GORDON A. CLEFTON
Senior Project Manager,
Engineering and Operations Support

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8086
gac@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

6/5/2014
79FR 32578
(3)

RECEIVED
2014 JUL -7 PM 2:43
RULES AND DIRECTIVES
BRANCH
USNRC

July 7, 2014

Ms. Cindy K. Bladey
Chief. Rules, Announcements, and Directives Branch (RADB)
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

Subject: Comments on Draft Regulatory Issue Summary (RIS) 2014-##, "Embedded Digital Devices in Safety-Related Systems" (Docket ID NRC–2014–0129) (*Federal Register* Notice 79FR32578)

Project Number: 689

Dear Ms. Bladey:

The U.S Nuclear Regulatory Commission (NRC), through the *Federal Register* Notice (79FR32578) and Docket ID: NRC–2014–0129, issued for public comment the Draft Regulatory Issue Summary (RIS) 2014-##, "Embedded Digital Devices in Safety-Related Systems." The Nuclear Energy Institute (NEI)[1] offers the attached of comments for NRC consideration.

The industry appreciates the implementation and resolution of our comments submitted in July 2013. This RIS discusses and better clarifies the NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with embedded digital devices.

The industry does have concerns with the reinterpretation of some definitions, broader scoping language that goes beyond safety-related equipment, and an expansion of factors to be considered in a Common Cause Failure (CCF) vulnerability assessment to reduce the apparent dependence upon diversity.

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

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add–
E. Egle (eee)

If you have any questions or require additional information, please contact me.

Sincerely,

Gordon A. Clefton

Attachment

c: Mr. Robert Austin, Electric Power Research Institute
Mr. Ray Torok, Electric Power Research Institute

Comments on Draft Regulatory Issue Summary 2014-##
"Embedded Digital Devices in Safety-Related Systems" (Docket ID NRC–2014–0129)

Assembled Industry Comments

#	Section, Page, Line #	Comment	Proposed Resolution
1	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 the selection of plant equipment.	Address the perceived ambiguity directly such that project decisions can be made with full understanding.
2	General	Branch Technical Position BTP 7-19 was written as an NRC internal document.	References to Regulatory Guides would seem more appropriate.

#	Section, Page, Line #	Comment	Proposed Resolution
3	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 10CFR 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 specifically revises 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.*	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 (Nuclear Security and Incident Response) to determine if the impact indicated is warranted.

#	Section, Page, Line #	Comment	Proposed Resolution
3	(continued) General	*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".* 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.	
4a	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.	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.
4b	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 requirements for non-safety equipment that contain embedded digital components.	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.

#	Section, Page, Line #	Comment	Proposed Resolution
4c	Page 1, Line 35	The RIS does not provide a definition for "Important to Safety" system.	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."*
4d	Page 1, Second Paragraph of Intent Section	On page 1, the second paragraph under "INTENT" reads: *"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. 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.	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).

#	Section, Page, Line #	Comment	Proposed Resolution
4e	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 (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 information only, and that information is pertinent to both safety and non-safety.	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.

#	Section, Page, Line #	Comment	Proposed Resolution
4f	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".* 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 affect multiple non-safety systems. "important to safety" is an undefined term. "beyond the design basis of safety related systems" is confusing when discussing non-safety systems and is irrelevant; the key point is that the condition is not analyzed.	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.

#	Section, Page, Line #	Comment	Proposed Resolution
4g	Page 1, Lines 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 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.	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.
5	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.	Clarify the definition of "simple" by stating that simple systems are those that meet the testability attribute of BTP 7-19 such that they are not considered to have a potential for software-based CCF.

#	Section, Page, Line #	Comment	Proposed Resolution
6	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 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 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 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 (Nuclear Security and Incident Response) to determine if the impact indicated is warranted.

#	Section, Page, Line #	Comment	Proposed Resolution
6	(continued) Page 2, First Paragraph	The language of the RIS appears to make it necessary to classify these components as CDA's despite the fact that 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.	
7	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 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).	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 components implementing safety-related sense and command or execute features (e.g., instrumentation, motor control centers, actuated equipment)"*

#	Section, Page, Line #	Comment	Proposed Resolution
8	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.	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.
9a	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.	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. IAEA NP-T-1.5 and EPRI TR-1002835 list a representative set of fault voidance, fault detection and removal defensive measures that are often useful in developing mitigation strategies against faults and resulting CCFs.
9b	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 to reasonably minimize the potential for software CCFs as an alternative to component diversity.	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.
9c	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.	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.

#	Section, Page, Line #	Comment	Proposed Resolution
10	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"."	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.
11	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" as another consideration. These are all defenses against CCF.	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.
12	Page 3, Paragraphs 3 & 4.	As a strictly editorial comment, the 3rd and 4th paragraphs on page 3 referencing information notices 1994-020 and 2007-015 and the failure mechanisms that underlie.	These references do not appear to be directly applicable to the RIS.
13	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 embedded digital devices, since not even 'simple' devices can be excluded from a diversity analysis.	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

#	Section, Page, Line #	Comment	Proposed Resolution
14a	Page 4, First Paragraph	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]." DI&C-ISG-04 should be referenced not just to identify the failure mode but to provide guidance for defenses against that failure mode.	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.
14b	Page 4, Background Information Section	The Background Information section 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>"*	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.
15	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.	NRC should add Regulatory Guide 1.53, Revision 2, to the list of applicable regulatory guidance.

#	Section, Page, Line #	Comment	Proposed Resolution
16	Page 6, Item 2	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.	Change sentence to read as follows: *"The need to conduct a CCF vulnerability assessment."*
17a	Page 6, Last Paragraph	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.	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 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)."*

#	Section, Page, Line #	Comment	Proposed Resolution
17b	Page 6, Last Paragraph	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.	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."*
18	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.	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

#	Section, Page, Line #	Comment	Proposed Resolution
19	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.	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.
20	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 equipment performing safety-related monitoring and display functions.	NRC should clarify expectations for the application of BTP 7-19 to monitoring and display functions.
21	Page 7, First Paragraph	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.	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."*
22	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.	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.

#	Section, Page, Line #	Comment	Proposed Resolution
23	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.*	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.

#	Section, Page, Line #	Comment	Proposed Resolution
24	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* *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.*	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.