GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

# Category	Section, Page, Line (Commenter)	Comment	Proposed Resolution (Correction, addition, deletion, future phase activity, etc.)	Status
67 Form & Content (Dec/16)	4.1, Page No. 26	Regarding: "**Use of Probable Risk Assessment (PRA)** This is the only Evaluation criterion in which PRA information may be used during the development of a response for the impact on accident frequency. However, the use of PRA remains subject to the guidance and restrictions contained in NEI 96-07, Section 4.3.1." There is no other guidance for PRA. Therefore it is not clear what value this sub-section adds to the document.	NEI should delete this sub-section.	
68 Form & Content (6/14/16) (Dec/16)	4.1 & 4.2	In response to 10 CFR 50.59 Questions No. 1 & 2, NEI 96-07 states (see NEI 96-07 Section 4.3.1 & 4.3.2): 'Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASME B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard.' This criteria is applicable to both the frequency of accidents and the likelihood of malfunctions. It is a little ambiguous, from a strictly literal interpretation perspective, how to implement this guidance for PDC plants.	NEI should state that meeting current RGs (e.g., RG 1.180) is one acceptable means of meeting this quotation for both GDC and PDC plants (and NEI 01-01 Issue No. 12). **Explanation** The NRC has identified certain standards as acceptable for meeting the GDCs (e.g., RG 1.180); in other areas the NRC has not established any standards applicable to that topical areas. In those areas where the NRC has NOT established any standards, then it is up to the inspector to determine if the standard chosen is acceptable. The inspector may choose to ask for HQ assistance.	It is not the purpose of 50.59 to identify which standards apply.
69 Internal Consistency Consistency	Section 4.2.1, Page 27	Section 4.2.1 contains a subsection on "Hazard Analysis;" however, only three examples address the guidance in this section (i.e., Section 5.5, Example 4, Page 59; Section 5.6, Example 4 5, Page 66; Section 5.7, Example 4, Page 79 - under the Evaluation against Criterion 2. Note: Example 6 is the only one to mention a	NEI should resolve inconsistency.	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

w/ Other Guidance (Dec/16)		Software Hazard Analysis). The guidance and associated examples strongly imply that a "Hazard Analysis;" is just a failure analysis. This is not consistent with NRC understandings of what constitutes a "Hazard Analysis." (See also the use of "Hazard Analysis" on page No. 35.) **Note:** Page 59 (see second paragraph under the section heading "CCF Considerations – Software") identifies Hazard Analysis and FMEA as separate things (Is this one page consistent?): "The review process, results, and conclusions are contained in the [critical digital review] CDR, Software Requirements Specification (SRS), Software Design Document (SDD), Software Verification and Validation Report (SVVR), Hazards Analysis, and FMEA." Why is there not a "Hazard Analysis," subsection in every evaluation example against Criterion 1 & 2?		
70 Internal Consistency (Dec/16)	4.1, Page 26 4.2.1, Page 27	These sections include a subsection on "Common Cause Failure Considerations;" therefore, applicants must address both aspects of CCF: (1) impact on reliability (i.e., likelihood of accident/malfunction) under Section 4.1 & 4.2, (2) impact on "new accidents" (as defined in the SAR) under Section 4.5. and (2) impact on "results" (as defined in the SAR) under Section 4.6. However, not all examples do this.	NEI should provide examples for each question where CCF should be addressed.	
71 Consistency w/ NEI 96-07 (Dec/16)	4.2.1, Page 27	The guidance in NEI 96-07 implies that ANY reduction in "system/equipment redundancy, diversity, separation or independence," would require prior NRC approval; however, Appendix D implies that there is some analysis that could demonstrate that the change "causes an attributable and discernible increase in the likelihood of occurrence of a malfunction previously evaluated," implying that SOME reduction in "system/equipment redundancy, diversity, separation or independence," may be acceptable. (see quotations below) Sub Section "**Hazard Analysis**" states: "The Hazard Analysis will assist in providing insights into determining **if** a reduction in redundancy, diversity, separation, or independence **causes an**	NEI should resolve inconsistency. It is not clear how a Hazard Analysis could be used to make a discernibility conclusion; please explain. Hazards analysis typically consist of the identification of potential hazards followed by their elimination, minimization, or mitigation. The probability of an undesirable outcome is	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

		attributable and discernible increase in the likelihood of occurrence of a malfunction previously evaluated in the UFSAR." [**emphasis** added] Which conflicts with NEI 96-07 Section 4.3.2, which states: "Examples 5-8 are cases that would require prior NRC approval because they would result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety: … Example 6 The change would reduce system/equipment redundancy, diversity, separation or independence." For the NRC to consider this change, the method and criteria for making the "discernible increase" evaluation must be identified.	normally not calculated in such an analysis.	
72 Consistency w/ Other Guidance (Dec/16)	4.2.2, Page 27	States: "For digital equipment that has undergone commercial grade dedication (CGD), the equipment is considered essentially equivalent to compliance with the regulatory guidance and industry standards normally applicable to safety-related" This position conflicts with NRC I&C review practices. The NRC position is that a high quality development process is a critical characteristic and should be explicitly evaluated, see SE for EPRI TR -106439: "While the staff finds TR-106439 acceptable, it is a generic proposal and therefore, licensees referencing TR-106439 will need to document the details regarding the dedication process and specific critical characteristics including the verification information described in Standard Review Plan Chapter 7 such as qualification reports, system description and software and hardware design and quality assurance documentation. … The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests."	NEI should resolve.	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

73 HSI (Dec/16)	Section 4.5.1	This section uses logic statements to argue away important human factors issues such as the number/type of parameters and information presentation. These logic statements are not clear and/or do not make sense. For example it states, "Namely, the number of parameters monitored (e.g. 3, 4, 5, etc.) cannot, by itself, initiate an accident." [emphasis added] This may be true, however changing the number parameters very easily can overwhelm or otherwise confuse the operator in a way such that the operator makes an error. In combination, the design and the operator may cause an accident. This error would be caused (or prevented), in part, by the HSI design.	NEI should clarify logical statements throughout Section 4.5.1. Evaluations should not allocate blame for errors on the operator when errors can be associated to the design of the system.	
74 Consistency w/ NEI 96-07 Inconsistent Terminology (Dec/16)	4.5.1, Page 29	The inclusion of a definition of "accident" from "a licensee's UFSAR" is provided in this general guidance document. This definition is not consistent with NEI 96-07 since NEI 96-07 clearly includes transients (or Anticipated Operational Occurrences (AOOs)) in the meaning of "Accident" as used in 10 CFR 50.59 (See NEI 96-07 Section 3.2 & 4.3.1), while this Appendix D definition seems to exclude those meanings. The problem is the 10 CFR 50.59 rule uses the term "accident" with a certain intended meaning (and it is NOT just things that initiate ESF); implementation guidance should not imply a different meaning.	NEI should ensure the use of the term "accident" in Appendix D is consistent with the discussions in NEI 96-07 for the term "accident" as used in 10 CFR 50.59. NEI should delete the example definition of "accident."	
75 Form & Content (Dec/16)	4.5.1, Page 29	The sub-section titled, "**Initiation of Multiple Accidents**," states: "the initiation of more than one accident due to any reason (including a CCF) creates an accident of a different type." If one uses the NEI 96-07 definition of accidents (i.e., includes AOOs), then this guidance would not allow the implementation of a distributed control system (where any node includes more than one previously independent function) under 10 CFR 50.59. The guidance provided may be found acceptable, if it can be stated without redefining terms (e.g., accident). Clearly the NRC would want to review any proposed changes that would result in the (new) potential need to initiate multiple	NEI should resolve.	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

		safety functions simultaneously.		
76 HIS Internal Consistency Consistency w/ Other Guidance (Dec/16)	4.5.1, Page 30 Sub-Section titled: "HSI Considerations"	States: "*Information Presentation* If an adverse impact resulted from the information presentation factor, there is no mechanism for a "manner of presentation" to initiate an accident. If an accident cannot be initiated, then it is impossible to initiate a new accident. If a new accident cannot be initiated, then a different accident cannot be created." Since it is "impossible" to create a new type of accident (or AOO), no examples are provided; however, this guidance neglects that a confused operator can make a mistake. This guidance is in effect stating that no matter how badly information is presented to the operator, it will never increase the probability of him making a mistake (e.g., initiating an AOO or an Accident). Also, this guidance is not consistent with guidance provided in Section 4.6.1 on Page No. 33: "*Information Presentation* If an adverse impact resulted from the information presentation factor, there is no mechanism for a "presentation method" to cause a result. Namely, the presentation method cannot, by itself, cause a result. However, the use or *application* of the presentation method could potentially create a different result." Why is the application of the presented information considered in Section 4.6.1, but not in Section 4.5.1?	NEI should provide guidance and examples associated with the impact of poorly presented information on operator performance.	
80 Consistency w/ NEI 96-07 (Dec/16)	4.6.1, Sub-Section "Types of Results" Page 35,	States: 'Many types of results can be described in a UFSAR. In the main body of NEI 96-07, Section 4.3.6, the second bullet/example after the first paragraph states: "Provided the **end result** of the component or subsystem failure is the same as, or is bounded by, the results...described in the UFSAR..., then...[the activity]...would not create a 'malfunction with a different result'." [bold underline emphasis added] In some cases, the result may be a transient or accident (i.e., a specific plant-level response) if the malfunction is a transient or accident initiator. In these cases, a discussion of the transient or accident that is initiated by the SSC	NEI should resolve inconsistency.	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

		malfunction will typically be described in the UFSAR in addition to the malfunction of the SSC itself and the physical result of the malfunctioning SSC. If a transient or accident is identified as a result of a malfunction, the plant-level response described in the transient or accident would be considered the **end result**. For activities involving digital modifications, only the **end result** will be the result of interest. For clarity, all results other than the **end result** will be classified as "intermediate results." No "intermediate results" need to be considered if more than one level of result is described.' The above excerpt is not consistent with NEI 96-07 Section 4.3.6. In evaluating a proposed activity against this criterion, the types and results of failure modes of SSCs that have previously been evaluated in the UFSAR and that are affected by the proposed activity should be identified. This evaluation should be performed consistent with any failure modes and effects analysis (FMEA) described in the UFSAR, recognizing that certain proposed activities may require a new FMEA to be performed. Attention must be given to whether the malfunction was evaluated in the accident analyses at the component level or the overall system level. While the evaluation should take into account the level that was previously evaluated in terms of malfunctions and resulting event initiators or mitigation impacts, it also needs to consider the nature of the proposed activity. Thus, for instance, if failures were previously postulated on a train level because the trains were independent, a proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether new outcomes have been introduced.		
81 Consistency w/ NEI 96-07 (Dec/16)	4.6.1, Sub-Section "Types of Results" Page 36,	States: "Therefore, if a transient or accident is identified as a result of a malfunction, the initiation of a different transient or accident than that which is already described in the UFSAR is not a different result provided that the plant-level response is bounded by another transient or accident." The above excerpt is also not consistent with NEI 96-07 Section 4.3.6, as described previously.	NEI should resolve in consistency.	

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

83 Form & Content (Dec/16)	Section 5, Page 39	The examples do not reference the specific criteria or guidance used to make the determinations in the examples. The examples do not include an explanation (or rational) of how the criteria or guidance have been met.	NEI should add reference to the specific criteria or guidance used to make the determinations in the examples. NEI should consider adding numbers and/or letters to Appendix D so that each piece of guidance is referenceable.	Discuss with Section 5, Examples
84 Form & Content Coping and Susceptibility Analysis (Dec/16)	Section 5, All Examples	The screening does not mention a Coping Analysis. Presumably Section 3.2.1.3, "Coping Analysis," was added to Appendix D so that this analysis would be considered as part of the screening process. Another assumption from the Examples is that a Coping Analysis does not always need to be performed. When does a Coping Analysis need to be performed? Why?	NEI should explicitly address Coping Analysis in these examples.	Discuss with Section 5, Examples
85 Internal Consistency (Dec/16)	5.2, page 42	Regarding: "there was no reduction in the reliability of performing a design function because no new malfunctions or accident initiators were created." This statement is not logical. The probability or likelihood of misbehavior should be distinct from the manner of misbehavior. How does one determine that "no new malfunctions or accident initiators were created?" This conclusion is stated, but not supported by evidence and reasoning. What constitutes sufficient evidence and reasoning?	NEI should address.	Discuss with Section 5, Examples
86 Consistency w/ Other Guidance (Dec/16)	5.4, Example 3 Page 50 5.5, Example 4 Page 57	Example 3 States: "Since identical software will be used in each DRA, there is an adverse impact on the independence of the EDGs described in the UFSAR." Example 4 States: "since identical software will be used in each digital control system, there is an adverse impact on the independence of the chillers described in the UFSAR." GDC 22 states: "Criterion 22—Protection system **independence**. The protection system shall be designed to assure that the effects of natural phenomena, and of normal	NEI should clearly state the criteria these two examples embody (i.e., employing the same software in multiple trains is inherently adverse for 10 CFR 50.59 screen purposes). This criteria could be stated in Section 3.1 or 3.2.1.3. NEI should evaluate the extent of	Discuss with Section 5, Examples

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

		operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. **Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.**" Diversity is recognized as one technique to address CCF.	applicability of this comment to all examples. The basic idea is the criteria must be stated, and the purpose of the example is to clarify the application of the criteria, NOT to provide the criteria in examples.	
87 Form & Content (Dec/16)	Section 5.3, Page 44 Section 5.4, Page 50 Section 5.5, Page 57 Section 5.6, Page 64	As part of the screening process (of these examples), under the sub-heading, "Dependability Assessment," it states: "Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment." However, Appendix D Section 3.2.1.4 does not mention a "Critical Digital Review"; therefore, it is not clear what guidance in Appendix D is followed or what acceptance criteria is used to perform a "critical digital review." **Note:** EPRI TR-106439 uses the term "critical design review," and "critical review." EPRI TR-107339 (NOT ENDORSED) uses the term "Critical Digital Review" (see Appendix A). Presumably following Appendix B is at least as good as commercial grade dedication (CGD); therefore, based on this criteria, all safety related equipment would screen out for this specific criteria. Dependability is achieved by specific features or properties of an item and the conditions in which that item is used. Features and conditions are application specific, and must be explicitly identified before they can be used in an evaluation. CGD or an Appendix B process are sufficient for ensuring an item has the proper features, once those features are explicitly stated, but not if the features and conditions are not stated. See also comment on Section 4.2.2.	In the public meeting on April 28, 2016, NEI stated that Appendix D would not contain or reference technical guidance; however, it was also identified that a mapping was required to direct users to the appropriate technical guidance. This mapping would not be in Appendix D.	Discuss with Section 5, Examples

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

88 Consistency w/ Other Guidance (Dec/16)	Section 5.4, Example 3 Page 49	There are different sets of criteria that may not be aligned: (1) 10 CFR 50.59 Bounding (see question vi) (2) SRM to SECY 93-087 Coping Analysis of I&C System (3) BTP 7-19 Analysis of RTS & ESFAS a. Design Attribute Analysis (see BTP 7-19 Section 1.9) b. Coping Analysis The point of the SRM was to state the Commission's position of what it takes to demonstrate the design meets a NPPs principle design criteria for digital technology.	Please read RIS 2016-04. A mapping is needed between 50.59 criteria, and the various analysis that are performed as part of the technical work. That is, how are the outcomes of these various analyses used to address 50.59 criteria?	Discuss with Section 5, Examples
90 Form & Content (Dec/16)	Section 5.5, Example 4 Page 55	Please read the Summer Violation for installing a digitally controlled chiller (ML14002A205 – Starting on the bottom of Page No. 5; PDF page 8) before or after reading this example.	None	Discuss with Section 5, Examples
91 Form & Content (Dec/16)	Section 5.5, Example 4 Page 57	Top of page states: "The UFSAR states that the MCR air conditioning system is designed "to maintain temperature and humidity conditions throughout the building for the protection, operation, and maintenance and testing of plant controls, and for the safe, uninterrupted occupancy of the main control room (MCR) habitability system (MCRHS) area during an accident and the subsequent recovery period" and the MCR air conditioning system consists of "two 100% capacity units. Each meets the single failure criterion...." In a two train system, generally the system meets the single failure criterion, but "Each Train" does not.	Change "Each" to "The system"	Discuss with Section 5, Examples
92 Inconsistent Terminology (Dec/16)	Section 5.5, Example 4	In this example, under the section termed "Hazard Analysis" the applicant states, in part, that the FMEA did not identify any single failure modes of the digital control system that would result in the loss of safety function. An FMEA is a type of hazard analysis; however, is it the appropriate type of hazard analysis to apply to a digital control system? What is the criteria to determine when a simple FMEA is insufficient for a digital control system?	Recommend NEI provide clarification on what they envision for performing hazard analysis on design modifications of varying complexity and the appropriateness of FMEAs on modifications of varying complexity.	Discuss with Section 5, Examples
93 Consistency w/ NEI 96-07	5.7, Page 78	States: "In the response to Criterion #5, the Increase in Heat Removal by the Secondary System - Increase in Feedwater Flow event [a frequency category II (Moderate	NEI should remove the inconsistency.	Discuss with Section 5,

GREEN - Comments will be addressed
BLUE - Comments applies to Section 5, Examples, and will be addressed in a future meeting
YELLOW - Comment not fully understood, needs further explanation [none]
RED - Comment is not related to 50.59 (or Appendix D) or the purpose of 50.59 guidance; will not be addressed in Appendix D meetings

DRAFT Comments on the Evaluation Section of Appendix D

(Dec/16)		Frequency) event] assuming the opening of both sets of feedwater regulating/bypass valves was determined to be bounded by the Increase in Heat Removal by the Secondary System - Steam System Piping Failure [a frequency category IV (Limiting Fault) event]…" This is not consistent with NEI 96-07 Section 2, which states: "For many licensees, ANSI standards define categories of accidents or malfunctions. For each category a probability (frequency) and a corresponding acceptable consequence is given in terms of barrier loss and radioactivity release. Consequences resulting from accidents and malfunctions are analyzed and documented in the UFSAR and are evaluated against dose acceptance limits that vary depending on the event frequency." This is also not consistent with NEI 96-07 Section 4.3.6, which states: "The possible malfunctions with a different result are limited to those that are as likely to happen as those described in the UFSAR." There are two types of changes possible: (1) changes to existing equipment, and (2) adding new functions or equipment. If new functions or equipment is being added, then it may not be obvious which SAR analysis should be compared to for the bounding determination, as explained below. There are many different AOOs and Accidents considered when analyzing a design. These events are grouped in terms of frequency and functionality (i.e., component or system analysis). The analysis of most limiting event in each group is summarized in the SAR. For any new events, one must first determine which group it belongs to, then the bounding analysis can be performed in accordance with the appropriate group bound. If NEI proposes a new system of bounding analysis, then NEI should explicitly and comprehensively describe that new system, as well as provide a rational for its acceptability.		Examples