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

BTP 7-19 Update
Modernization Plan #1D

Public Meeting

NRC Staff Presentation

June 26, 2019

Agenda

- Initial focus areas for BTP 7-19 revision
- Update on key focus areas since April 2019 Public Meeting (ML19092A396)
- Proposed approach to address CCF
- Feedback on industry comments received to date
- Schedule update

Initial Focus Areas

- Applicability of guidance within BTP 7-19 to changes made under 10 CFR 50.59
- Defining a graded approach for addressing CCF in digital I&C systems
  - Applicability of D3 assessment to safety significant systems
  - Methodologies that can be used to address CCF vulnerabilities for lower safety significant systems
- Clarification of guidance within Section 1.9

Additional Focus Areas Following the April 2019 Public Meeting

- Clarification of spurious actuation guidance
- Clarification on equipment credited for diverse manual operator actions
- Structure and flow of BTP 7-19

Applicability of BTP 7-19 to LARs, DCs and COLs

- BTP 7-19 is applicable to digital I&C systems proposed in LARs, DC and COL applications

- Use of BTP 7-19 outside these licensing frameworks is at the discretion of the licensee and is subject to the limitations of other licensing frameworks (e.g. 10 CFR 50.59)

Proposed Graded Approach Framework

- For assessing vulnerabilities to CCF, a graded approach refers to analyses performed for equipment of differing safety significance in which CCF concerns apply
- Categorizes digital I&C systems based on safety classification and safety significance
- While deterministic, this approach is generally consistent with the graded approach in the design-specific review standard
- Provides criteria for facilitating the use of defense-in-depth commensurate with the consequences of a potential CCF vulnerability
- Staff has continued to refine this proposed framework

Proposed System Categorization – Graded Approach*

	Safety-Related	Non-Safety Related
Safety Significant Significant Contributor to Plant Safety	**A1** **Analysis Needed:** D3 Assessment	**B1** **Analysis Needed**: Qualitative Assessment
Non-Safety Significant Not a significant contributor to plant safety	**A2** **Analysis Needed**: Qualitative Assessment	**B2** **Analysis Needed**: None may be needed

*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 - Updated

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) whose failure could directly lead to accident conditions which may cause unacceptable consequences if not mitigated by other A1 system
- 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 effect 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

Applicability of CCF Guidance to Operating and New Nuclear Power Plants

- Staff had considered use of licensing basis of nuclear power plants (e.g. operating plants versus advanced reactors) for determining applicability of CCF guidance

- After further consideration, the staff will continue applying the same CCF criteria independent of licensing basis

- Technical rigor and scope of CCF guidance will be based on differences in the level of integration and interconnectivity

Graded Approach and Digital Integration/Interconnectivity

- Digital integration and interconnectivity can be significant within and between the systems belonging to each category of systems due to combining of design functions, shared resources, an interconnectivity between divisions and systems, etc.

- The applicability of the D3 assessment should consider the level of integration and interconnectivity among systems belonging to each category

- In most cases, a D3 assessment will only be needed for a digital protection system (i.e. A1 system). For other systems, a qualitative assessment as described in RIS 2002-22, Supplement 1 would be adequate

- If digital interconnectivity and integration exists between the digital protection system and other systems (safety or non-safety-related) without demonstration that these connections/integrations do not adversely impact the digital protection system, the D3 assessment should also consider these interconnected systems and potential impacts

Proposed Clarifications to Spurious Actuation Guidance

- Spurious actuations resulting from a postulated CCF can be considered beyond design basis events
  - Spurious actuations due to CCFs should be considered transient initiators **without** a concurrent DBE
  - Spurious actuations resulting from single random failures within a digital I&C system (or component) should continue to be addressed

- Scope of spurious actuation considerations should focus on those with greater adverse consequences to plant safety

- Previous spurious actuation considerations in the existing licensing basis should not be invalidated by digital modification

- Allow methods to reduce the likelihood of postulated spurious actuations such that further consideration is unnecessary

Preliminary Staff Considerations of Industry Feedback

- April public meeting feedback generally aligns with the NRC staff's direction
- In May 2019, industry provided ***ten*** additional comments (ADAMS Accession# ML19135A401) that will be discussed in the following slides
- Some of the ten new comments require further clarification so that staff can:
  - Better understand industry's concern
  - Potential impacts on resources and schedule

*Note: The following slides do not constitute formal disposition of industry comments or NRC staff position.

Continued….

- Comment#1 – Regarding manual actions outside the MCR, clarification is needed on whether the desired flexibility is for Point 3 or Point 4 of the SRM on SECY 93-087
  - Potential flexibility can be considered for use of equipment outside the MCR to address Point 3
  - If the interest is to use controls and indications outside the MCR to address Point 4, staff would need to engage the Commission

- Comment#2 – Work on improving spurious actuation guidance is still on-going

Continued….

- Comment#3 – Regarding Testability
  - Staff agrees in concept with the industry's proposed flexibility for testability but not necessarily with the proposed wording. Work is still on-going
  - Regarding adding the 'defensive measures' concept to Section 1.9, staff is open to potential 'placeholder' language provided more substantive proposals by industry can address the follow items:
    - A framework that demonstrates how defensive measures can be applied as well as acceptance criteria
    - Clarify if there's interest in applying the defensive measures concept to proposed A1 systems to remove further consideration of CCF

Continued….

- Comment#4 – See Comment #1 Response
- Comment#5 – See Comment #2 Response
- Comment#6 – Related to Comment #1
  - With regard to using strategies similar to FLEX*, how does industry envision this new strategy?
  - Need to consider availability, reliability, and response time requirements of the equipment being used for the diverse means and the location of the equipment, etc.

*FLEX is the NRC's accepted safety strategy to maintain long-term core and spent fuel cooling and containment integrity with installed plant equipment that is protected from natural hazards, as well as backup portable onsite equipment.

Continued….

- Comment#7 – See response to Comment #2
- Comment#8 – Work is still on-going
- Comment#9 –
  - Staff agrees with portions of industry proposed definition of A1
  - References to “defense-in-depth” analysis have been removed

Continued….

- Comment#10 – Regarding Structure of BTP 7-19
  - Staff agrees with industry's comment that structure and flow of guidance could be improved
  - Staff is working on restructuring and consolidating content for readability and usability

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	Completed April 4, 2019
A.3	Category 2 public meeting to discuss topic focused areas of BTP 7-19	June 26, 2019
A.4	Finalize draft BTP 7-19 for staff review	July 31, 2019
A.5	Final Category 2 public meeting to discuss BTP 7-19 prior to NRC review and concurrence	Mid-Late August 2019
A.6	Agency review and concurrence on draft BTP 7-19 in preparation for public comment period	October 2019
A.7	ACRS Subcommittee Meeting	November 2019
A.8	Issue Draft BTP 7-19 for public comment period (60 day comment period) Public meeting, if needed – January 2020	December 2019
A.9	Public comment period ends	February 2020
A.10	Public Comment/ACRS Comment Resolution Complete	March 2020
A.11	ACRS Full Committee Meeting	April 2020
A.12	Prepare Final BTP 7-19 Concurrence Receive OMB Clearance Approval (non-major rule determination)	May 2020
A.13	Issuance of Final BTP 7-19	June 2020

Questions

Acronyms

BTP	Branch Technical Position	CCF	Common Cause Failure
CFR	Code of Federal Regulations	COL	Combined License
D3	Defense-in-Depth and Diversity	DBE	Design Basis Event
DC	Design Certification	I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency	IEC	International Electrotechnical Commission
LAR	License Amendment Request	MCR	Main Control Room
RIS	Regulatory Information Summary	SRM	Staff Requirements Memorandum

Background Information

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.

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.

Key Requirements for Protection Systems

10 CFR 50.55a(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.*