EDO Principal Correspondence Control

FROM: Said Abdel-Khalik, ACRS

DUE: 12/14/11

EDO CONTROL: G20110801
DOC DT: 11/14/11
FINAL REPLY:

TO:

Borchardt, EDO

FOR SIGNATURE OF : ** GRN **

CRC NO:

Borchardt, EDO

DESC:

Draft Final Revision 6 of Standard Review Plan Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems" (EDATS: OEDO-2011-0738)

DATE: 11/14/11

ROUTING:

Borchardt
Weber
Virgilio
Ash
Mamish
OGC/GC
Leeds, NRR
Sheron, RES
Kotzalas, OEDO

ASSIGNED TO: NRO

CONTACT: Johnson

SPECIAL INSTRUCTIONS OR REMARKS:

Please prepare response to ACRS for the signature of the EDO. Add the Commission and SECY as cc's. Also, include RidsAcrsAcnw_MailCTR to your distribution on the concurrence page. USE SUBJECT LINE IN RESPONSE.

Template: EDO-001

E-RIDS: EDO-01

EDATS

Electronic Document and Action Tracking System

EDATS Number: OEDO-2011-0738 **Source:** OEDO

General Information

Assigned To: NRO **OEDO Due Date:** 12/14/2011 11:00 PM

Other Assignees: **SECY Due Date:** NONE

Subject: Draft Final Revision 6 of Standard Review Plan Branch Technical Position 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"

Description:

CC Routing: NRR; RES

ADAMS Accession Numbers - Incoming: NONE **Response/Package:** NONE

Other Information

Cross Reference Number: G20110801 **Staff Initiated:** NO

Related Task: **Recurring Item:** NO

File Routing: EDATS **Agency Lesson Learned:** NO

OEDO Monthly Report Item: NO

Process Information

Action Type: Letter **Priority:** Medium

Sensitivity: None

Signature Level: EDO **Urgency:** NO

Approval Level: No Approval Required

OEDO Concurrence: NO

OCM Concurrence: NO

OCA Concurrence: NO

Special Instructions: Please prepare response to ACRS for the signature of the EDO. Add the Commission and SECY as cc's. Also, include: RidsAcrsAcnw_MailCTR to your distribution on the concurrence page. USE SUBJECT LINE IN RESPONSE.

Document Information

Originator Name: Said Abdel-Khalik **Date of Incoming:** 11/14/2011

Originating Organization: ACRS **Document Received by OEDO Date:** 11/14/2011

Addressee: R. W. Borchardt, EDO **Date Response Requested by Originator:** NONE

Incoming Task Received: Letter

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

November 14, 2011

Mr. R.W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT FINAL REVISION 6 OF STANDARD REVIEW PLAN BRANCH TECHNICAL POSITION 7-19, "GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS"

Dear Mr. Borchardt:

During the 588th meeting of the Advisory Committee on Reactor Safeguards, November 3-5, 2011, we completed our review of Draft Final Revision 6 of Standard Review Plan (SRP) (NUREG-0800), Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems." Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on September 7, 2011. During these reviews, we had the benefit of discussions with representatives of the NRC staff and comments from industry representatives. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. Draft Final Revision 6 to SRP BTP 7-19 should be issued subsequent to incorporation of the modifications noted in the discussion regarding Sections 1.8, 3.1, 3.5, 3.7, and 4.6.

2. The discussion of the difference between time available and time required in SRP Chapter 18, Appendix 18A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," should be revised to be consistent with Recommendation 1 for Sections 3.5 and 4.6.

BACKGROUND

In November 2006, industry representatives commented that there was confusion or insufficient guidance in the DI&C area, and that additional guidance was needed to provide for improved licensing certainty. In early 2007, a Steering Committee was formed and a project plan

developed for addressing issues associated with the application of computer-based DI&C systems in nuclear reactor protection and engineered safeguards systems. One of the results of the project plan was the issuance of Interim Staff Guidance (ISG) DI&C-ISG-02, "Diversity and Defense-in-Depth (D3) Issues," which provided guidance and positions that addressed seven problem statements from industry. We issued a report on DI&C-ISG-02 on October 16, 2007.

DISCUSSION

The purpose of BTP 7-19, Revision 6, is to provide guidance for evaluating an applicant's D3 assessment, design, and the design of manual controls and displays to ensure conformance with the NRC position on D3 for I&C systems incorporating digital, software-based or software-logic-based Reactor Trip System (RTS) or Engineered Safety Features (ESF), auxiliary supporting features, and other auxiliary features as appropriate. This BTP has the objective of confirming that vulnerabilities to common cause failures (CCFs) have been addressed in accordance with the guidance of the SRM on SECY-93-087, dated July 21, 1993, and clarification provided in this staff guidance, specifically:

- Verify that adequate diversity has been provided in a design to meet the criteria established by NRC guidance.

- Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by NRC guidance.

- Verify that the displays and manual controls for (plant) critical safety functions initiated by operator action are diverse from digital systems used in the automatic portion of the protection systems.

BTP 7-19, Revision 6, incorporates DI&C-ISG-02 guidance and acceptance criteria. In addition, it provides additional clarification and acceptance criteria on the independence of diverse means of actuation. It also addresses manual actions as a diverse means of actuation, the relationship between CCFs and diverse means of actuation, diversity considerations for automated and manual actions, and the diversity and CCF considerations when combining RTS and ESF actuation systems in a single controller or central processing unit.

Independence is a crucial attribute of reactor protection and safeguards systems. BTP 7-19, Revision 6, provides the following clarifying guidance on independence for the application of diverse means to these systems:

- Independence requirements of diverse means for safety protection systems (i.e., physical and electrical) are defined in IEEE Std. 603 and communication separation in DI&C-ISG-04, "Highly-Integrated Control Rooms—Communications Issues."

- Diverse means could be safety-related and part of a safety division, and would be subject to meeting divisional independence requirements.

- Diverse means could be non-safety-related; then the IEEE Std. 603 requirement to separate safety from non-safety equipment would still apply and would require independence of the two systems.

- In either case, the diverse means should be independent of the safety system such that a CCF of the safety system would not affect the diverse system.

The guidance in BTP 7-19, Revision 6, notes that diverse means for mitigating CCF may be automated or manual. Automated means are preferred. For an operator action to be acceptable as a diverse means, BTP 7-19, Revision 6, provides the following guidance:

- The D3 analysis should be performed using realistic assumptions.

- The diverse means to perform the safety function should not be subject to the same CCF.

- Circumstances where two manual actuation means would be needed are identified.

- If manual actuation is selected as diverse means, a Human Factors Engineering (HFE) analysis is needed to assure feasibility and reliability.

BTP 7-19, Revision 6, also provides criteria for assessing the acceptability of the HFE analysis by defining the time available and time required and including the following cautionary note in Sections 3.5 and 4.6:

> "Note: As the difference between Time Available and Time Required for operator action decreases, there can be increasing uncertainty in the estimate of time required for operator action. The uncertainty could invalidate a conclusion that operators can perform the action reliably within the time available. For actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed."

During our September 7, 2011, subcommittee meeting, it was noted that the first and second sentences are not inclusive of uncertainties in the determination of time available. To include evaluation of uncertainties in time available, the note should be revised to read as follows:

> Note: As the difference between time available and time required for operator action decreases, uncertainty in the estimate of both of these times must be evaluated carefully. These uncertainties could invalidate or reduce the level of assurance of a conclusion that operators can perform the action reliably within the time available. For actions with a limited margin of time to act, such as less than 30 minutes between the time available and the time required, additional staff review will be performed.

The discussion of the difference between time available and time required in SRP Chapter 18, Appendix 18A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses," should be revised to be consistent with this recommended revision.

Sections 1.8 and 3.7 of BTP 7-19 discuss the potential effects of CCFs on spurious actuations or trips of safety systems and considerations for their evaluation. Several examples of spurious actuations or trips caused by CCF are discussed. The guidance acknowledges that there may be plant and safety system challenges due to CCF-caused spurious actuations or trips. The discussion concludes that those actuations that are significant are already considered in the plant design basis evaluations. Sections 1.8 and 3.7 assert that "the effects of spurious trips and actuations do not need to be evaluated beyond what is set forth in the plant design basis evaluations" and that they are "of a lesser safety concern than failures to trip or actuate."

We disagree with these assertions. These statements are not consistent with the recognition that spurious actuations due to other causes such as fires can have significant effects. In addition, these statements send an implied message that D3 evaluations of CCF-caused spurious actuations or trips for DI&C systems are not expected. There may be circumstances where CCF-caused spurious actuations or trips could exacerbate an accident condition and mask operator information about the actual plant status.

Therefore, Section 1.8 should be revised to acknowledge this vulnerability of plants to CCF-caused spurious actuations or trips. The resulting plant conditions may not be fully evaluated in the design basis accident analyses because the applied single failure boundary conditions and supporting accident progression models do not predict the need for coincident initiation of the spuriously actuated functions. Thus, the D3 analyses should evaluate the effects from spurious actuations that can place the plant in a configuration that is not otherwise analyzed or bounded by the existing design basis accident analyses.

Additionally, the acceptance criteria in Section 3.7 should be revised to assure that the D3 assessments have evaluated the effects from spurious actuations that can place the plant in a configuration that is not otherwise analyzed or bounded by the existing design basis accident analyses, and that diverse mitigation strategies have been identified.

Section 3.1, "Specific Acceptance Criteria," Item 6 describes circumstances where two manual initiation means may be needed and where only one would suffice. In the November 3, 2011, briefing, a slide illustrating these circumstances was helpful in understanding the concept. We recommend that the figure from the briefing (Slide 20) be included in this section to provide an unambiguous illustration of the staff's basis on this issue.

BTP 7-19, Revision 6, also acknowledges that RTS and ESF actuation systems could be combined in a single controller or central processing unit. For such cases, it provides acceptance criteria that a complete D3 analysis should be performed to demonstrate and ensure that the combination does not result in any CCF vulnerability.

We commend the staff for their efforts in updating this SRP Branch Technical Position to incorporate this critical D3 information from DI&C-ISG-02. The staff has been responsive to our comments and issues.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

REFERENCES

1. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, Branch Technical Position (BTP) 7-19, Rev. 6, "Guidance for Evaluation of Diversity and Defense-in Depth in Digital Computer-Based Instrumentation and Control System," (ML110550791) (not officially issued)

2. Digital Instrumentation and Control, DI&C-ISG-02: Diversity and Defense-In-Depth Issues, Revision 2, June 5, 2009 (ML091590268)

3. Digital Instrumentation and Control, DI&C-ISG-05 Task Working Group #5: Highly-Integrated Control Rooms-Human Factors Issues (HCR-HF) Interim Staff Guidance Rev. 1, November 3, 2008 (ML082740440)

4. NUREG-080-Standard Review Plan (SRP)-Chapter 18, Appendix 18 A, Revision 0, "Guidance for Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analysis," November 20, 2009 (ML092950353)

5. SRM on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced LWR Designs," July 21, 1993 (ML003708056)

6. Digital Instrumentation and Control, DI&C-ISG-04 Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRs) Interim Staff Guidance Rev.1, March 6, 2009 (ML083310185)