NUCLEAR ENERGY INSTITUTE

Felix M. Killar, Jr.
SENIOR DIRECTOR
FUEL SUPPLY/MATERIAL LICENSEES
NUCLEAR GENERATION DIVISION

8/04/09
74FR38673
(1)

September 2, 2009

Mr. Mike Lesar
Chief, Rulemaking and Directives Branch
Office of Administration
U.S. Nuclear Regulatory Commission
Mail Stop TWB-05-B01M
Washington, D.C. 20555-0001

Subject: Industry Comments on Digital I&C Draft Interim Staff Guidance-07 for Fuel Cycle Facilities *Federal Register* (74FR38673)

Project Number: 689

Dear Mr. Lesar:

On behalf of the fuel cycle industry, the Nuclear Energy Institute (NEI)[1] submits the following comments on the Draft Interim Staff Guidance on "Digital Instrumentation and Control in Safety Systems at Fuel Cycle Facilities" issued in the *Federal Register* on August 4, 2009 for a 30-day comment period. We appreciate the staff's effort to work with industry on development of this draft and trust you will find the general comments below and the specific edits in the enclosure consistent with those expressed to the U.S. Nuclear Regulatory Commission (NRC) during the monthly public meetings and useful as you proceed to finalize it. We also request further dialogue with industry on this guide prior to its finalization as discussed at the end of this letter.

First, industry expressed concerns throughout the development process with: 1) the unnecessary level of complexity and detail in the guide that may, inadvertently, dissuade facilities from installing digital instrumentation and control (DI&C) systems; 2) overtones and references to cyber "security" rather than a cyber program focused on safety pursuant to 10 CFR Part 70; and 3) references and

[1] 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 fabrication facilities, nuclear materials licensees, and other organizations and entities involved in the nuclear energy industry.

SUNSI Review Complete
E-RIDS = ADM-03

1776 I Street, NW | Suite 400 | Washington, DC | 20006-3708 | P: 202.739.8126 | F: 202.533.0157 | fmk@nei.org | www.nei.org

Template = ADM-013
Add = D. Rahn (DLR1)

language more aligned with the higher risk operations at a commercial nuclear power reactor rather than the lower risk and more diverse fleet of fuel cycle facilities in operation today or planned for the future. Further, some gradation of a risk-informed approach should be used for the various categories of fuel cycle facilities licensed under Part 40 or 70 or certified under Part 76.

Secondly, the fuel cycle industry supports the use of and need for an effective cyber plan, whether the systems of concern utilize isolated networks that have no interconnection to other plant safety systems or are inherently part of them. In fact, some plants operating today have more than 30 years of experience using DI&C systems. Ultimately, the cyber system must be adequately protected and designed to minimize the risk and consequences from an inadvertent or intentional attack to any system relied on for the safe operation of the plant. That being said, it must be recognized that the health and safety consequences from a compromised system at a fuel facility are significantly much lower than those at a power reactor, and the guidance should reflect this reduced risk. Specifically, at a fuel cycle facility, there are applications that are fault-tolerant where the process and control system can be brought to a safe condition including shutdown nearly instantaneously, long before a failure has any chance to affect system safety.

Third, the Draft ISG describes difficulties of demonstrating adequate systems but generally lacks practical and achievable solutions and clear and rational criteria for accepting systems in safety applications. In this regard, we are concerned that the Draft ISG is far too complex for the average NRC license reviewer, inspector, manager or some fuel facility management. Further, and most importantly, the guidance forces DI&C systems to undergo a much higher level of scrutiny and demonstration of adequacy than many other systems and applications that are readily accepted today as meeting the applicable NRC regulations. We believe that this is an unfair burden for systems that have a far better track record of managing safety functions than many other systems relied on today.

Fourth, and equally important, industry agrees that this guidance should be applied to new license applications as stated in the Note on page 2 of the Draft ISG. Industry disagrees however with the remaining Note language which states that this guide will also be applied to the "review and evaluation of proposed amendments to existing fuel cycle facilities, and the review and evaluation of license renewal applications." This approach is not consistent with industry's understanding over the course of the guidance development process. Instead, industry suggests that this guide be applied to new licenses and amendments to existing licenses for new processes or previously un-reviewed control schemes that are submitted to NRC for approval after the effective date of the final staff DI&C guidance.

We appreciate the opportunity to comment on the Draft Guide. As evidenced by the significance and number of our comments, we continue to have concerns about its contents. Therefore, we request that the NRC conduct an additional workshop with industry to review our comments and work to identify mutually agreeable modifications to the draft guide, prior to its finalization, to increase its usefulness and applicability to existing and future fuel cycle facilities.

Please contact me or Janet Schlueter (202-739-8098; jrs@nei.org) with comments about this letter or to arrange a public meeting on the Draft ISG.

Sincerely,

Felix M. Killar, Jr.

Enclosure

c: Mr. David Rahn, NMSS

Enclosure

Specific Comments on Digital Instrumentation and Control
Interim Staff Guidance-07, "DI&C in Safety Application at Fuel Cycle Facilities"

Specific comments are offered by Section title below for the NRC's consideration.

Cyber Security for the Protection of IROFS:
Page 3: The NRC should consider deleting the section and, instead, refer to NRC-issued orders that require licensees to perform cyber security. This approach would also address the issue of malevolent acts which are not part of a site specific Integrated Safety Analysis evaluation. For Part 70 Category 3 facilities, the cyber security in place to protect intellectual property and MC&A information is adequate for protecting the IROFS.

Discussion:
Page 5, second paragraph: As stated, 10 CFR Part 70 requires licensees to implement management measures to ensure that digital assets performing safety functions or that support the performance of safety functions for the facility are continually protected. The guidance addresses performance goals, elements, and characteristics of management measures that could be used in fuel cycle facilities to provide reasonable assurance that the functions performed by digital safety equipment will be designed, implemented, and maintained such that they are programmatically protected. Further, management measures should be implemented to ensure that effective cyber security provisions are in place to prevent cyber events from compromising the confidentiality, integrity, and availability of all IROFS.

These standards appear to be taken from the guidance related to power reactor facilities. As stated previously, the level of risk for a fuel cycle facility is not commensurate with that of a reactor facility; therefore, different assumptions about the treatment for cyber security for fuel cycle facilities should be considered. Beginning with the discussion in paragraph b(2) and continuing through paragraph (g), the ISG appears to go beyond guidance for new applications and states new requirements: a cyber security plan, program, procedures, etc. are required for all licensees or applicants, regardless of need, and regardless of whether requesting licensing action of the NRC.

Staff Guidance:
Page 8, second bullet: This item implies that the licensee must add dedicated personnel to monitor against cyber intrusion. At some fuel cycle facilities, computer personnel would be used for this purpose. Industry does not believe that NRC should determine what category of employee performs this task. Therefore, the bullet should be modified to remove this implication.

Technical Review Guidance:
Page 12, first full paragraph, second sentence: The purpose of this sentence appears to redefine the ISA Summary. This appears to be outside the scope of defining cyber security requirements. It should be revised to indicate it is intended to refer only to cyber-security aspects of the ISA Summary or it should be relocated to the general introduction of the ISG.

Independence of Controls used for Safety Functions:
Recommend changing the title of this section to "Independence of Controls used for IROFS".

Pages 14 –17: Discussions in this major section suggest a new level of granularity to the individual instrument. The last sentence of the first paragraph on page 17 suggests that when identical equipment or operator actions provide the necessary redundancy that all credible common-case failures have been identified and taken into account when estimating the reliability of the protective measure. Please clarify whether this language is intended to suggest that redundancy is not accomplished by identical equipment performing the same function or by two operators performing the same procedure irrespective of configuration due to common cause concerns.

Discussion:
Page 16: Events and accident sequences are different. Events, especially initiating events, do not all have to be identified if the IROFS protect against the entire group of initiating events. For example, if an IROFS provides adequate protection in the event of the maximum credible flood, it does not matter how many specific events could cause the flood. In addition, NUREG-1520 allows for bounding of accident sequences.

Double Contingency Principle:
Page 17: This entire section should be removed from this document. This is a requirement that is reviewed and implemented by nuclear criticality specialists, not instrumentation and control specialists.

Page 19, bullet item 2: This item identifies a situation that may not result in two IROFS being independent from one another as the situation where two individuals use the same equipment or procedure. This seems to suggest that, for each system using an administrative control, two independent reviews using different procedures would have to occur for the reviews to be independent. This seems counter-intuitive because when an operator is performing an administrative procedure, such as calibrating a scale, a verification of the first operator's result is desirable. The ISG should be revised to clarify what is intended by this bullet.

Staff Guidance:
Page 22, paragraph 2, "1E-6/year": This frequency meets the criteria for "not credible". If the likelihood of an accident sequence / initiating event is "not credible," it does not need to be considered. Additionally, if the risk acceptance criteria for an accident sequence is E-4, then a common failure causing the accident at anything less than or equal to E-4 should be considered acceptable.

Page 22, paragraph 2, last sentence: One order of magnitude is more than adequate. A common mode failure of 1E-4 would, in a qualitative sense, still meet the acceptance criteria. If the risk acceptance criteria is E-4 for an accident, then a common failure of the IROFS at anything less than

or equal to E-4 should be considered acceptable—likewise, if the risk acceptance criteria is E-5, then anything less than or equal to E-5 should be acceptable.

Software Common Cause Failure Considerations:
Page 25, paragraph 3: "there is evidence that 100% of the time...." It is recommended that NRC change the wording regarding "100%" to address credible failure modes. As long as the PFOD or failure frequency credited is maintained, 100% fail safe is not required.

Evaluation of Vendor-identified Digital Control System Failure Alert Notices:
Page 27, sentence one: Delete "applied for use in safety applications". The licensee should evaluate controls/instrumentation notifications for their impact on IROFS.

Implementation of Safety Control System:
Page 27: This section implies that all IROFS related controls are third-party rated. It must be made very clear that third-party rated safety controls shall only be required for the following:

- An accident sequence that has a sole IROFS that is an active engineered control.
- An accident sequence that has multiple IROFS that rely on the same control system (non-independent).
- IROFS that required operation during and/or after an incident or do not fail safe.

The safety evaluation of the PLC should be based on proper configuration and/or installation of the hardware, proper use of software/hardware watchdogs, use of communication "Heartbeats" where applicable, and proper implementation of fault detection and response. This section is clearly excessive for systems with independent controller for each IROFS.

Digital Communications:
This section implies requirements relevant to 10 CFR 50 requirements for commercial nuclear reactors. The safety risks at part 70 facilities do not require this level of rigor on communications systems. The scheme presented implies completely separate safety and process systems. This is not a standard controls scheme at a part 70 facility. The communications protocols and error checking provided by high end process control systems will meet all of the requirements necessary for IROFS. A more rigorous communications review would be required for the following type of situations:

- An accident sequence that has a sole IROFS that is an active engineered control.
- An accident sequence that has multiple IROFS that rely on the same control system (non-independent).
- IROFS that required operation during and/or after an incident or do not fail safe.

Isolation of safety and process controls would have a significant impact on human factors related to how an operator interacts with the process and alarm/interlock situations.

Software Quality:
Most references and requirements are all based on part 50 requirements with the key reason being common mode failures. Common mode failures are only an issue if:

- An accident sequence that has a sole IROFS that is an active engineered control.
- An accident sequence that has multiple IROFS that rely on the same control system (non-independent).
- IROFS that required operation during and/or after an incident or do not fail safe.

High-Quality Software Design:

Page 42: Industry does not agree with the statement that software functioning cannot be tested after initial installation. On the contrary, management measures are in place to verify stimulus to response testing on a regular frequency (preventative maintenance (PM) program) and issue tracking systems are in place to react to any abnormal finding during operations or PM's. Reference to common mode failure only applies to multiple IROFS for a given accident sequence in one system.

Page 44: Regarding the four items listed by level of risk, Item 3 is not currently required by SIL certification companies to have the PC based software verified in order to certify a PLC for specific SILs. The PC based software that is provided by the PLC vendor is an engineering environment that contains the toolsets that are used to create the instructions used by the PLC firmware. The engineering environment should not be considered as part of the safety basis for the system, since this tool is only used during configuration and/or testing of the system.

References to "Commercial Grade Dedication" should be removed from this section as this is a software QA section and Commercial Grade Dedication is typically related to hardware. It should also be noted that NQA-1 Part II, Subpart 2.7 Section 302 discusses the requirements for acquired software that was not developed using a standard for its intended application. The acceptable documentation required is demonstrating that the limitations and capabilities of the intended use are tested and bounded. There is no requirement to have the vendor provide a second-party certification for the configuration software.