October 3, 2008

MEMORANDUM TO: Patricia A. Silva, Chief
Technical Support Branch
Special Projects and Technical
Support Directorate
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

FROM: David L. Rahn, Sr. I&C Engineer **/RA/**
Technical Support Branch
Special Projects and Technical
Support Directorate
Division of Fuel Cycle Safety
and Safeguards
Office of Nuclear Material Safety
and Safeguards

SUBJECT: SUMMARY OF THE SEPTEMBER 3, 2008, CATEGORY 2 PUBLIC MEETING AND TELECONFERENCE WITH THE NUCLEAR ENERGY INSTITUTE AND INDUSTRY, TO DISCUSS TASK WORKING GROUP #7, DIGITAL INSTRUMENTATION AND CONTROL FOR FUEL CYCLE FACILITIES

On September 3, 2008, Task Working Group (TWG) #7 held a Category 2 Public Meeting and Teleconference to discuss various issues related to fuel cycle facility digital instrumentation and control (I&C) problem statements and proposed licensing methodology.

A discussion was held regarding the draft White Paper submitted by Glen H. Smith of GE-Hitachi Fuels Growth Programs (GE-H) titled, “Alternative Approach for Evaluating Independence of Digital Controls” (see Enclosure). The paper was prepared in an effort to develop a justification for using a common, highly reliable control system to provide control of two independent control measures used as items relied on for safety (IROFS) for either criticality prevention or other safety measures. In it, an approach is advocated to evaluate the relative degree of independence that may exist between control channels based on the degree of overall reliability of the common controller. The paper makes use of the postulate that even though events may have been calculated as being mutually exclusive or mutually independent (such as that assumed when applying the Double Contingency Principle) in the world of physics there still remains a degree of interdependency, no matter how casual.

CONTACT: David L. Rahn, NMSS/FCSS
(301) 492-3115

The White Paper explores a method for evaluating the overall reliability of a digital process control system based on how well the design of the proposed control system complies with (i.e., degree of compliance) a set of system design reliability attributes that may be advocated in a referenced industry consensus standard. On the basis of this compliance, reliability (Beta) factor is computed, and then judged against a set of acceptance criteria, such that the control system being analyzed could be judged as one that is highly robust and reliable, or one which requires additional controls/management measures, or one that is not acceptable. The White Paper further proposes that a digital control system so judged to be highly robust and reliable would be considered reliable enough such that its potential contribution to common cause failure which could affect two independent safety control measures, were found to be negligible.

Several comments regarding the potential for adopting this theory were made by participants. Dr. Arndt requested clarification as to where he could find literature supporting the use of this type of theory. Mr. Smith (GE-H) replied that this paper was roughly based on the principles of Layers of Protection Analysis (LOPA) and the system of qualitatively calculating reliability attributes described in a paper presented by R. A. Humphreys, "Assigning a Numerical Value to the Beta Factor Common Cause Evaluation," **Reliability'87**, 1987. [Today this evaluation discussion is used in conjunction with Annex A, "Methodology for quantifying the effect of hardware-related common cause failures in Safety Instrumented Functions," which is part of the Instrumentation, Systems, and Automation (ISA) Society's Technical Report, ISA-TR84.00.02-2002 – Part 1, Safety Instrumented Functions (SIF) – Safety Integrity Level (SIL) Evaluation Techniques part 1: Introduction.] Several others wondered which attributes and what sources of data could be used for developing estimates of the appropriate beta factors to assign to describe the relative reliability for a particular design of control system. Mr. Smith stated that the best estimate would be one which draws information from a wide variety (library) of recognized standards—not just one or two standards. For example, attributes of diversity, software quality, isolation from normal control functions, etc., could be used from descriptions within existing industry design standards, supplemented by attributes that are defined within reliability based standards or texts, such as "fail safe", "self-announcing", "degree of dependence or independence", "probability of failure on demand" (ISA S84.00.01 or IEC 61508/61511 usage or within NUREG 1520), among others.

In the event that the beta factor thus calculated appears to be not high enough to provide the risk reduction capability sought in the control system application, externally applied management measures could be used to improve it. For example, special software, possibly prepared using a diverse language from that of the normal process control software, could be prepared to closely monitor the process data. Such software could be distributed among many processors to check to see if certain critical processes are being performed properly, and if not, a signal could be generated to stop the process, ensure it is put into the "safe state," and warn the operator. Another example of an effective management measure is to develop a detailed set of functional specifications and software requirements specifications when planning to procure and install a new digital process control system. (An example of the contents of such a functional specification is included in Appendix B to Mr. Smith's draft White Paper.) Among the specifications contained within the functional specifications document would be a description of how the controls should be partitioned so as to control each functional area of the process. A reliability table should be prepared for each partition of the process being controlled. For example, in addressing the double contingency principle, if material mass and moderator presence are two of the independent parameters being controlled within a process, the adverse and concurrent change of which is necessary in order to result in a nuclear criticality accident, then separate reliability tables should be prepared for the set of proposed IROFS, for each

parameter. The reliability design attributes for each parameter should be qualitatively assessed to determine whether there is sufficient reliability to consider that control system to be robust enough. If not, the proposed control measure(s) should be augmented with additional controls in order to achieve the degree of risk reduction deemed appropriate.

Further, the digital control system is designed to mitigate hazards that are of either a low, medium, or high consequence. The control measures applicable to mitigating high consequence events may require considerably more high reliability attributes than those for low consequence events. The methodology described above for qualitatively evaluating reliability of a control system design and implementation could also be used to qualitatively evaluate the relative reliability of the set of control measures applied to each parameter being controlled when mitigating high consequence events, to assure that sufficient high reliability design attributes have been incorporated.

The next public meeting will be a teleconference to be held Thursday, October 9, 2008.

ACTION ITEMS:

Item	Description	Responsibility
1.	Consideration of Nuclear Energy Institute (NEI)/Industry comments into the draft interim staff guidance (ISG) for Problem Statement 3	NRC Staff
2.	Evaluate IEEE 1012 V&V Requirements for Procurement Control and Incoming Quality Control	All
3.	Schedule visit to AREVA Richland, WA fuel manufacturing facility	David Rahn
4.	(From July meeting) Provide NEI position statement on the use of Digital I&C as Items Relied on for Safety in Criticality Safety applications	Felix Killar
5.	Update and re-issue drafts of Problem Statements 1,3, and 5, and prepare a rough draft of PS 4	David Rahn

PARTICIPANTS

NRC and external stakeholders, including members of NEI, industry representatives, consultants to the nuclear industry, and interested members of the Public:

NRC	Industry
D. Rahn	Felix Killar, NEI*
W. Smith	Janet Schlueter, NEI
P. Silva	Gordon Clefton, NEI
C. Doutt	Ed Prytherch, Westinghouse*
S. Bailey	Steve Powers, Areva*
S. Arndt*	Charlie Vaughan, NEI*
D. Edwards	Glenn H. Smith, GNF-A*

* Attended via teleconference

Enclosure: Draft White Paper submitted by Glen H. Smith of GE-Hitachi Fuels Growth Programs titled, “Alternative Approach for Evaluating Independence of Digital Controls.”

Safety (IROFS), for each parameter. The reliability design attributes for each parameter should be qualitatively assessed to determine whether there is sufficient reliability to consider that control system to be robust enough. If not, the proposed control measure(s) should be augmented with additional controls in order to achieve the degree of risk reduction deemed appropriate.

Further, the digital control system is designed to mitigate hazards that are of either a low, medium, or high consequence. The control measures applicable to mitigating high consequence events may require considerably more high reliability attributes than those for low consequence events. The methodology described above for qualitatively evaluating reliability of a control system design and implementation could also be used to qualitatively evaluate the relative reliability of the set of control measures applied to each parameter being controlled when mitigating high consequence events, to assure that sufficient high reliability design attributes have been incorporated.

The next public meeting will be a teleconference to be held Thursday, October 9, 2008.

ACTION ITEMS:

Item	Description	Responsibility
1.	Consideration of Nuclear Energy Institute (NEI)/Industry comments into the draft interim staff guidance (ISG) for Problem Statement 3	NRC Staff
2.	Evaluate IEEE 1012 V&V Requirements for Procurement Control and Incoming Quality Control	All
3.	Schedule visit to AREVA Richland, WA fuel manufacturing facility	David Rahn
4.	(From July meeting) Provide NEI position statement on the use of Digital I&C as Items Relied on for Safety in Criticality Safety applications	Felix Killar
5.	Update and re-issue drafts of Problem Statements 1,3, and 5, and prepare a rough draft of PS 4	David Rahn

PARTICIPANTS

NRC and external stakeholders, including members of NEI, industry representatives, consultants to the nuclear industry, and interested members of the Public:

NRC	Industry
D. Rahn	Felix Killar, NEI*
W. Smith	Janet Schlueter, NEI
P. Silva	Gordon Clefton, NEI
C. Doutt	Ed Prytherch, Westinghouse*
S. Bailey	Steve Powers, Areva*
S. Arndt*	Charlie Vaughan, NEI*
D. Edwards	Glenn H. Smith, GNF-A*

* Attended via teleconference

Enclosure: Draft White Paper submitted by Glen H. Smith of GE-Hitachi Fuels Growth Programs titled, “Alternative Approach for Evaluating Independence of Digital Controls.”

DISTRIBUTION:

FCSS r/f	TSB r/f	DEdwards, FCSS	CDoutt, NRR	SBailey, NRR
WSmith,	FCSS	PMNS	SArndt, NRR	

ADAMS Accession No.: ML082750394 (Memo) ML082750392

OFFICE	FCSS/TSB	FCSS/TSB	FCSS/TSB
NAME	DRahn	PJenifer	PSilva
DATE	10/2/08	10/1/08	10/3/08

OFFICIAL RECORD COPY