UNITED STATES
NUCLEAR REGULATORY
COMMISSION
WASHINGTON, D.C. 20555-0001

December 18, 2020

Matthew W. Sunseri, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: REVIEW OF NUREG-0800, BRANCH TECHNICAL POSITION 7-19, "GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON CAUSE FAILURE DUE TO LATENT DESIGN DEFECTS IN DIGITAL SAFETY SYSTEMS," REVISION 8

Dear Mr. Sunseri:

Thank you for your letter dated November 23, 2020 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML20328A157), about the Advisory Committee on Reactor Safeguards (ACRS) review of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense in Depth and Diversity to Address Common Cause Failure Due to Latent Design Defects in Digital Safety Systems," Revision 8. I appreciate the time and effort the ACRS devoted to this subject, as reflected in meetings held with the ACRS Subcommittee for Digital Instrumentation and Control (DI&C) on September 8, 2020, and the ACRS Full Committee on November 4, 2020.

Your letter contained three conclusions and recommendations; the U.S. Nuclear Regulatory Commission (NRC) staff's responses follow:

Conclusion and Recommendation 1:

BTP 7-19, Revision 8, should be issued subsequent to incorporation of Recommendations 2 and 3.

NRC Staff Response: The staff agrees with this recommendation to the extent described in the responses to Recommendations 2 and 3, below.

Conclusion and Recommendation 2:

Sections A and B.2.1 discuss the combining or integrating of the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) and associated communications architectures into a single protection system. This approach challenges two critical defense-in-depth and diversity (D3) elements, redundancy and independence. The BTP should ensure that reviewers verify these fundamental architecture principles are maintained.

NRC Staff Response: The staff appreciates this recommendation and agrees that redundancy and independence are critical elements of a plant's defense-in-depth posture. In response to the recommendation, the staff revised Section B.2.1 of BTP 7-19, Revision 8, to emphasize to the staff reviewer that reductions in design elements such as independence and redundancy can adversely affect the defense in depth of a plant. The staff also revised the Background section of BTP 7-19, Revision 8, to highlight other design elements (and associated NRC guidance) that can contribute to defense in depth, such as predictable, real-time (deterministic) process and automated self-testing features. (BTP 7-21, "Guidance on Digital Computer Real-Time Performance," and BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," provide guidance for these design elements, respectively.)

Design elements such as redundancy and independence are addressed by requirements and guidance documents that are primarily outside the scope of BTP 7-19, which is focused on the staff's review of a licensee's or applicant's methods to maintain overall plant defense in depth in the presence of a common-cause failure, consistent with the Commission's direction in the staff requirements memorandum, dated July 21, 1993, for SECY-93-087, "SECY-93-087—Policy, Technical, and Licensing Issues pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993. The guidance in BTP 7-19, Revision 8, reflects redundancy and independence requirements and incorporates lessons learned from operating and new reactor reviews that the staff, with ACRS review, has found acceptable (e.g., licensing activities for Oconee Nuclear Station and the design certifications for NuScale and the APR1400).

Conclusion and Recommendation 3:

Section B.2.1 should ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional digital communication devices rather than bi-directional communication devices (which reduce independence and defense-in-depth) to preclude compromise of High Safety-Significance Systems.

NRC Staff Response: The staff appreciates this recommendation and understands the concern that potential connections or communications between systems of higher and lower safety significance pose potential hazards to the systems of high safety significance. However, BTP 7-19, Revision 8, is guidance for staff reviewers and cannot prescribe or impose specific design requirements such as those described in this recommendation. The NRC addresses requirements and guidance that govern the design of interconnections between systems (e.g., to ensure unidirectional

communication) outside of BTP 7-19. The staff revised BTP 7-19, Revision 8, to point to relevant areas of the regulatory infrastructure that pertain to digital communications and control of access, such as Regulatory Guide (RG) 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” and RG 5.71, “Cyber Security Programs for Nuclear Facilities.” RG 1.152 provides guidance on measures to protect against undesirable actions (e.g., tampering with software code or logic) that can compromise the safety system. RG 5.71 provides guidance on protecting digital computers and communications systems and networks against cyber attacks.

The staff appreciates your review of BTP 7-19, Revision 8, and looks forward to future interactions with the ACRS on DI&C topics.

Sincerely,

Ho K. Nieh

Digitally signed by Ho K. Nieh
Date: 2020.12.18 11:01:42 -05'00'

Ho K. Nieh, Director
Office of Nuclear Reactor Regulation

SUBJECT: REVIEW OF NUREG-0800, BRANCH TECHNICAL POSITION 7-19, "GUIDANCE FOR EVALUATION OF DEFENSE IN DEPTH AND DIVERSITY TO ADDRESS COMMON CAUSE FAILURE DUE TO LATENT DESIGN DEFECTS IN DIGITAL SAFETY SYSTEMS," REVISION 8 DATED: DECEMBER 18, 2020

DISTRIBUTION: OEDO-20-00482
PUBLIC
EBenner, NRR
JJohnston, NRR
MWaters, NRR
WMorton, NRR
TGovan, NRR
RidsACRS_MailCTR Resource
RidsOgcMailCenter Resource
RidsNrrDex Resource
RidsNrrOD Resource
SECY

ADAMS Accession No.: ML20345A338 **NRR-106**

OFFICE	NRR/DEX/ELTB	NRR/DRO/IRAB	NRR/DEX/ELTB	NRR/DEX/EICB
NAME	WMorton	TGovan	JJohnston	MWaters
DATE	12/10/2020	12/10/2020	12/10/2020	12/10/2020
OFFICE	QTE	NRR/DEX/D	NRR/D	
NAME	JDougherty	EBenner	HNieh	
DATE	12/14/2020	12/14/2020	12/18/2020	

OFFICIAL RECORD ONLY