



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

September 27, 2022

Mr. Daniel H. Dorman
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

**SUBJECT: DRAFT REGULATORY GUIDE 1.250, REVISION 0, DEDICATION OF
COMMERCIAL-GRADE DIGITAL INSTRUMENTATION AND CONTROL ITEMS
FOR USE IN NUCLEAR POWER PLANTS**

Dear Mr. Dorman:

During the 698th meeting of the Advisory Committee on Reactor Safeguards, September 7-9, 2022, we reviewed draft Regulatory Guide (RG) 1.250, Revision 0, "Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants." Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter on July 21, 2022. During this review, we had the benefit of discussions with representatives of the United States Nuclear Regulatory Commission (U.S. NRC) and Nuclear Energy Institute (NEI) staffs. We also had the benefit of the documents referenced.

CONCLUSION AND RECOMMENDATIONS

1. RG 1.250 supplements RG 1.164 and endorses with clarifications NEI 17-06 and the International Electrotechnical Commission (IEC) 61508 standard. Together, they provide sufficient guidance to use Safety Integrity Level (SIL) certification for the dependability assessment portion of the dedication of commercial-grade DI&C items.
2. The staff should ensure applicants have confirmed that SIL-certified programmable electronic devices proposed for use in nuclear power plant safety applications can incorporate architecture and defense-in-depth functionality guidance contained in NRC review documents pertinent to the proposed applications.
3. RG 1.250 should be issued.

D. Dorman

INTRODUCTION

Title 10 of the *Code of Federal Regulations* (10 CFR) Part 21, "Reporting of Defects and Noncompliance," states in part that, "In all cases, the dedication process must be conducted in accordance with 10 CFR Part 50, Appendix B." In support of this requirement, Appendix B to 10 CFR Part 50 provides evaluation and acceptance requirements that are applicable to the dedication of commercial-grade items and services for use in nuclear power plants (NPPs).

Currently, RG 1.164 provides guidance regarding acceptance of commercial-grade dedication of items and services to be used as basic components for NPPs. RG 1.164, Revision 0, endorses Electric Power Research Institute (EPRI) 3002002982, Revision 1, to EPRI NP-5652 and Topical Report (TR)-102260. Specifically, RG 1.164 and EPRI 3002002982 cover the broad scope of dedication of commercial-grade items, while EPRI 3002002982 also references EPRI TR-106439 to provide guidance specific to digital equipment. This TR establishes a process for identifying and verifying critical characteristics for commercial-grade digital equipment.

The translation of design requirements into critical characteristics for a commercial-grade item is a key element in the dedication process. These critical characteristics are generally grouped into three categories for evaluation: physical, performance, and dependability. Dependability becomes significantly more important when dedicating digital equipment including software.

For software-based equipment, in addition to design requirements for the intended functions and anticipated failure modes, it is particularly important to identify requirements related to unused, unintended or prohibited functions, silent failures due to processor lock-up, and failure to complete processing all safety functions within a software operating system timing cycle.

The dependability of a digital device also can be heavily influenced by designed-in elements, including robustness of the hardware and software architectures, self-checking features such as watchdog timers (WDTs), and failure management schemes, such as use of redundant processors with automatic fail-over capabilities.

EPRI TR-106439 contains tables that provide examples of critical characteristics, acceptance criteria, methods of verification, application of methods, and assessment activities for "Built-in Quality" of commercial digital equipment. Verification of these characteristics typically involves a survey of the vendor's processes, and review of the vendor performance records and product operating history.

BACKGROUND

The purpose of RG 1.250, Revision 0, is to describe an alternate approach to meet, in part, regulatory requirements for the dedication of commercial-grade DI&C items for use in NPP safety applications using a third-party certification process. It endorses, with clarifications, NEI 17-06, which provides supplemental guidance on an alternate approach for licensees and applicants to determine acceptability of the dependability critical characteristics of digital equipment during the dedicating process pursuant to 10 CFR Part 21.

NEI 17-06 leverages an internationally recognized SIL certification process that relies on IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems." Before RG 1.250, guidance was not available for accepting a third-party certification

D. Dorman

to support verifying any critical characteristics of digital equipment. This regulatory guide provides guidance on an acceptable method to support verifying a DI&C item's dependability critical characteristics based on an accredited third-party certification of compliance with an IEC 61508 determined SIL in lieu of the TR-106439 verification process that typically involves a commercial-grade survey of the vendor's processes, performance records, and product operating history. The assessment of physical and performance critical characteristics continues to be based on RG 1.164.

The goal of IEC 61508 is for the automatic safety functions to perform their intended functions correctly or for the system to fail in a safe and predictable manner. The standard focuses attention on risk-based safety-related system design and ensures the attention to detail that is vital to safe system design.

Manufacturers of both electronic and programmable electronic equipment for safety applications seek independent, accredited third-party certification in accordance with IEC 61508. This certification verifies key criteria within IEC 61508 demonstrating the reliability goals and the systematic capability specifications for a targeted SIL.

The certifying bodies follow a rigorous process that validates the SIL, provides a certificate of compliance to IEC 61508 criteria, and documents the results of their analysis in the form of a certification report. The certifying body must be accredited by a national accrediting body. In the United States, the currently recognized accrediting body is the American National Standards Institute National Accrediting Board (ANAB). Accrediting bodies around the world are linked under the International Accreditation Forum Multilateral Recognition Arrangement.

Under NEI 17-06, the critical characteristic of dependability described in TR-106439 for commercial-grade dedication of electronic and programmable electronic equipment is verified to determine if the equipment is designed and manufactured to the appropriate SIL level in conformance with IEC 61508. The NRC staff considers SIL certification as described in NEI 17-06 to be a commercial-grade survey for the purposes of 10 CFR Part 21. The certification is performed on a periodic basis. The NRC staff found that the IEC 61508 process has many parallels to the requirements of 10 CFR Part 50, Appendix B. Therefore, the staff concludes that SIL certification by ANAB-accredited certifying bodies is a reliable method to verify the acceptability of the dependability critical characteristics of both electronic and programmable electronic equipment, if dedicated in conformance with RG 1.250, Section C.

DISCUSSION

The use of software-based systems for the Reactor Protection System (RPS) and Engineered Safety Feature Actuation System (ESFAS) introduces new modes of common cause failure (CCF). The operating systems of general-purpose computing platforms are susceptible to corruption by, among other things, unused, unintended or prohibited functions, silent failures due to processor lock-up, and failure to complete processing all safety functions within a software operating system timing cycle.

The primary protection against these types of CCFs is an overall robust RPS and ESFAS with multi-division architecture that meets the fundamental principles of DI&C design: redundancy, redundant division independence, deterministic operating system processing, diversity and defense-in-depth, and control of physical access and external source electronic access.

D. Dorman

One of the RPS and ESFAS key architecture design element is the incorporation of an external hardware based WDT that is independent of the operating system software. The WDT addresses the silent processor lock-up or failure to complete all function processing within its operating system timing cycle.

Both RG 1.164 and the proposed RG 1.250 provide guidance to use commercial-grade dedication of individual industrial-use programmable electronic computer platforms. The commercial-grade dedication certification, in part, is based on their performance in applications other than NPPs. These platforms are typically used in many industrial control systems where their performance can be evaluated as being reliable and dependable over a considerable period of time.

TR-106439 addresses the use of WDTs, including the need for external timers for silent failure detection. Section 6.4, "ESFAS Upgrade Using Programmable Logic Controllers (PLCs)," provides an example of an evaluation of the need for an external WDT for silent failures. It concluded that:

... "such a feature is not required; the internal diagnostics have a high degree of coverage of internal failures, and the implementation of the onboard watchdog timers is sufficiently robust (protects against the failure modes of interest) that these features, combined with the fact that the ESFAS circuits are functionally tested every month and there is manual backup capability, provide adequate protection against such failures."

The example also included a failure analysis considering the possibility of a software related CCF that could disable the redundant PLCs and prevent an automatic actuation of an ESFAS function. The analysis concluded:

"The likelihood of such a failure is considered very low based on the review of the software development process, the successful operating history of the controller in similar applications, knowledge of the device design and failure management provisions, monthly surveillance tests that check functionality of the system, and extensive testing performed by the vendor and the utility/integrator to support the dedication. However, because of the potential safety significance if such a failure were to occur, the utility performs a defense in depth evaluation to determine whether the existing defense in depth (e.g., operator actions using the manual actuation capability) would provide adequate protection for design basis events. The evaluation, using best-estimate methods, concludes that the existing manual capability could be used to adequately mitigate the design basis accidents of concern, with a high degree of confidence."

The TR-106439 conclusions are subjective and premised, in part, on operating system software internal timers being sufficiently robust, monthly tests being performed, device knowledge and vendor integration testing being sufficient, and manual action being available to mitigate consequences.

A major element of defense-in-depth for RPS and ESFAS is an independent multi-division architecture. Division independence is maintained through the inclusion of external hardware WDTs for programmable devices for data processing and voting by detecting lock-up due to software CCF and failure to complete all function processing, as well as independent asynchronous division clock operation. The inclusion of independent asynchronous clocks ensures that division data and voting processing are not set to the same time frame.


D. Dorman

RG 1.250 with NEI 17-06 and IEC 61508 standard, as well as the current RG 1.164, provide sufficient guidance to validate that a third-party SIL certification can be utilized for the dependability assessment of the individual electronic programmable devices. However, they lack sufficient context for application in complex multi-division systems, such as RPS and ESFAS. The context is contained in current NRC review standards and regulatory guides, such as the Standard Review Plan, Design-Specific Review Standard, Interim Staff Guidance DI&C-ISG-06, and Branch Technical Position (BTP) 7-19, which provide architecture and defense-in-depth design principles guidance for multi-division systems.

The staff should ensure applicants confirm that SIL-certified programmable electronic devices proposed for use in NPP safety applications can incorporate architecture and defense-in-depth functionality guidance contained in NRC review documents pertinent to the proposed applications.

RG 1.250 should be issued.

Sincerely,



Signed by Rempe, Joy
on 09/27/22

Joy L. Rempe
Chairman

D. Dorman

REFERENCES

1. U.S. Nuclear Regulatory Commission (NRC), Draft Guide (DG)-1402, Proposed New Regulatory Guide (RG) 1.250, "Dedication of Commercial-Grade Digital I&C Items for Use in Nuclear Power Plants," Revision 0, March 2022, Washington, DC (ML22003A180).
2. U.S. Nuclear Regulatory Commission (NRC), Regulatory Guide (RG) 1.164, "Dedication of Commercial-Grade Items for Use in Nuclear Power Plants," Revision 0, June 2017, Washington, DC (ML17041A206).
3. Nuclear Energy Institute, (NEI) 17-06, "Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications," Revision 1, Washington, DC, December 3, 2021 (ML21337A380).
4. Electric Power Research Institute (EPRI), TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Palo Alto, CA, October 1996.
5. U.S. Nuclear Regulatory Commission, "Safety Evaluation by the Office of Nuclear Reactor Regulation Electric Power Research Institute Topical Report, TR-106439, 'Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications'," July 17, 1997, Washington DC (ML12205A284).
6. International Electrotechnical Commission (IEC), IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems," Edition 2.0, Geneva, Switzerland, April 2010.
7. Electric Power Research Institute (EPRI) 3002002982, "Plant Engineer: Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications: Revision 1 to EPRI NP-5652 and TR-102260," Revision 1, Palo Alto, CA September 22, 2014.
8. NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (<https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/index.html>).
9. NuScale Design Specific Review Standard (DSRS) and Safety Review Matrix, April 2017 (ML17102A698).
10. Design-Specific Review Standard for NuScale Small Modular Reactor Design, December 21, 2015 (ML15355A295).
11. U.S. Nuclear Regulatory Commission, Interim Staff Guidance DI&C-ISG-06, "Licensing Process," Revision 2, December 2018 (ML18269A259).
12. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, "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, January 2021 (ML20339A647).

D. Dorman

September 27, 2022

SUBJECT: DRAFT REGULATORY GUIDE 1.250, REVISION 0, DEDICATION OF
COMMERCIAL-GRADE DIGITAL INSTRUMENTATION AND CONTROL ITEMS
FOR USE IN NUCLEAR POWER PLANTS

Accession No: ML22264A193 Publicly Available (Y/N): Y Sensitive (Y/N): N
If Sensitive, which category?

Viewing Rights: NRC Users or ACRS only or See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	LBurkhart	SMoore (LBurkhart for)	JRempe
DATE	09/21/22	09/21/22	09/21/22	09/23/22	09/27/22

OFFICIAL RECORD COPY