**Digital Instrumentation and Control Probabilistic Risk Assessment**

Lead Office/Division: RES/DRA
Supporting Offices/Divisions: RES/DE, NRO and NRR

Description

The U.S. Nuclear Regulatory Commission's (NRC's) current licensing process for digital systems rests on deterministic engineering criteria. In its 1995 probabilistic risk assessment (PRA) policy statement, the Commission encouraged the use of PRA technology in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data. Although much has been accomplished in the area of risk-informed regulation, the process of risk-informed analysis for digital systems is not fully developed. Since digital instrumentation and control (I&C) systems are expected to play an increasingly important safety role at nuclear power plants (NPPs), the NRC established a plan for digital system research defining a coherent set of projects to support regulatory needs (ADAMS Accession No. ML100541484). One of the projects included in this research plan addresses risk assessment methods and data for digital systems (described in Section 3.1.6 of the plan, and supported by work under Sections 3.1.5 and 3.4.5). Digital I&C systems have unique characteristics compared with analog I&C systems, such as using software, and may have different failure causes and/or modes; hence, incorporating them in NPP PRAs entails special challenges.

The objective of the NRC's digital system risk research is to identify and develop methods, analytical tools, and regulatory guidance for (1) including models of digital systems in NPP PRAs, and (2) incorporating digital systems in the NRC's risk-informed licensing and oversight activities. Previous and current RES projects identified a set of desirable characteristics for reliability models of digital systems and have applied various probabilistic reliability modeling methods to an example digital system (i.e., a digital feedwater control system [DFWCS]). Several NUREG/CR reports, which have received extensive internal and external stakeholder review, document this work. The results of these "benchmark" studies have been compared to the set of desirable characteristics to identify areas where additional research might improve the capabilities of the methods. One specific area currently being pursued by RES is the quantification of software reliability. To examine the substantial differences in PRA modeling of software (versus conventional NPP components), in May 2009, RES convened a workshop involving experts with knowledge of software reliability and/or NPP PRA (ADAMS Accession No. ML092780607). At the workshop, the experts established a philosophical basis for modeling software failures in a reliability model.

Subsequently, RES reviewed a spectrum of quantitative software reliability methods (QSRMs) to catalog potential methods that can serve to quantify software failure rates and per-demand failure probabilities of digital systems at NPPs, such that the system models can be integrated into a PRA (ADAMS Accession No. ML102240566). The QSRMs were identified by reviewing research on digital system modeling methods sponsored by the NRC or by the National Aeronautics and Space Administration, performed by international organizations, and published in journals and conferences. The strengths and limitations of QSRMs for PRA applications were categorized, described, and evaluated. In addition, a set of desirable characteristics of a QSRM was established.

RES is currently in the process of evaluating the QSRMs against the set of desirable characteristics, to assist in selecting one or two candidate QSRMs. The candidate QSRMs will be applied to an example software-based protection system in proof-of-concept studies.

The results of the benchmark studies also highlighted the following areas where enhancement in the state-of-the-art for PRA modeling of digital systems is needed:

- approaches for defining and identifying failure modes of digital systems and determining the effects of their combinations on the system
- methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures
- better data on hardware failures of digital components, including addressing the potential issue of double-crediting fault-tolerant features, such as self-diagnostics
- better data on the common-cause failures (CCFs) of digital components
- methods for modeling software CCF across system boundaries (e.g., when there is common support software)
- methods for addressing modeling uncertainties in modeling digital systems
- methods for human reliability analysis associated with digital systems
- process for determining if and when a model of controlled processes is necessary in developing a reliability model of a digital system

It should be noted that even if an acceptable method is established for modeling digital systems in a PRA and progress is made in the above areas, (1) the level of effort and expertise required to develop and quantify the models will need to be practical for vendors and licensees and (2) the level of uncertainty associated with the quantitative results will need to be sufficiently constrained so that the results are useful for regulatory applications.

Completed Milestones

- Issued NUREG/CR-6901, "Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments" (February 2006)
- Issued NUREG/CR-6942, "Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments" (October 2007)
- Issued NUREG/CR-6962, "Traditional Probabilistic Risk Assessment Methods for Digital Systems" (October 2008)
- Issued NUREG/CR-6985, "A Benchmark Implementation of Two Dynamic Methodologies for the Reliability Modeling of Digital Instrumentation and Control Systems" (February 2009)
- Issued NUREG/CR-6997, "Modeling a Digital Feedwater Control System Using Traditional Probabilistic Risk Assessment Methods" (September 2009)
- Conducted workshop on the philosophical basis for modeling software failures (May 2009)
- Issued Brookhaven National Laboratory (BNL) technical report, "Workshop on Philosophical Basis for Incorporating Software Failures in Probabilistic Risk Assessment" (November 2009)

- Issued BNL technical report, “Review of Quantitative Software Reliability Methods” (September 2010)

Future Milestones

- Issue final NUREG/CR that documents selection of candidate QSRMs to be applied in proof-of-concept studies (May 2012)
- Issue final NUREG/CR that documents the application of the first candidate QSRM to an example digital protection system (November 2013)
- Issue final NUREG/CR that documents the application of the second candidate QSRM to an example digital protection system (June 2014)