WILLIAM R. GROSS
Director, Incident Preparedness

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8123
wrg@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

May 14, 2020

Mr. Russell Felts
Acting Director, Division of Physical and Cyber Security Policy
Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: NRC Review of NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety-Related and Important-to-Safety Functions," Dated May 2020

Project Number: 689

Dear Mr. Felts:

By letter dated July 27, 2012,[1] the Nuclear Regulatory Commission (NRC) found NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012, acceptable for use by licensees to identify critical digital systems and critical digital assets. By letter dated September 7, 2017,[2] the NRC found NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017, acceptable for use by licensees to address the security controls provided in their cyber security plans. Lessons learned through the implementation of cyber security programs indicate that guidance improvements are necessary to enhance clarity, enable efficient and consistent program implementation and to support NRC oversight activities.

Accordingly, the Nuclear Energy Institute (NEI),[3] on behalf of its members, is submitting the attached white paper proposing changes to NEI 10-04 and NEI 13-10 for NRC review. The attached white paper describes proposed changes to previously approved NEI guidance for identifying and protecting Safety-Related and Important-to-Safety Critical Digital Assets. The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks, up to and including the design basis threat. The attached document provides a technical basis for the changes and provides a markup of the relevant

[1] ADAMS Accession No. ML12194A532

[2] ADAMS Accession No. ML17240A002

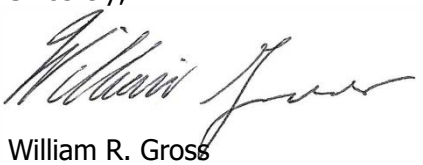
[3] The Nuclear Energy Institute (NEI) is the organization responsible for establishing unified industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all entities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel cycle facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

changes made to NEI 10-04 and NEI 13-10. The markup does not include all minor editorial and conforming changes. All changes will be incorporated into future revisions of NEI 10-04 and NEI 13-10.

NEI requests that the NRC review the NEI White Paper, "Changes to NEI 10-04 and NEI 13-10 Guidance for Identifying and Protecting Digital Assets Associated with Safety-Related and Important-to-Safety Functions," dated May 2020, by June 29, 2020. While each licensee must review changes to their Commission-approved Cyber Security Plan in accordance with the requirements of 10 CFR 50.54(p), NEI requests that the NRC's review confirm that the changes proposed in this white paper do not decrease the effectiveness of the cyber security plan provided in NEI 08-09. If any revisions to this document are desired, please include suggested wording and the technical data to support the proposed change(s).

If you have any questions or require additional information, please contact Richard Mogavero, at (202) 739-8174 or rm@nei.org, or me.

Sincerely,



William R. Gross
Attachment

c: Mr. James D. Beardsley, NSIR/CSD, NRC
NRC Document Control Desk

1 INTRODUCTION

1.1 PURPOSE

This white paper describes proposed changes to previously approved NEI guidance for identifying and protecting Safety-Related (SR) and Important-to-Safety Critical Digital Assets (CDAs). The changes are intended to improve the efficiency of licensee cyber security programs while maintaining program effectiveness to protect against cyber attacks, up to and including the design basis threat. The described changes affect, and will be incorporated into a future revision to:

- NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule," Revision 2, dated July 2012, and
- NEI 13-10, "Cyber Security Control Assessments," Revision 6, dated August 2017.

1.2 BACKGROUND

Title 10 of the Code of Federal Regulations (CFR), Part 73, "Physical Protection of Plants and Materials," § 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires power reactor licensees to provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in § 73.1, "Purpose and scope." Through implementation of the cyber security plans and programs required by § 73.54, the industry has identified several lessons learned that warrant an assessment and revision of the guidance in NEI 10-04, Revision 2 and NEI 13-10, Revision 6. This white paper describes proposed changes to NEI 10-04 and NEI 13-10 that would support more efficient performance of cyber security program activities, oversight, and promote consistent implementation of the requirement of § 73.54.

2 DISCUSSION

Within the scope of 10CFR73.54, the guidance provided here presents an objective methodology and process for identification of certain systems and equipment within the cyber security rule's scope that must be protected from cyber attacks as described in § 73.54 (b)(1). The systems and equipment are those performing or supporting Safety-Related (SR) or Important-to-Safety functions, or whose failure could adversely affect the satisfactory performance of SR or Important-to-Safety functions. The process relies on the current regulatory framework and guidance for identification of SR and Important-to-Safety systems and equipment. The fundamental goal of the guidance is to assure that the facility can be operated without undue risk to the health and safety of the public in the event of a cyber attack up to and including the design basis threat.

The identification of Safety-Related and Important-to-Safety systems and equipment is based on regulatory guidance contained in 10CFR50.2 (Definitions), 10CFR50 Appendix A (General Design Criteria (GDC) for Nuclear Power Plants); 10CFR50.49 (Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants); and Generic Letter 84-01, "NRC Use of the Terms, "Important-to-Safety" and "Safety-Related". Additionally, 10CFR54.4 (Scope) of 'Requirements for Renewal of Operating Licenses for Nuclear Power Plants'; (a)(2) and (a)(3) along with GL 84-01 is used to help identify Important-to-Safety systems and equipment.

Many sites' classification procedures have included criteria that identify systems and equipment as SR that do not perform SR functions. This has occurred to allow support of certain programmatic requirements typically applicable to SR systems and equipment. This was done so that sites did not need to create separate Quality Assurance (QA) programs specific to these systems and equipment. Examples of this equipment could include electrical equipment powered from 1E Safeguard power supply, instrumentation classified under Regulatory Guide (RG) 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants," and equipment with environmental or seismic qualification.

2.1 TERMINOLOGY

The terms utilized below contain historical context and are consistent with their current use.

Safety-Related

Safety-Related classification of systems and equipment has been performed and completed at each nuclear facility in support of requirements in 10CFR50 App B and other program requirements. Below is the definition of Safety-Related from 10CFR50.2:

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

In addition to the 10CFR50.2 definition, SR systems and equipment also include any other systems and equipment whose postulated failure during the Design Bases Events (DBEs) could prevent satisfactory accomplishment of the SR function described above.

Important-to-Safety

This term was initially described in Generic Letter 84-01 as part of the NRC's response to an industry concerned raised by the Utility Safety Classification Group (USCG); specifically, that the term Important-to-Safety was used in various regulatory documents, yet it was not defined. The USCG claimed that Important-to-Safety should be considered equivalent in meaning to Safety-Related. The Generic Letter refuted this claim but did not go so far as to provide a definition. The Generic Letter 84-01 stated:

> *NRC regulatory jurisdiction involving a safety matter is not controlled by the use of terms such as "safety-related" and "important to safety," and our conclusion that pursuant to our regulations, nuclear power plant … licensees are responsible for developing and implementing quality assurance programs for … plant operation which meet the more general requirements of General Design Criterion 1 for plant equipment "important to safety,"...*

> *...normal industry practice is generally acceptable for most equipment not covered by Appendix B within this class. Nevertheless, in specific situations in the past where we have found that quality assurance requirements beyond normal industry practice were needed for equipment "important to safety," we have not hesitated in imposing additional requirements commensurate with the importance to safety of the equipment involved. We intend to continue that practice.*

Although Generic Letter 84-01 did not result in adding an Important-to-Safety definition within 10CFR50.2, it did state that current industry practice has been acceptable and additional quality assurance requirements will be imposed if determined otherwise. Over the past 40 years this was evident by in the issuance of various regulatory guidance and regulations including RG 1.155, "Station Blackout" (SBO), 10CFR50.63, "Loss of All Alternating Current Power," GL 83-28, "Required Actions Based on Generic Implications of Salem ATWS Events," 10CFR50.62, "Anticipated Transient Without SCRAM (ATWS), 10CFR50.48, Fire Protection, 10CFR50.49 "Environmental Qualification," including certain post-accident monitoring equipment in RG 1.97 and applicable provisions in Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants."

2.2 CLASSIFICATION METHODOLOGY

As mentioned above, sites already have procedural guidance for identification of SR systems and equipment and other systems and equipment to which the 10CFR50 Appendix B QA Program requirements are applied. Briefly, this guidance is based on the 10CFR50.2 SR definition.

In addition to the 10CFR50.2 definition, SR systems and equipment should also include any other systems and equipment whose postulated failure during the DBEs could prevent satisfactory accomplishment of the SR function described above. DBEs for the context of this guidance includes events that are a condition of normal operation, including anticipated operational occurrences, design basis accidents or transients, external events, or natural phenomena for which the plant must be designed to ensure the three-basic safety-related functions are achieved.

Important-to-Safety systems and equipment includes any Non-Safety Related (NSR) systems and equipment whose failure under postulated environmental conditions, 10CFR50.49, could prevent satisfactory accomplishment of the SR function described above. Important-to-Safety systems and equipment also include those systems and equipment required to address postulated events described in the NRC regulations including Fire, SBO and ATWS events.

Identification of systems and equipment performing SR and Important-to-Safety functions is performed as follows. The classification steps are to be considered in the sequence presented and include the context from previous steps and tiers:

1. Identify under the Current Licensing Basis (CLB) the list of DBEs applicable to the system or equipment under consideration.
2. Identify systems and equipment that are credited in the DBE safety analyses for satisfying SR definition elements (i.e., maintain Reactor Coolant Pressure Boundary (RCPB), shutdown the reactor, maintain safe shutdown condition or the capability to prevent or mitigate the

consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11). Note that these systems and equipment are identified as SR.

3. Identify those systems and equipment that are required to support the functionality and operability (e.g. cooling water, lube oil, HVAC, electrical, etc.) of the systems and equipment identified in Step 2. Note that these systems and equipment are also identified as SR.

4. Identify any CLB commitments where a system or equipment is classified as SR. These systems and equipment are also determined to be SR under this guidance document.

5. Identify NSR systems and equipment that functionally interface (including digital pathways) with the SR systems and equipment. Determine if a compromise by cyber attack of the NSR system and equipment interfacing with the SR function could prevent or adversely impact the performance of the SR function, then identify the NSR equipment as a CDA for protection as SR equipment.

6. If identified SR systems and equipment contain a digital component that, if compromised, could adversely impact the proper operation of the identified SR systems and equipment, then the digital component is a SR CDA. **(REPEAT STEPS 2 THRU 6 FOR EACH DBE IDENTIFIED IN STEP 1)**

7. Identify any NSR systems and equipment that are used to meet the CLB commitments to assure the integrity of the RCPB, the capability to shutdown the reactor, or maintain it in a safe shutdown condition e.g., commitments for Fire Protection Program (FPP), SBO Analysis, ATWS Analysis and EQ Program. These systems and equipment are identified as Important-to-Safety.
    a. Identify systems and equipment required or credited in response to each of the following:
        i. For ATWS Analysis, identify systems and equipment required for complying with 10CFR50.62
        ii. For SBO Analysis, identify systems and equipment utilized in mitigating the SBO event per 10CFR50.63, and systems and equipment that support bringing the unit(s) to and maintain in safe shutdown.
        iii. For FPP, identify FP systems and equipment related to protecting systems and equipment required for bringing the unit(s) to and maintain in safe shutdown; and the FP systems and equipment (detection/suppression) used in response to a fire in areas containing SR equipment to comply with applicable fire protection requirements (10 CFR 50.48, 10 CFR 50 Appendix R, or GDC 3). These FP SSCs are important-to-safety systems and equipment.
        iv. For EQ (10CFR50.49), identify NSR electrical equipment whose failure under postulated environmental conditions could prevent satisfactory accomplishment of the SR function of electrical equipment; and certain equipment, per

10CFR50.49(b)(3) that must be qualified to perform a post-accident monitoring function in a harsh environment based on RG 1.97 Cat 1 and 2 classification.

8. Identify the systems and equipment that are credited or required to support the systems and equipment identified in Step 7. Identify these items as Important-to-Safety.

9. Identify NSR systems and equipment that functionally interface (including digital pathways) with the Important-to-Safety equipment. Determine if a compromise by cyber attack of the NSR equipment interfacing with the Important-to-Safety equipment could adversely impact the Important-to-Safety function, then identify the NSR equipment as a CDA for protection as Important-to-Safety equipment.
10. If identified Important-to-Safety systems and equipment contain a digital component that if compromised by a cyber attack, could adversely impact the proper operation of the identified Important-to-Safety systems and equipment, the digital component is an Important-to-Safety CDA.

3 COMPLIANCE WITH REGULATORY REQUIREMENTS

10 CFR 73.54(a)(1)(i) and (iv) require that licensees protect against cyber-attacks those digital computer and communication systems and networks associated with safety-related and important-to-safety functions, and support systems and equipment which, if compromised, would adversely impact safety functions.

10 CFR 73.54(b)(1) requires that licensees analyze digital computer and communication systems and networks and identify those assets that must be protected against cyber-attacks to satisfy 10 CFR 73.54(a).

10 CFR 73.54(b)(2) requires the licensee to establish, implement, and maintain a cyber security program for the protection of the assets identified in 10 CFR 73.54(b)(1).

With the incorporation of the proposed changes described in this document, a cyber security plan and program would ensure that:

a) Digital assets associated with SR and Important-to-Safety functions, and their respective support systems and equipment described in 10 CFR 73.54(a)(1)(i) and (iv) are analyzed as required by 10 CFR 73.54(b)(1).
b) Where the analysis determines that a cyber-attack would adversely impact SR or Important-to-Safety functions, those digital assets would be protected against cyber-attacks as required by 10 CFR 73.54(b)(2).

Licensee implementation of the changes discussed in this white paper will not decrease the effectiveness of a cyber security plan or compliance with the requirements of 10 CFR 73.54. The cyber security program will remain capable of protecting digital computer and communication systems and networks associated with SR and Important-to-Safety functions, and support systems

and equipment against cyber-attacks, up to and including the design basis threat as described in §73.1. The updated approach meets the intent of 10 CFR 73.54(b)(1). The analysis of SR and Important-to-Safety digital computer and communication systems and networks will identify those assets that must be protected against cyber-attacks to satisfy 10 CFR 73.54 (a).

The identification of SR and Important-to-Safety systems and equipment, is based on regulatory guidance contained in 10CFR50.2, “Definitions”; 10CFR50 Appendix A, “General Design Criteria”; and Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”; 10CFR50.49, “Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants”; certain post-accident monitoring equipment in RG 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident"; Generic Letter 83-28, “Required Actions Based on Generic Implications of Salem ATWS Events”; 10CFR50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants”; 10CFR50.48, “Fire Protection”; RG 1.155, “Station Blackout” (SBO) and 10CFR50.63, “Loss of alternating current power”, and Generic Letter 84-01, “NRC Use of the Terms, "Important-to-Safety" and "Safety-Related". Additionally, 10CFR54.4 of ‘Requirements for Renewal of Operating Licenses for Nuclear Power Plants’; (a)(2) and (a)(3) along with GL 84-01 is used to help identify Important-to-Safety systems and equipment.

Following implementation of the changes, CDAs associated with, or supporting, SR and Important-to-Safety functions can be assessed to determine if the CDAs continue to meet their current definitions. Previous screenings of CDAs associated with SR and Important-to-Safety functions may be credited. The revised guidance will identify Important-to-Safety CDAs based on the licensee’s Current Licensing Basis. The analysis will consider all applicable functional requirements described in the Current Licensing Basis.

In summary, it is expected that a licensee’s evaluation of necessary changes to their security plans could conclude the change does not:

- Affect compliance with any regulatory requirement including Safety-Related and Important-to-Safety requirements,
- Decrease the effectiveness of the Physical Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, and/or Cyber Security Plan, and does not
- Decrease the overall capability of Cyber Security program to adequately protect against cyber attacks, up to and including the design basis threat as described in § 73.1.

4 CHANGES TO NEI 10-04

NEI 10-04, “Identifying Systems and Assets Subject to the Cyber Security Rule,” Revision 2, provides guidance for determining whether a system and associated digital assets are subject to the requirements of 10 CFR 73.54. Protection as a CDA is required for those assets which would adversely impact Safety, Security and Emergency Preparedness (SSEP) functions if compromised by a cyber attack.

The following sections of NEI 10-04, Revision 2, will be revised to better align a licensee's cyber security program scope with the requirements in 10 CFR 73.54 for the protection of SR and Important-to-Safety functions.

[Proposed changes in redline/strikeout]
A paragraph with a 'bullet' is an explanation of the changes to the revised section. The indented text that is black, red or lined-out indicates original NEI 10-04 text, added text or deleted text, respectively.

Section 1.1 Overview of Scoping for the NRC Cyber Security Rule

- Section 1.1 is revised to include editorial changes to terminology. Additionally, it adds footnotes to define new terms used. It also provides clarity on the scope of 'Support Systems'.

The NRC Cyber Security Rule requires the identification of digital computer and communications systems, equipment and networks associated with Safety-related and Important-to-Safety functions, Security functions, Emergency Preparedness functions including offsite communication (SSEP), and support systems and equipment which, if compromised, would adversely impact SSEP functions. NEI 10-04 uses guidance from available references to support the identification of assets meeting the criteria of 10 CFR 73.54. In summary, the following functional references and rationale are used as a basis for the conclusions in this document.

1. Safety-Related and Important-to-Safety functions can be determined from ~~are defined in~~ each plant's Current Licensing Basis (CLB)[1] documents (e.g., Final Safety Analysis Report, licensing commitments[2], etc.).

2. Security functions necessary to prevent significant core damage and spent fuel sabotage are identified based on criteria described in 10 CFR 73.55. Site-specific commitments can be identified in licensee Physical Security Plans.

3. Emergency preparedness functions, including offsite communications necessary to respond to a radiological emergency are described in 10 CFR 50.47 (b) and Appendix E to Part 50. Site-specific commitments can be found in licensee Emergency Plans.

(Footnotes will be placed in the footer of the page where paragraphs numbered 1 and 2 reside)

1 Current Licensing Basis documents (CLB): The set of documents that specify the licensing requirements and commitments that form the basis used by the U.S. Nuclear Regulatory Commission (NRC) to license a nuclear power plant or a standard plant design.

2 Licensing commitment is a commitment specified in the plant CLB (e.g., a commitment to apply specific design criteria to an item or to implement the licensing guidance provided by NRC in a Generic Letter or Regulatory Guide).

For the purposes of Cyber Security, ~~the introduction of~~ the term "Support System and Equipment," are those systems and equipment credited or required for performance of the systems and equipment which perform SSEP functions. ~~as related to SSEP functions is a new classification unique to the NRC Cyber Security Rule.~~ These are systems and equipment which, if compromised, would adversely impact safety, important-to-safety, security, or emergency preparedness functions. In this context "safety" refers to Safety-Related ~~SSC~~ systems and equipment functions

Section 1.2 "Use of NEI 10-04"

- Section 1.2 is revised to delete paragraph six (6) in its entirety. This paragraph explained the purpose and use of Appendices A and B at the end of NEI 10-04 Revision 2. This revision deletes Appendices A and B completely, therefore no longer requiring paragraph six (6) of section 1.2.

~~Appendices A and B provide an example categorization of plant systems using the guidance in this document. These examples were derived principally from Maintenance Rule documentation and are not comprehensive. Licensees must conduct a site-specific analysis of digital computer and communication systems and networks to identify CDAs that must be protected.~~

Section 2.1 "Safety-Related and Important-To-Safety"

- Section 2.1 is revised to add clarification and historical relevancy to the terms in section 2.1.1 and 2.1.2. The first paragraph is revised to further explain how some non-Safety Related equipment were categorized within the Safety-Related scope because a site did not choose to create a separate Quality Assurance program for these specific equipment items. It states how this guidance can be used to separate out those non-Safety-Related equipment items currently categorized as Safety-Related. The second paragraph supports referencing section 2.1.2 for Important-to-Safety systems.

In the context of 10 CFR 73.54, identifying assets associated with Safety-Related and Important-to-Safety functions requires consideration of ~~not just safety and important-to-safety systems, but~~ those non-Safety-Related systems and equipment that can affect Safety-Related or Important-to-Safety functions, including those Balance of Plant (BOP) systems and equipment that can impact reactivity.

The identification of Safety-Related systems and equipment has already been performed by each licensee in support of the requirements of 10CFR50 Appendix B and other program requirements. Many sites' classification procedures have included criteria that identifies systems and equipment as SR that do not perform SR functions. This has occurred to allow support of certain programmatic requirements typically applicable to SR systems and equipment. This was done so that sites did not need to create separate Quality Assurance

(QA) programs specific to these systems and equipment. Examples of this equipment could include electrical equipment powered from 1E Safeguard power supply, instrumentation classified under Regulatory Guide (RG) 1.97, and equipment with environmental or seismic qualification.

~~An identification of safety-related and important-to-safety systems has been made by licensee and can be found in their current licensing and design basis documentation.~~

Section 2.1.1 “Safety-Related”

- Section 2.1.1 is revised to add a fourth paragraph at the end of the section which is a blanket statement to capture any systems or equipment whose postulated failure during a Design Basis Event could prevent the accomplishment of the Safety-Related function.

In addition to the 10CFR50.2 definition, SR systems and equipment also include any other systems and equipment whose postulated failure during the Design Bases Events (DBEs) could prevent satisfactory accomplishment of the SR function described above.

Section 2.1.2 “Important-To-Safety”

- Section 2.1.2 is revised to provide clarification on the historical basis for the term Important-To-Safety when compared to Safety-Related. It identifies regulatory rules/programs issued over time that reflect the position established in Generic Letter 84-01.

~~Each licensee has, over time, developed a working application of the term important-to-safety in their licensing basis. Licensees should rely on their site-specific application in the identification of important-to-safety systems. Systems that perform important-to-safety functions should include those that are required to maintain diversity and defense-in-depth for safety functions (e.g., the diverse actuation system and credited diverse display systems). Licenses may have identified important-to-safety systems during renewal under the criteria in 10 CFR 54.4 (a)(2) and (a)(3).~~

The identification of Important-to-Safety systems and equipment is based on regulatory guidance contained in Generic Letter 84-01, NRC Use of the Terms, "Important-to-Safety" and "Safety-Related"; 10CFR50.49; and 10CFR54.4 (a)(2) and (a)(3).

Generic Letter 84-01 was developed in response to a concern raised by the Utility Safety Classification Group; specifically, that the term Important-to-Safety was used in various regulatory documents, yet it was not defined. The Utility Safety Classification Group claimed that Important-to-Safety should be considered equivalent in meaning to Safety-Related. The Generic Letter refuted this claim; however, the Generic Letter did not go so far as to provide a definition. The Generic Letter 84-01 stated:

> *NRC regulatory jurisdiction involving a safety matter is not controlled by the use of terms such as "safety-related" and "important to safety," and our conclusion that pursuant to*

our regulations, nuclear power plant … licensees are responsible for developing and implementing quality assurance programs for … plant operation which meet the more general requirements of General Design Criterion 1 for plant equipment "important to safety,"…

…normal industry practice is generally acceptable for most equipment not covered by Appendix B within this class. Nevertheless, in specific situations in the past where we have found that quality assurance requirements beyond normal industry practice were needed for equipment "important to safety," we have not hesitated in imposing additional requirements commensurate with the importance to safety of the equipment involved. We intend to continue that practice

Although Generic Letter 84-01 did not result in adding an Important-to-Safety definition within 10CFR50.2, it did state that current industry practice has been acceptable and additional quality assurance requirements will be imposed if determined otherwise. Over the past 40 years this can be seen in the issuance of various regulatory guidance and regulations including RG 1.155, "Station Blackout" (SBO), 10CFR50.63, "Loss of All Alternating Current Power," GL 83-28, "Required Actions Based on Generic Implications of Salem ATWS Events," 10CFR50.62, "Anticipated Transient Without SCRAM (ATWS), 10CFR50.48, Fire Protection, 10CFR50.49 "Environmental Qualification," including certain post-accident monitoring equipment in RG 1.97 and applicable provisions in Appendix A to Part 50, "General Design Criteria for Nuclear Power Plants."

- Section 2.1.2 (paragraph 6) is revised, removing Technical Specifications and Maintenance Rule Documentation out of Important-to-Safety as a reference category.

References to aid in identifying Safety-Related and Important-to-Safety systems may include but not limited to:

a) FSAR
b) UFSAR
c) Design Basis documents
d) Deleted ~~Technical Specifications~~
e) Licensee commitments with respect to RG 1.97, "Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants"
f) Deleted ~~Maintenance Rule documentation~~
g) Licensee formal communications to the NRC (e.g., responses to Generic Communications or NRC Orders)

Section 2.4 "Support Systems and Equipment"

- Section 2.4 is revised is provide clarification on SSCs that are considered 'support systems.'

The NRC Cyber Security Rule requires protection from cyber attack assets associated with support systems and equipment which, if compromised, would adversely impact Safety-Related, Important-to-Safety, Security, or Emergency Preparedness functions.

Support systems ~~as~~ and equipment to be protected include, for example, those required to provide ~~a stable~~ an environment ~~conducive~~ to assure the operational requirements of systems performing ~~associated with~~ SSEP functions, or provide motive force (e.g., pneumatic, hydraulic, electrical) for the required performance of SSEP functions.

Separately, other systems and equipment that do not directly support the operational requirements of the SSEP function, but ~~or that~~, if compromised, would potentially adversely impact systems and equipment performing SSEP functions, are to be evaluated for protection. For example, malfunction or operation of a non-Safety-Related system or equipment ~~SSC~~ ~~which could~~ whose failure during the DBE could prevent satisfactory accomplishment ~~compromise the performance~~ of a Safety-Related system or equipment performing a Safety-Related function.

The determination of required or credited support systems, networks, and equipment can be found in a site's current licensing and design basis documentation.

For example, support systems and equipment may include, but not be limited to, the following:

a) Electrical Power systems whether primary or backup
b) HVAC systems
~~c) Fire protection systems~~
d) Secondary Power for Detection and Assessment Equipment
e) Diesel Generator lube oil systems ~~Support systems and equipment that are required to maintain diversity and defense-in-depth for safety functions (e.g., the diverse actuation system and credited diverse display systems).~~

Section 4 "Methodology for Identifying and Classifying Plant Systems

- Section 4 is revised to clarify the definition of 'Safety-Related System,' remove the reference to Appendices A and B which are being deleted. This section also provides a definition for and clarifies the relationship of Important-to-Safety to a licensee's system that coincides with the revised discussion in section 2.1.2. The guidance for identifying Important-to-Safety systems in questions 1-4 and 6 are removed from this section and relocated to Section 5.

  This section provides a methodology for identifying and classifying plant systems to determine the regulatory categorization of those systems. The goal of this section is to provide the method used for screening plant systems to determine whether the systems fall under the NRC's Cyber Security Rule. Systems that fall under the Cyber Security Rule are referred to as Critical Systems (CS). A site-specific evaluation of systems must be performed utilizing the licensee's CLB.

  ~~Appendix A and B provide examples of plant systems that have been categorized during the development of this document using the questions in Section 4. The results are listed in Appendix A for a typical Pressurized Water Reactor (PWR) and Appendix B for a typical~~

~~Boiling Water Reactor (BWR). These examples were derived principally from Maintenance Rule documentation and are not comprehensive. A site-specific evaluation of systems must be performed utilized the licensees CLB.~~

CATEGORIZATION OF PLANT SYSTEMS

SAFETY-RELATED

Is this system relied upon to remain functional during and following DBEs ~~design basis events (as defined in 10 CFR 50.49(b) (1))~~ to ensure:

1. The integrity of the reactor coolant pressure boundary?
2. The capability to shut down the reactor and maintain it in a safe shutdown condition?
3. The capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in 10 CFR 50.34(a)(1), 10 CFR 50.67(b)(2), or 10 CFR 100.11?

For purposes of this guidance, only systems are being considered. Systems are considered Safety-Related within the scope of the 10CFR73.54, if at least one of the system's design functions, as documented in the site's CLB, or other system design documents, is classified as Safety-Related.

IMPORTANT-TO-SAFETY

For purposes of this guidance, the Important-to-Safety equipment and functions are not specific plant systems but are typically part of existing plant systems and functions. Important-to-Safety equipment is NSR equipment that is used to meet the CLB commitments to assure the integrity of the RCPB, the capability to shutdown the reactor and maintain it in a safe shutdown condition (e.g., commitments for Fire Protection, SBO, ATWS and EQ).

See Section 5 for detailed screening of Important-to-Safety systems and equipment.

~~1. Is this a non-safety related system whose failure could adversely impact any of the functions identified in the previous three "Safety Systems" questions?~~
~~2. Is this a non-safety related system that is part of the primary success path and functions or actuates to mitigate a transient that either assumes the failure of or presents a challenge to the integrity a fission product barrier?~~
~~3. Has operating experience or a probabilistic risk assessment shown that a non-safety related system function is significant to public health and safety?~~
~~4. Does the non-safety related system function to provide real-time or near-real-time plant status information to the operators for the safe operation of the plant during transients, and accidents?~~
~~6. Is this a non-safety system required to maintain defense-in-depth and diversity requirements?~~

Section 5 "Methodology for Identifying Critical Digital Assets"

- Section 5 is revised to remove reference to source documents because they are not used to define the functions of systems in accordance with the CLB. The additional guidance provides historical NRC guidance on Safety-Related and Important-to-Safety. Additionally, the changes removed fire protection as an example of a support function and provides a classification methodology for identifying SR and Important-to-Safety CDAs.

  This section provides a methodology for identifying and classifying plant equipment performing SR or Important-to-Safety functions to determine the regulatory categorization of equipment. The goal of this section is to provide the method used for screening plant equipment to identify digital SR or Important-to-Safety equipment that would fall under the NRC's Cyber Security Rule. Digital equipment that falls under the Cyber Security Rule is referred to as a Critical Digital Asset (CDA).
  ~~The section describes an acceptable method to consistently identify Critical Digital Assets (CDA). There are a number of sources from which the meaning of the terms "digital" and "Critical Digital Asset" can be either explicitly or implicitly deduced, including 10 CFR 73.54; NEI 08-09, "Cyber Security Plan for Nuclear Power Reactors," Revision 6; Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," dated January 2010; Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2; IEEE 7-4.3.2-2003, and "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."~~

  Appendix B of NEI 08-09, Revision 6 defines a Critical Digital Asset (CDA) as a digital computer, communication system, or network that is:

  - A component of a critical system (this includes assets that perform SSEP functions; provide support to, protect, or provide a pathway to Critical Systems); or
  - A support system asset whose failure or compromise as the result of a cyber attack would result in an adverse impact to a SSEP Function.

  The following interpretation is consistent across various sources and provides an approach for identifying those digital assets that are associated with SSEP functions and are required to be protected from cyber attacks in accordance with 10 CFR 73.54.

  A digital asset may be identified as a programmable device (e.g., EPROM, microprocessor, etc.) that uses any combination of hardware, firmware and/or software to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action. Solid state devices (e.g., electro-mechanical on/off devices, relays, hard-wired logic devices, circuit boards, etc.) that do not have firmware and/or software are not considered digital devices.

  A digital device that communicates to a CDA need not be classified as a CDA simply due to the connectivity pathway. If the compromise of the digital asset can be used to

compromise a CDA, then the digital asset should be classified as a CDA. Where cyber security controls, implemented in accordance with CSP Section 3.1.6 for the CDA, address the threats associated with the pathway (i.e., the attack vector no longer exists to the CDA), then the digital device does not need to be classified as a CDA.

A digital device should be identified as a Critical Digital Asset (CDA) if it performs:

a) SSEP functions or whose compromise would adversely impact a SSEP function;
b) Balance of Plant ~~important-to-safety~~ functions whose compromise would result in an unplanned reactor shutdown or transient;
c) Support functions (e.g., primary or back-up power, HVAC, ~~fire protection,~~ etc.) whose compromise would adversely impact a SSEP function; or
d) Network boundary isolation, protection, or detection/prevention monitoring functions for CDAs as described in Section 4.3, "Defense-in-Depth Protective Strategies," of the licensee's Cyber Security Plan.

Identification of systems and equipment performing SR or Important-to-Safety functions is performed as follows. The classification steps are to be considered in the sequence presented and include the context from previous steps and tiers:

1. Identify under the Current Licensing Basis (CLB) the list of DBEs applicable to the system or equipment under consideration.
2. Identify systems and equipment that are credited in that DBE safety analyses for satisfying SR definition elements (i.e., maintain Reactor Coolant Pressure Boundary (RCPB), shutdown the reactor, maintain safe shutdown condition or the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to the applicable guideline exposures set forth in § 50.34(a)(1) or § 100.11). Note that these systems and equipment are identified as SR.
3. Identify those systems and equipment that are required to support the functionality and operability (e.g. cooling water, lube oil, HVAC, electrical, etc.) of the systems and equipment identified in Step 2. Note that these systems and equipment are also identified as SR.
4. Identify any CLB commitments where a system or equipment is classified as SR. These systems and equipment are also determined to be SR under this guidance document.
5. Identify NSR systems and equipment that functionally interface (including digital pathways) with the SR systems and equipment. Determine if a compromise by cyber attack of the NSR system and equipment interfacing with the SR function could

prevent or adversely impact the performance of the SR function, then identify the NSR equipment as a CDA for protection as SR equipment.

6. If identified SR systems and equipment contain a digital component that if compromised could adversely impact the proper operation of the identified SR systems and equipment, then the digital component is a SR CDA. **(REPEAT STEPS 2 THRU 6 FOR EACH DBE IDENTIFIED IN STEP 1)**

7. Identify any NSR systems and equipment that are used to meet the CLB commitments to assure the integrity of the RCPB, the capability to shutdown the reactor, or maintain it in a safe shutdown condition e.g., commitments for Fire Protection Program (FPP), SBO Analysis, ATWS Analysis and EQ Program. These systems and equipment are identified as Important-to-Safety.
    a. Identify systems and equipment required or credited in response to each of the following:
        i. For ATWS Analysis, identify systems and equipment required for complying with 10CFR50.62
        ii. For SBO Analysis, identify systems and equipment utilized in mitigating the SBO event per 10CFR50.63, and systems and equipment that support bringing the unit(s) to and maintain in safe shutdown.
        iii. For FPP, identify FP systems and equipment related to protecting systems and equipment required for bringing the unit(s) to and maintain in safe shutdown; and the FP systems and equipment (detection/suppression) used in response to a fire in areas containing SR equipment to comply with applicable fire protection requirements (10 CFR 50.48, 10 CFR 50 Appendix R, or GDC 3). These FP SSCs are important-to-safety systems and equipment.
        iv. For EQ (10CFR50.49), identify NSR electrical equipment whose failure under postulated environmental conditions could prevent satisfactory accomplishment of the SR function of electrical equipment; and certain equipment, per 10CFR50.49(b)(3) that must be qualified to perform a post-accident monitoring function in a harsh environment based on RG 1.97 Cat 1 and 2 classification.

8. Identify the systems and equipment that are credited or required to support the systems and equipment identified in Step 7. Identify these items as Important-to-Safety.

9. Identify NSR systems and equipment that functionally interface (including digital pathways) with the Important-to-Safety equipment. Determine if a compromise by cyber attack of the NSR equipment interfacing with the Important-to-Safety

equipment could adversely impact the Important-to-Safety function, then identify the NSR equipment as a CDA for protection as Important-to-Safety equipment.

10. If identified Important-to-Safety systems and equipment contain a digital component that if compromised by a cyber attack, could adversely impact the proper operation of the identified Important-to-Safety systems and equipment, the digital component is an Important-to-Safety CDA.

Licensees should note the following:

1) The above guidance should not inhibit the licensee from designating a component with multiple digital devices or a network containing multiple digital devices as a single CDA. However, the licensee must justify that protective requirements of the Cyber Security Plan are satisfied for these configurations.
2) The licensee may find a single digital device type associated with more than one Critical System, and that these Critical Systems perform different SSEP functions (e.g., safety-related and emergency preparedness).

Appendix A

- Appendix A in its entirety was deleted and replaced with a historical place marking.

[Appendix A DELETED]

Appendix B

- Appendix B in its entirety was deleted and replaced with a historical place marking.

[Appendix B DELETED]

5 CHANGES TO NEI 13-10

Changes to NEI 13-10, "Cyber Security Control Assessments," Revision 6, are required to integrate the CDA classification changes being made to NEI 10-04 as discussed in this white paper. The specific conforming changes to NEI 13-10 to address the changes in NEI 10-04 related to SR and ITS functions will be identified when NEI 13-10, Revision 7 is prepared. NEI 13-10, Revision 7, will involve integration of changes from the NEI Tiger Team initiatives for SR/ITS, EP, BOP and Security functions if and after the NRC endorses changes based on these initiatives. Changes included in NEI 13-10, Revision 7 will require separate NRC review and will consider prior NRC endorsements of changes to NEI 10-04. Therefore, specific changes to NEI 13-10 related to the SR and ITS classification guidance in this white paper are not included.