

This record has been redacted prior to discretionary release to the public.

NON-CONCURRENCE PROCESS COVER PAGE

The U.S. Nuclear Regulatory Commission (NRC) strives to establish and maintain an environment that encourages all employees to promptly raise concerns and differing views without fear of reprisal and to promote methods for raising concerns that will enhance a strong safety culture and support the agency's mission.

Employees are expected to discuss their views and concerns with their immediate supervisors on a regular, ongoing basis. If informal discussions do not resolve concerns, employees have various mechanisms for expressing and having their concerns and differing views heard and considered by management.

Management Directive, MD 10.158, "NRC Non-Concurrence Process," describes the Non-Concurrence Process (NCP), <http://nrcweb.nrc.gov:8600/policy/directives/catalog/md10.158.pdf>.

The NCP allows employees to document their differing views and concerns early in the decision-making process, have them responded to (if requested), and attach them to proposed documents moving through the management approval chain to support the decision-making process.

NRC Form 757, "Non-Concurrence Process" is used to document the process.

Section A of the form includes the personal opinions, views, and concerns of a non-concurring NRC employee.

Section B of the form includes the personal opinions and views of the non-concurring employee's immediate supervisor.

Section C of the form includes the agency's evaluation of the concerns and the agency's final position and outcome.

NOTE: Content in Sections A and B reflects personal opinions and views and does not represent official factual representation of the issues, nor official rationale for the agency decision. Section C includes the agency's official position on the facts, issues, and rationale for the final decision.

At the end of the process, the non-concurring employee(s):

- Concurred
- Continued to non-concur
- Agreed with some of the changes to the subject document, but continued to non-concur
- Requested that the process be discontinued
 - The non-concurring employee(s) requested that the record be non-public.
 - The non-concurring employee(s) requested that the record be public.
- This record is non-public and for official use only.
- This record has been reviewed and approved for public dissemination.

This record has been redacted prior to discretionary release to the public.

NON-CONCURRENCE PROCESS

NCP TRACKING NUMBER
NCP-2014-004

SECTION A - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL

TITLE OF SUBJECT DOCUMENT
Incorporation by Reference Institute of Electrical and Electronics Engineers Standards, 603-2009

ADAMS ACCESSION NO.
113191306

DOCUMENT SIGNER
Eric Leeds

SIGNER PHONE NO.
(301) 415-1270

TITLE
Office Director Nuclear Reactor Regulation

ORGANIZATION
NRR

NAME OF NON-CONCURRING INDIVIDUAL(S)
William Roggenbrodt

PHONE NO.
(301) 415-0678

TITLE
Electronics Engineer - Digital I&C

ORGANIZATION
NRO/DE/ICE1

DOCUMENT AUTHOR DOCUMENT CONTRIBUTOR DOCUMENT REVIEWER ON CONCURRENCE

REASONS FOR NON-CONCURRENCE AND PROPOSED ALTERNATIVES

TITLE OF NON-CONCURRENCE DOCUMENT:
Position Paper on Staff Update to 10 CFR 50.55a(h) Rule Affecting I&C Systems

REASON FOR PROPOSED NON-CONCURRENCE:
The currently proposed rule language updating 10 CFR 50.55a(h), "Protection and Safety Systems," fails to meet the threshold of adequately addressing overall system safety for modern instrumentation and controls (I&C) systems, as it overlooks critical issues that have emerged as a result of contemporary I&C system technology.

REFER TO ATTACHED DOCUMENT FOR POSITION PAPER THAT DESCRIBES NON-CONCURRENCE.

CONTINUED IN SECTION D

SIGNATURE *William A. Roggenbrodt*

DATE 3/14/2014

SEE SECTION E FOR IMPLEMENTATION GUIDANCE

Position Paper on Staff Update to 10 CFR 50.55a(h) Rule Affecting I&C Systems

Issue Statement

The currently proposed rule language updating 10 CFR 50.55a(h), "Protection and Safety Systems," fails to meet the threshold of adequately addressing overall system safety for modern instrumentation and controls (I&C) systems, as it overlooks critical issues that have emerged as a result of contemporary I&C system technology.

The following examples illustrate the unintended consequences of such an undertaking:

- 10 CFR 50.55a(h) incorporates by reference (IBR) IEEE Standard (Std.) 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The currently endorsed version, IEEE Std. 603-1991, is a "technology-neutral" standard whose criteria apply to all I&C safety systems. However, the 2009 version of IEEE 603, which the staff has proposed as the new IBR rule, includes technology-specific language that transforms part of the 'standard' into a technology-specific document rather than a 'standard.' The new rule, as currently proposed, will lead to applicants and licensees designing new I&C systems for licensing certainty rather than optimizing system safety.
- Adding technology specific requirements into a regulation that previously applied to all I&C safety systems, regardless of the technology utilized, places additional regulatory burden on licensees, and causes delays in new system designs and implementation that may result in hampering, rather than enhancing, overall plant safety.
- Additionally, due the economic risk and technical challenges associated with developing and licensing new, more modern and reliable I&C systems, licensees will continue to operate with obsolete components and systems rather than take on the risks, challenges and uncertainties associated with developing and licensing a new, more reliable I&C system due to provisions within the proposed rule language.
- The new rule, as currently written, is silent on how to address new failure modes created by the technological and architectural complexity of new I&C system designs. Since there is no requirement for a systems' hazards analysis to be conducted for these devices, some of which contain embedded digital technology, it results in the greater likelihood of common cause failures (CCFs) that have the potential to defeat system diversity. This issue was not addressed in the 2009 version of the IEEE Standard or other language within the proposed new rule.
 - As examples, this issue relates to priority modules and final actuation devices (FADs) containing digital technology. FADs are excluded from consideration within IEEE 603, and the new rule, yet they have evolved from simple electro-mechanical devices that now contain new failure modes that impact new I&C system designs in unexpected and unanticipated ways.

Given the infrequency with which the rule language impacting I&C safety systems is updated the prudent choice would involve re-examining the issues cited above and developing rule language that proactively addresses a greater range of safety concerns that solve the current and future needs of the staff and industry.

The goal of this paper is to present the consequences of not adequately addressing the issues described above and to propose mutually beneficial solutions that provide clear, concise rule language that is both effective and enforceable.

Concerns Related to the Incorporation of IEEE Standard 603-2009 Into Rule Language

The currently endorsed version of IEEE Std. 603, IEEE Std. 603-1991 is a “technology-neutral” standard whose criteria apply to all I&C safety systems. However, the 2009 version of the same standard includes technology-specific language that transforms part of the ‘standard’ into a technology-specific document rather than a ‘standard’.

In addition, the standard, and the associated rule, is silent on relevant issues (e.g. use of digital technology within FADs) that affect both regulators and licensees and the safety systems they design, develop and/or evaluate.

One of the unintended consequences of endorsing detailed technology-specific language in our guidance has already manifested itself in the nuclear industry by having one licensee attempt to avoid detailed regulatory guidance associated with digital systems by designing a replacement I&C system utilizing analog parts rather than digital technology that has been demonstrated to be more reliable than its analog counterparts.

Another result of establishing new regulations as well as existing guidance related to the use of digital technology is revealed itself in the guise of currently licensed nuclear power plants operating with outdated, obsolete I&C safety systems, with a rarity of spare parts rather than take on the economic risk and technical challenge of developing and licensing new, more reliable, modern I&C safety systems. Adding digitally-based requirements into a regulation that previously applied to all I&C safety systems, regardless of the technology utilized, places additional regulatory burden on licensees, and causes delays in new system designs and implementation that may hamper, rather than enhance plant safety.

The currently proposed rule language incorporates the IEEE Standard language in its entirety, as has been the approach with regard to this standard for over 20 years. However the nuances, intricacies and complexities of the digital language within this version of the standard required two NRC Offices to apply the rule differently. Thus, there is demonstrative evidence that the pattern of applying all the language within the standard in its entirety will not continue as a matter of policy for all Offices.

By allowing the inclusion of design-specific language into a previously standardized document, the reviewer and applicant/licensee both must become increasingly fluent in what may become various ‘design-specific data sets’ within ‘standardized’ documents. As such, the use of technology-specific language in the standard results in less clarity and more confusion since the applicability of certain declarative statements within the document may or may not apply to different I&C safety systems.

Further, as the staff does not control the information incorporated into any given IEEE standard beyond its membership in IEEE, the design-specific information that has been already incorporated into the 2009 standard sets a precedent. With the possibility that the Standards Committee will continue to allow the addition of technology-specific language into a future standard it would therefore continue to confuse the subject and its applicability to ‘all’ versus ‘certain portions’ of given I&C safety systems, should the staff choose to endorse the current and future versions of IEEE Std. 603. For example, whereas one might ask, “Does all the criteria of IEEE Std. 603-1991 apply to all safety related I&C systems?” the response is, “Yes, all the criteria in IEEE 603-1991 applies to all safety related I&C systems.” However, with the acceptance of the 2009 standard the answer would become – “Well... it depends.”

The long-established approach related to regulation when compared to guidance deals with subject matter that flows from the generic (applies to all systems) to the specific (applies to some systems) appears to be breaking down by allowing technology-specific language into regulation. True, this action has occurred before, but done so sparingly and not often with simple long-term results. In an era where designers have chosen to overly complicate I&C system designs (e.g. on-line system diagnostic testing, message traffic etc.), beyond what regulations require, the staff's proposed rule language inadvertently complicates our regulation.

Recommendations Related to the Use of IEEE Standard 603

The following recommendations discuss how IEEE 603 and technology-specific material should be incorporated into rule language and accompanying guidance documents.

1. Develop a Strategy Document – The first recommendation allows the I&C rule-making team members to formulate a mid-term and long-term strategy document that describes all the issues the staff and industry face with regard to I&C systems. This document may take several forms, up to and including a SECY Paper. The strategy document further explains 'how', 'why' and 'when' these important issues related to the development and implementation of I&C systems, both safety and non-safety, will be formally addressed.

For example, during the past four years 'scope creep' has occurred during the rule-making process and as a result the rule making process remained mired in professional disagreements. To remedy this issue, the staff should develop a strategy document that describes and maps out the multi-year effort to resolve all issues related to various I&C topics, but limit the scope of each effort into manageable pieces, thereby eliminating 'scope creep'.

2. Implement the Strategy Using a Two-Tiered Regulatory Model – The strategic method, described herein, involves adopting a format similar to the one implemented by the International Electrotechnical Commission (IEC) in which the regulations flow from the generic 'applies to all I&C protection and safety systems' to 'applies to some I&C protection and safety systems' dependent upon a number of different factors.

This approach would enable the regulator to focus on key factors that relate to a given type of system or to a development topic that would apply to all protection and safety systems. When utilizing this approach, updating the entire 'rule set' would not be required when updating a specific topic, such as software diversity that would impact only those systems executing software or those that are developed with a programming language.

As displayed in Figure 1, the IEC Standards structure supports requirements for all I&C safety systems, such as those described in IEC 61508, and then provides design-specific requirements for digitally-based I&C safety systems within nuclear power plants, similar to those defined in IEC 61226 and IEC 61513.

The comparison would hold for the proposed two-tier regulatory structure that would apply to safety related I&C systems utilized in American nuclear power plants. These regulations would reference certain IEEE Standards for all I&C safety systems, such as those described in IEEE Std. 603-1991, and then create regulations that provide design-

specific requirements for digitally-based safety systems or other 'application-specific' characteristics within I&C safety systems. For example, one could apply a portion of those characteristics defined in IEEE Std. 7-4.3.2, which could be used as a starting point when developing regulations for digitally-based I&C systems.

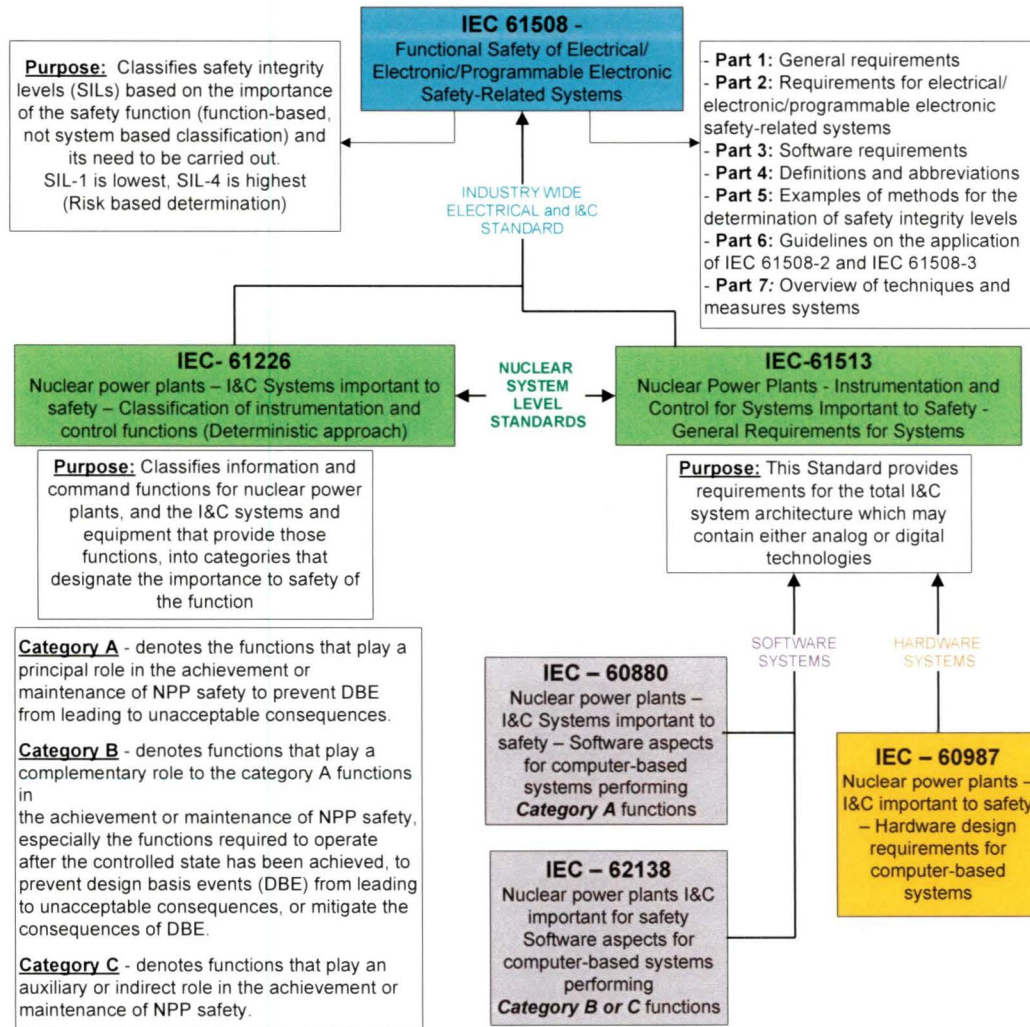


Figure 1:
Overview of International Standards as They Apply to I&C Related Nuclear Safety Systems

Utilizing this strategy provides a benefit since it would be possible to leave the 1991 version as the endorsed standard that applies to all I&C safety systems for nuclear power generating stations, while also allowing new language to be incorporated into another, more focused rule (or rules) that describes necessary design characteristics or attributes that pertain to 'application specific' applications for new or modified I&C systems. An example of this two-tiered approach to I&C protection and safety systems appears in Figure 2 (next page).

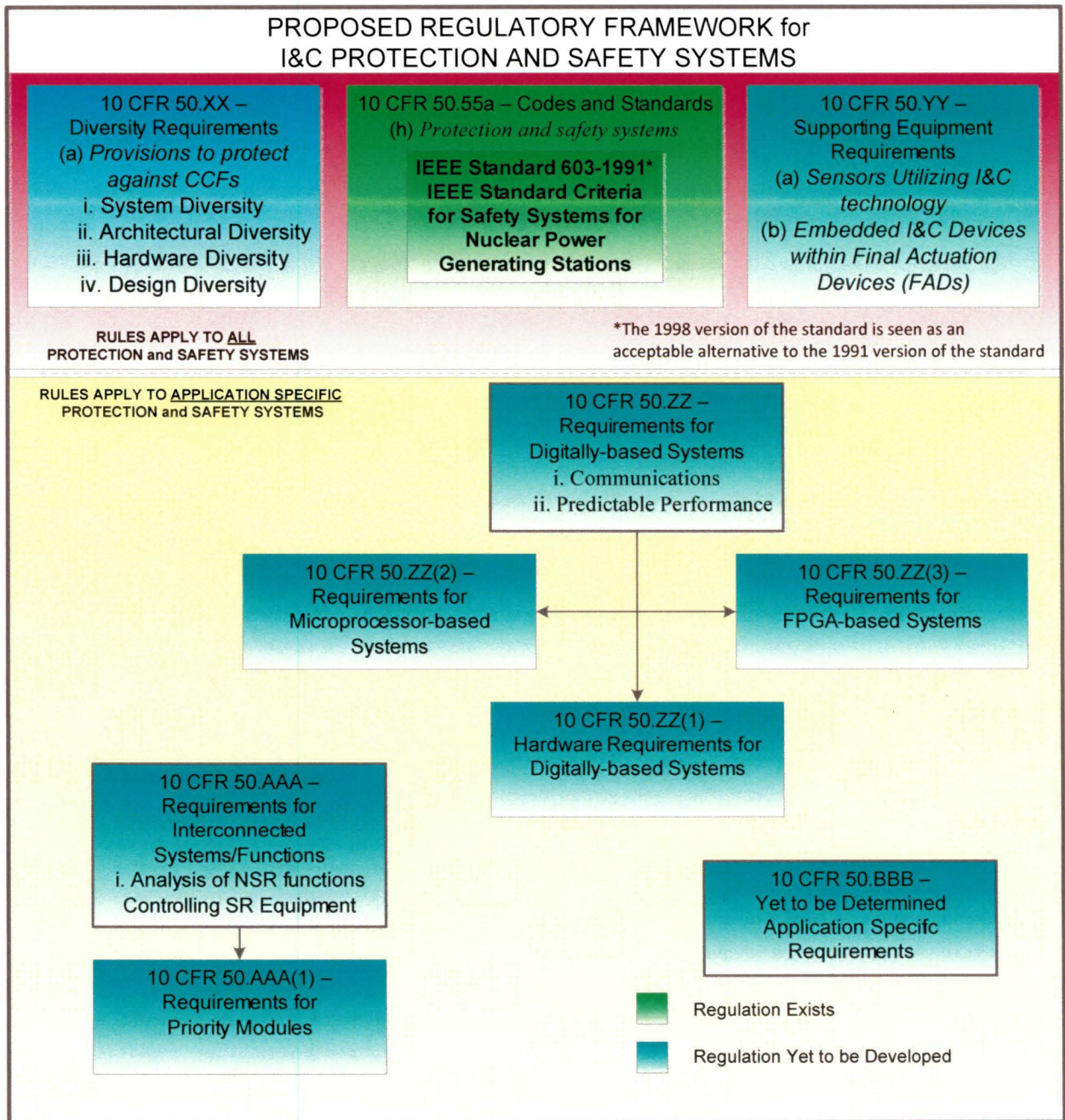


Figure 2: Proposed Regulatory Framework for Protection and Safety I&C Systems

3. Endorse the 1998 Version of IEEE Standard 603 for 10 CFR 50.55a(h) – In relation to which version of the IEEE 603 Standard to utilize, this author believes the best-fit solution involves upgrading the endorsed standard for all I&C systems to the 1998 version which includes language related to software common cause failures (CCFs), but does not yet contain technology-specific language related to a system’s independence, as does the 2009 version of the standard. It is the language related to the sufficient independence of digital systems that has caused such consternation between the two NRC Offices, which has resulted in a significant delay in the publication of the rule itself.

Additionally, by utilizing the 1998 version of the Standard it allows incorporation of the concept of CCFs, and their prevention or mitigation, without the divisive language related to independence. Additionally, it would be beneficial to expand the language in Clause 5.16 related to software CCF language and add language related to the necessity of performing an engineering evaluation and/or hazard analysis demonstrating how the plant would be designed in order to eliminate or mitigate and cope, in the presence of other types of CCFs, (e.g. design-based, culturally based, etc.)

This structure allows a more focused approach for both the designer and regulator when one attempts to determine the acceptability of a given design from both a design-neutral and design specific vantage point. Additionally, this solution allows for the application of technology-specific language into one or more 'lower-level' rules while also maintaining the flexibility of a higher-level more 'generic' rule relevant for all I&C systems.

Finally, while the examples presented in the current rule that discuss when a licensee is required to update the licensing basis due to modifying a safety related I&C system is valuable information, the language discussing those specifics would be more appropriate in regulatory guidance or a 'lower tier rule' rather than in generic rule language.

4. Revert to the 1991 Standard (if necessary) – Another approach the staff could utilize to solve the issue of technology-specific language within IEEE Std. 603-2009, and therefore the rule language, would involve leaving IEEE Std. 603-1991, including the correction sheet dated January 30, 1995 as the endorsed IBR rule for nuclear power plant I&C safety systems. By taking that action, the criteria in that standard would continue to apply to all I&C safety systems.

Some may suggest that using the 2009 version of the standard while taking exception to the 'digital-language' would be an acceptable approach, however this author deems it much *cleaner* to continue to incorporate the entirety of a standard and address independence and CCF concerns, as appropriate.

The Level of Technological and Architectural Complexity of Current and Future I&C Systems

With the advent of newly available technology the capabilities of a single device have multiplied exponentially over the past few decades. Previous I&C designs utilized discrete components to perform one or two simple functions within a system have been replaced by single multi-function devices or systems that are able to perform a myriad number of functions and calculations per second. Indeed, a single, integrated control system now has the capability to control entire areas of the power plant where it previously utilized thousands of discrete components within disparate systems, each with its own clearly defined boundaries and characteristics.

As such, some staff members have voiced concern over ensuring the consequences of utilizing highly-integrated and complex new I&C system designs are adequately examined and analyzed. The topic of a given system's complexity has been discussed during several Advisory Committee for Reactor Safeguards (ACRS) meetings and Commission briefings, discussing both the benefits and the potential consequences of having a single system control the majority of a plant's functions. However, no regulation and little guidance, referring to Branch Technical

Position 7-19, exists in regard to the subject area of analyzing a system's given level of complexity.

In the opinion of this author, the primary concern related to such system complexity is the lack of total and complete understanding of how a given system will respond under all actual 'real-world' conditions. Even if the verification and validation (V&V) program for a given system provides 100% testing coverage, there is no guarantee that the testing is all-encompassing or exhaustive for real-world conditions. Even if one tests ALL the requirements via a robust testing program, that fact in itself is no guarantee of a flawless or perfect system.

Additionally, since a single device is now capable of controlling so many control pathways within a given system architecture, (e.g. priority module), I&C system designs have been submitted to the staff that have the ability to minimize or eliminate overall I&C system diversity but still meet current regulations. In the aforementioned designs, the priority module receives all I&C control signals thus, a CCF of the priority module, software based or otherwise, would disable all automatic and manual functionality of safety related devices based upon commands from the safety-related, non-safety related and diverse I&C systems.

For example three submitted I&C system designs possess architectures such that the automatic and manual functionality for the non-safety-related, safety-related and diverse I&C systems for engineered safety functions (ESF) are routed through a single device. This single device of a common type will be replicated in multiple divisions, so that it meets regulations concerning single failure criteria via redundancy. However the staff's guidance in the area of CCFs pertains primarily to software CCF failures and other types of CCFs fall outside of the design basis. That is not to suggest that identifying and combating software-based CCFs is an incorrect approach, but rather an incomplete one in that other causes of CCFs need to be satisfactorily identified, examined and adequately addressed as well. The method the agency currently applies appears somewhat ad hoc based upon the fact that the primary focus is applied myopically towards that of a software-only based CCF.

In the area of CCFs, other examples of causal factors for CCFs are:

- System/Architecturally-based – layout of devices, or sub-systems in a larger, system-based construct allows CCF due to common routing of devices or control signals
(No inherent 'failure' of sub-system A or System B, failure is due to integrated system layout, when systems are combined together – then issues arise)
- Hardware-based
 - Previously undetected design flaw – (affects all devices)
 - Bad 'batch' of components – (affects some devices)
- Cultural/Organizational/ – personnel performing routine activities on a given
Human Factors CCF system or device that may cause a CCF via
implementing an incorrect practice or procedure
- Application-specific CCF – Newly developed system prone to unknown or
unanticipated operational conditions, classified as a first-of-
a-kind engineering (FOAKE) CCF, (e.g. lithium ion battery
system in the Boeing 787 Dreamliner fleet.)

All of these CCF ‘types’ must be adequately analyzed and, when necessary, have steps taken to minimize, mitigate or eliminate the given CCF type, however no regulation and limited guidance exists to require such an analysis.

Recommendations Related to I&C Safety System Architectural Complexity

1. Require Architectural Diversity – Construct I&C systems in a manner that requires designs to incorporate a minimum of two separate, diverse paths from sensor output to FAD for all I&C safety system functions (e.g. ESF functions) whose failure to actuate or actuation when system conditions do not require it, would cause the plant to exceed design limits. This requirement would be similar to the reactor trip requirements of 10 CFR 50.62. This requirement would prevent the system-level CCF that would potentially arise due to system layout.
2. Limit System Complexity – Require I&C safety systems to be only as complex as necessary to perform their functional and regulatory requirements to initiate and complete its safety function. Use of supplemental add-on features, (e.g. continuous on-line testing, system message traffic and system monitoring), that may be available due to the copious amounts of additional logic gates or unused memory within the system should be discouraged beyond the guidance in Branch Technical Position 7-14 in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition.” This requirement would enable the designers and regulators to better understand the system’s operational capabilities and failure mechanisms.

However, if the designer can demonstrate, through objective evidence and analysis, that any additional system complexity provides a significant safety benefit while only marginally raising the level of system risk, due to the higher level of system interconnectivity, (e.g. lessen the degree of independence between safety system divisions), the system with additional complexity may be found to be acceptable provided the staff evaluates the evidence and determines the adequacy and acceptability of the designer’s claims.

3. Require a Systems-based Hazards Analysis – As contemporary system designs are more integrated, and therefore complex, than in previous generations of I&C safety systems, require a detailed system wide, integrated hazard analysis to be conducted to ensure the system will cope with issues that arise from choosing a design with a high-level of integrated systems. Additionally, the hazard analysis should include internal failure mechanisms of a given device due to the complexity of the components within the system (e.g. unused memory, unused gates, clock overrun issues etc.) to ensure those failures are precluded from interfering with or otherwise interrupting the operation of the system’s safety function.

The Use of Embedded Digital Devices within Sensors and Final Actuation Devices

The use of EDDs within sensors and FADs has transformed simple electro-mechanical and pneumatic devices into highly capable and arguably, complex, digitally-controlled devices. However the benefit and potential consequences associated with the increased level of functionality within sensors and FADs lie outside the purview of IEEE Std. 603 and are therefore not addressed as I&C components with new types of failure modes. While there is no certainty as to why this is the case, the logic behind such a decision resides in the fact that traditionally, there were no I&C components, or more correctly, I&C functions carried out within the sensors

or FADs, beyond those of simple electro-mechanical relays, electro/hydraulic sensors, pneumatic/hydraulic valve positioners and so forth.

The concern related to these devices is the same as it is for other digital devices, components and sub-systems within I&C systems – that digitally-controlled devices are often more complex than their analog counterparts and, as such, require additional examination, analysis and scrutiny. As such, those devices that previously resided outside the realm of I&C system level scrutiny now exist within it due to their modern day designs and capabilities, although regulations and guidance may not reflect that reality.

In previous generations of sensors and FADs, the failure modes and mechanisms were easily defined in that the devices used proven time-tested, and arguably ‘simple’ technology. In today’s more complex equipment, the devices may possess new failure modes due to their upgrade in technology.

With regard to failure modes, at least one new reactor I&C system design claims that for the purposes of its failure modes and effects analysis (FMEA), its digitally-based device of an identical type is sufficient such that no secondary (diverse), independent path exists or is required for a control signal to pass to the FAD.

Indeed, our current guidance allows for such an architectural system structure since the current application of NRC policy states that software-based CCFs, although beyond design basis are the primary focus of CCFs and therefore must be considered and addressed. Per our current guidance, the 100% testing of a software-based device allows it to be treated as a ‘hardware only’ device, not susceptible to a software CCF, yet from the explanation given in Topic #2, 100% testing of the requirements is no guarantee of flawless system performance.

To its credit, the agency is working towards releasing a regulatory issue summary (RIS) related to embedded digital devices; however the RIS limits the application to safety-related components only and does not take into consideration the impact of non-safety-related devices that may impact its safety-related counterpart when dealing with highly-interconnected systems.

Recommendation for the Use of Embedded Digital Devices within Final Actuation Devices

1. Treat Sensors, FADs and other Non-Traditional I&C Devices as Part of the I&C System
– Analyze the I&C System from sensor to FAD to ensure the level of review is commensurate with the technology utilized for the given device, including sensors and FADs.

Summary

The staff effort to update regulations related to I&C systems under 10 CFR 50.55a(h) fails to address several technical issues that the staff and licensees face when designing and evaluating new I&C safety systems intended for use in nuclear power plants and fuel processing facilities.

Given the frequency with which this regulation has been updated, several additional steps must be taken in order to ensure the affected regulations remain current, precise, and comprehensive enough to provide reasonable assurance of safety for currently licensed and new nuclear power plants.

Those issues include

- The impact of the technology-specific language within IEEE Standard (Std.) 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations” will result in unintended consequences for both staff and industry
- The impact upon the nuclear industry by adding new requirements related to application-specific rule language for I&C safety systems and how it adds to the economic risk and licensing uncertainty for current licensees has not been adequately addressed. The issue causes licensees to forego updating I&C safety systems and deal with the struggle of maintaining obsolete systems or ‘work around’ regulations by developing re-engineered analog systems.
- The level of technological and architectural complexity of current and future I&C systems that may contribute towards a common cause failure (CCF) that limits, and potentially defeats, system diversity and
- Embedded digital devices (EDDs) are now being used in sensors as well as interim and final actuation devices (FADs) to complete their function. This development has blurred the line between simple electro-mechanical devices and those that may contain new failure mechanisms and thus impact new plant designs in unexpected ways. This issue was not addressed in the 2009 version of the IEEE Standard.

To counter or eliminate those concerns, the recommendations in this paper are:

- A. Develop a Strategy Document – The strategy document allows the I&C rule-making team members to formulate a mid-term and long-term strategy document that describes how to:
1. Map out all the issues the staff and industry face with regard to I&C systems.
 2. Group all these issues into manageable workgroups, based upon subject matter and expected level of effort to reach completion
 3. Develop a timeline that explains ‘how’, ‘why’ and ‘when’ these important issues related to the development and implementation of modern I&C systems, both safety and non-safety, will be formally addressed, perhaps through the use of a SECY Paper.
- B. Implement a Two-Tier Strategy – Once the strategy document has been developed, determine the best method with which to implement the strategy. This author recommends utilizing a two-tier method that allows generic safety system requirements that apply to all systems of a given type, such as IEEE Std. 603-1991, then develop additional upper tier and lower-tier ‘application-specific’ standards for those systems that utilize a specific technology or chose to develop a system or group of systems with a high level of system interconnectivity and therefore, complexity.

- C. Require Architectural Diversity – Construct I&C systems in a manner that requires designs to incorporate a minimum of two separate, diverse paths from sensor output to FAD for all I&C safety system functions (e.g. ESF functions) whose failure to actuate or actuating when system conditions do not require it, would cause the plant to exceed design limits. This requirement would be similar to the reactor trip requirements of 10 CFR 50.62. This requirement would prevent the system-level CCF that would potentially arise due to chosen system layout.
- D. Limit System Complexity – Require I&C safety systems to be only as complex as necessary to perform their functional and regulatory requirements to initiate and complete its safety function. Use of supplemental add-on features, (e.g. continuous on-line testing, system message traffic and system monitoring), that may be available due to the copious amounts of additional logic gates or unused memory within the system should be discouraged beyond the guidance in Branch Technical Position 7-14 in NUREG-0800. This requirement would enable the designers and regulators to better understand the system’s operational capabilities and failure mechanisms.

However, if the designer can demonstrate, through objective evidence and analysis, that any additional system complexity provides a significant safety benefit while only marginally raising the level of system risk, due to the higher level of system interconnectivity, and potentially lessen the degree of independence between divisions, the complex system may be found to be acceptable provided the staff evaluates the evidence and determines the adequacy and acceptability of the designer’s claims.

- E. Require a Systems-based Hazards Analysis – As contemporary system designs are more integrated and therefore, complex than in previous generations of I&C safety systems, require a detailed system wide, integrated hazard analysis to be conducted to ensure the system will cope with issues that arise from choosing a design with a highly-level of integrated systems. Additionally, the hazard analysis should include internal failure mechanisms of a given device due to the complexity of the components within the system (e.g. unused memory, unused gates, clock overrun issues etc.) to ensure those failures are precluded from interfering with or otherwise interrupting the operation of the system’s safety function.
- F. Treat Sensors and FADs as Part of the I&C System – Analyze the I&C System from sensor to FAD to ensure the level of review is commensurate with the technology utilized for the given device, including FADs.

NON-CONCURRENCE PROCESS

NCP TRACKING NUMBER

NCP-2014-004

TITLE OF SUBJECT DOCUMENT

Incorporation by Reference Institute of Electrical and Electronics Engineers Standards, 603-2009

ADAMS ACCESSION NO.

113191306

SECTION B - TO BE COMPLETED BY NON-CONCURRING INDIVIDUAL'S SUPERVISOR

NAME

Terry Jackson

TITLE

Branch Chief

PHONE NO.

(301) 415-7313

ORGANIZATION

NRO/DE/ICE1

COMMENTS FOR THE NCP REVIEWER TO CONSIDER

Immediate supervisor comments for NCP-2014-004, which was submitted by William Roggenbrodt, is provided in the attachment, "Supervisor Comments on NCP-2014-004."

CONTINUED IN SECTION D

SIGNATURE



DATE

4/22/2014

SEE SECTION E FOR IMPLEMENTATION GUIDANCE

Supervisor Comments on NCP-2014-004

Terry W. Jackson, Chief
Instrumentation, Controls, Electronics Engineering Branch 1
Division of Engineering
Office of New Reactors

EXECUTIVE SUMMARY

A non-concurrence was submitted by Mr. William Roggenbrodt regarding the incorporation of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-2009 by reference into 10 CFR 50.55a(h). Specifically, the non-concurrence is focused on the proposed rule's coverage of overall system safety for modern instrumentation and controls (I&C) systems and states the rule overlooks critical issues that have emerged as a result of contemporary I&C system technology. Currently, 10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. The non-concurrence states that if technology-specific portions of the rule are adopted, it would

- Discourage designs that optimize system safety
- Create additional regulatory burden on licensees and cause delays in new system design and implementation
- Create economic risk and technical challenges that would prevent implementation of new I&C systems
- Fail to address new failure modes created by the technological and architectural complexity of new I&C system designs

As part of this rulemaking effort, the staff reviewed IEEE Std. 603-2009 and concluded, in accordance with the process for reviewing IEEE standards, that, with conditions on its application, this standard is technically adequate, is consistent with current NRC regulatory policy, and should be used to specify regulatory criteria. The staff included several conditions on the application of IEEE Std. 603-2009 in the proposed rule to amplify and clarify the requirements imposed by the standard. They include conditions on applicability of the standard, predictability and repeatability of safety systems, independence between redundant portions of safety systems and between safety and non-safety systems, software common-cause failure (CCF), and maintenance bypass.

I appreciate the issues discussed in the non-concurrence and believe that they have been considered and discussed during the development of the proposed rule. The proposed rule does not restrict the types of technologies that can be implemented in both safety and non-safety I&C systems. However, various technologies (e.g., analog, microprocessor, and field programmable gate array (FPGA), etc.) are significantly different from one another in the system development processes, format of the function logic (e.g., arrangement of discrete electronic components versus software versus hardware description language, respectively), supporting hardware components, and operating and maintenance characteristics. Therefore, safety issues arising from these differences in characteristics between technologies could be sufficiently different that a licensee or applicant could be challenged to address issues such as electromagnetic compatibility (EMC), equipment qualification (EQ), CCF mitigation, and digital communication independence. As such, the proposed rule includes conditions on use of digital

technology to ensure that use of different digital technologies does not adversely impact the ability of I&C systems to perform their intended safety functions.

The non-concurrence provides several recommendations to address the technology-specific aspects of the proposed rule and architectural/technological complexity with modern I&C systems. The recommendations include:

- Development of a strategy document to address important I&C safety issues,
- Implement the strategy using a two-tiered regulatory model,
- Endorse the 1998 version of IEEE Std. 603 for 10 CFR 50.55a(h),
- Revert to the 1991 version of IEEE Std. 603 for 10 CFR 50.55a(h),
- Require architectural diversity,
- Limit system complexity,
- Require a systems-based hazards analysis, and
- Treat sensors, final actuation devices, and other non-traditional I&C devices as part of the I&C system.

I have evaluated the dissenting views and recommendations expressed in the non-concurrence. Based on the technical basis provided in the Statements of Consideration (SOCs) and discussed in this document, I believe that the proposed rule should go forward for public comment. The proposed criteria provide a means to address technology-specific failure modes when implementing digital-based safety systems. It is the responsibility of applicants and licensees to ensure that, for a particular technology chosen to implement in their safety I&C system, they address the safety issues associated with the technology and its applications as part of the I&C system design. The non-concurrence also addresses safety topics such as architectural diversity, complexity, and hazards analyses which the staff is currently considering. However, thorough evaluation as to the safety benefits and implications of imposing such topics as regulatory requirements has not been completed and thus inappropriate for inclusion in the current proposed rule. For example, hazards analyses are performed by various industries, but there is little guidance for assessing the adequacy of such analyses. I find that the proposed rule provides regulatory certainty and timely criteria for applicants by explicitly addressing safety issues that have been sufficiently evaluated to date. The staff plans to continue to evaluate ways to improve the I&C regulatory framework and improve on the safety criteria and its associated technical basis. The recommendations that were proposed in this non-concurrence can be considered in future regulatory infrastructure development which the staff is planning to pursue.

Table of Contents

EXECUTIVE SUMMARY	2
1 INTRODUCTION.....	5
2 SUMMARY OF DISSENTING VIEW.....	5
3 BASIS FOR INCORPORATION BY REFERENCE IEEE STD. 603-2009 AND INCLUSION OF ADDITIONAL CONDITIONS IMPOSED BY THE PROPOSED RULE	6
4 RESPONSE TO SPECIFIC ISSUES IN THE NON-CONCURRENCE	9
4.1 Use of Technology-Specific Language	9
4.1.1 Discourages Designs That Optimize Safety	10
4.1.2 Creates Additional Regulatory Burden on Licensees and Causes Delays.....	11
4.1.3 Creates Economic Risk and Technical Challenges	11
4.2 Fails to Address New Failure Modes Created by the Technological and Architectural Complexity of New I&C System Designs	12
4.2.1 Complexity.....	12
4.2.2 Systems Hazard Analysis.....	13
4.2.3 Architectural Diversity.....	13
4.2.4 Final Actuation Devices	14
4.3 Other Issues Raised by the Non-Concurrence	15
5 CONCLUSIONS AND RECOMMENDATIONS	16
REFERENCES	18

1. INTRODUCTION

On March 14, 2014, a non-concurrence was submitted by Mr. William Roggenbrodt regarding the incorporation of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std.) 603-2009 by reference into 10 CFR 50.55a(h) [1],[2]. Specifically, the non-concurrence is focused on the proposed rule's coverage of overall system safety for modern instrumentation and controls (I&C) systems and states the proposed rule overlooks critical issues that have emerged as a result of contemporary I&C system technology. This document provides a response to the non-concurrence. Contained within this document is a summary of the dissenting view; a summary of my response to the dissenting view; and a detailed response to the specific conclusions and statements provided in the non-concurrence.

2. SUMMARY OF THE DISSENTING VIEW

The non-concurrence states that the current version of the proposed rule to incorporate IEEE Std. 603-2009 by reference into 10 CFR 50.55a(h) fails to meet the threshold of adequately addressing overall system safety for modern I&C systems as it overlooks critical issues that have emerged as a result of contemporary I&C system technology. The following are the issues identified in the non-concurrence:

A. *Discourages Designs that Optimize System Safety*

"10 CFR 50.55a(h) incorporates by reference (IBR) IEEE Standard (Std.) 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The currently endorsed version, IEEE Std. 603-1991, is a "technology-neutral" standard whose criteria apply to all I&C safety systems. However, the 2009 version of IEEE 603, which the staff has proposed as the new [Incorporate by Reference] (IBR) rule, includes technology-specific language that transforms part of the 'standard' into a technology-specific document rather than a 'standard.' The new rule, as currently proposed will lead to applicants and licensees designing new I&C systems for licensing certainty rather than optimizing system safety."

B. *Creates Additional Regulatory Burden on Licensees and Causes Delays in New System Design and Implementation*

"Adding technology specific requirements into a regulation that previously applied to all I&C safety systems, regardless of technology utilized, places additional regulatory burden on licensees, and causes delays in new system designs and implementations that may result in hampering, rather than enhancing, overall plant safety."

C. *Creates Economic Risk and Technical Challenges*

"...due to the economic risk and technical challenges associated with developing and licensing new, more modern and reliable I&C systems, licensees will continue to operate

with obsolete components and systems rather than take on the risks, challenges and uncertainties associated with developing and licensing a new, more reliable I&C system due to provisions within the proposed rule language.”

D. Fails to Address New Failure Modes Created by the Technological and Architectural Complexity of New I&C System Designs

“The new rule, as currently written, is silent on how to address new failure modes created by the technological and architectural complexity of new I&C system designs. Since there is a no requirement for a systems’ hazards analysis to be conducted for these devices, some of which contain embedded digital technology, it results in the greater likelihood of common cause failures (CCFs) that have the potential to defeat system diversity. This issue was not addressed in the 2009 version of the IEEE Standard or other language within the proposed new rule.”

3. BASIS FOR INCORPORATION BY REFERENCE IEEE STD. 603-2009 AND INCLUSION OF ADDITIONAL CONDITIONS IMPOSED BY THE PROPOSED RULE

This section discusses the rationale for incorporation by reference of IEEE Std. 603-2009 and the purpose of imposing additional conditions in the proposed rule. The non-concurrence makes several recommendations, including incorporation by reference of earlier versions of IEEE Std. 603 and avoiding additional conditions that would prevent the rule from being technology neutral. The following information discusses considerations and the basis for why the 2009 version of IEEE Std. 603 was proposed for incorporation by reference into 10 CFR 50.55a(h) and why the additional conditions were included; particular those related to communication independence.

In publishing IEEE Std. 603-2009, the IEEE departed from the approach in IEEE Std. 603-1991. The IEEE Std. 603-2009:

1. Addresses potential safety issues that might arise from incorporating components that use advanced technologies in safety systems;
2. Contains additional and updated references and does not include references that are no longer in effect;
3. Provides guidance to address EMC issues;
4. Adds new criteria for CCF;
5. Contains classification requirements for equipment not credited to perform a safety function but connected to safety-related equipment;
6. Removes the requirement in Section 6.7, “Maintenance bypass,” for meeting the single failure criterion during maintenance activities; and

7. Specifically requires electrical isolation and digital communication independence between safety systems and non-safety systems.

The NRC proposes to update 10 CFR 50.55a to incorporate by reference IEEE Std. 603-2009, with conditions, in addition to retaining the incorporation by reference for IEEE Std. 279-1971, IEEE Std. 603-1991, and the IEEE Std. 603-1991 correction sheet dated January 30, 1995. As part of this rulemaking effort, the staff reviewed IEEE Std. 603-2009 and concluded that, with conditions on its application, this standard is technically adequate, is consistent with current NRC regulatory policy, and should be used to specify regulatory criteria. The staff included several conditions on the application of IEEE Std. 603-2009 in the proposed rule to amplify and clarify the requirements imposed by the standard. They include conditions on applicability of the standard, predictability and repeatability of safety systems, independence between redundant portions of safety systems and between safety and non-safety systems, CCF, and maintenance bypass.

The staff included conditions on independence between redundant portions of safety systems and between safety and non-safety systems to clarify requirements that apply to Section 5.6 of IEEE Std. 603-2009. Safety system independence is a design principle that accounts for failures and interdependencies (both known and unknown) between plant systems and helps minimize the propagation of failures and errors. To ensure independence, a safety system should not rely upon the performance or receipt of information from other external safety or non-safety systems to perform its safety function. Communications independence provides a degree of protection against hazards that may impair a safety system. Sections 5.6.3.1.a.2.ii and 5.6.3.1.b in IEEE Std. 603-2009 use the term “digital communications independence.” This term excludes consideration for technologies other than digital, which could also impair safety. Therefore, the staff clarified in the SOCs that communications independence between safety systems and other systems should be applied for all signal technologies. However, the staff recognizes that digital technologies may present unique failure modes that need to be addressed to ensure communications independence between redundant portions of safety systems and between safety and non-safety systems. Digital technology, including the use of digital communications features, may provide additional flexibility and functionality in safety and non-safety functions of nuclear power plant I&C systems. However, an integrated and interconnected digital communication system may also introduce additional unique failure modes and unexpected dependencies and behaviors. Except for very simple systems, the performance of verification testing to identify all failure modes and interdependencies (e.g., latent defects) in the digital system development process is very difficult, due to the number of input and system states that increase with the level of integration and interconnectivity. These errors and interdependencies may challenge the independence between redundant portions of safety systems and between safety systems and non-safety systems. These failure modes and dependencies may outweigh the benefits offered by the interconnectivity.

The proposed rule would clarify that the signal processing portions of the safety system should provide the capability to ensure that degradation or failure of signals exchanged among redundant safety divisions or between safety systems and other systems do not propagate in a manner that result in impairment of the safety functions being performed by the safety system. The proposed rule would also clarify that safety systems should be designed with provisions for detecting and mitigating the effects of signal faults or failures received from outside the safety division. Redundant divisions of safety systems should have the capability of tolerating such faults or failures originating from outside the safety division in a manner that does not degrade the ability of the safety division to perform its safety functions.

For new reactors, the proposed rule establishes new, specific criteria for the implementation of communications between redundant portions of safety systems and between safety and non-safety systems. This is done to limit failure modes and unexpected behaviors associated with communications, while preserving the benefits of digital technology and allowing functionality that improves reliability and availability. As a general safety engineering principle, attempts should be made to eliminate hazards when possible during the design stage. Otherwise, hazards should be mitigated. Communications that use programmable means to enforce independence could introduce additional failure modes including design errors. By implementing communication independence in the hardware architectural design, the potential for the introduction and propagation of the failures modes (e.g., design errors) and unexpected behaviors are minimized. Failure modes and unexpected behaviors can be minimized in such a design by implementing redundancy in the I&C system architecture design. It is important from a safety and licensing point of view to design systems to promote elimination of failure modes and unexpected behaviors as opposed to incorporating strategies to mitigate the results of failures. New reactor designs are able to more readily accommodate the rule as these designs do not have a current licensing basis (CLB) for an existing system that may impact the particular design. As such, paragraph (h)(5)(iii)(D) does not apply to currently operating nuclear power plant licenses or operating licenses whose construction permits were issued before the effective date of the rule. The proposed independence requirements would increase consistency of the regulatory framework for I&C systems with the Commission's policy (Federal Register Notice 73 FR 60612) on advanced reactors by having a simplified means to accomplish safety functions.

The staff proposed additional requirements in the rule to amplify the requirements stated in IEEE Std. 603-2009, Section 5.16, "Common cause failure criteria." The use of digital technology in safety systems has led to concerns that design errors could lead to software-related CCFs that might disable one or more safety functions in redundant divisions of a safety system. Errors can be introduced into a system at any stage of the system development life cycle, including specification, development of requirements, design, implementation, integration, maintenance, or modification. Faults may result from errors that are undetected until challenged by a triggering mechanism (i.e., a specific event or operating state). A fault is systemic if it exists in multiple components in

an integrated I&C system. A systemic fault becomes a CCF if a triggering event occurs that causes concurrent failures in multiple divisions of the safety system, thereby defeating one or more safety functions. Safety systems must have adequate diversity and defense-in-depth to compensate for credible CCFs and their potential effects.

4. RESPONSE TO SPECIFIC ISSUES IN THE NON-CONCURRENCE

I appreciate the issues discussed in the non-concurrence and believe that they have been mostly considered and discussed during the development of the proposed rule. In fact, some of the recommendations (e.g., a two-tiered approach) will be considered during future regulatory framework development. As described in "Supplemental Response to Advisory Committee on Reactor Safeguards Recommendation on Draft Design Specific Review Standard for mPower Small Modular Reactor integral pressurized water reactor (iPWR) Chapter 7 Instrumentation and Control Systems" (ADAMS Accession Number ML14071A121), the staff intends to develop a SECY paper to the Commission regarding a number of technical issues specific to the highly-integrated I&C systems designed for new reactors [3]. The correspondence will provide the Commission with options, which would include an option for a rulemaking for new reactors. In addition, during development of the proposed draft rule, the staff made attempts to implement technology neutral criteria to the extent possible while also addressing critical safety issues. Some of the issues require additional research and input from all stakeholders to formulate logical and technically solid requirements and guidance. The following are specific responses to concerns that were raised in the non-concurrence.

4.1 Use of Technology-Specific Language

The non-concurrence proposes that the use of technology-specific language would (1) discourage designs that optimize system safety, (2) create additional regulatory burden on licensees and cause delays, and (3) create economic risk and technical challenges. To address these issues, the non-concurrence recommends that either the 1998 version of IEEE Std. 603 be incorporated by reference or make no changes to the existing rule (e.g., keep the 1991 version of IEEE Std. 603 as the standard incorporated by reference). The following sections discuss the three particular issues listed above. It also provides a basis as to why endorsing the 1998 version or maintaining the 1991 version of IEEE Std. 603 would not satisfy the specific safety issue surrounding digital communication independence or the differing opinions surrounding it. Whether the 1998 or 2009 version of the standard is incorporated by reference, the safety issue of digital communication independence needs to be resolved to ensure adequate safety and provide a stable regulatory environment. Incorporation by reference of IEEE Std. 603-2009 would also address a number of other technical issues discussed in Section 3 of this response.

4.1.1 *Discourages Designs That Optimize System Safety*

The non-concurrence states that incorporation by reference of the 2009 version of IEEE Std. 603, which includes technology-specific language, will lead to applicants and licensees designing new I&C systems for licensing certainty rather than optimizing system safety. The non-concurrence further states that one of the unintended consequences of endorsing detailed technology-specific language in our guidance has already manifested itself in the nuclear industry by having one licensee attempt to avoid detailed regulatory guidance associated with digital systems by designing a replacement I&C system utilizing analog parts rather than digital technology that has been demonstrated to be more reliable than its analog counterparts.¹

The decision by licensees and applicants on what technology they use in their safety I&C systems can be dependent upon a number of factors, including equipment availability, maintainability, functionality, licenseability, and cost, to name a few. For the NRC, the primary goal is to ensure a reasonable assurance of safety for the technology chosen and its application as part of the overall I&C system design. Consideration is given to the cost-benefit and practicality of rules and guidance. However, primary consideration is given to safety, and in this case, by acknowledging the fact that different technologies have different inherent hazards that must be addressed.

I am not able to directly address the comment regarding how the proposed rule leads applicants and licensees to design new I&C systems for licensing certainty rather than optimizing system safety as the non-concurrence does not identify or define how it prevents applicants and licensees from optimizing their design to promote safety. As stated in Section 3 of this document, the proposed rule establishes new, specific criteria for the implementation of communications between redundant portions of safety systems and between safety and non-safety systems. These criteria limit failure modes and unexpected behaviors associated with communications, while preserving the benefits of digital technology and allowing functionality that improves reliability and availability. In addition, Section 3 also describes additional criteria needed to address the potential for software CCFs created by the use of digital technologies in safety I&C systems. The proposed rule does not restrict the types of technologies that can be implemented in both safety and non-safety I&C systems. However, various technologies (e.g., analog, microprocessor, and FPGA, etc.) are significantly different from one another in the system development processes, format of the function logic (e.g., arrangement of discrete electronic components versus software versus hardware description language, respectively), supporting hardware components, and operating and maintenance characteristics. Therefore, safety issues arising from these differences in characteristics between technologies could be sufficiently different that a licensee or applicant could be challenged to address issues such as EMC, EQ, CCF mitigation, and digital

¹ In the example cited, the non-concurrence does not identify the type of analog components used, the functionality of the system, or its architecture to provide a clear comparison to other digital I&C systems. Furthermore, the NRC staff did not complete a safety review for the system to determine its adequate safety as the plant decided to shut down permanently.

communication independence. As such, the staff determined the proposed rule should include conditions on the use of digital technology to ensure that use of different digital technologies does not adversely impact the ability of the I&C systems to perform their intended safety functions. It is the responsibility of applicants and licensees to ensure, that, for a particular technology chosen to implement in their safety I&C system, they address the safety issues associated with the technology and its applications as part of the I&C system design.

4.1.2 Creates Additional Regulatory Burden on Licensees and Causes Delays

The non-concurrence states that adding digital-based requirements into a regulation that previously applied to all I&C safety systems, regardless of technology utilized, places additional regulatory burden on licensees, and causes delays in new system designs and implementations that may result in hampering, rather than enhancing, overall plant safety.

As stated in Section 4.1.1 of this document, the proposed rule does not restrict the types of technologies that can be implemented in both safety and non-safety I&C systems. The majority of the proposed rule applies to all technologies. However, various technologies are significantly different from one another in the system development processes, format of the function logic, supporting hardware components, and operating and maintenance characteristics. Therefore, safety issues arising from these differences in characteristics between technologies could be sufficiently different that a licensee or applicant could be challenged to address issues such as EMC, EQ, CCF mitigation, and digital communication independence. As such, the proposed rule includes conditions on use of digital technologies in I&C safety systems to ensure that safety issues associated with the use of digital-based technologies do not adversely impact the ability of these systems to perform their intended safety functions. Although the staff considers the cost-benefits associated with the additional requirements in the proposed rule for digital-based systems, the primary goal of the agency is to ensure safety of the plant. Therefore, it is necessary to include these additional requirements to address the different failure modes introduced by digital technology.

Furthermore, the non-concurrence states that the proposed rule imposes a regulatory burden on licensees and applicants, but provides no evidence or cause-effect relationship to support this claim. It is the applicant's choice to select the technology best suited for their application, and it is also the applicant's responsibility to submit a quality and complete application that addresses all safety issues prior to NRC review. The staff finds that the proposed rule provides increased certainty for applicants by explicitly defining some of the safety issues that should be considered.

4.1.3 Creates Economic Risk and Technical Challenges

The non-concurrence states that due to the economic risk and technical challenges associated with developing and licensing new, more modern and reliable I&C systems, licensees will continue to operate with obsolete components and systems rather than

take on the risks, challenges and uncertainties associated with developing and licensing a new, more reliable I&C system due to provisions within the proposed rule language.

I am unable to directly address how the proposed rule will impose economic risk and technical challenges for licensees and applicants such that they will continue to operate with obsolete components and systems since the non-concurrence does not provide any evidence or cause-effect relationship to support this claim. Overall, licensees are responsible for ensuring the safe operation of their facilities which includes any necessary modifications to their I&C systems. Regulations such as 10 CFR 50.65 (“Maintenance Rule”) and 10 CFR Part 50, Appendix B, Criterion XVI, “Problem Identification and Resolution,” are in place to enforce the need to address I&C equipment issues that may exist. For new reactors, it is not anticipated that applicants will use obsolete components and systems, but will use modern digital I&C equipment as evidenced with recent designs such as AP1000, ESBWR, U.S. EPR, and US-APWR. As stated in Section 4.1.1 of this document, the proposed rule does not restrict the types of technologies that can be implemented in both safety and non-safety I&C systems, and the majority of the proposed rule applies to all technologies. Although the staff considers the cost-benefits associated with the additional requirements in the proposed rule for digital systems, the primary goal of the agency is to ensure a reasonable assurance of safety of the plant. Therefore, it is necessary to include these additional requirements to address the different failure modes introduced by digital technology.

4.2 Fails to Address New Failure Modes Created by the Technological and Architectural Complexity of New I&C System Designs

The non-concurrence states that the new rule, as currently written, is silent on how to address new failure modes created by the technological and architectural complexity of new I&C system designs. It also states that since there is no requirement for a systems’ hazards analysis to be conducted for these devices, some of which contain embedded digital technology, it results in the greater likelihood of CCFs that have the potential to defeat system diversity. The non-concurrence states that, as an example, this issue relates to priority modules and final actuation devices (FADs) containing digital technology. FADs have evolved from simple electro-mechanical devices that now contain new failure modes that impact new I&C system designs in unexpected and unanticipated ways.

4.2.1 Complexity

The non-concurrence discusses the highly-integrated nature and complexity of modern digital I&C systems. The non-concurrence recommends a requirement be established that I&C safety systems be only as complex as necessary to perform their functional and regulatory requirements. The staff considers simplicity (as compared to complexity) to be a safety engineering principle to apply to designs. However, it is considered difficult to develop a requirement and enforce simplicity at a generic level, and it is likely to require additional work to define specific criteria and requirements for simplicity. In the proposed rule and in current guidance, the staff implemented the

principle of simplicity to address specific hazards associated with I&C technology. For example, the proposed rule provides data communication independence criteria for new reactors which address potential communication hazards at the architectural level versus the more detailed design level of hardware and software. In doing so, the mechanism to ensure communication is simple to design and verify and, at the same time, eliminates the potential hazards instead of mitigating them. Guidance in Digital I&C Interim Staff Guidance 04, "Highly Integrated Control Rooms – Communication," Revision 1, Section 1, Item 3, identifies the principle of simplicity and provides guidance to not include functionality in a safety-related I&C system that is not necessary to perform the safety function [4]. Therefore, the staff has taken measures to incorporate the principle of simplicity in the I&C regulatory framework and will continue to utilize that principle as necessary based on experience and additional technical knowledge gained. However, I believe it is premature to provide a general requirement to address complexity in a proposed rule at this time; primarily when a full set of guidance is not available to support it.

4.2.2 *Systems Hazard Analysis*

I agree that the proposed draft rule does not explicitly contain requirements for a systems hazard analysis that would be beneficial to address technological and architectural complexities in new I&C system designs. However, the guidance for how to evaluate a systems hazard analysis is not mature for inclusion at this time into the proposed draft rule. The staff developed the Design-Specific Review Standard (DSRS) for review of the mPower iPWR small modular reactor, and Chapter 7 of the DSRS contains a section on hazards analysis (i.e., 7.0 Appendix A, "Instrumentation and Controls – Hazard Analysis"). The staff is working with the potential applicant of the mPower iPWR design to 'pilot' the use of hazards analysis with the goal of a more efficient and effective licensing review of the small modular reactor design. Along with this effort, the NRC and industry are also engaged in research to develop criteria for performing and assessing the results of systems hazard analysis. This work may lead to inclusion of this topic in the NRC's regulatory framework in the future. It is important to note that NRC regulations do not prevent applicants from applying systemic analysis techniques, such as hazard analysis, to support their design developments and safety demonstrations.

4.2.3 *Architectural Diversity*

The non-concurrence provides a recommendation to apply architectural diversity in safety I&C systems; from sensor to final actuation device similar to the requirements in 10 CFR 50.62, "Anticipated transient without scram." 10 CFR 50.62 requires diversity from sensor to final actuation device for reactor trip functions, but not engineered safety feature (ESF) functions. The concern raised in the non-concurrence is that lack of diversity in ESF functions, particularly those designs that use a common type of priority module for all ESF functions, may result in undue risk from CCFs. The non-concurrence notes that no regulation and limited guidance exist to analyze such conditions.

First, the staff notes that the potential for such CCFs exists today with ESF actuation systems in operating plants. Common equipment, such as relays, timers, motor starters, etc., could experience a CCF resulting in a loss of safety function. The agency considers such CCFs as beyond design basis and addresses them through programs such as the corrective action program, operating experience program, and 10 CFR Part 21 for reporting of component defects. The nuclear industry has experienced events with the potential for such CCFs in the past, such as normally-energized Agastat relay failures and oil loss in Rosemount transmitters. In these examples, the programs mentioned above were used to address the safety issues.

While the non-concurrence points out a good issue for further consideration in the regulatory framework, additional effort is needed to determine the context and safety-significance of the issue, what is the cost-benefit and impact of potential regulatory criteria, and where to place such criteria (regulations or guidance). Thus, the issue is not mature enough at this point to be included in the current rulemaking effort. The issue should be considered as part of the overall effort to pursue development of I&C regulations for new reactors, discussed earlier in this response (Section 4.2.2).

4.2.4 *Final Actuation Devices*

The non-concurrence states that “the benefit and potential consequences associated with the increased level of functionality within sensors and FADs lie outside the purview of IEEE Std. 603, and are therefore not addressed as I&C components with new types of failure modes.” I disagree with the example provided in the non-concurrence regarding how IEEE Std. 603-2009 and the proposed rule exclude consideration of FADs. As stated in both the 1991 and 2009 version of the standard, the scope of the standard includes “execute” features as well as “sense” and “command” features. As defined in the standard, execute features include “the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.” As such, the standard applies to FADs.

The non-concurrence points out that certain final actuation devices and priority modules may contain embedded digital devices. Furthermore, applicants and licensees may consider such embedded digital devices to be simple. Current guidance in Digital I&C Interim Staff Guidance 04, “Highly Integrated Control Rooms – Communication,” Revision 1, allows 100 percent testing of such simple devices; yet provides no guarantee of flawless system performance. The non-concurrence is correct in that 100 percent testing of such embedded digital devices does not prove absence of CCFs as they could still occur from sources such as hardware design errors, incorrect requirements specifications, or improper maintenance. However, it was not the goal of the guidance to address all CCFs, but to reduce the likelihood of software CCFs to such a level that the device could be treated, from a regulatory perspective, similar to analog equipment.

4.3 Other Issues Raised by the Non-Concurrence

The non-concurrence states that with the inclusion of design-specific language into a previously standardized document, the reviewer and applicant/licensee must both become increasingly fluent in what may become various design-specific data sets within standardized documents. As such, the use of technology-specific language in the standard results in less clarity and more confusion because the applicability of certain declarative statements within the document may or may not apply to different I&C safety systems. The non-concurrence also states that as the staff does not control the information incorporated into any given IEEE standard beyond its membership in IEEE, the design-specific information that has been already incorporated into the 2009 standard sets a precedent. With the possibility that the Standards Committee will continue to allow the addition of technology-specific language into a future standard, it would therefore continue to confuse the subject and its applicability to “all versus” “certain portions” of given I&C safety systems. Further, the non-concurrence states that the long-established approach related to regulation when compared to guidance deals with subject matter that flows from the generic (applies to all systems) to the specifics (applies to some systems) appears to be breaking down by allowing technology-specific language into regulation. The non-concurrence goes on to state that “True, this action has occurred before, but done so sparingly and not often with simple long-term results. In an era where designers have chosen to overly complicate I&C system designs ... beyond what regulations require, the staff’s proposed rule language inadvertently complicates our regulation.”

The rule language and associated SOCs provide explanations on applicability for each section of the proposed rule. This includes definitions and examples to illustrate the intentions of the rule. For example, paragraph (h)(5)(iii)(D)(iii) states “A safety system may receive signals from non-safety systems while the safety system is in operation only if the received signal supports diversity and automatic anticipatory reactor trip functions. These signals must be transmitted over a hardwired connection using means other than data communication.” The staff provided definitions for both hardwired and data communications in the SOCs to facilitate the application and understanding of this requirement. In addition, the majority of the draft proposed rule applies to all technologies. Only in the area of data communications independence and software CCFs does the draft proposed rule include additional conditions on safety systems that use digital-based technologies in order to address the unique failure modes of digital-based technologies. I do not believe that the limited requirements imposed by these conditions will complicate NRC regulations. In the event that designers choose complex I&C system designs, it creates the need to have these additional conditions to ensure the demonstration of safety for these highly complex I&C system designs in an effective manner.

With regard to the statement in the non-concurrence that the staff does not control the information incorporated into any given IEEE standard beyond its membership in IEEE, I respectfully disagree. Prior to incorporating by reference into NRC regulation or

endorsement through NRC regulatory guides, the staff evaluates and often provides limitations or conditions on use of industry developed standards in order to support the NRC regulatory framework and mission. If the staff finds that future versions of IEEE Std. 603 are not consistent with the NRC regulatory framework and mission, the staff may choose to not incorporate by reference those versions of the standard or incorporate by reference the standard with conditions.

5 CONCLUSIONS AND RECOMMENDATIONS

The non-concurrence states that the current version of the proposed rule to incorporate IEEE Std. 603-2009 by reference into 10 CFR 50.55a(h) fails to meet the threshold of adequately addressing overall system safety for modern I&C systems, as it overlooks critical issues that have emerged as a result of contemporary I&C system technology. The non-concurrence proposed several recommendations to address these issues. As addressed in the previous sections, the non-concurrence brings up issues worthy of consideration. I believe the issues were either adequately addressed in the rulemaking process or require additional research and consideration before moving forward with criteria in a proposed rule. The following are specific recommendations from the non-concurrence and my disposition of them.

1. Develop a strategy document – The non-concurrence recommends a strategy document to address all I&C issues. I partially agree with the recommendation. First, I conclude that the proposed rule package addresses the relevant I&C safety issues currently facing nuclear power reactors, and it should go forward for public comment in order to provide timely regulatory criteria to the industry. I do agree that the staff should continue to evaluate the state of I&C development, safety assessments, and other relevant technical developments. To this end, as described in this document, the staff is planning to draft a SECY paper to the Commission with options to address technical I&C safety issues facing new reactors. This paper will play a large part in formulating a strategy document to address I&C safety issues for the future.
2. Implement the strategy using a two-tiered regulatory model – The non-concurrence recommends a two-tiered regulatory structure for I&C regulations and guidance. The recommendation would require a fundamental change in the I&C regulatory framework and requires additional consideration before proceeding. The staff determined that such a recommendation can be considered as part of the overall strategy described earlier above.
3. Endorse the 1998 version of IEEE Std. 603 for 10 CFR 50.55a(h) – The non-concurrence suggested incorporation by reference of the earlier version of IEEE Std. 603 to avoid dissenting views on the issue of digital communication independence. However, endorsing an earlier version of the standard would not resolve the safety issue surrounding digital communication independence or the differing opinions surrounding it. Whether the 1998 or 2009 version of the

standard is incorporated by reference, the safety issue of digital communication independence needs to be resolved to ensure adequate safety and provide a stable regulatory environment.

4. Revert to the 1991 version of IEEE Std. 603 for 10 CFR 50.55a(h) – Similar to the recommendation above, the non-concurrence also suggests keeping the current state of 10 CFR 50.55a(h) as it would avoid technology-specific criteria. As pointed out in the SOCs of the proposed rule and this document, there are safety reasons for addressing aspects of certain technologies that may be used in nuclear power reactors. In addition, the SOCs identify other bases for updating the rule, including when to use updated criteria for digital upgrades and treatment of software CCFs.
5. Require architectural diversity – To address potential CCFs in I&C systems where common types of equipment may be used (particularly for ESF actuation), the non-concurrence recommends that criteria be developed similar to 10 CFR 50.62 to require diversity for ESF actuation from sensor to FAD. While treatment of CCFs has been beyond design basis and typically addressed by programs such as the corrective action program, 10 CFR Part 21, and operating experience, the staff will continue evaluating regulatory criteria associated with CCFs. As discussed in this document, the staff should first understand the impact of imposing diversity on ESF actuation systems; particularly the safety benefit gained versus potential impact to safety. The staff believes this recommendation can be considered as part of the overall strategy development described earlier.
6. Limit system complexity – As noted in the non-concurrence, modern digital I&C systems are complex and highly integrated as compared to I&C systems in current reactors. The non-concurrence suggests that the staff place a requirement limiting the functionality performed on safety I&C systems to essentially those associated with safety functions. I agree that the principle of reducing complexity benefits safety. However, addressing complexity on a generic basis is difficult to achieve given the interface, functionality, and responsibilities of a safety I&C system. I believe the principle of simplicity has been incorporated in the draft proposed rule as evidenced by its criteria for communication independence for new reactors. Additional research and evaluation is needed to determine where the principle of simplicity can be further applied to the regulatory framework. The principle of simplicity should be considered for future I&C regulatory development as described earlier.
7. Require a systems-based hazards analysis – The non-concurrence recommends that system-based hazards analysis be required for I&C systems. Current guidance addresses certain hazards analysis, including single failure analysis and defense-in-depth and diversity analysis. The non-concurrence is correct that there are a number of systems-based hazards analyses that have been used.

The staff is currently evaluating the use of systems-based hazard analyses and is piloting such an effort with the mPower design-specific review standard. The staff notes there is little guidance on assessment of a systems-based hazard analyses by regulatory bodies, and the staff is currently conducting research to improve upon that guidance. As such, I believe it would not be appropriate to require systems-based hazards analysis in the current proposed rule without the accompanying review guidance. However, the staff should consider systems-based hazard analysis in future I&C regulatory framework development as described earlier.

8. Treat sensors, FADs, and other non-traditional I&C devices as part of the I&C system – The non-concurrence recommends that the staff analyze the I&C system from sensor to FAD to ensure the level of review is commensurate with the technology utilized for the given device. As described in this document, IEEE Std. 603-2009 is applicable to I&C components from sensor to FAD and there is current guidance available to address those components. The staff continues to evaluate new technology entering nuclear power reactors and will consider embedded digital devices when developing future changes to the I&C regulatory framework.

I evaluated the dissenting views expressed in the non-concurrence. Based on the technical basis provided in the Statements of Consideration (SOCs) and discussed in this document, I believe that the proposed rule should go forward for public comment. The proposed criteria provide a means to address technology-specific failure modes when implementing digital-based safety systems. It is the responsibility of applicants and licensees to ensure that for a particular technology chosen to implement in their safety I&C system, they address the safety issues associated with the technology and its applications as part of the I&C system design. I find that the proposed rule will provide certainty and timely criteria for applicants by explicitly defining some of the safety issues that should be considered. I also find that many of the proposed recommendations in the non-concurrence, such as development of a strategy document and criteria for systems-base hazards analysis, have merit and should be considered in future regulatory infrastructure development.

REFERENCES

1. W. Roggenbrodt. "Position Paper on Staff Update to 10 CFR 50.55a(h) Rule Affecting I&C Systems," U.S. Nuclear Regulatory Commission, ADAMS Accession No. ML113191306, March 2014.
2. U.S. Nuclear Regulatory Commission, "Rulemaking: FRN: Proposed Rule Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard, 603-2009," U.S. Nuclear Regulatory Commission, ADAMS Accession No. ML113191306, February 2014.
3. Letter from Mark Satorius, EDO, to John Stetkar, ACRS Chair, "Supplemental Response to Advisory Committee on Reactor Safeguards Recommendation on Draft Design Specific

Review Standard for mPower Small Modular Reactor iPWR Chapter 7 Instrumentation and Control Systems,” ADAMS Accession No. ML14071A121, April, 2014.

4. U.S. Nuclear Regulatory Commission, “Digital I&C Interim Staff Guidance 04: Highly Integrated Control Rooms – Communication,” Revision 1, ADAMS Accession No. ML ML083310185.

NON-CONCURRENCE PROCESS

NCP TRACKING NUMBER
NCP 2014-004

TITLE OF SUBJECT DOCUMENT

Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009

ADAMS ACCESSION NO.
ML113191306

SECTION C - TO BE COMPLETED BY DOCUMENT SPONSOR

NAME

Patrick L. Hiland

TITLE

Division Director

PHONE NO.

(301) 415-3298

ORGANIZATION

Office of NRR, Division of Engineering

SUMMARY OF ISSUES

Document Sponsor's comments for NCP 2014-001, NCP 2014-003, and NCP 2014-004, are provided in a consolidated report, "Actions taken to address Non-concurrences NCP-2014-001, NCP-2014-003 and NCP 2014-004 to the Draft Rulemaking for incorporation by reference of IEEE Std. 603-2009." See attached.

ACTIONS TAKEN TO ADDRESS NON-CONCURRENCE

Document Sponsor's comments for NCP 2014-001, NCP 2014-003, and NCP 2014-004, are provided in a consolidated report, "Actions taken to address Non-concurrences NCP-2014-001, NCP-2014-003 and NCP 2014-004 to the Draft Rulemaking for incorporation by reference of IEEE Std. 603-2009." See attached.

SIGNATURE--DOCUMENT SPONSOR

Patrick L. Hiland

TITLE

Division Director

ORGANIZATION

NRR/DE

DATE

6/22/15
John W. Wanski

SIGNATURE--NCP REVIEWER

Daniel H. Jones

TITLE

ACTING DIRECTOR

ORGANIZATION

NRR

DATE

10/3/2014

NCP OUTCOME

SEE COVER PAGE

Non-Concurring Individual: CONCURS NON-CONCURS WITHDRAWS NON-CONCURRENCE (i.e., discontinues process)

AVAILABILITY OF NCP FORM

Non-Concurring Individual: WANTS NCP FORM PUBLIC WANTS NCP FORM NON-PUBLIC

CONTINUED IN SECTION D

SEE SECTION E FOR IMPLEMENTATION GUIDANCE

Actions taken to address Non-concurrences NCP-2014-001, NCP-2014-003 and NCP 2014-004 to the Draft Rulemaking for incorporation by reference of IEEE Std. 603-2009

Background

As part of its role to ensure public health and safety, the U.S. Nuclear Regulatory Commission (NRC) routinely updates its regulations and guidance to ensure that the agency incorporates the current technology, maintains appropriate references, and improves regulatory efficiency and predictability. In January 2007, the NRC initiated a project to improve the regulatory efficiency and predictability of licensing digital Instrumentation and Control (I&C) safety systems in new and existing nuclear power plants. During a Commission meeting the previous November, the industry panel expressed concerns over the ability to license digital I&C safety systems and implement certain NRC policies regarding digital I&C. As a result, the Digital I&C project was initiated, and through this project, the NRC developed, over a five year period, seven I&C Interim Staff Guidance (ISG) documents to provide additional clarification for successful implementation of digital I&C systems. One of the long term goals of the project was to draft more permanent guidance that would incorporate the ISGs into existing NRC regulatory guidance. Most of the ISGs have been incorporated into NRC regulatory guides, however, ISG-04, digital system communications, has not been incorporated into the targeted regulatory guide (RG), RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

Shortly after its publication, the NRC began consideration of incorporating by reference the updated version of the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-2009, "IEEE Standard Criteria for Safety Systems in Nuclear Power Generating Station (IEEE Std. 603-2009)." The applicable regulation that incorporates a previous version of this standard (IEEE Std. 603-1991) is 10 CFR 50.55a(h). IEEE Std. 603-1991 is a voluntary consensus standard that has been incorporated by reference into NRC regulations to establish functional and design requirements for safety systems for nuclear power plants since 1999. Previously, IEEE Standard 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," (IEEE Std. 279) was used. Incorporation by reference of IEEE Std. 603-2009 would be consistent with the provisions of the National Technology Transfer and Advancement Act of 1995, which encourages Federal regulatory agencies to consider adopting voluntary consensus standards as an alternative to de novo (from the beginning) agency development of standards.

In 2010, the NRC formed a working group including technical representatives from the Office of Nuclear Reactor Regulation (NRR), the Office of New Reactors (NRO), and the Office of Regulatory Research (RES), and representatives for the Office of the General Council and rulemaking project management. The working group reviewed IEEE Std. 603-2009 to determine its acceptability for incorporation by reference in the NRC regulations, and it concluded that, while the standard is technically adequate and consistent with the current NRC regulatory process, several conditions needed to be included to clarify and augment several acceptance criteria and the applicability of IEEE Std. 603-2009. During the evaluation of IEEE Std. 603-2009, the working group sought to develop practical solutions to ensure safety and address the various technical issues identified. The working group addressed a number of challenging technical issues and was able to arrive at a consensus position on most of these issues; however despite extensive working group efforts, it became clear by the summer of 2012 that the working group was having problems reaching a consensus on some of technical issues, the most challenging of which was digital system communication independence.

To assist the rulemaking working group in developing potential solutions in the area of independence, NRC senior management issued a memorandum on July 5, 2012 (Agencywide Document Access and Management System Accession No. ML12187A208), to encourage the working group to develop a common solution to provide a level of safety that meets the minimum needs of the various members of the working group and consistent with the NRC principles of good regulation. At the same time, the Senior Technical Advisors for this area in both NRR and NRO were tasked with developing potential “out-of-the-box” solutions to assist the rulemaking working group in developing a common solution.

By memorandum dated October 19, 2012 (ML12293A106), the Senior Technical Advisors provided their input to the working group and Senior Management. The working group used the recommendations provided to restart discussion on digital system independence and other issues and incorporated some of the Senior Technical Advisors’ recommendations, such as the enhanced use of hazards analysis as part of the preliminary draft proposed rule text, however the primary recommendation to provide a graded approach to digital system independence requirements based on system architecture was not adopted. The working group continued to explore options that could resolve the differences of technical judgment between working group members on the topics of digital system communications, diversity requirements, and other issues based primarily on regulatory experience on recent digital system upgrades to operating reactors such as the Oconee reactor protection and engineer safeguards actuation system and new reactor reviews such as the AREVA U.S. Evolutionary Pressurized Reactor (EPR). The most recent evolution was the proposal to bifurcate the rule to have one requirement for digital system independence for new reactors and a different requirement for modifications and upgrades to I&C systems in operating reactor reviews. In the end, the rulemaking steering committee determined that sufficient consensus existed to move the preliminary draft proposed rule text to the concurrence process. As part of the concurrence process, three non-concurrences have been filed by eleven (11) individuals from the instrumentation and control branches in NRR and NRO including three (3) of the original five (5) working group members. The non-concurrences, which involved digital system communications, the adequacy of diversity requirements, the use of technology-specific language in the standard, and the need for enhanced hazards analysis, are summarized below.

Summary of Issues

Summary of Issues (NCP-2014-001)

The non-concurring staff objects to the inclusion of restrictions on data communications for the digital I&C safety systems for new reactors in the current version of the proposed rule to incorporate by reference IEEE Std. 603-2009. The non-concurring staff believes the proposed criterion for communication independence is contrary to fourteen years of regulatory precedent that has been successfully applied to operating nuclear power plants, and that no technical basis has been provided to demonstrate that current regulatory practices are either adverse to public health, safety, or security or to warrant the use of different regulatory requirements for the use of digital communications technology in new reactors. The proposed rule would institute a different set of regulations for new reactors that would not be applied to operating plants, which the non-concurring staff believes would promote inconsistencies between operating and new reactor plants and discourage the nuclear industry from using available technologies to enhance safety system performance. The non-concurring staff proposes to ensure safety of digital

communication through incorporation of IEEE Std. 603-2009 without the exception for independence and incorporation of IEEE 7-4.3.2-2010 (which has been updated to include ISG-4) in a revision of Reg. Guide 1.152.

Summary of Issues (NCP-2014-003)

The non-concurring staff objects to the inclusion of restrictions on data communications for the digital I&C safety systems for new reactors in the current version of the proposed rule to incorporate by reference IEEE Std. 603-2009. The non-concurring staff believes the proposed criteria for communication independence are intended to simplify the regulatory decision making process for new reactor I&C systems by prescriptively specifying the design of the applicant's I&C data communication architecture, thus reducing the need for staff judgment when applying the regulations. The non-concurring staff believes the opposite may turn out to be the case, because applicants will choose to request alternatives under 50.55a(z), making reviews more challenging and adding to regulatory uncertainty. The reviews, in this case, would need to be completed outside of established guidance and staff review plans. The non-concurring staff is also concerned that the prescriptive nature of the data communication clauses in the proposed rule is being used to supersede staff judgment, where use of the staff's reasoned judgment would better serve the goal of ensuring safety. The non-concurring staff proposes to ensure safety of digital communication through incorporation of IEEE 7-4.3.2-2010 in RG 1.152.

Summary of Issues (NCP-2014-004)

The non-concurring staff objects to the currently proposed rulemaking because it fails to adequately address several technical issues that the staff and licensees face when designing and evaluating new I&C systems. The non-concurring staff believes that additional steps must be taken in order to ensure the regulations remain current, precise and comprehensive enough to provide reasonable assurance of safety. The non-concurring staff believes that including by reference IEEE Std. 603-2009, that includes some technology-specific language, will lead applicants and licensees to design new I&C systems for licensing considerations rather than optimizing system safety and could result in unintended consequences for both the staff and industry. Additionally, the non-concurring staff believes that adding technology specific requirements in the proposed regulation that previously applied to all I&C safety systems places additional regulatory burden on licensees and causes delays in new system designs and implementation that may result in hampering, rather than enhancing overall plant safety. Additionally, the non-concurring staff asserts that such requirements may add to regulatory uncertainty causing licensees and applicants to forego updating I&C safety systems and instead opt for maintaining obsolete systems.

The non-concurring staff believes that new technology and the level of complexity of current and future I&C systems may contribute to common cause failures that are not addressed in the proposed rule and could defeat system diversity. Additionally, the non-concurring staff believes that embedded digital devices that are now being used in sensors as well as final actuation devices are not adequately addressed in the proposed rule, and that system complexity is also not sufficiently addressed. This staff member is concerned that since there is no requirement for systems' hazards analysis to be conducted for these devices (sensors, priority modules and final actuation devices), there is a greater likelihood of common cause failures that have the potential to defeat systems diversity, because these devices contain new failure modes that impact new I&C system designs in unexpected and unanticipated ways.

The non-concurring staff proposes re-examining the issues cited above and developing rule language that proactively addresses the greater range of safety concerns as outlined in the non-concurrence. To counter or eliminate these concerns, the non-concurring staff recommends that the staff develop a two tiered strategy that would first allow generic safety system requirements, applicable to all systems of a given type, such as IEEE Std. 603-1991, and then would develop additional upper tier and lower tier “application-specific” standards for those systems that utilize a specific technology. Further, the non-concurring staff recommends rulemaking that would revise the current diversity requirements, to require all I&C safety systems to incorporate a minimum of two separate, diverse paths from sensor output to final actuation device for all I&C safety system functions (trip and ESF functions) whose failure to actuate, or whose actuation when system conditions do not require it, would cause the plant to exceed design limits. The non-concurring staff’s recommendation would be to also add additional hazards analysis requirements to support a better understanding of system operational capabilities and failure mechanisms. The diversity requirements and the analysis of the I&C safety systems would have to include all components from sensor to final actuation device to ensure the level of review is commensurate with the technology utilized for the given device, including the final actuation devices.

Actions taken to address each of the issues and rationale for resolution of non-concurrences

In non-concurrence NCP-2014-001 and 2014-003, the non-concurring staff proposes to ensure the safety of digital communication through incorporation of IEEE Std.603-2009 without exception to the criteria for independence, and incorporation of IEEE 7-4.3.2-2010 in a revision of Reg. Guide 1.152. While I agree with the non-concurring staff that to add more prescriptive requirements for data communication for new reactors is a significant change to past regulatory precedent that has been successfully applied to current and new reactors, I believe that the proposed rule text can be successfully implemented. The draft proposed rule text for digital communication in new reactors provides regulations that will ensure safety while providing greater predictability in the licensing process. Additionally, as pointed out by the non-concurring staff, I understand that the proposed rule text would preclude some future digital safety system designs that may in fact be as safe, or safer, than those outlined in the rule forcing an applicant to request and justify an alternative. I believe that the added regulatory predictability for both the staff and the applicants outweighs the associated uncertainty necessarily caused by applicants pursuing this path as delineated in Title 10 of *The Code of Federal Regulations* (10 CFR) 50.55a(z) rather than the new requirements for digital communications provided in 10CFR 50.55a(h)(5)(iii)(D).

This may add to the uncertainty associated with new reactor I&C reviews but the NRC staff has reviewed digital systems based on the less prescriptive requirements associated with IEEE Std. 603-1991 for many years and can do so in the future, so I believe that the increased licensing certainty of the new rule outweighs this argument. To help mitigate this concern, as part of implementing changes associated with the new rule, the staff will consider enhancing standard review plan (NUREG-0800) Chapter 7 guidance to provide to support this possibility. Although, as pointed out in the non-concurrence, the proposed restrictions on digital communications may affect the opportunity to use some of the features of advanced communication technologies to improve safety for new reactors, it has been the experience of the Office of New Reactors that the need to request an alternative to the incorporated standard and additional requirements is

less of a burden than that experienced by other members of the working group working primarily in the Office of Nuclear Reactor Regulation.

The non-concurring staff points to the Commission's direction in staff requirement memorandums (SRM)-M061108, which established the Digital I&C Steering Committee and the Digital I&C Project in 2007. This effort was a proactive effort by the NRC to work with the industry to provide additional guidance associated with how licensees and applicants could meet NRC requirements for digital systems and reduce licensing uncertainty associated with the use of these systems. As part of this effort, as pointed out by the non-concurring staff, the NRC developed ISG-04 (ML083310185), which established acceptable methods for incorporating communication features into digital systems. The staff used this guidance to license digital I&C systems portions of which would not be permitted for new reactors under the provisions of the proposed 10 CFR 50.55a(h)(5)(iii)(D). The non-concurring staff pointed out that to implement this provision of the proposed draft rule will be a significant change to the direction set in the ISG and by inference the SRM. However, as discussed in SECY-09-0061, the staff always planned to update the final guidance after the "staff gains experience with the use of the ISGs through current reviews" and "the SRP, regulatory guides, and other regulatory guidance will be revised to incorporate the ISGs and **lessons learned** (emphasis added)." The experience that new reactor reviewers have had regarding this area has led me to believe that the added regulatory certainty associated with the proposed draft rule language is a lesson learned in this area and is a valid reason for adding this additional regulatory requirement for new reactors.

However, because the non-concurrence packages make reasonable assertions regarding the possible negative impact of the proposed draft rulemaking on safety and regulatory predictability, the rulemaking package has been modified to elicit input from the public to better inform the agency regarding several of the issues raised. The following questions have been added to the "Specific Request for Comments" section of the rulemaking package:

- 1) Will the proposed bifurcation of the independence requirements (50.55a(h)(5)) provide more regulatory certainty for new and current reactor I&C designs? Are there better ways to achieve independence with regulatory certainty? What additional guidance is necessary to implement the proposed criteria?
- 2) How likely is it that applicants and licensees will use the alternative process (as provided in the 50.55a(z) associated with the new requirements for "independence" (IEEE Std. 603-2009, section 5.6)? In what respects would alternatives be sought and what would be the basis for seeking the alternatives? Will the proposed rule language act to limit different design solutions to address independence?
- 3) Will the added requirements and restrictions on digital communications independence discourage the nuclear industry from using available technologies to enhance safety system performance or replace aging and obsolete safety systems?
- 4) Will different requirements for digital system independence for new and current reactors lead to inconsistencies between reactor designs that will impact safety or the ability of the NRC to effectively carry out inspections or regulatory reviews? Will this difference between new and operating reactor I&C review criteria improve regulatory certainty?

Also as part of the public comment process, the NRC will proactively engage the public by holding one or more public workshops to discuss the proposed rule and provide opportunities for all stakeholders to discuss and comment on these and other parts of the proposed rule text. The public workshop(s) will use these and other questions associated with the proposed changes to the rule to discuss the rulemaking and the issues discussed in the non-concurrences as part of the public comment process.

In non-concurrence NCP-2014-004, the non-concurring staff proposes to not go forward with the proposed rulemaking and rethink a number of technical issues before moving forward with a new rulemaking package. The non-concurring staff objects to the currently proposed rulemaking because it fails to adequately address several technical issues that the staff and licensees face when designing and evaluating new I&C systems. While I agree with the non-concurring staff that there are a number of technical issues that have not been fully resolved by this proposed draft rulemaking, I am not persuaded that the rulemaking should be abandoned at this point.

One of the non-concurring staff concerns is that by referencing, IEEE Std. 603-2009, that includes some technology-specific language, will lead to applicants and licensees to design new I&C systems for ease of licensing rather than optimizing system safety and thus result in unintended consequences for both the staff and industry. Although there has been some inclusion of technology-specific language in IEEE Std. 603-2009, I believe it will not have a significant impact on current I&C designs or the designs that the NRC will review for the next several years. In discussions with members of the IEEE Standards organization, I am informed that the Nuclear Power Engineering Council is already reviewing a proposal for the next revision of IEEE Std. 603 that is to be completed in 2018 or 2019. I am also informed that the current plan for revision to the standard includes removal of the technology specific language as part of the next revision. Based on this information and likelihood that the NRC will review this new revision of the standard, I have determined not to revise the draft proposed rule text to address this issue at this time. The non-concurring staff also believes that adding technology specific requirements in the proposed regulation that previously applied to all I&C safety systems places additional regulatory burden on licensees and causes delays in new system designs and implementation. I do not believe the level of added technology specific requirements will result in this effect but will carefully review public comments in this area to ensure we have not underestimated this concern.

The non-concurring staff believes that new technology and the level of complexity of current and future I&C systems may contribute to common cause failures that are not addressed in the draft proposed rule and could defeat system diversity. Additionally, the non-concurring staff believes that embedded digital devices are not sufficiently addressed nor is the need for systems' hazards analysis. The staff is moving forward with a Regulatory Information Summary (RIS) on embedded digital devices that will partially address the concerns raised by the non-concurring staff. This RIS will highlight to the licensees and applicants the need to address embedded digital devices and adequately review their potential failure modes. The agency is also moving to more proactively address the identified need to better address digital system hazards analysis. In addition to the sections in the proposed draft rule text associated with hazards analysis (50.55a(h)(5)(i) and (ii)), the NRC's efforts include ongoing research into this area being conducted in the Office of Nuclear Regulatory Research (RES) and its contractors. To date, this effort has informed NRO's development of the Design Specific Review Standard for mPower and will be used to inform the next revision of the Standard Review Plan (NUREG-

0800) Chapter 7. Therefore, although I agree that these issues are of concern, I believe the current efforts underway within the agency will adequately address the non-concurring staff's issues with embedded digital devices and hazards analysis.

With respect to the non-concurring staff's concern that new technology and the level of complexity of current and future I&C system may contribute to areas that are not addressed in the draft proposed rule text associated with common cause failures, I agree. The current position on digital system common cause failures was provided in a Commission Paper (SECY 93-087) and the Commission's staff requirements memorandum responding to that Commission Paper (SECY 93-087) and represents the technical and regulatory thinking on the subject at that time. Because of the significant changes to the technology since that time, including the expanded use of Field Programmable Gate Array (FPGA) and similar technologies, new methods and tools, and significant operational experience associated with the use of digital systems in nuclear power plants and other fields, the assumptions provided in SECY 93-087 are outdated and likely in need of reevaluation. Therefore, I have removed the diversity requirement from the rulemaking text (50.55a(h)(6)) and plan to provide the commission a paper proposing a new rulemaking effort (already prioritized as NRR-40) that will look at a number of issues including some discussed by the non-concurring staff, such as the sufficiency of overall system level diversity. Issues would include the changes to the state of the art in digital system technology since the Commission policy on digital system diversity was established in SECY 93-087 such as FPGAs, the need to incorporate diverse paths from sensor output to final actuation device for all I&C safety system functions (trip and ESF functions) and the emergence of embedded digital devices in nuclear power plant I&C channels from smart sensors to final actuation devices.

Finally, the non-concurring staff recommends that the staff develop a two tiered strategy that allows generic safety system requirements, that applies to all systems of a given type, such as IEEE Std. 603-1991, then develop additional upper tier and lower tier "application-specific" standards for those systems that utilize a specific technology, similar to the strategy used by the International Electrotechnical Commission (IEC) standards. The NRC is familiar with the IEC standards and has a representative on the IEC standards committees that develop the IEC-61513 series of standards discussed in non-concurrence NCP-2014-004. Although I appreciate the non-concurring staff's perspective on this structure and understand the potential benefit, I do not believe that it is practical at this time to completely revise the NRC's structure to parallel the IEC structure. However, because I agree that there is merit to this line of argument; NRR is currently preparing a User Need Request for RES to prepare a regulatory guide that would address FPGAs and similar Hardware Description Languages based technology. If successful, this regulatory guide would serve as a second tier guidance document parallel to RG 1.152 for software based systems under IEEE Std. 603-2009. In this way, the NRC would move to a structure that would, at least partially, parallel the IEC structure in which IEC-61513 serves as the higher level standard and IEC-60880 and IEC-62566 serve as the lower tier standards as proposed by the non-concurring staff.