U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-01

Task Working Group #1:
Cyber Security

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-01

Task Working Group #1:
Cyber Security

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

OFFICE	DI&C/TWG1	DI&C/TWG/D	OGC/NLO	NRO/DE	NSIR/DSP
NAME	MGareri	PSilva	RWeisman	MMayfield	SMorris
DATE	12/13/ 07	12/14/07	12/31/07	12/17/07	12/14/07
OFFICE	RES/DFERR	NMSS/FCSS	NRR/ADES		
NAME	JUhle	JGiitter	JGrobe		
DATE	12/18/07	12/17/07	12/14/07		

DIGITAL INSTRUMENTATION AND CONTROLS

DI&C-ISG-01

Task Working Group #1:
Cyber Security

Interim Staff Guidance

Revision 0
(Initial Issue for Use)

IMPLEMENTATION

Except in those cases in which an applicant or licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the NRC staff will use the methods described in this Interim Staff Guidance (ISG) to evaluate applicant and licensee compliance with NRC requirements as presented in submittals in connection with applications for standard plant design certifications and combined licenses.

This ISG provides acceptable methods for addressing Cyber Security in digital I&C system designs. This guidance is consistent with current Commission policy on digital I&C systems and is not intended to be a substitute for NRC requirements, but to clarify how a licensee or applicant may satisfy those regulations.

This ISG also clarifies the criteria the staff will use to evaluate whether an applicant or licensee digital system design is consistent with cyber security guidelines. The staff intends to continue interacting with stakeholders to refine digital I&C ISGs and to update associated guidance and generate new guidance where appropriate.

CYBER SECURITY ASSOCIATED WITH
DIGITAL INSTRUMENTATION AND CONTROLS
DI&C-ISG-01

1. ISSUE

The nuclear power industry requested clarification of differences in guidance associated with implementation of cyber security programs at nuclear power plants. Specifically, the industry asserted that Regulatory Positions 2.1-2.9 provided within Regulatory Guide 1.152 Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants*, conflicts with the industry-developed, NRC-accepted guidance in NEI 04-04 *Cyber Security Program for Power Reactors, Revision 1,* with regard to the protection of safety-related digital instrumentation and control systems.

This issue is addressed in the Interim Staff Guidance (ISG) provided below and Appendix A and B as follows:

> Appendix A: RG 1.152 (Rev. 2) and draft NEI 04-04 (Rev. 2) Cross-Correlation Table, (Agencywide Documents Access and Management System (ADAMS) Accession No. ML072980164, not publicly available)
>
> Appendix B: Draft NEI 04-04, Rev. 2, Cyber Security Program for Power Reactors (ADAMS Accession No. ML073461212, not publicly available)

2. PURPOSE:

The purpose of this ISG is to clarify the NRC staff's guidance with regard to the implementation of cyber security measures for nuclear power plant safety systems.

3. BACKGROUND

In response to the terrorist attacks of September 11, 2001, and information provided subsequently by intelligence and law enforcement agencies, the NRC completed the following actions to enhance the protection of power reactors from both physical and cyber threats:

A. NRC Order EA-02-026*, Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants,* February 2002

   This order specified numerous interim compensatory measures to address the elevated threat environment. Part of this order contained cyber security requirements mandating nuclear power plant licensees to identify digital systems critical to the safe operation of the facility, and to evaluate the potential consequences to the facility should these systems be compromised. The material aspects of EA-02-026 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

B. NRC Order EA-03-086*, Design Basis Threat for Radiological Sabotage,* April 2003

   This order supplemented the Design Basis Threat (DBT) for nuclear power plants specified in 10 CFR 73.1. Among other things, this order established requirements for the development of a cyber security program at each nuclear power plant. The material aspects of EA-03-086 are withheld from public disclosure in accordance with 10 CFR 73.21, "Requirements for the Protection of Safeguards Information."

C. NUREG/CR-6847*, Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants,* October 2004

The NRC staff, assisted by its contractor, the Pacific Northwest National Laboratory developed a cyber security self-assessment methodology that could be used by licensees to assess the risk to systems deemed critical to the operation of nuclear power plants. The method was developed utilizing a multidisciplinary team that included nuclear power industry personnel. The material aspects of NUREG/CR-6847 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

D. NEI 04-04 Revision 1*, Cyber Security Program for Power Reactors,* November 2005

The NRC staff reviewed the Nuclear Energy institute (NEI) guidance in NEI 04-04, Rev. 1, and commented on that guidance. In a letter dated December 23, 2005 the NRC staff notified NEI that NEI 04-04 Rev. 1, is an acceptable method for establishing and maintaining a cyber security program at nuclear power plants. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

E. Regulatory Guide 1.152 Revision 2*, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* January 2006

This document provides specific cyber security guidance for nuclear power plant licensees in the development and implementation of protection measures for digital instrumentation and controls used in safety system applications. This guidance addressed aspects of the implementation of cyber security within safety systems that were not covered adequately in IEEE Standard 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.*

F. Branch Technical Position 7-14 Revision 5, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems,* March 2007

This document provides NRC staff review guidelines for evaluating software life-cycle processes associated with safety-related digital instrumentation and control systems at nuclear power plants. It also addresses characteristics that should be present within an acceptable software management plan (e.g., licensees should provide a description of the methods employed to prevent corruption of the software by viruses, Trojan horses, or other malicious intrusions).

G. 72 Federal Register 12705*, Design Basis Threat – Final Rule,* March 19, 2007

This final rule requires licensees to protect against "cyber attacks."

H. NEI 04-04 Revision 2*, Cyber Security Program for Power Reactors,* August 2007

Following numerous discussions with the NRC staff, NEI revised NEI 04-04 primarily to clarify cyber security guidance for safety-related digital instrumentation and control systems. The material aspects of NEI 04-04 are withheld from public disclosure in accordance with 10 CFR 2.390, "*Public Inspections, Exemptions, Requests for Withholding*."

I. 71 Federal Register 62664*, Power Reactor Security Requirements - Proposed Rule,* October 26, 2006

The Commission has also proposed new cyber security requirements for nuclear power plants in a proposed regulation, 10 CFR 73.55 (m). The proposed regulation maintains the intent of the previously issued security orders (i.e., EA-02-026 and EA-03-086) and would require licensees and applicants to implement an effective program to detect and prevent cyber attacks on plant computer systems associated with safety, security, and emergency response.

4. DISCUSSION

Subsequent to the issuance of NEI 04-04 Rev. 1, as nuclear power plant licensees worked to identify and implement security enhancements to further secure their facilities from internal and external cyber threats, the industry identified differences between certain guidance provided in Regulatory Guide 1.152 and in NEI 04-04, Rev. 1. The details of these differences are not described here because NEI 04-04 Rev. 1 is designated as 10 CFR 2.390 information that is exempt from public release under the Freedom of Information Act (5 U.S.C. 522).

In October 2006, the NRC staff, NEI, and industry representatives met to discuss methods to resolve the differences among the various guidance documents listed above. Subsequently, an NRC Task Working Group (TWG) was established to address these issues and to ensure that the cyber security guidance provided was coherent and consistent for both existing licensees and future applicants for combined operating licenses.

To resolve the differences between Regulatory Guide 1.152 and NEI 04-04, the TWG conducted a "gap" analysis, identifying areas in which the two documents overlapped and were inconsistent. The gap analysis concentrated on Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev.2 and the programmatic elements of NEI 04-04 Rev. 1. The TWG also reviewed previously issued cyber security guidance to identify other possible areas of inconsistency.

The TWG met with industry representatives on May 8, 2007, to review the gap analysis. The ensuing discussion and review of the gap analysis revealed that no major inconsistencies existed between the two documents. Instead, the TWG found that Regulatory Guide 1.152 Rev. 2 was complementary to NEI 04-04 Rev. 1 on the subject of cyber security related to safety systems.

Although no major inconsistencies were revealed between the two documents, the TWG determined that there was overlapping guidance in a few programmatic areas. The industry suggested addressing the overlapping guidance to lessen the possibility of confusion during implementation of the guidance. Accordingly, NEI offered to revise NEI 04-04 to minimize the possibility of misinterpretation and to provide clarification with respect to the cyber security guidance for safety-related instrumentation and control systems. Following the revision, the document would be resubmitted to the NRC staff for review.

NEI also suggested that, following the review of the revised NEI 04-04, the NRC staff should provide written direction that would allow the use of either Regulatory Guide 1.152 or NEI 04-04 with respect to the cyber security licensing guidance and criteria for safety-related digital instrumentation and control systems. Although the staff agreed that the proposed modifications to NEI 04-04 would help to minimize confusion in implementation, it was nonetheless viewed as a sub-optimal solution for the long term. The staff noted further that because of the likelihood of changes in this area due to emerging threats and advances in digital technology, regulatory guidance to address these changes would also need to be modified, necessitating changes to NEI 04-04. As such, the NRC staff did not consider NEI 04-04 to be an appropriate long-term repository for such guidance and stated instead that a new Regulatory Guide would be developed to address cyber security defense measures required by 10 CFR 73.1 and the proposed new 10 CFR 73.55(m). In the meantime, the TWG acknowledged that NEI would submit a revision to NEI 04-04 consistent with the foregoing discussion as a short-term solution.

NEI submitted draft NEI 04-04 Rev. 2 to the TWG on August 6, 2007. The TWG met with industry representatives on August 17, 2007, to review the changes made to draft NEI 04-04 Rev. 2 and to determine if the modifications to the document were adequate to allow its use in lieu of the guidance provided within Regulatory Guide 1.152 Regulatory Positions 2.1-2.9. During the discussions, the NRC staff identified concerns regarding an applicant's or licensee's ability to directly correlate the topical elements embodied within Regulatory Positions 2.1-2.9 with the programmatic guidance

provided within draft NEI 04-04 Rev. 2. The NRC staff maintained that a clear correlation must exist between the two programs to ensure that license amendment requests provided by licensees, permit holders, and applicants using NEI 04-04 Rev. 2 when designing, constructing, implementing or upgrading safety-related digital instrumentation and control systems would be consistent with the guidance provided within Regulatory Guide 1.152.

As a result of the additional discussions with the NRC staff, industry agreed to provide a correlation table to the TWG that demonstrated how the topical elements within Regulatory Positions 2.1-2.9 mapped directly to the guidance stated within NEI 04-04. NEI also indicated that it would resubmit an updated version of draft NEI 04-04 Rev. 2 along with the correlation table. NEI submitted an updated version of draft NEI 04-04 Rev. 2 to the TWG on September 5, 2007. A correlation table was submitted to the TWG on September 6, 2007.

The TWG met with industry representatives on September 10, 2007, to discuss the results of its review of the previously submitted material. The NRC staff indicated that the updated version of draft NEI 04-04 Rev. 2 still did not embody all of the applicable criteria of RG 1.152, so the correlation table provided required additional information to adequately demonstrate how the topical elements within Regulatory Positions 2.1-2.9 mapped directly to the programmatic guidance stated within NEI 04-04. Further, the NRC staff noted that direction needed to be included in the correlation table to unambiguously state what specific documentation related to cyber security should be provided by a licensee or applicant when submitting safety system designs for staff review. The staff considered this direction to be essential to ensure that reviews of submissions using NEI 04-04 Rev. 2 (in lieu of RG 1.152 Rev. 2 Regulatory Positions 2.1-2.9) did not result in unnecessary requests for additional information by the staff.

At the conclusion of the meeting, the NRC staff agreed to provide the necessary corrections and additions to the supplied correlation table.

The TWG and industry representatives met on October 25, 2007, to review the corrected correlation table. An industry representative suggested that guidance concerning licensing submittal criteria be removed from the correlation table and instead be incorporated into guidance being developed by TWG#6 (Licensing Process). The NRC agreed and the suggestion was adopted.

The TWG and industry representatives met a final time on December 18, 2007, to discuss the NRC staff position regarding the use of draft NEI 04-04 Rev. 2 in lieu of Regulatory Guide 1.152 Rev. 2, Regulatory Positions 2.1-2.9.

5. STAFF POSITION

The original issue raised by NEI asserted that Regulatory Positions 2.1-2.9 provided within Regulatory Guide 1.152 Rev. 2 conflict with NEI 04-04 Rev. 1 with regard to the protection of safety-related digital instrumentation and control systems. However, through the TWG effort, the NRC staff has illustrated that the programs are in fact complementary.

The guidance provided within Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2 describes an acceptable method that can be used by licensees and applicants to provide cyber security protection for digital I&C systems used in safety-related applications. The NRC staff recognizes that alternative methods may be employed to achieve an equivalent level of protection. The staff is also sensitive to the fact that the industry is interested in pursuing efficient implementation of cyber security enhancements through the use of existing programs whenever possible.

The NRC is planning to issue additional regulatory guidance on the subject of cyber security defensive measures for safety systems. This regulatory guidance will be based on requirements in 10 CFR 73.1 and the proposed security regulations (i.e., 10 CFR 73.55m), if the Commission ultimately adopts this provision. Until this new regulatory guidance is issued, licensees, permit holders, and applicants involved in the design, construction, implementation, or upgrade of safety-

related digital instrumentation and control systems in nuclear power plants may address applicable cyber security issues through the use of either Regulatory Guide 1.152 Rev. 2 (Regulatory Positions 2.1-2.9) or the attached version of draft NEI 04-04 Rev. 2 in conjunction with the correlation table. The NRC staff plans to employ the correlation table presented in Appendix A when evaluating the adequacy of the cyber security defensive measures being established for safety systems.

Licensees, permit holders, and applicants are still required to identify, consider, and address all other applicable regulations, standards, and guidance when designing, constructing, implementing, and upgrading digital safety systems. This NRC staff position included herein is limited to the applicability of Regulatory Positions 2.1-2.9 found in Regulatory Guide 1.152 Rev. 2. No extrapolation or extension of this concept is implied, approved or authorized for any other portion of Regulatory Guide 1.152 Rev. 2. In addition, because the NRC's review of draft NEI 04-04 Rev. 2 has not been completed, this ISG does not constitute the NRC's formal acceptance of NEI 04-04 Rev. 2.

6. RATIONALE

The TWG has determined that no major inconsistencies exist between Regulatory Guide 1.152 Rev. 2 and NEI 04-04 Rev. 1. Indeed, the TWG's analysis indicates that the guidance provided in Regulatory Positions 2.1-2.9 of Regulatory Guide 1.152 Rev. 2 actually complements the NEI-generated programmatic guidance contained within NEI 04-04 Rev. 1.

Draft NEI 04-04 Rev. 2 submitted by NEI provides further clarification regarding the protection of safety systems from cyber threat. Although the objectives of draft NEI 04-04 Rev. 2 are similar in goal to Regulatory Guide 1.152 Rev. 2, the context of the program is significantly different. NEI 04-04 is designed to address the protection of all identified critical systems within a nuclear plant (including safety systems, security systems, and systems required for emergency response), whereas Regulatory Guide 1.152 Rev. 2 is concerned solely with licensing new or modified safety systems. The objective of NEI 04-04 is to address cyber security in a holistic manner and encompasses many elements and considerations not addressed by Regulatory Guide 1.152 Rev. 2.

The TWG has reviewed draft NEI 04-04 Rev. 2 and finds that the modifications proposed by the industry amplify the subject matter related to safety system cyber security. The TWG understands that an updated version of NEI 04-04 will be submitted to the NRC for formal review.

Despite the modifications made to NEI 04-04 by the industry, the TWG found that a direct correlation is not obvious between Regulatory Positions 2.1-2.9 stated within Regulatory Guide 1.152 Rev. 2 and the programmatic guidance provided within draft NEI 04-04 Rev. 2. This is due largely to the stylistic differences between the documents with regard to the language employed in each. The language of Regulatory Guide 1.152 Rev. 2 is more prescriptive and deterministic than that used in draft NEI 04-04 Rev. 2.

To reconcile the differences in language style and contextual focus, and to ensure that an adverse effect does not result if draft NEI 04-04 Rev. 2 is used in lieu of Regulatory Guide 1.152 Rev. 2 to address cyber security issues affecting safety systems, the TWG finds that a correlation table which definitively maps the topical elements within Regulatory Positions 2.1-2.9 to the elements of the guidance within NEI 04-04 is necessary. A correlation table provides an essential aid to individuals involved in the design, construction, implementation, and upgrade of safety systems as well as to the NRC staff who analyze and review safety system submittals provided by licensees, permit holders, and applicants. The TWG has reviewed and clarified the correlation table provided by NEI and has determined that the correlation table attached as Appendix A of this ISG sufficiently maps Regulatory Positions 2.1-2.9 to programmatic guidance contained within NEI 04-04.

7. REFERENCES

A. NRC Order EA-02-026, *Interim Compensatory Measures*, dated February 25, 2002

B. NRC Order EA-03-086, *Design Basis Threat for Radiological Sabotage,* April 29, 2003

C. IEEE Standard 603-1998, *Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, July 1, 1998

D. IEEE Standard 7-4.3.2-2003, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, December 19, 2003

E. NRC Standard Review Plan NUREG-0800, Appendix 7.1-D, *Guidance for Evaluation of the Application of IEEE STD 7-4.3.2,* March 2007

F. NRC Standard Review Plan NUREG-0800, Branch Technical Position 14 *Guidance on Software Reviews for Digital computer-Based Instrumentation and Control Systems,* Revision 5, March 2007

G. NRC Regulatory Guide 1.152, Revision 2, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* January 2006

H. Federal Register Vol. 71, No. 207, *Power Reactor Security Requirements*, October 26, 2006

I. NEI 04-04 Revision 1, *Cyber Security Program for Power Reactors,* November 18, 2005

J. Draft NEI 04-04 Revision 2, *Cyber Security Program for Power Reactors,* August 4, 2007

K. NEI White Paper, *Cyber Security Guidance for Nuclear Power Plants - The Need for a Coherent Approach*, March 5, 2007