U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Modernization Plan #1D
BTP 7-19 Update

Public Meeting

NRC Staff Presentation

April 4, 2019

Agenda

- How did we get here?
- Examination of previous D3 Assessments
- NRC response to industry stated concerns regarding Staff position on D3 Assessments
- New risk-informed graded approach to address common cause failures (CCF)
- Schedule update / SRP revision process

Key Messages

- NRC staff fully supports the safe modernization of plants with Digital I&C
- Updating guidance to include guiding principles described in SECY 18-0090
  - Clarify CCF expectations
  - Clarify NRC's guidance to improve usability for stakeholders
- Industry participation in this process is essential

How Did We Get Here?

- Industry has stated that key sections of BTP 7-19 may be a barrier towards modernization of plants using digital I&C technology based upon:
  - Feedback received during several CCF public meetings
  - Written feedback provided to NRC Staff
  - Feedback during development of RIS 2002-22 Supplemental guidance for 10 CFR 50.59
- Industry and Staff identified challenges and the need for the right balance between flexibility and clarity regarding when and where a D3 assessment would be required, as well as the level of effort necessary

Directions to Update BTP 7-19 (MP#1D)

- The update will be consistent with the guiding principles in SECY 18-0090 **(ML18179A066)**
  - Alignment with Supplement 1 to RIS 2002-22 **(ML18143B633)**

- The update will support on-going activities along with similar industry approach done under MP1A

NRC Response to Stated Industry Concerns

Industry Concern	NRC Response
Does the NRC staff require BTP 7-19 to be used when performing a DI&C modification under 10 CFR 50.59 for non-RPS/ESF system modernizations?	No, the licensee is NOT required to implement BTP 7-19 for digital modifications under 10 CFR 50.59. BTP 7-19 is specifically targeted as guidance to staff for license amendments and design certifications.
Does the NRC staff require a full D3 analysis of postulated failure concurrent with a DBE to be performed for all safety significant systems?	No. Defense-in-depth needs to be evaluated for systems to address vulnerabilities against CCF as commensurate with relative safety significance to the plant.

NRC Response to Stated Industry Concerns

Industry Concern	NRC Response
Is it true that NRC staff requires diverse systems to backup all DI&C safety systems and they have to be analog?	No. BTP 7-19 does not "require" diverse systems or specify technology. There are multiple options for addressing defense-in-depth.
Does the NRC staff require that applicants perform 100% testing of the digital system to address CCF?	100% testability is NOT required to address CCF. BTP 7-19 states testability can be used to eliminate further consideration of CCF under certain conditions (i.e. sufficiently simple). This provision is being clarified.

Examination of D3 Assessments Approved by NRC

- NRC staff examined D3 assessment approaches previously approved by NRC (provided in a separate handout)
- Diverse systems were not required, unless identified for limited protective functions which could not meet BTP 7-19 criteria
- Applicants have decided to include diverse actuation systems up-front in the design, but this was not required by NRC staff
  - Conversely, an applicant may choose not to (e.g. NuScale)

Potential Update Areas in BTP 7-19 to Date

- Scope of Applicability for D3 Assessment
- Defining a Graded Approach
- Clarification of Design Attributes in Section 1.9
- Clarification of Acceptance Criteria Guidance in Section 3

Proposed Scope of Applicability for D3 Assessments

- A D3 Assessment is needed for protection systems (RPS, RTS, ESF, ESFAS) in most plant designs.
  - Consistent with diversity requirements (e.g. GDC 22 & IEEE standards)
  - Consistent with Commission direction per SRM SECY 93-087 and staff evaluation in SECY 18-0090
  - Aligns with Standard Review Plan for I&C
- D3 assessment for other safety-related (e.g. safety chillers) or non-safety systems not needed. Failure analysis, defense-in-depth analysis, and qualitative assessments can be used to address vulnerabilities to CCF, consistent with RIS 2002-22, Supplement 1.

Why are D3 Assessments Needed for Protection Systems?

- Key Criteria within IEEE Standards 279, 603, and GDC-22 require protection systems to use functional diversity or diversity in component design “to the extent practical” to prevent the loss of protective function.
- Original analog protection systems incorporated functional diversity to address the potential for CCF, using independent components.
- With digital technology, the potential exists to combine automatic protection functions in a way that negates or reduces the intended level of functional diversity or introduces new sources of or different plant consequences from potential CCF.

Why are D3 Assessments Needed for Protection Systems?

- D3 Assessments are needed to evaluate whether required systematic diversity is being preserved, and to identify whether additional diversity may be needed to demonstrate that vulnerabilities to new sources of CCF have been adequately addressed to assure the accomplishment of protection functions.
- The D3 assessment allows the use of best estimates (realistic assumptions) with a 10% allowance on offsite dose consequence for AOOs, and reliance on other systems (including high-quality, commercial grade systems) and operator actions to make this determination.

Potential Graded Approach

- A graded approach based on the classification and safety significance of the system should be used to categorize the proposed I&C system
- While deterministic, this approach is generally consistent with risk-informed categorization in 10 CFR 50.69 and graded approach in the design-specific review standard

Potential Graded Approach for Systems Categorization Concept

	Safety-Related	Non-Safety Related
Risk Significant	A1 (e.g. Protection System, Safety Control Systems*, Load Sequencers*)	B1 (e.g. Rod Control System, Feedwater Control system, Certain BOP Control Systems)
Not Risk Significant	A2 (e.g. Safety Chillers, Safety Control Systems*, Load Sequencers*)	B2 (e.g. Plant Computer, Service Water System Controls)

*The staff recognizes actual categorization may be driven by specific plant system configurations, the exact nature in which systems may be interconnected by digital equipment, and the plant's licensing basis. Systems that depend on the overall plant design may be safety significant or non-safety significant.

Proposed Criteria for Determination of Safety Significance

Proposed Deterministic Approach:

- A1: Safety-related system that is (1) relied upon to initiate actions essential to maintain plant parameters within acceptable limits established for a DBE or (2) supports the mitigation of the consequence of a DBE.
- A2: Safety-related system that (1) provides an auxiliary or indirect function in the achievement or maintenance of plant safety or (2) maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.
- B1: Non-safety related system (1) that directly affects the reactivity or power level of the reactor or (2) whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system.
- B2: Non-safety related system or component (1) that does not have direct affect on reactivity or power level of the reactor or (2) whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin.

Starting point of this concept based on IAEA/IEC familiarity. Plant specific Probabilistic Risk Assessment (PRA) results or data can be used as risk insights on safety significance with consideration of uncertainty in the data and the plant sensitivity to that uncertainty. However, the available methodology to model digital I&C systems in the PRA may not be sufficient for the digital I&C modifications contemplated for operating plants.

Conceptual Framework for a Proposed Graded Approach for Assessing CCF and Defense-in-Depth

Goal: Ensures appropriate defense-in-depth commensurate with the consequences of a potential CCF vulnerability.

A1 Systems **D3 Analysis**	**B1 Systems** **Defense-in-Depth/Qualitative Assessment**
A2 Systems **Defense-in-Depth/Qualitative Assessment**	**B2 Systems** **Assessment May be Needed***

*Performance of defense-in-depth/qualitative assessment will be dependent upon changes that may introduce new failure modes based on combined design functions, shared resources, or connectivity to other plant systems.

Proposed Clarification for Section 1.9

- Section title edited to state "Design Attributes to Eliminate ***Further*** Consideration of CCF"
  - Aligns with NRC Staff direction in SECY 18-0090
  - Consistent with positions taken in RIS 2002-22, Supplement 1, and other licensing activities with regard to CCF consideration
- The goal is to provide more flexibility to ensure that this is a practical tool in the demonstration of a safety case – this is not a requirement

Proposed Clarification for Section 1.9 (continued)

- Two refinements on Item #2, "Testability"
  1. Edit first sentence to state, in part: "A system ***or component***…."
     - Clarifies that components are a consideration
  2. Clarify 100% testing of active logic versus 100% testing of all logic:
     - On a case by case basis, demonstrating 100% of active logic used may be acceptable
     - Requires technical basis that unused or inactive logic does not affect performance in any operational condition
     - See SSPS' evaluation – ADAMS Accession # - ML14260A143

Suggested Conceptual Improvement Operating Reactors versus New Reactors

- Differences in licensing bases and degree of digital systems integration present challenges in balancing D3 criteria **(See D3 Comparison Table)**
- It may be beneficial to tailor specific guidance based on the degree of digital system integration and/or plant design and licensing basis
- Separate treatment would facilitate more customization to address industry concerns

Topics Needing Additional Feedback

- The specific implementation plans and system configurations that are being planned for NRC approval
  - Important to provide context in detailed discussions on the guidance
- Clarifying D3 approaches for A1 equipment
- Guidance for reviewing CCF in A2 and B1 systems that could be provided in a LAR
- Industry plans in developing potential design guidance for addressing CCF

Industry Participation in Improvements to BTP 7-19

- Industry participation is essential to ensure new revision addresses stakeholder concerns
- The NRC Staff welcomes proposals from industry on refining or improving key portions of BTP 7-19, including ideas to refine the proposed D3 Assessment

Schedule Milestones

	Activity	Completion Date
A.1	Begin revision to draft BTP 7-19	In progress
A.2	Category 2 public meeting to discuss the direction of draft BTP 7-19	April 4, 2019
A.3	Finalize draft BTP 7-19 for NRR review and concurrence	June 2019
A.4	Agency review and concurrence on draft BTP 7-19	August 20, 2019
A.5	ACRS Subcommittee Meeting	September 20, 2019
A.6	Issue Draft BTP 7-19 for public comment period (60 day comment period) Public meeting, if needed – November 2019	October 2019
A.7	Public comment period ends	December 2019
A.8	Public Comment/ACRS Comment Resolution Complete	January 2020
A.9	ACRS Full Committee Meeting	February 2020
A.10	Prepare Final BTP 7-19 Concurrence Receive OMB Clearance Approval (non-major rule determination)	March 2020
A.11	Issuance of Final BTP 7-19	April 2020

Questions

Acronyms

BTP	Branch Technical Position	CFR	Code of Federal Regulations
D3	Diversity and Defense-in-Depth	DBE	Design Basis Event
SRP	Standard Review Plan	RPS	Reactor Protection System
I&C	Instrumentation and Control	RTS	Reactor Trip System
CCF	Common Cause Failure	ESF	Engineered Safety Feature
BOP	Balance of Plant	SSPS	Solid State Protection System
PRA	Probabilistic Risk Assessment	IEEE	Institute of Electrical and Electronics Engineers
MP	Modernization Plan	ESFAS	Engineered Safety Feature Actuation System
SRM	Staff Requirements Memorandum	GDC	General Design Criteria
DI&C	Digital Instrumentation and Control	DSRS	Design Specific Review Standard
AOO	Anticipated Operational Occurrence		

Official Copy Accession Number:
ML17250A229

Background Information

Modernization Plans (MPs)

- Developed in accordance with Staff Requirements Memorandum (SRM) to SECY-16-0070
- MP#1 – Common Cause Failure
  - MP#1A: Supplement 1 to RIS 2002-22
  - MP#1D: Update to Branch Technical Position (BTP) 7-19
- MP#2 – 10 CFR 50.59 Guidance
- MP#3 – Commercial Grade Dedication
- MP#4A – ISG-06 Revision
- MP#4B – Broader Modernization Activities

Key Requirements for Protection Systems

10CFR50.55a(h) Incorporates IEEE-279-1971 and IEEE 603-1991:

- IEEE 279, Clause 4.7.4 identifies the need for design bases for protection systems that address scenarios involving multiple failures resulting from a credible single event.
- IEEE 603 Clause 4.8 requires documentation of the conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions.
- IEEE 603 Clause 5.1, requires that "safety systems shall perform all safety functions required for a design-basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable, but non-detectable failures...."

GDC-22 requires protection systems to use design techniques such as diversity (to the extent practical) *to prevent the loss of protection function.*

SECY-18-0090 – Five Guiding Principles

1. Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, “Domestic Licensing of Productions and Utilization Facilities” or under 10 CFR Part 52, “Licensees, Certifications and Approvals for Nuclear Power Plants” should continue to assess and address CCFs due to software for DI&C systems and components.
2. A defense-in-depth and diversity analysis for reactor trip systems and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. In performing this analysis, the vendor, applicant, or licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report. This defense-in-depth and diversity analysis can be either a best estimate analysis or a design-basis analysis.
3. This analyses should also be commensurate with the safety significance of the system. An analysis may not be necessary for some low-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.

Five Guiding Principles continued

4. If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should perform either the same function or a different function. The diverse or different function may be performed by either a safety or a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions in a reliable manner. Use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the defense-in-depth and diversity analysis demonstrates that a CCF, when evaluated in the accident analysis section of the safety analysis report, can be reasonably mitigated through other means (such as with current systems), a diverse means that performs the same or a different function may not be needed.
5. The level of technical justification needed to demonstrate that defensive measures (i.e., prevention and mitigation measures) are adequate to address potential CCFs should be commensurate with the safety significance of the DI&C system. For the systems of higher safety significance, any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented.

SRM to SECY-93-087

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.