From:	Govan, Tekia
To:	Govan, Tekia
Subject:	FW: Follow-up to January 31st Meeting on Digital I&C
Date:	Thursday, March 28, 2019 11:18:23 AM
Attachments:	image001.png SunPort Paper - Alternative Software Development Standards - Updated.pdf SunPort Paper - Technical Guidance for Digital I&C Components with Limited Functionality - Updated.pdf SunPort Paper - Technical Guidance for I&C System Architectures - Updated.pdf SunPort Paper - Update SRM-SECY-93-087 and Associated Regulatory Guidance -Updated.pdf IEC 61226 Excerpt.pdf

---

From: Zhang, Deanna
Sent: Tuesday, February 05, 2019 1:18 PM
To: Govan, Tekia <Tekia.Govan@nrc.gov>
Cc: Morton, Wendell <Wendell.Morton@nrc.gov>
Subject: FW: Follow-up to January 31st Meeting on Digital I&C

Tekia,

This is the email I received from Mark last week.
Thanks.

Deanna Zhang
Senior Electronics Engineer
Office of Nuclear Reactor Regulations
U.S. Nuclear Regulatory Commission
OWFN-8D18
(w) 301.415.1946

From: Mark Burzynski [mailto:m.burzynski@sunport.ch]
Sent: Thursday, January 31, 2019 6:28 PM
To: Zhang, Deanna <Deanna.Zhang@nrc.gov>
Subject: [External_Sender] Follow-up to January 31st Meeting on Digital I&C

Dear Deanna,

I appreciate the spirit you conveyed during your presentation on the Introduction of the IEC Endorsement Project. As you know, I have had a strong interest in the topic. I prepared some talking point papers on opportunities to modernize the digital I&C regulatory framework. I updated some of the papers based on what I heard during the meeting today. I have attached the updated papers for your consideration. I think there is a place now to target certain IEC standards for endorsement to help address known gaps in guidance for protection system architecture design, FPGA development process quality requirements, and evaluation of limited functionality digital devices in the commercial grade dedication process. I also think the IEC standards also can provide a practical alternative for software development process quality requirements. The attached papers address these topics and how one could use the IEC standards to address these needs. I think that NRC endorsement of the relevant portions of the IEC standards would not conflict with any other

modernization efforts. I would see IEC 61513 providing process guidance for the development of system architectures, which would capture the local regulatory requirements (i.e., IEEE Std 603) as an input to the system requirements development. I would not see the technical requirements in IEC 61513 used as an alternative to the technical requirements in IEEE Std 603.

I am interested in supporting this effort and would like to discuss how I could participate.

As a small comment on the presentation, I see IEC 62340 as applicable only to Category A functions. In clause 1.a it says: The scope of this standard is to give requirements related to the avoidance of CCF of I&C systems that perform
category A functions. This applicability is also reflected in IEC 61226 (see attached excerpt).

Regards,

Mark J. Burzynski
CHIEF EXECUTIVE OFFICER

Tel: +1 (423) 834-4455
Email: m.burzynski@sunport.ch
www.sunport.ch

logo

Alternative Software Development Standards for Safety-Related Systems and Components

Background

The IEEE software development standards currently endorsed for use in the design of safety-related systems were not developed specifically for the nuclear industry but endorsed by NRC for safety-related systems. The software development process standards are the source of problems, unnecessary burden, or regulatory review delays. Additional flexibility is needed in this area to better focus NRC reviews on the software development process elements with a true nexus to safety to improve efficiency, effectiveness, and consistency.

Existing NRC Guidance

The NRC review guidance for software development for safety-related systems are found in six Regulatory Guides (RGs) that endorse various IEEE Standards

RG 1.168, Revision 2, *Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1012-2004, *IEEE Standard for Software Verification and Validation Plans*, and IEEE Std 1028-2008, *IEEE Standard for Software Reviews and Audits.*

RG 1.169, Revision 1, *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 828-2005, *IEEE Standard for Software Configuration Management Plans*.

RG 1.170, Revision 1, *Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 829-2008, *IEEE Standard for Software Test Documentation*.

RG 1.171, Revision 1, *Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1008-1987, *IEEE Standard for Software Unit Testing*.

RG 1.172, Revision 1, *Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 830-1998, *IEEE Recommended Practice for Software Requirements Specifications*.

RG 1.173, Revision 1, *Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, endorses IEEE Std 1074-2006, *IEEE Standard for Developing Software Life Cycle Processes*.

These standards are characterized by hundreds of mandatory process requirements that range from important tasks (e.g., perform validation testing) to those with little to no nexus to safety (e.g., format of test documents).[1] The regulatory reviews focus on the degree of conformance to these many mandatory requirements and the justification for areas where conformance is not achieved.

The IEEE Standards endorsed by NRC for nuclear safety-related software are fragmented, incomplete, and not current with technology.

Available Industry Guidance

IAEA Specific Safety Guide No. 39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, provides guidance on software development for safety-related I&C systems (see Sections 9.1 through 9.95). It provides guidance on I&C architecture design principles and the proper application of independence within the overall I&C architecture to prevent the propagation of failures between systems.

The IEC standards for software development for safety-critical applications provide better guidance for nuclear digital I&C applications (i.e., holistic organization, integrated guidance, and technologically relevant).

- IEC 61513, *Nuclear power plants - Instrumentation and control important to safety - General requirements for systems*
- IEC 60880, *Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions*
- IEC 62566, *Nuclear power plants - Instrumentation and control important to safety - Development of HDL-programmed integrated circuits for systems performing category A functions*
- IEC 62138, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*
- IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*[2]

These standards are the ones most commonly used by digital equipment vendors servicing the nuclear sector. They are maintained to reflect changes in technology and are practical because they are widely used. They each contain process requirement for the development of safety-critical software.

IEC 61513 contains system-level develop process level requirements for system requirements development, system architecture design, allocation of requirements to hardware and software, system integration, and system validation. IEC 60880 then defines the requirements for software development from requirements through implementation. It also identified software specific aspects of system integration and validation to be used with IEC 61513 for these phases of the process. IEC 62566 augments IEC 60880 for programmable logic devices technology (e.g., FPGA). It also identified software specific aspects of system integration and validation to be used with IEC 61513 for these phases of the process. The relevant software development requirements from these standards (see Appendix) provide holistic and robust software

[1] For a perspective of the nature of the process standards, look at IEEE Stds 829, 1012, and 1028 to get a good sense of the software process standards and contrast them with technical standard IEEE Std 603.

[2] This is a sector-independent standard used for safety-critical applications.

development process for safety-related systems that should be accepted as an alternative to the regulatory guidance currently provided in RG 1.168 through 1.173. It is not expected that the IEC set must be shown to be equivalent to the IEEE set. NRC endorsement of the relevant portions of these standards should be tailored to address the software development process requirements and not other technical requirements that are outside the development process scope of the RGs.

IEC 62138 provides software development process requirements for lower classified systems. It should be considered as another alternative that could be used for lower safety significance equipment discussed in RIS 2002-22, Supplement 1, *Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems*.

IEC 61508 also contains a set of software development process requirements for a full system development life cycle. The standard uses a graded approach. The software development requirements specified for safety integrity level 3 provide holistic and robust software development process that should be accepted as another alternative for safety-related systems to the regulatory guidance currently provided in RG 1.168 through 1.173. It is not expected that the IEC set must be shown to be equivalent to the IEEE set. The software development requirements specified for safety integrity level 2 should be considered as another alternative that could be used for lower safety significance equipment discussed in RIS 2002-22, Supplement 1.

Objective

The goal is to broaden the regulatory toolbox for acceptable software development requirements for safety-related systems. It would provide practical alternatives based on commonly used standards, allow for using the right tool for the right job in a graded way, and align with a broader set of vendor practices.

Recommendations

1. NRC should build on the work done in the international nuclear community related to the software development for safety-related I&C systems.

2. NRC should build on the work it has already done in support of the Multinational Design Evaluation Programme (MDEP) development of Generic Common Position for important digital I&C issues. Relevant work related to software development for safety-related I&C systems can be found in Generic Common Position DICWG-03, *Common Position on Verification and Validation Throughout the Life Cycle of Digital Safety Systems*, and Generic Common Position DICWG-05, *Common Position on the Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems.*

3. NRC should endorse the IEC standards associated with safety-related software development as an alternative to the IEEE software development standards currently endorsed for use in the design of safety-related systems. This action does not require any rulemaking to implement.

4. NRC could also introduce additional flexibility by revising the RG endorsements for the IEEE Standards for safety-related software development by focusing only on those requirements with a true nexus to safety. This action does not require any rulemaking to implement.

Appendix - Software Development Process – IEEE and IEC Approaches

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 1074-2006	Software Lifecycle (RG 1.173)	IEC 61513 Section 6 (system lifecycle)
		IEC 60880 (software lifecycle)
		IEC 62566 (FPGA lifecycle)
IEEE Std 1074-2006 (Section A.1.2)	Software Development Planning (BTP 7-14 Section B.3.1)	IEC 61513 Section 5.5 (overall I&C planning) IEC 61513 Section 6.3 (individual system planning)
		IEC 60880 Sections 5.4 (software project management) and 5.5 (software quality assurance)
		IEC 62566 Sections 5.3 (FPGA project management) and 5.4 (FPGA quality assurance)
-	Secure Development and Operating Environment (RG 1.152)	IEC 61513 Section 5.5.3 (overall I&C security plan) IEC 61513 Section 6.3.3 (Individual system security plan)
		IEC 60880 Section 5.7 (software security)
-	System Architecture	IEC 61513 Sections 5.2, 5.3 (documentation), 5.4, and 5.6 (overall architecture) and 6.2.2.3.2 (system architecture)
-	System Requirements	IEC 61513 Sections 6.2.2 (requirements) and 6.4.2 (documentation)

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 828-2005	Software Configuration Management (RG 1.169)	IEC 61513 Section 6.3.2.3 (system configuration management plan) IEC 60880 Section 5.6 (software configuration management)
		IEC 60880 Section 5.6 (software configuration management)
		IEC 62566 Section 5.5 (FPGA configuration management)
IEEE Std 830-1998	Software Requirements Specification (RG 1.172)	IEC 61513 Section 6.2.3.4 (software requirements specification)
		IEC 60880 Section 6 (software requirements specification)
		IEC 62566 Section 6 (FPGA requirements specification)
IEEE Std 1012-2004	Software Verification and Validation (RG 1.168)	IEC 61513 Sections 6.4.2.3, 6.4.3.3, 6.4.4.4, 6.4.5.3, 6.4.6.3, and 6.4.7.3 (system verification) IEC 61513 Sections 6.2.5 (system integration) and 6.2.6 (system validation)
		IEC 60880 Section 8 (software verification) IEC 60880 Section 10 (software aspects of system integration) IEC 60880 Section 11 (software aspects of system validation)
		IEC 62566 Section 9 (FPGA verification) IEC 62566 Section 10 (FPGA aspects of system integration) IEC 62566 Section 11 (FPGA aspects of system validation)

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 1008-1987	Software Unit Testing (RG 1.171)	IEC 60880 Sections 8.2.3.1.1.3 and 8.2.3.1.1.4
		IEC 62566 Sections 9.5, 9.6, and 9.7
IEEE Std 829-2008	Software Test Documentation (RG 1.170)	IEC 61513 Sections 6.4.5 (system integration documentation), 6.4.6 (system validation documentation)
		IEC 60880 Sections 8.2.3.1.1.5, 8.2.3.1.2, and 8.2.3.1.3
		IEC 62566 Sections 9.2.6, 10.6, and 11.4

Technical Guidance for Digital I&C Components with Limited Functionality

Background

The nuclear power industry is increasingly interested in using industrial digital devices of limited functionality (also known as 'smart' devices) in systems important to safety but that have not been developed specifically for use in nuclear power applications. These devices should meet certain specific requirements in order to be selected and used in systems important to safety at nuclear power plants. Typically, some of these devices are found embedded in plant components and actuating devices (e.g., sensing instrumentation, motors, pumps, actuators, breakers, etc.).

Many of the replacement I&C devices now are only available in the commercial market (due to the loss of nuclear safety-related suppliers in the US). NRC has not issued any technical guidance to safety implement digital components with limited functionality. Practical technical guidance is needed to ensure that digital components with limited functionality can be consistently implemented over time with minimal regulatory uncertainty.

Existing NRC Guidance

Limited guidance exists to support the selection and use of industrial digital devices of limited functionality in safety-related systems.

NRC Regulatory Issue Summary (RIS) 2016-05, *Embedded Digital Devices in Safety-Related Systems*, alerts the industry that modern components (e.g., digital displays, motor controllers, sequencers, pumps, valve actuators, breakers, uninterruptable power supplies, etc.) now contain embedded digital devices. RIS 2016-05 does not provide any recommended solutions; instead, it simply reiterates that the existing NRC guidance for digital I&C equipment applies.

RIS 2002-22, Supplement 1, *Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems*, resolves some of the regulatory problems (i.e., 10 CFR 50.59 evaluations) associated with implementing digital-based equipment with lower safety significance (where limited functionality devices would typically be considered). RIS 2002-22, Supplement 1, discusses the need to address various technical attributes but only provides some examples to consider in a technical evaluation.

The NRC-approved guidance for commercial grade dedication of digital I&C equipment (i.e., EPRI TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications*, defines an effective process for dedication of commercial grade items. It specifies that critical characteristics need to be defined and evaluated for physical, performance, and dependability attributes and provides some examples. EPRI TR-106439 does not provide technical guidance relevant to digital components with limited functionality.

Regulation through information-only documents does not provide durable technical guidance that can be consistently implement over time. Better and consistent NRC guidance for the commercial grade dedication evaluation and use of digital components with limited functionality would ensure consistency in the technical evaluation and regulatory acceptance.

Available Industry Guidance

IAEA Specific Safety Guide No. 39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, provides guidance on the qualification of industrial digital devices of limited functionality that are to be used in nuclear power plant safety systems but that have not been developed specifically for use in such applications (see Sections 7.165 through 7.175). It provides guidance on:

- Confirmation that devices are suitable for intended functions and designed correctly;
- Use of compensatory evidence to address identified gaps in evidence;
- Use of third-party certification as evidence; and
- Specification of restrictions on use.

IEC 62671, *Nuclear Power Plants – I&C Important to Safety – Selection and Use of industrial Digital Devices of Limited Functionality*, provides requirements for determining whether digital devices of industrial quality (that are of dedicated, limited, and specific functionality and of limited configurability), are suitable for use in a nuclear application. It provides guidance on:

- Section 6 provides criteria for functional and performance suitability;
- Section 7 provides criteria for dependability – evidence of correctness;
- Section 8 provides criteria for integration into the application (i.e., limits and conditions of use); and
- Section 9 provides considerations for preserving acceptability.

Objective

The goal is to broaden the regulatory toolbox for acceptable commercial grade equipment. EPRI TR-106439 would be retained a general purpose guidance document for commercial grade dedication of digital I&C equipment. EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*, would be retained as an alternative for commercial grade dedication of digital I&C platforms. IEC 62671 would be available as an alternative to EPRI TR-106439 for a subset of digital devices of industrial quality that are of dedicated, limited, and specific functionality and of limited configurability). The ongoing work for NRC's DI&C Integrated Action Plan Modernization Plan #3 will provide options to simplify the use of EPRI TR-106439 and IEC 62671 with respect to evaluation of dependability characteristics. These actions would provide practical alternatives based on commonly used standards, allow for using the right tool for the right job in a graded way, and align with a broader set of vendor practices.

Recommendations

1. NRC should endorse relevant industry standards associated with the selection and use of industrial digital devices of limited functionality.

2. NRC should build on the work it has already done in support of the Multinational Design Evaluation Programme (MDEP) development of Generic Common Position for important digital I&C issues. Relevant work related to digital components with limited functionality can be found in Generic Common Position DICWG-07, *Common Position on Selection and Use of Industrial Digital Devices of Limited Functionality*. The common positions in DICWG-07 address these topics:

    - Confirmation that devices are suitable for intended functions and designed correctly;
    - Use of compensatory evidence to address identified gaps in evidence;
    - Use of third-party certification as evidence; and
    - Specification of restrictions on use.

3. It seems practical that NRC could endorse IEC 62671 based on the MDEP work, which would provide U.S. licensees with useful guidance selection and use of industrial digital devices of limited functionality that is in alignment with the applicable IAEA safety guidance.

Technical Guidance for I&C System Architectures

Background

System architecture issues have complicated digital I&C retrofit projects at both Oconee and Diablo Canyon. Existing NRC regulatory guidance does not directly address system architectures and associated areas of regulatory concern that were evident in the Oconee and Diablo Canyon reviews.

The fundamental regulatory challenge posed by "highly-integrated" I&C designs is not one related to technology or design; instead it is a problem of understandability. The overall I&C architecture provides a framework to systematically develop, present, and understand the I&C design bases in the necessary context (i.e., the plant-level) before attempting to understand the I&C design at the system/technology level.

An I&C system I&C design approach should facilitate the systematic documentation of the 'Why' questions:

- Why do the various I&C functions exist?
- Why are I&C systems scoped the way they are?
- Why are the I&C functions allocated as they are?
- Why do the interfaces between I&C systems exist?

The benefits inherent in a given design can usually be derived from the *why* and not from the *how*. Only the *hazards* can be seen in the *how*. Understanding the *why* and the *how* is critical before understanding the requirements imposed to mitigate *hazards* imposed by the *how*.

The regulatory review challenges experienced on the Oconee and Diablo Canyon projects were all based on NRC addressing requirements imposed to mitigate *hazards* without having adequate descriptions of those imposed by the *why* and the *how*.

Existing NRC Guidance

Limited guidance exists to support the design of system architectures for safety-related systems.

NRC issued Design-Specific Review Standard for NuScale Small Modular Reactor Design. It incorporated lessons learned from the NRC's reviews of new plant Design Certification Applications. Section 7.0 Appendix B, *Instrumentation and Controls — System Architecture*, provides an approach to describe an I&C system architecture and identifies relevant information to assess the design's conformance to the relevant regulations and application of the diversity and defense-in-depth (D3) concept.

There is no comparable review guidance for I&C system architectures in Chapter 7, *Instrumentation and Controls*, of NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition*.

Technical standards for I&C system architectures would provide better and consistent guidance for the evaluation I&C system architectures, which would improve efficiency and ensure consistency in technical evaluation and regulatory acceptance.

Available Industry Guidance

IAEA Specific Safety Guide No. 39, *Design of Instrumentation and Control Systems for Nuclear Power Plants*, provides guidance on the design of I&C system architectures (see Sections 4.13 through 4.24). It provides guidance on I&C architecture design principles and the proper application of independence within the overall I&C architecture to prevent the propagation of failures between systems.

IEC 61513, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*, provides requirements for the design of safety-related I&C systems. It provides guidance on:

- Clause 5 addresses the overall architecture of the I&C systems important to safety:
  - defining requirements for the I&C functions and associated systems and equipment derived from the plant safety analysis, the categorization of I&C functions, and the plant lay-out and operational context;
  - structuring the overall I&C architecture, dividing it into a number of systems, and assigning the I&C functions to systems; and
  - planning the overall architecture of the I&C systems.
- Clause 6 addresses the requirements for the individual I&C systems important to safety, particularly the requirements for computer-based systems.
- Clauses 7 and 8 address the overall integration, commissioning, operation, and maintenance of the I&C systems.

IEC 61513 is the most widely accepted source of guidance related to nuclear power plant overall I&C architecture design. It is a system engineering oriented standard that is consistent with the EPRI Digital Design Guide and offers more guidance to support system architecture design work. The IEC 61513 approach to I&C system architectures was used to frame how this information would be presented when Revision 2 to DI&C-ISG-06 was developed.

Objective

The goal of this effort would be to provide regulatory guidance regarding the technical information required to support the reviews of safety-related architectures for major safety systems like (e.g., Protection System).

Recommendations

1. NRC should build on the work done in the international nuclear community related to the design of I&C system architectures.

2. NRC should build on the work it has already done in support of the Multinational Design Evaluation Programme (MDEP) development of Generic Common Position for important digital I&C issues. Relevant work related to I&C system architectures can be found in Generic Common Position DICWG-09, *Common Position on Selection and Safety Design Principles and Supporting Information for the Overall I&C Architecture*. The common positions in DICWG-09 address these topics:

    - Defense in Depth
    - Consideration of Common Cause Failures
    - Independence
    - Diversity
    - Compliance of safety groups with the single failure criterion
    - Reliability
    - Complexity

    The common positions also identify the important information and associated design features (e.g. design characteristics, commitments, etc.) about the overall I&C architecture that should be provided to assist in the safety demonstration and ensure safety.

3. NRC should endorse relevant technical standards associated with the design of I&C system architectures utilizing digital technologies.

4. It seems practical that NRC could endorse IEC 61513 based on the MDEP work. NRC endorsement of IEC 61513 would help standardize the I&C system design approach to be consistent with the lessons learned that were factored into DI&C-ISG-06 Revision 2.

5. NRC endorsement of the relevant portions of IEC 61513 related to I&C system architecture (see Appendix) design and documentation would not be incompatible with the regulatory use of IEEE Std 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. IEC 61513 is more of a process standard than a technical standard. IEEE Std 603 is a technical standard. The IEC 61513 approach recognizes that local technical regulatory requirements will exist and provides a methodology that incorporates these kinds of plant-specific requirements into the development of the system requirements. The portions of IEC 61513 related to I&C system architecture design and documentation can be implemented within the U.S. framework and help support architecture decisions for major I&C systems.

6. Any decision to pursue endorsement should be coordinated with the plans for regulatory use of the EPRI Digital Design Guide.

Appendix - Software Development Process – IEEE and IEC Approaches

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 1074-2006	Software Lifecycle (RG 1.173)	IEC 61513 Section 6 (system lifecycle)
		IEC 60880 (software lifecycle)
		IEC 62566 (FPGA lifecycle)
IEEE Std 1074-2006 (Section A.1.2)	Software Development Planning (BTP 7-14 Section B.3.1)	IEC 61513 Section 5.5 (overall I&C planning) IEC 61513 Section 6.3 (individual system planning)
		IEC 60880 Sections 5.4 (software project management) and 5.5 (software quality assurance)
		IEC 62566 Sections 5.3 (FPGA project management) and 5.4 (FPGA quality assurance)
-	Secure Development and Operating Environment (RG 1.152)	IEC 61513 Section 5.5.3 (overall I&C security plan) IEC 61513 Section 6.3.3 (Individual system security plan)
		IEC 60880 Section 5.7 (software security)
-	System Architecture	IEC 61513 Sections 5.2, 5.3 (documentation), 5.4, and 5.6 (overall architecture) and 6.2.2.3.2 (system architecture)
-	System Requirements	IEC 61513 Sections 6.2.2 (requirements) and 6.4.2 (documentation)

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 828-2005	Software Configuration Management (RG 1.169)	IEC 61513 Section 6.3.2.3 (system configuration management plan) IEC 60880 Section 5.6 (software configuration management)
		IEC 60880 Section 5.6 (software configuration management)
		IEC 62566 Section 5.5 (FPGA configuration management)
IEEE Std 830-1998	Software Requirements Specification (RG 1.172)	IEC 61513 Section 6.2.3.4 (software requirements specification)
		IEC 60880 Section 6 (software requirements specification)
		IEC 62566 Section 6 (FPGA requirements specification)
IEEE Std 1012-2004	Software Verification and Validation (RG 1.168)	IEC 61513 Sections 6.4.2.3, 6.4.3.3, 6.4.4.4, 6.4.5.3, 6.4.6.3, and 6.4.7.3 (system verification) IEC 61513 Sections 6.2.5 (system integration) and 6.2.6 (system validation)
		IEC 60880 Section 8 (software verification) IEC 60880 Section 10 (software aspects of system integration) IEC 60880 Section 11 (software aspects of system validation)
		IEC 62566 Section 9 (FPGA verification) IEC 62566 Section 10 (FPGA aspects of system integration) IEC 62566 Section 11 (FPGA aspects of system validation)

IEEE Approach	NRC Topic	IEC Approach
IEEE Std 1008-1987	Software Unit Testing (RG 1.171)	IEC 60880 Sections 8.2.3.1.1.3 and 8.2.3.1.1.4
		IEC 62566 Sections 9.5, 9.6, and 9.7
IEEE Std 829-2008	Software Test Documentation (RG 1.170)	IEC 61513 Sections 6.4.5 (system integration documentation), 6.4.6 (system validation documentation)
		IEC 60880 Sections 8.2.3.1.1.5, 8.2.3.1.2, and 8.2.3.1.3
		IEC 62566 Sections 9.2.6, 10.6, and 11.4

Update SRM-SECY-93-087 and Associated Regulatory Guidance

Background

The preferred approach addressing digital common cause failure vulnerabilities considered at the time SRM-SECY-93-087, *Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs*, was issued was to bound the consequences of a digital common cause failure (CCF) in a black box manner, based on the underlying concerns with the use of digital technology in plant safety systems described in SECY-91-292, *Digital Computer Systems for Advanced Light Water Reactors*. The concerns stemmed from lack of experience in nuclear applications, evolving technology, absence of requirements and standards related to digital-specific design aspects, and lack of guidance and standards related to software development processes.

The digital technology used in nuclear safety systems has changed significantly since 1991. There is a vast body of operational data from the global deployment of digital instrumentation and controls (I&C) in nuclear plants. The safety-critical platforms developed for the global nuclear market have mature design features that provide for deterministic behaviors through the use modern IEC[1] standards. The development process standards for digital I&C systems (both IEEE[2] and IEC) have matured and are now widely accepted by nuclear regulatory bodies.

It is also clear that the application of system-level diversity as a panacea for the digital CCF concern has resulted in more complex system architectures with no clear connection between the application of the diversity to the most relevant or important CCF vulnerabilities. The downsides to the added complexity are not really considered in the regulatory decisions.

Problems with Current NRC Guidance

SRM-SECY-93-087 has not provided the necessary regulatory stability required for the industry to implement major modernizations of safety systems with digital technology. The underlying staff review guidance has been revised several times and each change has expanded the scope of systems and equipment to be addressed, the scenarios and failure modes to be considered, the acceptance criteria, and the documentation requirements. Each change has had a detrimental effect on the licensees' ability to effect I&C modernization and manage equipment obsolescence.

The concept of likelihood is no longer a part of the CCF evaluation process. The I&C CCF journey starts with the ATWS rule[3] where the focus was on risk (both likelihood and consequences). The rule focuses on the loss of feedwater scenario. Later Branch Technical Position (BTP) 7-19, Revision 4, *Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based*

---

1 International Electrotechnical Commission

2 Institute of Electrical and Electronics Engineers

3 10 CFR 50.62, Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants

Instrumentation and Control Systems, looked to address protection system CCFs for all abnormal operating occurrences (AOOs) and postulated accidents (PAs), which were given a different treatment in a graded manner. The digital CCF evaluation was focused on the protection system with some general guidance on how to perform best-estimate analyses and apply manual actions. NRC accepted solutions that focused on diversity (largely functional diversity) in the reactor trip protection algorithms for AOOs and manual engineered safety feature actions for PA mitigation. The NRC decisions on the Diablo Canyon license amendment (circa 1993) and Watts Bar Unit 1 initial licensing (circa 1996) resulted in approved digital protection systems that did not require separate diverse actuation system. The NRC review approach reflected a defense-in-depth and diversity orientation. The BTP 7-19 guidance at the time mentioned how leak-before-break concepts could be used to support the decisions for manual actions for the PAs.

BTP 7-19, Revision 5, *Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems***,** represented a shift in the NRC approach, which shifted focus more on diversity rather than defense-in-depth, as reflected in the title change. The new guidance applied rigorous best estimate analysis methods and coverage for all AOOs and PAs analyzed in Chapter 15 of the plant Final Safety Analysis Report and a rigorous human factors engineering analysis for any operator actions proposed in the first 30 minutes. The emphasis is on the design of a diverse actuation system. The BTP 7-19 guidance also removed the discussion of how leak-before-break concepts could be used to support the decisions for manual actions for the PAs. The NRC guidance became less risk informed because protection system spurious actuation, CCF coincident with an AOO, and a CCF coincident with a PA were treated equally. All PAs are treated equally even though large and small breaks have significantly different likelihoods. The treatment of CCF does not have 'cutoff' frequencies to distinguish between scenarios that should be addressed and those that do not have to be addressed. This new guidance resulted in the diverse actuation system addition for the Oconee retrofit project and very elaborate diverse actuation systems for the new plant designs under review. In addition, the likelihood of the failure mode is never considered. There is likely agreement that failure to actuate (i.e., lock-up) is much more likely than some coherent CCF that creates an incorrect actuation for a given set of inputs. Given this likelihood aspect, a well-designed watchdog might well be a sufficient defensive measure to address the CCF concern.[4,5]

BTP 7-19 Revision 6, expanded the scope from the protection system to all safety-related systems and applied the same rigorous methods to expanded scope. As a result, the NRC guidance became less graded because front line actuation systems, long-term event management, and support systems were treated the same. The change in scope was made without any defined regulatory basis to support the change (i.e., no change in Commission direction on treatment of CCFs, no plant CCF events that exposed vulnerabilities, or new research on CCF that identified new concerns with less risk-significant systems). The recent Regulatory Issue Summary (RIS) 2002-22, Supplement 1, *Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,* has restored some aspects

---

[4] This solution was also identified in a letter from the ACRS to the NRC EDO dated August 5, 2014, *Proposed Revision for 10 CFR 50.55a to Incorporate by Reference IEEE Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"*

[5] The Oconee digital platform has a well-designed watchdog that will put the outputs in the pre-defined safe state (typically actuate but not always). These features will actuate more equipment and for all scenarios if a CCF were to occur, whereas, the diverse actuation system only actuates for large and small loss of coolant accident scenarios.

of a graded approach with the use of qualitative assessments rather than quantitative assessments for less risk-significant systems. A risk-informed or graded approach would look to define boundaries for the qualitative/quantitative methods or to cut-off consideration CCF for lower risk systems.

The NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, evaluation process for a diverse actuation system looks at subsets of potential common cause failures based on the six attributes of diversity that are defined. These CCF issues and equipment associated with these attributes vary widely. There is no clear guidance on how to focus on the likely or most important attributes. As such, the acceptable solutions have migrated from ones that focused on preserving the signal and functional diversity in the original I&C system designs in retrofit projects. Later, the acceptable solutions have had to address software and equipment diversity. No approved solution addresses all attributes. This main guidance document has not been updated to address the improvements in the digital technology now being used for nuclear plant safety systems.

The CCF evaluation process is not clear on failure modes. One can look at history and see that the original emphasis was on failure to actuate, which resulted in diverse actuation systems. Examples presented in the back of NUREG/CR-6303 suggest that highly deterministic operating system software need not be considered a source of common-mode software failures.[6,7] However, NRC has never allowed the exclusion of operating systems as a source of CCF vulnerability in the defense-in-depth and diversity (D3) analyses reviewed and approved. BTP 7-19, Revision 6, expanded the CCF review to also include postulated spurious actuations and partial actuations. The introduction of smart spurious CCF failure modes would lead to <u>new mitigation</u> features for events like multiple main steam isolation valve closures or multiple steam generator or pressurizer power operated relief valve openings.

The result of this expanding trend for D3 analyses is that I&C obsolescence projects become significant safety analysis projects to develop the documentation required to support the 'best estimate' analyses to support the expanded scope of CCF evaluation. The Oconee D3 analysis took three years to review. The Oconee D3 was approved by letter with a formal safety evaluation report (SER) using similar arguments to Diablo Canyon and Watts Bar. Six days later, the D3 SER was formally withdrawn by letter. The Oconee protection system upgrade was approved three and a half years later after the addition of a diverse actuation system. The Diablo Canyon

---

6 From NUREG/CR-6303:

> *<u>Effect of the Operating System</u>: The operating system, which is common to all subsystems in this design, will not be included as a source of common-mode software failures. It is assumed that the operating system as described by (the vendor) is simple enough that failures are related to service demands and that service demands are distributed differently enough in subsystems defined as dissimilar (above) to exclude the operating system as a separate cause of common-mode failure. Consequently, any common-mode operating system failures are subsumed by (the previous paragraph). This assumption is not valid if (the vendor) uses a complex, multitasking operating system or uses more than a simple clock-updating timer interrupt.*

7 Some designs accepted in Europe focus on preserving functional diversity as a priority, couple CCFs only with AOOs, and do not consider highly deterministic operating system as a source of CCF concern. The resulting designs have two subsystems that separated the primary and backup trip signals into separate application layers, both using the same operating system.

D3 analysis for the Eagle 21 replacement took one year to review. The Diablo Canyon replacement design for Eagle 21 resulted in an intricate design using two diverse safety-related digital platforms and elimination of operator actions previously accepted for Eagle 21 installation.

The recent Hope Creek license amendment for a digital retrofit required significantly more work to address human factors engineering justification for the same operator actions that had been previously reviewed and accepted on several other similar projects for other plant I&C modernizations.

One can compare the impacts on the protection system I&C design complexity by comparing the Diablo Canyon Eagle 21 version (circa 1993) with the later replacement system approved in 2016 (see Figure 1). These differences were all driven by changes in the NRC's implementation of SRM-SECY-93-087 (which has not changed).[8]

SECY-18-0090, *Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls*, identified that NRC management recognizes that SRM-SECY-93-087 provides flexibility for the treatment of digital common cause failures in digital I&C systems. In the U.S. regulatory framework, hazards that can affect structures, components, equipment, and systems are defined in two parts of the plant Final Safety Analysis Report: Chapter 3 (design criteria for structures, components, equipment, and systems) and Chapter 15 (plant transients and accidents to be considered). In effect, the NRC guidance issued by management states the hazards to consider and how to design for them. NRC management has defined the reasonable assurance boundary that allows NRC reviewers to work effectively to review implementation of the design criteria and check results against established acceptance criteria.

Other beyond design basis issues addressed by management (e.g., ATWS, station blackout, certain security scenarios, and the recent diverse and flexible coping strategies (FLEX)) have resulted in a better understanding of the reasonable assurance boundaries and acceptance criteria for the equipment and associated analyses. As a result, the industry has had an easier time implementing the associated design features.

However, BTP 7-19 is a methodology guidance that lacks reasonable assurance boundaries issued by NRC management. As a result, many widely different solutions to the digital CCF problem are the end results because of the lack of boundaries on key evaluation parameters (i.e., credible scenarios, credible failure modes, and application of diversity). The accepted solutions are not equal in providing protection nor consistent in addressing the CCF vulnerabilities. The NRC management decision making on the issue has not matured to the point that it can be incorporated into the more appropriate home for such hazard criteria (i.e., Chapters 3 and 15). As such, industry struggles with a process that pushes the regulatory assurance decision down to the individual reviewer with the resulting management problem of trying to herd cats. The review process for digital CCF has been more of a journey than a destination.

Relevant International Guidance

The scope of IEC 62340:2007, *Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements for Coping with Common Cause Failure*, is limited to the

[8] Watts Bar Unit 2 was licensed in 2016 with an Eagle 21 system without any diverse actuation system.

avoidance of CCF of I&C systems that perform Category A functions. The IEC approach is consistent with the Multinational Design Evaluation Programme (MDEP) Generic Common Position DICWG-01, *Common Position on the Treatment of Common Cause Failure Caused by Software within Digital Safety Systems*. The common position in DICWG-01 is that nuclear power plants should be systematically protected from the effects of CCFs caused by software in digital I&C safety systems.[9] The common positions are limited to the potential for software CCFs within digital safety system safety functions arising from latent design deficiencies introduced in any of the three software development activities (i.e., software requirements, software design and software implementation). As such, the scope of common position is limited to the consideration of the potential for software CCF caused by the introduction of latent errors in the design of digital safety systems.

Recommendations

1. As near-term action, BTP 7-19 should be rolled back to Revision 5, as a minimum, to be consistent with RIS 2002-22 Supplement 1 regarding scope. Ideally, it should return back to Revision 4, which would be consistent with a risk-informed, graded approach to the treatment of digital CCF for safety-related systems.

2. Update SRM-SECY-93-087 to incorporate the advances in the digital technology for safety-critical applications, incorporate risk insights into the evaluation methodology, and apply a graded approach to the implementation guidance. The update to SRM-SECY-93-087 is necessary to ensure that the approach to digital CCF remains stable to provide the necessary regulatory certainty needed to support major capital investments to modernize protection systems.

3. The updated direction in SRM-SECY-93-087 for the evaluation of digital CCF should reflect risk insights and factor in assessments of likelihood for consideration for failure modes and scenarios. For example:

    - Limit scenarios for evaluation to risk-significant AOOs coincidence with a CCF. Exclude other scenarios (e.g., PAs coincident with CCF) from further consideration.
    - Limit failure modes for evaluation to fail-to-actuate (i.e., lock-up). Eliminate other failure modes (e.g., 'smart' spurious actuations, partial actuations, etc.) from further consideration.
    - Accept leak-before-break concepts to define the significance and timing for crediting manual operator mitigation of any high consequence PA scenarios to be considered.

4. The updated direction in SRM-SECY-93-087 for the evaluation of digital CCF should reflect risk significance in defining the scope. For example:

---

[9] The usage of *safety systems* is interpreted in the European context and is considered equivalent to Category A functions and *safety-related* is considered equivalent to Category B and C functions (see IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*. The protection system is classified as performing Category A functions.

- Limit the scope to the protection system. Exclude other safety-related and non-safety systems from further consideration.

5. The updated direction in SRM-SECY-93-087 for the evaluation of digital CCF should reflect a graded approach for the D3 analyses. For example:

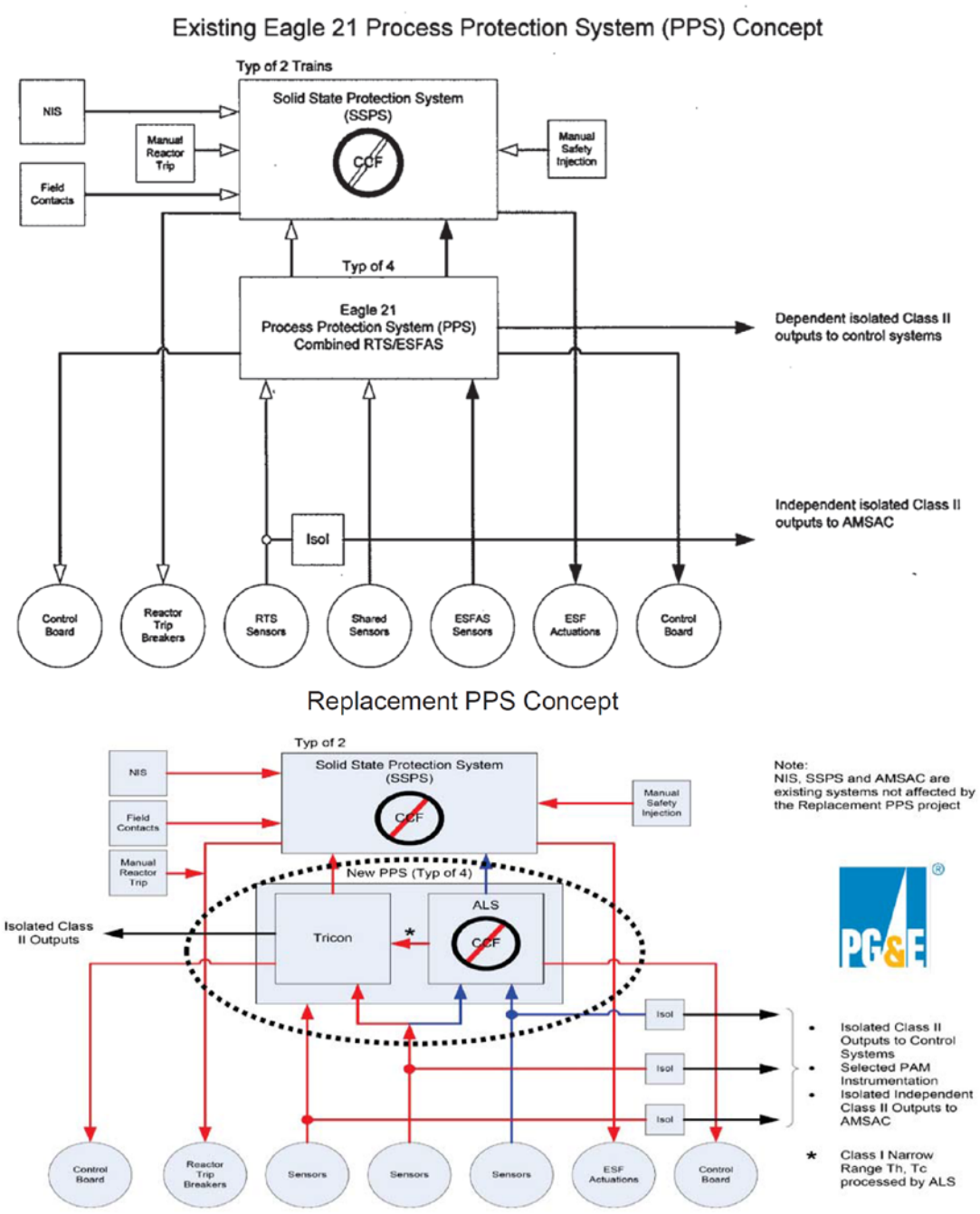
    - The rigor required for the beyond design basis CCF evaluation for any best estimate analysis or human factors engineering evaluations should be less rigorous than that required for design basis events

6. The updated direction in SRM-SECY-93-087 for the evaluation of digital CCF should reflect the advances in the digital technology for safety-critical applications. For example:

    - Well-designed watchdogs that provide appropriate safe-state actuations should be accepted as effective mitigation for the credible failure mode (i.e., lock-up).
    - Operating system software that is well-designed as deterministic can exclude the operating system as a separate cause of common-mode failure.

7. The risk basis for the update to SRM-SECY-93-087 should be addressed generically to the extent practical to minimize the impact on I&C modernization projects from extensive plant-specific analysis work to support I&C projects.

Figure 1: Comparison of Eagle 21 and Replacement System Architectures



The Eagle 21 replacement uses two safety-related digital platforms (instead of one) with with sensor sharing, allocation of protection functions to the two platforms to address D3 rather than all in one), and additional system interfaces to manage sensor input functions between the two platforms and outputs from two systems.

Table 1 – Tabular correlation between categories and other IEC standards

Category	Applicable IEC standards		Main requirements for			
	Systems	**Equipment**	**Functions**	**Design of systems**	**Equipment features**	**General**
General	IEC 61513 IEC 60964, IEC 60965 IEC 61771, IEC 61772 IEC 61839 IEC 60709	IEC 61000-4 IEC 61000-6-2	Functional specification	Testability HMI specification	Electromagnetic compatibility	QA program Quality control FAT, SAT Periodic testing
A	 IEC 60812[5] IEC 60880 IEC 60987	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories High assurance of reliability	Single failure criterion Independence, separation Design to cope with internal common cause failure Diversification case by case FMEA Back-up power supply	Qualification to postulated environment and to seismic conditions	IAEA GS-R-3 Verification on identical equipment Full FAT/SAT Frequent periodic testing
B	 IEC 60987 IEC 62138	IEC 60780, IEC 60980	Appropriate codes, standards, guides Separation from lower categories	Single failure criterion, separation both possibly at functional level Back-up power supply	Qualification to environment and seismic conditions that the equipment must withstand	IAEA GS-R-3 Verification on similar equipment Limited SAT and periodic testing
C	IEC 62138			Redundancy and separation case by case	Qualification case by case	Normal industrial practice Periodic test if not used continuously