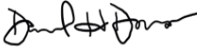




UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 23, 2023

MEMORANDUM TO: Chair Hanson
Commissioner Baran
Commissioner Wright
Commissioner Caputo
Commissioner Crowell

FROM: Daniel H. Dorman  Signed by Dorman, Dan
Executive Director for Operations on 01/23/23

SUBJECT: SUPPLEMENT TO SECY-22-0076, "EXPANSION OF CURRENT
POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN
DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS"

This memorandum supplements SECY-22-0076, "Expansion of Current Policy on Potential Common Cause Failures in Digital Instrumentation and Control Systems," dated August 10, 2022 (Agencywide Documents Access and Management System Accession No. ML22193A290). Subsequent to providing SECY-22-0076, the staff received stakeholder views, including those expressed during public meetings and the Advisory Committee on Reactor Safeguards (ACRS) meetings. Specifically, the views received were on the staff's recommendation regarding the need for independent and diverse displays and manual controls in the main control room in the event of a digital instrumentation and control (I&C) common-cause failure (CCF), as discussed in Point 4 of SECY-22-0076. The purpose of this memorandum is to provide supplemental information as a result of stakeholder views received.

The staff's view is that the policy direction in Point 4 remains essential to providing reasonable assurance of adequate protection for digital I&C systems. Specifically, Point 4 provides what the staff considers to be the minimum level of defense in depth by ensuring operators remain equipped to readily: (1) identify the need for, (2) initiate, and (3) confirm the actuation of critical safety functions, even in the event of a beyond-design-basis CCF in the digital I&C system. The staff acknowledges that current reactor designs provide for manual control capability outside of the control room (e.g., licensees have remote shutdown controls in case of a fire in the control room, and equipment operators can be sent to operate field equipment).

CONTACTS: Samir Darbali, NRR/DEX
301-415-1360

Steven M. Alferink, NRR/DRA
817-200-1548

Bhagwat P. Jain, NRR/DORL
301-415-6303

However, the staff's position is that an adequate level of defense in depth necessitates a minimum set of diverse manual controls to ensure that a digital I&C CCF does not compromise the operators' capability in the control room to place and maintain the plant in a safe and stable condition during or after certain anticipated and unanticipated events. Although the analysis in Points 1–3 may credit some manual actions to cope with the loss of a safety function, Point 4 ensures the capability to manually actuate all critical safety functions. The importance of uncompromised operator control is reinforced by recent events, such as the Boeing 737 Max events.¹ Additionally, in discussing the significance of Point 4 in its November 21, 2022, letter to the Chair (ML22313A101), the ACRS stated that “an ... important principle [of digital I&C design] is providing manual backup means to initiate critical reactor shutdown and safeguards actuation that are not dependent on software.” While the staff agrees with having diverse manual controls, consistent with the Commission direction in SRM-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” dated July 21, 1993 (ML18145A018), the staff's recommendation for Point 4 is not as prescriptive as the language in the ACRS letter in that it does not exclude the use of software-based manual controls as long as they are diverse.

The staff recognizes that industry anticipates the implementation of modern digital control rooms where safety-related indication and control (automatic or manual) are implemented in software-based systems. As such, in developing SECY-22-0076 the staff considered whether Point 4 should be revised to better accommodate modern digital control room designs. The staff concluded that Point 4 already accommodates fully digital control rooms because it is not prescriptive in how the diverse displays and manual controls are implemented (e.g., the diverse displays and manual controls do not have to be hardwired). Although there are regular criteria for the design of manual controls referenced below, Point 4 is risk-informed because it focuses only on those critical safety functions needed to ensure the safety of the facility and because the diverse displays and manual controls do not have to be safety-grade or hardwired. In addition, Point 4 does not require a separate analysis beyond what is required in Points 1–3 of the policy. Therefore, the staff anticipates future fully digital control rooms to provide the displays and manual controls called for by Point 4, in a risk-informed manner (e.g., as have been provided for in the NuScale design and AP1000 design used at Vogtle Electric Generating Plant, Units 3 and 4).

In addition to the supplemental information above, the staff is including a clarification on whether an exemption or alternative is needed if a particular application identifies critical safety functions that are different from those listed in SECY-22-0076 (i.e., reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity). This list is not in the regulations; therefore, an exemption or alternative would not be needed merely because a different set of critical safety functions was identified for a particular reactor design. This also permits licensees and applicants to risk inform what safety functions are defined as critical. An exemption or alternative would only be needed if the proposed displays and manual controls for the design-specific critical safety functions did not comply with the requirements in Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(h) (i.e., Institute of Electrical and Electronics Engineers Standard 279 or Standard 603) or in Appendix B to 10 CFR Part 50, “Criterion 22 - Protection System Independence.”

¹ The introduction section of the U.S. Nuclear Regulatory Commission (NRC) report “Boeing 737 Crashes: Lessons Learned for NRC Digital Instrumentation and Controls Evaluation Process,” dated September 22, 2022 (ML22241A039), explains the 2018 and 2019 Boeing 737 Max events.

This memorandum does not identify any additional commitments to those identified in SECY-22-0076. The Office of the General Counsel reviewed this memorandum and has no legal objection.

cc: SECY
OGC
OCA
OPA
CFO

SUBJECT: SUPPLEMENT TO SECY-22-0076, "EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS" DATED January 23, 2023

DISTRIBUTION: SECY-22-0076-A

Public
 RidsNrrOd
 RidsEdoMailCenter
 RidsOgcMailCenter
 RidsNrrMailCenter
 SDarbali, NRR
 SAlferink, NRR
 BJain, NRR
 SClark, OGC
 DJohnson, OEDO
 TKeene, OEDO

ADAMS Accession No.: ML22357A037

EDO-004

OFFICE	NRR/DORL/PM	NRR/DORL/LA	NRR/DEX/EEEE/BC	NRR/DEX/DD
NAME	MMarshall	KZeleznock	JPaige	EBenner
DATE	12/22/2022	01/12/2023	11/30/2022	11/30/2022
OFFICE	QTE	OGC (NLO)	NRR/D	EDO
NAME	JDougherty	SClark	AVeil (AKock for)	DDorman
DATE	12/29/2022	01/12/2023	01/18/2023	01/ 23 /2023

OFFICIAL RECORD COPY