NON-CONCURRENCE PROCESS COVER PAGE

The U.S. Nuclear Regulatory Commission (NRC) strives to establish and maintain an environment that encourages all employees to promptly raise concerns and differing views without fear of reprisal and to promote methods for raising concerns that will enhance a strong safety culture and support the agency's mission.

Employees are expected to discuss their views and concerns with their immediate supervisors on a regular, ongoing basis. If informal discussions do not resolve concerns, employees have various mechanisms for expressing and having their concerns and differing views heard and considered by management.

Management Directive, MD 10.158, “NRC Non-Concurrence Process,” describes the Non-Concurrence Process (NCP).

The NCP allows employees to document their differing views and concerns early in the decisionmaking process, have them responded to (if requested), and include them with proposed documents moving through the management approval chain to support the decisionmaking process.

NRC Form 757, “Non-Concurrence Process," is used to document the process.

Section A of the form includes the personal opinions, views, and concerns of a non-concurring NRC employee.

Section B of the form includes the personal opinions and views of the non-concurring employee's immediate supervisor.

Section C of the form includes the agency's evaluation of the concerns and the agency's final position and outcome.

NOTE: Content in Sections A and B reflects personal opinions and views and does not represent the official agency's position of the issues, nor official rationale for the agency decision. Section C includes the agency's official position on the facts, issues, and rationale for the final decision.

1. If the process was discontinued, please indicate the reason (and skip to #3):

   - ☐ Non-concurring employee(s) requested that the process be discontinued
   - ☐ Subject document was withdrawn

2. At the completion of the process, the non-concurring employee(s):

   - ☐ Concurred
   - ☑ Continued to non-concur
   - ☐ Agreed with some of the changes to the subject document, but continued to non-concur

3. For record keeping purposes:

   - ☐ This record is non-public and for official use only
   - ☑ This record has been reviewed and approved for public dissemination

NRC FORM 757
(06-2019)
NRC MD 10.156

U.S. NUCLEAR REGULATORY COMMISSION

NON-CONCURRENCE PROCESS (Continued)

1. NCP Tracking Number: NCP-2020-005

Date: 5/26/2020

Section A - To Be Completed By Non-Concurring Employee

2. Title of Subject Document	3. ADAMS Accession Number
RG 1.187 Draft Rev. 2, "Guidance for Implementation of 10 CFR 50.59... "	ML20125A685

4. Document Signer	5. Document Signer's Phone Number (Enter 10 numeric digits)
Louise Lund	(301) 415-0377
6. Title of Document Signer	**7. Office** (Choose from the drop down list or fill in)
Director, Division of Engineering	RES
8. Name of Non-Concurring Employee(s)	**9. Employee's Telephone Number** (Enter 10 numeric digits)
Norbert Carte	(301) 415-5890
10. Title of Non-Concurring Employee	**11. Office** (Choose from the drop down list or fill in)
Sr. Electronics Engineer	NRR

12. ☐ Document Author ☑ Document Contributor ☐ Document Reviewer ☐ On Concurrence

13. Name of Non-Concurring Employee's Supervisor	14. Office (Choose from the drop down list or fill in)
Michael Waters	NRR
15. Title of Non-Concurring Employee's Supervisor	**16. Supervisor's Telephone Number** (Enter 10 numeric digits)
Chief, Instrumentation and Controls Branch B	(301) 415-4039

17. ☑ I would like my non-concurrence considered and would like a written evaluation in Section B and C.

☐ I would like my non-concurrence considered, but a written evaluation in Sections B and C is not necessary.

18. When the process is complete, I would like management to determine whether public release of the NCP Form (with or without redactions) is appropriate (Select "No" if you would like the NCP Form to be non-public):

☑ Yes ☐ No

19. Reasons for the Non-Concurrence, Potential Impact on Mission, and the Proposed Alternatives

See the attached documents for a full description of my concerns.

Summary: There are two major concerns with the NRC's endorsement of Appendix D in this RG:
(1) Appendix D is confusing, ambiguous, and hard to undertstand which will create an unecessary regulatory burden.
(2) The relaxation in Section 4.3.6 are not consistent with: (1) the wording of the rule, (2) the intent of the rule, and (3) the policies and practices of the Commission.

20. Signature and Date of Non-Concurring Employee

Norbert Carte

Digitally signed by Norbert Carte
Date: 2020.05.14 12:17:39 -04'00'

Section B - To Be Completed By Non-Concurring Employee's Supervisor

2. Title of Subject Document	3. ADAMS Accession Number
RG 1.187 Draft Rev. 2, "Guidance for Implementation of 10 CFR 50.59... "	ML20125A685

4. Name of Non-Concurring Employee's Supervisor	5. Office (Choose from the drop down list or fill in)
Michael Waters	NRR
6. Title of Non-Concurring Employee's Supervisor	**7. Supervisor's Telephone Number** (Enter 10 numeric digits)
Chief, Instrumentation and Controls Branch B	(301) 415-4039

8. Comments for the NCP Reviewer to Consider

I generally agree with Norbert's view that the new guidance is a departure from the long-standing application of 10 CFR 50.59(c)(2)(vi), and the interpretation clearly provided in Section 4.3.6 of NEI 96-07. The Appendix D guidance may now permit reevaluation of plant transients, and acceptance of results that are more severe than the AOO transient results documented in the licensed UFSAR accident chapter (e.g., up to analytical safety limits). This evaluation option can be used in lieu of demonstrating that the likelihood of a digital CCF malfunction in sufficiently low. However, this new guidance appears to legally satisfy the rule, and I believe the RG sufficiently clarifies the consideration of UFSAR `basic assumptions' and `acceptance criteria' to permit this approach. We also intend to notify the Commission of this departure from past practices.

I partially agree with Norbert's view of ambiguity, within selected portions of Section 4.3.6 of Appendix D. But I do not consider them so significant to prohibit endorsement. NRC maintains the power of inspection to verify correct implementation of the guidance with sound technical analyses.

I do acknowledge some of the concerns raised regarding the stakeholder interactions on past versions of Appendix D. Discussions were often steered towards gaining agreement on interpretative 50.59 findings allowed by the rule and narrow hypotheticals - - without substantive discussion of the underlying digital I&C engineering and technical analysis that would justify such findings. This made the endorsement review challenging and longer than needed.

I have no comment on other viewpoints and information provided in the non-concurrence.

Finally, I appreciate Norbert's commitment to the collaborative process and providing his viewpoints here. Many of his concerns address potential digital upgrades that could interconnect active balance-of-plant components or systems. While improving overall safety and plant reliability, potential failure modes of these systems (if not properly designed) can be just as risk-significant as safety-related protection systems.

9. Signature and Date of Non-Concurring Employee's Supervisor

Michael D. Waters

Digitally signed by Michael D. Waters
Date: 2020.05.27 11:46:44 -04'00'

NON-CONCURRENCE PROCESS (Continued)

1. NCP Tracking Number	Date
NCP-2020-005	5/26/2020

Section C - To Be Completed By NCP Coordinator

2. Title of Subject Document	3. ADAMS Accession Number
RG 1.187 Draft Rev. 2, "Guidance for Implementation of 10 CFR 50.59... "	ML20125A685

4. Name of NCP Coordinator	5. Office (Choose from the drop down list or fill in)
Philip McKenna	NRR
6. Title of NCP Coordinator	**7. Coordinator's Telephone Number** (Enter 10 numeric digits)
Chief, Oversight and Support Branch, DRO	(301) 415-0037

8. Agreed Upon Summary of Issues

1. NEI 96-07 Rev.1 Appendix D does not solve the digital modification common cause failure guidance issue. The NRC should write the technical document to give guidance on digital modifications common cause failure.
2. The entire guidance structure for evaluating digital modifications is complicated and confusing which creates an unnecessary regulatory burden.
3. The relaxation in RG 1.187 on Appendix D, section 4.3.6, is not consistent with the wording of the 10 CFR 50.59 rule.
4. The changes that NEI made to section 4.3.6 in NEI 96-7, Appendix D to address the exception in draft RG 1.187 Rev. 2 did not go far enough in making licensee engineering departments understand the section 4.3.6 six step process.

9. Evaluation of Non-Concurrence and Rationale for Decision

1. For Summary Issue 1, Appendix D to NEI 96-07 Rev. 1 was not meant to be the document that provides licensees with digital modification common cause failure (CCF) design guidance. Rather, Appendix D provides guidance to licensees on conducting a 10 CFR 50.59 review of digital modifications that have already completed the design process. RG 1.187, Rev. 2 endorses the 50.59 guidance in Appendix D for digital modifications. Another NEI document was intended to provide the guidance on CCF. In the beginning of the Appendix D development process which began over three years ago, NEI was going to develop two documents: 1) Digital modification 50.59 guidance (now Appendix D) and 2) An industry-proposed guidance document outlining a technical basis for application of such development practices and defensive measures for CCF. This document was originally identified as NEI 16-16. These actions were described in the "Integrated Action Plan [IAP] to Modernize Digital Instrumentation and Controls" as Modernization Plan (MP) 2A and MP 1B respectively. NEI submitted NEI 16-16 to the NRC in 2017, and after substantive engagement on the document, NEI withdrew that document in lieu of developing another document that met the same objectives. That document has been identified as NEI 20-07, and NEI stated that they are planning to have a draft of this document ready for review by the NRC in summer 2020. The staff will take into account the non-concurring individual's perspectives on CCF, as discussed in his attachment to this document, as they review NEI 20-07. For the reasons given above, no action was taken on revising RG 1.187 Rev. 2 based on this issue.

2. For Summary Issue 2, the staff recognizes that the guidance structure for evaluating digital modifications can be complicated to navigate and has had discussions in public meetings with industry about this particular topic. A significant contributing factor to this is the lengthy time horizon during which the various guidance documents have

been developed and issued. In the public discussions, industry recommended pursuing better coordination of the guidance documents in the future but did not see it as an immediate barrier to using the existing and pending guidance in pursuing near term digital upgrades. In recognition of the long-term benefits of pursuing this goal, better coordination and streamlining of the guidance was listed as task MP 4B in the IAP, as a longer-term goal to improve the NRC's guidance structure for evaluating digital modifications. Specifically, the goal is to evaluate and strategically implement holistic improvement of the NRC's digital I&C regulatory infrastructure. The infrastructure improvements will result in a state in which the nuclear power industry can perform digital upgrades under the 10 CFR 50.59 licensing process or, where necessary, obtain regulatory approval to use digital technology that provides for adequate safety and security through processes that are efficient, minimize uncertainty, and can be consistently applied across different technologies. Efforts are already underway for this task, with the staff having already developed a “straw-man” for the improved holistic guidance infrastructure and having discussed it at a public meeting with industry for initial feedback and to identify near term priorities for documents within the infrastructure to initiate the revisions.

Given that the IAP laid out the plan for approving and issuing the guidance structure for evaluating digital modifications and that there is a longer term goal to evaluate this guidance, as also described in SECY-19-0112, "Annual Update on the Integrated Strategy to modernize the U.S. Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure," the plan to issue RG 1.187 Rev. 2 should go forward as planned. Furthermore, subsequent to the issuance of the RG, the industry plans to conduct workshops on Appendix D and RG 1.187 Rev. 2 and in a similar manner, the NRC also plans on conducting inspector training. This training will focus attention on the regulatory infrastructure for digital I&C modifications and will provide an appropriate venue to address any questions or areas of confusion as to the use of either document in the context of already existing guidance regarding digital I&C upgrades. Within the NRC, HQ experts in the 50.59 rule are always available for questions about Appendix D and will be sensitive to the issues that need further clarification during the holistic infrastructure revision. Because of the nuances of the 10 CFR 50.59 rule, inspectors and regional branch chiefs regularly confer with HQ experts about inspection issues involving the rule, which is also a good forum to identify areas for clarification in the holistic infrastructure revision. For the reasons given above, no action was taken on revising RG 1.187 Rev. 2 based on this issue.

3. For Summary Issue 3, which states that the relaxation in RG 1.187 on Appendix D, section 4.3.6, is not consistent with the wording of the 10 CFR 50.59 rule, the staff had significant interactions with the NRC Office of General Counsel (OGC) in the evaluation of Appendix D, section 4.3.6 and in writing the clarification, "Step 6: Basic Assumptions and Acceptance Criteria," in RG 1.187. Since section 4.3.6 of Appendix D does not define the term "Basic Assumption;" and "Acceptance Criteria" was not discussed in NEI 96-07, Revision 1, the NRC clarified the term "Basic Assumption" and the use of "Acceptance Criteria." The RG contains a clarification which defines the term "Basic Assumption" and clarifies licensee use of “Acceptance Criteria” when conducting digital I&C modifications using Appendix D. This clarification to Appendix D provides the consistency to the wording of the 10 CFR 50.59 rule, so as a result, no action was taken on revising RG 1.187 Rev. 2 based on this issue. However, in recognition of the extensive dialogue between NEI and NRC on this topic subsequent to the public comment period, the staff is considering a post-promulgation comment period for the RG, to identify if there are any critical questions still unanswered in this area.

4. For Summary Issue 4, it is agreed that NEI could have placed more guidance into section 4.3.6 of Appendix D, but NEI decided that the guidance listed was enough for conducting a 10 CFR 50.59 criterion 6 evaluation. To supplement the guidance in section 4.3.6, and to be able to identify questions on using the guidance and need for clarifications such as those mentioned by the non-concurring individual in real time, the industry plans to conduct workshops on Appendix D and RG 1.187 Rev. 2 and the NRC also plans on conducting inspector training subsequent to the issuance of these documents. As with other questions/clarification that arise for 50.59 reviews, NRC HQ experts in the 50.59 rule are always available for questions about Appendix D. Because of the nuances of

the 10 CFR 50.59, inspectors and regional branch chiefs regularly confer with HQ experts about inspection issues concerning the rule, and that will ensure that issues that arise from the implementation of this guidance are identified and resolved. Based on the plans for post-issuance outreach and training for both the NRC and industry, no action is needed or was taken on revising RG 1.187 Rev. 2 based on this issue.

10. Signature and Date of NCP Coordinator

Philip J. McKenna

Digitally signed by Philip J. McKenna
Date: 2020.06.08 17:04:59 -04'00'

11. Signature and Date of NCP Approver

Anita Lund

Digitally signed by Anita Lund
Date: 2020.06.30 16:38:35 -04'00'

Attachments to Non-Concurrence on Regulatory Guide 1.187, Revision 2

NCP-2020-005

The NRC Should not Endorse NEI 96-07 Rev. 1 Appendix D

My Personal Perspective on the Regulation of Digital I&C Technology: The NRC should facilitate the use of digital I&C technology in the nuclear industry because it can improve safety. This facilitation should be through the publication of clear guidance: (1) to the industry for meeting regulatory requirements, and (2) to the staff for evaluating adequate means for conformance with regulatory requirements and/or endorsed guidance (i.e., to provide reasonable assurance of adequate safety). I believe that most technical reviewers in the I&C discipline agree with this position. Furthermore, I believe poor guidance is the largest regulatory burden the industry faces; that is, with uncertainty about what is acceptable, industry either does too much, or does nothing and lives with inefficiencies.

My Personal Perspective on Appendix D: Appendix D contains sufficiently ambiguous and/or misleading guidance that the NRC should not endorse it. After working with NEI for more than seven years[1] on the improvement of 50.59 guidance for digital I&C, I believe it would be more efficient and effective for the I&C Technical Review staff to write 50.59 guidance for digital I&C. Whether or not the NRC chooses to endorse Appendix D, the NRC should pubish a clear and well written description of the intent of the 50.59 rule, and how the eight (8) evaluation questions work together to accomplish that intent (e.g., as an appendix to the RG). The guidance in the many 50.59 related documents (i.e., RG 1.187, NEI 96-07 Rev. 1, RIS 2002-22, NEI 01-01, RIS 2002-22 Supplement 1, Appendix C, and Appendix D) could be more easily interpreted if the intent of the 50.59 rule was clearly stated. This clear statement of intent would reduce the regulatory burden produced by the NRC's endorsement of these various complicated and confusing documents.

General Explanatory Approach: For the last seven years the technical review staff for I&C and the agencies 50.59 lead have been trying to explain to NEI the specific problems with Appendix D; NEI has chosen not to address our concerns. If directed by NRC management, I can compile a comprehensive analysis of all the problems in the most recent version, but the time allowed by the non-concurrence process does not allow for this (it would also be quicker and easier to draft 50.59 guidance for digital I&C). Rather the problem seems to be more at the conceptual level. That is, both NEI and Senior NRC management do not appreciate the regulatory burden (and associated safety concern) posed by unclear or vague guidance; therefore, this document will attempt to make both arguments through a series of attachments.

Specific Concerns with Section 4.3.6: The relaxation proposed in Section 4.3.6 is so large that it effectively eliminates the regulatory requirement in 10 CFR 50.59(c)(2)(vi) – effectively a rule change. For example, one constraint imposed by Section 4.3.6 is that a change cannot be inconsistent with regulatory requirements; does this really need to be said? That is, does anybody believe that 50.59 can be used to not conform (or comply) with regulatory requirements or technical specifications? (Besides, this constraint is already articulated in NEI 96-07 Sections 4.3.1 & 4.3.2.) Another constraint imposed by Section 4.3.6 is that a change cannot cause the acceptance criteria to be violated. If one examines many of the acceptance criteria described in the accident analysis, they are the same as the regulatory requirements; therefore, this constraint may be redundant to the first constraint (In order for this constraint to be completely redundant to the first one, one must assume that some acceptance criteria are more conservative than regulatory requirements.). Both of these relaxation result in some basic principles of licensing being violated; these principles are that the NRC reviews: (1) the most limiting events of the facility, (2) the methods used too address the most limiting events, (3) that there is adequate margin (where required by regulations), and (4) whether regulations are met.

[1] The problem with the Guidance for 50.59 in NEI 01-01 was first identify in a violation in 2009 which was addressed in an Information Notice in 2010; therefore, it took 5 years and a second related violation (in 2013) before NEI started to develop improved 50.59 guidance for Digital I&C.

Attachments:

Knowledge Management is a Safety Concern

History of Published Considerations of CCF

An Engineers Understanding of the Intent of the 50.59 Rule

Guidance Clarity is a Regulatory Burden Concern

Example Source of Regulatory Uncertainty

Divide and Conquer and the Lost Third Step

Common Misunderstandings Regarding 50.59

Consistency with 10 CFR 50.92(c)

Inappropriate Implementation of RG

Safe – Necessary but Not Sufficient

Licensing versus Engineering

Specific Issued with Appendix D

Knowledge Management is a Safety Concern

Safety is a system property, created by good engineering. That is, a particular system is maintained and used in a certain manner, in a specific context, and can be demonstrated (by appropriate analysis) to provide reasonable assurance of adequate safety; each of these specific aspects (system, manner of maintenance and use, context, & analysis) are interrelated. If one changes any one of these aspects too much, the system will no longer be safe. The key to ensuring safety is understanding the bounds or limitations of each of these aspects. That is, the key to safety is engineering knowledge management. As a corollary, anything that undermines sound engineering, undermines safety. The basic approach taken by NEI in Appendix D is to use several partial quotations (taken out of context) to construct a "licensing" meaning that is unclear and inconsistent with then engineering needed to demonstrate reasonable assurance of adequate safety. Maybe we can learn something from other disciplines and contexts…

The safety implications of failures in knowledge management have been articulated in the Structural Engineering domain, as summarized below:

> In May of 1977 a paper in the Proceedings of the Institute of Civil Engineers by civil engineers Paul Sibly and Alastair Walker, "Structural Accidents and Their Causes," summarized their theory based on observations of the pattern of major bridge collapses. They concluded:
>
> > "47. All the accidents described above were preceded by accidents on a smaller scale which, properly interpreted, would have served as warnings for the designers. At the present there is no organization which undertakes the collection of structural accident statistics. It would be a valuable duty of a review body to serve as a clearing house for accident data, and, as with design trends, this information could be put into anonymous form for wider distribution." [1]
> >
> > "43. There are a number of common features in the circumstances leading to the accidents described above. In each case one can identify a situation where, in early examples of the structural form, a certain factor was of secondary importance with regard to stability or strength. With increasing scale, however, this factor became of primary importance and led to failure. The accidents happened not because the engineer neglected to provide sufficient strength as prescribed by the accepted design approach, but because of the unwitting introduction of a new type of behavior. As time passed during the period of development, the bases of the design methods were forgotten and so were their limits of applicability."
>
> Henry Petroski is a professor of civil engineering at Duke University and design guru, also known for popularizing the theory that there's major bridge collapse every 30 years. He theorizes (in part based on the paper above) that bridge collapses happen approximately every 30 years because that's how long it takes a new generation of engineers to emerge and then ignore the old lessons, to disastrous results. Put in other words, engineering knowledge management is a safety concern.

Brief history of knowledge management at NPPs: Initially, the NRC did not require licensees to maintain and resubmit the FSARs submitted as part of their operating license applications. In 1980, the NRC issued a rule—10 CFR 50.71(e)—requiring licensees to submit an updated FSAR within 2 years and annual updates thereafter (ML031080517). In the mid-1980s, the NRC staff conducted many system-specific engineering inspections and developed inspection findings that demonstrated that some licensees had not adequately maintained their design bases information as required by NRC regulation.[2] In response to the problems identified during the NRC inspections and those identified by licensees, most reactor licensees initiated design bases reconstitution programs. These programs sought to identify missing design

[1] It should be noted the NRC may not have been trying to learn from other industries at that time, and the nuclear industry had to wait until 1979 for the three mile island accident to provide the incentive to create an operating experience program.

[2] This requirement is probably why NEI is trying to redefine "design basis function" in Appendix D to be different that in 10 CFR 50.2.

documentation and to selectively regenerate missing documentation.[3] In 1996, the staff's findings during inspections and reviews began to identify broad programmatic weaknesses that resulted in design and configuration deficiencies at some plants; these deficiencies could have affected the operability of required equipment, raised unreviewed safety questions, or indicated discrepancies between the plant's UFSAR and the as-built or as-modified plant or plant operating procedures. As a result of these findings, the staff issued a letter in accordance with 10 CFR 50.54(f) to all licensees requesting information to provide the NRC added confidence and assurance that the plants were operated and maintained within the design bases and any deviations were reconciled in a timely manner.

Since the nuclear industry started, effectively in the late 1960s, the effective half-life of design basis information in the nuclear industry may be less than in civil engineering. Furthermore, it is approaching 30 years since the design basis re-constitution was implemented for the second time. More importantly, the limitations of the previously established design, analysis, and licensing methodologies for addressing new types of behavior (e.g., those unique to digital SSCs) may not be well understood. Therefore, more and better guidance, rather than more discretion is warranted.

Some think the Boeing 737 Max accidents demonstrate there is a danger in providing too much discretion to licenses for determining whether a license amendment is required.

Some might argue that the CORONA-19 virus response by some countries demonstrates the safety significance of putting economic considerations above basic medical considerations. One could also argue that in the end it is more expensive to think about money first and the health and safety of the public second. An ounce of prevention is worth a pound of cure (i.e., this is not a new idea)!

Jean-Francois Rouet in "The Skills of Document Use," noted: "There are numerous cases of errors and accidents that can be attributed, at least in part, on poor or inappropriate design of technical documents."

[3] The NRC cared about such things because the NRC must have considered knowledge management to be a safety concern.

History of Published Considerations of CCF

Reason for Creating this Document: There are at least two quotations that have been misunderstood or misinterpreted and this document was first generated to correct this misinterpretation (the proper understanding is described in the abstract). (1) SRM to SECY 93-087 stated: "First, inasmuch as **common mode failures are beyond design-basis events**, the analysis of such event should be on a best estimate basis." [**emphasis** added] (2) NEI 01-01 states: ""sufficiently low" means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other **common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors)**." These two quotations have been used to argue that a licensee does not need to consider CCF; the promulgation of this misunderstanding, in light of the many examples below, demonstrate a failing of knowledge management. (See Example Source of Regulatory Uncertainty for a more complete explanation of the second concern.)

Abstract: CCF (e.g., design error) has been a concern of the NRC (and should continue to be a concern), and CCF has been addressed as part of the licensing process for a very long time (in part by diversity and defense-in-depth); however, except for a very few exceptions (e.g., feedwater), CCFs have not been analyzed in Chapter 15. An "analog" NPP is considered to have sufficient design features (i.e., Diversity and Defense-in-Depth - D3) and criteria in their UFSAR to address "analog" CCFs. When a different technology is used (i.e., digital), how does a licensee determine whether the use of different equipment results in the need for additional design features to address the specific vulnerabilities of the different equipment (e.g., Software CCF)? Furthermore, what measures are appropriate (technically) to address each specific vulnerability? **Note:** Some of the text below is shaded; shading of the same color is to highlight related passages.

Meaning of CCF: The NRC has used the terms CCF and CMF interchangeably, however, not everybody does. The meaning of CCF (as used by the NRC) has changed over time. Specific sources of CCF got their own name (e.g., protection from natural phenomenon, single failure criteria, Fire Protection...) and are not included in CCF. The scope of CCF has been shrinking over time, and in the end will only include "unknowns" which can only be addressed by diversity and defense-in-depth.

Design Attributes to Address CCF: Early documents described hazards (e.g., CCF), but as design techniques (e.g., incorporation of specific design attributes) were found that address these hazards (e.g., diversity and defense-in-depth), these design techniques became the subject of regulatory criteria, and discussion of the specific hazards was reduced. That is, in some parts of the NRC today, there is a lot of discussion about defense-in-depth, but very little about the various hazards (e.g., CCF) this design attribute addresses.

Threads of thought: The text below is organized in chronological order and contains several different significant threads of thought, each with its own color of shading.

consideration of CCF

Diversity, different principles, or different

CCF; CMF; common disasters; systematic, nonrandom, concurrent failures of redundant elements

Separation of Protection and Control, or Control and Protections System Interaction

In **1967**, the NRC initially proposed (32 FR 10213) the GDCs, and stated:

> "The purpose of the proposed amendment would be to provide guidance to applicants in developing the principal design criteria to be included in applications for Commission construction permits. These General Design Criteria would not add any new requirements, but are intended to describe more clearly present Commission requirements to assist applicants in preparing applications. …
>
> *Criterion 20-Protection Systems Redundancy and Independence (Category B).* Redundancy and independence designed into protection systems shall be sufficient to assure that no single failure or removal from service of any component or channel of a system will result in loss of -the protection function. The redundancy provided shall include, as a minimum, two channels of protection for each protection function to be served. Different principles shall be used where necessary to achieve true Independence of redundant Instrumentation components.
>
> *Criterion 21-Single Failure Definition (Category B).* Multiple failures resulting from a single event shall be treated as a single failure.
>
> *Criterion 22-Separation of Protection and Control Instrumentation Systems (Category B).* Protection systems shall be separated from control instrumentation systems to the extent that failure or removal from service of any control instrumentation system component or channel, or of those common to control instrumentation and protection circuitry, leaves intact a system satisfying all requirements for the protection channels.

Criterion 23-Protection Against Multiple Disability for Protection Systems (Category B). The effects of adverse conditions to which redundant channels or protection systems might be exposed in common, either under normal conditions or those of an accident, shall not result in loss of the protection function."

In **1968**, IEEE 279-1968 was published. This version is almost identical to IEEE 279-1971, with the largest difference being in Clause 4.7, "Control and Protections System Interaction." IEEE 279-1968 (incorporated by reference in 10 CFR 50.55a(h)) states:

"**4.7 Control and Protections System Interaction.** Where a plant condition that requires protective action can be brought on by a failure or malfunction of the control system, and the same failure or malfunction prevents proper action of the protection system channel or channels designed to protect against the resultant unsafe condition the remaining portions of the protection system shall independently meet the requirements of Paragraphs 4.1 and 4.2.

…

4.1 General Functional Requirement. The nuclear power plant protection system shall with precision and reliability, automatically initiate appropriate protective action whenever a plant condition monitored by the system reaches a preset level. This requirement applies for the full range of conditions and performance enumerated in 3(g), 3(h), and 3(i).

4.2 Single Failure Criterion. Any single Failure within the protection system shall not prevent proper protection system action when required. Note: "single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes the single credible malfunctions or event that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a single failure even though several transistor failures result. Mechanical damage to a mode switch would be a "single Failure" although several channels might become involved."

In **1968**, ORNL published, for the AEC, ORNL-NSIC-51, "Design Principles of Reactor Protection System instrumentation," which stated (Page No. 56 on PDF page 71 of 110):

Identical elements may be subject to simultaneous failures as the result of a single event. Such failures can be brought about by external events or environmental factors. This class of failures we call "common disasters." A recent study of common disasters in instrument systems indicates that their rate of occurrence may be ten times the rate at which the coexistent independent failures of two redundant channels will cause a system to fail. The coexistent failure rate from independent failures can always be decreased by increasing the number of channels or by decreasing the testing interval, but common disaster rate for identical channels of instruments is determined by nonrandom external events and cannot be so reduced…A possible solution to the common disaster situation is the use of diversity.

In February of **1969**, the Division of Reactor Standards of the AEC requested the various reactor manufacturers to systematically examine their plant designs in respect to common-mode-type failures.

In **1969**, Westinghouse published WCAP-7306 which stated:

"More recently, the question of the failure mode changed from that of a single random failure to common-mode failure - a failure mode which would adversely affect all redundant channels of a particular protective function in the Protection System. It is generally recognized that separation of control and protection does not provide defense against the common-mode failures. The nuclear power plant Control and Protection System design employed by Westinghouse was evaluated in detail with respect to the common-mode failure and presented in a series of meetings to members of the AEC. This report documents the information transmitted in these meetings and provides a technical basis for the development of criteria for design of Protection Systems with adequate consideration for common-mode failures ...The extent of Protection System diversity has been evaluated for a wide variety of postulated accidents. In most cases, two or more diverse protective functions would terminate an accident before intolerable consequences could occur...(Systematic failures are also known as common-mode, or nonrandom failures.)"

Section 1.1, "Common-mode Failures and Diversity," summarizes the specific CCF concerns and how they can be addressed. Therefore, this report documents that CCF has been a concern of the NRC since before 1969, and NPPs include features to address CCF. This report also states that the IEEE 279-1968 did not contain sufficient criteria to be accepted by the AEC-ACRS:

"In these cases, Westinghouse provides Control System inputs from Protection System channels. The "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," IEEE No. 279, permits this design approach, subject to certain restrictions. However, this proposed resolution was not unanimously accepted by members of other United States standards and regulatory agencies, in particular, USASI Sectional Committee N3 (N42), and the AEC-ACRS."

Finally, it should be noted that the protection provided by the secondary or backup trips, did not provide the same level of protection as the credited trip functions.

By letter dated April 9, 2010, Diablo Canyon supplemented it's LAR by docketing (See Enclosure 3): Diablo Canyon Power Plant Topical Report, "Process Protection System Replacement Diversity & Defense-in-Depth Assessment," Revision 0 (Nonproprietary). Section 2.1.1, "Reference Diversity and Defense in depth," references WCAP-7306.

In **1970**, General Electric responded to the 1969 AEC letter and docketed a topical report for review and approval: NEDO-10189, "An Analysis of Functional Common Mode Failures in GE BWR Protection and Control Instrumentation."

By application dated March 3, 1971, the Jersey Central Power & Light Company submitted Change Request No. 6 to the Technical Specifications appended to Provisional Operating License No. DPR-16 for your Oyster Creek Reactor. By letter dated March 18, 1971, the AEC approved the change to the technical specifications and added reference to NEDO-10189 after the last paragraph on Page 3.1.6.

In **1970**, Babcock & Wilcox published Topical Report BAW-10019, "Systematic Failure Study of Reactor Protection Systems."

By letter dated September 8, 1970, Duke Power Company filed Amendment No. 19 to its Application for Licenses for the Oconee Nuclear Station. This Amendment incorporates by reference, as part of the license application, BAW-10019, "Systematic Failure Study of Reactor Protection Systems," dated August, 1970, which has been submitted by Babcock & Wilcox.

By letter dated April 3, 1978, the NRC stated (to TVA regarding Bellefonte): "The ATWS analysis in Topical Report BAW-10099, in part, utilizes assumption in Topical Report BAW-10019 -Systematic Failures Study of Reactor Protection Systems."

Revision 31 to the Davis-Besse Unit 1 UFSAR Chapter 15 states: "The effects of failure to obtain the primary reactor trip signal are discussed in B&W Topical Report BAW-10019 (September 1970), Systematic Failure Study of Reactor Protection System."

In **1971**, Combustion Engineering published Topical Report CENPD-11 "Reactor Protection System Diversity," W. C. Coppersmith, C. I. Kling, A. T. Shesler, and B. M. Tashjian, to demonstrate that functional diversity has been incorporated in the protective system design.

By letter dated November 8, 2006, Dominion requested to amend Operating License DPR-65 for Millstone Power Station Unit 2 to modify the Technical Specification Action and Surveillance Requirements for instrumentation identified in Technical Specifications 3.3.1 and 3.3.2., and referenced CENPD-11.

In **1971**, IEEE 279-1971 was published. Specifically, this version expanded Clause 4.7, "Control and Protections system Interaction." Presumably this expansion of the standard was to address the AEC-ACRS's concerns. IEEE 279-1971 (incorporated by reference in 10 CFR 50.55a(h)) states:

"**4.7 Control and Protection System Interaction.**
4.7.1 Classification of Equipment. Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the requirements of this document.

4.7.2 Isolation Devices. The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design bases. Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible ac or dc potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the protection system.
4.7.3 Single Random Failure. Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure. Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.
4.7.4 Multiple Failures Resulting from a Credible Single Event. Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, one of the following must be met.
4.7.4.1 Alternate channels, not subject to failure resulting from the same single event, shall be provided to limit the

consequences of this event to a value specified by the design bases. In the selection of alternate channels, consideration should be given to (1) channels that sense a set of variables different from the principal channels, (2) channels that use equipment different from that of the principal channels to sense the same variable, and (3) channels that sense a set of variables different from those of the principal protection channels using equipment different from that of the principal protection channels. Both the principal and alternate protection channels shall meet all the requirements of this document.
4.7.4.2 Equipment, not subject to failure caused by the same credible single event, shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment shall meet all the requirements of this document."

In **1971**, the AEC promulgated (36 FR 325) the final version of the GDCs, which now state:

"Further revisions of these General Design Criteria are to be expected. In the course of the development of the revised criteria, important safety considerations were identified, but specific requirements related to some of these considerations have not as yet been sufficiently developed and uniformly applied in the licensing process to warrant their inclusion in the criteria at this time. Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include:...(iv) Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of the protection systems and reactivity control systems."

The current version of the GDCs expand item (iv) to point to specific criteria:

"(See Criteria 22, 24, 26, and 29.)"

The current GDCs state:

"Criterion 22—Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function…

Criterion 24—Separation of protection and control systems. The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

In **1974**, the AEC published Volume 2 of the AEC I&C Handbook. Chapter 12 of this handbook discusses CCF as a concern, and Diversity as a means of addressing this concern. Specifically, Chapter 12, "Protection Systems," Section 12-3.1, "Categories of Failures and Failure Defenses," states):

"**(a) Performance Failures.** Performance failures are those failures in which the protection system operates as designed but is not able to protect the plant adequately. Such failures are attributable to designer error. Note that the distinction between performance failures and common-mode failures (to be discussed later) is somewhat arbitrary. For this reason some listings of failures consider performance failures as one type of common-mode failure. Performance failures of protection systems include the following

1. Failure by the designer to predict the accident. Potential examples are discussed in Sec. 12.2.8(a)
2. Failure by the designer to select a plant variable that would sense the accident at its inception
3. Failure by the designer to recognize what protective action IS needed
4. Failure by the designer to include all accidents in the set studied for the safety analysis

The defenses against performance failures seem rather obvious, but they are difficult to put into practice. The designer must study potential accident behavior and failure modes of the plant thoroughly during the establishment of the design bases. A study of accident and operating experience on similar plants is necessary. Several types of diversity should be considered as possible defenses against performance failures. Diversity in types of plant variables used to initiate action, in protective actions, and in the designers and design reviewers can provide added defense against failures. Providing ample design margins in all elements of the protection system is one way to reduce the effects of unforeseen failures. Each type of instrument or component should be tested at least once under realistic accident conditions to add further assurance that the system will perform as required.

(b) Common mode failures. Common mode failures are those in which some single event prevents multiple and identical components from performing in accordance with design. These failures may or may not involve component

damage, and they may result from causes that are external or internal (with propagation) to the protection system. Furthermore, they may be safe or unsafe types of failures. Some causes of common mode failures are:

1. Changes in the characteristics of the plant being protected. Potential changes are discussed in Sections 12-2.6(b) and 12-2.8(a).
2. Disablement of protection system by the accident. Potential failure mechanisms are discussed in Sections 12-2.6(e) and 12-2.8(a) and (b).
3. External catastrophes. Examples are described in Section 12-2.8(b).
4. Unrecognized dependence on a common element. Potential common elements include ventilation for instrumentation, power-supply frequency and voltage, instrument air supply, physical support structure for instrumentation, etc.
5. Propagation of a failure in a single channel or component to other redundant channels. This would be produced by lack of independence of channels or redundant components.
6. Errors in maintenance or operating procedures. Potential errors include miscalibration of similar protection-system channels, disconnection of vital components, faulty equipment repair, operation with known failures, etc.
7. Protection system equipment inability to function as specified in the design base. Potential disabling mechanisms include sensor or amplifier overloads, sensor or amplifier outputs that cannot reach the trip set point, plant variables that change at a predicted rate but at a rate that prevents the instrument channels from tripping, actuators that are slow to start, actuator speeds that are slower than predicted, etc. [see Sections 12-2.6(e) and 12-2.7(a), (b), and (d)].
8. Interaction between the operating control system and the protection system. Where this interaction is allowed to occur, a single failure in the operating control system that initiates an accident can also produce a failure in the protection system.

Common-mode failures have been recognized for several years and are receiving considerable study. The defenses against common-mode failures include some that overlap with defenses against performance failures and single-channel or component failures. A study of past accident and failure experience is a necessary requirement for the study of potential common-mode failures. In addition to the diversity mentioned previously, a diversity in equipment, such as sensors, logic, and actuators, to serve identical functions and a diversity in maintenance and operating procedures provide some defense against common mode failures. For safety purposes, reliability credit should not be given for more than two redundant channels or components Redundant channels and components should be separated from each other both electrically and physically to the degree practicable. Fail safe designs and continuous monitoring can be very effective."

In **1978**, the NRC issued a license to ANO. The ANO design includes a digital Core Protection Calculator (CPC). This may be the first digital safety system used in a NPP in the united states (I am not aware of any earlier example – please let me know if you find one!).

In **1979**, the NRC published NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System." It is less important that the RESAR-414 was considered (at the time) an Advanced Light Water Reactor (ALWR). The important aspect to consider (from a CCF perspective) is that one of the major innovations of the Westinghouse RESAR-414 design, as compared with previous designs, is its integrated protection system (IPS). It is important to note that, it was not until 1991 that Westinghouse got NRC approval for using its Eagle 21 digital I&C Platform to replace existing analog equipment. Therefore, the discussion in NUREG-0493 of integrated equipment (i.e., digital based) was in the ALWR area before it was discussed as replacements for existing NPP equipment. The following quotations are of particular interest:

Section 1.1, "Background," states:

> "The failures of potential concern are common-mode failures (CMF) of redundant elements. (We can adequately protect against independent failures.) The interconnections of the RESAR-414 design have the potential to propagate a CMF, if it were to occur, and to affect the functioning of systems other than the one in which the failure originated. The defense against such failures are, first, care in design, manufacture, and operation, and, second, the use of diversity in the design to provide alternate means of effecting the safety action."

Section 2, "Technical Discussion," contains a summary of the general diversity and defense-in-depth principles and associated concepts.

Section 2.1, "General Principles," states:

"it is mainly the control system that determines the frequency of challenges that the protection system has to meet. In an interconnected system like RESAR-414, it is important that transients or control system failures needing protection system action for safety not also induce protection system failure. This concern is expressed by GDC 24, "Separation of Protection and Control System," of 10 CFR 50 and within Section 4.7.4, "Multiple Failures Resulting From a Credible Single Event," of IEEE 279-1971."

Section 2.2, "Problem of Multiple Failures," states:

"If a system could be relied upon to function every time, defense in depth would not be required. In reality, however, such perfection is not attainable. Therefore, in addition to the high reliability required of safety-related systems, defense in depth is used to provide additional assurance of safety despite the imperfections. Most failures are tolerable because of the function of one or more of the other echelons of defense."

Section 2.3, "Separation and Diversity of Instrumentation," states: "Diversity is the design approach for achieving a reduced probability of functional failure, as a result of postulated common-mode failures, by providing different signals or equipment as redundant backup...The CMF is principally concerned with those kinds that have not yet occurred and those that have not yet been thought about...Requirements for separation and diversity are included in various NRC regulations, guides, and Standard Review Plans, and in IEEE Standards...These texts and references show that CMF ("multiple failures resulting from a single event") and diversity are recognized by NRC requirements."

Westinghouse introduced the concept of microprocessor based Protection Systems in the early 1970's on the Integrated Protection System (IPS) which was part of the RESAR 414 standard plant design. The software verification program conducted on this prototype is documented in WCAP-9153 "414 Integrated Protection System Prototype Verification Program", and WCAP-9739 "Summary of Westinghouse Integrated Protection System Verification and Validation Program".

It should be noted that the following anticipated transient without scram (ATWS) events (and the publication of associated guidance) all occurred before digital protections systems were employed in existing NPPs. (This is not completely correct since the Core Protection Calculators (CPCs) for Combustion Engineering (CE) design plants were first licensed in 1978, but this digital equipment only computed one protection function, DNBR Trip, and only a few plants have them. Furthermore, GE started developing its NUMAC digital I&C equipment in 1983 and did not produce associated topical reports until the late 1980s.)

In **1983**, the Salem Nuclear Generating Station experienced anticipated transient without scram (ATWS) events. These events prompted the NRC to issue IE Bulletin 83-01, "Failure of Reactor Trip Breakers (Westinghouse DB-50) to Open on Automatic Trip Signal," to address the short-term corrective actions. The NRC also formed a task force to assess the generic implications of these events. Upon reviewing the findings of the task force, the NRC issued GL 83-28.

In **1984**, the NRC promulgated the ATWS rule (i.e., 10 CFR 50.62). This rule required diverse equipment to protect against AOOs for existing plant designs, and that this equipment can be non-safety related. Therefore one can understand SECY 91-292 and SECY 93-087 to address, more specifically, the CCF of protection systems for future plant designs.

In **1985**, the NRC published GL 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related." This GL stipulated the quality criteria that non-safety related ATWS equipment must meet.

In **1991**, the NRC staff approved WCAP-12374 Rev. 1, the Eagle 21 topical report for replacing the existing analog process protection equipment with modular digital equipment. This was to be a system replacement with no integration to other systems. This report stated:

"The majority of nuclear power generation stations presently employ analog process protection equipment. This equipment was designed in the 1960's and early 1970's. …

Westinghouse Process Protection Systems include three generations of analog electronics: Foxboro H-Line, Westinghouse 7100 Series, and Westinghouse 7300 Series Equipment.

The first generation of analog process protection equipment was Foxboro H-Line which is described in WCAP 7671 "Topical Report - Process Instrumentation for Westinghouse Nuclear Steam Supply Systems." This equipment was manufactured for use during the 1965 - 1972 time frame. Twenty-five nuclear generating stations utilize this equipment.

The second generation of analog process protection equipment was the Westinghouse 7100 Series, also described in WCAP 7671. This equipment was manufactured for use during the 1970 - 1973 time frame. Thirteen nuclear generating stations utilize this equipment.

The third generation of analog process protection equipment was the Westinghouse 7300 Series, described in WCAP 7913 "Process Instrumentation for Westinghouse Nuclear Steam Supply Systems (4 Loop Plants Using WCID 7300

Series Process Instrumentation). This equipment was manufactured for use during the 1973 - 1983 time frame. Forty-four nuclear generating stations utilize this equipment.…

The Westinghouse Eagle-21 Process Protection System is a modular microprocessor-based upgrade system for replacing the existing analog process protection equipment…

The Eagle-21 Process Protection System…is a digital form, fit, and functional replacement for the existing analog equipment. All system inputs (from plant sensors) and system outputs (reactor trip logic, engineered safety features logic, indication and control) are preserved. Thus, the installation of Eagle-21 process equipment has no effect on the existing external interfaces."

In **1991**, the NRC published SECY-91-292, which further articulated the NRC's concerns about CCF and digital technology, which is summarized by the quotations below. The "Background" section (page 2) states:

"The use of digital computer technology in protection and control systems raises a concern that the software and hardware for these computer systems could be vulnerable to design and programming errors that could lead to safety-significant common mode failures."

The "Discussion" section (page 3) states: "The digital I&C system has a greater degree of sharing of data transmission, functions, and process equipment compared to the analog system. Although this sharing forms the bases for many of the advantages of the digital system it also raises a key concern with respect to its reliability. The concern is that a design using shared data bases and process equipment has the potential to propagate a common cause or common mode failure of redundant equipment. Another key concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure."

Enclosure 2 (page 5) states: "When diversity is considered for a particular application, care should be exercised to ensure that the diversity actually achieves the desired increase in reliability of the implemented design. If diverse components or systems are used, there should be reasonable assurance that such additions are of overall benefit, taking into account any disadvantages, such as additional complications in operating, maintenance and test procedures, or the consequent use of equipment of lower reliability.

One of the more effective means of achieving diversity is to require some form of diversity between preselected sets of functions (functional diversity) to ensure that common mode failures of M-MIS [man-machine interface systems] equipment do not degrade the performance of more than one set of these functions. The concept of functional diversity is discussed in NUREG-0493, "A Defense In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. In that assessment, the preselected sets of functions were control, including general monitoring functions; reactor trip; and engineered safety features. A block concept was introduced to provide a mechanism for systematically analyzing the effect of common mode failures on the defense in depth of the I&C system. The block concept aggregates the equipment (components and modules) of the system into a manageably small number of functional blocks. The staff chose three such blocks: measured variable, derived variable and command blocks. These blocks provide the equipment structure for the preselected sets of system level functions. The resulting block structure is used for the analysis of the consequences of postulated common mode failures…

Since its initial introduction, this approach has been refined (on the U.K. Sizewell B design) to provide for some level of diversity within both the reactor trip system and the engineered safety features (ESF). This diversity will provide assurance that common mode failures of software or hardware will not defeat all the reactor trip or ESF functions."

In **1992**, the NRC published 57_FR_36680, that is, it proposed a Generic Letter stating that Analog-to-Digital Replacements require a LAR per 10 CFR 50.59 (the final GL was GL 95-02, see below).

In **1993**, the NRC published SECY-93-087 and SRM to SECY-93-087. In summary, the SRM requires the assessment of the "defense-in-depth and diversity of the proposed instrument and control system to demonstrate vulnerabilities to common mode failure have adequately been addressed." One source of confusion is that neither the staff nor the commission described the regulatory basis for their position. However, one should notice that the position taken by the commission, for new plants, is similar to the position taken on ATWS in 1983 and 1984 (i.e., diverse actuation systems are held to a lower standard than the primary system). If one assumes there was a regulatory basis for the Commission's position, then it could be, in part, GDC 22, because the Commission's position is consistent with GDC 22 which states: "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." Furthermore, the commission position is also consistent with IEEE 279-1971 Clause 4.7.4, "Multiple Failures Resulting from a Credible Single Event," which described the criteria for alternate channels. If the SRM does not apply to a particular plant, then effectively the same position could be supported, based on the discussion above, or a more conservative position could be taken, since the labeling of CCF as beyond design basis is not applicable.

In **1994**, the NRC published IN 94-20, “Common-Cause Failures Due to Inadequate Design Control and Dedication,” which describes a common-cause failure (CCF) incident of an EDG load sequencer following the replacement of electromechanical timer/relays to generate the timed steps and sequencer reset function with microprocessor-based timer/relays. This event illustrates that safety-significant CCF can occur when the design review does not ensure that the digital, microprocessor-based replacement is compatible for the specific application and service environment. This incident illustrates that a digital replacement can produce a new susceptibility to a CCF.

In **1994**, the NRC published NUREG/CR-6303. The purpose of this NUREG is to describe a method for analyzing computer-based nuclear reactor protection systems that discovers and identifies design vulnerabilities to common-mode failure. The potential for common-mode failure has become an important issue as the software content of protection systems has increased...It is the purpose of the analysis method described here to postulate common-mode failures and to determine what portions of a design are uncompensated either by diversity or defense-in-depth. ... NRC staff considers that software design errors are a credible source of common-mode failures. Diverse digital or non-digital systems are acceptable means of compensating for such failures, as is manual action it sufficient time and information are available to operators.

In **1995**, the NRC staff approved NEDC-32410P-A, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option lll Stability Trip Function, Volume 1 & 2." The development of this platform stated in 1983, but because of the 1988 La Salle oscillation event, this platform was not strictly a digital replacement, but also included a required functional enhancement.

In **1995**, the NRC published GL 95-02 which stated in part, “Software failure, including common-mode failure, must be considered during the 10 CFR 50.59 evaluation.” This GL also stated how software CCF was to be considered under 50.59. The GL 95-02 position on software related malfunctions was referenced and summarized in the SOCs (63 FR 56098) for the proposed 50.59 rule change (see Section I on page 63 FR 56106); however, the guidance on how digital instrumentation should be considered was revised in the SOCs (64 FR 53582) for the promulgation of the 50.59 rule change in 1999 (see Section I on page 64 FR 53594).

In **1996**, the NRC staff approved BAW-10191P, "STAR System Components for Reactor Protection System Digital Upgrades", describing the STAR System of digital components proposed as an upgrade to existing reactor protection system equipment. This modular, digitally programmable and designed for safety-related protection and control applications in nuclear power plants. This system included internal diversity to addresses the concerns of common mode failures in digital hardware and software.

In **1997**, the National Science foundation (NSF) published “Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues (1997),” which was supported by Contract No. NRC-04-94-055 from the U.S. Nuclear Regulatory Commission. The six technical issues addressed: systems aspects of digital I&C technology; software quality assurance; common-mode software failure potential; safety and reliability assessment methods; human factors and human-machine interfaces; and dedication of commercial off-the-shelf hardware and software. This document stated:

> “The various aspects of quality, especially those associated with quality assurance, to provide discipline in the design, manufacture, … of systems important to safety, assist in minimizing common cause failures due to human error.”

In **1997**, the NRC staff issued SRP Chapter 7 Rev. 4. This version of Chapter 7 of the SRP was the first time BTP 7-19 Rev. 4 was issued (Since BTP were temporary, the numbers were recycled) to address SRM to SECY 93-087. In addition this version of the SRP included BTP 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.”

In **1999**, the NRC staff incorporated IEEE 603-1991 into the CFR by reference. IEEE 603-1991 has a greater scope of applicability than does IEEE 279.

In **1999**, the NRC promulgated a 50.59 rule change (64 FR 53582) that included guidance on how digital instrumentation should be considered under 50.59 (see Section I on page 64 FR 53594)

In **2000**, the NRC staff issued RG 1.187 endorsing NEI 96-07 Rev. 1 as one acceptable way of implementing the new version of 50.59.

In **2002**, the NRC staff issued RIS 2002-22 which endorsed NEI 01-01. NEI 01-01 states that a diversity and defense-in-depth assessment should be performed for RTS and ESFAS, in accordance with SRM to SECY-93-087; however, it also stated that Software CCF could be eliminated from consideration under 50.59 based on a qualitative assessment of the high quality development process. As a description of a high quality development process, NEI 01-01 references the Regulatory Guides (RGs) that were included in Rev. 4 of Chapter 7 of the SRP (dated 1997). These RGs endorse IEEE

standards, some of which were written in the 1980s. Some of these IEEE standards are probably not being followed by any vendor today, and some would probably not be considered to be generally accepted engineering practices today.

NEI 01-01 defined "sufficiently low:" to mean:

> "much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors)."

Since many of the references above describe certain CCF that must be considered, this quotation should not be understood to state that no CCFs were considered (only that some were and some were not).

In **2003** the NRC published NUREG/CR-6819, "Common-Cause Failure Event Insights" (in four volumes: Emergency Diesel Generators, Motor-Operated Valves, Pumps, and Circuit Breakers). This report documents a study performed on a set of common-cause failures (CCF) from 1980 to 2000.

Volume 1 states: "Forty-one CCF events affected the instrumentation and control sub-system of EDGs. Of these 41 events, 25 were fail-to-start and 16 were fail-to-run. Twelve instrumentation and control EDG CCF events were Complete CCF events."

Volume 2 Executive Summary states: "The study identified 149 events occurring at U.S. nuclear power plant units during the period from 1980 through 2000. Twenty-eight units each had one CCF event during the period; 42 units did not experience a CCF event. About 64 percent of the units had zero or one CCF event. Eleven percent of the units have experienced four or more MOV CCF events. Of the 149 events, 22 (15 percent) were Complete common-cause failures (failure events with all components failed due to a single cause in a short time)."

Volume 3 states: "The study identified 274 events occurring at U.S. nuclear power plant (NPP) units during the period from 1980 through 2000. Thirty-three NPP units each had one CCF event during the period; 21 NPP units did not experience a CCF event. This accounts for about 50 percent of the NPP units. While only 38 NPP units experienced more than two pump CCF events, these 38 NPP units account for 76 percent of the total number of pump CCF events. Of the 274 events, 62 (23 percent) were Complete common-cause failures (failure events with all components failed due to a single cause in a short time)…The most likely piece parts involved in driver segment CCF events were circuit breakers and instrument and control circuits…The Complete events in the driver segment were dominated by instrument and control failures and circuit breaker failures…There were 18 events involving the driver segment in the Design / Construction / Installation / Manufacture Inadequacy proximate cause group, of which five were Complete and three were Almost Complete (see Table B-I in Appendix B, items 16 - 33). Most of these events were caused by design related errors with instruments and control circuits."

Volume 4 states: "The study identified 119 events occurring at U.S. Twenty-nine NPP units each had one CCF event during the period; 54 NPP units did not experience a circuit breaker CCF event. This accounts for about 76 percent of the NPP units. Seventy-four percent of the total circuit breaker CCF events occurred at 51 of the NPP units. Of the 119 events, four of them (three percent) were Complete common-cause failures (failure events with all components failed due to a single cause in a short time) and two events were Almost Complete. The small fraction of Complete and Almost Complete events is mainly due to the large populations of circuit breakers in NPP units and the large number of minor events such as slow closing times, trip voltage out-of-specification, etc…Testing was the most likely method of discovery for instrumentation and control circuit breaker events (38 out of the 50 events, 76 percent)... The reactor trip breakers are frequently tested. This tends to make testing the most likely method of discovery.

In **2007**, the NRC staff issued SRP Chapter 7 Rev. 5 to prepare for the expectant new reactor applications. This version of Chapter 7 of the SRP included BTP 7-19 Rev. 5 (which did not expand the scope of SRM to SECY 93-087).

In **2007** the NRC published IN 07-15, "Effects of Ethernet-based, Non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," which described how digital communication lead to a CCF.

In **2008** the NRC made publicly available a document titled: "Background Defense-in-Depth and Diversity Supporting Basis Including Single Failure Criterion references and Risk Informed Initiatives."

In **2010**, the NRC staff issued two information notices IN 10-10, "Implementation of a Digital Control System Under 10 CFR 50.59," and IN 10-17, "Common Cause Failure of Boiling-Water Reactor Recirculation Pumps with Variable Speed Drives." In IN 10-10 the NRC described how a Software CCF was eliminated from consideration based on a high quality design process, but was inappropriately documented. In IN 10-17 the NRC describes how a common cause failure resulted from design flaw.

In **2011**, the NRC published Revision 1 of RG 1.177, "An Approach for Plant Specific, Risk Informed Decision making: Technical Specifications." In short this RG explain the NRC position that, even considering risk information, a License Amendment should not reduce defense-in-depth (or "introduce any new CCF modes not previously considered"), by stating (Does 10 CFR 50.59 allow changes that are inconsistent with the defense-in-depth philosophy?):

> "License amendment requests for TS changes that are consistent with currently approved staff positions (e.g., regulatory guides, standard review plans, branch technical positions, or the Standard Technical Specifications (STS) (Refs. 3-7)) are normally evaluated by the staff using traditional engineering analyses. A licensee would not be expected to submit risk information in support of the proposed change. Licensee-initiated TS change requests that go beyond current staff positions may be evaluated by the staff using traditional engineering analyses as well as the risk-informed approach set forth in this regulatory guide.
>
> …
>
> In implementing risk-informed decisionmaking, TS changes are expected to meet a set of key principles. Some of these principles are written in terms typically used in traditional engineering decisions (e.g., defense-in-depth). Although written in these terms, it should be understood that risk analysis techniques can be, and are encouraged to be, used to help ensure and show that these principles are met. These principles include the following:
>
> …
>
> 2. **The proposed change is consistent with the defense-in-depth philosophy.** The guidance contained in Regulatory Position 2.2.1 of this regulatory guide applies the various aspects of maintaining defense-in-depth to the subject of changes in TS.
>
> …
>
> 2.2.1 Defense-in-Depth
>
> …
>
> Defenses against potential common-cause failures (CCFs) are maintained and the potential for introduction of new CCF mechanisms is assessed (e.g., TS change requests should consider whether the anticipated operational changes associated with a change in an CT [(completion time)] or SF [(surveillance frequency)] could introduce any new CCF modes not previously considered)."

In **2012**, the NRC staff issued SRP Chapter 7 BTP 7-19 Rev. 6.

In **2013**, the NRC staff issued a memo identifying 11 concerns with NEI 01-01. Concern No. 7 stated that NEI 01-01 incorrectly stated that Software CCF could be eliminated from consideration based on a likelihood judgment. Historically, CCF has been eliminated from consideration based on either the consequences of the CCF, diversity, or simplicity.

In **2016**, the NRC published NUREG/KM-0009, "Historical Review and Observations of Defense-in-Depth," in response to commission direction to do so.

In **2016**, the NRC staff issued SRP Chapter 7 (most sections are at Rev. 6, but BTP 7-19 is at Rev. 7). This version was generated primarily to update references (i.e., several RGs were updated in 2013) and fix very minor problems.

In **2016**, the NRC issued IN 16-01, "Recent Issues related to the Commercial Grade Dedication of Allen Bradley 700-RTC Relays," that describes how the installation of a digital timing relays resulted in a common cause failure (i.e., two emergency diesel generators simultaneously unable to tie to their respective emergency busses). This event reinforces the 1994 illustration that safety-significant CCF can occur when the design review does not ensure that the digital, replacement is compatible for the specific application and service environment. This incident further illustrates that a digital replacement can produce a new susceptibility to a CCF.

In **2016**, the NRC issued IN 16-05, "Embedded Digital Devices in Safety-Related Systems," described how Embedded Digital Devices (EDDs) could result in CCF.

In **2018**, the NRC issued RG 1.174 Rev. 3, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," which states:

> "This revision of the guide (Revision 3) presents up-to-date defense-in-depth guidance using precise language to assure consistent interpretation and implementation of the defense-in-depth philosophy. Revision 3 contains

> significant changes including expansion of the guidance on the meaning of, and the process for, assessing defense-in-depth considerations.
>
> …
>
> the Commission directed the staff to revise the defense-in-depth guidance in this RG using precise language to assure that the defense-in-depth philosophy is interpreted and implemented consistently"

RG 1.174 also goes on to explain, in part through references, that certain reductions in defense-in-depth (i.e., coupling different echelons) is not acceptable, even under a License Amendment Request (LAR). It is hard to imagine that the commission would want vague guidance for addressing changes that affect defense-in-depth (under 10 CFR 50.59).

In **2018**, the NRC issued RIS 2002-22 Supplement 1 which provided additional guidance performing qualitative assessment in order to eliminate CCF from further consideration per NEI 01-01.

An Engineers Understanding of the Intent of the 50.59 Rule

Abstract: In order to reach agreement on acceptable guidance for 50.59, as applied to Digital I&C, one must first agree on the overarching intent of 50.59. Therefore, the purpose of this paper is to summarize the intent of 50.59 as documented by the NRC. That is, establishing the overarching intent of: (1) licensing and (2) the limits of allowable changes without prior NRC approval.

Establishing the Licensed Envelope: 10 CFR 50.34 contains requirements for what should be in a SAR. RG 1.70 Rev. 3 contains guidance for meeting 50.34. The first two pages of Chapter 15 (of RG 1.70) describe how the events that are analyzed in detail in the accident analysis are categorized by type and expected frequency, and that not all events must be analyzed. The analyses of the most limiting events[1] of each type and frequency are summarized in the SAR chapter on accident analysis[2] and evaluated by the NRC staff. Generally, more stringent acceptance criteria are applied to the higher frequency categories (e.g., see GDC 20). In previous chapters of the SAR, the structures, systems, and components (SSCs) important to safety should have been evaluated for their susceptibility to malfunctions and failures. The susceptibility of SSCs to malfunctions and failures and the associated outcomes are reviewed to determine how the various events are categorized by type and expected frequency.

SSCs Credited for event Prevention and Mitigation: Generally, a SAR will describe more features which prevent or mitigate unwanted events than are explicitly identified in the accident analyses, because: (1) events that are prevented from occurring are not evaluated in the accident analyses, (2) some features may only be used to mitigate "non-limiting events," (3) some features may only be used as anticipatory initiators or backup aspects (e.g., addressing margin or defense-in-depth), and (4) the summary of the safety analysis, in the SAR, only describes the most important aspects and assumes others.

Overarching Intent of 50.59: The SOCs for the promulgation of the final rule states:

> "The final rule clarifies the specific types of changes…conducted at a licensed facility…that require evaluation, and revises the criteria that licensees…must use to determine when NRC approval is needed before such changes…can be implemented…The intent of the § 50.59 process is to permit licensees to make changes to the facility, provided the changes **maintain acceptable levels of safety as documented in the SAR**. The process was thus structured around the licensing approach of design basis events (anticipated operational occurrences and accidents), safety-related mitigation systems, and consequence calculations for the design basis accidents." [**emphasis** added]

Possible Ways to Fail to Maintain Safety: In an overly simplistic categorization one can fail to "maintain acceptable levels of safety as documented in the SAR" by (1) making an existing situation worse, or (2) by creating a new situation that is worse than any of the currently existing situations. The 50.59(c)(2) criteria must address both possibilities. However, 50.59(c)(2) also includes criteria to: (1) ensure the application as amended demonstrates to the NRC the methods used to determine the adequacy of existing situations are adequate – for example, see 50.59(c)(2)(viii), and (2) the NRC has reviewed most limiting events of each type and frequency – for example, see 50.59(c)(2)(v).

In summary, a plant is licensed to operate within a specified envelope, part of which is defined by the frequency and consequences of events previously evaluated in the SAR; the first four questions of 50.59(c)(2) require that changes that would result in more than a minimal increase of these frequencies or consequences, would require prior approval by the NRC. In addition, 50.59 question (c)(2)(vii) does not allow a design basis limit for a fission product barrier as described in the FSAR (as updated) to be exceeded or altered without a license amendment. There is also the possibility that a change could result in a new (and distinct) type of accident or a new malfunction exceeding the evaluated malfunctions; 50.59 questions (v) and (vi) require NRC review and approval of such events. Changes that include different equipment or different designs have the potential to create a possibility for new or different events than any previously evaluated.

[1] Typically, many analyses are conducted to ensure the most limiting events are in fact the most limiting events.

[2] Some type/frequency categories may have more than one limiting event because different events may be most limiting on different aspects.

An Engineers Understanding of the Intent of the 50.59 Rule

Accident, Malfunction, or Both

Abstract: For exiting accidents and malfunctions, the criteria for determining whether the NRC needs to review a change are the same (i.e., "more than minimal increase…"); however, if a (new or different) failure or misbehavior meets the definition for "accident," then question 10 CFR 50.59(c)(2)(v) is more limiting than question (vi).

New Rule New Meanings: The old rule (e.g., 1998) applied exactly the same criteria to accidents and malfunctions; therefore, there was never a need to determine whether an event should be considered an accident or a malfunction. The new rule (e.g., 2000) uses different criteria for (new or different) accidents and malfunctions.

Accident, Malfunction, or Both: In 10 CFR 50.59, two different words are used in six evaluation questions (i.e., "accident" and "malfunction"). Furthermore NEI 96-07 has a definition for each. Based solely on the definitions in NEI 96-07, one could understand a particular event as satisfying only one, or both definitions. For example, a loss of normal feedwater is a failure of an SSC to perform a design function (i.e., it meets the definition of malfunction), and is analyzed as an AOO (i.e., it meets the definition of accident).

Irrelevant or Conservative: For question (i) through (iv) the criteria applied to existing accidents and malfunctions are the same (i.e., "Result in more than a minimal increase in…"); therefore, there is no practical reason to make a distinction between the two. However, for questions (v) and (vi) (i.e., new or different events) there are different criteria applied to accidents and malfunctions. That is, the determination of whether an event is an accident, a malfunction, or both effectively defines the criteria that are applicable. Since questions (v) and (vi) are for new types of events created by the change, for any events that are considered to be both, question (v) is more conservative.

Guidance is needed: Since different 50.59 criteria will be applied to new accidents and malfunctions, clear guidance (for determining how an event is classified (i.e., accident, malfunction, or both) is needed to ensure the right evaluation criteria are applied.

An Accident of a Different Type

Abstract: Whether a new and distinct accident has been created by a change should be determined by its distinctiveness.

Questions (v) Intent: The SOCs for the promulgation of the final rule states (64 FR 53593):

> "accidents of a different type are distinct from those (design basis) accidents evaluated in the FSAR."

Endorsed Implementing Guidance: NEI 96-07 Rev. 1 Section 3.2 defines "Accident," which includes DBA, AOOs, transients, and natural phenomenon. In addition, NEI 96-07 Rev. 1 Section 4.3.5 describes what it means to be distinct; however, this description was misinterpreted and it was therefore clarified in a revision to RG 1.187.

An Engineers Understanding of the Intent of the 50.59 Rule

A Malfunction with a Different Result

Abstract: New or different malfunctions (i.e., malfunction modes or malfunction results) created by a change should be distinct and should be evaluated at the FMEA level of detail.

Background: The **old** 50.59 rule stated:

> "A proposed change, test or experiment shall be deemed to involve a USQ (i) if the probability of occurrence or the consequences of an accident or malfunction of equipment important to safety previously evaluated in the SAR may be increased, (ii) if a possibility for an accident or **malfunction of a different type** than any evaluated previously in the SAR may be created, or (iii) if the margin of safety as defined in the basis for any TS is reduced." [**emphasis** added to 10 CFR 50.59(a)(2)]

SECY-97-035 proposed to provide guidance for interpreting the **old** 50.59 rule:

> "If the proposed activity could lead to **a different initiator, or involves a failure mode of a different type** than the types previously evaluated, then the failure results from a malfunction of a different type (and involves a USQ), even though the accident may be the same…For example, if a pressure transmitter using mechanical linkage is replaced with an oil-filled transmitter, oil loss is now a failure mechanism which might result in a type of failure at the output of the transmitter that did not exist previously, and therefore was never analyzed. This is a new type of malfunction and should need staff review. If a digital trip system is now being used, and software failure is a new failure mode, staff review is also required." [**emphasis** added]

Subsequently the NRC proposed (63 FR 56098 see specifically 56106) to revise the 50.59 rule language and stated:

> "in response to the comments on the staff proposed guidance (NUREG-1606) on the interpretation of malfunction (of equipment important to safety) of a different type. The commenters believe that the cause of the malfunction should be a consideration in determining whether the probability of the malfunction may have increased, and that a malfunction of a different type would only be created if the effects of the malfunction are not already bounded by the FSAR analysis. The recent industry guidance states that if a component were subject to failure from a new failure mode but the failure of the component is already considered in the safety analysis, then there would not be a failure of a different type. The Commission does not agree that the industry interpretation is consistent with the rule as written, which refers to creation or possibility of a malfunction of a different type, not of a different result. However, the Commission recognizes that in its reviews, equipment malfunctions are generally postulated as potential single failures to evaluate plant performance; thus, the focus of the NRC review was on the result, rather than the cause/type of malfunction. **Unless the equipment would fail in a way not already evaluated in the safety analysis, there is no need for NRC review of the change that led to the new type of malfunction.** Therefore, as the third change in § 50.59(a)(2)(ii), the Commission is proposing to change the phrase "of a different type" to "with a different result"." [**emphasis** added]

In short, this proposed change was to eliminate the "different initiator[s]" (i.e., "cause/type of malfunction") from consideration under question (vi), and just include new modes of failure (i.e., "result"). Furthermore the SOCs (64 FR 53582) for the promulgation of the final rule stated:

> "The proposed rule discussion further stated that this determination should be made either at the component level, or consistent with the failure modes and effects analyses (FMEA), taking into account single failure assumptions, and the level of the change being made. Several commenters stated that this guidance should be revised to refer only to the failure modes and effects analysis in the FSAR, and not to specify the component level. The Commission agrees that this criterion should be considered with respect to the FMEA, but also notes that certain changes may require a new FMEA, which would then need to be evaluated as to whether the effects of the malfunctions are bounding."

In summary, new failure modes (at the FMEA level of detail) need staff review.

Guidance Clarity is a Regulatory Burden Concern

Abstract: Ambiguous guidance produces a regulatory burden.

Example: The requirements for what changes a licensee can make to a facility are governed by 10 CFR 50.59, "Changes, tests and experiments." The NRC also provides guidance for and acceptable way to implement this regulatory requirement in: RG 1.187 (which conditionally endorses NEI 96-07 Rev. 1), RIS 2002-22 (which conditionally endorsed NEI 01-01), RIS 2002-22 Supplement 1, and Appendix C.

NEI 01-01 was first endorsed by the NRC in 2002, and in 2009, the first violation (LaSalle) written as a result of the an ambiguity in NEI 01-01. The NRC issued IN 2010-10 in an attempt to clarify the ambiguity and the associated consequences. In 2013, a second violation associated with the same ambiguity was issued (Harris); subsequently the NRC issued a memo identify 11 concerns with NEI 01-01 (in subsequent meetings an additional concern was identified). During 2013 time period NEI started the effort to resolve the ambiguity; and we are still working on it today. The total time spent by industry and NRC staff is many thousands of hours.

The statement in NEI 01-01 that caused all the problems is:

> "Engineering evaluations of the quality and design processes determine if there is reasonable assurance that the likelihood of failure due to software is sufficiently low. In this evaluation, "sufficiently low" means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors)."

With the proper understanding of the engineering and associated analyses, this statement can be properly implemented, but with an inadequate engineering understanding, the implementation of this guidance has been problematic (as described above). The following paragraphs will highlight some of the engineering concepts that are needed to properly understand this guidance.

(1) CCF has consistently been a concern of the NRC since the middle of 1960s (see: History of Published Considerations of CCF). These concerns have been considered and addressed in the UFSARs, mostly through design features. Only a few CCFs are explicitly required to be addressed (e.g., ATWS, SBO, Feedwater) by specific systems or analyses.

(2) Digital system CCF come from many sources, not just failure due to software.

(3) Different design techniques are used to address different types of hazards. For example, (a) margin and conservative analyses are used to provide some protection against the design error of underestimating the severity of the event to be protected against, (b) diversity and defense in depth provide some protection against event that one cannot imagine or confidently characterize, (3) a high quality design process provides some protection against making errors.

Source of Regulatory Uncertainty

Summary: At first, the following two quotes (defining "sufficiently low") may seem clear, but this paper explains why they are misleading. This explanation will center on three terms: “that,” “considered,” and “common cause failure (CCF).” Specifically, this paper will identify some CCFs that were explicitly considered in some UFSARs.

RIS 2002-22 endorses NEI 01-01 which states:

> "sufficiently low" means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

RIS 2002-22 Supplement 1 states:

> On page 4-20 of NEI 01-01, NEI defines “sufficiently low” to mean much lower than the likelihood of failures that are considered in the updated final safety analysis report (UFSAR) (e.g., single failures) and comparable to other CCFs that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors).

That: The internet is quick to tell us how the term “that” should be understood grammatically:

> The battle over whether to use which or that is one many people struggle to get right. It’s a popular grammar question and most folks want a quick rule of thumb so they can get it right.
>
> Here it is:
>
> If the sentence doesn’t need the clause that the word in question is connecting, use which. If it does, use that. (Pretty easy to remember, isn’t it?) Let me explain with a couple of examples.
>
> (1) Our office, which has two lunchrooms, is located in Cincinnati.
>
> (2) Our office that has two lunchrooms is located in Cincinnati.
>
> These sentences are not the same. The first sentence tells us that you have just one office, and it’s located in Cincinnati. The clause which has two lunchrooms gives us additional information, but it doesn’t change the meaning of the sentence. Remove the clause and the location of our one office would still be clear: Our office is located in Cincinnati.
>
> The second sentence suggests that we have multiple offices, but the office with two lunchrooms is located in Cincinnati. The phrase that has two lunchrooms is known as a restrictive clause because another part of the sentence (our office) depends on it. You can’t remove that clause without changing the meaning of the sentence.

The simple literal understanding of the quotations above imply that some CCFs were considered in the UFSAR, and that some were not. If all CCF were not considered in the UFSAR, then “which” would have been the right word to use.

Considered: One interpretation of the term “considered” (in the first two quotations above) is, “analyzed in the accident analysis (or safety analysis);” however, this interpretation is not consistent with how CCF is typically addressed (see further below) and the use of “consider” in 10 CFR Part 50 Appendix A which states:

> “The development of these General Design Criteria is not yet complete. For example, some of the definitions need further amplification. Also, some of the specific design requirements for structures, systems, and components important to safety have not as yet been suitably defined. Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include:
>
> (1) Consideration of the need to design against single failures of passive components in fluid systems important to safety. (See Definition of Single Failure.)
>
> (2) Consideration of redundancy and diversity requirements for fluid systems important to safety. A "system" could consist of a number of subsystems each of which is separately capable of performing the specified system safety function. The minimum acceptable redundancy and diversity of subsystems and

components within a subsystem, and the required interconnection and independence of the subsystems have not yet been developed or defined. (See Criteria 34, 35, 38, 41, and 44.)

(3) Consideration of the type, size, and orientation of possible breaks in components of the reactor coolant pressure boundary in determining design requirements to suitably protect against postulated loss-of-coolant accidents. (See Definition of Loss of Coolant Accidents.)

(4) Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems. (See Criteria 22, 24, 26, and 29.)"

Is short, the all applicants should have "considered," among other things, "the possibility of systematic, nonrandom, concurrent failures," and they have in fact done so, as described further below.

CCF: The NRC has used the terms CCF and CMF interchangeably, however, not everybody does. The scope of CCF includes "unknowns" which can only be addressed by diversity and defense-in-depth. CCF includes but in not limited to, "systematic, nonrandom, concurrent failures."

Design Attributes to Address CCF: Early documents described hazards (e.g., CCF), but as design techniques (e.g., incorporation of specific design attributes) were found that address these hazards (e.g., diversity and defense-in-depth), these design techniques became the subject of regulatory criteria, and discussion of the specific hazards was reduced. That is, in some parts of the NRC today, there is a lot of discussion about defense-in-depth, but very little discussion about the various hazards (e.g., CCF) this design attribute addresses.

See History of Published Considerations of CCF for a comprehensive description of how CCFs were explicitly considered.

Likelihood of CCFs that are considered in the UFSAR: The two RIS 2002-22 related quotations above imply CCFs that were not considered are less likely than those that were. It may not be possible to quantify the likelihood of CCFs that were not considered, but we can characterize the likelihood of CCFs that were considered, by looking at a historical document. The General Electric response to the 1969 AEC letter (i.e., NEDO-10189) characterized the likelihood of the CCFs that it considered:

"This report contains analyses of the effects of a broad spectrum of simultaneous multiple functional failures in critical safety and protection equipment in the General Electric Boiling Water Reactor. These are hypothetical failures, presented herein for purposes of analysis only. These failures have not occurred, nor are they expected to occur. In fact, the subject equipment has been designed specifically to avoid these failures. In many cases, it is virtually impossible to identify even a hypothetical cause for the failures; yet the effects are thoroughly evaluated in this report in the interest of better understanding of the protection provided."

Likelihood of CCFs that are NOT considered in the UFSAR: One can only conclude that the likelihood of CCF not considered in the UFSAR are less likely than one where "it is virtually impossible to identify even a hypothetical cause for the failure;" therefore, if you can think of a hypothetical cause for CCF (e.g., software), then it is of higher likelihood than the CCF considered in the UFASR.

Ambiguity: Do you think NEI would agree with this position, which is based on quotations? If the answer is "no," then there must be some ambiguity in the first two quotations above.

Example errors that were considered: The NEDO-10189 states:

"resistance to random failures does not necessarily guarantee resistance to failures potentially arising from such causes as (1) the use of equipment with a common defect, (2) the erroneous calibration of redundant channels by one maintenance technician, or (3) the limitation in predicting changes in a key plant parameter used for protection or control following a postulated incident.

…

The task of common-mode failure analysis seems to have infinite proportions limited only by the human imagination unless bounded in some manner. For this reason, General Electric found it necessary to develop a rationale for approaching the problem that would yield useful results without at the outset becoming burdened with unnecessary detail.

The balance of this introduction is devoted to a discussion of various types of common-mode failures that have been identified, various potential remedies for them, and a basis for the selection of functional diversity as the primary emphasis for this study.

There are several types of common-mode failures which could potentially affect the performance of protection or control instrumentation. Four general categories of common-mode failures are:

1. **Functional deficiency -** The plant variable being monitored does not provide the information· needed during or following a plant event. One cause of such a deficiency could be the inability to predict with sufficient accuracy the changes in the key variable as a result of the event. An unanticipated change in plant characteristics could also be the cause of a functional deficiency.
2. **Maintenance error -** This common-mode failure could be caused by consistent mis-calibration of all instrumentation for a given parameter. Also included in this category are failures resulting from repair work errors which functionally disable all the instrumentation for a given parameter.
3. **Design deficiency -** This category includes those failures attributable either to unrecognized dependence on a single, common element or to a common deficiency in a characteristic of all the instrumentation of a certain type.
4. **External event -** This category includes those failures resulting from such events as fire, earthquake, flood, etc. Inadequate physical separation of instrumentation channels or components could produce a susceptibility to common failure due to lesser events such as a falling object or a small steam leak."

In short, all of the examples in the first two quotations above, were in fact considered; however, they may not have been specifically analyzed in Chapter 15.

Divide and Conquer and the Lost Third Step

There is a general methodology or cognitive strategy used when dealing with complex or multifaceted phenomena, and this strategy sometimes goes by the name of "Divide and Conquer." The problem with this name is that some people think it describes the entire strategy, and because of this they forget to implement the third step (another failure of knowledge management). The first step is to separate or partition the phenomena into separate facets or categories, each of which can be worked relatively independently. The second step is to work each of the separate partitions. The final and often forgotten step is to then integrate the results of the individual efforts into a cohesive whole and evaluate as a whole (Ok, maybe there are more steps, i.e., repeat as needed). This final step is very important because: (1) it helps identify problems with the initial plan (or implementation of that plan), and (2) individual disciplines or sectors tend to think or reason in different manners using different terms or concepts which can lead to inconsistencies or incompatibilities.

By simply endorsing Appendix D, the NRC would be failing to implement this "lost third step." That is, the NRC should clearly document the intent of the 50.59 rule and the role that each of the eight evaluation questions plays in accomplishing that very intent. In addition, the NRC should document the evaluate of how the endorsed guidance meets the intent of the rule. A simple clean endorsement of Appendix D is simply inappropriate. Put another way, simply stating that something is acceptable, does not explain why it is acceptable, which has led to problems in the past. No one can predict the future, but some use that past as indicators of what could happen in the future (e.g., operational experience program). Why create the potential for problems?

In short, without a clear statement of the intent of the 50.59 rule, or a documented evaluation of how the guidance meets the intent of the rule, the NRC has not demonstrated that it fully understands what it is endorsing.

Common Misunderstandings Regarding 50.59

Abstract: The 50.59 guidance is complicated and confusing to some; therefore, some people create simplified, and inaccurate summaries of the guidance, as described below. Some of these inaccuracies need to be explicitly identified so they do not result in the acceptance (e.g., by endorsing Appendix D) of inconsistencies with existing guidance. **Note:** Guidance is only guidance (i.e., it is not a regulatory requirement); therefore, one should clearly distinguish between: (1) conformance with guidance (and therefore complying with the underlying rule), and (2) non-conformance with the guidance but compliance with the rule. This is part of knowledge management.

(A) General Consideration on the use of terms

(1) We must keep in mind that when using words in conversation, some words have very few meanings (e.g., bubble gum & sunshine) while other words have many different meanings (e.g., Love), which have their specific meanings determined by the specific context. Different disciplines within the NRC may use the same terms in different ways.

(2) The lawyers at the NRC like us to use certain specific words as if they had one and only one specific meaning (e.g., Requirement).

(3) Sometimes (2) conflicts with (1). That is why if you use the word “requirement” in casual conversation to mean something other than what is written in the CFR, a good NRC employee will correct you.

(B) Meaning of Term “Margin” NEI 96-07 Rev. 1

Some people say, “the licensee is allowed to play with margin,” or “the licensee owns the margin,” under 50.59 and understand this as a general delegation to the licensees; however, these statements are overly simplistic and misrepresent the NRC endorsed 50.59 guidance. For example, 50.59(c)(2)(iii) and (iv) only allow a minimal increase in consequences (regardless of the amount of margin that may exist wit hrespect to consequences). Furthermore, RG 1.187 endorses NEI 96-07 Rev. 1., which only uses the term “margin” in very specific ways:

(1) margin of error, for example, NEI 96-07 Section 3.4 states:

> “Results are "essentially the same" if they are within the margin of error for the type of analysis being performed.”

(2) Space between expected plant behavior and “the analysis presented in the UFSAR”, for example, NEI 96-07 Section 4.2.1.3 Example 3, which states:

> “The steamline break mass and energy release calculations were originally performed at a power level of 105% of the nominal power (plus uncertainties) in order to allow margin for a future power up-rate. The utility later decided that it would not pursue the power up-rate and wished to use the margin to address other equipment qualification issues….”

(3) The space between the “Design basis limits” and “the analysis presented in the UFSAR” for example, NEI 96-07 Rev. 1 Section 4.3.8.1 states:

> “Gaining margin by changing one or more elements of a method of evaluation is considered to be a nonconservative change and thus a departure from a method of evaluation for purposes of 10 CFR 50.59. Such departures require prior NRC approval of the revised method. Analytical results obtained by changing any element of a method are "conservative" relative to the previous results, if they are closer to design bases limits or safety analyses limits (e.g., applicable acceptance guidelines). For example, a change from 45 psig to 48 psig in the result of a containment peak pressure analysis (with design basis limit of 50 psig) using a revised method of evaluation would be considered a conservative change when

applying this criterion. In other words, the revised method is more conservative if it predicts more severe conditions given the same set of inputs."

In another location, relating to guidance on whether an activity results in a design basis limit for a fission product barrier being exceeded or altered, NEI 96-07 Rev. 1., implies there is a space between the "Design basis limits" and "the analysis presented in the UFSAR" (but does not explicitly refer to this as margin), for example, NEI 96-07 Rev. 1. Section 4.3.7 states:

"If an engineering evaluation demonstrates that the analysis presented in the UFSAR remains bounding, then no 10 CFR 50.59(c)(2)(vii) evaluation is required. When using these techniques, both indirect and direct effects must be considered to ensure that important interactions are not overlooked…

Any increase in peak containment post-accident pressure would be compared to the design basis limit, in this case, containment design pressure. If the revised peak post-accident containment pressure exceeded the design basis limit, then a license amendment would be required."

As stated above, **some** changes in margin are described as being acceptable under 50.59 and some are not, other changes that allow a bad situation to get worse are also acceptable.

In summary, if one changes the analysis methods, and the new method shows less margin, this acceptable (**Note:** If it shows more margin it would not be acceptable.). However, changing the plant to approach (but not exceed) design basis limits for fission product barriers is acceptable (as summarized above), but this is a very different case from changing the design basis limit (in either direction), which is not acceptable.[1] Another margin that can be reduced is the margin between how the plant behaves and how the analysis was conducted (i.e., the analysis was way too conservative). The first four 50.59(c)(2) criteria revolve around retaining the limiting values in the analysis of the limiting events, thus in effect maintaining margin between the analysis and any associated acceptance criteria and associated regulatory requirements.

In addition to the specific guidance (for 50.59) referenced above, the term "margin" is also used in other regulatory requirements, for example:

"Criterion 2—Design bases for protection against natural phenomena. Structures, systems, and components important to safety shall be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. The design bases for these structures, systems, and components shall reflect: (1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with **sufficient margin** for the limited accuracy, quantity, and period of time in which the historical data have been accumulated, (2) appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena and (3) the importance of the safety functions to be performed.

Criterion 10—Reactor design. 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

[1] NEI 96-07 Section 4.3.7 example 3 states:
"Example 3
Recently identified corrosion inside the primary containment has prompted a re-evaluation of the existing containment design pressure of 55 psig. This reevaluation has concluded that a design pressure of 48 psig is the maximum supportable. As the final resolution to the degraded containment condition, the licensee proposes to reduce the containment design pressure as reflected in UFSAR safety analyses from 55 to 48 psig.
…
The design basis limit itself has been "altered" and thus a license amendment is required. The issue of conservative vs. nonconservative is not germane to requiring a submittal. That is, prior NRC approval is required regardless of direction because this is a fundamental change in the facility's design."

exceeded during any condition of normal operation, including the effects of anticipated operational occurrences.

Criterion 26—Reactivity control system redundancy and capability. Two independent reactivity control systems of different design principles shall be provided. One of the systems shall use control rods, preferably including a positive means for inserting the rods, and shall be capable of reliably controlling reactivity changes to assure that under conditions of normal operation, including anticipated operational occurrences, and with **appropriate margin** for malfunctions such as stuck rods, specified acceptable fuel design limits are not exceeded. The second reactivity control system shall be capable of reliably controlling the rate of reactivity changes resulting from planned, normal power changes (including xenon burnout) to assure acceptable fuel design limits are not exceeded. One of the systems shall be capable of holding the reactor core subcritical under cold conditions.

Criterion 27—Combined reactivity control systems capability. The reactivity control systems shall be designed to have a combined capability, in conjunction with poison addition by the emergency core cooling system, of reliably controlling reactivity changes to assure that under postulated accident conditions and with **appropriate margin** for stuck rods the capability to cool the core is maintained.

Criterion 31—Fracture prevention of reactor coolant pressure boundary. The reactor coolant pressure boundary shall be designed with **sufficient margin** to assure that when stressed under operating, maintenance, testing, and postulated accident conditions (1) the boundary behaves in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the boundary material under operating, maintenance, testing, and postulated accident conditions and the uncertainties in determining (1) material properties, (2) the effects of irradiation on material properties, (3) residual, steady state and transient stresses, and (4) size of flaws.

Criterion 50—Containment design basis. The reactor containment structure, including access openings, penetrations, and the containment heat removal system shall be designed so that the containment structure and its internal compartments can accommodate, without exceeding the design leakage rate and with **sufficient margin**, the calculated pressure and temperature conditions resulting from any loss-of-coolant accident. This **margin** shall reflect consideration of (1) the effects of potential energy sources which have not been included in the determination of the peak conditions, such as energy in steam generators and as required by § 50.44 energy from metal-water and other chemical reactions that may result from degradation but not total failure of emergency core cooling functioning, (2) the limited experience and experimental data available for defining accident phenomena and containment responses, and (3) the conservatism of the calculational model and input parameters.

Criterion 51—Fracture prevention of containment pressure boundary. The reactor containment boundary shall be designed with **sufficient margin** to assure that under operating, maintenance, testing, and postulated accident conditions (1) its ferritic materials behave in a nonbrittle manner and (2) the probability of rapidly propagating fracture is minimized. The design shall reflect consideration of service temperatures and other conditions of the containment boundary material during operation, maintenance, testing, and postulated accident conditions, and the uncertainties in determining (1) material properties, (2) residual, steady state, and transient stresses, and (3) size of flaws."

The NRC concluded the applicant met these requirements, and therefore provided reasonable assurance of adequate safety. Those margins explicitly required by the regulations and evaluated by the staff should not be reduced under 50.59.

(C) Definitions in Guidance

RG 1.187 endorses NEI 96-07 Rev. 1., which includes definitions for:

(1) "Accident Previously Evaluated in the FSAR (as updated)" - This phrase is used in 10 CFR 50.59(c)(2)(i) and (iii).
(2) "Malfunction of an SSC Important to Safety" - This phrase is used in 10 CFR 50.59(c)(2)(ii), (iv) and (vi).
(3) "Safety Analysis" - The phrase "safety analyses" is used in 10 CFR 50.59(a)(2) and (c)(2)(viii).

In casual conversation the first two definitions are sometimes used as general definitions of the terms "accident" and "malfunction;" however, this understanding is not correct. The 10 CFR uses the terms "accident" and "malfunction" in many places (e.g., for malfunction see GDC 25 & 26), and the general meaning of these terms in the CFR (and guidance) is not changed by the definition of these phrases in 50.59 related guidance. If we generally made the assumption that definitions in guidance changed the meaning of terms in the CFR (as opposed to clarifying their meaning), then the endorsement of guidance which contains definitions of terms in the CRF should generally be considered rule making.

In short, definitions in guidance should always be understood in a way that is consistent with how the terms are used in the CFR and not as a change to the meaning of the terms in the CFR. Furthermore, the definition and use of terms in one set of guidance (e.g., 50.59) should not be applied more generally to all guidance (e.g., the SRP); this basic understanding is necessary, otherwise it would not be possible for the NRC to understand what it is approving. The volume of CFR and related guidance is so large, that it would not be possible to evaluate the effect that a change in meaning in one location had on all other locations.

Consistency with 10 CFR 50.92

Contradiction: Effectively the guidance in Appendix D states that anything short of a significant reduction in a margin of safety (which is also understood to constitute a "significant hazard") maintains acceptable levels of safety as documented in the SAR, which seems to be contradiction.

Abstract: The guidance for determining whether a proposed change would constitute a "significant hazard" includes guidance for determining whether there is "a significant reduction in a margin of safety". This guidance basically states that a change which exceeds or alters a design basis or safety limit (i.e., the controlling numerical value for a parameter established in the UFSAR or the license) is a significant reduction in a margin of safety and therefore a significant hazard. The SOCs for the promulgation of the final 50.59 rule state the intent of the rule is to maintain acceptable levels of safety as documented in the SAR. The proposed guidance in Appendix D Section 4.3.6 uses, in part, the "design basis limit" (i.e., a value that is considered to be a significant reduction in a margin of safety) as the value for maintaining acceptable levels of safety as documented in the SAR.

It is generally assumed that a licensee should not be able to make a change to a facility under 10 CFR 50.59, "Changes, tests and experiments.," which the staff cannot approve without a public hearing per 10 CFR 50.91, "Notice for public comment; State consultation," and 10 CFR 50.92, "Issuance of amendment," which states:

> "(c) The Commission may make a final determination, under the procedures in § 50.91, that a proposed amendment to an operating license or a combined license for a facility or reactor licensed under §§ 50.21(b) or 50.22, or for a testing facility involves no significant hazards consideration, if operation of the facility in accordance with the proposed amendment would not:
> (1) Involve a **significant** increase in the probability or consequences of an accident previously evaluated; or
> (2) Create the possibility of a **new or different** kind of accident from any accident previously evaluated; or
> (3) Involve a **significant** reduction in a margin of safety."

Since 50.59 does not allow changes, without prior staff approval, that would more than minimally increase the probability or consequences of an accident (per 10 CFR 50.59(c)(2)(i) and (III)), the above assumption is confirmed in the statements of the regulatory requirements themselves.

Since 50.59 does not allow changes, without prior staff approval, that would create the possibility of a different type of accident (per 50.59(c)(2)(v)), the above assumption is confirmed in the statements of the regulatory requirements themselves. The SOCs for the 50.59 rule explicitly discussed the wording in 50.92 when explaining the choice of the wording for 50.59(c)(2)(v).

In order to continue the above consistency described above, and guidance in 50.59 for malfunctions should not violate the criteria in 50.92(c). Specifically, any new malfunctions created should not be allowed to significantly reduce the margin of safety (or violate 50.92(c)(1) & (2) for that matter).

The SOCs (51 FR 7746) for the promulgation of the initial "no significant hazards" consideration stated:

> "It is important to bear in mind as one reads this background statement and the final regulations that there is no intrinsic safety significance to the "no significant hazards consideration" standard.…
>
> In short, the "no significant hazards consideration" standard is a procedural standard which governs whether an opportunity for a prior-hearing must be provided before action is taken by the Commission, and, as discussed later, whether prior notice for public comment may be dispensed with in emergency situations or shortened in exigent circumstances."

Based on this reasoning, the criteria in 50.59 should also be understood as procedural, not based on safety significance; however, the justification (promoted by NRC senior management) for acceptability of the proposed criteria in Appendix D is that it is not safety significant. Furthermore, 10 CFR 50.91(a)(1) requires that the licensee provide its analysis of the issue of no significant hazards consideration (NSHC) using the standards in 10 CFR 50.92. RIS 2001-22 (ML011860215) provides the following guidance to licensees on preparing an NSHC analysis:

> "Safety margins are applied at many levels to the design and licensing basis functions and to the controlling values of parameters to account for various uncertainties and to avoid exceeding regulatory or

licensing limits. The specific values that define margin are established in each plant's licensing basis. Licensees should identify the safety margins that may be affected by the proposed change and review the conservatism in the evaluation and analysis methods that are used to demonstrate compliance with regulatory and licensing requirements. The safety margin before the change should be compared to the margin after the proposed change to determine if the amendment will reduce the margin, and if the change is significant. **If a change does not exceed or alter a design basis or safety limit (i.e., the controlling numerical value for a parameter established in the UFSAR or the license) it does not significantly reduce the margin of safety.** In other cases, the assessment of significance for this standard should be made on the same basis as discussed in the guidance for the first standard. Uncertainties and errors need to be considered in calculating the margin." [**emphasis** added]

NEI has, in effect, proposed, in Appendix D Section 4.3.6, that this same **emphasized** criterion be used for 10 CFR 50.59(c)(2)(vi) which is not consistent with the "not more than minimal" philosophy of 50.59.

Inappropriate Implementation of RG Development

The implementation of the revision to RG 1.187 to incorporate Appendix D has been inconsistent with: (1) regulation, (2) the commission's policy that activities be undertaken in an open and transparent manner, (3) NRC Management Directives, RES Office Instructions. Based on these procedural transgressions, the RG should not be issued.

10 CFR 50.59: The guidance in Appendix D does not implement the requirements stated in the 10 CFR 50.59 rule, which states:

> "(2) A licensee shall obtain a license amendment pursuant to Sec. 50.90 prior to implementing a proposed change, test, or experiment if the change, test, or experiment would:…
>
> (vi) Create a possibility for a malfunction of an SSC important to safety with a different result than **any** previously evaluated in the final safety analysis report (as updated);" [**emphasis** added]

There are various results that can occur from each malfunction, for example:

The number of valves failing (e.g., open or closed)
The impact of the valves failing on the flow
The impact of the flow on analysis assumptions
The impact of the flow on analysis outcomes (e.g., temperature, pressure, DNBR, …)
The impact on compliance with guidance
The impact on compliance with regulatory requirements

The guidance in Appendix D chooses to use the least conservative impact as the acceptance criteria; therefore, in effect, the guidance changes the meaning of "any" in the rule to be "all."

Management Directive: RES Office instruction TEC-004, "Regulatory Guide Review, Development, Revision, and Withdrawal Process," referenced MD 6.6, "Regulatory Guides," which states:

> "It is the policy of the U.S. Nuclear Regulatory Commission that—
>
> — Activities are undertaken in an open and transparent manner.
>
> — Staff decisions are sound and consider the need for and impact of proposed actions."

Contrary to the first policy position above, the NRR front office, and OGC have engaged in substantive technical discussion regarding the content of Appendix D (for many months), without any public meeting or the majority of technical staff assigned to being involved.

Contrary to the second policy position above, the technical review staff for Appendix D do not believe the guidance in Appendix D is technically sound. The NRR front office believes it to be technically sound because OGC provided an NLO. There is no explanation provided as to why the guidance in Appendix D is technically sound.

Safe – Necessary but Not Sufficient

Some in NRC management put forth the position that a license should be able to make changes under 50.59 that are safe. I agree, but this position is misleading, as explained below.

Does this position lead one to conclude that only unsafe changes require prior NRC approval? No. By law, the NRC cannot approve changes that it deems unsafe. Therefore, the NRC would probably either agree with the licensee (that the change is unsafe) and deny the proposed change, or disagree with the licensee (i.e., the NRC could conclude the change is safe even though the licensee stated under oath and affirmation that it was unsafe) and tell the licensee they should make this change under 50.59. This reasoning seems ridiculous, but seems to be a logical extension to the position first stated above.

The problem is that both changes made under 50.59 and those approved by the NRC must be safe. That is, "safe" is a necessary but not sufficient condition for determining a change can be made under 50.59. Without changing the rule, one must look at the eight criteria under 10 CFR 50.59(c)(2) for making the determination. It should be noted that these eight criteria do not include the term "safe," nor are the eight criteria in 50.59 adequate for determining safety. Effectively, the entire UFSAR demonstrates adequate assurance of reasonable safety.

Licensing versus Engineering

Abstract: In Appendix D, NEI has chosen an approach which they characterize as "licensing." That is, NEI has taken several partial quotations, out of context, and combined them to create new meaning or new interpretations of existing text. This approach is technically incorrect and removes focus from the engineering aspects necessary to ensure a change is within the licensing basis. Furthermore, the NRC should not encourage this approach since new or different definition in one document may be used change the meaning in another (i.e., a change in meaning the NRC neither considered or explicitly approved).

Out of Process Meetings: It is a shame that all the discussions between: (1) NEI, and (2) NRC/ OGC and NRC Senior Management were not made in a public setting (and even more so that the majority of the technical staff were also not included), furthermore, the various versions and comments on those versions are also not publicly available. Because these items are not publicly available (some versions were internally available), I cannot provide references to them, and you the reader, must either believe me, or not. This material would have provided some indication on how NEI intends their text in Appendix D to be used.

Radiation Monitor Example: In one example, a propose change resulted in a CCF (whose likelihood was not sufficiently low) which would have resulted in the complete loss of all radiation monitors; however, the example concluded this was consistent with regulations because GDC 64 did not include any "single failure" requirement. There are many things that are wrong (technically) with this example and associated reasoning. First there are several design techniques that are all used to address CCF, as stated in various NRC documents (see History of Published Considerations of CCF), for example: a high quality design process, margin, conservative assumptions, independence, diversity, and defense-in-depth. In an engineering approach, one must examine the specifics of the UFSAR to determine which if any, design techniques were employed in the design of the radiation monitors to address CCF, then one must determine why the likelihood of CCF was not sufficiently low, and finally if the change resulted in an inconsistency with a design technique or principle.

Different Result Example: Section 4.3.6 of Appendix D starts with two and a half pages of partial quotation (and associated "interpretations") taken out of context to justify a different interpretation of the meaning and intent of 10 CFR 50.59(c)(2)(vi). The statements of consideration for the promulgation of the final rule very clearly state that the malfunction result should be considered at the level of the FMEA in the UFSAR. Section 4.3.6 effectively states that a "different result" evaluation is effectively a plant level evaluation of compliance with regulations. In affect for the NRC to provide "prior" approval of a change that fails the criteria in Section 4.3.6, the applicant would need to docket an exemption request (per 10 CFR 50.12) and/or possibly make a significant hazard declaration.

Specific Issues with NEI 96-07 Rev. 1 Appendix D

Abstract: Although there are many individual problems with the guidance and examples in Appendix D, the bigger issues are the conceptual problems.

NRC Review of Most Limiting Events: As a result of the guidance in Section 4.3.6 described below, the basic licensing principle that the NRC reviews the most limiting events, the methods to address them, and the associated evaluations will no longer be true.

The criterion of 10 CFR 50.59 (c)(2)(vi) are applied to changes that effect a design function:

> "(2) A licensee shall obtain a license amendment pursuant to Sec. 50.90 prior to implementing a proposed change, test, or experiment if the change, test, or experiment would: …
>
> (vi) Create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the final safety analysis report (as updated);"

Some of the guidance in Section 4.3.6 (see quotation below) does not include evaluation (or comparison) of the new malfunction against what was evaluated in the UFSAR, but rather but rather against regulatory requirements (which is inconsistent with the plain language understanding of the regulatory requirement of 10 CFR 50.59 (c)(2)(vi)).

> "If the results of revised evaluations are inconsistent with the "regulations, license conditions, orders or technical specifications" that were identified as part of Step 2, then the proposed activity creates the possibility for a malfunction of an SSC important to safety with a different result."

In addition, the criteria used for making the determination are being redefined to be the acceptance criteria for limiting event evaluations in the accident analysis, which in many cases are the associated regulatory requirements.

> "if any of the previous evaluations of involved malfunctions of an SSC important to safety have become invalid due to their basic assumptions no longer being valid (e.g., single failure assumption is not maintained), or if any existing safety analysis is no longer bounding (e.g., the revised safety analysis no longer satisfies the acceptance criteria identified in the associated safety analysis), then the proposed activity creates the possibility for a malfunction of an SSC important to safety with a different result. If the acceptance criteria are still satisfied and the basic assumptions remain valid, there is no different result even if the malfunction of an SSC important to safety would otherwise cause changes to input parameters described in the UFSAR.
>
> As part of the response and determining if the malfunction results continue to be bounded, include the impact on the severity of the initiating conditions and the impact on the initial conditions assumed in the associated safety analysis. Specifically, consider any design functions that, if not performed, would initiate a transient or accident that the plant is required to withstand."

The safety analysis and acceptance criteria (which in many cases are a restatement of the regulatory requirements) are two different things, but the highlighted portion seems to be trying to redefine "safety analysis" to be "regulatory requirements." As a result of this guidance, a licensee can make changes that result in a malfunction which is significantly worse than the most limiting event analyzed by the staff. (Note: In one UFSAR examined the event outcome was an order or magnitude less severe than the associated acceptance criteria – i.e., the associated regulatory requirement.)

Meeting Obligations: In NEI 96-07 Rev. 1, the guidance for both questions (c)(2)(i) and (c)(2)(ii) states:

> "Although this criterion allows minimal increases, licensees must still meet applicable regulatory requirements and other acceptance criteria to which they are committed (such as contained in regulatory guides and nationally recognized industry consensus standards, e.g., the ASMIE B&PV Code and IEEE standards). Further, departures from the design, fabrication, construction, testing and performance standards as outlined in the General Design Criteria (Appendix A to Part 50) are not compatible with a "no more than minimal increase" standard."

If this guidance is inadequate, then it should be modified in Sections 4.3.1 & 4.3.2 of NEI 96-07 Rev. 1 (or, less preferably, Sections 4.3.1 & 4.3.2 of Appendix D). It is unnecessary and redundant to put similar guidance in Section 4.3.6 of Appendix D, because:

> If criteria, that is less conservative than that in (c)(2)(i) & (ii) were added to another evaluation question, it would serve no practical purpose, because the criteria in (c)(2)(i) & (ii) would be limiting. In addition, if criteria, that is more conservative than that in (c)(2)(i) & (ii) are added to another evaluation question, it could be considered a backfit. (**Note:** Based on these last two sentences alone, it is inappropriate to add guidance or examples to address meeting applicable regulatory requirements and other acceptance criteria to which they are committed in Appendix D Section 4.3.6.)
>
> In addition to the regulatory burden of doing effectively the same thing in two different ways, it could add confusion since the different wording of the guidance could lead to different conclusions.

Fission Product Barriers: Question (c)(2)(vii) applies to all changes that affect the design basis limits for fission product barriers described in the SAR. Any change that fails 50.59 question (c)(2)(vii) requires a license amendment. No other questions should be used for evaluating changes to design basis limits for fission product barriers because:

> If criteria, that is less conservative than that in (c)(2)(vii) were added to another evaluation question, it would serve no practical purpose, because the criteria in (c)(2)(vii) would be limiting. In addition, if criteria, that is more conservative than that in (c)(2)(vii) are added to another evaluation question, it could be considered a backfit. (**Note:** Based on these last two sentences alone, it is inappropriate to add guidance or examples to address fission product barriers in Appendix D Section 4.3.6.)
>
> In addition to the regulatory burden of doing effectively the same thing in two different ways, it could add confusion since the different wording of the guidance could lead to different conclusions.

Guidance for when to do an FMEA: It is generally understood that a good change process (e.g., design change process) will consider the things that could go wrong and will generate an FMEA if appropriate. In addition, the guidance associated with updating/maintaining the UFSAR is adequate for when the FMEA in the UFSAR should be updated. The guidance related to FMEAs in Appendix D should not be construed to effect or alter the previous two sets of guidance; therefore, it appears that Appendix D is adding criteria for performing an additional FMEA as part of the 50.59 evaluation process, which could be considered a backfit. The FMEA guidance is not necessary for applying the criteria in the guidance for performing the evaluation questions. Finally, it presumes the change process is inadequate since the consideration of the possible things that could go wrong were not adequately performed.

GDC vs. Principle Design Criteria of the facility: The guidance in Appendix D Section 4.3.6 is based on the generally design criteria (GDC) (with a small note about the principle design criteria of the facility). The guidance should only address the principle design criteria of the facility. The application of processes based on the GDCs to facilities that are not obligated to meet the GDCs has been considered in other contexts to be a backfit.

Distinction between "design function" and "design basis function": The guidance in Appendix D Section 4.3.6 requires making a determination of whether a function impacted is a "design function" or a "design basis function," but in the last step, the same criteria is applied to both; therefore, this distinction and the associated complication to the guidance are unnecessary. Furthermore, the guidance is confusing and therefore an unnecessary regulatory burden.

Wrong Criteria: The acceptability of CCFs should also be evaluated by Questions (C)(2)(ii). The guidance in NEI 96-07 Rev. 1 Section 4.3.2 states

> "The safety analysis assumes certain design functions of SSCs in demonstrating the adequacy of design. Thus, certain design functions, while not specifically identified in the safety analysis, are credited in an indirect sense.
>
> …

if failures were previously postulated on a train level because the trains were independent, a proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether the likelihood of malfunction has been increased.

…

Examples 5-8 are cases that would require prior NRC approval because they would result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety:…

Example 6

The change would reduce system/equipment redundancy, diversity, separation or independence."

Certain, but not all CCFs should be considered a reduction of "system/equipment redundancy, diversity, separation or independence;" therefore, criteria should be included in Section 4.3.2 of Appendix D to determine when a CCF is a reduction. For example, if the likelihood of CCF of redundant and independent trains of a safety system is determined to be "not sufficiently low," then independence has been reduced. Another approach would be that if the licensing guidance in BTP 7-19 is met, then diversity and independence have not been reduced (this would allow some reductions – most engineers agree that some reductions are ok, but there is no guidance to determine which).