SUNSI Review Complete
Template = ADM-013
E-RIDS=ADM-03
ADD: Mark Notich

COMMENT (4)
PUBLICATION DATE:
1/14/2020
CITATION 85 FR 2152

# PUBLIC SUBMISSION

**As of:** 2/10/20 6:58 AM
**Received:** February 08, 2020
**Status:** Pending_Post
**Tracking No.** 1k4-9ewm-9yv0
**Comments Due:** March 16, 2020
**Submission Type:** Web

**Docket:** NRC-2019-0253
Proposed Revisions to Standard Review Plan Branch Technical Position 7-19 "Guidance for Evaluation of Potential Common Cause Failure in Digital Instrumentation and Control Systems"

**Comment On:** NRC-2019-0253-0001
Proposed Revision to Standard Review Plan Branch Technical Position 7–19 Guidance for Evaluation of Potential Common Cause Failure Due to Latent Software Defects in Digital Instrumentation and Control Systems

**Document:** NRC-2019-0253-DRAFT-0004
Comment on FR Doc # 2020-00350

## Submitter Information

**Name:** Mark Burzynski

## General Comment

The review guidance for the treatment of beyond design basis condition (i.e., CCF causing spurious operation) in NSR equipment lacks a clear, integrated, and coherent regulatory basis. Draft Revision 8 of Branch Technical Position 7-19 adds to the confusion. It does not integrate the other review guidance in SRP Section 7.7 or DI&C-ISG-04, Revision 1, regarding spurious actuations caused by safety-related and NSR digital I&C equipment. It also does not clearly establish the regulatory basis for the various technical positions, especially regarding NSR digital I&C systems not directly connected to safety-related components. A detailed set of comments is provided as an attachment.

## Attachments

SunPort Paper - Treatment of Spurious Actuations in Brach Technical Position 7-19

# Treatment of Spurious Actuations in Branch Technical Position 7-19

## Background

Standard Review Plan (SRP) Section 7.7 has some limited guidance for the treatment of control system failures causing spurious operations. The guidance is confusing because it introduces the ideas of software design errors and random hardware failures but also says that the evaluation of multiple independent failures is not intended.

DI&C-ISG-04, Revision 1, addresses malfunctions and spurious actuations in non-safety related (NSR) control systems. The guidance is incomplete in that it only identifies failure conditions that should be addressed but does not address the evaluation methodologies or acceptance criteria.

SRM-SECY-93-087 is the current basis for the NRC position on digital CCFs. Point 1 – 3 do not explicitly address treatment of new postulated beyond design basis conditions caused by CCFs resulting in multiple spurious operations in safety-related or NSR equipment.

Draft Revision 8 of Branch Technical Position (BTP) 7-19 is proposing changes to the guidance regarding the treatment of malfunctions and spurious actuations in NSR control systems. It makes the broad statements that IEEE Std 603-1991, Clauses 4.8 and 5.6.3, provide the basis for requiring licensees to address the potential for spurious operation of safety-related components and components that are NSR. This position requires a new understanding of the standard and not consistent with other governing regulatory criteria.

## Problems with Draft Revision 8 of Branch Technical Position 7-19

The review guidance for the treatment of beyond design basis condition (i.e., CCF causing spurious operation) in NSR equipment lacks a clear, integrated, and coherent regulatory basis. Draft Revision 8 of Branch Technical Position 7-19 adds to the confusion. It does not integrate the other review guidance in SRP Section 7.7 or DI&C-ISG-04, Revision 1, regarding spurious actuations caused by safety-related and NSR digital I&C equipment. It also does not clearly establish the regulatory basis for the various technical positions, especially regarding NSR digital I&C systems not directly connected to safety-related components.

IEEE Std 603-1991, Clauses 4.8 and 5.6.3 are relevant for the case where NSR systems can directly actuate safety-related systems or components. On the other hand, it requires new and different interpretations of the terminology used is these requirements to extend applicability to NSR systems or components that are not directly connected to safety-related equipment. It is not clear what the regulatory basis for the treatment of spurious actuation hazards would be for plants with IEEE Std 279 as their licensing basis.

It is not consistent to use Clause 4.8 to conclude a new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety-related equipment) as

part of defined safety function (i.e., design basis condition) or that it causes degradation of a safety-related system.[1]

It is also not appropriate to use Clause 5.6.3 to conclude a new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety-related equipment). Clause 5.6.3.1, Interconnected Equipment, is not applicable to NSR equipment with no direct connection to safety-related equipment. Clause 5.6.3.2, Equipment in Proximity, requires physical separation, which is not relevant to the postulated CCF scenarios for NSR equipment. Clause 5.6.3.3, Effects of a Single Random Failure, addresses the case where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. This clause would require assessment of random hardware failures associated with shared hardware resources in NSR distributed control systems; however, it does not address beyond design basis conditions caused by postulated software CCFs in NSR equipment.

SRM-SECY-93-087 is cited as the basis for the NRC position on digital CCFs. Point 1 in the SRM addresses the need to assess potential CCF vulnerabilities. Point 2 addresses how diversity can be used to address the CCF vulnerabilities for each accident event analyzed in the FSAR.[2] Point 3 addresses how the CCF vulnerabilities can be mitigated by diverse actuations. Points 1 – 3 do not explicitly address treatment of new postulated beyond design basis conditions caused by CCFs resulting in multiple spurious operations in safety-related or NSR equipment. Clearly the existence of NSR distributed control systems and digital human-machine interfaces were contemplated at the time SECY-93-087 was written (as discussed in SECY-91-292) yet these digital systems were not included in the Commission directions to the staff.

The review guidance in SRP Section 7.7 is based on IEEE Std 603-1991 Clause 5.6.3. The concern with random hardware failures associated with shared hardware resources in NSR distributed control systems fits the context of IEEE Std 603-1991 Clause 5.6.3.3; however, the treatment of other postulated multiple spurious actuations is not consistent with the governing regulatory criteria. SRP Section 7.7 also references SRM-SECY-93-087 to the extent that control system functions are credited as diverse means for performing safety functions to satisfy Point 3 in SRM-SECY-93-087; however, it is not used to address beyond design basis conditions caused by postulated software CCFs in NSR equipment.

## A Deeper Look at IEEE Std 603

The treatment of spurious control system actuation hazards can be considered in a broader context of IEEE Std 603-1991. The relevant requirements are identified below, and observations are provided regarding each.

---

1 As understood in the context of RIS 2005-20, “Revision to NRC Inspection Manual Part 9900 Technical Guidance, Operability Determinations & Functionality Assessments for Resolution of Degraded or Nonconforming Conditions Adverse to Quality or Safety".

2 In practice this point has looked at each abnormal operation occurrence and postulated accident analyzed in the FSAR (typically Chapter 15).

**Clause 4. Safety System Designation**

4.1 The design basis events applicable to each mode of operation of the generating station along with the initial conditions and allowable limits of plant conditions for each such event.

*Observation: Design basis events are defined in SRP Chapter 15*

4.2 The safety functions and corresponding protective actions of the execute features for each design basis event.

*Observation: The plant-specific safety functions and corresponding protective actions are based on the safety analyses in FSAR Chapter 15*

4.8 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 (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

*Observation: This criterion addresses various types of qualification criteria. Each one has a specific set of analysis rules and acceptance criteria defined in other sections of the SRP. This IEEE clause is relevant for the case where NSR systems can directly actuate safety-related systems or components. On the other hand, it requires new and different interpretations of the terminology used is these requirements to extend applicability to NSR systems or components that are not directly connected to safety-related equipment.*

*It is not consistent to use clause 4.8 to ca new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety related equipment). It is not correct to consider these new scenarios as part of defined safety function (i.e., design basis condition) or that it causes degradation of a safety-related system.* [1]

*The treatment of failures in NSR systems is expanded in IEEE Std 603-1991, Clauses 5.1 and 5.6.3.*

*It should be noted that the Clause 4.8 requirement in IEEE Std 603-2018 was expanded to better address the case of spurious control system actuations. It now reads:*

> The conditions having the potential for ~~functional degradation of~~ degrading or defeating the safety ~~system performance~~ function and for which provisions shall be incorporated to retain the capability ~~for performing~~ to perform the safety functions (e.g., missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems). Analyses shall be performed to identify and address these potential hazards of the system and shall be used to establish design basis. These analyses should determine which hazards require system design provisions to retain the capability to perform the safety functions or require other means to maintain plant safety. (changes from 1991 version shown in color)

*This addition sets the stage to address spurious control system actuation hazards in a graded manner and establish criteria for the set that are treated as design basis events (i.e., Chapter 15 postulated initiating events) and those hazards that are treated as beyond design basis events with its own set of hazard analysis rules and acceptance criteria.*

4.12 Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).

*Observation: The regulatory agency criteria has been used in the past to address the 'special design basis' for diverse actuation systems. It has worked because there are a reasonable set of analysis methodologies (i.e., NUREG/CR-6303) and BTP 7-19 for loss of protection system functions (i.e., RTS and ESFAS) due to software common cause failures (CCFs). In contrast, such a set of guidance does not exist to address spurious control system actuation hazards and makes it more difficult to address this clause in a predictable and consistent manner. The guidance proposed in BTP 7-19 Draft Revision 8 is confusing and does not adequately distinguish between what hazards should be treated as design basis event and those that can be treated as beyond design basis events. There is no guidance on the hazard analysis methodologies that is comparable to NUREG/CR-6303. The approach used for the licensing of Watts Bar Unit 2 is a reasonable precedent to use to generate the needed guidance.*

*It should be noted that the Clause 4.12 requirement in IEEE Std 603-2018 was modified to delete the regulatory agency criterion. It now reads:*

> Any other special design basis that may be imposed on the system design (e.g., to address topics such as diversity, or interlocks~~, regulatory agency criteria~~). (changes from 1991 version shown in color)

5.1 Single-failure criterion. The 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; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379 provides guidance on the application of the single-failure criterion.

*Observation: IEEE Std 379-2000 has relevant guidance in clause 6.3.1, Other systems coupled to safety systems:*

> All non-safety systems (e.g., non-safety test circuitry) or other safety systems (e.g., alternate channels) coupled in some manner to safety systems to which the single-failure criterion is applied shall be examined to establish whether any failure within these systems can degrade the safety systems to which they are coupled. If they can degrade any portion of the safety systems to the point of failure, those failures shall be assumed to exist as an initial condition to the single-failure analysis of the safety system. For further guidance in this area, see IEEE Std 384-1992.

*These requirements reinforce the focus on interconnection between the safety-related component and the NSR control system and associated independence as defined in IEEE Std 384.*

**Clause 5.6 Independence**

5.6.3 Between Safety Systems and Other Systems. The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

5.6.3.1 Interconnected Equipment

(1) Classification: Equipment that is used for both safety and nonsafety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.
(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

5.6.3.2 Equipment in Proximity

(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of nonsafety equipment. Physical separation may be achieved by physical barriers or acceptable separation distance. The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384.
(2) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of 5.3, 5.4 and 5.5 for the applicable conditions specified in 4.7 and 4.8 of the design basis.

5.6.3.3 Effects of a Single Random Failure. Where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379 for the application of this requirement.

*Observation: These criteria address various elements of independence for NSR equipment connected to or in the proximity of safety-related equipment. It is not appropriate to use Clause 5.6.3 to conclude a new postulated beyond design basis condition (CCF causing spurious operation in NSR equipment that has no direct connection to safety-related equipment). Clause 5.6.3.1, Interconnected Equipment, is not applicable to NSR equipment with no direct connection to safety-related equipment. Clause 5.6.3.2, Equipment in Proximity, requires physical separation, which is not relevant to the postulated CCF scenarios for NSR equipment. Clause 5.6.3.3, Effects of a Single Random Failure, addresses the case where a single random failure in a NSR system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate*

*single failure. This clause would require assessment of random hardware failures associated with shared hardware resources in NSR distributed control systems; however, it does not address beyond design basis conditions caused by postulated software CCFs in NSR equipment.*

*It should be noted that the Clause 5.6.3 requirements in IEEE Std 603-2018 were modified to clarify the independence requirements. It now reads:*

5.6.3 Between safety systems and other systems.

The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4 item h) of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.

5.6.3.1 Interconnected equipment

a) Classification
   1) Equipment that is ~~used for both~~ credited to perform a safety ~~and nonsafety functions~~ function shall be classified as part of ~~the~~ a safety system~~s~~.
   2) Equipment that is not credited to perform a safety function but is connected to safety-related equipment shall meet one of the following:
      i) Be classified as an associated circuit.
      ii) Be electrically isolated from the safety system, have functional independence for all signal technologies, and be classified as non-Class 1E.
   3) Isolation devices used to ~~effect~~ establish a safety system boundary shall be classified as part of the safety system.

b) Isolation. No credible failures or events on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. Isolation devices shall ensure electrical isolation and functional independence for all signal technologies. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

5.6.3.2 Equipment in proximity

a) Separation. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety function in the event of the failure of non-safety equipment. Physical separation may be achieved by physical barriers or ~~acceptable~~ sufficient separation distance. ~~The separation of Class 1E equipment shall be in accordance with the requirements of IEEE Std 384-1981.~~

b) Barriers: Physical barriers used to effect a safety system boundary shall meet the requirements of Sub-clauses 5.3, 5.4, and 5.5 for the applicable conditions specified in Clause 4 items g) and h) of the design basis.

5.6.3.3 Effects of a single random failure

Where a single random failure in a non-safety system can result in a design basis event, and also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be

> capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379 ~~1988~~ for the application of this requirement.
>
> (changes from 1991 version shown in color)

*These changes do not alter the earlier observations regarding the independence clause.*

The IEEE Std 603 issues are summarized in Table 1. The items in ***bold italics*** are the issues that are introduced but not well-defined in BTP 7-19 draft revision 8.

## Conflicts with Other NRC Review Guidance

SRP Section 7.7, Revision 6, provides review guidance for assessing the effects of control system failures:

> The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should ensure that failure modes that can be associated with digital systems such as software design errors and random hardware failures, as well as the methods used to account for these failure modes, are addressed and documented. (The evaluation of multiple independent failures is not intended.)

*Observation: The guidance in SRP 7.7 is confusing because it suggests that postulated NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components can be treated as beyond design basis events with other acceptance criteria.*

*Observation: The guidance in SRP 7.7 is also confusing regarding the statement "evaluation of multiple independent failures is not intended," since it is not clear whether meeting the physical separation and electrical isolation (i.e., independence) required by IEEE Std 603-1991 Clause 5.6.3 is sufficient (i.e., independence for a direct connection between a safety-related and NSR system meeting the requirements of IEEE Std 384 is sufficient. That same statement has also been used to require additional features within an NSR system design to provide some other type of 'independence' (e.g., controller segmentation) that has no established regulatory definition.*

DI&C-ISG-04, Revision 1, provides review guidance for assessing the effects of spurious actuations from control system failures in Section 3.1.5 (bulleted items) that should be clarified and considered in Draft Revision 8 of BTP 7-19:

- Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed.

*Observation: This guidance in DI&C-ISG-04 is confusing because it suggests that postulated safety-related and NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components caused by common software errors can be treated as beyond design basis events with other acceptance criteria.*

- No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond "do you want to proceed?" The operator should then be required to respond "Yes" or "No" to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors.

*Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.*

- Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety-related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein.

*Observation: This guidance in DI&C-ISG-04 sets the expectations for qualification of NSR digital I&C equipment to prevent spurious actuations or other adverse effects on safety-related equipment or devices as a result of a design basis condition, both during the condition and afterwards. The design basis conditions that should be considered for such qualification testing is not specified; however, it suggests that they are limited to transient conditions by the during and afterwards criteria.*

- Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses.

*Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.*

- The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire

or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations.

*Observation: This guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.*

- Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions.

*Observation: This guidance in DI&C-ISG-04 is confusing because it suggests that postulated safety-related and NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components caused by common software errors can be treated as beyond design basis events with other acceptance criteria.*

## Relevant International Guidance

The Multinational Design Evaluation Programme (MDEP) program has issued two Generic Common Positions that are relevant to the treatment of postulated spurious actuations caused by NSR digital I&C equipment:

- DICWG No. 10, Version 7, *Common Position on Hazard Identification and Controls for Digital Instrumentation and Control Systems*
- DICWG No. 13, *Common Position on Spurious Actuation*

These documents recommend using hazards analyses to assess the vulnerabilities and to credit design attributes that reduce the likelihood or mitigate the consequences of the spurious actuation such that it can be removed from further analysis.

## Other Factors to Consider

The issues associated with postulated common cause failures in safety-related digital I&C systems that result in the failure of the safety-related system to act when needed (Condition 1) are fundamentally different than hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components (Condition 2).

<u>Condition 1 Attributes</u>

- Regulatory basis is specifically addressed by SRM-SECY-93-087
- Concerns are clearly defined as a beyond design basis event
- Conditions to be evaluated are well defined as postulated loss of actuation capability due to software CCF coincident with postulated initiating events (i.e., abnormal operation occurrences and postulated accidents)

- Well-developed evaluation methodology is available in NUREG/CR-6303 to identify software CCF vulnerabilities of concern
- Best-estimate analysis methodologies and acceptance criteria are well understood
- Software CCF vulnerabilities of concern can be addressed by familiar and understood design features (e.g., diverse actuation systems or defensive measures) or coping analyses

Condition 2 Attributes

- Regulatory basis is not addressed by SRM-SECY-93-087
- Regulatory basis for spurious actuation concerns caused by safety-related or NSR digital I&C systems is not well developed and therefore confusing
- Concerns are expressed in ways that create confusion regarding their treatment as either design basis conditions or beyond design basis events
- Conditions to be evaluated are not well-defined or understood for multiple spurious component actuation scenarios except to be treated as with no other coincident conditions to be assumed
- No well-developed hazard evaluation methodology is available to guide the evaluation of spurious actuation concerns caused by postulated safety-related or NSR digital I&C system failures
- Use of design basis or best-estimate analysis methodologies and acceptance criteria are not clearly identified for evaluation of the new postulated initiating events
- Spurious actuation vulnerabilities of concern are addressed by a less-familiar and understood set of design features

The goal for the treatment of spurious actuations should be defined and reviewed by the various stakeholder groups. In particular, the acceptability of the defensive measures discussed in DI&C-ISG-04 be confirmed as acceptable solutions. The use of sufficient defensive design measures that can be shown to prevent credible transients that are not bounded by the plant Chapter 15 safety analyses. The most direct approach is to use segmentation of control groups to limit adverse effects along with recognition that these control groups also rely on different signal trajectories and will have non concurrent triggers. The NSR control systems are in continuous operation under the observation of the control room operators. These points are differentiators from safety-related system designs that have redundancies all relying on signal inputs from the same system parameter that makes them vulnerable to concurrent triggers. This approach would be consistent with the Watts Bar Unit 2 precedent.

## Recommendations

A better way to address the concerns with potential hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components has five specific actions:

1. Remove the applicable guidance from BTP 7-19 Draft Revision 8 (as shown in the attached mark-ups), since it is premature to issue guidance that creates more confusion than it solves regarding the treatment of spurious actuation hazards.

2. Clarify the regulatory basis for the treatment of spurious actuation hazards as either design basis or beyond design basis events. It may be useful to couple this regulatory basis issue to Clause 4.h in IEEE Std 603-2018, when it is endorsed.

3. Develop a complete and separate set of unambiguous regulatory guidance with a clear compliance framework that is focused on the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components.

4. Coordinate the development of the new regulatory guidance documents with other industry stakeholders (e.g., Nuclear Energy Institute) to ensure the guidance is consistent with other industry guidance documents being developed.

5. Update the evaluation criteria found in DI&C-ISG-04, Revision 1, Section 3, *Multidivisional Control and Display Stations*, and Standard Review Plan Section 7.7, Revision 6, with the new regulatory guidance developed for the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components.

This approach would provide the clarity in the promulgation of a new regulatory guidance document focused on the treatment of hazards in safety-related and NSR digital I&C control systems that are postulated to cause spurious actuation of safety-related and other important components in an unambiguous and complete manner within a clear compliance framework.

**Table 1 – Summary of Issues**

| Safety-Related Controls with Direct Connection to Safety Components | | Non-Safety Related Controls with Direct Connection to Safety Components | | Non-Safety Related Controls with No Direct Connection to Safety Components | |
|---|---|---|---|---|---|
| Design Basis | Beyond Design Basis | Design Basis | Beyond Design Basis | Design Basis | Beyond Design Basis |
| Single failure criterion and consequential failures caused by design basis event (Clause 5.1)<br>Qualification for environment and external events to avoid hardware CCF (Clauses 4.h and 5.2) | Software CCF to prevent actuation (Clause 4.12 has been cited for some license amendment requests)<br>***Software CCF from control room HMI causes spurious actuation (only new plant precedents)*** | Credible failures in and consequential actions by other systems, as documented in Clause 4.h of the design basis (qualification), shall not prevent the safety systems from meeting its requirements.<br>Requirements for isolation, physical separation and consideration of single random failures are specified.<br>(Clause 5.6.3) | ***Software CCF in control systems and control room HMI causes spurious actuation of safety-related components*** | No requirements in IEEE Std 603 | ***Software CCF in control systems and control room HMI causes spurious actuation of non safety-related components that represent new transients not evaluated in Chapter 15*** |
| Note: Protection system safety functions are derived from analysis of specific postulated initiating events in FSAR Chapter 15, which have been standardized in SRP Chapter 15.<br>(Clauses 4.1 and 4.2) | Note: CCF from ESFAS not generally considered as source of spurious actuation in approved precedents | Note: It is often considered that the design basis events evaluated in Chapter 15 are related to a failure assessment of the non-safety related systems, but they are not. There are some events that are specified for evaluation in SRP Chapter 15 that would only occur with multiple non-mechanistic failures (e.g., loss of all feedwater, loss of feedwater enthalpy, etc.). | | | |

**Attachment: Suggested Changes to BTP 7-19 Draft Revision 8**

U.S. NUCLEAR REGULATORY COMMISSION

# STANDARD REVIEW PLAN

## BRANCH TECHNICAL POSITION 7-19

## GUIDANCE FOR EVALUATION OF ~~COMMON CAUSE FAILURE HAZARDS DUE TO LATENT SOFTWARE DEFECTS~~ IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

## REVIEW RESPONSIBILITIES

Primary – Organization responsible for the review of instrumentation and controls (I&C)

Secondary – Organization responsible for the review of reactor systems and the organization responsible for the review of human factors engineering (HFE)

Review Note: The revision numbers of regulatory guides (RGs) and the years of endorsed industry standards referenced in this branch technical position (BTP) are centrally maintained in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear

Draft Revision 8 – January 2020

Power Plants: LWR Edition," (SRP), Section 7.1-T, "Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety" (Table 7-1). References to industry standards incorporated by reference into regulations (Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279-1968, IEEE Std 279-1971, and IEEE Std 603-1991) and industry standards that are not endorsed by the agency do include the associated year in this BTP. See Table 7-1 to ensure that the appropriate RGs and endorsed industry standards are used for the review.

## A. BACKGROUND

Common-cause failures (CCFs) have been identified as a type of hazard that digital I&C (DI&C) systems could be more susceptible to due to the ability to integrate design functions using DI&C technology and its inherent complexity compared to analog technologies. DI&C systems or components can be vulnerable to a CCF due to defects in hardware or to latent defects in the software or software-based logic. Latent defects in hardware, software, or system components within redundant portions (e.g., safety divisions[1]) of a safety-related system can be triggered by an event or condition and thus lead to a systematic fault. A CCF hazard[2] (e.g., loss of the capability to perform a safety function) can result from the occurrence of such a systematic fault during a design-basis event (DBE). This BTP is focused on addressing CCF hazards resulting from systematic faults caused by latent defects in the software or software-based logic. [3]

~~A CCF of a DI&C system or component can also initiate the operation of a safety-related function or other design functions without a valid demand or can result in erroneous system actions. These conditions are typically referred to as "spurious operations," but the term can be used interchangeably with the term "spurious actuation." For this BTP, the term "spurious operations" is used.~~

In NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," issued March 1979, the U.S. Nuclear Regulatory Commission (NRC) staff documented a defense-in-depth and diversity (D3) assessment of a digital computer-based reactor protection system (RPS) in which defense against software CCF, which resulted in loss of a safety function during a DBE, was based upon an approach using a specified degree of system separation between echelons of defense. The RESAR-414 RPS consisted of the reactor trip system (RTS) and the engineered safety features (ESF) actuation system. Subsequently, in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991, the NRC staff discussed its concerns about CCF hazards in digital systems used in nuclear power plants (NPPs).

As a result of reviews of applications for certification of evolutionary and advanced light-water reactor designs using DI&C systems, the NRC staff documented its position regarding vulnerabilities to CCF hazards in DI&C systems and D3 in Item II.Q of SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor

[1] This BTP uses the term "division" as defined in IEEE Std 603-1991.
[2] If a CCF as a result of a systematic fault due to latent defects does not disable a safety function credited to mitigate a DBE, then the occurrence of this CCF is not considered a CCF hazard. The term "hazard" is defined as potential for harm, which in this context means disabling of the safety function ~~or causing unmitigated initiating events resulting from spurious operation of safety functions or other design functions~~.
[3] Other types of CCF hazards can exist and are addressed in other staff review guidance.

(ALWR) Designs," dated April 2, 1993. The Commission subsequently modified this position in Item 18 of the associated staff requirements memorandum (SRM) on SECY-93-087, dated July 21, 1993, in which the Commission indicated that CCF hazards of a DI&C system are considered beyond-design-basis events.

The NRC staff provided plans to the Commission to clarify the guidance associated with addressing CCF hazards of DI&C systems in SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018. This SECY paper documented the NRC staff's evaluation of the SRM on SECY-93-087. The staff concluded that the SRM provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. SECY-18-0090 outlines five guiding principles to ensure consistent application of the direction provided in the SRM on SECY-93-087. These principles provide a framework for addressing CCF hazards in DI&C systems using a graded approach based on the safety significance of the DI&C system. In SECY-18-0090, the NRC staff committed to incorporating these guiding principles into the NRC staff's review guidance.

In summary, while the NRC considers CCF hazards due to software in DI&C systems to be beyond design basis, the application should include an evaluation of CCF hazards due to software in DI&C systems and should verify that the plant is protected from the effects of these CCF hazards. ~~In addition, the application should include an evaluation of sources of this CCF hazard that can result in spurious operations, some of which may be considered within the design basis, as discussed later in this BTP.~~

Over the years, the NRC staff has approved applications with numerous design solutions, and in some cases, multiple design solutions for a single DI&C system, to address CCF hazards in DI&C systems. During these reviews, the NRC staff has observed that different solutions may be used to address CCF hazards, and that one standard solution may not be applicable to all DI&C systems. This BTP provides guidance for reviewing the design and analysis for addressing CCF hazards due to latent software defects in DI&C systems.

## 1. Regulatory Basis

The regulations listed below may not necessarily apply to all applicants. The applicability of these requirements is determined by the plant licensing basis and any changes to the licensing basis in the proposed DI&C system under evaluation:

- For NPPs with CPs issued before January 1, 1971, Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h), "Protection and Safety Systems," requires compliance with the plant-specific licensing basis or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

- For NPPs with CPs issued between January 1, 1971, and May 13, 1999, 10 CFR 50.55a(h) requires compliance with the requirements stated in IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems," or the requirements in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991 and the correction sheet dated January 30, 1995.

- For applications for construction permits (CPs), operating licenses (OLs), combined licenses (COLs), standard design approvals (SDAs), design certifications (DCs), filed after May 13, 1999, 10 CFR 50.55a(h) requires compliance with IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995.

- ~~IEEE Std 603-1991, Clause 5.6.3, requires, in part, that "safety system design shall be such that credible failures in and consequential actions by other systems, as documented in [Clause] 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard." IEEE Std 603-1991, Clause 4.8, requires, in part, that the safety-related system design bases shall document "[t]he 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 (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems)." These two clauses provide the basis for requiring licensees of plants licensed under IEEE Std 603-1991 to address the potential for spurious operation of safety-related components and components that are NSR.~~

- GDC 22, "Protection System Independence," requires, in part, that the protection system design shall ensure "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 … 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." GDC 22 provides the regulatory basis for the requirement to address CCF hazards and for requiring the use of design techniques, such as functional diversity or diversity in component design, to prevent the loss of the protection function.

- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants," governs applications for early site permits, DCs, COLs, SDAs, and manufacturing licenses (MLs) for nuclear power facilities.

- 10 CFR Part 100, "Reactor Site Criteria," provides guideline values for fission product releases from NPPs licensed to operate prior to January 10, 1997, for which the licensee has voluntarily implemented an alternative source term under the provisions of 10 CFR 50.67, "Accident Source Term." These guideline values can be commonly referred to as the site dose guideline values and provide the acceptance criteria for radiological release limits to bound the consequences of a CCF hazards concurrent with a DBE.

- 10 CFR 50.67 provides guideline values for fission product releases from currently operating NPPs for which the licensee has implemented an alternative source term.

- 10 CFR 50.34(a)(1)(ii)(D) provides site dose guideline values for CP applications filed under 10 CFR Part 50 after January 10, 1997.

- ~~NUREG-0800, SRP Section 7.7, "Control Systems" provides review guidance for addressing the potential for inadvertent (i.e., spurious) operation signals from control systems.~~

- NUREG-0800, SRP Section 7.8, "Diverse Instrumentation and Control Systems," describes the review process and additional acceptance criteria for diverse I&C systems provided to protect against CCF hazards.

- NUREG-0800, SRP Chapter 18, "Human Factors Engineering," defines a methodology, applicable to both existing and new reactors, for evaluating manual operator action as a diverse means of coping with anticipated operational occurrences (AOOs) and postulated accidents that are concurrent with a CCF hazard due to latent defects that disables a safety function credited in the safety analysis report (SAR).

3. Scope

The guidance of this BTP is intended for reviews of (1) proposed modifications that require a license amendment to be implemented, and (2) applications for CPs, OLs, COLs, DCs, SDAs, and MLs. This BTP is not applicable to proposed modifications performed under the 10 CFR 50.59, "Changes, Tests and Experiments," change process.

4. Purpose

The purpose of this BTP is to provide guidance for reviewing an evaluation of (1) a DI&C system's vulnerability to a CCF hazard due to latent defects in the software or software-based logic, (2) any diverse means credited to address remaining vulnerabilities to a CCF hazard, and (3) the effects of any unmitigated vulnerabilities to a CCF hazard on plant safety. This BTP also provides guidance on implementing a graded approach to address CCF hazards due to latent defects in the software or software-based logic in DI&C systems based on the safety significance of the system. In this guidance, software includes software, firmware,[5] and logic developed from software-based development systems (e.g., hardware description language programmed devices).

This BTP is intended to address an applicant's approach to address CCF hazards caused by latent defects in the software or software-based logic. This type of CCF hazard is considered a beyond-design-basis event for structures, systems, and components (SSCs) that employ a robust design process to reduce the likelihood of design defects. The plant response to these beyond-design-basis events may be analyzed using either conservative or best-estimate methods. ~~However, in integrated DI&C systems, a single random hardware failure can have cascading effects, similar to a CCF hazard (e.g., loss of multiple functions within a safety group, or spurious operation of functions within multiple safety groups).~~ Single random hardware failures with cascading effects are considered DBEs, because random hardware failures are expected during the life of the facility. DBEs should be analyzed using conservative methods to demonstrate that the plant response to these events is bounded by the events in the accident

[5] IEEE 100, "The Authoritative Dictionary of IEEE Standards Terms," defines "firmware" as the combination of a hardware device and computer instructions and data that reside as read-only software on that device.

analysis section of the SAR. RG 1.53 provides guidance for the deterministic analysis of single failures in safety-related systems.

This BTP provides guidance for reviewing (1) design attributes, such as the use of diverse equipment within a system or component to eliminate the CCF hazard from further consideration,[6] (2) diverse external equipment, including manual controls and displays to mitigate a CCF hazard, and (3) other measures to ensure conformance with the NRC's position on addressing CCF hazards in DI&C systems as specified in the SRM on SECY-93-087 and SECY-18-0090. The objectives of this review are to verify the following:

- Vulnerabilities to a CCF hazard have been adequately identified and addressed for DI&C systems using a graded approach based on the safety significance of the system.

- For DI&C systems of high safety significance, an adequate D3 assessment has been conducted and meets the acceptance criteria described in this BTP. An adequate D3 assessment consists of
    - An evaluation of vulnerabilities to a CCF hazard due to latent defects in system and the effectiveness of any credited attributes to eliminate the CCF hazard from further consideration;
    - Identification of any credited diverse means to mitigate CCF hazards that have not been eliminated from further consideration and the evaluation of the effectiveness of these diverse means; and
    - An assessment of the consequences of residual CCF hazards that have not been eliminated from further consideration or mitigated to demonstrate that the consequences remain bounded[7] by the events analyzed in the accident analyses.
- A qualitative assessment of proposed DI&C systems of lower safety significance obtains results that meet the acceptance criteria within this BTP.

~~This BTP also addresses the applicant's assessment of vulnerabilities to a CCF hazard due to latent software defects that can cause the spurious operation of a safety-related component or a component that is NSR, because such spurious operations have the potential to put the plant in a condition that has not been previously analyzed in the accident analysis. If these conditions have not been analyzed, then such conditions may not be adequately mitigated by an I&C system. This BTP provides criteria for reviewing an applicant's assessment of CCF hazards of DI&C systems that can result in spurious operation of safety-related components or components that are NSR.~~

## B. BRANCH TECHNICAL POSITION

1. Introduction

[6] The description of how a CCF hazard is eliminated from further consideration is discussed in Section B.3.1 of this BTP.
[7] The term "bounded" as used in the BTP means that the plant conditions remain within the acceptance criteria of the events analysis in the accident analysis.

accident analysis. Typically, the automatic safety-related I&C system is credited, but for some events, manual safety-related controls are the ones credited.

The four positions from the SRM on SECY-93-087, acknowledge that DI&C system development errors (i.e., latent defects) are a credible source of CCF hazards. Generally, DI&C systems containing software or logic cannot be fully tested except for very limited cases, nor can their failure modes be completely predicted because software does not have a physical manifestation that limits its behavior. Therefore, DI&C systems may be vulnerable to CCF hazards if ~~either (1)~~ identical system designs and identical copies of the software or software-based logic are present in redundant divisions of safety-related systems~~, or (2) previously separated functions have been integrated into a single DI&C system~~. Also, some errors, such as those labeled as "software design errors," normally result from errors in the higher-level requirements (e.g., system requirements or design specifications), in which the system design misrepresents the actual process. As used in this BTP, terms such as "higher-level requirements" do not refer to NRC regulatory requirements but to system or component design or operating characteristics that are relied upon to accomplish the stated system or component functions. Throughout this BTP, context indicates whether requirements are NRC regulatory requirements.

SECY-18-0090 recognizes that, although significant effort has been applied to the development of highly reliable DI&C systems, some residual faults may remain undetected within a system and could result in CCF hazards that can challenge plant safety. ~~This includes CCF hazards that result from loss of the safety function or those caused by spurious operation of a safety function or other design function.~~ To address these CCF hazards, the NRC staff should verify that for each event analyzed in the accident analysis section of the SAR, the application has:

- Identified vulnerabilities to CCFs due to a design or implementation defect in a DI&C system and evaluated the impacts of these postulated CCFs to safety functions or other design functions to determine whether these postulated CCFs can lead to a hazard;
- Demonstrated that a CCF hazard due to these residual defects has been either adequately prevented through use of appropriate measures (e.g., diversity within the design, testing, and defensive measures) or mitigated through use of a diverse means; and
- Assessed the ability of the overall plant design (e.g., I&C systems, mechanical systems, and manual operator action) to maintain plant safety, using conservative or "best estimate" methods, for those CCF hazards that have not been shown to be prevented or mitigated.

## 1.2. Critical Safety Functions

In the revised SECY-93-087, Item II.Q, included with the SRM, the NRC staff identified the following critical safety functions to be managed from the MCR per Position 4 of this SRM:

- reactivity control
- core heat removal
- reactor coolant inventory

- containment isolation
- containment integrity

Therefore, a safety function identified in the SAR may not always be a “critical safety function,” as defined in the SRM on SECY-93-087.

2. Graded Approach and Level of Integration for Addressing Common-Cause Failure

2.1. Graded Approach for Categorizing Digital Instrumentation and Control Systems

This BTP adopts a graded approach, described in Table 2-1, for determining how to address CCF hazards based on the safety category and significance of the SSC. For assessing vulnerabilities to CCF hazards, a graded approach refers to analyses performed for equipment of differing safety significance in which CCF hazard concerns apply.

**Table 2-1: Categorization Scheme for Implementing a Graded Approach To Address CCF Hazards**

| | Safety-Related | ~~Not Safety-Related~~ |
|---|---|---|

| | | |
|---|---|---|
| **Safety Significant**<br>A significant contributor to plant safety | **A1 DI&C SSCs**<br><br>Relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE.<br><br>**or**<br><br>Failure could directly lead to accident conditions that may cause unacceptable consequences (i.e., exceeds siting dose guidelines for a DBE) if not mitigated by other A1 systems.<br><br>**Application should include a D3 assessment as described in Section B.3** | ~~**B1 DI&C SSCs**~~<br><br>~~Directly changes the reactivity or power level of the reactor, or affects the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).~~<br><br>~~**or**~~<br><br>~~Failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system.~~<br><br>~~**Application should include a qualitative assessment as described in Section B.4**~~ |
| **Not Safety Significant**<br>Not a significant contributor to plant safety | **A2 DI&C SSCs**<br><br>Provides an auxiliary or indirect function in the achievement or maintenance of plant safety.<br><br>**or**<br><br>Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state.[9]<br><br>**Application should include a qualitative assessment as described in Section B.4** | ~~**B2 DI&C SSCs**~~<br><br>~~Does not have a direct effect on reactivity or power level of the reactor or affect the integrity of the safety barriers (fuel cladding, reactor vessel, or containment).~~<br><br>~~**and**~~<br><br>~~Failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin.~~<br><br>~~**Application may need to include a qualitative assessment as described in Section B.4** if the proposed design could introduce conditions[10] that have not been previously analyzed in the SAR.~~ |

For example, an assessment of CCF hazards for a digital RTS would be expected to be more rigorous than an assessment of CCF hazards for a safety-related MCR Heating, Venting, and Air Conditioning (HVAC) chiller. While the HVAC chiller is a safety-related system that maintains certain temperature and humidity in the MCR for equipment and personnel to operate properly, a failure of this system is not as significant as the failure of the RTS because operators will have operating procedures or diverse means to control temperature and humidity and will shut down the plant, if necessary.

Risk insights in terms of safety consequences from site-specific probabilistic risk assessments (PRAs) can be used to support the safety-significance determination in categorizing the DI&C system. Use of such risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system. The application should document the basis for categorizing the proposed DI&C system, including any use of risk insights.

[9] The plant safe shutdown state is site-specific, as defined in the particular facility's licensing basis.
[10] For example, newly combined design functions, shared resources, or connectivity to other plant systems.

The reviewer should reach a conclusion that the application provides adequate information to show that consequences of CCF hazards of an A1 or portions of an A1 system are acceptable if the application shows the following acceptance criteria are met:

a. For each AOO in the design basis occurring in conjunction with the CCF hazard, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.

b. For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic or conservative assumptions does not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).

4. Qualitative Assessment

RIS 2002-22, Supplement 1, describes a methodology that the NRC staff finds acceptable to assess the likelihood of failure of a proposed modification of an SSC with digital technology, referred to as a qualitative assessment. The qualitative assessment described in RIS 2002-22, Supplement 1, is intended for modifications to SSCs of low safety significance (i.e., A2~~ and B1~~) and not for SSCs of high safety significance (i.e., A1 systems).

The qualitative assessment considers three factors that, when taken in the aggregate, can be used to demonstrate that a proposed digital modification to an SSC will exhibit a low likelihood of failure (e.g., low likelihood of CCF) such that likelihood of failure of the proposed DI&C system is consistent with the assumptions in the SAR. These three factors include:

a. design attributes and features of the DI&C system or component;

b. quality of the design process of the DI&C system or component; and

c. applicable operating experience regarding the DI&C system or component.

Consideration of these factors, as well as supporting failure analysis information as described in RIS 2002-22, Supplement 1, is an acceptable method to address CCF hazards in A2~~, B1, and applicable B2~~ systems. The application should include a qualitative assessment that documents (1) how these three factors have been used to reduce the likelihood of CCF hazards to eliminate it from further consideration, and (2) the supporting failure analysis.

Acceptance Criteria

As described in RIS 2002-22, Supplement 1, the acceptance criteria used to determine whether an SSC has a low likelihood of failure such that current licensing assumptions continue to be met are referred to as “sufficiently low.” The concept of “sufficiently low” was developed to address the likelihood of a CCF hazard due to latent digital defects of a system or component

modified with digital technology. The “sufficiently low” definition incorporates consideration of failure likelihood of a proposed SSC to failures documented in the SAR. This approach can also be used for a new reactor design.

The reviewer should reach a conclusion that the application has addressed a CCF hazard in A2~~, B1, or applicable B2~~ systems if the application provides a qualitative assessment demonstrating the likelihood of the CCF hazard is sufficiently low based on any of the following criteria :

a. Design attributes and features of the proposed system that reduce the likelihood of CCF hazards.

b. Quality of the design process of the DI&C system that reduces the likelihood for CCF hazards due to latent defects in the software or software-based logic in the DI&C system or component.

c. The applicable operating experience regarding the DI&C system or component collectively supports a conclusion that the DI&C system or component will operate with high reliability for the intended application. Operating experience in most cases can serve to compensate for weakness in addressing the other two criteria.

d. The proposed system will not result in a failure that could invalidate the plant licensing basis (e.g., maintaining diverse systems for reactivity control).

~~5. Spurious Operation Assessment~~

~~5.1. Operating Reactors Not Required To Address IEEE Std 603-1991~~

~~For proposed DI&C modifications in plants not licensed under IEEE Std 603-1991, the application should include an assessment demonstrating that the spurious operations assumed in the accident analysis are not invalidated by the proposed modification to the DI&C system.~~

~~Acceptance Criteria~~

~~The reviewer should reach a conclusion that the application includes adequate information on the results of the spurious operation assessment if the application demonstrates the spurious operation of safety-related components or components that are NSR assumed in the accident analysis have not been invalidated by the proposed modification of the DI&C system or component.~~

~~5.2. IEEE Std 603-1991 Applies~~

~~Pursuant to the incorporation by reference in 10 CFR 50.55a, IEEE Std 603-1991, Clauses 4.8 and 5.6.3, require that safety-related systems be designed to prevent conditions that can lead to performance degradations of the safety-related system. This includes conditions such as failures or consequential actions by systems that are NSR that could lead to spurious operation of both safety-related components and components that are NSR. For DI&C systems in plants that have IEEE Std 603-1991 as part of their licensing basis or for applications for CPs, OLs, SDAs, DCs, COLs, or MLs, the potential for spurious operation resulting from a CCF hazard of~~

the DI&C system should be assessed using the following considerations:

a. The spurious operation should be considered as an initiating event without a concurrent DBE.

b. For an A1 system, potential spurious operation of safety-related components or components that are NSR due to CCF hazards can be adequately addressed through any combination of the following:

   1. CCF hazard has been eliminated from further consideration per the criteria within Section B.3.1;

   2. CCF hazard has been adequately mitigated, per the criteria within Section B.3.2, using a diverse means to mitigate the initiating event created by the spurious operation of components; or

   3. The consequences of the initiating event created by the spurious operation of safety related components or components that are NSR are acceptable per the acceptance criteria within Section B.3.3.

      i When applying the acceptance criteria within Section B.3.3, whether the initiating event created by the CCF hazard is considered an AOO or postulated accident should be justified and documented in the application.

      ii The quality development process of an A1 system or components may be credited to reduce the likelihood of CCF hazards that could lead to spurious operation of a safety function. As such, the application should demonstrate that the initiating event created by potential spurious operation of a single safety function (e.g., spurious operation of both emergency core cooling system trains) is bounded by the accident analysis.

c. For an A2 or B1 system, potential spurious operation of safety-related components or components that are NSR due to CCF hazards can be adequately addressed through any combination of the following:

   1. Likelihood of CCF hazards are reduced to “sufficiently low” level using the measures described in Section B.4

   2. CCF hazard has been adequately mitigated, per the criteria within Section B.3.2, using a diverse means to mitigate the initiating event caused by spurious operation of components;

   3. The consequences of the initiating event created by the spurious operation of safety related components or components that are NSR are acceptable per the acceptance criteria within Section B.3.3.

      i When applying the acceptance criteria within Section B.3.3, whether the initiating event created by the CCF hazard is considered an AOO or postulated accident should be justified and documented in the application.

      ii For highly-integrated B1 systems (e.g., distributed control systems), the application should demonstrate that potential spurious operation of multiple functions is bounded by the accident analysis.

iii For discrete B1 systems, the application should demonstrate that potential spurious operation of the control functions performed by each discrete B1 system is bounded by the accident analysis.

iv The analysis of potential spurious operation should include A2 or B1 systems that are considered multi-divisional control and displays.

Acceptance Criteria

The reviewer should reach a conclusion that the spurious operation assessment results are acceptable if the application demonstrates the following acceptance criteria are met:

a. Any defensive measures or design attributes implemented for an A1 system to eliminate CCF hazard from further consideration meet the acceptance criteria within Section B.3.1.

b. Any measures implemented for an A2 or B1 system to demonstrate that the likelihood of CCF hazard is sufficiently low meet the acceptance criteria within Section B.4.

c. Any automatic functions or manual operator action credited to mitigate the conditions caused by potential spurious operation of safety-related components or components that are NSR meet the acceptance criteria within Section B.3.2.

d. For those CCF hazards that have not been shown to be mitigated or prevented, consequences resulting from spurious operation of safety-related components or components that are NSR are bounded by the events analyzed in the accident analysis.

6. Manual System Level Actuation and Indications to Address Position 4 of the SRM on SECY-93-087, Item 18.

Displays and manual controls provided for compliance with Position 4 of the SRM on SECY-093-87, Item 18 should be sufficient both to monitor the plant state and to enable control room operators to actuate critical safety functions. For DI&C system modifications to operating plants, retention of existing analog displays and controls in the MCR could satisfy Position 4. However, if existing displays and controls are digital, or the same platform is used both for mitigating the DBE and to provide signals to these analog displays and controls, retaining existing analog displays and controls may not be sufficient to meet Position 4.

For displays and manual controls used to conform to Position 4, the following criteria should be met:

a. The displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

b. The indication and manual controls to actuate these critical safety functions should be at the system- or division-level and located within the MCR.

c. Equipment that is NSR may be used for these manual controls and indications, provided that the equipment is reliable and of sufficient quality. This equipment should be similar

attributes or measures are effective. Identification of any remaining vulnerabilities to CCF hazards.

2. For CCF hazards that have not been eliminated from further consideration, identification of any diverse means provided to accomplish the same or a different function than the safety function disabled by a postulated CCF. If any diverse means are credited to mitigate the CCF hazard, the NRC staff should review the information provided to demonstrate the effectiveness of the diverse means, including any HFE analysis associated with manual operator action as a diverse means.

3. For CCF hazards that have not been eliminated from further consideration or mitigated using diverse means, identification of any analysis performed to demonstrate that consequences of a CCF hazard are within acceptable limits for each AOO and postulated accident. If any consequence analysis has been performed, the NRC staff should review the results of this analysis.

c. For A2 ~~and B1~~ systems, the results of the qualitative assessment of these systems, specifically, the following:

1. Information supporting the use of design attributes and features to reduce the likelihood of a CCF hazard such that it is sufficiently low.

2. Information regarding the quality of the design and development process to reduce the likelihood of CCF hazards due to latent defects in the software or software-based logic of the system or component.

3. Information regarding applicable operating experience to show that the DI&C system will operate with high reliability for the intended application.

~~d. For a B2 system, information to show that the proposed design will not introduce any conditions not bounded by the events in the accident analysis due to the specific implementation.~~

~~e. Results of the spurious operation assessment, for I&C systems in NPPs to which IEEE Std 603-1991 applies, specifically, information showing the following:~~

~~1. Vulnerabilities to potential spurious operations due to a CCF hazard in an A1 system have been addressed through use of design attributes, defensive measures, or diverse means to prevent, limit, or mitigate the consequence of a CCF;~~

~~2. Vulnerabilities to potential spurious operations due to a CCF hazard in an A2 or B1 system have been addressed through use of a combination of the three factors described in Section B.4; or~~

~~3. The consequence of a potential spurious operation due to a CCF hazard is bounded by the accident analysis;~~