UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

April 20, 2011

Mr. R. W. Borchardt
Executive Director for Operations
U. S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT FINAL REVISION 3 OF REGULATORY GUIDE 1.152, "CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

Dear Mr. Borchardt:

During the 582nd meeting of the Advisory Committee on Reactor Safeguards, April 7-9, 2011, we completed our review of Draft Final Revision 3 of Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," dated January 2011. Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on February 23, 2011. During these reviews, we had the benefit of discussions with representatives of the NRC staff and industry. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. Draft Final Revision 3 of RG 1.152 should not be issued until Recommendations 2, 3, and 4 are incorporated.

2. RG 1.152, Revision 3, Regulatory Position 2.3, “Design Phase,” should be revised to reference RG 5.71 and state that digital safety system designs should incorporate hardware and software architectures capable of providing a cyber security defensive architecture to combat malicious cyber security threats.

3. Explicit statements that the licensing design reviews will not address cyber security design features for other than their effect on the safety system should be deleted. Licensees should understand that as part of the safety system review, all features of their designs will be reviewed for licensing purposes, including cyber security, to the extent possible.

4. If the staff cannot provide hazard identification guidance for acceptable methods, RG 1.152 Regulatory Position 2.1, “Concepts Phase,” should be revised to state that, while Annex D of IEEE Standard 7-4.3.2-2003 is not endorsed by the NRC, the hazard identification guidance in Annex D may provide useful information on the assessment of the susceptibility of safety systems to inadvertent access.

5. The Standard Review Plan (SRP) for Chapters 7, “Instrumentation and Controls,” and 13, “Conduct of Operations,” should formally require internal staff coordination of reviews to RGs 1.152 and 5.71 during the system design reviews.

BACKGROUND

In January 2006, Revision 2 of RG 1.152 was issued to refer to the 2003 version of IEEE Standard 7-4.3.2. In addition, Regulatory Positions 2.1 through 2.9, which provided specific digital system cyber security guidance not included in IEEE Standard 7-4.3.2, were added. These regulatory positions provide cyber security guidance for the DI&C safety systems from concept through retirement phases.

The impetus for Revision 2 of RG 1.152 was the issuance of NRC Order EA-02-026, “Interim Safeguards and Security Compensatory Measures for Nuclear Power Plants,” dated February 2002 and NRC Order EA-03-086, “Design Basis Threat for Radiological Sabotage,” dated April 2003 subsequent to the attacks of September 11, 2011. In March 2009 these orders were incorporated in 10 CFR 73.54, “Protection of digital computer and communication systems and networks,” which requires all licensees under 10 CFR Part 50 to submit a "cyber security plan that satisfies the requirements of this section," and a 10 CFR 73.1 revision to include cyber attacks as a design basis threat. As a result, each licensee is required 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 10 CFR 73.1.

Subsequently, RG 5.71, “Cyber Security Programs for Nuclear Facilities,” was issued in January 2010. It describes an approach that the NRC staff deemed acceptable for developing cyber security plans that comply with 10 CFR 73.54 and 73.1 for malicious cyber security attacks. As stated by the staff, RG 5.71 includes performance based, programmatic cyber security provisions, and its associated guidance addresses Regulatory Positions 2.6 through 2.9 of RG 1.152.

DISCUSSION

RG 1.152, Revision 3 describes a method deemed acceptable for complying with the Commission's regulations for promoting high functional reliability, design quality, and a secure development and operational environment (SDOE) for the use of digital computers in the safety systems for nuclear power plants. The purpose of this revision is to provide consistency with RG 5.71. In the staff’s view, this was accomplished by eliminating reference to cyber security, by deleting Regulatory Positions 2.6 through 2.9 which apply from system site installation through retirement, and eliminating all references or inferences to malicious actions or attacks from the discussion and Regulatory Positions 2.1 through 2.5 except to state explicitly that:

- "This guide is not intended to address the ability of those protective features to thwart malicious cyber attacks," and

- "For licensees that choose to provide, as part of their license submittal, descriptions of cyber security features incorporated in the design of digital safety systems intended to address the guidance of RG 5.71, the extent of the staff's review of these features is limited to ensuring that these features do not adversely affect or degrade the system's reliability or its capability to perform its safety function."

In effect, Revision 3 of RG 1.152 distinctly separates these functions by relegating the "safety" guidance to RG 1.152 and “security” guidance to RG 5.71. RG 1.152 will now focus only on non-malicious and inadvertent actions and will be reviewed during licensing. RG 5.71 will focus only on malicious action or attacks and will be reviewed during the development of the cyber security plan after licensing. RG 5.71, Sections C.3.2 and C.3.3.1 describe defense-in-depth protective strategies and technical controls as primary measures to thwart malicious cyber attacks. The strategy consists of a series of security boundary levels with increasing degrees of security as one moves from the public to the most critical plant level. The technical controls are safeguards or protective measures that are executed through hardware, firmware, operating systems, or application software. These controls are not accomplished through administrative procedures and human actions.

The ability of the digital safety, non-safety, and other digital systems to thwart malicious attacks is dependent on the capability of the hardware and software architectures to implement the measures needed to meet the requirements of the cyber security plan. Thus, the ability to combat cyber security attacks should be considered at all stages of the design process. The deliberate separation of safety and cyber security considerations in the proposed Revision 3 of RG 1.152 is detrimental to integrated consideration of cyber security in the design phase of the digital systems. To help ensure proper consideration of cyber security in all phases of digital system design and licensing:

- RG 1.152, Revision 3, Regulatory Position 2.3, “Design Phase,” should be revised to reference RG 5.71 and state that digital safety system designs should incorporate hardware and software architectures capable of providing a cyber security defensive architecture to combat malicious cyber security threats.

- Explicit statements that the licensing design reviews will not address cyber security design features for other than their effect on the safety system should be deleted. Licensees should understand that as part of the safety system review, all features of their designs will be reviewed for licensing purposes, including cyber security, to the extent possible.

- The Standard Review Plan for Chapters 7, “Instrumentation and Controls,” and 13, “Conduct of Operations,” should formally require internal staff coordination of reviews to RGs 1.152 and 5.71 during the system design reviews.

This is consistent with Commission direction in SRM - SECY-05-0120 that nuclear power plant designs should address safety and security issues in a fully integrated manner. RG 1.152, Revision 3 endorses conformance with the requirements of IEEE Standard 7-4.3.2-2003 as an acceptable method for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. However, Annexes B-F are not endorsed.

Annex D of IEEE Standard 7-4.3.2-2003, “Identification and Resolution of Hazards,” provides general information on the use of qualitative or quantitative fault tree analysis (FTA) and failure modes and effects analysis (FMEA) techniques throughout the system development life cycle. It is reasonable for the staff to withhold full endorsement of Annex D because it does not represent a consensus position. Although it does not provide complete guidance on FTA and FMEA methods, many aspects of the hazard identification process in Annex D are informative. If the staff cannot provide alternative guidance for acceptable methods, then the hazard identification guidance in Annex D should be recognized as a useful source of information. This was done in RG 1.152, Revision 1, and similar language could be included in the current revision.

During our subcommittee discussion of the defensive architectures described in RG 5.71, it was noted that this guide states that one-way data flow from higher security levels to lower security levels is an example of an acceptable architecture. The associated discussion emphasizes that digital isolation is the preferred method, wherever feasible. This isolation can be accomplished with a variety of means such as firewalls, diodes, routers, and other digital communication interface devices. A prominent characteristic of many of these devices is that they can have their uni-/bidirectional capability enabled or disabled via software commands, which provides a potential superhighway for compromise during cyber attacks. While RG 5.71, Appendices B and C emphasize the use of hardware mechanisms for one-way data flows, it is suggested that this guide be expanded in the next revision to also emphasize the use of components where software commands cannot be used to enable or disable uni-/bidirectional data flow as well.

Draft Final Revision 3 to Regulatory Guide 1.152 should not be issued until the recommended revisions are incorporated.

During our deliberations, the staff indicated that a number of future revisions of RG 1.152, RG 5.71, and the SRP are being considered. We have already noted one specific revision of RG 5.71 that should be considered and agree that other revisions will be needed. We support the staff efforts to complete all revisions in a timely manner.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

References:

1. Draft Final RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Rev. 3, 10/21/2011 (ML110200231)

2. Regulatory Guide RG 5.71, “Cyber Security Programs for Nuclear Facilities,” Rev 0, January 2009 (ML090760860)

3. IEEE Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” December 2003, Institute of Electrical and Electronics Engineers, Piscataway, NJ

4. SRM SECY-05-0120 - Security Design Expectations for New Reactor Licensing Activities, 09/09/2005 (ML052520334)

During our subcommittee discussion of the defensive architectures described in RG 5.71, it was noted that this guide states that one-way data flow from higher security levels to lower security levels is an example of an acceptable architecture. The associated discussion emphasizes that digital isolation is the preferred method, wherever feasible. This isolation can be accomplished with a variety of means such as firewalls, diodes, routers, and other digital communication interface devices. A prominent characteristic of many of these devices is that they can have their uni-/bidirectional capability enabled or disabled via software commands, which provides a potential superhighway for compromise during cyber attacks. While RG 5.71, Appendices B and C emphasize the use of hardware mechanisms for one-way data flows, it is suggested that this guide be expanded in the next revision to also emphasize the use of components where software commands cannot be used to enable or disable uni-/bidirectional data flow as well.

Draft Final Revision 3 to Regulatory Guide 1.152 should not be issued until the recommended revisions are incorporated.

During our deliberations, the staff indicated that a number of future revisions of RG 1.152, RG 5.71, and the SRP are being considered. We have already noted one specific revision of RG 5.71 that should be considered and agree that other revisions will be needed. We support the staff efforts to complete all revisions in a timely manner.

Sincerely,
/RA/
Said Abdel-Khalik
Chairman

References:

1. Draft Final RG 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Rev. 3, 10/21/2011 (ML110200231)

2. Regulatory Guide RG 5.71, “Cyber Security Programs for Nuclear Facilities,” Rev 0, January 2009 (ML090760860)

3. IEEE Standard 7-4.3.2-2003, “Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,” December 2003, Institute of Electrical and Electronics Engineers, Piscataway, NJ

4. SRM SECY-05-0120 - Security Design Expectations for New Reactor Licensing Activities, 09/09/2005 (ML052520334)

Distribution:
See next page

Accession No:ML11101A013 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	CSantos	EHackett	EHackett for SAbdel-Khalik
DATE	4/19/11	4/19/11	4/19/11	4/20/11	4/20/11

OFFICIAL RECORD COPY

Letter to Mr. R. W. Borchardt, Executive Director for Operations, NRC, from Said Abdel-Khalik, Chairman, ACRS, dated April 20, 2011

SUBJECT: DRAFT FINAL REVISION 3 OF REGULATORY GUIDE 1.152, "CRITERIA FOR USE OF COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS"

Distribution:
ACRS Staff
ACRS Members
B. Champ
A. Bates
S. McKelvin
L. Mike
P. Lien
B. Rini
RidsSECYMailCenter
RidsEDOMailCenter
RidsNMSSOD
RidsNSIROD
RidsFSMEOD
RidsRESOD
RidsOIGMailCenter
RidsOGCMailCenter
RidsOCAAMailCenter
RidsOCAMailCenter
RidsNRROD
RidsNROOD
RidsOPAMail
RidsRGN1MailCenter
RidsRGN2MailCenter
RidsRGN3MailCenter
RidsRGN4MailCenter