NRR-DMPSPEm Resource

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Thursday, April 13, 2017 7:50 AM
To: Drake, Jason
Cc: Rahn, David; Holonich, Joseph; Morton, Wendell
Subject: [External_Sender] Recommendations and Comments on Staff Documents Issued in Conjunction with March 30, 2017 Public Meeting on CCF
Attachments: Draft Framework for Supplemental Qualitative Assessment Guidance for NEI 01-01 _KS.docx; Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01_KS.docx; Recommended Input for New RIS on CCF.docx; Recommendations Summary for New RIS on CCF.pptx

Jason,
I'm sending the files attached for Staff consideration regarding the documents made public by the staff for use in conjunction with the NRC public meeting held March 30, 2017. There are four attachments:

1. My comments on the "Draft Framework for Supplemental Qualitative Assessment Guidance for NEI 01-01".
2. My comments on the "Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01".
3. My "Recommended Input for New RIS on CCF". These are common questions that this RIS should answer.
4. My "Recommendations Summary for New RIS on CCF". This powerpoint slide summarizes the key points from Attachment 3 above.

Thank you for considering this input for the RIS on CCF. I would be happy to discuss any of these comments.

Ken

_____

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192

Hearing Identifier: NRR_DMPS
Email Number: 206

Mail Envelope Properties (00a901d2b44c$1e05daa0$5a118fe0$)

Subject: [External_Sender] Recommendations and Comments on Staff Documents Issued in Conjunction with March 30, 2017 Public Meeting on CCF
Sent Date: 4/13/2017 7:50:06 AM
Received Date: 4/13/2017 7:51:00 AM
From: Ken Scarola

Created By: KenScarola@NuclearAutomation.com

Recipients:
"Rahn, David" <David.Rahn@nrc.gov>
Tracking Status: None
"Holonich, Joseph" <Joseph.Holonich@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Drake, Jason" <Jason.Drake@nrc.gov>
Tracking Status: None

Post Office: NuclearAutomation.com

Files	**Size**	**Date & Time**
MESSAGE	906	4/13/2017 7:51:00 AM
Draft Framework for Supplemental Qualitative Assessment Guidance for NEI 01-01_KS.docx	50884	
Draft_RIS_to_Clarify_RIS_2002-22_Endorsement_of_NEI_01-01_KS.docx	40165	
Recommended Input for New RIS on CCF.docx	26273	
Recommendations Summary for New RIS on CCF.pptx	47173	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

DRAFT - Qualitative Assessment Framework

Introduction:

This draft framework outlines the NRC staff's initial thoughts on providing guidance for an improved qualitative assessment process that takes into account differences in the level of evidence needed for SSCs of varying safety significance. The NRC staff recognizes that greater clarity in guidance for documenting the technical basis supporting proposed digital I&C modifications to SSCs of lower safety significance under 10 CFR 50.59 is needed.

The term "qualitative assessment" is referenced in both NEI 96-07 (as endorsed by RG 1.187) and NEI 01-01 (as endorsed by RIS 2002-22). For example, Section 5.3.1 of NEI 01-01 states, in part, that "….reasonable assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features". Reliance on high quality development or design processes alone may not always serve as a sufficient qualitative argument. The intent of this supplemental guidance is to enable licensees to ensure that adequate qualitative arguments are presented consistently, through an evaluation of all appropriate qualitative evidence available[As I have commented before: Qualitative evidence is sufficient to conclude that the likelihood of a CCF is significantly less than that of a single failure, thereby concluding (1) the CCF is beyond design basis and (2) enabling the use of best estimate methods and acceptance criteria for the CCF malfunction result analysis. But deterministic evidence (e.g., 100% testability, internal diversity) is needed to conclude that a CCF is not credible, thereby precluding any further consideration of the CCF (i.e., no need for a CCF malfunction result analysis). If you allow qualitative evidence alone to reach a CCF not credible conclusion then you are in conflict with the SRM to SECY 93-087, BTP 7-19 and NUREG 6303.] , and the use of a consistent format and rationale by which the evidence supports the conclusions needed to respond to the criteria within a 10 CFR 50.59 evaluation.

Purpose:

This enclosure to RIS 2017-XX provides guidance for performing and documenting qualitative assessments developed in support of 10 CFR 50.59 evaluations of proposed digital I&C plant modifications. Such qualitative assessments are needed to document the technical bases for concluding whether there is reasonable assurance that any failures or failure modes due to the implementation of the proposed digital I&C modification are as likely, or significantly less likely to occur as failures and failure modes already considered in the plant safety analysis [I agree with this statement, because this statement does not allow the use of qualitative assessments to reach a CCF not credible conclusion; it only allows the use of qualitative assessments to reach a conclusion of 'significantly less likely…' which would still require a CCF malfunction result analysis.]. This determination is needed because a decision must be made as to whether the proposed change meets the evaluation criteria in 10 CFR 50.59(c)(2) without prior NRC staff approval, or whether a license amendment request (LAR) will be required [This statement implies that this analysis to determine the likelihood of the CCF (i.e., a CCF susceptibility analysis) is the only determination needed for the 50.59 evaluation. But this is not correct,

because if the CCF is credible (i.e., either case above – "as likely", or "significantly less likely" but still credible), then additional analysis of the CCF malfunction result is needed to answer 50.59 Questions 5 and 6.].

The qualitative assessment is needed to support the process for making the following conclusions:

- The activity does not result in more than a minimal increase in the likelihood of failure of an SSC important to safety to perform its intended design functions as described in the UFSAR or credited in the plant safety analyses.
- For activities that could introduce a potential CCF, there is reasonable assurance that the likelihood of a CCF is much lower than the likelihood of failures that are already considered in the current plant design basis described in the UFSAR.
- For activities that could introduce a potential CCF, there reasonable assurance that the likelihood of a CCF is comparable (or less) to other CCFs that are not considered in the UFSAR.

For activities that introduce a potential CCF that meets all of the above conditions, CCF would not be considered in the UFSAR. [This is somewhat confusing, because if you meet bullet 3, then you also meet bullet 2. It would be clearer if bullet 2 is omitted from this section.]

For activities that introduce a potential CCF that do not meet all of the above conditions, the CCF would need to become part of the design basis [I agree, if you don't meet bullet 1. But if you meet bullets 1 and 2 (but not 3), then the CCF can be considered beyond design basis. This would not require the CCF malfunction to be added to the Chapter 15 safety analysis, but it would require additional CCF malfunction results analysis to determine the answers to 50.59 Questions 5 and 6.]. The licensee would be required to update the UFSAR to reflect the revised design basis accounting for the CCF and update the UFSAR safety analyses that must be revised to account for the CCF using design basis methods and acceptance criteria, as currently used in the abnormal operating occurrences and postulated accidents of the UFSAR. NRC staff approval of such a change (via 10 CFR 50.90) would be required.

This qualitative assessment clarification is intended to supplement, rather than replace the guidance provided for qualitative assessments that are described in NEI 01-01, Sections 4.4 , 5.1, 5.3 as well as Appendix A (Items Nos. 2(i) & 6(b)).

Qualitative Assessment Scope:

The qualitative assessment process may be applied to any proposed digital I&C plant modifications to safety and non-safety systems. However, at this time, it is not intended for this RIS to apply to reactor protection or essential safety feature initiation functions. Consistent with the staff's endorsement of NEI 01-01 in RIS 2002-22, it is likely that when applying NEI 01-01 for completing the 10 CFR 50.59 evaluation process for proposed changes to reactor protection

and engineered safeguards initiation systems, it will be found that a license amendment request will be necessary to make the change.

Qualitative Arguments and Documentation: This Qualitative Assessment clarification highlights four general categories of proposed design-related characteristics, each of which need to be evaluated to formulate effective qualitative arguments deemed sufficient to address the questions posed in the "Purpose" section above. The staff finds that an evaluation of the degree to which each category of design characteristic has been addressed and weighed collectively in the design is adequate to support arguments within acceptable technical bases for responding to the 50.59 evaluation questions. These areas should be evaluated in conjunction with the supplemental questions provided in NEI 01-01, Appendix A. Those four general categories are:

- Design Attributes of the proposed modification that serve to prevent or limit failures from occurring~~, or that mitigate the consequences of such possible failures~~ [To avoid confusion, design attributes internal to and external to the target modification should be clearly distinguished. When the CCF is not prevented by internal design attributes, the CCF malfunction result must be analyzed. Design attributes external to the target modification can be credited in that CCF malfunction result analysis to mitigate the consequences of the CCF.]. Evidence of design attributes supporting arguments for the high reliability and dependability of the proposed modification should be described. [Design attributes are the 'deterministic evidence' that I discussed in my first comment. It is confusing to lump these together with qualitative evidence, because qualitative evidence requires subjective judgement, design attributes are either there or they are not (this is not subjective).]

- Quality Processes employed in the development of the proposed modification, including software development, hardware and software integration processes, hardware design, and validation and testing processes that have been incorporated into the development process.

- Defense in Depth: Evidence that the proposed design incorporates both internal and external layers of defense against potential failures [This is very confusing, because external layers do not prevent or limit a CCF; they can be credited to mitigate the CCF when it occurs.] of the modified I&C system or component that could result in modes of failure not already analyzed in the UFSAR or result in the initiation of a design basis Anticipated Operational Occurrence (AOO) or Postulated Accident (PA), or new AOOs or PAs that have not been previously analyzed [This is silent on the issue of 'bounded'. It is very important that this RIS provide sufficient guidance to allow a digital modification to be implemented under 50.59, if that mod results in a previously unanalyzed CCF malfunction that is still bounded by previous analyses. If you don't allow this, you will bring the use of distributed control system technology to an end, because new malfunctions are almost always credible (but in most cases can be demonstrated to be bounded).

- Operating Experience: Evidence that the proposed system or component modification employs equipment configured in the same manner [this is important because there is a lot of operating experience that is not applicable] with significant operating history in nuclear power plant applications or non-nuclear applications with comparable risk-significant performance requirements, and the suppliers of such equipment incorporate quality processes such as continual process improvement, incorporation of lessons learned, etc. [I agree this is a qualitative attribute.]

These categories are not mutually exclusive and may overlap in certain areas. Adequate qualitative arguments for systems of varying safety significance should address the degree to which the proposed modification has addressed each of the above categories. It's the staff's expectation that ALL of these categories be addressed [I disagree. For a specific source of CCF (e.g., single random hardware failure), if the modification contains sufficient deterministic attributes to reach a CCF not credible conclusion, there is no reason to assess qualitative attributes. It is much more important to say that all applicable sources of CCF need to be systematically assessed. When doing this systematic assessment of all applicable sources of CCF, it is likely that most of the areas above will be assessed. However, if a CCF not credible conclusion is reached for all applicable sources of CCF, then a defense-in-depth assessment to evaluation the capability to mitigate the CCF is not required.] to the degree possible, and that the uncertainty to the degree to which the proposed modification has or has addressed each category is identified. **See Table 1**.

Documentation:

The qualitative assessment guidance also describes the areas of consideration that should be documented in order to present a consistent explanation of likelihood arguments supporting technical bases for responding to 50.59 evaluation questions. It's the staff's expectation that ALL of these categories be addressed to the degree possible. **See Table 2**. This table provides the 'process flow' that should be followed in terms of the structure of the qualitative assessment presentation as well as specific steps that should be addressed in the process.

Table 1 - Qualitative Argument Areas	
Topical Area	Description
Design Attributes	• Design Criteria [Criteria is not an attribute. The evaluation must confirm design attributes exist to meet the criteria.]– For example: Diversity (if applicable), Independence, Redundancy • Inherent Design Features for software, hardware or architectural/network – For example: external watchdog timers, isolation devices, segmentation, self-testing and self-diagnostic features • Sufficiently Simple (i.e. enabling 100% testing) • Unlikely series of events – For example, the evaluation of a given DI&C modification would necessarily have to postulate multiple independent random failures in order to arrive at a state in which a CCF is possible. • Failure state always known to be safe NOTE: It is the staff's expectation that potential triggers, and the basis for concluding those triggers would not be concurrent and therefore not cause a ~~of~~ CCF in an SSC to be modified, be specifically identified and addressed in terms of design attributes presented as an argument for demonstrating likelihoods of CCF being as unlikely as other CCFs not considered in a plant's safety analyses. [I'm very happy to see that the Staff is embracing non-concurrent triggers.]
Quality	• Compliance with industry codes and standards - It is the expectation that for non-NRC endorsed codes and standards, the licensee must provide an explanation for why use of the particular non-endorsed standard(s) is acceptable. • Use of Appendix B vendors, or if not Appendix B, which generally accepted industrial quality program applies • Environmental qualification (e.g. EMI/RFI, Seismic) • Development Process rigor
Defense-In-Depth	• Coping measures • Operator Intervention/administrative controls and sufficient time to respond available • Physical restrictions external to the DI&C modification (e.g. mechanical restrictions on control valve movements) [See previous comments. We should be distinguishing deterministic and qualitative measures that prevent or limit a CCF (internal to the target digital modification), from the deterministic measures credited to cope with a CCF when it occurs (external to the target digital modification).
Operating Experience	• Wide range of operating history with the same configurations or configurations that bound the targeted modification. • History of lessons learned from field experience addressed in the design • High volume production usage in different applications- Note that for software, the concern is centered on lower volume, custom or user-configurable software applications. High volume commercial products used in different applications provides a higher likelihood of resolution of potential deficiencies.

Table 2 - Qualitative Assessment Documentation Structure[1]	
Topical Area	Description
Identification	Describe the full extent of the SSC(s) to be modified—boundaries of the design change.
Step 1 - Design Function	• What is the entirety of the design function(s) of the upgraded component(s) within the context of the plant system, subsystem, etc. • Describe what functions were covered by the previously installed equipment, and how those same functions will be accomplished by the modified design. Also describe any new functions to be performed by the modified design that were not part of the original design. • Assumptions and conditions associated with the expected safety or power generation functions
Step 2 - Failure Modes	What are they for the upgraded component(s), and why they are different or the same as previously installed? [You can't identify failure modes without first conducting a CCF susceptibility analysis. The failure modes are quite different if a CCF is credible vs. not credible. The failure modes for a credible CCF are quite different if there are limiting measures vs. no limiting mearsures.]
Step 3 - Consequences of their Failure	In terms of existing safety analysis or in terms of an enhanced safety analysis, what are the consequences of any postulated single failures or CCF of modified SSC(s)? [Why would you postulate a CCF and determine its consequences, if the CCF is not credible. The process should conduct a CCF susceptibility analysis first (to determine CCF credibility), followed by a CCF malfunction results analysis for all CCFs determined to be credible.]
Step 4 - Claims and sub-claims	What are the assertions being made: [Why would you make any assertions with first conducting a CCF susceptibility analysis.] • The digital component is at least as reliable, dependable, etc, as the device previously installed? • Its postulated CCF likelihood is significantly lower than single failures considered in the UFSAR or comparable to CCFs that are not considered in the safety analyses (e.g. design flaws, maintenance errors)? ALL claims should fully address the consequences of a postulated CCF of the SSC(s) to be modified [Why would you postulate a CCF and determine its consequences, if the CCF is not credible. The process should conduct a CCF susceptibility analysis first (to determine CCF credibility), followed by a CCF malfunction results analysis for all CCFs determined to be credible.] and the likelihood status of postulated CCF. The qualitative assessment will not determine the absolute likelihood of failure in terms of failures-per-operating hour.

[1] Establishes structure specifically for qualitative assessment to supplement guidance provided in NEI 01-01 Appendix B.

Step 5 - Evidence (Qualitative Arguments of likelihood)	Should support each of the claims (e.g. evidence of the 4 qualitative assessment arguments) including codes and standards applied, qualification for the environment (e.g., seismic, EMI/RFI, ambient temperature, heat contribution, etc.) Quality Processes employed in the development (V&V processes used as evident in a traceability matrix, QA documentation, unit test and system test results, etc.,), defense-in-depth (e.g. inherent internal diversity, manual back-up capability, etc.), and Operating History (e.g., platform used in tens of thousands of applications worldwide, etc. with minimal failure history, etc.) The level of evidence provided should be commensurate to the safety significance of the SSC(s) to be modified. [This needs to be clarified, because it sounds like a risk informed assessment; I don't think that is the intent. I prefer to say that there is a graded approach in that when assessing deterministic and qualitative attributes, control systems are not expected to comply with the same codes and standards as safety systems.]
Step 6 - Rationale	Stating why the claim can be considered to be true, based on the evidence described. Include arguments both supporting and detracting (pros and cons) so that the 10 CFR 50.59 user of the QA has a feel for the relative magnitude of the uncertainties are associated with each claim is evident. Justification supporting the use of the rationale. [This step seems to unnecessarily duplicate the Evidence and Consequence steps above. You either have sufficient evidence to conclude that a CCF is less likely, or you don't. For a credible CCF the consequences are either bounded or they are not. This step just adds more uncertainty and more potential for inconsistent application of the process across the industry.]
Step 7 - Conclusion	Apply the results of the qualitative assessment to respond to 50.59 evaluation questions. [It is still not clear to me how you correlate the assessments above with the 50.59 questions.]

Consequences of the Failure (Evidence Determination):

The level of evidence needed to be provided in the qualitative assessment should be commensurate with the consequences of the postulated failure of the SSC to be modified. For example, the higher the safety significance of the SSC being modified, the more evidence is necessary to be presented and evaluated [Again this sounds like a risk informed assessment. We should be discussing only a graded approach for defensive attributes, as commented above. There is no place for a risk informed assessment in a 50.59 evaluation (at least today).].

Consideration of what is the impact of a failure on the ability of the plant to continue to accomplish critical plant safety functions may provide an indication of the level of evidence needed to support effective qualitative assessments [You are completely missing the problem of control system CCFs potentially challenging critical safety functions in a manner that was not previously analyzed. This is an equal threat to plant safety.]. Critical safety functions[2] (CSFs)[3] are those safety functions that are essential to prevent direct and immediate threat to the health and safety of the public. These are accomplishing or maintaining of:

[2] Source: IEEE Std. 497-2002 as endorsed by RG 1.97, Revision 4.
[3] For AP1000, critical safety functions are Subcriticality – Core Cooling – Heat Sink – Integrity – Containment - Inventory

- Reactivity control
- Reactor core cooling
- Reactor coolant system integrity
- Primary reactor containment integrity
- Radioactive effluent control

Additional questions that could be asked include based upon consideration of CSFs include: [None of the question below should be asked if the CCF is not credible. Most of the questions are not relevant if the CCF malfunction result is bounded.]

- Is there an immediate safety impact to the plant?
- Is there a longer term safety impact if condition is not repaired/addressed/adequately coped with?
- Is the CCF/malfunction detectable by operators? If so, are there validated procedural actions in place (or proposed as part of the plant modification) to enable plant operators to identify the malfunction and take appropriate remedial action? [This question is relevant only if operator action is credited to either prevent the CCF or to cope with a credible CCF. Otherwise there is no reason to ask this question.]
- Postulate the failure (CCF) concurrent with an AOO/PA in the safety analyses: What's the impact on plant safety? [This should be asked only for a credible CCF that can go undetected for long periods of time (as for many CCFs in safety systems, because they are in standby operation). It does not need to be asked for a CCF that is immediately detectable (as for most CCFs in control systems, because they are in continuous operation).]

Example Applications:

In general, potential impacts on the plant critical safety functions (CSFs) require a greater level of evidence to be presented and weighed qualitatively than impacts on non-CSFs [If there is no potential challenge to CSFs then there is no need for any CCF consideration. This is why the first question in NEI 16-16 is "Is the equipment an initiator [of a transient] or credited for event mitigation" . For example, using CSFs to assess risk significance, and comparing them against proposed modifications could yield the following results[4]:

- For RPS/ESF control and actuating logic modifications – (Considered out of scope for this guidance)
- EDG Voltage Regulators – Impacts multiple critical safety functions; therefore, one could do under 50.59 [this conclusion is unrelated to the first phrase of this sentence] but requires significantly greater level of evidence.

Main Control Room HVAC Safety Chillers – Do not appear to have any appreciable or immediate effects on the CSFs above, therefore level of evidence could be lower [Chillers are a support system credited to keep control systems, and safety I&C systems within their

[4] Additional input necessary if more granularity is needed

qualification envelope (thereby preventing CCF of these systems). Chillers are also credited to maintain MCR habitability for plant operators. I&C systems and operators are both credited to avoid challenges to CSFs or maintain CSFs. Therefore, failure of a Chiller threatens CSFs.].

UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NEW REACTORS
WASHINGTON, D.C. 20555-0001

July 2017

NRC REGULATORY ISSUE SUMMARY 2017-XX
UPDATE TO THE STAFF ENDORSEMENT ON THE USE OF
EPRI/NEI JOINT TASK FORCE REPORT,
"GUIDELINE ON LICENSING DIGITAL UPGRADES: EPRI TR-102348,
REVISION 1, NEI 01-01: A REVISION OF EPRI TR-102348 TO
REFLECT CHANGES TO THE 10 CFR 50.59 RULE"
(REPORT PREVIOUSLY ENDORSED WITHIN RIS 2002-22)

ADDRESSEES

All holders and applicants for power reactor operating licenses or construction permits under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," except those who have permanently ceased operations and have certified that fuel has been permanently removed from the reactor vessel, and all holders of, and applicants for, a power reactor combined license, standard design approval, or manufacturing license, and all applicants for a standard design certification, under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing a clarification to the staff's endorsement of the Electric Power Research Institute (EPRI)/Nuclear Energy Institute (NEI) Joint Task Force report entitled, "Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule," (hereinafter referred to as "NEI 01-01.") In RIS 2002-22 (ADAMS Accession Number ML023160044), the staff previously endorsed the use of the NEI 01-01 document as guidance in designing and implementing digital upgrades to instrumentation and control systems a) to ensure that digital upgrade regulatory and technical issues are adequately addressed, b) to provide criteria for performing the 10 CFR 50.59 evaluation and, if necessary, c) to identify when licensees need to submit a License Amendment Request under 10 CFR 50.90.

Specifically, within this RIS, the staff clarifies the applicability of its endorsement for proposed system and component upgrades to systems that initiate and complete design basis preventative or mitigative safety functions credited in the plant safety analyses, versus proposed

system and component upgrades to systems that support the successful operation of those systems or perform non-safety related functions. This RIS also provides clarification of the staff's endorsement of NEI 01-01 regarding the use of criteria stated within NEI 01-01 to address the performance of plant safety evaluations as outlined in 10 CFR Part 50.59, "Changes, tests, and experiments." Specifically, the staff clarifies its endorsement of the NEI 01-01 guidance for performing adequate qualitative [Based on your framework document, you are also requiring deterministic assessments, not just qualitative assessment. I agree with this.] assessments of proposed digital I&C changes within the scope of the endorsement. The documentation of appropriately prepared qualitative assessments is considered an acceptable means for supporting the development of adequate responses to safety evaluation criteria required to be addressed under 10 CFR Part 50.59(c)(2)(i) through (viii). The attachment to this RIS and its enclosures document the staff's clarified basis for continuing its endorsement of NEI 01-01.

Where potential conflicts may exist between the contents of this RIS and that of RIS 2002-22 regarding acceptable guidance for performing 10 CFR 50.59 evaluations, the provisions within this RIS shall supersede those provided within RIS 2002-22.

It is intended that this RIS provide clarity of the staff's endorsement of NEI 01-01 for use in future digital I&C changes to licensed nuclear power plants. No backfitting is intended or approved in connection with the issuance of this RIS.

This RIS requires no action or written response on the part of an addressee.

BACKGROUND INFORMATION

By letter dated March 15, 2002, NEI submitted EPRI TR-102348, Revision 1 (NEI 01-01) for staff review. This report replaced the original version of EPRI TR-102348, dated December 1993, which the NRC endorsed in Generic Letter (GL) 95-02, "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades,' in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59," dated April 26, 1995. In 2002, the staff issued Regulatory Issue Summary (RIS) 2002-22 to notify addressees that the NRC had reviewed NEI 01-01: "A Revision of EPRI TR-102348 To Reflect Changes to the 10 CFR 50.59 Rule," and was endorsing the report for use as guidance in designing and implementing digital upgrades to nuclear power plant instrumentation and control systems.

Following the staff's 2002 endorsement of NEI 01-01, holders of construction permits, standard design certifications, and operating licenses have been using this guidance, as endorsed, in support of the performance of digital I&C-related design modifications, in conjunction with Regulatory Guide (RG) 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments," dated November 2000, which endorsed NEI 96-07, "Guidelines for 10 CFR 50.59 Evaluations," Revision 1, dated November 2000.

Subsequent to the issuance of the staff's 2002 endorsement of NEI 01-01, NRC inspections of plant digital I&C modifications performed under 10 CFR 50.59 have revealed that some licensees have encountered difficulties in addressing the guidance and acceptance criteria within other applicable technical guidance documents while conforming to the endorsed guidance within NEI 01-01 and subsequently performing effective safety evaluations as required by 10 CFR 50.59, as amended. NRC staff inspections of design modifications performed by some licensees have also revealed weaknesses in the adequacy of documentation specifying the technical basis regarding licensee conclusions that the safety evaluation criteria within 10 CFR 50.59 are being met in the proposed modernization project, and that no prior NRC staff review (via evaluation of a license amendment request) is required.

For example, licensees encounter difficulty addressing the staff review acceptance criteria regarding the adequacy of diversity and defense-in-depth (D3) analyses to address the potential for common cause failure, as outlined within NUREG-0800 Standard Review Plan Chapter 7, Branch Technical Position BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Revisions 6 and 7) when they attempt to apply them for use in lower safety-significant I&C systems under the 10 CFR 50.59 design change evaluation process, and subsequently provide an effective response to 10 CFR 50.59(c)(2) safety evaluation criteria (i) through (viii). As another example, staff inspectors have identified cases where licensee documentation supporting the technical basis for conclusions reached in 10 CFR 50.59 evaluations is unclear as to which applicable industry codes and standards were followed, and which specific aspects of those standards provides the basis for concluding the 10 CFR 50.59 safety evaluation criteria are satisfied.

Section 5.2 of NEI 01-01 provides guidance regarding the need for D3 analyses to be completed for key reactor protection and engineered safeguards features systems. Based on regulatory experience with the use of NEI 01-01, the staff has identified that the applicability of this guidance to certain portions of plant systems needs to be clarified. (The staff notes that guidance for assessing the diversity and defense-in-depth of digital I&C systems was originally developed for use by NRC staff in their review of high safety-significant I&C systems such as reactor protection systems and engineered safeguards systems in conjunction with its evaluation of license applications and amendments, rather than for use in performing design changes for less safety significant systems under 10 CFR 50.59.)

In an effort to remedy the difficulties described above, the staff, NEI, and industry representatives have been meeting to discuss these issues and are working to develop revised guidance for incorporating digital I&C systems under the 10 CFR 50.59 process, and new guidance for addressing the potential for digital system related common cause failures. This effort is part of a broader effort to modernize the current regulatory infrastructure to efficiently address risks associated with the introduction of digital technology for nuclear power plant applications that have potential impact on plant safety. The staff's plan for accomplishing this regulatory modernization, is outlined in the NRC "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ADAMS Accession Number ML17XXXXXXX), including the planned schedule for completion of key infrastructure

improvements. As part of this plan, however, the staff and stakeholders have identified an immediate need for clarification of the staff's guidance for performing adequate safety evaluations of proposed digital I&C modernization projects being implemented under the 10 CFR 50.59 design change process.

In this RIS, the staff is clarifying the applicability its previous endorsement of NEI 01-01 to RPS and ESF initiation, ~~and~~ completion and manual control functions [Several Ch. 15 events credit manual operator actions.], versus its applicability to safety support systems and non-safety systems. The staff is also clarifying its position with regard to acceptable methods for applying the guidance in NEI 01-01 to digital I&C modifications performed under the 10 CFR 50.59 process, in conjunction with the use of the staff's other technical guidance documents. The staff's previous endorsement is also being augmented to provide the staff's position on acceptable methods for developing and documenting qualitative assessments of the proposed digital I&C design change to serve as a technical basis for responding to the eight safety criteria that must be evaluated within 10 CFR 50.59(c)(2)(i) through (viii).

ISSUE SUMMARY

The revision of 10 CFR 50.59 effective on March 13, 2001, used evaluation criteria that are difficult to apply to software-based I&C systems. Therefore, the EPRI/NEI Joint Task Force included relevant supplemental guidance in developing NEI 01-01, and provided supplemental guidance on the use of NEI 96-07 for evaluating the safety of proposed digital upgrades to I&C systems.

In its 2001-2002 review of NEI 01-01, the staff concluded that the document provides suitable guidance both for designing a digital I&C replacement and for determining whether it can be implemented under 10 CFR 50.59 without prior staff approval. Nevertheless, the staff's evaluation of the report attached to RIS 2001-22 provided statements that qualify the NRC staff's endorsement, and provided staff positions on several aspects of the design and licensing processes. In particular, the staff noted that when using the submittal as guidance for the analysis of digital modifications of some safety-significant systems such as the reactor protection system and engineered safety features actuation systems, "it is likely these digital modifications will require staff review (i.e., via a license amendment under 10 CFR 50.90) when the 10 CFR 50.59 criteria are applied and evaluated."

It is the intent of this RIS to provide further clarification of the staff's endorsement stated in RIS 2002-22 with regard to the endorsed scope of its applicability, and the methods licensees can use to document its assessments of the design features and capabilities of proposed digital I&C changes to licensed facilities, to facilitate the development of adequate responses to the 10 CFR 50.59 criteria that must be evaluated for any facility changes proposed to be conducted under 10 CFR 50.59. For example, the staff's guidance for performing adequate qualitative assessments in Enclosure 2 of this RIS is not intended for use in making proposed changes to logic systems forming a part of reactor protection systems and engineered safety feature

systems initiation, completion and manual control [Again credited manual actions are as safety significant as the ESFAS, sometimes more so.] systems, for which a license amendment request is needed. In addition, this RIS provides clarification of the endorsement in other areas where recent inspections have revealed inconsistencies in licensee adoption of guidance within NEI 01-01.

Changes proposed under 10 CFR 50.59

NEI 01-01 contains several references to key sections within NEI 96-07, "Guidelines for 10 CFR 50.59 Evaluations," Revision 1 (November 2000), an industry guidance document that is endorsed within Regulatory Guide (RG) 1.187, "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments." When followed properly while implementing a proposed facility design change, NEI 96-07 provides for the use of qualitative assessments and qualitative engineering judgment and/or industry precedent when addressing whether the frequency of ~~accidents~~ malfunctions occurring would be more than minimally increased, or whether a possibility for a malfunction of a system or component important to safety has been introduced that could alter the conclusions of the safety analysis. Guidance within NEI 96-07 states that normally, the determination of ~~an accident~~ a malfunction [Question 2 is about malfunctions, not accidents] frequency increase is based upon a qualitative assessment using engineering evaluations consistent with the UFSAR analysis assumptions. However, a plant-specific accident frequency calculation or PRA may be used as one of the tools for evaluating the effects of a proposed activity in a quantitative sense. Also, "reasonable engineering practices, engineering judgment and PRA techniques, as appropriate," should be used in determining whether the frequency of occurrence of ~~an accident~~a malfunction would more than minimally increase as a result of implementing a proposed activity. The effect of a proposed activity on the frequency of ~~an accident~~a malfunction must be "discernable and attributable" to the proposed activity in order to exceed the "more than minimal increase" standard. This concept was endorsed in RG 1.187, along with the endorsement of the balance of the NEI 96-07, Revision 1 document.

NEI 01-01 provides a failure analysis-based and D3 analysis-based approach to manage risk that encompasses digital-specific issues and other possible failure causes, addressing both according to their potential effects at the system level. This RIS clarifies the staff's previous endorsement regarding the need for performance of D3 evaluations of potential digital I&C upgrades to RPS and ESF systems to confirm adequate diversity exists, in accordance with regulatory requirements and NEI 96-07 guidance, as well as the performance of defense-in-depth (D2) assessments of safety support systems and non-safety systems [You are introducing a completely new concept here that is not supported by your framework document. As I have commented many times, there are two parts to a D3 analysis (1) an assessment of CCF vulnerability (we call this a CCF susceptibility analysis) and (2) an assessment of the plant's ability to cope with a CCF, when a CCF is credible (we call this a CCF malfunction results analysis). Both of these analyses are needed even for control systems and support systems.

This is consistent with your framework document]. The clarified endorsement in this RIS identifies important design attributes and quality measures [I just want to point out that here you distinguish design attributes from quality measures. This distinction should be made everywhere, because qualitative measures alone are not sufficient to reach a conclusion that a CCF is not credible or to reach a conclusion that the likelihood of CCF is significantly less than a single failure.] that, if applied appropriately, could be considered as adequate to demonstrate a sufficient reduction in uncertainty when performing qualitative assessments of likelihood of occurrence of a potential CCF for such lower-safety significant digital I&C proposed upgrades. Whereas the guidance in NEI 01-01 provides a "road map" to relevant standards and other sources of detailed guidance, the clarified endorsement of NEI 01-01 within this RIS identifies how the potential effectiveness of the design features and quality measures that are applied to the proposed design using such standards and guidance should be described and evaluated within licensee documentation supporting any conclusions that a reduction in uncertainty could be credited.

NRC inspections of plant modifications recently implemented or proposed have uncovered inconsistencies and weaknesses in the documentation of digital upgrade technical and safety evaluations performed by licensees. These specific evaluations have not included adequate documentation of the licensee's technical basis as to why it may be concluded that a particular plant design, once implemented, will not result in more than a minimal increase in the frequency of occurrence of an accident (10 CFR 50.59(c)(2)(i)) [This RIS should make it clear that unless there is an I&C malfunction there can be no accident caused by an I&C system. Therefore, for I&C systems it is sufficient to refer to Question 2 when answering Question 1.], or more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety (10 CFR 50.59(c)(2)(ii)) [This RIS should make it clear that unless a CCF is as likely as a single failure, the contribution of a CCF to malfunction frequency is negligible. Therefore, to answer this question licensees must assess the likelihood of single failures, not CCFs.]. A similar weakness was found in the manner in which licensees document the technical basis as to why a particular proposed modification will not create a possibility for an accident of a different type (10 CFR 50.59(c)(2)(v)), and why the proposed modification will not create a possibility for a malfunction of an SSC important to safety with a different result (10 CFR 50.59(c)(2)(vi)) [This RIS should make it clear that for Questions 5 and 6 a bounded plant-level end-result is not a different type of accident and not a malfunction with a different result. The distinction in 'bounded' criteria (i.e., analysis methods and acceptance criteria) must be explained for CCFs that are within the design basis and CCFs that are beyond design basis.] .

To remedy this, the staff has included within Enclosure 2 of this clarified endorsement of NEI 01-01, its position on the minimum content, rationale, and evaluation factors that must be addressed and evaluated within licensee-developed qualitative assessments that serve as input to developing responses to the 10 CFR 50.59 safety evaluation criteria. Specifically, the guidance within Enclosure 2 describes the staff expectations for such qualitative assessments to document an adequate technical basis for conclusions that are made regarding the relative likelihood of failure of the proposed digital I&C modification, based on evidence demonstrating

how adequate design measures, quality processes, layers of defense, and operating experience were considered to contribute to such likelihood of failure.

Clarification of staff endorsement of NEI 01-01 to address 12 concerns regarding the interpretation of specific provisions within NEI 01-01

On November 5, 2013, the NRC issued a letter (ADAMS Accession No. ML13298A787) to NEI summarizing 11 NRC staff concerns regarding inconsistent interpretation of provisions within the guidance of NEI 01-01. On October 9, 2014, the NRC issued a meeting summary (ADAMS Accession No. ML14255A059) that identified a 12th concern. Within this RIS, the staff considers the concerns regarding adequate means for addressing the evaluation criteria in 10 CFR 50.59 to be resolved for safety support systems and non-safety systems. The remaining concerns that are not addressed here, will be addressed as part of the staff's evaluations for possible endorsement of Appendix D to NEI 96-07 addressing 10 CFR 50.59 processes, and new NEI guidance NEI 16-16, now being developed to address common cause failure of digital systems, as described within the NRC Digital I&C Integrated Action Plan, as summarized in SECY 17-XXXX. (ADAMS Accession Number ML17XXXXXXXX.)

Recommended Input for New RIS on CCF

The following questions, which are commonly asked by industry engineers, should be clearly answered in this RIS.

1. Why does the credibility of a CCF need to be considered?

   When a CCF is credible, the component level, system level and/or plant level effect of that CCF must be assessed to determine if the CCF results in a plant level end result that is bounded by previous plant analysis or a new unbounded condition exists that requires new analysis. The plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF (e.g., DNBR, pressure boundary analytical limits).

2. For which digital devices does the credibility of a CCF need to be considered?

   Digital devices offer the potential for increased design complexity compared to their analog predecessors, including control (and potential failure) of multiple plant components which were traditionally controlled by separate analog devices (i.e., a CCF). This design complexity was very difficult to achieve, hence typically not attempted when analog technology was employed; therefore, only very specific CCFs were considered in the original design basis of most operating plants (e.g., loss of all feedwater, ATWS, SBO).

   Digital systems typically integrate functions and/or controlled plant components that were separately implemented in analog systems. This integration occurs either (1) directly in the same digital device, (2) indirectly through interconnection of multiple digital devices using digital data communication interfaces and/or common video display units (VDU), or (3) indirectly through the use of common digital designs in independent digital devices. This integration introduces new sources of CCF that if not prevented can adversely affect more plant components (i.e., a CCF) than their analog predecessor, which can result in unanalyzed plant transients.

   When any digital technology is employed (e.g., software, FPGA, CPLD), the potential for a failure that affects multiple plant components (i.e., a CCF) should be considered for all plant components that (1) can cause a plant transient, or (2) are credited for mitigating plant transients either directly or as an auxiliary safety support function. This potential should be assessed through

a documented CCF susceptibility analysis, which is a systematic evaluation of credible CCF sources (i.e., a single random hardware failure, environmental conditions and a design defect) and the defensive measures included in the design to prevent a CCF from those sources.

Plant components controlled by an embedded digital device (EDD) have potential CCF vulnerabilities just like plant components controlled by any other digital device. Therefore, a documented CCF susceptibility analysis is needed. Depending on the simplicity of the EDD, that analysis may be able to credit the testing conducted for the EDD and supporting analysis, to reach a conclusion that a CCF is not credible; this is discussed in Item 3b below.

3. What criteria are considered when determining the credibility of a CCF?

   Because a credible CCF can put the plant in an unanalyzed condition that may be unsafe, only deterministic criteria should be used in determining if a CCF is credible or not. Deterministic criteria should be used, because these criteria do not require subjective judgements for such an important issue essential to plant safety. Deterministic criteria are design attributes such as (1) separate communication processors and function processors, as described in ISG-04, to ensure a function processor is not adversely affected by a digital communication data storm, or (2) testability or internal diversity, for prevention of a CCF due to a design defect.

   Additional examples of deterministic criteria that can be used to reach a CCF not credible conclusion are as follows:

   a. A design defect in a digital device can affect multiple plant components controlled by a single digital device or controlled by multiple independent digital devices, when that same design is shared among those digital devices. Despite the presence of common design elements (e.g., operating system, function blocks) within multiple independent digital devices, internal diversity within the configuration of those common design elements (e.g., different cycle times, different application software, different I/O and communication interfaces, different operating modes) can be credited in reaching a conclusion that a CCF of those independent digital devices (and the multiple plant components that they control) is not credible, if a triggered malfunction

in one digital device is self-announcing; therefore, the design defect is correctable before it can be triggered in the second digital device (i.e., to become a CCF of both digital devices).

b. The simplicity alone of a digital device can be credited in reaching a conclusion that a CCF due to a design defect is not credible, only if all external and internal state combinations are tested, or an analysis is provided that demonstrates that untested state combinations are irrelevant; this deterministic criterion is typically relevant to single purpose EDDs with very few external inputs and very limited configurability.

4. Why is it important to assess the likelihood of a credible CCF?

   Anticipated Operational Occurrences (AOO) are plant accidents that are expected to occur one or more times during the life of the plant. These were historically defined based on the component/system level malfunction results of single random hardware failures in plant components, or the I&C and electrical systems that control those components. Due to this relatively high frequency expectation, AOOs are within the plant's design basis and are analyzed using conservative methods and acceptance criteria.

   Therefore, when a credible CCF can be caused by a single random hardware failure, the malfunction result of that CCF must be considered an AOO and must be assessed using conservative design basis analysis methods and acceptance criteria. In essence, the CCF is a design basis AOO.

   Conservative analysis methods require consideration of worst case plant conditions, use of only safety systems for event mitigation, worst case performance of those mitigating systems, and acceptance criteria with significant margin to critical safety limits. Conservative acceptance criteria mean that for a design basis CCF in a control system, the CCF malfunction result must be bounded by the plant level end result of current anticipated operational occurrences (AOO). Conservative acceptance criteria for a design basis CCF in an auxiliary safety support system, means that the CCF malfunction cannot result in an adverse component/system level effect on the auxiliary safety support system that is not previously analyzed in the FSAR; this is typically limited to single safety division.

On the other hand, when a credible CCF is significantly less likely than a CCF due to a random hardware failure, the CCF can be considered beyond design basis. Therefore, the malfunction result of that CCF can be assessed using best estimate analysis methods and acceptance criteria.

Best estimate methods allow the use of nominal plant conditions, use of high quality non-safety systems for event mitigation, nominal performance of those mitigating systems, and acceptance criteria that does not exceed critical safety limits. Best estimate acceptance criteria mean that for a beyond design basis CCF in a control system, the CCF malfunction result must be bounded by the plant level end result of current AOOs or postulated accidents (PA). Best estimate acceptance criteria for a beyond design basis CCF in an auxiliary safety support system, means that the CCF malfunction cannot result in an adverse effect on the safety systems supported by that auxiliary system. For mitigating a beyond design basis CCF, the analysis can credit safety systems, control systems in continuous operation, or other non-safety systems that are normally in standby but have augmented quality.

In both cases (within or beyond design basis), the analysis can only credit systems that currently exist in the plant, because these have had prior regulatory review. A bounded plant level end result refers to maintaining the margin to critical safety functions, such as DNBR and pressure boundary analytical limits, for the corresponding current accident analysis (AOO or PA).

5. Why is it acceptable to use best estimate methods when assessing a CCF that is concluded to be beyond design basis (i.e. significantly less likely than a CCF due to a random hardware failure)?

   The precedence for using best estimate analysis methods and acceptance criteria for beyond design basis events was established for the analysis of Anticipated Transients Without Scram (ATWS) and Station Blackout (SBO) events. Both of these are beyond design basis events. Best estimate analysis methods and acceptance criteria were employed for the original analyses of these events in the plant's FSAR; therefore, these same methods would be applicable to any upgrades to the ATWS or SBO mitigating systems.

   This use of best estimate analysis methods and acceptance criteria is also supported by the SRM to SECY 93-087 and BTP 7-19, which establish this

beyond design basis methodology for a CCF due to a design defect in safety systems. While the SRM to SECY 93-087 and BTP 7-19 were originally written to address the complexity of digital systems in new plants, that same complexity concern is applicable to the digital systems being applied to digital upgrades in operating plants today. This is also consistent with the SRM to SECY-15-0106 which states "the same requirements should apply to operating and new reactors."

6. What criteria are considered when determining the likelihood of a credible CCF?

   The conclusion in the SRM to SECY 93-087 that a CCF due to a design defect in a safety system is beyond design basis is based on (1) the low likelihood of a design defect due to a robust design process in safety systems, and (2) the inability of a triggered defect in one division to propagate to multiple safety divisions to actually cause a CCF, due to the independence of those safety divisions. Item 1 is a qualitative assessment; Item 2 is a deterministic assessment.

   Therefore, using the technical basis from the SRM to SECY 93-087, for any credible CCF, the likelihood of that CCF can be assessed using a combination of (1) qualitative measures to assess the effectiveness of the design process in reducing the likelihood of the CCF source, and (2) deterministic measures to assess the effectiveness of the segmentation/independence in preventing propagation of a triggered CCF source to multiple digital devices or multiple plant components. When both of these attributes exist, a credible CCF can be considered significantly less likely than a CCF due to a single random hardware failure; hence, the CCF can be considered beyond design basis. Therefore, the malfunction result of that CCF can be assessed using best estimate analysis methods and acceptance criteria, as explained in Item 4 above.

   The beyond design basis conclusion of the SRM to SECY 93-087 is clearly applicable to a digital design defect in safety systems, because they have a robust design process and divisional independence, both governed by regulatory guidance and criterion. However, the same technical basis can also be applied to non-safety control systems. A CCF due to a design defect in a non-safety control system can be considered beyond design basis, if the

control system exhibits (1) comparable design process attributes to reduce the likelihood of a design defect (qualitative), and (2) comparable design attributes to prevent the propagation of a triggered defect (deterministic).

However, due to their lower safety significance compared to safety systems, for non-safety control systems a graded approach can be applied when assessing these qualitative and deterministic attributes. For example, when assessing the likelihood of a CCF due to a design defect within a distributed control system: (1) Control systems that can initiate plant transients are expected to adhere to high quality commercial design life cycle standards that include well documented requirements, design and testing; they are not expected to adhere to the same regulated design life cycle criteria as safety systems. (2) Segmentation of control functions into different digital controllers is an acceptable means to limit the effect and prevent propagation of a triggered defect; divisional independence is not required as it is for safety systems.

It is important to note that while the SRM to SECY 93-087 establishes the precedence for using these two attributes (one qualitative and one deterministic) to conclude that the likelihood of a CCF has been significantly reduced (i.e., beyond design basis), based on the SRM to SECY 93-087 they are not sufficient attributes to consider a CCF due to a design defect not credible. Therefore, for this example the effect of a CCF due to a design defect in multiple distributed digital controllers would be analyzed using best estimate methods. To reach the conclusion that a CCF due to this design defect is not credible and thereby requires no further CCF malfunction result analysis, additional deterministic attributes would be required, as described in Item 3a, above.

7. When analyzing a credible CCF, what failure modes need to be considered for digital devices?

   The documented CCF susceptibility analysis described in Item 2 above, should assess the effects of a credible CCF at the component and/or system level. Where the component and/or system level effect is different than previously analyzed in the plant's FSAR, a documented CCF malfunction result analysis

should assess the effects of the CCF at the plant level to determine if the plant level end result is bounded by previously analyzed plant accidents.

Digital devices have the same failure modes as analog devices (i.e., failure to perform the intended control function, and spurious or erroneous control of the intended function). However, due to the integration of controlled components either (1) directly in the same digital device, (2) indirectly through interconnection of multiple digital devices using digital data communication interfaces and/or common video display units (VDU), or (3) indirectly through the use of common digital designs in independent digital devices, those failure modes have the potential to adversely affect more plant components (i.e., a CCF) than their analog predecessor. In addition, digital devices have the additional failure mode of data storms, where valid or erroneous data can be generated at an abnormally high rate that has the potential to adversely affect all connected digital devices.

NUREG 6303 provides guidance for decomposing complex digital systems into hardware/software blocks. A CCF susceptibility analysis considers the failure of only one block at a time (e.g., a single hardware component, a software function block). However, it must be recognized that the effect of that single hardware/software block failure can result in erroneous signals that propagate through the system to affect multiple functions or multiple plant components concurrently. This failed signal propagation is unlikely to result in all controlled plant components failing in the worst possible way, but it could certainly result in multiple plant components failing in different ways, depending on how the output of the failed block is used in the system.

Therefore, when conducting a CCF susceptibility analysis, if a CCF is concluded to be credible, the output(s) of a failed digital block should be assumed to fail as-is, high and low, and in a data storm mode. However, the propagation and adverse effect of these output failures can be restricted with the use of deterministic limiting measures such as a watch dog timer, or redundancy with output voting, which can detect an erroneous operation and force a single specific failure output state that is more easily analyzed.

8. Response to 50.59 Questions

There are three 50.59 questions that are particularly relevant to digital upgrades:

Question 2: Result in more than a minimal increase in the likelihood of occurrence of a malfunction…?

This question pertains to all malfunctions, not just malfunctions that result in a CCF. This requires a comparison of the analog and digital systems, to assess single point vulnerabilities and the qualitative reliability of the analog vs. digital components; reliability calculations can be used, but are not required. A CCF would be pertinent to this assessment only if the CCF is concluded to be credible and within the design basis (i.e., as likely as a single random hardware failure); a beyond design basis CCF is sufficiently unlikely to have no bearing on this assessment.

Question 5: Create the possibility of an accident of a different type…?

The transients analyzed in the UFSAR typically include events that challenge only a single critical safety function, such as reactivity control, pressure control, volume control, **OR** heat removal. Digital designs that maintain clear segregation between the controls for these critical safety functions do not create the possibility for an accident of a different type.

However, when these control functions are integrated, either directly or indirectly, and there is a credible CCF that is within the design basis and can adversely affect multiple critical safety functions, then there is the possibility of an accident of a different type.

When these control functions are integrated, either directly or indirectly, and there is a credible CCF that is beyond the design basis and can adversely affect multiple critical safety functions, then a CCF malfunction result analysis is conducted to determine if the plant level end result is bounded by the plant level end result determined for other AOOs or PAs previously analyzed in the FSAR. As stated in Item 1 above, plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF. As stated in Item 4 above, for a credible CCF that is beyond design basis, the CCF malfunction result analysis uses best estimate methods with best estimate acceptance criteria.

Question 6: Create a possibility for a malfunction … with a different result…?

This question can clearly be answered favorably for a CCF that does not result in a different component level or system level malfunction, as determined through the documented CCF susceptibility analysis. Where there is a different component/system level malfunction, a CCF malfunction result analysis is conducted to determine if the plant level end result is bounded by the plant level end result determined for other accidents previously analyzed in the FSAR. As stated in Item 1 above, plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF.

As stated in Item 4 above, for a credible CCF that is within the design basis, the CCF malfunction result analysis uses conservative design basis methods with conservative acceptance criteria. For a credible CCF that is beyond design basis, the CCF malfunction result analysis uses best estimate methods with best estimate acceptance criteria.

9. What is the impact of new NRC/Industry guidance?

   Current regulatory guidance establishes the basis for determining the credibility of a CCF, and the likelihood of a CCF that is concluded to be credible. Some examples:

   a. The deterministic guidance for communication independence in ISG-04 is appropriate to consider when determining if a CCF is credible due to a single random hardware failure or design defect in a data communication interface, including a failure/defect that results in a data storm.
   b. The software life cycle guidance in Regulatory Guides 1.68 through 1.73 is appropriate to consider when qualitatively assessing the likelihood of a design defect in a safety system that could lead to a CCF.
   c. Adherence to the guidance in RG 1.152 Rev. 3 for a secure development and operational environment (SDOE) is sufficient to reach a conclusion that an unwanted design change is not credible; therefore, a design defect due that could lead to a CCF due to an unwanted design change is also not credible.

While control systems are not expected to adhere to these same regulatory guidance documents, a graded approach can be taken to determine if a control system has comparable (not equivalent) attributes that can be credited to meet the same intent as these more prescriptive criteria that are applied to safety systems. For example, a graded approach can be taken to determine if a control system has comparable (not equivalent) security attributes that can be credited to meet the same intent as the more prescriptive SDOE criteria in RG 1.152.

10. What digital upgrades would screen out for a 50.59 evaluation?

    Due to the complexity of digital designs and the potential for new susceptibilities to CCF, the Staff would not expect any analog to digital upgrades in control systems that can cause plant transients, safety systems or auxiliary safety support systems to screen out. An analog to digital upgrade needs a CCF susceptibility analysis, and for any sources of CCF determined to be credible, that upgrade also needs a CCF malfunction results analysis. Digital to digital upgrades also need these analyses, if they were not previously conducted or if the new digital design requires changes to previous analyses.

11. Does the analysis of a CCF require a new method of evaluation?

    The use of digital technology does not require a new method of evaluation. The CCF susceptibility analysis (Item 2 above) and CCF malfunction result analysis (Item 7 above) are extensions of previously employed failure modes and effects analysis (FMEA) and plant transient and accident analysis (TAA). The best estimate methods and acceptance criteria that can be employed for a credible CCF that is determined to have low likelihood (Item 4 above) are the same as methods employed for other beyond design basis events, such as ATWS and SBO. All analyses that support 50.59 evaluations must be documented and maintained.

12. Is a D3 analysis required?

    The SRM to SECY 93-087 requires a D3 analysis, which consists of (1) an assessment to determine the vulnerability of the I&C systems to CCF; this is referred to as the CCF susceptibility analysis in Item 2, and (2) a plant level analysis to demonstrate adequate plant diversity, for each CCF vulnerability; adequate diversity is demonstrated for each credible CCF by the CCF

malfunction result analysis described in Item 6. If there is no credible CCF (i.e., no CCF vulnerability) then a CCF malfunction result analysis is not required.

The SRM does not distinguish CCF in safety vs. non-safety systems; this distinction arose through BTP 7-19 which limited consideration of CCF to safety systems only. The staff now recognizes that CCF in non-safety control systems that can cause plant transients is of equal concern, due to the potential that a CCF in those systems can result in unanalyzed transients. Therefore, these systems are included in the guidance of Item 2 above.

The SRM states that a CCF is beyond design basis, hence permits the use of best estimate methods when conducting the CCF malfunction results analysis. The Staff clarifies that the credibility of CCF should be determined based on an assessment of deterministic attributes (Item 3 above) and the likelihood of any credible CCF should be determined based on an assessment of both qualitative and deterministic attributes, as described in Item 6. When the appropriate attributes exist to conclude that the likelihood of a credible CCF is significantly less than the likelihood of a CCF due to a random hardware failure, the CCF can be considered beyond design basis and best estimate methods and acceptance criteria can be used.

CCF Susceptibility Analysis		CCF Malfunction Result Analysis	
Assessment →	Likelihood Conclusion →	Assessment →	Conclusion
Insignificant defensive measures exist. Limiting measures (e.g., watch dog timer) may exist to force a specific failure mode. When assessing 50.59 Q2, CCF may increase the likelihood of a malfunction.	CCF is as likely or the same order of magnitude as a CCF due to a single random hardware failure. CCF is expected during the life of the plant (~100 years). CCF is within the plant's design basis.	CCF malfunction analyzed with conservative methods and acceptance criteria. Method of coping is limited to safety systems.	CCF could produce same type of accidents (a 'No' answer to 50.59 Q5). CCF could be bounded by previous AOOs (a 'No' answer to 50.59 Q6). Or CCF could require a new analysis, FSAR update and LAR.
<u>Likelihood Reduction Measures</u> exist: • Qualitative defensive measures to reduce likelihood of failure source. AND • Deterministic measures to reduce likelihood that failure will propagate to become a CCF. Limiting measures may exist to force a specific failure mode. When assessing 50.59 Q2, CCF likelihood is an insignificant contributor.	↓ CCF is significantly less likely than a CCF due to a single random hardware failure. CCF is not expected during the life of the plant. CCF is beyond design basis.	CCF malfunction is analyzed with best estimate methods and acceptance criteria. Method of coping can employ quality non-safety systems.	CCF could be bounded by previous AOOs or PAs (a 'No' answer to 50.59 Q5 and Q6), or could require a new analysis, FSAR update and LAR.
For the two rows above, if the CCF component/system level malfunction is previously analyzed in the FSAR.		A CCF malfunction result analysis is not required (a 'No' answer to 50.59 Q5 and Q6).	
<u>Preventive Measures</u> exist: • Deterministic measures to eliminate failure source. OR • Deterministic measures to ensure failure source does not become a CCF. When assessing 50.59 Q2, there is no likelihood contribution from CCF.	↓ CCF is as unlikely as other sources of CCF that are not considered in deterministic accident analysis (e.g., earthquake/EMI exceeding design basis, maintenance error). CCF is not credible.	CCF is never expected (a 'No' answer to 50.59 Q5 and Q6). A CCF malfunction result analysis is not required. CCF should be analyzed in the Probabilistic Risk Assessment.	