Gallagher, Carol

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Wednesday, July 02, 2014 11:48 AM
To: Gallagher, Carol
Subject: RE: Comment on the Draft RIS for Embedded Digital Devices
Attachments: 06-09-14_APC_Request for Industry Comments on Draft RIS 2014-## Embedded Digital Devices-RIS_Attachment 2_KS.pdf; COMMENT FORM Draft RIS 2014-## Embedded Digital Devices-Form_KS.doc

Carol,
I am sending my comments to you on the Draft RIS for Embedded Digital Devices in accordance with directions in Federal Register notice: Federal Register / Vol. 79, No. 108 / Thursday, June 5, 2014 / Notices, [NRC-2014-0129], ML13338A769. The PDF file just gives pointers; the comments and suggested changes are in the WORD file.

Thank you for the opportunity to comment.

Ken

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
Phone: 412-612-1192

6/5/2014
79 FR 32578

2

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM-03
Add=
E. Eagle (roe)

Comments on Draft Regulatory Issue Summary 2014-##
"Embedded Digital Devices in Safety-Related Systems" (Docket ID NRC–2014–0129)

By ___ Ken Scarola Nuclear Automation Engineering _____

#	Section, Page, Line #	Comment	Proposed Resolution
1	Page 1, Intent, Second paragraph: The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems. Although this RIS excludes systems that are not safety-related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a nonsafety system that, if inadequately addressed, could adversely affect safety	Saying this RIS excludes systems that are not safety related and then saying this RIS identifies considerations for non-safety is very ambiguous. The RIS provides information only, and that information is pertinent to both safety and non-safety.	This RIS identifies considerations for both safety and non-safety systems. I have only corrected this one sentence. Sentences throughout the document should be changed to address both safety and non-safety systems, as applicable. Alternately, delete all discussion of non-safety applications, and address them in a separate RIS.
2	Page 1, Intent, Second paragraph: For example, a software common cause failure (CCF) in redundant nonsafety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses.	The words "software common cause failure" are being used in correctly. Software defects may result in CCF. "redundant" is an irrelevant attribute. The more important concern is that a design defect may effect multiple non-safety systems. "important to safety" is an undefined term. "beyond the design basis of safety related systems" is confusing when discussing non-safety systems and is irrelevant; the key point is that the condition is not analyzed.	For example, a software defect in one or more nonsafety controllers might create a common cause failure (CCF) of multiple non-safety control functions that has not been analyzed in the nuclear facility's transient and accident analyses. This concern is pertinent to non-safety systems that can directly initiate plant transients. These systems are often referred to as control systems "important to safety"; they are the systems described in Chapter 7 of the plant's UFSAR.

3	Page 2, Third paragraph: Addressees should be aware of any potential vulnerability that could result from a postulated software common-cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices, which includes components implementing safety-related execute features (e.g., motor control centers, actuated equipment)	The use of CCF is incorrect. We postulate a defect, which **may** cause a CCF **if** triggered concurrently in multiple systems. We do not postulate a CCF. The concern is not limited to execute features, it applies also to sense and command features (eg. digital transmitters). Diversity is not the only defense against CCF. Other defenses are addressed below (eg. simplicity, non-concurrent triggers).	Addressees should be aware of any potential CCF of redundant safety related equipment that could result from a postulated software defect within embedded digital devices, which includes components implementing safety-related sense and command or execute features (e.g., instrumentation, motor control centers, actuated equipment)
4	Page 2, fourth paragraph: Inadequate consideration of these devices in diversity assessments to address potential software CCFs could lead to an adverse safety consequence.	We don't do diversity assessments. In accordance with BTP 7-19 we do CCF vulnerability assessments. Diversity is just one defense against CCF; it is not the only defense. Other defenses are addressed below.	Inadequate consideration of these devices in CCF vulnerability assessments could lead to an adverse safety consequence. "assessment of diversity" should be changed to "CCF vulnerability assessment" throughout this document.
5	Page 2, last paragraph: ... that requires the use of software, software-developed firmware, or software-developed logic and that is integrated into equipment to implement one or more system safety functions.	All logic is developed using software, even conventional logic. Clarify applicability to "programmable logic".	... that requires the use of software, software-developed firmware, or software-developed programmable logic that is integrated into equipment to implement one or more system safety functions. "logic" should be changed to "programmable logic" throughout this document.

6	Page 3, Second paragraph: The firmware of an embedded digital device may provide limited functionality with a well-documented design basis such that the embedded digital device could be characterized as "simple."	Defining "simple" as "limited functionality with a well-documented design basis" is quite different than BTP 7-19 which defines "simple" as 100% testable including all combinations of input states and internal states. This will cause confusion in the industry. Add "concurrent triggers" as another consideration. These are all defenses against CCF.	The NRC staff provides guidance applicable to components containing software, firmware, and programmable logic developed from software-based development systems. NRC staff guidance does not automatically exclude the application of these embedded digital devices from consideration within CCF vulnerability assessments. Simplicity, diversity, design documentation, quality development, testing, operational history and the potential for concurrent defect triggers are some of the important factors to be considered within CCF vulnerability analyses to evaluate the suitability for use of an embedded digital device.
7	Page 4, Paragraph 1 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 the 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]."	ISG-04 should be referenced not just to identify the failure mode but to provide guidance for defenses against that failure mode.	The failure mode ... (DI&C)-ISG-04, "Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance [ISG]." ISG-04 provides guidance for defensive measures, such as separate communication processors and shared memory, that prevent nodes on the communication network from being adversely effected by excessive data rates.
8	Page 6, last paragraph; It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function	Again, software CCF is being used incorrectly. This issue is not limited to execute features.	It may be possible that the intended safety protection could be defeated by a CCF of redundant safety divisions caused by a software defect within an embedded digital device, when the same device is used within those redundant divisions and the defect is triggered in multiple divisions. Such a software defect could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (ie. a CCF).

9	Page 6, Item 2 Title The need to address potential vulnerabilities to CCFs	This title implies the CCF will occur, therefore the emphasis is on coping. The emphasis should be on the assessment of the potential for the CCF to occur at all.	The need to conduct a CCF vulnerability assessment.
10	Page 6,Last paragraph It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function.	"software CCF" is used incorrectly. Not limited to execute features. Also, it is not clear what licensees are expected to do. The expectation needs to be well defined.	It may be possible that the intended safety protection could be defeated by a software defect within an embedded digital device when the same device is used within redundant safety system sense and command or execute features. Such a software defect could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function (ie. a CCF). Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered in redundant divisions concurrently (ie. causing a CCF). The CCF vulnerability assessment should also consider defects that may be triggered non-concurrently but remain undetectable; therefore allowing non-concurrent triggering to accumulate in multiple redundant divisions during that same time duration (ie. again, causing a CCF). If a CCF vulnerability is concluded, then licensees should conduct a CCF coping analysis to demonstrate how plant safety is maintained during design basis accidents with the safety system CCF.

11	Page 7, First paragraph Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release)	"beyond design basis of safety-related equipment" is confusing and irrelevant. Again, it is not clear what licensees are expected to do. The expectation needs to be well defined.	Consideration of CCF applies to equipment that is not safety-related to the extent that a software defect could create a transient that is unanalyzed in the plant's accident analysis. Licensees should conduct a CCF vulnerability assessment, considering the likelihood of a software defect and the likelihood that the defect would be triggered for multiple control functions concurrently. For control functions that are in continuous use, the analysis should consider that a triggered defect may be self-announcing. Therefore, the defect may be correctable before it is triggered for multiple control functions (ie. before it causes a CCF of multiple control functions). Therefore, the software defect may be correctable before it causes an unanalyzed transient.

Note: As stated in the Federal Register Notice that released this request: "The NRC cautions you not to include identifying or contact information that you do not want to be publicly disclosed in your comment submission."

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

Month XX, 2014

Draft Revised NRC REGULATORY ISSUE SUMMARY 2014-## 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 reactors or medical isotope production facilities under 10 CFR Part 50, 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, mixed-oxide fuel fabrication fuel cycle facilities under 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material."

All holders of, and applicants for, certificates of compliance for gaseous diffusion enrichment fuel cycle facilities under 10 CFR Part 76, "Certification of Gaseous Diffusion Plants."

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.

The scope of this RIS is limited to equipment, including instrumentation and controls (I&C), in safety-related systems. Although this RIS excludes systems that are not safety-related from its scope, this RIS identifies considerations involving the application of embedded digital devices in a nonsafety system that, if inadequately addressed, could adversely affect safety. For example, a software common cause failure (CCF) in redundant nonsafety equipment with embedded digital devices of an "important to safety" system might create a condition that is beyond the design basis of safety-related systems or a condition that has not been analyzed in the nuclear facility's safety analyses.

ML13338A769

The scope of this RIS excludes embedded digital devices in systems 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." This RIS does not address the cyber security regulation provided in 10 CFR Part 73.54, "Protection of Digital Computer and Communication Systems."

This RIS reminds addressees of the need to identify, review, document, and control equipment with embedded digital devices in safety-related systems to comply with applicable regulations for the nuclear facility. For clarity, this RIS separately discusses two nuclear facility sectors to address regulatory differences. These nuclear facility sectors are: (1) the nuclear reactor sector, which addresses both power and non-power reactors, and (2) the fuel cycle facility sector.

Identification, review, documentation, and control of safety-related equipment with embedded digital devices are necessary to demonstrate quality and reliability. This demonstration should address material control, development processes, and equipment qualification. Addressees should be aware of any potential vulnerability that could result from a postulated software common-cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices, which includes components implementing safety-related execute features (e.g., motor control centers, actuated equipment).

The NRC's intent in issuing this RIS is to heighten awareness that embedded digital devices may 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 diversity assessments to address potential software CCFs could lead to an adverse safety consequence. Therefore, addressees should implement early efforts to identify these devices.

The following sections identify the regulations that apply to the use of equipment containing embedded digital devices 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" provides the complete set of guidance from both sectors.

This RIS requires no specific action or written response on the part of an addressee.

BACKGROUND INFORMATION

Nuclear facilities have increased the use and reliance on digital technology in systems and equipment (e.g., I&C, electrical systems, and fluid systems). The use of digital technology may reduce operating and maintenance costs, improve equipment reliability, and enhance overall safety. Examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, and uninterruptible power sources. It is important for licensees and applicants to ensure that the digital technology introduced in nuclear facility safety-related equipment is identified, reviewed, and controlled.

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 logic and that is integrated into equipment to implement one or more system safety functions.

The NRC guidance (e.g., Branch Technical Position (BTP) 7-19 Revision 6) does not accept embedded digital devices as strictly hardware components. Embedded digital devices include digital components with executable code or software-developed logic that is permanent or semi-permanently installed within the device (commonly referred to as firmware). Firmware includes devices such as programmable logic devices (PLDs), field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), erasable programmable read-only memory (EPROMs), electrically erasable programmable read-only memory (EEPROMs), and complex programmable logic devices (CPLDs).

The NRC staff provides guidance applicable to components containing software, firmware, and logic developed from software-based development systems. The firmware of an embedded digital device may provide limited functionality with a well-documented design basis such that the embedded digital device could be characterized as "simple." However, NRC staff guidance does not automatically exclude the application of these (so-called "simple") devices containing the firmware from consideration within an assessment of diversity to evaluate and address vulnerabilities to potential CCF. Nevertheless, simplicity, diversity, design documentation, quality development, testing, and operational history are some of the important factors to be considered within analyses to evaluate the suitability for use of an embedded digital device.

NRC Information Notice (IN) 1994-020, "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, following the replacement of electromechanical timer/relays with microprocessor-based timer/relays. This incident occurred before additional guidance (e.g., Electric Power Research Institute topical 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 a digital component replacing an analog component before the replacement component is put into 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 inservice environment to demonstrate the replacement component's compatibility.

The NRC issued IN 2007-015, "Effects of Ethernet-Based Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," to alert licensees about the effects of potential interactions and unanticipated failures of Ethernet-connected nonsafety equipment on the safety and performance capability of nuclear power plants. 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 embedded digital

devices) 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 the 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]."

Safety-related systems, equipment, instrumentation, and controls that include components with embedded digital devices must satisfy regulatory requirements, including quality and reliability, consistent with the safety significance of the equipment. Quality and reliability considerations related to safety significance include potential vulnerabilities to CCFs and electromagnetic compatibility (EMC). The EMC established for original equipment may be insufficient to support reliable operation of new equipment containing an embedded digital device. Likewise, the EMC characteristics of new equipment containing an embedded digital device may be insufficient to support continued reliable operation of nearby unmodified equipment, given its original EMC qualification envelope. In both cases, equipment containing an embedded digital device should be identified, evaluated, and tested to ensure reliable operation for the inservice environment.

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 from the use of embedded digital devices has been adequately addressed.

SUMMARY OF ISSUE

The key issue is that the increased use of embedded digital devices in safety-related equipment may increase a facility's vulnerability to a CCF, challenge equipment EMC, or otherwise degrade equipment reliability to adversely affect safety. Potential safety issues from using embedded digital devices 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 embedded digital devices that exist in actuation equipment;

(2) the need to address potential facility vulnerabilities to CCFs; and

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

Nuclear Reactor Sector

The term "safety-related" as applicable to nuclear 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.

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), without prior NRC approval.

This RIS applies to equipment, instrumentation, and controls that contain embedded digital devices in safety-related systems for nuclear power plants and non-power reactors in order to address the following:

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

Safety-related equipment with embedded digital devices must comply with the following regulations and should address the following guidance, as applicable:

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criterion 1, "Quality Standards and Records"
- 10 CFR Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
- 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 50.55a(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"
- 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

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

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

Equipment consisting of commercial grade items with older non-digital technology is being replaced with commercial grade products containing embedded digital devices that include software, software-developed firmware, or software-developed logic that may not have been developed in accordance with guidance and acceptable industry standards.

(2) <u>The need to address potential vulnerabilities to CCFs</u>

Safety-related equipment with embedded digital devices must comply with the following regulations and should address the following guidance, as applicable:

- 10 CFR Part 50, Appendix A, General Design Criterion 22, "Protection System Independence"

- 10 CFR 50.55a(h), "Protection and Safety Systems"

- 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"

Applicable regulations, guidance, and industry standards are relied on to assure the safety system sense and command features provide the logic signals to the safety system execute features. It may be possible that the intended safety protection could be defeated by a software CCF of an embedded digital device when the same device is used within redundant safety system execute features. Such a software CCF could prevent more than one train of otherwise independent redundant equipment from accomplishing the intended safety function.

Consideration of CCF applies to equipment that is not safety-related to the extent that a CCF could create a condition that is beyond the design basis of safety-related equipment (i.e., when the results of the CCF are not bounded by the facility design-basis accident analysis and a safety vulnerability results with respect to a radiological release).

The guidance in BTP 7-19 is helpful when considering potential CCFs of embedded digital devices located in equipment performing safety-related system execute features.

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

Safety-related equipment with embedded digital devices must comply with the following regulations and should address the following guidance, as applicable:

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 10 CFR Part 50, Appendix A, General Design Criterion 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
- RG 2.5, "Quality Assurance Program Requirements for Research and Test Reactors," Revision 1, June 2010

Licensees should include, as part of their specifications for vendors supplying commercial products, requirements to identify the use of embedded digital devices and to sufficiently document the quality of the embedded digital devices to support commercial grade item dedication per the guidance in EPRI TR-106439, as identified in RG 1.152, Revision 3, July 2011.

In the early stages of a design, vendors, licensees, and applicants should fully understand the challenges that embedded digital devices 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 items containing embedded digital devices document the presence of these devices to alert licensees, so that the licensees can adequately consider the issues discussed in this RIS.

Fuel Cycle Facility Sector

Fuel cycle facilities (FCFs) may implement control systems that make use of digital technology with embedded digital devices. Identification, review, documentation, and control of equipment in safety-related systems with embedded digital devices 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. Their functionality ensures key regulatory requirements (and license commitments), such as exposures to or levels of radiation, radioactivity, or hazardous chemicals released, are met.

This RIS applies to equipment, instrumentation, and controls that contain embedded digital devices in safety-related systems for FCFs to comply with the following regulations and address the following guidance, as applicable:

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 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," paragraph 70.24, "Criticality Accident Requirements," paragraphs 70.61, "Performance Requirements," through 70.65, "Additional Content of Applications," for enrichment, fuel fabrication, and mixed-oxide fuel fabrication facilities
- 10 CFR 76.87, "Technical Safety Requirements," and 10 CFR 76.89, "Criticality Accident Requirements," for gaseous diffusion fuel cycle 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 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. The provisions in 10 CFR 76.68, "Plant Changes," contain requirements for the process by which 10 CFR Part 76 certificate holders may make changes to the plant or the plant's operations without prior Commission 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 order.

Safety-related systems and components that include embedded digital devices 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 embedded digital devices in safety-related systems:

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 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.
- 10 CFR 76.93, "Quality Assurance," is applicable to gaseous diffusion facilities.

Potential safety issues from using embedded digital devices should be adequately addressed. The increased presence of embedded digital devices 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 embedded digital devices.

This is further addressed in the following three categories:

(1) <u>The need to ensure adequate quality and reliability of embedded digital devices that exist in actuation equipment</u>

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 (if applicable).

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

(2) <u>The need to address potential vulnerabilities to CCFs</u>

Applicable regulations, guidance, and industry standards are relied on to assure the safety system sense and command features provide the logic signals to the safety system execute features. It may be possible that the intended safety protection could be

defeated by an undetected error in the software or software-developed logic in embedded digital devices within these redundant safety system execute features that could prevent accomplishment of their intended safety function.

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 for the protection of 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 embedded digital devices

Licensees should include, as part of their specifications for vendors supplying commercial products, requirements to identify the use of embedded digital devices and to sufficiently document the quality of the embedded digital devices 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 embedded digital devices 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 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 embedded digital devices should support the documentation of item failures in order to aid in the identification of specific devices and vendors of suspect quality.

SUMMARY OF APPLICABLE REGULATIONS

- 10 CFR Part 21, "Reporting of Defects and Noncompliance"
- 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 50.55a(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," 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 70.24, "Criticality Accident Requirements"
- 10 CFR Part 70, "Domestic Licensing of Special Nuclear Material," paragraphs 70.61, "Performance Requirements," through 70.65, "Additional Content of Applications"
- 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"
- 10 CFR 76.68, "Plant Changes"
- 10 CFR 76.87, "Technical Safety Requirements"
- 10 CFR 76.89, "Criticality Accident Requirements"
- 10 CFR 76.93, "Quality Assurance"

SUMMARY OF APPLICABLE STAFF GUIDANCE

- Staff Requirements Memorandum SECY 93-087 II.Q, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" April 2, 1993 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML003708056)
- Regulatory Guide (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 1994-020, "Common-Cause Failures Due to Inadequate Design Control and Dedication," March 17, 1994 (ADAMS Accession No. ML031060589)

- NRC Information Notice 2007-015, "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 2010-010, "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 embedded digital devices 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 embedded digital devices in safety-related systems in order 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; 10 CFR Part 76; 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), 10 CFR 70.76, or 10 CFR 76.76; 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 an individual member of the public, the Pressured Water Reactor Owners Group (PWROG), Nuclear Energy Institute (NEI), Exelon Generation Company, LLC, AREVA, and an internal comment set. This draft revised RIS reflects the NRC staff's consideration of these comments. The staff's resolution of these comments is publicly available under ADAMS Accession No. ML13351A204.

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.

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

Marissa G. Bailey, Director
Division of Fuel Cycle Safety and Safeguards
Office of Nuclear Material Safety and Safeguards

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

Larry W. Camper, Director
Division of Waste Management
and Environmental Protection
Office of Federal and State Materials
and Environmental Management Programs

Technical Contacts:
Ian Jung, NRO/DE/ICE2
301-415-2969
E-mail: Ian.Jung@nrc.gov

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

Eugene Eagle, NRO/DE/ICE2
301-415-3706
E-mail: Eugene.Eagle@nrc.gov

Booma Venkataraman, NMSS/FCSS/PORSB
301-287-9143
E-mail: Booma.Venkataraman@nrc.gov

Bernard Dittman, RES/DE/ICEEB
301-251-7494
E-mail: Bernard.Dittman@nrc.gov

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