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

April 29, 2008

The Honorable Dale E. Klein
Chairman
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS INTERIM STAFF GUIDANCE

Dear Chairman Klein:

During the 551st meeting of the Advisory Committee on Reactor Safeguards, April 10-12, 2008, we reviewed three new Digital Instrumentation and Control (DI&C) Systems Interim Staff Guidance (ISG) documents on Cyber Security, DI&C Licensing Process, and Review of New Reactor DI&C Probabilistic Risk Assessments (PRAs). We also reviewed the staff's operational experience review and the digital categorization update. Our DI&C Systems Subcommittee also reviewed these matters during a meeting on March 20, 2008. During these reviews, we had the benefit of discussions with representatives of the NRC staff, the Nuclear Energy Institute (NEI), and the Electric Power Research Institute (EPRI). We also had the benefit of the documents referenced.

Conclusion and Recommendation

1. The ISG on Cyber Security will clarify the staff's guidance regarding the implementation of cyber security requirements and will facilitate the licensing process when NEI 04-04, Revision 2, "Cyber Security Program for Power Reactors," is used in lieu of Regulatory Guide (RG) 1.152 Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

2. The draft ISG on the Review of New Reactor DI&C PRAs should be revised to emphasize the importance of the identification of failure modes, deemphasize sensitivity studies that deal with probabilities, and discuss the current limitations in DI&C PRAs. The staff has indicated that this ISG will be revised taking our comments into consideration.

Background and Discussion

As licensees worked to identify and implement security enhancements to secure their facilities from cyber threats, they raised concerns of possible conflicts between RG 1.152, Revision 2 and the NRC-accepted guidance contained in NEI 04-04, Revision 1. The NRC Task Working Group (TWG) #1 on Cyber Security compared these documents to identify inconsistencies. As a result of this review, NEI produced NEI 04-04, Revision 2.

The purpose of the ISG on Cyber Security is to clarify the staff's guidance regarding the implementation of cyber security requirements. This ISG includes a cross-correlation table that demonstrates how the topical elements in RG 1.152, Revision 2 map to the guidance in NEI 04-04, Revision 2. This ISG states that NEI 04-04, Revision 2 used in conjunction with the cross-correlation table provides an acceptable method that can be used in lieu of RG 1.152, Revision 2 to provide cyber security protection for DI&C systems used in safety-related applications.

The staff is planning to issue additional regulatory guidance on the subject of cyber security to support the new rule 10 CFR 73.54. We offer the following comments to contribute to the staff's deliberations in developing such additional guidance:

- A threat assessment should be performed to ensure that the defensive measures are addressing the right cyber security threats. This assessment should include both internal and external threats.

- Dependency analysis is necessary to identify plant infrastructure services (power, heating, ventilation, and air conditioning, etc.) that support Critical Digital Assets (CDAs). The cyber security program should protect the CDAs and ensure that their support systems and any interfacing data systems are also protected.

- The process for the identification of CDAs is expected to use insights from the plant PRA. Although we concur with this practice, we note that DI&C systems are modeled at a simplistic level in current PRAs. Therefore, any insights from the PRA regarding the risk significance of these systems should be viewed with caution.

The draft ISG on the DI&C Licensing Process has been prepared by TWG #6. Its purpose is to clarify what documentation is required and when, as well as to provide guidance on the scope and content of a license amendment request to address the regulatory requirements. These clarifications will help streamline the licensing process.

The draft ISG on the Review of New Reactor DI&C PRAs is being prepared by TWG #3. The purpose of this is to provide interim guidance for review of new reactor DI&C PRAs. In the development of this ISG the staff used insights gained from previous NRC licensing experience, industry white papers outlining proposed current methods and lessons learned, NRC research completed to date, and NRC review of current guidance and methods. The draft ISG contains guidance to help a reviewer confirm that contributions from DI&C PRAs are reflected adequately in the overall plant risk.

The state of the art in PRA methodology for systems that include software-based DI&C is primitive[a]. The Office of Nuclear Regulatory Research has been supporting research efforts to improve this methodology. What makes it different from that of traditional PRAs is the

[a] Even with analog I&C systems, the PRA state of the art in identifying spurious signals is still evolving.

realization that DI&C may introduce new failure modes that are not well understood. The software failure probabilities that are generally used do not have a sound technical basis. Any results that are based on these probabilities are suspect. This includes the "dominant" failure modes that the draft ISG mentions.

The draft ISG recommends that the reviewer perform sensitivity studies using the probabilities that the applicant will provide in the PRA. These probabilities cannot be very meaningful in the absence of a good understanding of the failure modes. The use of these probabilities may create the impression that the agency is implicitly accepting them and their derivation. Finally, the whole concept of sensitivity analysis should be well defined (i.e., by how much is it reasonable for the reviewers to increase the probabilities?; should all of them be increased at the same time?; is it meaningful to increase probabilities that are suspect?)

Although it is not the purpose of the draft ISG to develop a methodology for failure mode identification, it would be helpful to provide guidance to the reviewer. For example, several application-independent classes of failure modes from the DI&C processor can be defined and standardized at the processor level, with the I&C effects defined separately. The following example list of processor classes of failure modes reported in the literature (References 2 and 3) could be the starting point of a comprehensive list for NRC use:

- Task[b] Crash: The control software task exits unexpectedly.
- Task Hang: The process goes into an infinite loop.
- Task Late Response: The output of the task exceeds the specified response time.
- Task Early Response: The output of the task is too early.
- Task Incorrect Response: The output of the task is timely but violates specifications.
- Task No Response: There is no output from the task (but the task is not hung).
- Processor Crash: The processor software kernel (or operating system) crashes bringing down all tasks running on the operating system.
- Corrupted Input: The input signal from the plant sensors receives corrupted data due to either an analog electrical problem, an analog-to-digital conversion problem, or noise in a digital network.

[b] A "task" is meant to be a real-time program executing under control of a kernel or operating system. It is assumed that the processor of the DI&C system has an architecture consisting of tasks that are specific to the application and a general purpose kernel or operating system that interfaces with the hardware and provides the infrastructure that provides services and access to hardware resources on which the task relies.

- Corrupted Output: The output signal to plant actuators is corrupted due to an analog electrical problem, a digital-to-analog conversion problem, or noise in a digital network is corrupted.

- Out of Sequence Data: Data packets arrive at the destination in a sequence different than expected (applicable to digital networks using Transmission Control Protocol/Internet Protocol (TCP/IP) and other protocols collectively referred to as "field buses" or "data highways").

The effects of these failure modes can be investigated at three levels. The first-level effects would be at the processor boundary. The second level would be effects on the control or safety system, and the third level would be effects on the plant.

The above classes of failure modes could also be useful in the review of common-cause failure analyses. The extent to which all common software components are assumed to have been disabled by a common-cause failure has to be examined in light of the individual failure modes that apply. For example, if it is assumed that application software has an algorithmic or arithmetic flaw of some type, then this flaw would be triggered on all channels simultaneously.[c] However, for timing-related failures such as crashes or hangs, this is not necessarily the case. The particular sequence of events that causes a hang due to a priority inversion on one processor in a multi-channel system might not cause the same event to occur on another processor simply because of the difference in which events were processed. Even in the case of coding flaws that cause memory leaks leading to a processor crash, it is unlikely that memory leaks will cause all processors to fail at precisely the same time.

The draft ISG on the Review of New Reactor DI&C PRAs should be revised to emphasize the importance of the identification of failure modes, deemphasize sensitivity studies that deal with probabilities, and discuss the current limitations in DI&C PRAs. We have been informed by the staff that our comments will be taken under advisement and the draft ISG will be revised, as appropriate.

We are looking forward to future interactions with the staff on these matters.

Sincerely,

/RA/

William J. Shack
Chairman

[c] Such defects may not be common in software developed with the highly disciplined processes that are used in Class 1E systems.

References

1. U.S. Nuclear Regulatory Commission, Digital Instrumentation & Control (DI&C)-ISG-01, "Cyber Security," dated December 31, 2007 (ML072980150), Appendix A, "RG 1.152 (Rev 2) and Draft NEI 04-04 (Rev 2) Cross-Correlation Table," Appendix B, "NEI 04-04 (Rev 2), 'Cyber Security Program for Power Reactors'." (Note: Appendices A and B are restricted documents, "need to know".)

2. U.S. Nuclear Regulatory Commission, Draft DI&C-ISG-06, "Digital I&C Licensing Process," dated October 15, 2007 (ML072980287) including "Documents Needed for Review of Different Complexities."

3. U.S. Nuclear Regulatory Commission, Draft DI&C-ISG-03, "Review of New Reactor Digital I&C PRAs," March 2008 (ML080570048).

4. Draft White Paper, "Assessment of Digital Systems Operating Experience Data & System Inventory and Classification Structure."

5. U.S. Nuclear Regulatory Commission, Draft NUREG/CR, "Approaches for Using Traditional PRA Methods for Digital Systems," February 2008, Appendix A, "Summary Report of the External Review Panel Meeting on Reliability Modeling of Digital Systems (May 23–24, 2007)," Appendix B, "Detailed FMEA of the DFWCS at Different Levels," Appendix C, "Modeling of Software Failures," Appendix D, "Other Methods for Modeling Digital Systems."

6. IBM Center for Software Engineering, "Details of ODC V 5.11," http://www.research.ibm.com/softeng/ODC/DETODC.HTM, dated February 1, 2002.

7. H. Pentti and H. Atte, "FMEA for Software-Based Automated Systems," **STUK,** STUK-YTO-TR 190 /August 2002, Radiation and Nuclear Safety Authority, Finland.

8. Proposed 10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks."