 states there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: sufficient diversity or 100% testability. For testability, a system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested). Generally, it is thought this is not achievable either due to the internal memory states or too many input combinations to be tested in a reasonable period of time. It is a high test bar, but there may be digital components now or in the future, that may be that simple, either with a reasonable number of

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				inputs AND no intermediate states, perhaps a type of FPGA. It may be easier to achieve sufficient diversity. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors, could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCFs and support reaching a reasonable assurance of safety.
54	E9	**Comment:** [Page 1, Intent, second paragraph and page 7. "Summary of Issue" section 2] This RIS is limited to safety related equipment. However, there is extensive discussion of non-safety CCF within the "Intent" section and Summary of Issue" section that will lead to some confusion and possibly the incorrect assumption that safety related requirements must be applied to non-safety equipment. Of particular concern is the scope of the second point: "the need to address potential facility vulnerabilities to CCFs", as this should be applicable only to CCF of safety-related equipment. **Proposed Change:** Discussion of non-safety CCF is out of scope for this RIS and should be removed to: 1. Provide better clarity and focus of the stated scope and intent of the RIS. 2. Reduce confusion and enhance implementation of the RIS The discussion of non-safety CCF is better discussed in other products	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.” Also, the staff has deleted the first paragraph on Page 7 that stated: "Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)"
55	E10	**Comment:** [Page 2 and 3, definition of "embedded digital device"] The definition and extended list of technology (ASIC, etc.) has become overly broad and ambiguous. The full definition of "software- developed firmware" and "software-developed logic" needs additional definition. The inclusion of various host technologies would include nearly all electronics, analog or digital. Workable definitions that define the scope of the RIS more deterministically is recommended as the current definition will hinder RIS implementation.	N	The staff disagrees with the suggested change. The purpose of the RIS is to address EDDs, not just devices that are microprocessor-based. The key point is EDDs generally require software, firmware, or software developed programmable logic.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: Refine the definitions to deterministically exclude electronic circuitry that does not include a load, store, execute architecture or working memory. Structure the definition to differentiate the means of execution from the means of program storage.		
56	F1	**Comment:** [General Comment] The RIS provides a very wide interpretation of the function and use of embedded digital devices. This leaves the position of the NRC up for continuous interpretation and revision. The INTENT Section stated is to provide a "technical" position on existing regulatory requirements. **Proposed Change:** The RIS should provide clear technical positions that may be used by the industry. General references to other industry documents or Regulatory Guides should be specific.	N	The staff disagrees, in part, with the comment. The staff agrees that the RIS provides a very wide interpretation of the function and use of EDDs. In fact, the use of EDDs is widespread. The staff believes the RIS does refer to existing regulatory and guidance documents. The RIS separately discusses the nuclear reactors and the fuel cycle facilities in two different sectors. The RIS categorized the potential safety concerns into three points under each sector and then references specific regulations and guidance that are applicable under each point. The NRC's intent in issuing this EDD RIS is to heighten awareness that EDDs may exist in procured equipment used in safety-related systems without the devices having been explicitly identified by the vendor. This particularly may be the case for non-nuclear industry developed equipment used in the execute features (e.g., motor control centers). The RIS has been adjusted for clarity by further grouping the regulations and guidance for non-power reactors separately from those for power reactors in the nuclear reactor sector.
57	F2	**Comment:** [INTENT] The RIS indicates that it applies only to I&C in safety related systems and then later describes embedded digital devices used in Electrical systems for power distribution which are typically not I&C systems. **Proposed Change:** A clear scope is needed for this RIS.	N	The staff disagrees that further clarification is needed for the scope of the RIS. The first sentence of the second paragraph of the INTENT section of the draft RIS stated: "The scope of this RIS is limited to equipment, **including** instrumentation and controls (I&C), in safety-related systems."
58	F3	**Comment:** [INTENT] The RIS states that it is limited to Safety Related systems and then in the next sentence states that it applies to embedded systems in non-safety systems. **Proposed Change:** Any reference to non-safety systems should be eliminated throughout the RIS.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
59	F4	**Comment:** [General Comment] This RIS appears to be focused on Software Common Cause Failure (SCCF) and does not address more generic common cause failures (CCF) that would be part of a Common Cause Analysis (CCA). While a software failure may be the cause of a CCF, there are other systematic failures which manifest themselves as software failures but are caused by expected external events such as lightning, EMI, RFI, etc. **Proposed Change:** The RIS should approach this subject from a CCA perspective vice drilling down on one part of a CCA which is represented by the SCCF. SCCF are those failures where the causal factor is the software (functional requirement failure, hardware failure, human coding errors, etc.) vice conditions where the software may be damaged or corrupted by external events. A CCA would better serve the industry vice only evaluating a SCCF.	N	The staff disagrees, in part, with the comment. The RIS: (1) addresses in general the prevention of CCF resulting from undetected EDD defects including latent software defects, (2) specifically mentions additional problems with EDDs related to EMC, and (3) defines EDD defects to include more than just programmer errors. They also include specifications errors and omissions that cause the EDD logic in some way to not accurately reflect the environment and process. As stated in the 6th paragraph, the intent of this RIS is to heighten awareness of the existence of EDDs and associated potential hazards. The RIS highlighted one of the potential hazards of software CCF. It is not the function of a RIS to provide any solutions and/or new guidance for addressing the hazards that may be created by EDDs. The need for additional guidance for safe use of EDDs in critical applications is being addressed separately. The staff agrees that there are other hazards that must be considered in EDD applications. These hazards will be considered in guidance on dealing with EDDs. For example EPRI is developing digital CCF guidance that will apply to EDDs.
60	F5	**Comment:** [Background Information] NRC guidance from BTP 7-19 does not provide any reference to embedded digital devices. **Proposed Change:** A reference should be provided that supports the RIS position on embedded digital devices.	N	The staff disagrees with the comment. The staff believes that BTP 7-19 provides guidance relevant to the EDDs issue. A key concern with components with EDDs is the possibility that an undetected EDD defect such as a latent software error within the firmware of an EDD may be triggered to cause the equipment with the EDD to fail to function as intended. If this defective software is triggered to cause the failure of redundant safety-related equipment in otherwise independent divisions or trains, a CCF may be created. BTP 7-19 specifically provides guidance on addressing assessment of vulnerabilities to CCF regardless of whether it is a microprocessor or equipment with EDDs.
61	F6	**Comment:** [Page 1, Section INTENT, 2nd Paragraph] By title, the RIS is applicable to safety-related systems. The statements within this paragraph expand the scope to include non-safety-related systems. **Proposed Change:** Other than the first sentence, consider deleting the entire paragraph.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
62	F7	**Comment:** [Page 2, Section BACKGROUND INFORMATION, 1st paragraph] (a) Consider expanding the 1st sentence to add perspective to this background statement (b) The 3rd sentence does not add perspective to this paragraph and should be deleted. **Proposed Change:** (a) "... and fluid systems) in response to increasing obsolescence and age-related failures or where analog spare parts are neither available nor can they be substituted." (b) Consider deleting the 3rd sentence in its entirety	Y	The staff agrees, in part, with the comment. The RIS has been adjusted to create a separate paragraph that emphasizes that the NRC understands licensees may use digital technology with the intent to achieve the potential benefits of digital I&C This includes help with obsolescence issues and the potential enhancement in overall nuclear facility operation and reliability. The staff disagrees that the third sentence should be deleted, because it expands on the increased use of digital technology with examples of specific equipment other than the typical control room I&C. The "3rd sentence" referenced in the comment has been modified to add clarity: "In addition to instrumentation and controls, examples of safety related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources."
63	F8	**Comment:** [Page 2, Section BACKGROUND INFORMATION, 2nd paragraph, (ends on the top of Page 3)] The definition appears too broad and includes, to a large extent, digital devices that are already enveloped within Regulatory and industry guides and standards. The definition should be narrowed to those devices within the RIS target population of concern. **Proposed Change:** Consider revising the paragraph in its entirety to the following: "For purposes of this RIS, an embedded digital device is a stand-alone or actuation device (that is not thought of as a computer}, but contains embedded software written to control that stand-alone or actuation device, where the software performs one or more functions that is specialized for the particular device that it runs on, along with time and memory constraints. [NOTE: Embedded software in this case should not be used interchangeably with firmware because firmware can be applied to ROM-based code on a computer, on top of which the OS runs, whereas embedded software is the only software on the device]"	N	The staff disagrees with the suggested change. Even though some digital devices may be enveloped within regulations and industry guides and standards, the purpose of this RIS is to heighten awareness that EDDs may exist in procured equipment used in safety-related systems without the devices having been explicitly identified by the vendor. This particularly may be the case for non-nuclear industry developed equipment used in the execute features (e.g., motor control centers). The staff recognizes that in general, the data communication systems and certain other nuclear facility equipment from the actuated equipment or execute features (e.g., motor control centers) and commonly used unit components from the sense and command features (e.g., transmitters, meters, and other indicating units), may be designed as non-nuclear industry commercial products with EDDs.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
64	F9	**Comment:** [Page 3, Section BACKGROUND INFORMATION, 3nd paragraph] The statements made in this paragraph are challenging for two reasons: (1) BTP 7-19 makes no direct reference to embedded digital devices; and, (2) BTP 7-19 criteria is intended for regulatory guidance only and not as criteria for industry use when implementing digital upgrades. (Reference: NRC Letter, Dated August 12, 2013 to the Shearon Harris Nuclear Power Plant, Titled: Shearon Harris Nuclear Power Plant Unit 1 - NRC Evaluation of Changes, Tests, and Experiments and Permanent Plant Modifications Baseline Inspection Follow-up Report 05000400/2013009. **Proposed Change:** Consider deleting paragraph in its entirety.	N	The staff disagrees with the comment. While BTP 7-19 does not mention EDDs directly, the staff believes that BTP 7-19 provides guidance relevant to the EDDs issue. A key concern with equipment with EDDs is the possibility that an undetected EDD defect such as a latent software defect within the firmware of an EDD may be triggered to cause the equipment with that EDD to fail to function as intended. If this software defect is triggered to cause the failure of redundant equipment, in otherwise independent divisions or trains, a CCF may be created. BTP 7-19 specifically provides guidance on addressing assessment of vulnerabilities to postulated CCF regardless of whether it is a microprocessor or equipment with EDDs. The staff agrees that the primary function of BTP 7-19 is guidance to the NRC staff. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering postulated CCFs in systems with equipment with EDDs located in safety-related systems. BTP 7-19 is part of Chapter 7 of the SRP, which is used to provide acceptance criteria to the staff, especially for nuclear power reactors that the applicable regulations have been met. Therefore, as a secondary function, an applicant may find helpful guidance in the development of a license amendment request and system and equipment designs that will satisfy the NRC regulations. Note that the regulations for construction permits [10 CFR 50.34(h)(1)(i)] and new design certifications [10 CFR 52.47(a)(9)] require, in part, applicants to indicate how their application conforms with or differs from the SRP acceptance criteria.
65	F10	**Comment:** [Page 3, Section BACKGROUND INFORMATION, 4th paragraph] Recommend editorial changes for clarification purposes. **Proposed Change:** 2nd Sentence: "The embedded software within an embedded digital device..." 3rd Sentence: "... exclude the application of embedded digital devices from consideration within an assessment... "	N	The proposed editorial changes in Page 3, Section BACKGROUND INFORMATION, 4th paragraph, 2nd sentence and 3rd sentence, are no longer applicable because in the restructuring and revising the draft RIS, these sentences are no longer included.
66	F11	**Comment:** [Page 3, Section BACKGROUND INFORMATION, 5th paragraph] Using NRC IN 1994-020 may not be a good example for demonstrating the concern expressed in the RIS for two reasons:	N	The NRC staff agrees in part with this comment. (1) Although the NRC staff agrees that the condition was not the result of a CCF due to software defects, this event was still the result of design deficiencies which resulted in a CCF. This design deficiency is what is

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		(1) The condition was not the result of a software common cause failure. The condition was the result of a common mode failure resulting from a design review that did not ensure that replacement equipment was compatible with the specific application service environment. This was clearly a design deficiency regardless of the digital aspects of the device. (2) The OE is significantly dated. This was clearly acknowledged as such by the cross-reference to industry documents published since the event occurred. **Proposed Change:** Consider deleting in its entirety.		highlighted in the RIS. Note that the RIS does not refer to this event as cause by a software CCF. (2) The NRC staff agrees that this OE is significantly outdated. However, this does not affect the applicability of the OE.
67	F12	**Comment:** [Page 3, Section BACKGROUND INFORMATION, 6th paragraph] Using NRC IN 2007-015 may not be a good example for demonstrating the concern expressed in the RIS for two reasons: (1) The RIS is attempting to demonstrate the importance of a "software common cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices." However, the event that occurred as described in IN 2007-015, does not demonstrate this. IN 2007-015 states in conclusion that the industry needs to focus on "design and control of network architecture". (2) Same as comment 6. **Proposed Change:** Consider deleting in its entirety.	N	The NRC staff disagrees with this comment in part. (1) The staff disagrees that this example is attempting to demonstrate the importance of a software CCF. The RIS does not attribute this failure to a CCF but to a failure of the licensee to "understand the operation and failure modes of digital systems (including EDDs), and the effects of these failure modes on operations and safety." (2) The NRC staff does not agree that this OE is significantly outdated since this event occurred in 2006.
68	F13	**Comment:** [Page 4, Section BACKGROUND INFORMATION, 7th paragraph] The latter part of the second sentence through to the end of the paragraph appears to tangent off into a discussion of electromagnetic compatibility (EMC). EMC is an important in-service environment design consideration, but it is not the only one. Also, there appears to be no clear discussion as to the tie between EMC and software failure. **Proposed Change:** Consider deleting in its entirety.	N	The staff disagrees with the comment. In addition to the benefits of digital technology, the RIS refers to technical and design concerns that should be considered when introducing equipment with EDDs in upgrades, replacement components, and new nuclear power plant designs. These concerns could involve not only potential EDD defects in programmable technology that could lead to potential CCF, but also potential increase in susceptibility to EMC issues and other hazards that may affect quality and reliability. For example, components in equipment and instrumentation in a current nuclear system may have met the equipment qualification (EQ) for the EMC environment at the time of licensing, yet could potentially not meet the EQ requirements with new digital replacements in the

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				same environment. Thus, EMC is one of the potential concerns that should be addressed and is specially mentioned in the RIS.
69	F14	**Comment:** [Page 4, under SUMMARY OF ISSUE, 1st paragraph] The first sentence states the following: "The key is that the increased use of embedded digital devices in safety-related equipment may increase a facilities vulnerability to a CCF... " However, no basis is stated as to what the "increase" is compared to. The first sentence goes on to state, "...challenge equipment to EMC... " Here again (see comment 13 above), EMC is neither the issue nor a demonstrated cause of software CCF with embedded digital devices. The first sentence concludes with, "... or otherwise degrade equipment reliability to adversely affect safety. There appears to be no point of reference given or an OE analysis that would reach that conclusion. **Proposed Change:** Consider deleting the first sentence in its entirety.	N	The staff disagrees with the proposed change. These are general engineering judgment observations widely accepted in the nuclear industry. Further, these statements were preferenced with “may” as there could be an exception when viewed on an individual basis. In the referenced sentence from the Summary of Issue Section, there is a summary of the potential issues from increased use of equipment with EDDs that was discussed in the Background Section. The RIS points out that the introduction of EDDs in equipment in safety-related systems may introduce concerns for quality, reliability, and safety not present in analog or boards with discreet electronic components or present in a greater degree or different manner than previous. One of the major concerns is the potential that an undetected EDD defect such as a latent software error in the coding might, when concurrently triggered, result in failure of safety-related equipment in redundant, but otherwise independent systems, creating a CCF. CCF is not the only potential concern. EMC is an example of another potential concern that was discussed in the RIS prior to this summary sentence.
70	F15	**Comment:** [Page 4, under SUMMARY OF ISSUE, 1st paragraph, Item (2)] Item (2) assumes a new failure mode exists that could result in a CCF. Therefore, the statement needs clarification as such. **Proposed Change:** Revise Item (2) as follows: "the need to address new failure modes, and if a new failure mode exists, address the potential vulnerabilities to software CCFs; and,"	N	The staff disagrees with the need for the proposed change. The purpose of Item (2) is to bring focus on the need to consider the possibility of CCF. The staff believes Item (2) is a simple and sufficient summary statement to accomplish this purpose. One of the areas of concern in digital technology is the need to assess the vulnerability to equipment with a potential undetected EDD defect such as a latent software error in the coding or specification error that may cause the failure of the equipment to achieve its intended function and potentially result in a CCF in redundant, but otherwise independent, safety-related systems. NRC regulations and guidance, and industry standards provide considerations with respect to CCFs, which can be used when evaluating suitability of equipment with EDDs.
71	F16	**Comment**: [Page 5, under SUMMARY OF ISSUE, 2nd to last bullet] Reference to BTP should be removed based on discussion in Comment (F)5, above.	N	The staff disagrees with the comment. One of the areas of concern in digital technology is the need to assess the vulnerability of equipment with EDDs, and a potential undetected EDD defect such as a latent software error in the

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: Consider removing reference to BTP 7-14.		coding that may result in a CCF in redundant, but otherwise independent, safety-relate systems. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy is used in systems in nuclear facilities, the potential for CCF is significantly reduced. While BTP 7-14 may not specifically address embedded EDDs, one of the EDD's significant characteristics is that they contain software, firmware, or software developed programmable logic. BTP 7-14 provides guidance on quality software development.
72	F17	**Comment:** [Page 6, under SUMMARY OF ISSUE, the 2nd paragraphs before item (2)] The first statement may not be accurate because IEEE 379-2000 was endorsed by Reg. Guide 1.53, Revision 1, and addresses actuation devices. The second statement should be clarified to more closely represent issue and application of embedded software in actuation devices. **Proposed Change:** Consider deleting first sentence in its entirety Consider revising the second sentence as follows: "Manufacturers are increasingly introducing digital technology into non-actuation and actuation devices that, in turn, are used in applications such as; digital displays, motor controllers, sequencers, pumps, valve actuators, breakers, uninterruptible power supplies, emergency diesel generator controls, etc."	Y	The staff agrees with the comment, and the RIS has been modified to incorporate the comment.
73	F18	**Comment:** [Page 6, under SUMMARY OF ISSUE, the first paragraph before item (2)] Clarification is needed to address commercial grade items **Proposed Change:** Revise a portion of the paragraph as follows:	N	The staff disagrees with the comment. The proposed wording ("devices that contain embedded software") is too specific, and does not cover other types of technology addressed by the RIS (i.e., software-developed firmware, and software developed programmable logic)

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		"... non-digital technology is being replaced with commercial grade devices that contain embedded software that may not have been developed in accordance with..."		
74	F19	**Comment:** [Page 6, under SUMMARY OF ISSUE, Item (2), 3rd bullet] Reference to BTP 7-19 should be removed based on response to Comment (F)5 above. **Proposed Change:** Consider removing reference to BTP 7-19.	N	The staff disagrees with the comment that BTP 7-19 should be removed. The staff believes that BTP 7-19 provides guidance relevant to the EDD issue. A key concern with components with EDDs is the possibility that an undetected EDD defect such as a latent software error within the firmware of an EDD may be triggered to cause the component to fail to function as intended. If this defective software is concurrently triggered in redundant safety-related equipment, in otherwise independent divisions or trains, a CCF may be created. BTP 7-19 specifically provides guidance on addressing assessment of vulnerabilities to CCF regardless of whether it is a microprocessor or equipment with EDDs.
75	F20	**Comment:** [Page 6, under SUMMARY OF ISSUE, last paragraph on the page] The second sentence does not appear to clearly communicate the adverse effect of the software CCF concern and should be clarified. **Proposed Change:** The second sentence should be revised to state the following: "It may be possible that an intended safety protection feature could be defeated by a new software failure mode of an embedded digital device and result in a software common cause failure when the same embedded digital device is used in the redundant safety system execute feature."	Y	The staff agrees with the comment, and the RIS has been revised similar to the proposed change as follows: The last two sentences in the original Page 6 referenced paragraph have been adjusted to read: "Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD, when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF)."
76	F21	**Comment:** [Page 7, SUMMARY OF ISSUE, top paragraph] Same response as Comment (F)1, above. **Proposed Change:** Consider deleting paragraph in its entirety.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
				The staff also agrees with the removal of the first paragraph on Page 7, SUMMARY OF ISSUE that starts with, "Consideration of CCF applies to equipment that is not safety-related to the extent …."
77	F22	**Comment:** [Page 7, SUMMARY OF ISSUE, second from the top paragraph] Same response as Comment (F)1, above. **Proposed Change:** Consider deleting paragraph in its entirety.	N	The staff disagrees with the comment that the paragraph on Page 7, SUMMARY OF ISSUE, second from the top paragraph should be deleted. This paragraph recommends that the guidance in BTP 7-19 may be helpful in evaluating and addressing potential vulnerability to CCF even when BTP 7-19 is not directly applicable guidance as in the case of NPRs. The staff believes that BTP 7-19 provides guidance relevant to the EDDs issue. A key concern with equipment with EDDs is the possibility that an undetected EDD defect such as a latent software error within the firmware of an EDD may be triggered to cause the equipment to fail to function as intended. If this defective software is triggered to cause the failure of redundant safety-related equipment in otherwise independent divisions or trains, a CCF may be created. BTP 7-19 specifically provides guidance on addressing assessment of vulnerabilities to CCF regardless of whether it is a microprocessor or equipment with EDDs.
78	F23	**Comment:** Page 7, under SUMMARY OF ISSUE, Item (3), 2nd paragraph] The first sentence should be clarified to ensure specifications to vendors apply to more than just commercial products. **Proposed Change:** Consider revising the first sentence as follows: "... specifications for vendors supplying safety-related and commercial products targeted for commercial grade dedication, requirements to identify the use of..."	Y	The staff agrees with the comment and the RIS has been revised to incorporate the comment.
79	D1	**Comment:** [Page 1, Intent Section, 2nd Paragraph] Discussion narrows scope to safety-related equipment and then broadens underlying concern to non-safety equipment. Consequently, message is made ambiguous. Remaining discussion does not answer the question on how NRC expects the industry needs to treat requirements for non-safety equipment that contain embedded digital components. NRC should clarify the scope regarding non-safety components with embedded	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified, and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		digital devices. The discussion of non-safety equipment should be deleted, since it is not governed by any specific regulation **Proposed Change:** NRC should clarify the scope regarding non-safety components with embedded digital devices. The discussion of non-safety equipment should be deleted, since it is not governed by any specific regulation.		
80	D2	**Comment:** [Page 2, Intent Section, 5th and 6th Paragraphs] Discussion of postulated software CCFs in non-diverse embedded digital devices coupled with discussion about inadequate diversity assessments implies diversity is the necessary mitigation strategy to use embedded digital devices. **Proposed Change:** NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support obsolescence management strategies or new plant design and procurement strategies.	Y	The staff agrees, in part, with the proposed change. Further clarification has been made to emphasize how current guidance implies that that there are other preliminary options that can be used to reduce the likelihood of an undetected EDD defect causing a failure of safety-related equipment to perform the intended function and potentially creating a CCF in redundant, otherwise independent systems and divisions. This RIS identifies existing regulations and guidance applicable to safety-related equipment with EDDs. For example, while not applicable to all nuclear facilities, BTP 7-19 provides the strategy for dealing with postulated CCFs in digital devices. BTP 7-19 (Revision 6), Section B.1.9, explains that the application of many system design and testing attributes, procedures, and practices, can help significantly reduce the probability of CCF. An initial and underlying premise of this RIS concerning the development and application of digital technology is that a quality development process should be applying the appropriate design measures and practices, and a thorough test program to prevent EDD defects, and perhaps achieve a degree of immunity from triggers. Therefore, when equipment with EDDs developed by such a strategy is used in systems in nuclear facilities, the potential for CCF is significantly reduced. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF, and support reaching a reasonable assurance of safety. It is not the function of a RIS to provide detailed solutions, and/or new guidance for addressing obsolescence management strategies, or new plant design and procurement strategies that may be created by equipment with EDDs.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
81	D3	**Comment:** [Page 2, Intent Section, 5th and 6th Paragraphs] There are no bounds on postulated software CCFs and there is no mention of other design approaches to reasonably minimize the potential for software CCFs as an alternative to component diversity. RIS should reflect discussion between the industry and NRC regarding plans to update NEI 01-01. **Proposed Change:** RIS should reflect discussion between the industry and NRC regarding plans to update NEI 01-01.	N	The staff agrees that potential results from an undetected EDD defect that is triggered to cause failure in redundant equipment resulting in a CCF could involve a number of possibilities similar to envisioning what human errors a reactor operator could make. BTP 7-19 is referenced in the RIS as helpful guidance, even when not directly applicable to certain nuclear facilities. BTP 7-19 used the term "credible CCF" to indicate that postulated CCF are not completely unbounded. BTP 7-19 (Revision 6), Section B.1.9, acknowledges that the first approach is the application of many system design and testing attributes, procedures, and practices that can significantly reduce the probability of CCF. Two design attributes, either of which is sufficient to eliminate consideration of software based or software programmable logic based CCF are: sufficient diversity and (100%) testability. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors, could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary defensive against a CCF. As stated in the 6th paragraph of the Intent Section on Page 2, the intent of this RIS is to heighten awareness of the existence of EDDs and associated potential hazards. It is not the function of a RIS to provide detailed solutions and/or create new guidance for addressing the hazards that may be created by EDDs. The need for additional guidance for safe use of EDDs in critical applications is being addressed separately. The staff agrees that updates to NEI documents, or other industry/EPRI developed guidance documents, may provide further needed guidance on dealing with EDDs.
82	D4	**Comment:** [Page 2, Intent Section, 5th and 6th Paragraphs] Implications can be understood to extend to needing diversity in non-safety equipment when considered in conjunction with scope comment above. **Proposed Change:** (Change implication)	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified and now appears in the final RIS as the third paragraph of the Intent Section as follows: "The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems."

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
83	D5	**Comment:** [Page 3, Background Information Section, 4th Paragraph] Discussion reinforces an expectation that diversity is a required mitigation strategy for embedded digital devices, since even 'simple' devices are not excluded from a diversity analysis. **Proposed Change:** NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support obsolescence management strategies or new plant design and procurement strategies.	Y	The staff agrees in part with the concepts of the comment. The paragraph referenced in the comment has been revised to remove the term "simple," since it is difficult to define. The RIS now states that while the staff does not automatically exclude any equipment with EDDs from consideration in CCF vulnerability assessments, justification should be supplied by the licensee as appropriate for the specific nuclear facility and application. An initial and underlying premise of this RIS in the development and application of digital technology should be a quality development process (using appropriate defensive design measures and practices), and a thorough test program to significantly reduce the chance of EDD defects, and achieve a degree of immunity from triggers, and therefore reduce the potential for CCF when used in systems in nuclear facilities. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF, and support reaching a reasonable assurance of safety. This RIS identifies existing regulations and guidance applicable to safety-related equipment with EDDs. For example, while not applicable to all nuclear facilities, BTP 7-19 provides the strategy for dealing with postulated CCFs in digital devices. It is not the function of a RIS to provide detailed solutions and/or new guidance for addressing obsolescence management strategies, or new plant design and procurement strategies that may be created by equipment with EDDs.
84	D6	**Comment:** [Page 5, Bullet List in Item I in Summary of Issue Section] RG 1.53 R2 is missing from list. RG endorses IEEE 379-2000, which has relevant guidance for the treatment of CCFs. **Proposed Change:** NRC should add RG 1.53 R2 to list of applicable regulatory guidance.	Y	The staff agrees with the comment and the proposed change. The RIS has been revised to add RG 1.53 R2 to the list of applicable regulatory guidance.
85	D7	**Comment:** [Pages 6 and 7, Summary of Issue Section, 2nd Paragraph in Item 2] Reference to BTP 7-19 for treatment of potential CCFs reinforces expectation that diversity is a necessary mitigation strategy for embedded digital devices. BTP 7-19	N	The staff disagrees in part with the comment. The strategy for dealing with postulated CCFs in digital devices is defined in BTP 7-19 that is referenced in the RIS. While BTP 7-19 does not apply to all nuclear facilities, the guidance in BTP 7-19 may be helpful when considering potential postulated CCFs in systems with equipment with EDDs located in safety-related system. BTP

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		describes "two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: Diversity or Testability." The Testability approach, as defined in BTP 7-19, is not a practical option for the types of equipment addressed in the RIS. **Proposed Change:** NRC should clarify how other options to address digital CCF for components with simple embedded devices can be applied to support obsolescence management strategies or new plant design and procurement strategies		7-19, Section B.1.9, first states that applying system-design attributes, complete testing, good procedures and practices can contribute to significantly reducing the probability of CCF. There are two design attributes, either of which is sufficient to eliminate consideration of software based or software programmable logic based CCF: diversity and testability. For testability, a system is sufficiently simple such that every possible combination of inputs, and every possible sequence of device states are tested and all outputs are verified for every case (100% tested). Generally, it is thought this is not achievable either due to the internal memory states, or too many input combinations to be tested in a reasonable period of time. It is a high test bar, but there may be digital components now, or in the future, that may be that simple, either with a reasonable number of inputs AND no intermediate states, perhaps a type of FPGA. Depending on certain factors such as complexity, the risk significance of the system the components are in, knowledge of quality development, thorough testing, and a successful operational history, a licensee may be able to supply sufficient justification for a reasonable assurance of safety. This may be the case with non-nuclear industry developed commercial products even with EDDs. Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors, could mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF, and support reaching a reasonable assurance of safety. It is not the function of a RIS to provide detailed solutions and/or new guidance for addressing obsolescence management strategies, or new plant design and procurement strategies that may be created by equipment with EDDs.
86	D8	**Comment:** [Pages 6 and 7, Summary of Issue Section, 3rd Paragraph in Item 2] Discussion broadens underlying concern to non-safety equipment. Consequently, message is made ambiguous. Overall discussion does not answer questions on how NRC expects industry to treat requirements for non-safety embedded digital components. **Proposed Change:** NRC should clarify scope regarding non-safety components with embedded digital devices.	Y	The staff agrees that further clarification is needed to help avoid any ambiguity that the scope is limited to safety-related systems and equipment, and excludes non-safety systems and equipment. The second paragraph of the Intent Section has been simplified, and now appears in the final RIS as the third paragraph of the Intent Section as follows: “The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety related systems.” Also, the staff has deleted the first paragraph on Page 7 that stated: "Consideration of CCF applies to equipment that is not safety-related to the

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Discussion of non-safety equipment should be deleted, since it is not governed by any specific regulation.		extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)"
87	D9	**Comment:** [Pages 6 and 7, Summary of Issue Section, 4th Paragraph in Item 2] Discussion of BTP 7-19 is limited to equipment performing safety-related system execute features. However, guidance in BTP 7-19 is also relevant equipment performing safety-related monitoring and display functions. NRC should clarify expectations for the application of BTP 7-19 to monitoring and display functions that contain embedded digital devices. **Proposed Change:** NRC should clarify expectations for the application of BTP 7-19 to monitoring and display functions that contain embedded digital devices.	Y	The staff agrees with the comment that the referenced paragraph should not use terms limiting the discussion of BTP 7-19 to equipment performing safety-related system execute features. The RIS has been adjusted to remove any unintentional ambiguity concerning BTP 7-19. The RIS has been adjusted to state in the power reactor portion of the Nuclear Reactor Sector, “In addition to the safety-related sense and command features, the guidance in BTP 7 19 is helpful when considering postulated CCFs in systems with equipment with EDDs performing safety related system execute features.” In “Figure 3” in IEEE Std. 603-1991 (incorporated by reference in 10 CFR 50.55a(a)(2) with the requirements statements in 10 CFR 50.55a(h)) indicates that the sense and command features include I&C equipment performing safety-related monitoring and display functions.
88	M1	**Comment:** [p.1] "The U.S. Nuclear Regulatory Commission (NRC) is issuing this regulatory issue summary (RIS) to clarify NRC's technical position on existing regulatory requirements ... " None of the NRC documents listed in the RIS that refer to digital equipment requirements (including BTP 7-19 and NUREG-0800) are applicable to non-power reactors (NPRs). The only NRC regulatory document specifically addressing the use of digital equipment in NPRs is a proposed amendment to Chapter 7 of NUREG-1537, which, as far as we can determine, is still in draft form. Because specific regulatory requirements on digital equipment for NPRs are not yet officially established, and the purpose of the RIS is stated as clarification on existing regulatory requirements. **Proposed Change:** Inclusion in this RIS of non-power reactor digital equipment is premature. At the very least,	Y	The staff agrees, in part, with the comment, and the regulations applicable to NPRs have been grouped together and annotated in the nuclear reactor sector. The RIS specifically mentions I&C guidance for NPRs, including digital equipment, as NUREG-1537 “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors”, dated February 1996. The draft regulatory guidance in the form of Interim Staff Guidance (ISG) to Chapter 7 of NUREG-1537, does not contain new references that did not previously exist in the February 1996 version of NUREG-1537. As was discussed for the ISG at public meetings held September 13, 2011, June 21, 2012, and September 25, 2012, the updates to NUREG-1537 for instrumentation and control (I&C) were made to update to the most current industry guidance, and to simplify the process of NPR licensees in determining which specific guidance in these industry standards applied to NPRs by incorporating the specific text from these documents as opposed to incorporating the documents in their entirety by reference. NPRs are not included in a sector separate from nuclear power plants due to the significant amount of overlap in the basic premise of instrumentation and control systems for reactors, and the generic nature of the RIS with respect to precautions to

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		NPRs should be included in a sector separate from nuclear power plants, as was done for fuel cycle facilities, in order to better clarify which guidance documents NRC would consider applicable for digital equipment use at NPRs**.**		be exercised when procuring replacement parts that may contain EDDs. As referenced in the published NUREG-1537, many industry and guidance documents that exist are cited as applicable to both power reactors and NPRs (i.e., IEEE 7-4.3.2 and RG 1.152).
89	M2	**Comment:** [p.3] "The NRC Staff provides guidance applicable to components containing software, firmware, and logic developed from software-based development systems." As NUREG-0800 and BTP 7-19 do not apply to NPRs, it is difficult to interpret the applicability of this section to NPRs such as the MIT Reactor, and thus it is unclear whether such guidance exists. **Proposed Change:** (Address Comment)	Y	The staff agrees, in part, with the comment, and the regulations applicable to NPRs have been grouped together and annotated. NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996 and Regulatory Guide (RG) 2.5, "Quality Assurance Program Requirements for Research and Test Reactors", dated June 2010 are both listed and applicable to NPRs in the appropriate section under Nuclear Reactor Sector references in the RIS. The statement concerning BTP 7-19 has been clarified to better indicate that it is only a possible helpful aid for NPRs, and is not applicable guidance for NPRs. Examples were specific to power reactors. However, the staff provided references to the applicable NPR guidance.
90	M3	**Comment:** [p 5-6] "Safety-related equipment with embedded digital devices must comply with the following regulations and should address the following guidance, as applicable:" We agree that sufficient planning and review are necessary for any safety-related component, regardless of whether or not it contains an embedded digital device. The three documents listed here that are relevant to the MITR (NUREG-1537 Part I, NUREG-1537 Part 2, and RG 2.5) contain guidance for review of safety-related components but do not, in their current form, address digital devices. **Proposed Change:** (Address comment)	N	The staff disagrees in part with the comment. The RIS specifically mentions I&C guidance for NPRs, including digital equipment, as NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996. NUREG-1537 contains specific reference to both analog and digital hardware, and to software for computerized systems in Section 7.3 for Reactor Control, Section 7.4 for Reactor Protection Systems, Section 7.5 for Engineered Safety Features Actuation Systems and Section 7.6 for Control Console and Display Systems. The intent of the RIS is that the NPR licensees perform sufficient planning and review as necessary for safety-related components that may contain an EDD, consistent with the applicable guidance, and approved quality standards for the facility.
91	M4	**Comment:** [p. 6] "Equipment consisting of commercial grade items with older non-digital technology is being replaced with commercial grade products containing embedded digital devices ... that may not have been developed in accordance with guidance and acceptable industry standards."	Y	The staff agrees, in part, with the comment and the regulations applicable to NPRs have been grouped together and annotated. The RIS specifically mentions the guidance for NPRs as NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996. The RIS statement referenced is somewhat misleading for NPRs since commercial grade items (as defined in 10 CFR Part 21) do not apply to NPRs. However, the basic premise of the

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		Proposed Change: It is not clear from this RIS what guidance and industry standards would be acceptable for use in NPRs.		statement, and the caution is that products containing EDDs [to be used in NPRs] may not have been developed in accordance with guidance and acceptable industry standards referenced in NUREG-1537 for NPRs.
92	M5	**Comment:** [p 6-7] "Safety-related equipment with embedded digital devices must comply with the following regulations and should address the following guidance, as applicable:" **Proposed Change:** As none of the guidance documents listed in this section are applicable to NPRs, it is unclear what, if any, common-cause failure (CCF) criteria should be applied.	Y	The staff agrees, in part, with the comment, and the regulations applicable to NPRs have been grouped together and annotated. NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996 and Regulatory Guide (RG) 2.5, "Quality Assurance Program Requirements for Research and Test Reactors", dated June 2010 are both listed and applicable to NPRs.
93	M6	**Comment:** [p.13, Backfitting and Issue Finality] As stated above, we believe it premature to issue an RIS for NPRs based on draft regulatory guidance. **Proposed Change:** If it is the intent of the NRC to apply some or all of the nuclear power plant guidance to NPRs, or, by use of this RIS, to enact draft requirements, a backfit analysis would be necessary, as this would represent a change from previous NRC positions.	N	The staff disagrees with the comment. This RIS does not enact any new requirements for NPRs. The current guidance on I&C for NPRs is published in NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996. While there exists draft regulatory guidance in the form of Interim Staff Guidance to Chapter 7 of NUREG-1537, that Interim Staff Guidance does not contain any references to power reactor guidance that did not previously exist in the February 1996 version of NUREG-1537. As was discussed at public meetings held on September 13, 2011, June 21, 2012, and September 25, 2012, the updates to NUREG-1537 for I&C were made to update to the most current industry guidance and to simplify the process of NPR licensees in determining which specific guidance in these industry standards applied to NPRs by incorporating the specific text from these documents as opposed to incorporating the documents in their entirety by reference. Additionally, as a point of reference, the Commission's position is that the backfit rule does NOT apply to NPRs.
94	P1	**Comment:** [General] The Penn State Breazeale Reactor (Docket 5.0-005) has reviewed the subject RIS and opines that the RIS should not be applicable to non-power reactors (NPRs). The document as written is applied to multiple licensees including NPRs. The regulatory basis for applying this document and its stated regulatory positions to NPRs is unclear and seems tenuous. While the NRC's position that NPRs need to use a deliberate process when evaluating	Y	The staff agrees with the comment, and the regulations and guidance applicable to NPRs has been grouped together and annotated. The RIS specifically mentions the I&C guidance for NPRs, including digital equipment, as NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-power Reactors", dated February 1996 and Regulatory Guide (RG) 2.5, "Quality Assurance Program Requirements for Research and Test Reactors", dated June 2010, and both are listed and applicable to NPRs in the appropriate section under Nuclear Reactor Sector references in the RIS.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		changes to ensure that replacement equipment is capable of performing the required functions is appropriate, the cited power reactor regulations and standards are not applicable to NPRs and no case for application of these standards as more than a useful reference is made. **Proposed Change:** (Address Comment)		The basic premise of the statement and the caution is that products containing EDDs [to be used in NPRs] may not have been developed in accordance with guidance and acceptable industry standards referenced in NUREG-1537 for NPRs.
95	P2	**Comment:** [General] The inherent safety in the design of NPRs makes the application of power reactor equipment standards un-necessary and the NRC application of the cited requirements unwarranted. This RIS appears to implement by position statement new regulation on NPR licensees. The imposition of more stringent requirements once an adequate level of safety or an acceptable level of risk has been achieved exceeds the requirements of the Atomic Energy Act. Therefore, the issuance of this document to NPRs citing non-applicable regulatory requirements does not meet the stated intent of clarifying the NRCs technical position. Issuance will likely increase confusion, delay needed system upgrades, and further threaten the continued viability of the Nation's civilian held research reactors. **Proposed Change:** (Address comment)	Y	The staff agrees with the comment and the regulations and guidance applicable to NPRs has been grouped together and annotated. The statements in the RIS do not impose any new requirements on non-power reactors. The intent of the RIS is that the NPR licensees perform sufficient planning and review as necessary for safety-related components that may contain an EDD, consistent with the applicable guidance and approved quality standards for the facility.
96	U1	**Comment:** [Page 4] The Nuclear Reactor Sector section begins with a discussion of the 10 CFR 50.2 definition of "safety-related". The term "safety-related" is applicable to all reactors but only "testing reactors" subject to Part 100 have structures, systems, and components (SSCs) meeting this definition. Based on their definitions in 10 CFR 50.2, the terms "safe shutdown" and "reactor coolant pressure boundary" apply only to PWRs and BWRs. Only a small percentage of NPR facilities are "testing reactors". **Proposed Change:** To provide the intended clarification, the RIS should be revised to indicate that it only applies to	Y	The staff agrees in part with the comment. The RIS has been adjusted for clarification by following the 10 CFR 50.2 definition with the following statement: ”For non-power reactors, the term ‘safety-related structures systems and components,’ as used in this RIS, refers to those structures, systems and components (SSCs) required to ensure the safety of the public and to protect the environment, as described in each facility’s safety analysis report.”

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		those "testing reactors" which have safety-related SSCs meeting the definition of 10 CFR 50.2.		
97	U2	**Comment:** [Page 5] The introductory statement immediately preceding the bulleted list of regulations and guidance in Section (1) uses the qualifying term "as applicable". **Proposed Change:** To provide the intended clarity, the lists of regulations and guidance documents should be better annotated or explained to indicate the applicable reactor type.	Y	The staff agrees with the comment, and the regulations applicable to NPRs have been grouped together and annotated.
98	U3	**Comment:** [Page 6] The bulleted list of regulation and guidance in Section (2) is not applicable to NPRs. In its current form, the draft RIS gives the impression of imposing power reactor regulations and guidance on NPRs. **Proposed Change:** If this is intentional, the NRC should initiate a new DI&C rulemaking docket specific to NPRs and ensure compliance with Section 104(c) of the Atomic Energy Act of 1954.	Y	The staff agrees with the comment, and the regulations applicable to NPRs have been grouped together and annotated.
99	S1	**Comment:** [General] As noted in Reference 1, the Nuclear Regulatory Commission (NRC) published its draft revised NRC Regulatory Issue Summary 2014-XX, "Embedded Digital Devices in Safety-Related Systems," soliciting public comments. STARS appreciates the opportunity to comment on this draft RIS. STARS Alliance LLC endorses the comments submitted on July 7, 2014 by the Nuclear Energy Institute (Reference 2) regarding this issue. **Proposed Change:** (None requested here – see NEI comments with N Commenter ID)	N	No comment response is required.
100	I1	**Comment:** [INTENT Section and general]	N	The Staff disagrees with the proposal to mention non-safety systems and

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		I fully agree with the industry comment about ambiguity. But your solution of taking non-safety out of the discussion is the wrong solution. This is not new guidance for non-safety control systems because SRP 7.7 says: "The objectives of the review are to confirm that …effects of operation or failure of these systems are bounded by the accident analyses in Chapter 15 of the safety analysis report (SAR). Effects of control system failures - The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. Based on the review of the applicant/licensee's diversity and defense-in-depth analysis and the quality of control system functions credited in this analysis, the staff concludes that the control system complies with the criteria for defense against common-cause failure in digital instrumentation and control systems. The staff also confirmed that failure of the control systems themselves …does not result in plant conditions more severe than those described in the analysis of design basis accidents and anticipated operational occurrences." The purpose of the RIS is not to solve the problem, but to bring the problem to industry's attention. We are working through the NEI 01-01 task force (and EPRI) to define criteria that would allow a "CCF unlikely" conclusion to be reached for all applications, including applications with EDDs. In the interim, utilities should be using their best judgment, but not ignoring the problem **Proposed Change:** Remove the ambiguity by saying:		non-safety related CCFs in this RIS by adding the proposed change, although the staff agrees with the concept. First, many of the public comments were concerned about the RIS mentioning non-safety systems. While some commenters believed there was not enough discussion on postulated non-safety related CCF, and the discussion should be expanded, the vast majority of the comments concerned with the mentioning of non-safety systems stated that including non-safety systems in the scope was creating an ambiguity after declaring the scope was safety-related equipment only. The latter commenters proposed deleting any mention of non-safety systems in the scope. Since it is not the function of a RIS to provide new guidance, and work is being done to consider further guidance for non-safety related equipment concerning postulated CCF by the NRC's Office of New Reactors, this EDD RIS will address only safety-related components and equipment. Finally, the sections from SRP 7.7 quoted do not apply directly to NPRs and to the fuel cycle facilities. Retaining the scope as applicable to safety-related equipment with EDDs avoids ambiguity concerns with the NPRs and the fuel cycle facilities. The SRP 7.7 quoted applies to both current and new power reactors. During 10 CFR 50.59 evaluations of proposed changes involving equipment with EDDs, the licensees must consider whether this change would introduce failure modes that have not been previously analyzed, including consideration of failure modes that potentially could involve safety-related and/or non-safety related equipment. Thus, potential effects from the introduction of EDDs or new or revised equipment with EDDs in non-safety systems would not be ignored.

Mstr Cmnt #	Cmntr ID & #	Comment and Proposed Change	Ch	NRC Staff Response
		"This RIS is about the potential for CCF caused by EDD failures in safety or non-safety applications. In safety applications, EDD failures can result in multiple redundant divisions failing to actuate when needed. In non-safety and safety applications, EDD failures can lead to erroneous control actions that may cause unanalyzed plant transients. Either application of EDDs presents a safety hazard for nuclear power plants."		