Initiative: Risk-Informing Digital Instrumentation and Control

Lead Office/Division: Task Working Group-3 (TWG-3) NRR/DRA
Supporting Offices/Divisions: RES, NRO and NRR

Description

The basis for the digital instrumentation and control initiative was derived from the November 8, 2006 Commission meeting, the December 6, 2006 Staff Requirements Memorandum (SRM) and the January 12, 2007 memorandum from the Executive Director for Operations (EDO) that chartered the Digital I&C Steering Committee. Also reflected is the Commission's directive following the June 7, 2007 meeting with the Advisory Committee on Reactor Safeguards (ACRS) and the associated SRM M070607, dated June 22, 2007.

The digital I&C TWGs, including TWG-3, "Risk-Informing - Digital Instrumentation and Control Systems," were established to include technical staff from appropriate NRC offices to focus on six key areas including digital system risk. The TWG interacts with industry counterparts to facilitate discussion of technical and regulatory issues and the development of recommendations to effectively address digital I&C concerns for each TWG area. The NRC representatives in each TWG are responsible for the development of their individual TWG project plans and the execution of those plans. The TWGs coordinate actions between groups to ensure consistency and alignment.

Background

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 reactor protection I&C system.

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.

TWG-3

TWG -3 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-3 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."

The TWGs interface with industry-identified contacts in each of the key areas. The industry contacts will interact as necessary with reactor vendors, licensees, applicants, and other industry stakeholders to obtain design information that may be needed to support the work of the TWGs.

The industry contacts have provided input to the problem statements, deliverables, and milestones related to individual TWG project plan objectives. The industry contacts have provided input on the schedules for completing the deliverables. Some industry contacts have indicated that they will provide technical papers to the TWGs to address specific issues. The TWGs have considered industry's input in the development of the project plan.

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. The NRC must also develop additional staff policy or guidance to support risk-informing digital system reviews.

A TWG -3 task will evaluate the feasibility of risk-informing 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.

To address these issues, TWG-3 developed the following problem statements:

PROBLEM STATEMENT 1 – Modeling Digital Systems in PRA: 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 STATEMENT 2 – Risk Insights: 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.

PROBLEM STATEMENT 3 - State-of-the-Art: An acceptable state-of-the-art method for detailed modeling of digital systems has not been established. An advance in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems

Completed Milestones (date complete)

- Public Meetings (TWG-3)

  Five public meetings have been held with industry (2/23/2007, 4/11/2007, 5/30/2007, 7/11/2007 and 8/14/2007)

- Issued Digital System Project Plan (7/12/07)

Future Milestones

Selected Major Near Term Milestones and Schedules				
Major Milestones	**Original Target Date**	**Revised Date**	**Completion Date**	**NRC Responsibility**
Problem Statement 1				TWG-3 (NRR/NRO/RES)
Issue DRAFT guidance	November 2007			TWG-3 (NRR/NRO/RES)
Issue Guidance	March 2008			TWG-3 (NRR/NRO/RES)
Problem Statement 2				TWG-3 (NRR/NRO/RES)
Receive Industry White Paper	August 31 2007		August 2007	NEI
Problem Statement 3				TWG-3 (NRR/NRO/RES)
Publish NUREG/CR on use of traditional PRA methods for modeling digital systems	January 2008			RES