APRIL 13, 2007

PROJECT PLAN - TWG # 3
RISK-INFORMING DIGITAL I&C

1. BACKGROUND:

The Risk-Informing Digital Instrumentation and Control (RIDIC) Task Working group (TWG) will address issues related to the risk assessment of digital systems with particular emphasis on risk-informing digital system reviews for operating plants, new reactors and fuel cycle facilities. The TWG efforts will be consistent with the NRC's policy statement on probabilistic risk assessment (PRA), which states, in part, the NRC supports the use of PRA in regulatory matters "to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."

Historically, analog instrumentation and control (I&C) systems can be modeled to the level necessary for the PRA to support risk-informed decision-making. Although digital I&C systems are intended to be at least as reliable as the analog systems they replace, digital systems have unique failure modes. Of significant concern are digital I&C system common cause failures that can propagate to multiple safety channels and divisions thereby defeating the defense-in-depth and diversity that was considered adequate for an analog I&C system. Since digital systems play an increasingly important role in nuclear facility control and safety systems, the need for risk assessment methods for digital I&C systems is evident.

The current methodology for evaluating a digital I&C system in either an operating plant or new reactor involves a broad range of deterministic guidance for the development, testing, implementation, and maintenance of digital systems to manage digital system failures. This guidance is "process based" in that the regulatory guidance is designed to provide software and hardware of "high quality" with adequate diversity (of various types) such that the potential for failure, including common cause, is minimized. Specific guidance is provided to assess defense-in-depth and diversity by identifying potential vulnerabilities to digital system common cause failures that could disable a safety function. Where potential vulnerabilities are identified, diverse means are put in place to perform either that safety function or a different safety function. However, these reviews typically involve significant staff effort in the determination of adequate defense-in-depth and diversity when using current staff guidance.

To address this, the TWG task is to evaluate the feasibility of risk-informing the digital system evaluations with the intent of improving the effectiveness and efficiency of the digital system review process while adhering to the five key principles of risk-informed decision-making including adequate defense-in-depth and diversity when implementing a digital I&C system either as a retrofit or new reactor installation.

Draft

2. SCOPE:

One of the key concerns with the current state-of-the-art in digital system modeling is it does not yet support risk-informed decision-making for digital systems, particularly with respect to software reliability quantification. Therefore, adequate digital system risk and reliability methods are needed to support the integration of digital systems into a risk evaluation method. After this risk method is developed, the NRC must also develop additional staff policy or guidance to support risk-informing digital system reviews.

As part of risk-informing the current regulatory process for the review of digital systems, there is a need to develop NRC guidelines to establish quality and completeness of digital system risk and reliability modeling in current generation plant PRAs and PRAs being developed to support Part 52 Design Certifications (DC) and Combined Licensee (COL) applications. These PRAs need to be completed in the short term. Although current guidance (i.e., Regulatory Guide 1.200, etc.) provides attributes associated with PRA quality, there is limited guidance available as to the completeness of digital I&C system modeling, the level of detail needed in digital I&C system modeling, and the uncertainties associated with digital system modeling. Guidance as to what risk metrics are appropriate for evaluating digital I&C systems in operating reactors and DC and COL PRAs also may be needed. Additionally, in the short term, guidance on how risk-insights could be used to support digital I&C systems reviews in the evaluation of key digital system issues, such as diversity and defense-in-depth and inter-channel communications is needed.

The NRC is actively working to develop tools and methods to perform risk assessments of nuclear power plant digital systems. NRC is investigating both traditional fault tree/event tree methods and dynamic methods that may be used to support risk-informed digital system reviews. The NRC staff recognizes the industry's interest in risk-informing digital system reviews, and seeks to leverage insights and approaches developed by industry in the staff resolution process. However, the NRC also recognizes the challenges in integrating digital systems into PRAs and the practicality of using a PRA to assess digital systems. Therefore, guidance on how to risk-inform digital system applications and associated performance based acceptance guidelines to support licensing of operating reactor upgrades, new reactors, and fuel cycle facilites is also needed.

The TWG recommendations are not expected to involve significant changes to NRC policy or rulemaking. However, recommendations proposed may impact the regulatory burden for both NRC staff and industry. When developing recommendations, these burdens will be considered in conjunction with the potential benefit.

Therefore, the following will be addressed by the RIDIC TWG:

1. The use and application of risk-insights in the evaluation of digital I&C systems for both operating and new reactors.

2. Tools and methodologies to enable improved risk assessments of digital I&C systems

in nuclear power plants.

3. Regulatory guidance to enable the use of risk-informed decision-making in the evaluation of digital I&C systems for operating and new reactors.

4. The resolutions to other key digital issues are integrated into the RIDIC TWG recommendations.

The following define the limitations of the RIDIC TWG scope:

1. Work products will be consistent with the five key principles of risk-informed decision-making

2. Work Products will be consistent the commission guidance outlined in Staff Requirements Memorandum (SRM) to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactors (ALWR) Designs,"

3. Security issues (i.e, cyber security) are not within the TWG scope.

4. The RIDIC TWG schedules represent only goals and milestones as they do not reflect budget or priority impacts on current staff schedules and budgets

3. PROBLEM STATEMENT:

The NRC and nuclear power industry share the goal of risk-informing the decision-making in licensing reviews of digital systems for current and future reactors and fuel facilities. However, currently there is no detailed guidance on what would constitute adequate digital system modeling in probabilistic risk assessments (PRAs), including: modeling of digital system common-cause failures (including software), level of modeling detail, failure data, adequacy of modeling methods, uncertainties and interfacing digital system models with the rest of the PRA. There is also no detailed guidance on integrating risk insights into digital system reviews or risk-informing digital system reviews.

PROBLEM 1

Existing guidance does not provide sufficient clarity on how to use current methods to properly model digital systems in PRAs for design certificate applications or license applications (COL) under Part 52. The issue includes addressing common-cause failure modeling and uncertainty analysis associated with digital systems.

PROBLEM 2

Using current methods for PRAs, NRC has not determined how or if risk-insights can be used to assist in the resolution of specific key digital system issues in operating reactor

draft

licensing action requests.

PROBLEM 3

An acceptable state-of-the-art method for detailed modeling of digital systems has not been established. An advancement in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems for current and future reactors and fuel facilities.

4. DELIVERABLES:

For Problem 1:

a. Issue interim guidance addressing use of current methods in modeling of digital systems for design certification and COL application PRAs.

b. In the longer term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

For Problem 2:

a. Develop, if possible, an acceptable approach for using risk insights in operating reactor and fuel facility licensing reviews of digital systems, including consideration of proposed industry methods.

b. If an acceptable approach can be established, issue interim guidance and acceptance criteria for use of risk insights in operating reactor and fuel facility licensing reviews of digital systems.

c. In the longer term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

For Problem 3:

a. Identify an approach to implement appropriate collaboration with and leverage the capabilities of the industry, international counter parts, other industries and NRC staff and contractors to develop the technical basis for state-of-the-art methods for modeling of digital systems to support risk-informed decision-making for digital systems, including: (1) review of current modeling methods (including software modeling), (2) characteristics of acceptable modeling methods, (3) assessment of failure data, (4) criteria for level of modeling detail, (5) assessment of uncertainties, and (6) defining how to interface digital system models with the rest of the PRA.

b. Issue regulatory guidance on risk-informed decision-making review methods applicable to digital I&C systems.

c. Update NRC PRA data, models and tools to support NRC assessment of digital

draft

system risk and reliability.

draft

5. MILESTONES, ASSIGNMENTS AND DELIVERABLES:

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due date**	**Fsct/Actual**	**Lead**	**Support**
From Problem Statement 1					
1a) Industry provides technical paper that discusses lessons learned and proposed guidelines associated with modeling of digital systems for DC and COL applications	✓		F	NEI	N/A
1b) CRGR interaction (as needed)			F	NRC	
1c) Issue draft interim guidance if appropriate	✓		F	NRC	N/A
1d) Receive public comments.			F	NRC	N/A
1e) CRGR interaction (as needed)			F	NRC	
1f) ACRS interaction (as needed)			F	NRC	
1g)Issue final interim guidance if appropriate	✓		F	NRC	N/A
From Problem Statement 2					
2a) Industry provides technical paper that proposes simplified modeling methods using risk insights to support reviews of operating plant digital systems.	✓		F	NEI	N/A
2b) CRGR interaction (as needed)			F	NRC	
2c) Issue draft interim guidance if appropriate	✓		F	NRC	N/A

draft

NEAR-TERM					
Milestones, Assignments and Deliverables	**Deliverable**	**Due date**	**Fsct/Actual**	**Lead**	**Support**
2d) Receive public comments.			F	NRC	N/A
2e) CRGR interaction (as needed)			F	NRC	
2f) ACRS interaction (as needed)			F	NRC	
2g)Issue final interim guidance if appropriate	✓		F	NRC	N/A
LONG -TERM					
From Problem Statement 3 Dynamic and Traditional PRA					
3a) Develop risk-Informed decision-making review methods applicable to digital systems.	✓		F	NRC	N/A
3b) CRGR interaction (as needed)					
3c) Issue draft guidance	✓		F	NRC	N/A
3d) Receive public comments.			F	NRC	N/A
3e) CRGR interaction (as needed)			F	NRC	
3f) ACRS interaction (as needed)			F	NRC	
3g) Issue final guidance	✓		F	NRC	N/A

Draft