UNITED STATES
NUCLEAR REGULATORY COMMISSION
OFFICE OF NEW REACTORS
OFFICE OF NUCLEAR REACTOR REGULATION
OFFICE OF NUCLEAR MATERIAL SAFETY AND SAFEGUARDS
WASHINGTON, DC 20555-0001

April 29, 2016

NRC REGULATORY ISSUE SUMMARY 2016-05
EMBEDDED DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS

ADDRESSEES

All holders of, and applicants for, licenses for conversion and deconversion fuel cycle facilities under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 40, "Domestic Licensing of Source Material."

All holders of, and applicants for, a power reactor operating license or construction permit under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities," including those that have permanently ceased operations and have spent fuel in storage in the spent fuel pool.

All holders of, and applicants for, a construction permit or an operating license for non-power production or utilization facilities under 10 CFR Part 50, including all existing non-power reactors and proposed facilities for the production of medical radioisotopes, such as molybdenum-99, except those that have permanently ceased operations and have returned all of their fuel to the U.S. Department of Energy.

All holders of, and applicants for, a power reactor combined license, standard design approval, or manufacturing license, and all applicants for a standard design certification, under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

All holders of, and applicants for, licenses for enrichment, fuel fabrication, or mixed-oxide fuel fabrication fuel cycle facilities under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

INTENT

The U.S. Nuclear Regulatory Commission (NRC) is issuing this regulatory issue summary (RIS) to clarify the NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with embedded digital devices (EDDs). This RIS requires no specific action or written response on the part of an addressee.

The NRC's intent in issuing this RIS is to heighten awareness that EDDs might exist in procured equipment used in safety-related systems without the devices having been explicitly identified in

procurement documentation. Inadequate consideration of these devices in digital technology system upgrades, component replacements, and new equipment applications could lead to an adverse safety consequence. Therefore, addressees should implement early efforts to identify these devices.

The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems.

Regulatory issues associated with equipment with EDDs related to common defense and security under 10 CFR Part 73, "Physical Protection of Plants and Materials," and 10 CFR Part 74, "Material Control and Accounting of Special Nuclear Material" are beyond the scope of this RIS.

For clarity, this RIS separately discusses two nuclear facility sectors to address regulatory differences between these two sectors. These nuclear facility sectors are: (1) the nuclear reactor sector, which addresses both power and non-power reactors (also called research and test reactors), and (2) the fuel cycle facility sector. As used in this RIS, the term "non-power reactor" refers to all non-power production and utilization facilities licensed under 10 CFR Part 50 excluding non-power production and utilization facilities that have permanently ceased operations and have returned all of their fuel to the U.S. Department of Energy.

BACKGROUND INFORMATION

Nuclear facilities have increased their use and reliance on digital technology in systems and equipment (e.g., I&C, electrical systems, and fluid systems). In addition to I&C, examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources.

For the purposes of this RIS, an embedded digital device is a component consisting of one or more electronic parts that requires the use of software, software-developed firmware, or software-developed programmable logic, and that is integrated into equipment to implement one or more system safety functions.

The NRC does not accept EDDs as strictly hardware components. EDDs include digital components with executable code or software-developed programmable logic that is permanently or semi-permanently installed within the device (commonly referred to as firmware). Firmware includes, but may not be limited to, devices such as programmable logic devices, field programmable gate arrays, application specific integrated circuits, erasable programmable read only memory, electrically erasable programmable read only memory, and complex programmable logic devices.

The NRC understands that licensees may use digital technology, including equipment and components containing EDDs, with the intent to:

- increase accuracy, speed, and quantity of transmitted data
- reduce operating and maintenance cost, and help with obsolescence issues
- improve equipment reliability, fault detection, and procurement
- add new or additional functionality, especially in the human machine interface

Broad use of safety-related equipment with EDDs also carries potential safety concerns. Concerns include the potential increase in a facility's vulnerability to hazards from undetected EDD defects, potential increase in susceptibility to electromagnetic interference, and other potential hazards from the in-service environment. It is important for licensees and applicants to ensure that the digital technology introduced in nuclear facility safety-related equipment is identified, reviewed, controlled, and evaluated for the potential effects of hardware and software defects in accordance with regulations and guidance applicable for the specific nuclear facility.

Defects in EDDs can include errors other than software programming errors in the code. It also includes a failure of the software and hardware specifications to correctly model the physical environment and functioning of the process. For example, the software programmable logic may perfectly reflect the software specification documents with no programming code error as proven by extensive review and testing, yet when installed, an unconsidered situation may cause the safety equipment to not achieve the required safety function.

Safety-related equipment with EDDs possibly could fail to function as intended because of a latent defect. A condition (referred to as a trigger) usually must occur to reveal the latent defect. For example, in the software or firmware, the trigger must direct the execution through the defective portion of the code or logic to cause a function failure. If a trigger results in a latent software defect causing the failure of multiple functions concurrently within a system, it is a software common cause failure (CCF) within a system. If a trigger results in a latent software defect causing the failure of identical functions in redundant, but otherwise independent systems or channels, it is a software CCF across systems (divisions, trains, or channels).

This RIS identifies regulations and guidance for identifying and eliminating defects. The NRC does not automatically exclude any equipment with EDDs, even those of limited functionality with a well-documented design, from consideration in CCF vulnerability assessments; instead, justification should be supplied by the licensee as applicable for the specific nuclear facility and application.

Despite a quality development process and thorough testing, complexity and other factors such as the inability to detect and remove errors may mean that defect-free EDDs cannot be guaranteed with a reasonable assurance of safety. When this is the case, diversity may become a primary strategy to prevent CCF and support reaching a reasonable assurance of safety. This may be the situation in many commercial equipment units with EDDs, where the development process is either not of the same quality as required by the NRC regulations and recommended by guidance, if applicable, different but equivalent, or unknown.

NRC Information Notice (IN) 1994-20, "Common-Cause Failures Due to Inadequate Design Control and Dedication," describes a CCF incident of an emergency diesel generator load sequencer at Beaver Valley Power Station, Unit 2, after the replacement of electromechanical timer/relays with microprocessor-based timer/relays. This incident occurred before additional guidance (e.g., Electric Power Research Institute Technical Report (EPRI TR)-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," and Nuclear Energy Institute (NEI) 01-01, "Guideline on Licensing Digital Upgrades") was developed to ensure that adequate equipment qualification or commercial grade item dedication is performed on digital components replacing analog components before replacement components are placed in service. Even so, the incident illustrates that a digital replacement can produce a new susceptibility to a CCF. In this case, the commercial grade

dedication that was performed for this component did not adequately represent the in-service environment to demonstrate the replacement component's compatibility with the operating environment.

The NRC issued IN 2007-15, "Effects of Ethernet-Based Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," to alert licensees about the effects on the safety and performance capability of nuclear power plants from potential interactions and unanticipated failures. On August 19, 2006, Browns Ferry Nuclear Plant, Unit 3 operators initiated a manual reactor shutdown following the loss of both reactor recirculation pumps. The root cause investigation determined that the recirculation pump variable frequency drive controllers malfunctioned because of excessive traffic on the plant integrated computer system network. The excessive traffic was likely caused by a faulty programmable logic controller (PLC) in the condensate demineralizer controller on the same network. This was not a failure mode applicable to the technology used when the plant was started up in 1977. However, the new failure mode should have been considered when the PLC and the plant integrated computer system were added as upgrades since initial operation of the plant. This event illustrates that vendors, licensees, and applicants must understand the operation and failure modes of digital systems (including EDDs), and the effects of these failure modes on operations and safety. The failure mode of excessive data rates, which could exceed the capacity of a communications link or the ability of nodes to handle excessive traffic, has also been identified by NRC staff in Digital Instrumentation and Controls (DI&C)-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance [ISG]." DI&C-ISG-04 provides guidance for defensive measures, such as separate communication processors and shared memory that prevents nodes on the communication network from being adversely affected by excessive data rates.

Quality and reliability considerations related to safety significance include potential vulnerabilities resulting from inadequate electromagnetic compatibility (EMC). The EMC established for original equipment may be insufficient to support reliable operation of new equipment with EDDs. Likewise, the EMC characteristics of new equipment with an EDD may be insufficient to support continued reliable operation of nearby unmodified equipment, given its original EMC qualification envelope. Equipment with an EDD should be identified, evaluated, and tested to ensure reliable operation for the in-service environment in accordance with regulations and guidance applicable for the specific nuclear facility.

The regulations identified in each nuclear facility sector provide requirements for the process by which changes to a facility, procedure, or other controlling document may be made without prior NRC approval, except for 10 CFR Part 40 facilities (further discussed in the Fuel Cycle Facility Sector). Records of changes to the facility must be maintained. These records must include a written evaluation that provides the bases for the determination that the change, test, or experiment does not require prior NRC approval. The records of changes to the facility should show that any potential safety issue arising from the use of EDDs has been addressed adequately.

The following sections identify the regulations that apply to the use of equipment with EDDs for the two nuclear facility sectors. The "Summary of Applicable Regulations" provides the complete set of regulations from both sectors. Similarly, each nuclear facility sector identifies applicable guidance documents, and the "Summary of Applicable Staff Guidance" supplies the complete set of guidance from both sectors.

SUMMARY OF ISSUE

The key issue is that the increased use of EDDs in safety-related equipment may increase a facility's vulnerability to a CCF, or otherwise degrade equipment reliability that could adversely affect safety. Potential safety issues from using EDDs should be adequately addressed. This key issue is further summarized by the following three points:

(1) the need to ensure adequate quality and reliability of EDDs that exist in actuation equipment;

(2) the need to address potential facility vulnerabilities to CCFs of equipment with EDDs; and

(3) the need to ensure sufficient procurement planning and material control to identify, review, test, and control EDDs.

Nuclear Reactor Sector

The term "safety-related" as applicable to nuclear power reactors is defined in 10 CFR 50.2, "Definitions," as:

> Safety-related structures, systems and components means those structures, systems and components that are relied upon to remain functional during and following design basis events to assure:
>
> (1) The integrity of the reactor coolant pressure boundary
>
> (2) The capability to shut down the reactor and maintain it in a safe shutdown condition; or
>
> (3) The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11 of this chapter, as applicable.

For non-power reactors, the term "safety-related structures, systems and components," (SSCs) does not apply. For the purposes of this RIS, "safety-related" for non-power reactors refers to the definition of safety-related items used in ANS/ANSI-15.8 (endorsed by the NRC in RG 2.5) as those physical SSCs whose intended functions are to prevent accidents that could cause undue risk to the health and safety of workers and the public, or to the research reactor's programs; and to control or mitigate the consequences of such accidents.

The safety-related I&C in general can be grouped into three categories: (1) the protection systems and associated sense and command features (see Figure 3 of IEEE Std. 603-1991), (2) data communications, and (3) certain other nuclear facility equipment (actuated equipment, execute features, or power sources). The application software and programmable logic in these protection systems and associated sense and command features are usually designed, reviewed, and regulated specifically in accordance with regulations and guidance applicable for the specific type of nuclear facility. In general, the data communication systems and certain other nuclear facility equipment (e.g., motor control centers) and commonly used unit components from the sense and command features (e.g., sensors, transmitters, meters,

indicating units, etc.) may be designed as non-nuclear industry commercial products. However, these commercial products may have a successful operating history outside the nuclear industry that may be useful in helping justify these units for use in nuclear facilities.

Although I&C cabinets and components usually operate in a mild environment, some commercial components may operate in harsh or potentially harsh environments. The one unique difference in the nuclear facilities, such as nuclear power reactors, is the potential for some equipment and components to operate in a radiation environment either normally or during an accident condition. Commercial products intended to operate in a nuclear facility's potentially harsh environment should be qualified to meet the applicable requirements of NRC regulations (e.g., 10 CFR 50.49, for nuclear power plants) and recommendations of guidance regarding environmental qualification, which includes criteria addressing radiation in addition to temperature and humidity extremes.

The 10 CFR 50.59, "Changes, tests, and experiments," rule contains requirements for the process by which licensees may make changes to their facilities and procedures, as described in the facility's Final Safety Analysis Report (FSAR, as updated (UFSAR)), without prior NRC approval.

This RIS applies to equipment, instrumentation, and controls that contain EDDs in safety-related systems for either nuclear power plants or non-power reactors as noted, to address the following:

(1) The need to ensure adequate quality and reliability of EDDs that exist in actuation equipment

Safety-related equipment with EDDs for power reactors must comply with the following regulations, and should address the following guidance to the extent to which these regulations and guidance documents have been invoked, or committed to, in specific sections of the UFSAR, and in other plant specific design and licensing basis documents:

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion (GDC) 1, "Quality Standards and Records"
- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," GDC 21, "Protection System Reliability and Testability"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- 10 CFR 50.55a(h), "Protection and safety systems"
- NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition" (SRP),Chapter 7, "Instrumentation and Controls," (power reactors)
- NUREG-0800, SRP, Chapter 7, Branch Technical Position (BTP), BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems"

Regulations such as 10 CFR Part 21, “Reporting of Defects and Noncompliance” and 10 CFR 50.34(a)(7), which requires a description of the quality assurance program and how requirements of Appendix B will be satisfied, are not included in the above list because they apply to licensees or applicants, not equipment. Nevertheless, licensees should comply with these regulations because they could indirectly result in assuring quality and reliability of equipment with EDDs.

Appendix A and Appendix B of 10 CFR Part 50 are not applicable to non-power reactors. Instead, in 10 CFR 50.34(a)(7), each applicant for a construction permit must include a preliminary safety analysis report with a description of the quality assurance program to be applied to the design, fabrication, construction, and testing of the SSCs of the facility. Regulatory Guide (RG) 2.5 (and by reference ANS/ANSI 15.8) is applicable for new construction and pre-operational quality programs. The RG 2.5 describes a method acceptable to NRC staff for complying with the Commission’s regulations with regard to the overall quality assurance program for non-power reactors. Furthermore, 10 CFR 50.34(b)(6)(ii) requires that each applicant for a license to operate a facility include, in the FSAR, a description of the managerial and administrative controls to be used to ensure safe operation. Managerial and administrative controls for quality are dictated by the Technical Specifications (and licensing conditions, if necessary) once the facility is operational.

Non-power reactors should address the guidance from the following documents that may be useful in assuring quality concerning EDDs that exist in actuation equipment in non-power reactors:

- NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” Part 1, “Format and Content,” February 1996

- NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” Part 2, “Standard Review Plan and Acceptance Criteria,” February 1996

- U.S. Nuclear Regulatory Commission, “Interim Staff Guidance Augmenting NUREG-1537, Part 1, ‘Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Format and Content,’ for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors,” October 2012

- U.S. Nuclear Regulatory Commission, “Interim Staff Guidance Augmenting NUREG-1537, Part 2, ‘Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Standard Review Plan and Acceptance Criteria,’ for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors,” October 2012

- RG 2.5, “Quality Assurance Program Requirements for Research and Test Reactors,” Revision 1, June 2010

Manufacturers are increasingly introducing digital technology into non-actuation and actuation devices that, in turn, are used in applications such as digital displays, motor

controllers, sequencers, pumps, valve actuators, breakers, uninterruptable power supplies, and emergency diesel generator controls. Equipment consisting of commercial grade items with analog and older digital technology is being replaced with commercial grade products containing EDDs that include software, software-developed firmware, or software-developed programmable logic that might not have been developed in accordance with NRC guidance and acceptable industry standards.

(2) The need to address potential vulnerabilities to CCFs

Safety-related equipment with EDDs for power reactors must comply with the following regulations, and should address the following guidance to the extent to which these regulations and guidance documents have been invoked or committed to in specific sections of the UFSAR, and in other plant specific design and licensing basis documents:

- 10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence"
- 10 CFR 50.55a(h), "Protection and safety systems," also incorporates by reference IEEE Std. 603-1991
- NUREG-0800, SRP, Chapter 7, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"
- RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, endorses IEEE Std. 379-2000 without exception.

Applicable regulations, guidance, and industry standards are relied on to assure the safety system sense, and command features supply the logic signals to the safety system execute features. Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD when the same device is used in redundant safety system execute features. Such a defect could, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF).

In addition to the safety-related sense and command features, the guidance in BTP 7-19 is helpful when considering postulated CCFs in systems with components containing EDDs in equipment performing safety-related system execute features.

Non-power reactors should use the following guidance when considering potential CCFs in safety-related equipment with EDDs:

- NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors," Part 1, "Format and Content," February 1996
- NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors," Part 2, "Standard Review Plan and Acceptance Criteria," February 1996

- U.S. Nuclear Regulatory Commission, "Interim Staff Guidance Augmenting NUREG-1537, Part 1, 'Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Format and Content,' for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors," October 2012

- U.S. Nuclear Regulatory Commission, "Interim Staff Guidance Augmenting NUREG-1537, Part 2, 'Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Standard Review Plan and Acceptance Criteria,' for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors," October 2012

- RG 2.5, "Quality Assurance Program Requirements for Research and Test Reactors," Revision 1, June 2010

Research and test reactor licensees can find other useful guidance in the regulatory information developed for power reactor licensees. For example, the guidance developed for power reactors in BTP 7-19 provides helpful information to non-power reactor licensees when evaluating potential CCFs.

(3) The need to ensure sufficient procurement planning and material control to identify, review, test, and control EDDs

Safety-related equipment with EDDs for power reactors must comply with the following regulations and should address the following guidance to the extent to which these regulations and guidance documents have been invoked or committed to in specific sections of the UFSAR, and in other plant specific design and licensing basis documents:

- 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records"

- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"

- EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, Palo Alto, CA, October 1996

- RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 3, July 2011

The regulations in 10 CFR Part 21, "Reporting of Defects and Noncompliance" and 10 CFR 50.34(a)(7), which requires a description of the quality assurance program and how requirements of Appendix B will be satisfied, are not included in the above list because they apply to licensees or applicants, not equipment. Nevertheless, licensees should comply with these regulations because they indirectly support procurement planning and material control of equipment with EDDs.

Licensees should include, as part of their specifications for vendors supplying safety-related and commercial products, requirements to identify the use of EDDs and to sufficiently document the quality of the equipment with EDDs to support commercial grade item dedication per the guidance in EPRI TR-106439, as identified in RG 1.152.

In the early stages of a design, vendors, licensees, and applicants should fully understand the challenges that EDDs may pose. Procurement activities, including commercial grade item dedication processes, should be sufficient to ensure adequate quality and to prevent the introduction of components that could degrade system reliability.

Licensees should ensure vendors of equipment with EDDs document the presence of these devices to alert licensees, so that licensees can adequately consider the issues discussed in this RIS.

Safety-related equipment with EDDs for non-power reactors must comply with the following regulations and should address the following guidance:

- NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors," Part 1, "Format and Content," February 1996

- NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors," Part 2, "Standard Review Plan and Acceptance Criteria," February 1996

- U.S. Nuclear Regulatory Commission, "Interim Staff Guidance Augmenting NUREG-1537, Part 1, 'Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Format and Content,' for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors," October 2012

- U.S. Nuclear Regulatory Commission, "Interim Staff Guidance Augmenting NUREG-1537, Part 2, 'Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors: Standard Review Plan and Acceptance Criteria,' for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors," October 2012

- RG 2.5, "Quality Assurance Program Requirements for Research and Test Reactors," Revision 1, June 2010

The regulation in 10 CFR Part 21, "Reporting of Defects and Noncompliance" that applies to non-power reactors is not included in the above list because it applies to licensees or applicants, not equipment. Nevertheless, licensees should comply with this regulation because it indirectly supports procurement planning and material control of equipment with EDDs.

Fuel Cycle Facility Sector

Fuel cycle facilities (FCFs) may put control systems into place that use digital technology with EDDs. Identification, review, documentation, and control of equipment with EDDs in safety-related systems are necessary to demonstrate the quality and reliability of these systems.

This demonstration should address material control, development processes, and equipment qualification as appropriate to the facility.

For the purpose of this RIS, the term "safety-related" as applicable to FCFs applies to systems, structures, components, procedures and controls (of a facility or a process) that are relied upon to protect the health and safety of workers, the public, and the environment, in accordance with the applicable regulations for the facility and the facility licensing basis documents. Their functionality ensures key regulatory requirements (and license commitments), such as exposures to or levels of radiation, radioactivity, or hazardous chemicals released, are met.

Equipment, instrumentation, and controls that contain EDDs in safety-related systems for FCFs must comply with the following regulations and should address the following guidance, as applicable:

- 10 CFR Part 40, "Domestic Licensing of Source Material," for conversion and deconversion facilities, subject to 10 CFR Part 70, Subpart H, "Additional Requirements for Certain Licensees Authorized to Possess a Critical Mass of Special Nuclear Material," where required by license condition(s) or order

- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," section 70.24, "Criticality accident requirements," section 70.61, "Performance requirements," through section 70.65, "Additional content of applications," for enrichment, fuel fabrication, and mixed-oxide fuel fabrication facilities

- NUREG-1520, "Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility"

- NUREG-1718, "Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility"

- DI&C-ISG-07, "Task Working Group #7: Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities, Interim Staff Guidance"

The regulation in 10 CFR Part 21, "Reporting of Defects and Noncompliance," applies to FCFs, but is not included in the above list (for the purpose of defining "safety-related" as applied to FCFs) because it applies to licensees or applicants, not equipment. Nevertheless, it would be a good practice for licensees to voluntarily comply with this regulation because it supports quality, reliability, procurement planning, and material control of equipment with EDDs.

The provisions in 10 CFR 70.72, "Facility changes and change process," contain requirements for the process by which 10 CFR Part 70 fuel cycle facility licensees may make changes to the site, structures, processes, systems, equipment, components, computer programs, and activities of personnel without prior NRC approval. There are no equivalent regulations for 10 CFR Part 40 facilities. Provisions in 10 CFR 70.72 may be applicable to 10 CFR Part 40 facilities where required by license condition(s) or orders.

Safety-related systems and components that include EDDs must satisfy regulatory requirements, including quality and reliability, commensurate with the safety significance of systems and components. The following regulatory requirements address quality assurance requirements for equipment, instrumentation, and controls that contain EDDs in safety-related systems:

- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants," is applicable to mixed-oxide fuel fabrication facilities and other existing or new FCFs subject to license condition(s) or order

- 10 CFR 70.62(d), "Management measures," and 10 CFR 70.64(a)(1), "Quality standards and records," are applicable to fuel fabrication, mixed-oxide fuel fabrication and enrichment facilities regulated under 10 CFR Part 70

- 10 CFR 70.62(d) and 10 CFR 70.64(a)(1) are applicable to conversion and deconversion facilities regulated under 10 CFR Part 40, where required by license condition(s) or order

Potential safety issues from using EDDs should be adequately addressed. The increased presence of EDDs in commercially procured safety-related components creates a need for heightened awareness by vendors, licensees, and applicants. This heightened awareness is important for new facilities (e.g., initial installation) as well as modernization (e.g., upgraded components at existing facilities), because safety-related systems in these facilities may include commercial equipment with EDDs.

This is further addressed in the following three categories:

(1) The need to ensure adequate quality and reliability of EDDs that exist in actuation equipment

Regulations and review guidance focus on safety-related system control and protection logic rather than the actuated device. Digital technology is being introduced into actuation and actuated equipment. Examples include motor controllers, pumps, valve actuators, breakers, uninterruptible power supplies, and emergency diesel generator controls.

In many instances, equipment consisting of analog and older digital technology is being replaced with commercially procured products containing EDDs that include software, software-developed firmware, or software-developed programmable logic that may not have been developed in accordance with guidance and acceptable industry standards.

(2) The need to address potential vulnerabilities to CCFs

Applicable regulations, guidance, and industry standards are relied upon to ensure the safety system sense and command features supply appropriate logic signals to the safety system execute features. Once the actuation logic signal has been successfully received by the execute features, it may be possible that the intended safety protection could be defeated by an undetected defect within an EDD when the same device is used in redundant safety system execute features. Such a defect may, when triggered concurrently, prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (i.e., a CCF).

The guidance provided in DI&C-ISG-07 is helpful when considering CCFs for digital controls and functions in safety-related applications. The criteria of "independence," "redundancy," and "diversity" are addressed with regard to protecting digital I&C system channels and functions from potential CCFs.

(3) The need to ensure sufficient procurement planning and material control to identify, review, test, and control EDDs

Licensees should include, as part of their specifications for vendors supplying commercial products, requirements to identify the use of EDDs, and to sufficiently document the quality of the EDDs to support the licensee's specific quality verification process (e.g., commercial grade dedication, management measures).

In the early stages of design, vendors, licensees, and applicants should fully understand the challenges that EDDs may pose. Procurement activities, including commercial grade item dedication processes and product testing and inspection, should be sufficient to ensure adequate quality, and to prevent the introduction of components that could degrade system availability and reliability. Where there is a strong reliance on functional testing to verify component quality, performance and reliability, such testing should enable identification of product deficiencies. Licensee monitoring of components with EDDs should support the documentation of item failures to aid in the identification of specific devices and vendors of suspect quality.

SUMMARY OF APPLICABLE NRC REGULATIONS

- 10 CFR Part 40, "Domestic Licensing of Source Material"
- 10 CFR 50.34(a)(7), requires a description of the quality assurance program and how requirements of Appendix B will be satisfied
- 10 CFR 50.34(b)(6)(ii), the final safety analysis report shall describe managerial and administrative controls to be used to assure safe operation
- 10 CFR 50.49, "Environmental qualification of electric equipment important to safety for nuclear power plants"
- 10 CFR 50.55a(h), "Protection and safety systems"
- 10 CFR 50.59, "Changes, tests, and experiments"
- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," including General Design Criterion 1, "Quality Standards and Records," General Design Criterion 21, "Protection System Reliability and Testability," and General Design Criterion 22, "Protection System Independence"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants"
- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," section 70.61, "Performance requirements," through section 70.65, "Additional content of applications"
- 10 CFR 70.24, "Criticality accident requirements"

- 10 CFR 70.62(d), “Management measures”
- 10 CFR 70.64(a)(1), “Quality standards and records”
- 10 CFR 70.72, “Facility changes and change process”
- 10 CFR Part 73, “Physical Protection of Plants and Materials”
- 10 CFR Part 74, “Material Control and Accounting of Special Nuclear Material”

Regulations such as 10 CFR Part 21, “Reporting of Defects and Noncompliance” and 10 CFR 50.34(a)(7), which requires a description of the quality assurance program and how requirements of Appendix B will be satisfied, are not included in the above list because they apply to licenses or applicants, not equipment directly.

SUMMARY OF APPLICABLE NRC GUIDANCE

- Staff Requirements Memorandum SECY 93-087 II.Q, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML003708056)
- RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Revision 3, July 2011 (ADAMS Accession No. ML102870022)
- RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems,” Revision 1, October 2003 (ADAMS Accession No. ML032740277)
- RG 2.5, “Quality Assurance Program Requirements for Research and Test Reactors,” Revision 1, June 2010 (ADAMS Accession No. ML093520099)
- DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc), Interim Staff Guidance,” Revision 1, March 6, 2009 (ADAMS Accession No. ML083310185)
- DI&C-ISG-07, “Task Working Group #7: Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities, Revision 1,” December 1, 2010 (ADAMS Accession No. ML101900316)
- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (SRP), Chapter 7, Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems,” Revision 5, March 2007 (ADAMS Accession No. ML070670183)
- NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition” (SRP), Chapter 7, Branch Technical Position 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” Revision 6, July 2012 (ADAMS Accession No. ML110550791)

- NUREG-1520, Revision 1, “Standard Review Plan for the Review of a Licensee Application for a Fuel Cycle Facility,” May 2010 (ADAMS Accession No. ML101390110)

- NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors;” Part 1, “Format and Content,” February 1996, (ADAMS Accession No. ML042430055)

- NUREG-1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” Part 2, “Standard Review Plan and Acceptance Criteria,” February 1996 (ADAMS Accession No. ML042430048)

- U.S. Nuclear Regulatory Commission, “Interim Staff Guidance Augmenting NUREG 1537, “Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” Part 1, “Format and Content,’ for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors,” October 2012, (ADAMS Accession No. ML12156A069)

- U.S. Nuclear Regulatory Commission, “Interim Staff Guidance Augmenting NUREG-1537, ‘Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors,” Part 2, Standard Review Plan and Acceptance Criteria,’ for Licensing Radioisotope Production Facilities and Aqueous Homogeneous Reactors,” October 2012, (ADAMS Accession No. ML12156A075)

- NUREG-1718, “Standard Review Plan for the Review of an Application for a Mixed Oxide (MOX) Fuel Fabrication Facility,” August 2000 (ADAMS Accession Nos. ML003741461 and ML003741581)

- NRC Safety Evaluation Report, “Review of EPRI Topical Report TR-106439—Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (TAC No. M94127),” July 17, 1997 (ADAMS Accession No. ML092190664)

- NRC Regulatory Issue Summary 2002-22, “Use of EPRI/NEI Joint Task Force Report, “Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule,” November 25, 2002 (ADAMS Accession No. ML023160044)

RELATED INDUSTRY GUIDANCE

- Electric Power Research Institute (EPRI) TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,” October 1996 (ADAMS Accession No. ML103360462)

- Nuclear Energy Institute (NEI) 01-01/EPRI TR-102348, Revision 1, “Guideline on Licensing Digital Upgrades,” March 2002 (ADAMS Accession No. ML020860169)

OTHER RELATED GENERIC COMMUNICATIONS

- NRC Information Notice 1994-20, "Common-Cause Failures Due to Inadequate Design Control and Dedication," March 17, 1994 (ADAMS Accession No. ML031060589)

- NRC Information Notice 2007-15, "Effects of Ethernet-based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," April 17, 2007 (ADAMS Accession No. ML071010303)

- NRC Information Notice 2010-10, "Implementation of a Digital Control System under 10 CFR 50.59,"May 28, 2010 (ADAMS Accession No. ML100080281)

BACKFITTING AND ISSUE FINALITY

This RIS clarifies the NRC's technical position on existing regulatory requirements related to EDDs and heightens awareness that these devices may exist in safety-related systems. The NRC staff position in the RIS does not represent a new or changed position with respect to the need for applicants and licensees to identify, review, document, and control EDDs in safety-related systems to comply with 10 CFR 50.55a(h), "Protection and Safety Systems;" 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants;" 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants;" 10 CFR Part 40; 10 CFR Part 70; and other NRC regulations and guidance as identified above under "Summary of Applicable Regulations," and "Summary of Applicable Staff Guidance." Therefore, this RIS does not represent backfitting, as defined in 10 CFR 50.109(a)(1), or 10 CFR 70.76, nor is it otherwise inconsistent with any issue finality provision in 10 CFR Part 52. Therefore, the NRC did not prepare a backfit analysis for this RIS or further address the issue finality criteria in Part 52.

FEDERAL REGISTER NOTIFICATION

The NRC published a notice of opportunity for public comment on this RIS in the *Federal Register* (78 FR 29392) on May 20, 2013. The Commission received comments from a member of the public, the Pressured Water Reactor Owners Group (PWROG), Nuclear Energy Institute (NEI), Exelon Generation Co., LLC, AREVA, and NRC staff. The staff's resolution of those comments is publicly available under ADAMS Accession No. ML13351A204. The NRC published a notice of opportunity for public comment on the draft revised RIS in the *Federal Register* (79 FR 32578) on June 05, 2014. The Commission received ten sets of comments as identified in the NRC staff's resolution of these comments in a publicly available document under ADAMS Accession No. ML15118A012. This RIS reflects the NRC staff's consideration of these comments.

CONGRESSIONAL REVIEW ACT

The NRC has determined that this RIS is not a rule as designated by the Congressional Review Act (5 U.S.C. §§ 801-808) and, therefore, is not subject to the Act.

PAPERWORK REDUCTION ACT STATEMENT

This RIS contains and references information collection requirements that are subject to the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.). These information collection

requirements were approved by the Office of Management and Budget (OMB), approval numbers 3150-0035, 3150-0020, 3150-0011, 3150-0151, and 3150-0009.

Public Protection Notification

The NRC may not conduct or sponsor, and a person is not required to respond to, a request for information or an information collection requirement unless the requesting document displays a currently valid OMB control number.

CONTACT

Please direct any questions about this matter to the technical contacts listed below or to the appropriate regional office.

/ra/ (AMohseni for)

Lawrence E. Kokajko, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

/ra/ (SHelton for)

Craig G. Erlanger, Acting Director
Division of Fuel Cycle Safety and Safeguards and Environmental Review
Office of Nuclear Material Safety and Safeguards

/ra/

Michael C. Cheok, Director
Division of Construction Inspection
Office of New Reactors

Technical Contacts:

Eugene Eagle, NRR/DE/EICB
301-415-3706
E-mail: Eugene.Eagle@nrc.gov

Duane Hardesty, NRR/DPR/PRLB
301-415-3724
E-mail: Duane.Hardesty@nrc.gov

Samir Darbali, NRR/DE/EICB
301-415-1360
E-mail: Samir.Darbali@nrc.gov

Booma Venkataraman, NRR/DORL/LPL1-1
301-415-2934
E-mail: Booma.Venkataraman@nrc.gov

Ian Jung, RES/DE/ICEEB
301-415-2969
E-mail: Ian.Jung@nrc.gov

Dinesh Taneja, NRO/DE/ICE
301-415-0011
E-mail: Dinesh.Taneja@nrc.gov

Note: NRC generic communications may be found on the NRC public Web site, http://www.nrc.gov, under NRC Library/Document Collections.

CONTACT

Please direct any questions about this matter to the technical contacts listed below or to the appropriate regional office.

/ra/ (AMohseni for)
Lawrence E. Kokajko, Director
Division of Policy and Rulemaking
Office of Nuclear Reactor Regulation

/ra/ (SHelton for)
Craig G. Erlanger, Acting Director
Division of Fuel Cycle Safety and Safeguards and Environmental Review
Office of Nuclear Material Safety and Safeguards

/ra/
Michael C. Cheok, Director
Division of Construction Inspection
Office of New Reactors

Technical Contacts:

Eugene Eagle, NRR/DE/EICB
301-415-3706
E-mail: Eugene.Eagle@nrc.gov

Duane Hardesty, NRR/DPR/PRLB
301-415-3724
E-mail: Duane.Hardesty@nrc.gov

Samir Darbali, NRR/DE/EICB
301-415-1360
E-mail: Samir.Darbali@nrc.gov

Booma Venkataraman, NRR/DORL/LPL1-1
301-415-2934
E-mail: Booma.Venkataraman@nrc.gov

Ian Jung, RES/DE/ICEEB
301-415-2969
E-mail: Ian.Jung@nrc.gov

Dinesh Taneja, NRO/DE/ICE
301-415-0011
E-mail: Dinesh.Taneja@nrc.gov

Note: NRC generic communications may be found on the NRC public Web site, http://www.nrc.gov, under NRC Library/Document Collections.

ADAMS Accession No.: Package: ML15118A011; RIS ML15118A015 *via e-mail TAC No. ME9020

Office	NRR/DE/EICB*	QTE Tech Editor*	RES/DE/ICEEB*	NRO/DE/ICE2*	NRO/DE/ICE2*	NRR/DE/EICB*
Name	EEagle	JDougherty	BDittman	DZhang	DTaneja	SDarbali
Date	05/21/2015	04/23/2015	05/26/2015	05/27/2015	05/26/2015	05/26/2015
Office	RES/DE/ICEEB*	NRR/DPR/PRLB*	NMSS/FCSE/PORSB*	NSIR/CSD	NRO/DE/ICE2/BC	NRR/DE/EICB/BC*
Name	MWaterman	DHardesty	BVenkataraman	ELee	TJackson	JThorp
Date	05/22/2015	05/26/2015	06/19/2015	05/29/2015	06/18/2015	06/24/2015
Office	RES/DE/ICEEB/BC*	NRR/DPR/PRLB/BC*	NMSS/FCS/PORSB/BC*	NSIR/CSD/D*	NRO/DE/D*	NRR/DE/D*
Name	RSydnor	AAdams	MKotzalas	BWestreich	JTappert	JLubinski
Date	06/15/2015	06/02/2015	07/01/2015	07/22/2015	07/09/2015	06/25/2015
Office	RES/DE/D*	NRR/DORL/D*	NRR/PMDA*	OIS*	OE*	OGC/NLO*
Name	BThomas	(GWilson for) LLund	LHill	TDonnell	(CFaria for) NHilton	HBenowitz
Date	07/09/2015	05/27/2015	06/04/2015	06/09/2015	07/20/2015	08/13 /2015
Office	NRR/PGCB/LA	NRR/DPR/PGCB/PM	NRR/DPR/PGCB/BC	NRR/DPR/DD	NRO/DCIP/D	NMSS/FCSE/D
Name	ELee	AGarmoe	SStuchell	AMohseni	MCheok	CErlanger (SHelton w/ edits)
Date	09/29/2015	10/06/2015	10/06/2015	10/20/2015	10/22/2015	4/18/2016
Office	NRR/DPR/D					
Name	LKokajko (AMohseni for)					
Date	4/29/2016					

OFFICIAL RECORD COPY