



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

March 25, 2010

The Honorable Gregory B. Jaczko
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT FINAL REVISION 1 TO DIGITAL INSTRUMENTATION AND CONTROL INTERIM STAFF GUIDANCE - 07: "DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN SAFETY APPLICATIONS AT FUEL CYCLE FACILITIES"

Dear Chairman Jaczko:

During the 570th meeting of the Advisory Committee on Reactor Safeguards, March 4 - 6, 2010, we reviewed Draft Final Revision 1 to Digital Instrumentation and Control (DI&C) Interim Staff Guidance (ISG)-07, "Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities." Our DI&C Systems Subcommittee also reviewed this matter during a meeting on August 21, 2009. During these reviews, we had the benefit of discussions with representatives of the NRC staff. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. Revision 1 to DI&C-ISG-07 should not be issued as final until Recommendation 2 is addressed.
2. Revision 1 to DI&C-ISG-07 should be revised to state that any reduction in the level of rigorous management measures applied to redundant Items Relied on for Safety (IROFS), relative to sole IROFS with the same design requirements, should be justified by a comprehensive analysis that identifies the common cause failure modes and other dependencies that must be mitigated or prevented to ensure reliable operation.
3. Future efforts should include development of a systematic approach for identifying dependencies and common cause failures (CCFs) in IROFS to enhance the effective application of graded management measures.
4. Future efforts should also include development of an approach for structuring the individual scenario results of an Integrated Safety Assessment (ISA) to facilitate review and understanding of the associated risk significance.

BACKGROUND

The licensing of fuel cycle facilities is governed by Title 10 of the Code of Federal Regulations (10 CFR) Part 70, "Domestic Licensing of Special Nuclear Material." Guidance for review is contained in NUREG-1520, "Standard Review Plan for the Review of a License Application for a

Fuel Cycle Facility.” Neither of these documents contains either analog or DI&C design criteria using industry codes and standards analogous to those contained in 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” or NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports For Nuclear Power Plants: LWR Edition.” ISG-07 was developed in response to industry and NRC concerns regarding the consistency of review of fuel cycle facility applications.

DISCUSSION

Revision 1 to DI&C-ISG-07 is intended to provide consistent guidance for licensing review criteria regarding acceptable means for the implementation of DI&C used to accomplish safety functions in fuel cycle facilities. 10 CFR 70.61(e) requires that each engineered or administrative control or control system necessary to meet performance requirements shall be designated as an IROFS, and that a facility safety program shall ensure that each IROFS will be available and reliable to perform its intended function. In addition, 10 CFR 70.64(a)(1) requires new facilities, or new processes at existing facilities, to address baseline design criteria and quality standards in accordance with management measures, to ensure that IROFS will perform their intended function when needed. ISG-07 will be incorporated into future revisions of NUREG-1520.

ISG-07 describes review criteria for the following DI&C design, implementation, and maintenance topics:

- Cyber Security for the Protection of IROFS,
- Independence of Controls used as IROFS,
- Digital Communications, and
- Quality Design Process for Systems Development.

Each of these topics provides guidance for design and implementation and for the management measures that ensure the design is developed in accordance with the design criteria. Revision 1 to DI&C ISG-07 also includes guidance for management measures needed to provide reasonable assurance of compliance with facility performance requirements and for post-installation operation and maintenance.

A major element in all four topics is the application of a graded approach to the implementation of management measures for the design and development process and for post-installation operation of IROFS. This graded approach is described under the Quality Design Process for Systems Development in ISG-07. The use of a graded approach, that applies reduced management measures for IROFS when there is a low likelihood of occurrence and low severity of consequence, is reasonable.

Relative to applying redundant IROFS, Revision 1 to DI&C-ISG-07 suggests that a high degree of risk reduction can be achieved using multiple redundant channels of controls, even though each individual channel may only provide a low risk reduction. Redundant IROFS may be either diverse or non-diverse. When redundancy is provided by identical equipment or operator actions, it is important to ensure that all credible CCF modes have been identified and taken into account when estimating the reliability of the protective measure.

However, Revision 1 to DI&C-ISG-07 does not provide a systematic approach for identifying common cause failure modes and other dependencies that must be mitigated or prevented.

Therefore, Revision 1 to DI&C-ISG-07 should be revised to state that any reduction in the level of rigorous management measures applied to redundant IROFS, relative to sole IROFS with the same design requirements, should be justified by a comprehensive analysis that identifies the CCF modes and other dependencies that must be mitigated or prevented to ensure reliable operation.

In light of the above, future efforts should include the development of a systematic approach for identifying CCFs and other dependencies in IROFS to enhance the effective application of graded management measures.

We discussed the use of probabilistic risk assessment methods and risk-informed reviews in applying the graded approach to management measures. The staff noted that although quantification is not required, most licensees do use some form of quantification to determine the significance of an event sequence instead of solely relying on expert judgment when evaluating IROFS needed for individual event sequences.

Qualitative descriptive reviews are performed by “horizontal cuts” (examining completeness within the analysis of specific scenarios) and “vertical cuts” (examination of the same failure event over multiple scenarios). Such reviews impart a sense of the quality of the analysis. However, given the complex nature of the analysis, a more structured approach is needed.

Without an integrated quantification (i.e., summation over specific scenarios to provide quantification of overall risk and of classes of scenarios), the risk importance of IROFS cannot be determined. More importantly, absent this quantification, there is no clear structure framing the bulk of the ISA results. Future efforts should include development of an approach to facilitate understanding and review; clarify the risk importance of scenarios, equipment, and human actions; and organize the results into classes of scenarios and consequences.

Sincerely,

/RA/

Said Abdel-Khalik
Chairman

References:

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Controls, DI&C-ISG-07 Revision 1, “Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities,” 02/01/2010 (ML100480228)
2. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Controls DI&C-ISG-07 Revision 0, “Digital Instrumentation and Control Systems in Safety Applications at Fuel Cycle Facilities,” 06/01/2009 (ML091550599)
3. NUREG-1520, “Standard Review Plan for the Review of a License Application for a Fuel Cycle Facility,” Rev 0, 03/31/2002 (ML020930033)

4. NUREG- 0800, "Standard Review Plan For the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition"
5. U.S. Code of Federal Regulations, Title 10, Energy, Part 50, "Domestic Licensing of Production and Utilization Facility," Appendix A, "General Design Criteria for Nuclear Power Plants"
6. U.S. Code of Federal Regulations, Title 10, Part 70, "Domestic Licensing of Special Nuclear Material"

4. NUREG- 0800, "Standard Review Plan For the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition"
5. U.S. Code of Federal Regulations, Title 10, Energy, Part 50, "Domestic Licensing of Production and Utilization Facility," Appendix A, "General Design Criteria for Nuclear Power Plants"
6. U.S. Code of Federal Regulations, Title 10, Part 70, "Domestic Licensing of Special Nuclear Material"

Distribution:

ACRS Staff & ACRS Members

B. Champ

A. Bates

S. McKelvin

L. Mike

J. Ridgely

RidsSECYMailCenter

RidsEDOMailCenter

RidsNMSSOD

RidsNSIROD

RidsFSMEOD

RidsRESOD

RidsOIGMailCenter

RidsOGCMailCenter

RidsOCAAMailCenter

RidsOCAMailCenter

RidsNRROD

RidsNROOD

RidsOPAMail

RidsRGN1MailCenter

RidsRGN2MailCenter

RidsRGN3MailCenter

RidsRGN4MailCenter

Accession No: ML100690026

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	ADias for CAntonescu	ADias for CAntonescu	ADias for CSantos	EHackett	EHackett for SAbdel-Khalik
DATE	3/25/10	3/25/10	3/25/10	3/25/10	3/25/10

OFFICIAL RECORD COPY