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 was established to address issues related to the risk assessment of digital systems with particular emphasis on risk-informing digital system reviews for operating plants and new reactors. The TWG-3 efforts are to 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."

TWG-3 has interfaced with industry-identified contacts in each of the key areas. The industry contacts 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 TWG.

The industry contacts have provided input to the problem statements, deliverables, and milestones related to the TWG-3 project plan objectives. The industry contacts have provided input on the schedules for completing the deliverables and have provided technical papers to address specific issues. TWG-3 has 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.

TWG-3 task evaluated 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 – Evaluation of digital systems in PRA: Existing guidance does not provide sufficient clarity on how to use current methods to properly evaluate digital systems in PRAs for DC or 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 advancement in the state-of-the-art is needed to permit a comprehensive risk-informed decision making framework in licensing reviews of digital systems

The TWG issued an updated project plan on March 14, 2008. The TWG has held several public meetings with industry stakeholders since April 2007. On December 3, 2007, the staff issued the draft interim staff guidance (ISG) for new reactors for public comment. This ISG is intended for use in reviewing current methods in modeling digital systems for design certification and combined license (COL) application PRAs. The TWG discussed the draft ISG with stakeholders in public meetings held in February, March, and May 2008 and with the Advisory Committee on Reactor Safeguards (ACRS) on March 20, 2008, and May 11, 2008. The TWG also supported a Commission brief on April 7, 2008. After addressing ACRS and industry comments, the staff issued the TWG ISG on August 11, 2008.

The ACRS also provided comments during two briefings by the staff on the application of traditional PRA methods to digital systems (April 17, 2008, and May 8, 2008). The ACRS emphasized the importance of failure mode identification, the limitations of

sensitivity studies that dealt with probabilities, the usefulness of available failure rate data sources, and the current limitations of "traditional" PRAs in identifying failure modes. Given the ACRS comments and the staff's concerns, the staff reassessed the problem statement and associated project plan on the application of current PRA methods to risk-inform specific digital systems issues for operating reactors. The concern is that given the stated limitations in PRA technology, the development and implementation of a risk-informed methodology per the current project plan using traditional PRA methods may be premature. However, the staff continues its research into PRA methodologies for assessment of digital system risk and plans to publish two NUREG-series reports—one on approaches for using traditional PRA methods for digital systems and another that benchmarks two dynamic methodologies for reliability modeling of digital systems. The staff completed the first report in August 2008 and will finish the second report in October 2008. These two reports continue the agency's overall effort to advance the state of the art in digital systems risk and reliability modeling to enable the use of risk-insights in licensing reviews of digital systems and to incorporate related models into nuclear power plant PRAs. In addition, the staff received a Nuclear Energy Institute (NEI) white paper on May 12, 2008, that compared industry approaches to modeling digital systems to draft staff criteria and review guidelines. The staff received a second NEI white paper on May 19, 2008, that assessed the benefits and risks of diverse actuation system functions. Both NEI white papers were issued in support of the project plan and will be considered as the staff continues work to identify potential review areas where risk insights from PRA modeling of digital systems may be applicable to staff reviews of operating plants and new reactors.

<u>Completed – Meetings and Project Plan</u>

- Public Meetings (TWG-3)

  Public meetings held with industry (1/14/2008, 2/8/2008, 3/21/2008, 5/5/2008, 7/10/2008)

  Meetings with ACRS (3/20/2008, 4/11/2008, 4/17/2008, 5/8/2008)

  Commission Brief (4/7/2008)

- Issued initial Digital System Project Plan (7/12/07 Revision 0) Revision 1 to the project plan was issued March 14, 2008.

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 Staff Interim Guidance	November 2007	Develop Draft Completed 11/06/2007	12/03/2007	TWG-3 (NRR/NRO/RES)
Receive Industry Feedback	January 2008	As Scheduled	01/04/2008	TWG-3 (NRR/NRO/RES)
Discuss final version of draft Interim Staff Guidance	02/08/2008	As scheduled	02/08/2008	TWG-3/NEI/Public
Issue Interim Staff Guidance	March 03/28/2008	July 7/30/2008	August 8/11/2008	TWG-3 (NRR/NRO/RES)
Problem Statement 2				TWG-3 (NRR/NRO/RES)
Identify potential review areas where risk insights may be applied	January 2008	As scheduled	01/14/2008	NEI
Receive Industry White Papers on applying risk insights to selected ISGs	August 31	04/01/2008 Delayed again 04/30/2008	May 5/19/2008 5/12/2008	NEI
Industry issues topical/ proposal of pilot application	July 2008			NEI
Issue Interim Staff Guidance	September 2009			TWG-3 (NRR/NRO/RES
Problem Statement 3				TWG-3 (NRR/NRO/RES)
Send to Publications NUREG/CR on use of traditional PRA methods for modeling digital systems	April 2008	August 2008	August 2008	RES
Send to Publications NUREG/CR Benchmark Implementation of Two Dynamic Methodologies for Reliability Modeling of DI&C	October 2008			RES

Additional information may be found on the NRC public website at:

http://www.nrc.gov/about-nrc/regulatory/research/digital.html

The Digital I&C Project Plan can be viewed at:

http://www.nrc.gov/about-nrc/regulatory/research/digital/steering-committee.html