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

BTP 7-19 Update – Spurious Operation Considerations

Public Meeting
MP1D Working Group
NRC Staff Presentation
August 1, 2019

Agenda

- Summary of Concerns with Spurious Operation of SSCs due to Digital CCF
- Licensing and Technical Considerations
- Examples of Licensing Successes

Spurious Operation of SSCs

- Spurious operation of an SSC(s) is a potential outcome of CCF in an I&C system.

- Due to potential interconnectivity and integration of design functions through introduction of digital technology (rather than the traditional assumption of single random hardware failures), spurious operation of multiple SSCs could result.

- Previous FSAR assumptions on spurious operation could become invalid (e.g. Spurious operation of multiple SSCs could place a plant in an unanalyzed condition).

- Prior licensing reviews have identified a need to clarify guidance in this area to ensure adequate technical rigor is applied and documented.

Licensing and Technical Considerations

- Previous spurious operation considerations in the existing licensing basis should not be invalidated by digital modification.
  - e.g. Spurious operations resulting from single random failures.
- A spurious operation due to a CCF of a DI&C system should be considered as an initiating event without a concurrent design basis event.
- Design attributes or defensive measures can be credited in the analysis to eliminate from further consideration a CCF of a DI&C system that can cause a spurious operation.
  - These attributes or measures can be used to prevent the occurrence of a spurious operation or limit their effects/consequences.
  - Any credited attributes or measures should be identified and their effectiveness should be shown.

Licensing and Technical Considerations

- In cases where it cannot be shown that the design attributes or defensive measures are adequate to prevent or limit the effects/consequence of a spurious operation, an analysis should be performed to evaluate the consequence of the spurious operation.
  - The analysis should focus on those functions whose spurious operation can create an unbounded condition in the safety analysis or result in consequences that exceed acceptable limits.
  - The technical rigor of this analysis should be commensurate with the safety significance of the DI&C system.
  - The results of the analysis should be used to inform any changes to the design to show that either the spurious operation is prevented or their effects/consequence are limited.

Examples of Accepted Methods

- Staff has accepted a number of different methods to address spurious operation, including the following:
  - Design features to reduce likelihood of failure.
  - Effects of the spurious are bounded (e.g. design basis or D3 analysis, qualitative assessments).
  - Mitigating measures: Crediting of manual actions.

Watts Bar Unit 2 DCS (ML102240384)

This modification utilized a number of methods to address digital CCF, thereby addressing potential new modes of spurious operation of equipment, such as the following:

- Design Features
  - Signal Selection and Validation
  - Digital Network 'Data Storm' testing
- Safety Analysis Review
  - Systematic review of analyzed events affected by the digital upgrade
  - Review ensured that no new failure modes would have an adverse impact on analyzed events
- Control Function Segmentation
  - Provides for functional diversity and independence between controller pairs on each network 'segment'
  - Design function distribution helps ensure failure effects of a 'segment' are limited

AP1000 and APR1400

- AP1000 (ML11171A500)
  - Onerous Functions: Certain key safety-related controls removed from NSR operator workstation due to spurious operation hazard
  - Measures taken to reduce the likelihood of spurious operation of ESF functions in the AP1000 PMS, including addition of ADS blocking device that is independent of PMS failure modes
- APR1400 (CCF Coping Analysis Technical Report - ML18086B754 and Control System CCF Technical Report - ML18087A108)
  - Thermo-hydraulic analysis performed on plant protection system postulating spurious operation of a single safety function
  - Control function segmentation
  - Thermo-hydraulic analysis performed on NSR operator workstation postulating multiple spurious operation of multiple SSCs both safety and non-safety
  - Network traffic monitoring

Questions

Acronyms

- ADS: Automatic Depressurization System
- BTP: Branch Technical Position
- CCF: Common Cause Failure
- D3: Defense-in-Depth and Diversity
- DCS: Distributed Control System
- DI&C: Digital Instrumentation and Controls
- ESF: Engineered Safety Feature
- FSAR: Final Safety Analysis Report
- NSR: Nonsafety-Related
- PMS: Protection and Monitoring System
- SSC: Structures, Systems, and Components

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.*