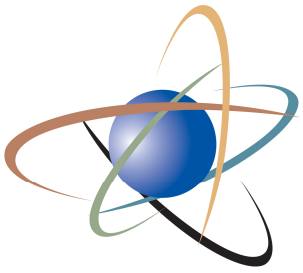


U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-02

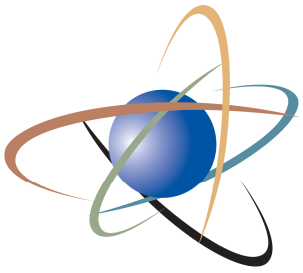
Task Working Group #2:
Diversity and Defense-in-Depth Issues

Interim Staff Guidance

Revision 2

June 5, 2009

ML091590268



U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

*By E-mail ** See Previous

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-02

Task Working Group #2:
Diversity and Defense-in-Depth Issues

OFFICE	NRR/DE/EICB	NRO/DCIP/COLP	NRO/DE/ICE2	OGC/NLO	NRR/DE
NAME	WKemper	MJunge	TJung	RWeisman	S. Walker
DATE	05/28/09*	05/28/09*	05/28/09*	03/23/09**	05/28/09
OFFICE	NRO/DE	NSIR/DSP	RES/DFER	NMSS/FCSS	NRR/ADES
NAME	LDudes	SMorris	SRichards	MBailey	JGrobe
DATE	05/29/09*	06/04/09*	06/01/09*	06/01/09*	06/05/09*

Interim Staff Guidance
Revision 2

June 5, 2009

ML091590268

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-02

Task Working Group #2:
Diversity and Defense-in-Depth Issues

Interim Staff Guidance
Revision 2

IMPLEMENTATION

This Interim Staff Guidance (ISG) provides acceptable methods for implementing diversity and defense-in-depth (D3) in digital I&C system designs. This guidance is consistent with current NRC policy on digital I&C systems and is not intended to be a substitute for NRC regulations, but to clarify how a licensee or applicant may satisfy those regulations.

This ISG also clarifies the criteria the staff would use to evaluate whether a digital system design is consistent with D3 guidelines. The staff intends to continue interacting with stakeholders to refine digital I&C ISGs and to update associate guidance and generate new guidance where appropriate.

Except in those cases in which a licensee or applicant proposes or has previously established an acceptable alternative method for complying with specified portions of NRC regulations, the NRC staff will use the methods described in this ISG to evaluate compliance with NRC requirements.

1. ADEQUATE DIVERSITY and 2. MANUAL OPERATOR ACTIONS

SCOPE

1. Adequate Diversity: Additional clarity is desired on what constitutes adequate D3. For example: 1) How much D3 is enough; 2) Are there precedents for good engineering practice; 3) Can sets of diversity attributes and criteria provide adequate diversity; 4) How much credit can be taken for designed-in robustness in determining the appropriate amount of diversity; and 5) Are there standards that can be endorsed?

2. Manual Operator Actions: Clarification is desired on the use of operator action as a defensive measure and corresponding acceptable operator action times.

STAFF POSITION

There is no distinction in the D3 guidance for digital Reactor Protection System (RPS) designs for new nuclear power plants and current operating plants. In the context of this interim staff guidance, the RPS consists of the Reactor Trip System (RTS) and the Engineered Safety Features Actuation System (ESFAS).

While the NRC considers common cause failures (CCFs) in digital systems to be beyond design basis, the digital RPS should be protected against CCFs.

The licensee or applicant should perform a D3 analysis to demonstrate that vulnerabilities to CCFs are adequately addressed. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," dated December 1994 (Reference 1-1) and Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," of NUREG-0800, "Standard Review Plan," (Reference 1-2) describe an acceptable process for performing a D3 analysis. The D3 analysis may determine that one or more RPS safety functions could become subject to a CCF. In that case, the licensee or applicant may use realistic assumptions to analyze the plant response to design-basis events with a CCF. In this way, the applicant can identify backup systems or actions necessary for accomplishing the required safety functions.

When an independent and diverse method is needed as backup to an automated system used to accomplish a required safety function, the backup function can be accomplished via either an automated system, or manual operator actions performed in the main control room. The preferred independent and diverse backup method is generally an automated system. The use of automation for protective actions is considered to provide a high-level of licensing certainty. Further, the licensee or applicant should provide sufficient information and controls (safety or non-safety) in the main control room that are independent and diverse from the RPS (i.e., not subject to the CCF).

If automation is used as the backup, it should be provided by equipment that is not affected by the postulated RPS CCF and should be sufficient to maintain plant conditions within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident. The automated backup function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function(s) under the associated event conditions. The automated backup system should be similar in quality to systems required by the Anticipated Transient Without Scram (ATWS) rule (10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants") (Reference 1-3), as described in the enclosure to Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related" (Reference 1-4). Other systems that are credited in the analysis that are in continuous use (e.g., the normal RCS inventory control system or normal steam generator level control system) do not warrant the augmented quality discussed above.

If manual operator actions are used as backup, a suitable human factors engineering (HFE) analysis should be performed to demonstrate that plant conditions can be maintained within BTP 7-19 recommended acceptance criteria for the particular anticipated operational occurrence or design basis accident. The staff will review the

acceptability of such actions in accordance with DI&C-ISG-05, "Highly-Integrated Control Rooms - Human Factors Issues," Revision 1 (Reference 1-5). For actions with limited margin, such as less than 30 minutes between time available and time required for operators to perform the protective actions, a more focused staff review will be performed.

In addition to the above guidance, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be unaffected by the CCF in the RPS. However, these displays and controls could be those used for manual operator actions as described above. Implementation of these manual controls should be in accordance with existing regulations.

The following three examples illustrate applications of the above guidance:

(1) An RPS design consists of two channels using one type of digital system and another two channels using a diverse digital system. A D3 analysis, (e.g., performed consistent with NUREG/CR-6303 and BTP 7-19 guidance), determines that the two diverse digital systems are not susceptible to a CCF. No additional diversity is needed in this design. Note that in this design, a channel removed from service for testing or maintenance may be subject to an allowable outage time limit. This should be addressed in plant technical specifications and associated bases.

(2) An RPS design performs safety functions on a common computer system replicated in redundant channels. A D3 analysis reveals that certain safety functions could be subject to a CCF. Consequently, a diverse automated backup system is provided to perform the safety functions affected by the CCF. The non-safety diverse automated backup system is of augmented quality, similar to systems required by the ATWS rule.

(3) As in Example 2 above, a D3 analysis reveals that certain RPS safety functions are subject to a CCF. An analysis of plant responses to Chapter 15 events is performed to determine the time available to implement the protective actions so as to maintain the plant within the BTP 7-19 recommended acceptance criteria. An associated HFE analysis in accordance with DI&C-ISG-05, Revision 1, demonstrates that manual operator actions may be performed for some events, within the time available. For these events, manual operator action could be used as a diverse method to perform the safety functions affected by the CCF.

RATIONALE

Typically, new reactor designs will have four independent divisions (or channels) for RPS. In some cases the divisions may consist of two subdivisions, thus further reducing the probability of losing the full safety function of a division. However, the concern is that an error in software common in all divisions could cause all divisions of a protection system to malfunction. Consolidation of many safety functions into a limited number of digital components duplicated in all four divisions increases this concern. In this

guidance, common software includes firmware[1] and logic developed from software-based development systems.

A CCF could result in the operator losing availability of automatic RPS functions and the instrumentation and controls the operator has been trained to use to operate the plant and to mitigate abnormal operational occurrences and design basis events. Operators receive regular simulator training that includes many unusual and emergency situations. However, specific CCFs may be exceedingly difficult to anticipate. Despite the Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (AOPs), which may include some CCF-related actions, operators will likely be under significant pressure to respond appropriately to mitigate unanticipated plant events. Good human factors dictate that this pressure to perform should be minimized.

The use of automated in lieu of manual independent and diverse backup for the automatic RPS actions subject to a CCF has the advantages of reducing dependence on operators for a potentially hazardous situation, improving the design process, and simplifying the staff's safety review. Further supporting the use of automated backup actions, probabilistic risk analyses have shown that the factor of failure by humans is significantly higher than that of digital instrumentation and control (I&C) equipment.

In current plants, some EOPs and AOPs call for operator action in less than 30 minutes. Even if symptom-based, it is unlikely these procedures are designed to account for the full range of potential CCF events that may arise when digital systems are used instead of existing analog systems. Further, the automated diverse backup is for the automatic RPS functions, not the usual manual operator follow-on actions that are prescribed by post-trip procedures and emergency operating procedures. In light of these considerations, the guidance in ISG-5 for crediting manual operator actions in D3 analyses is intended to ensure that licensees and applicants that elect to use manual protective actions conduct a rigorous analysis and validation process that provides high confidence the credited actions can be reliably performed within the time available and that the capability to perform the actions will be maintained.

REFERENCES

1-1. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.

1-2. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," March 2007.

1-3. *U.S. Code of Federal Regulations,* Title 10, *Energy,* Part 50, Section 62, "Requirements for Reduction of Risk from Anticipated Transient Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."

1-4. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," April 16, 1985 (Accession No. ML031140390).

[1] 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.

1-5. DI&C-ISG-05, “Highly-Integrated Control Rooms - Human Factors Issues,” Revision 1, November 3, 2008 (ML082740440).

3. BTP 7-19 POSITION 4 CHALLENGES

SCOPE

BTP 7-19 Position 4 Challenges: Current Commission policy addresses system-level actuation in BTP 7-19, Position 4 (Reference 3-1). Further clarification is needed for whether credit can be taken for component-level versus system-level actuation of equipment. The NRC should clarify the rationale for applying BTP 7-19, Position 4 for digital system upgrades in existing plants.

STAFF POSITION

The staff recommends that BTP 7-19, Position 4 be re-written to state:

> "In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual system level actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hard-wired connections."

Diverse backup system manual initiations of safety systems should be performed on a system-level basis for each division. This recommendation does not prohibit the use of manual controls for operating individual safety system components after the corresponding safety system functions have been actuated.

This guidance applies to both the currently operating reactors and new reactors; however, no backfit is intended or required for existing systems. The potential for CCF in digital safety systems should be considered whether the systems are to be used in new plants or for retrofits in existing plants. The main difference is that new plants will predominantly use digital technology, but operating plants will typically introduce digital retrofits in a phased approach. Therefore, Point 4 of BTP 7-19 should apply both to new plants and to existing plants installing substantial digital equipment to upgrade existing RTS or ESFAS.

For safety systems, IEEE-603 Sections 6.2 and 7.2, which are incorporated by reference in 10 CFR 50.55a(h), require means in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manual manipulations and shall depend on operation of a minimum of equipment. If the means is diverse from the software-based automatically initiated RPS, the design meets the system-level actuation criterion in Point 4 of BTP 7-19.

RATIONALE

BTP 7-19, Position 4 states:

> "A set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Staff Positions 1 and 3."

The intent of providing for system level actuation was to assure that the actuation, however achieved, was possible using a minimum number of controls from within the control room, instead of requiring plant operators to actuate or control individual equipment at various locations within the plant. However, the method of actuating the protective functions is not as important as the actuation being:

a) at the division level;
b) from the control room;
c) required with sufficient time available for the operators to determine the need for protective actions even with malfunctioning indicators, if credited in the D3 coping analysis;
d) appropriate for the event;
e) supported by sufficient instrumentation that indicates that;
    1. the protective function is needed
    2. the safety-related automated system did not perform the protective function
    3. the manual action was successful in performing the safety function

The interim staff guidance described above is consistent with this rationale.

REFERENCES

3-1. NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems." March 2007.

4. EFFECTS OF COMMON CAUSE FAILURE (CCF)

SCOPE

Effects of Common Cause Failure (CCF): BTP 7-19 guidance recommends consideration of CCFs that "disable a safety function." The nuclear industry requested clarification regarding the effects of CCFs that should be considered (e.g., fails to actuate and/or spurious actuation). Industry also requested that the staff determine whether spurious actuations should be considered when evaluating software CCF.

STAFF POSITION

Many possible types of protection system failures may occur as a result of failure to actuate. Among these, a simple failure of the total system might not be the worst case failure, particularly when analyzing the time required for identifying and responding to the condition. For example, a failure to trip might not be as limiting as a partial actuation of an emergency core cooling system, with digital indications of a successful actuation. In cases such as this, it may take an operator longer to evaluate and correct the safety system failure than it would if there was a total failure to send any actuation signal. For this reason, the evaluation of failure modes as a result of software CCF should include the possibility of partial actuation and failure to actuate with false indications, as well as a total failure to actuate.

The primary concern is that an undetected failure within the digital system could prevent proper system operation. A failure or fault that is detected can be addressed; however, failures that are non-detectable may prevent a system actuation when required. Consequently, non-detectable faults are of concern. Therefore, a diverse means to provide the required safety function, or some other safety function that will adequately address each licensing basis event should be provided. (Software CCF was declared a beyond design basis event by the Commission in Staff Requirements Memorandum dated July 21, 1993 (Reference 4-1), issued in response to SECY-93-087, dated April 2, 1993 (Reference 4-2).This issue is addressed in Staff Position 7.) Industry also requested that the staff determine whether spurious actuations should be considered when performing single failure analyses associated with software CCF.

Software CCFs that cause an undesired trip or actuation can be detected because these types of failures are self-announcing. However, there may be circumstances in which a spurious trip or actuation would not occur until a particular signal trajectory within the software is reached. In these cases, the spurious trip or actuation would not occur immediately upon system startup, but could occur under particular plant conditions. This circumstance is still self-announcing, even if the annunciation did not occur on initial test or startup. Use of design techniques (e.g., a constant and unchanging signal trajectory within the software that is unaffected by plant conditions) is therefore recommended.

In general, spurious trips and actuations are of a lesser safety concern than failures to trip or actuate. There may be plant and safety system challenges and stresses; however, these challenges are not as significant as failures to respond to abnormal operating occurrences and design basis events.

For these reasons, spurious trips or actuations of safety-related digital protection systems resulting from CCFs do not need to be addressed beyond what is already set forth in plant design basis evaluations.

However, in accordance with the augmented quality guidance for the diverse backup system used to cope with a CCF, the design of a diverse automated or diverse manual backup actuation system should consider and address how to significantly reduce or eliminate the potential for a spurious actuation of the protective system.

RATIONALE

There are two inherent safety functions that safety-related trip and actuation systems provide. The first safety function is to provide a trip or system actuation when plant conditions necessitate that trip or actuation. However, in order to avoid challenges to the safety systems and to the plant, the second function is to not trip or actuate when such a trip or actuation is not required by plant conditions. A simple metric would be:

	Plant conditions require a trip or actuation	Plant conditions do not require a trip or actuation
Trip or Actuation occurs	Proper System Operation	**System Failure** (Spurious Actuation)
Trip or Actuation does not occur	**System Failure** (Actuation does not occur or incomplete activation)	Proper System Operation

Therefore, to be consistent with the above guidance, the effects of failures to actuate and the effects of spurious trips and actuations should be evaluated to ensure the effects are bounded by the plant design basis.

REFERENCES

4-1. SRM to SECY-93-087 93, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993 (ML003708056).

4-2. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993 (ML003708021).

5. COMMON CAUSE FAILURE (CCF) APPLICABILITY

SCOPE

Common Cause Failure (CCF) Applicability: Clarification is needed for identification of design attributes that are sufficient to eliminate consideration of CCFs (e.g., degree of simplicity).

STAFF POSITION

There are two design attributes that are sufficient to eliminate consideration of CCF:

> (1) Diversity - In Example 1 of Staff Positions 1 and 2 in this ISG, sufficient diversity exists in the protection system such that CCFs within the channels can be considered to be fully addressed without further action.
>
> Example: An RPS design in which each safety function is implemented in two channels that use one type of digital system and another two channels use a diverse digital system. A D3 analysis performed consistent with the guidance in NUREG/CR-6303 (Reference 5-1) and BTP 7-19 (Reference 5-2) determines that the two diverse digital systems are not subject to a CCF.
>
> In this case, no additional diversity would be necessary in the safety system.
>
> (2) Testability - A system is sufficiently simple such that every possible combination of inputs, internal and external initial states, and every signal path can be tested; that is, the system is fully tested and found to produce only correct responses.

What constitutes "sufficient diversity" should be evaluated on a case-by-case basis, considering design and process attributes that preclude or limit certain types of CCFs. The Staff Positions 1 and 2 in this ISG provide guidance for evaluating the need for diversity in a system design.

In assessing the system states, the guidance provided in IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” Clause 5.4.1, “Computer system [equipment qualification] testing,” (Reference 5-3) should be addressed:

> Computer system qualification testing (see 3.1.36) shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and

interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

Clause 5.4.1 of IEEE Std 7-4.3.2-2003 directs the system developer/user to perform equipment qualification of the system (i.e., hardware and software) in its operational states while the system is operating at the limits of its equipment qualification envelope. The software and diagnostics should be representative of the software used in actual operation to a degree that provides assurance that the system states produced by the actual system will be tested during the equipment qualification process.

RATIONALE

The design attributes of sufficient diversity and testability, as explained above, can be used to eliminate consideration of CCF.

REFERENCES

5-1. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994 (ADAMS Legacy Library Accession No. 9501180332).

5-2. NUREG-800, Standard Review Plan, BTP 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems.”

5-3. IEEE Std 7-4.3.2-2003, “IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.”

6. ECHELONS OF DEFENSE

SCOPE

Echelons of Defense: As described in NUREG-0737 Supplement 1 (Reference 6-1), sufficient information should be provided to the operators to monitor (and thereby control) the following plant safety functions and conditions:

1. Reactivity control
2. Reactor core cooling and heat removal from the primary system
3. Reactor coolant system integrity
4. Radioactivity control
5. Containment conditions

BTP 7-19 guidance references the echelons of defense described in NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," (Reference 6-2) for maintaining the above safety functions within safe margins for currently operating nuclear power plants:

1. Control systems
2. Reactor Trip System (RTS)
3. Engineered Safety Features Actuation System (ESFAS)
4. Monitoring and indications

Additional clarification is desired regarding how the echelons of defense for maintaining the above safety functions should factor into D3 analyses. A particular concern is that the current BTP 7-19 guidance does not consider plant design characteristics and operating procedures that affect how D3 is actually used to maintain the safety functions.

STAFF POSITION

The RTS and ESFAS functions may be combined into a single digital platform. The four echelons of defense described in BTP 7-19 are only conceptual and, with the exception of the subset of monitoring and indication noted in Point 4, BTP 7-19 does not imply that these echelons of defense must be independent or diverse. Rather, where a postulated CCF impairs a safety function, a plant response in accordance with the acceptance criteria of Section 3 of BTP 7-19 should be demonstrated, regardless of the echelons of defense that may be affected.

RATIONALE

SECY-91-292 (Reference 6-3) described the above four echelons of defense. SECY-93-087 (Reference 6-4) and the associated Staff Requirements Memorandum addressed defense against CCFs in digital I&C systems, among other issues. SECY-91-292 and SECY-93-087 did not address the consolidation of these echelons of defense-in-depth into one digital system, nor did the Commission address combining echelons of defense at the time it established policy on digital system CCFs.

The use of digital I&C systems that combine all RTS and ESFAS functions within a single digital system software program have been proposed. Combining echelons of defense into a single software program could introduce new common cause digital system failure mechanisms that do not exist in systems that use separate software programs. CCFs involving multiple echelons of defense should be addressed using the applicable interim staff guidance and BTP 7-19. In other words, whether or not the RTS and ESFAS functions are combined into a single platform, the digital protection system should be protected against potential CCFs. Conformance to the applicable interim staff guidance and BTP 7-19 is an acceptable method to meet the acceptance criteria.

REFERENCES

6-1. NUREG-0737 Supplement 1, "Clarification of TMI Action Plan Requirements."

6-2. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994 (ADAMS Legacy Library Accession No. 9501180332).

6-3. SECY-91-292, "Digital Computer Systems for Advanced Light Water Reactors."

6-4. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993 (ML003708021).

7. SINGLE FAILURE

SCOPE

Single Failure: Additional clarification is required regarding classification of digital system CCFs as single failures in design basis evaluations.

STAFF POSITION

Based upon the definition of single failure in 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," (Reference 7-1) and the guidance provided by IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," (Reference 7-2) as endorsed by Regulatory Guide (RG) 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems, Rev. 2" (Reference 7-3), a digital system CCF, which includes software CCFs, does not meet the criteria of a single failure in design basis evaluations (which assume a single failure coincident with a design basis event). IEEE Std 379-2000 states, "Common cause failures not subject to single-failure analysis include those that can result from external environmental effects (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference), design deficiencies, manufacturing errors, maintenance errors, and operator errors."

Since digital system CCFs are not classified as single failures, postulated digital system CCFs should not be assumed to be a single random failure in design basis evaluations. Consequently, best-estimate techniques can be employed in performing analyses to evaluate the effect of digital system CCFs coincident with design basis events.

As with ATWS mitigation systems, if a postulated digital system CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is not subject to the same CCF, should be included in the overall system design. This diverse means should perform either the same function or a different function that will mitigate accidents or events that require the safety function assumed failed by the postulated CCF. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform under the associated event conditions.

RATIONALE

An error in identical software logic that is operating in otherwise independent safety system channels could cause a digital system CCF. As with ATWS events (i.e., reactor trip system CCFs), a digital system CCF, even when caused by a software error, is considered a failure that is beyond design basis. This conclusion is consistent with the Commission position described in the SRM for SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," (Reference 7-4 and Reference 7-5, respectively).

Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants," defines single failure as follows:

"Single failure. A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."

This definition addresses single failures that result in the loss of capability of a component. This is not the case for software CCFs, in which multiple failures (albeit by the same cause) occur in redundant components. Further, a CCF is not the result of a single component failing and causing cascading failures; instead, it is several related but independent failures arising from a common cause.

A loss of capability in redundant components caused by a digital system CCF is considered the result of a design deficiency, manufacturing error, maintenance error, or an operator error. These types of errors are specifically exempted from single failure analysis consideration by IEEE Std 379-2000, which is referenced by IEEE Std 603-1991 and endorsed by RG 1.53. As discussed in IEEE Std 379-2000, extensive NRC requirements for design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors. Further, requirements for personnel training; proper control room design; and operating, maintenance, and surveillance procedures are intended to afford protection from maintenance and operator errors.

REFERENCES

7-1. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”

7-2. IEEE Std 379-2000, “IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.”

7-3. Regulatory Guide (RG) 1.53, “Application of the Single-Failure Criterion of Nuclear Power Plant Protection Systems,” Rev. 2 (ML003740182).

7-4. SRM for SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs” (ML003708056).

7-5. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs” (ML003708021).