PUBLIC SUBMISSION

SUNSI Review Complete
Template = ADM-013
E-RIDS=ADM-03
ADD: Tom Boyce (RES), Philip McKenna, Stephen Burton

COMMENT (8)
PUBLICATION DATE: 5/30/2019
CITATION 84 FR 25077

As of: 8/7/20 9:12 AM
Received: August 06, 2020
Status: Pending_Post
Tracking No. kdj-j0is-ww2x
Comments Due: August 06, 2020
Submission Type: Web

Docket: NRC-2019-0086
Draft Regulatory Guide, DG- 1356, Guidance for Implementation of 10 CFR 50.59, "Changes, Tests, and Experiments"

Comment On: NRC-2019-0086-0006
Guidance for Implementation of Changes, Tests, and Experiments

Document: NRC-2019-0086-DRAFT-0012
Comment on FR Doc # 2020-14564

Submitter Information

Email: KenScarola@NuclearAutomation.com
Organization: Nuclear Automation Engineering, LLC

General Comment

Ken Scarola, Principal Officer of Nuclear Automation Engineering, provides the comments attached.

Attachments

NAE Comments on RG 1.187 Rev. 2 Endorsement of NEI 96-07 App. D Rev. 1

Comments from Nuclear Automation Engineering on RG 1.187 Rev. 2 GUIDANCE FOR IMPLEMENTATION OF 10 CFR 50.59, "CHANGES, TESTS, AND EXPERIMENTS" issued June 2020

RG. 1.187 Rev. 2 should have included the following clarifications regarding the endorsement of NEI 96-07 Appendix D Rev. 1:

1. In RG 1.187 Section C.2.b.ii, the Staff endorsed Example 4-18 to illustrate a proposed activity that does not create the possibility for a malfunction of an SSC important to safety with a different result for the evaluation of 10 CFR 50.59(c)(2)(vi). This is based on the minimum DNBR result being within the accident acceptance criteria of 1.30. Therefore, this example is judging the acceptability of the change based only on the impact to the acceptance criteria for a fission product barrier, which is clearly the purpose of 10 CFR 50.59(c)(2)(vii). Based on this interpretation in NEI 96-07 Appendix D, 10 CFR 50.59(c)(2)(vi) adds no unique criteria to the evaluation. RG 1.187 should explain the basis of the Staff's acceptance that there is no uniqueness between 10 CFR 50.59(c)(2)(vi) and (vii).

   In addition, Example 4-18 states that the minimum DNBR for the current design is 1.42 and the new minimum DNBR calculated for the proposed design is 1.33. Therefore, although the proposed design does not create a malfunction with a different result, it significantly reduces the margin to the acceptance criteria. Therefore, it is reasonable to conclude that the proposed design creates more than a minimal increase in the consequences of a malfunction of an SSC important to safety previously evaluated in the final safety analysis report, which must be evaluated for 10 CFR 50.59(c)(2)(iv). 10 CFR 50.59(c)(2)(iv) directly correlates to General Design Criterion (GDC) 10, "Reactor Design," which states:

   > "The reactor core and associated coolant, control, and protection systems shall be designed **with appropriate margin** to assure that specified acceptable fuel design limits are not exceeded during any condition of normal operation, including the effects of anticipated operational occurrences. [**emphasis** added]".

   The NRC Staff reviewed the accident analysis and determined that there was "appropriate margin." The proposed design significantly reduces the "appropriate margin" that the Staff had approved, which brings compliance to GDC 10 into question. RG 1.187 should explain why this significant reduction in margin does not require additional Staff review to remain in compliance with GDC 10.

   It is recognized that NEI 96-07 Section 4.3.4 says that only radiological consequences are considered when evaluating 10 CFR 50.59(c)(2)(iv). However, there is a direct correlation between DNBR, fuel damage and radiological consequences. Since NEI 96-07 Appendix D does not explain the correlation between a reduction in DNBR margin and an increase in the radiological consequences of this malfunction, RG 1.187 should clarify the Staff's position on this point. In addition, since the rule language in 10 CFR 50.59(c)(2)(iv) does not limit the increase in the consequences of a malfunction to only radiological consequences, RG 1.187 should clarify the basis of the Staff's endorsement of this guidance in NEI 96-07 Section 4.3.4.

2. In RG 1.187 Section C.2.c says “RIS 2002-22 Supplement 1 … may be used in conjunction with NEI 96-07, Appendix D, Revision 1.” Section 1.2 of Appendix D states “The guidance in this appendix applies to … a complete replacement of an analog reactor protection system with an integrated digital system." However, on page 2 the RIS states “This RIS supplement is not directed toward digital I&C replacements of the reactor protection system …” These statements clearly conflict; RG 1.187 should address this discrepancy. For example, RG 1.187 could reiterate that (1) to preclude further consideration of a CCF due to a digital design defect, reactor protection system (RPS) replacements require a deterministic assessment of sufficient diversity or sufficient simplicity (i.e., testability), not simply a qualitative assessment to reach a “sufficiently low likelihood” conclusion and (2) if a CCF due to a digital design defect cannot be precluded for the RPS, then an analysis is needed for each accident to demonstrate CCF coping using alternate methods.

3. For evaluating 50.59(c)(2)(vi) - Create a possibility for a malfunction of an SSC important to safety with a different result - page 9 of RG 1.187 says “the test fails if the change would invalidate “basic assumptions… examples of “basic assumptions” include the assumptions (1) that credited plant and reactor protection system functions will be performed, (2) that credited engineered safety system functions will be performed, and (3) that credited plant system functions and associated instrumentation and controls functions will be performed.” Contrary to this regulatory position, NEI 96-07 Appendix D Example 4-20 describes a proposed change where a credited system function will not be performed due to a software CCF (i.e., a basic assumption is invalidated by the CCF); however, the ability to cope with loss of that credited function using alternate methods is the basis for 10 CFR 50.59(c)(2)(vi) acceptance. RG 1.187 should address this inconsistency.

   Example 4-20 emphasizes that the alternate methods are “currently proceduralized” and are “NOT compensatory actions for addressing degraded or nonconforming conditions.” But the described alternate methods are not the methods credited in the accident analysis, and one alternate method is “a new digital control system “restart” feature to … clear any software faults.” As written, this is certainly a new compensatory action to address a degraded condition in the new digital control system. Therefore, this change appears to invalidate a basic assumption of the original accident analysis. RG 1.187 should clarify the Staff’s position on crediting compensatory actions to avoid invalidating basic assumptions.

   RG 1.187 should also clarify the Staff’s position on crediting “restart” to clear software faults; there is no technical basis to conclude that any/all software faults can be cleared by restart. I have never seen restart credited in any coping analysis for compliance to SRM SECY 93-087 or BTP 7-19; the Staff’s position has always been that unless the design defect that caused the software fault is corrected, whatever caused the software fault is likely to recur. Therefore, restart cannot be relied on as a coping action.

4. BTP 7-19 and SRP 18-A require a human factors evaluation to conclude that there is acceptable time margin between Time Required and Time Available to credit manual actions for coping with a CCF. However, NEI 96-07 Appendix D Example 4-20 concludes that

the plant can cope with loss of a credited safety function using manual actions, with no mention of a human factors evaluation. RG 1.187 should address this omission.

5. NEI 96-07 Appendix D Example 4-1 concludes that a proposed change is not adverse. But there is no discussion of documenting a "Qualitative Assessment" to reach a "sufficiently low likelihood" conclusion, as is required by RIS 2002-22. Furthermore, per the guidance in NEI 96-07, Section 5, there is no regulatory requirement to document screenings (only evaluations). RG 1.187 should address this discrepancy.

6. NEI 96-07 Appendix D Example 4-2, which maintains the segmented configuration of the original analog design, but with identical digital devices, correctly concludes that the proposed change is adverse because it introduces the potential for a CCF due to a design defect in both digital controllers. But Example 4-3, which describes the same configuration in Option 1, concludes that this proposed change is not adverse because the segmented configuration of the analog design is maintained. Even though the segmented design is maintained, this example fails to mention the potential for a CCF due to a design defect, as in Example 4-2. RG 1.187 should address this discrepancy within NEI 96-07 Appendix D.

   It is recognized that NEI 96-07 Appendix D Section 1.5 discusses "deliberate exclusion of other pertinent and/or related aspects". However, this example clearly states that the two analog control systems are "physically and functionally the same" (i.e., this is not excluded). Therefore, unless the example describes new intentional diversity built into the digital controllers, the reader is very likely to conclude that the digital systems are also "physically and functionally the same"; and regardless of this conclusion, a CCF due to a design defect does not require consideration due the segmentation. But segmentation alone does not preclude the need to consider a design defect in all segments that utilize the same design. RG 1.187 should address this problem in Example 4-3 to circumvent this misleading conclusion.

7. NEI 96-07 Appendix D Example 4-4 concludes that the proposed digital design is not adverse, because although the new design can cause multiple function failures, compared to only single function failures in the original design, the multiple failures all cause loss of the ability to control temperature, which is stated to be the same as in the original design.

   But this example discounts that there are two controllers in the original design – one for temperature monitoring/control and a separate controller for air damper control – whereas in the proposed digital design all functions are combined into one controller. Therefore, in the original design if the temperature controller fails, the air damper can be manually controlled by putting the air damper controller in the manual mode. If the air damper controller fails the temperature in the room can be monitored remotely; therefore, if the temperature gets too high an auxiliary operator can be sent to the room to manually reposition the damper. In the proposed design a failure of the digital controller prevents both damper control and room monitoring. Therefore, the proposed design changes the human systems interface (HSI) design, and it reduces defense-in-depth; therefore, the

screening should have concluded that the change is adverse; therefore, the change requires further evaluation. RG 1.187 should address this error in NEI 96-07 Appendix D.

8. NEI 96-07 Appendix D Example 4-5 reaches an adverse conclusion, because previously separate analog control functions are combined into a single digital controller; this is correct. However, contrary to Example 4-2, this conclusion incorrectly implies that separate digital controllers can resolve this adversity. The example should have clarified that, as in Example 4-2, even if there are two separate digital controllers, if those controllers employ the same digital platform, the digital design is still adverse due to the potential for a CCF of both controllers due to a design defect in the digital platform. Without this clarification, adverse conditions in distributed control systems that are being commonly deployed throughout the industry can be overlooked. RG 1.187 should address this clarification.

9. NEI 96-07 Appendix D Example 4-6 concludes that a proposed change from conventional HSI to touch screen HSI is not adverse because the operator can still manually control the valves. It is not possible to reach this not adverse conclusion without a thorough evaluation of touch screen navigation. In the current design the knob is spatially dedicated continuously visible (SDCV). In the proposed design, accessing this touch control could require numerous screen navigation steps to get to the screen that has the touch controls for this flow control valve. This additional screen navigation increases the Time Required to take a manual action, which increases the task burden and decreases the margin to Time Available. Screen navigation and selectable controls also introduce the potential for human error. Therefore, this change is adverse and requires further evaluation. RG 1.187 should address this error in NEI 96-07 Appendix D.

10. NEI 96-07 Appendix D Example 4-7 has the same problem as discussed in Item 9 above, regarding the change from conventional controls to touchscreen controls. RG 1.187 should address this error in NEI 96-07 Appendix D.

    In addition, Example 4-7 concludes that a change from conventional analog meters and indicator lights to flat screen displays does not impact the operator’s ability to monitor and detect changes in plant parameters; therefore, the change is not adverse. But this conclusion cannot be reached without a thorough human factors evaluation, because the change from SDCV information to selectable information changes the operator's ability to monitor these functions. Needing to navigate to appropriate screens to obtain information adversely impacts task burden and situation awareness. Therefore, from a screening perspective this change is adverse.

    It is noted that Example 4-8 does reach a correct adverse conclusion due to the negative impact on situation awareness. RG 1.187 should clarify that this adversity is likely to apply to every digital modification that converts conventional HSI to selectable flat screens, unless an SDCV display (e.g., a plant overview display) is also included in the modification to maintain a comparable level of situation awareness as in the original analog design that utilized SDCV indicators.

In Example 4-7, there is also no discussion of the separate analog indications and controls being combined on a single flat panel. This results in several adverse conditions that are not mentioned at all in this example:

- Even though there are separate flat panels for each division, a single malfunction or design defect in a flat panel could result in failure of many more functions (i.e., multiple indications and multiple controls) than a single malfunction in the analog design which could result in failure of only one indication or one control. Therefore, the digital design reduces defense-in-depth, which is adverse.
- In the analog design, when there is a malfunction that results in failure of an indicator, the control is not impacted (and vice versa); in the digital design a single malfunction or design defect results in failure of both indication and control. Therefore, the digital design reduces defense-in-depth, which is adverse.
- Since the digital design combines multiple indications, a single malfunction or design defect could result in multiple erroneous indications, not just failure of indications. This could result in human performance errors which are adverse.
- Since the digital design combines multiple controls, a single malfunction or design defect could result in multiple spurious operations, not just failure of control functions. This could result in unanalyzed transients which are adverse.

In Example 4-7, there is also no discussion of a design defect that could result in a CCF of the flat panels in both divisions. That CCF could result in loss of all indications/controls or erroneous indication/control in both divisions. Since a design defect leading to a CCF of both divisions was not considered for the previous analog design, due to it's simplicity, the potential for a CCF due to a design defect in the new digital design, due to its complexity, is adverse.

RG 1.187 should address the numerous errors in NEI 96-07 Appendix D Example 4-7.

11. NEI 96-07 Appendix D Example 4-8 reaches a not adverse conclusion for a change from conventional HSI to touch screen HSI, even though it acknowledges that the proposed design would result in an increase in response time for operator actions. Unless a thorough evaluation is conducted to determine the plant level effect of this increase in response time for any credited manual actions the "minimal increase in the consequences of a malfunction" requirements of 50.59(c)(2)(iv) cannot be determined. RG 1.187 should address this error.

    In addition, this example provides no discussion regarding the potential for CCF of multiple erroneous indications, multiple spurious operations and multiple failures, due to the consolidation of numerous indications and controls into only two flat panels and use of common digital designs. All of these present adverse conditions that require further evaluation. RG 1.187 should address this omission.

12. On page 24, NEI 96-07 Appendix D states "the "negative" impact due to a software CCF likelihood being **not sufficiently low** could be partially or wholly offset by the "positive" impacts due to the digital system/component itself and/or its design features." There is no

technical basis for this statement; there are no digital benefits that negate the need to demonstrate the ability to cope with a CCF whose likelihood is not sufficiently low. This statement in NEI 96-07 Appendix D contradicts both RIS 2002-22 Supplement 1 and BTP 7-19. RG 1.187 should correct this statement.

13. NEI 96-07 Appendix D Example 4-10 incorrectly concludes that with the failure likelihood introduced by the modified SSC being not sufficiently low, there is more than a minimal increase in the frequency of occurrence of the accident previously evaluated in the UFSAR. But not sufficiently low is most likely to mean that the failure likelihood is comparable to single malfunctions, which establish the frequency of this event for the FSAR. Therefore, digital failures that have comparable likelihood to analog failures do not automatically increase the frequency of the accident; RG 1.187 should correct this error. RG 1.187 should also clarify that digital failures that have a comparable likelihood to analog failures may increase the frequency of the event if there are more digital vulnerabilities; but this is rarely the case for modern digital designs.

14. NEI 96-07 Appendix D Example 4-11 concludes that an adverse impact on the likelihood of occurrence of the malfunction has occurred due to the potential for a CCF due to a design defect in redundant safety controllers. But this conclusion does not credit that for compliance to other regulatory guidance for safety systems, the digital equipment must be designed with a robust design process. Therefore, in accordance with SRM SECY 93-087 the likelihood of a CCF due to a design defect is low enough to consider the CCF a beyond design basis event; this supports a qualitative assessment with "sufficiently low likelihood" conclusion in accordance with RIS 2002-22 Supplement 1. Therefore, the increase in the likelihood of the event due to a digital CCF is minimal; a minimal increase is permitted by 10 CFR 50.59(c)(2)(i). RG 1.187 should correct this conclusion and clarify the correlation to SRM SECY 93-087.

15. NEI 96-07 Appendix D Example 4-12 describes a sufficiently low likelihood, which supports a conclusion that there is not more than a minimal Increase in the likelihood of occurrence of a malfunction. The example states that “The *qualitative assessment* considered system design attributes, quality of the design processes employed, and operating experience of the proposed equipment.” But unless interconnections are described, as they are in the same example for the screening, Example 4-3 Option 1 “retaining two discreet, unconnected control systems”, it is not possible to assess the likelihood of malfunctions due to a failure of a shared resource (e.g., network, workstation). Without adequate defensive measures, shared resources are typically new sources of failure that increase the likelihood of malfunctions. I agree that the design process may support a "sufficiently low likelihood" conclusion for failure due to a design defect. But to reach a conclusion that the likelihood of failure has not increased due to single random hardware failures, an assessment is needed for the likelihood of failures in all shared resources. RG 1.187 should clarify that a sufficiently low likelihood conclusion for a design defect does not preclude malfunctions due to shared hardware resources.

It is recognized that NEI 96-07 Appendix D Section 1.5 discusses "deliberate exclusion of other pertinent and/or related aspects". However, since the potential for CCF due to a single malfunction in a shared resource is frequently overlooked, this example should help industry avoid that oversight, not contribute to the potential for that oversight.

16. NEI 96-07 Appendix D Example 4-13:
    a. Saying the failure likelihood introduced by the modified SSC is not sufficiently low is unrealistic, because a digital modification for any safety equipment must have a robust design process. If not, it does not comply with other regulatory guidance for safety systems. If there is a robust design process, that complies with regulatory guidance, then a sufficiently low likelihood conclusion for a CCF due to a design defect will be reached. Understanding 10 CFR 50.59 is difficult enough; unrealistic examples compound this challenge and are very likely to mislead industry. RG 1.187 should address the unrealistic evaluation conclusion in this example.
    b. Saying "the single failure criteria are no longer met" [should be '<u>criterion</u> is no longer met'] is unrealistic, because the single failure criterion (SFC) must always be met for redundant safety equipment. Even the potential for a CCF due to a design defect does not negate SFC compliance, because for a safety system (i.e., a system with a robust design process) SECY 93-087 defines CCF due to a design defect as a beyond design basis event. BTP 7-19 has clarified that a design defect in a safety system is not a single failure. RG 1.187 should correct the inconsistency between this example and other NRC guidance.

17. NEI 96-07 Appendix D Example 4-14 is used to illustrate a modification that does not create an accident of a different type because the likelihood of a CCF is sufficiently low. But in contrast, even if the failure likelihood is <u>not</u> sufficiently low, loss of feedwater and excess feedwater (even if more severe than previously analyzed) are not accidents of a different type, because these feedwater anomalies were previously analyzed. The consequences of the malfunction may increase, but that requires evaluation for 10 CFR 50.59(c)(2)(iv). RG 1.187 should clarify this point.

18. NEI 96-07 Appendix D Example 4-15 is used to illustrate the creation of an accident of a different type when two separate control functions are combined into a single digital controller. I agree that this configuration could result in an accident of a different type. However, the example should also emphasize that the same conclusion would be reached if there were separate digital controllers that employed a common shared hardware resource (e.g., network, touch screen), because with a shared hardware resource a single malfunction could adversely affect both controllers. The same conclusion would also be reached if there were separate controllers, with each sharing the same digital design, and a sufficiently low likelihood conclusion could not be reached for a design defect; since this is a non-safety application, a robust design process cannot be assumed. RG 1.187 should add these points.

19. NEI 96-07 Appendix D Example 4-16 describes a replacement of analog transmitters that are part of the ESFAS with digital transmitters under 10 CFR 50.59 based on a qualitative assessment that concludes the likelihood of CCF due to a design defect is sufficiently low. However, RIS 2002-22 Supplement 1 does not permit the use of a qualitative assessment for ESFAS components. In addition, SRM SECY 93-087 and BTP 7-19 require AOOs and PAs in the UFSAR be re-analyzed with a concurrent CCF to demonstrate coping unless there is sufficient diversity or simplicity to preclude further consideration of a CCF due to a design defect.

    RG 1.187 should address this conflict between NEI 96-07 Appendix D and other regulatory guidance. The Standard Review Plan (NUREG-0800) includes transmitters in Section 7.3 for the ESFAS, and transmitters are covered within the scope of IEEE 603. Clearly the ESFAS cannot function without process measurements from transmitters. If the Staff does not consider transmitters part of the ESFAS, the basis should be explained in RG 1.187.

20. NEI 96-07 Appendix D Example 4-16 describes an analog design whose failure could affect only one of four feedwater valves and a proposed digital design whose failure could affect all four feedwater valves. The example states that this proposed design does not create the possibility for a malfunction of an SSC important to safety with a different result, because the existing loss of feedwater analysis assumed a failure of all four feedwater valves.

    Since the loss of all feedwater is a different malfunction, and far more safety significant, than loss of feedwater from one valve, the digital design clearly presents a more severe challenge to plant safety. Therefore, RG 1.187 should clarify that this is more than a minimal increase in the consequences of a malfunction of an SSC important to safety per 10 CFR 50.59(c)(2)(iv), or explain why it is not as discussed in Item 1, above.

    RG 1.187 should also clarify the conditions under which a licensee is permitted to first revise their accident analysis to address anticipated digital modifications (e.g. failure of all valves vs. one valve), so that they can subsequently conclude that the proposed digital design is bounded by the “existing” analysis.

21. NEI 96-07 Appendix D Example 4-21 describes the combining of previously separate control systems, Steam Bypass Control System (SBCS) and Pressurizer Pressure Control System (PPCS), into a single digital controller, and concludes that this does not create the possibility of a malfunction with a different result. This conclusion is reached based on two reasons, which both have inconsistencies; therefore, additional explanation is required:

    a. The evaluation states “In the Increased Main Steam Flow accident analysis, the pressurizer pressure control system is assumed to be in automatic and would attempt to mitigate the results of the accident.” Clearly, if the analysis credits mitigation by the PPCS, then mis-operation of the PPCS would aggravate this event.

    b. The evaluation states “regardless of the … mis-operation of the pressurizer pressure control system during the event, the malfunction of the pressurizer pressure control system would have no effect on this event”. This conclusion presumes a certain manner of “mis-operation” (i.e., no pressure control or fail as-is) which one cannot

do for CCF. This conclusion fails to recognize that the same design defect or random hardware failure within the controller that caused the SBCS valves to erroneously open could also cause the PPCS function in the same digital controller to erroneously close pressurizer spray valves and energize pressurizer heaters (i.e., erroneously increase pressure); this failure cannot be precluded without a detailed FMEA that considers other defensive measures. Even if the PPCS is not credited to mitigate the event, as would be the case for most accident analyses (I believe the statement in Example 4-21, discussed in item a above is actually incorrect), accident analyses do not consider a concurrent unrelated failure of other systems. Therefore, for the Main Steam Flow event, in the current analysis the SBCS is assumed to fail, but the PPCS is assumed to not fail in a manner that would aggravate the accident. The potential for a single malfunction (within the design basis) or a single design defect (beyond the design basis) to cause concurrent pressure increase by both the SBCS and PPCS is certainly a malfunction with a result that requires more analysis to determine its effect on the plant's critical safety functions.

RG 1.187 should correct the inconsistencies in this example or explain their bases.

22. NEI 96-07 Appendix D Example 4-22 describes replacement of solid-state cards in the reactor protection system (RPS) with digital cards. The example states that the likelihood of CCF is not sufficiently low. But these are safety cards; therefore, other regulatory requirements impose a robust design process. Therefore, in accordance with SRM SECY 93-087 and BTP 7-19 the likelihood of a CCF due to a design defect is low enough to consider the CCF a beyond design basis event; this supports a "sufficiently low likelihood" conclusion. However, RIS-2002-22 Supplement 1 precludes using a qualitative assessment for components of the RPS; therefore, the likelihood conclusion is irrelevant. RG 1.187 should clarify this inconsistency.

    Also, saying that a design defect could invalidate SFC compliance is incorrect. As clarified in BTP 7-19, a design defect is not a single failure. For most applications, SFC compliance is invalidated only when there is insufficient redundancy or insufficient independence between redundancies. RG 1.187 should correct this incorrect statement in this example.

23. NEI 96-07 Appendix D Example 4-23 describes replacement of safety related analog voltage regulators with safety related digital regulators. This example has the same incorrect statements regarding "sufficiently low likelihood" and SFC compliance as discussed above for Example 4-22. RG 1.87 should address these points.

24. NEI 96-07 Appendix D Example 4-24 describes replacement of analog pressurizer pressure transmitters and associated circuitry used to control the Low Temperature Overpressure Protection opening signal for the pressurizer Power Operated Relief Valve (PORV) with digital equipment. Since these are safety related components, this example has the same incorrect statements regarding "sufficiently low likelihood" as discussed above for Example 4-22. Regardless, this example fails to mention that these are components of the RPS, for

which RIS 2002-22 Supplement 1 does not permit a qualitative assessment. RG 1.87 should address both of these points.

25. NEI 96-07 Appendix D limits the discussion to only software CCF. However, RIS 2002-22 Supplement 1 addresses all sources of digital CCF; software CCF is just one example. Draft BTP 7-19 Revision 8 also addresses all sources of digital CCF. RG 1.187 should address this discrepancy between NEI 96-07 Appendix D and other regulatory guidance.

26. Several sections of NEI 96-07 Appendix D rely on a conclusion that the likelihood of a failure is sufficiently low. RG 1.187 should clarify that it is possible to conclude that the likelihood of a design defect is sufficiently low. But it is not technically possible to conclude that the likelihood of failure of a shared hardware resource (e.g., controller, network, touch screen) is sufficiently low. This is because hardware resources fail randomly and those random failures must be assumed to occur during the life of the plant.

    Without sufficient defensive measures, failure of a shared hardware resources can adversely affect multiple functions that were previously separate in the analog design. For example, (1) erroneous operation of multiple control functions can result in a transient (i.e., accident) of a different type, (2) erroneous asynchronous control rod movements can result in a transient (i.e., accident) of a different type.

    Therefore, RG 1.187 should clarify that the qualitative assessment may reach different likelihood conclusions for different failure sources.

27. The words “different result” appear in many sections of NEI 96-07 Appendix D, as well as in the main body of NEI 96-07. But there is no definition of these words in any of these sections. RG 1.187 should clarify that the "result" of concern is the impact on the critical safety functions of the plant; other interim results that may be different than previous results are not a concern for the 10 CFR 50.59 evaluation.

28. NEI 96-07 Appendix D Rev. 1 was published May 2020. NEI requested NRC endorsement in a letter dated May 13, 2020. Then NRC issued RG 1.187 Rev. 2 June 2020 with an effective date of July 7, 2020. The Staff should explain why there was no public comment period prior to the issuance of RG 1.187 Rev. 2.