U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RESEARCH ON RISK-INFORMING DIGITAL I&C REVIEWS

February 23, 2007

Steven A. Arndt
Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering, and Radiological Research,
Office of Nuclear Regulatory Research

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

INTRODUCTION

- Background
- Strategy
- Dynamic Methods Research
- Tradition Methods Research
- Short Term Actions
- Summary

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

BACKGROUND

- Licensing digital systems using risk-informed guidance presents challenges
  - Industry has expressed interest in incorporating risk insights and risk-informed decisionmaking in the licensing of digital systems.
  - NRC regulatory guidance does not currently provide specific support for use of quantitative risk analysis in licensing digital systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

BACKGROUND

- Licensing digital systems using risk informed decisionmaking presents challenges
  - Lack of consensus on an acceptable methodology to evaluate digital system risk (hardware and software).
  - Lack of a generally accepted methodology for inclusion of digital system reliability models in current generation PRAs
  - Research into the strengths and limitations of digital system reliability modeling needs to be completed for NRC to support risk-informed decisionmaking in licensing digital systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

STRATEGY

- Develop guidelines to provide risk-informed acceptance criteria for digital system reviews
- Develop tools and procedures to perform risk-informed digital system reviews
- Conduct research to resolve open technical issues, develop and validate tools, develop guidance needed to implement a risk-informed digital system reviews.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

STRATEGY

- Review available methods
- Develop the most promising methods (both traditional and dynamic) and apply them in a proof-of-concept application
- Exercise the methods (both traditional and dynamic) on a digital protection and control system
- Use the results to develop a review methodology and regulatory guidance.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DYNAMIC METHODS RESEARCH

- Review of the current state of the art and determine best candidate methods for evaluation (Complete, NUREG/CR-6901)
- Develop Benchmark # 1 (DFWCS) (Complete)
- Develop methods and apply to Benchmark # 1 candidate methods to provide proof-of-concept (NUREG/CR goes to press next week)
- Develop Benchmark # 2 (RPS system)
- Apply methods to Benchmark # 2 to provide proof-of-principle example and demonstrate practicality
- Develop and demonstrate integration methods applicable to conventional PRAs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

REVIEW OF THE CURRENT STATE-OF-THE-ART IN DYNAMIC METHODS

- Reviewed of the current state of the art and determine best candidate methods for evaluation
- Determined that Markov and Dynamic Flowgraph methodology (DFM) where the most likely to be successful
- Recommended two benchmark systems to support proof of concept analysis and determine practicality
- Results published as NUREG/CR-6901

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DEVELOP BENCHMARK # 1

- Based on availability, the first benchmark selected was a digital feedwater control system used in a nuclear power plant application.
- System FMEA was completed
- System description was developed based on FMEA, system requirements, design and other information
- A fault injection method coupled with plant and industry data was used to develop failure data

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DEVELOP DYNAMIC METHODS AND APPLY TO BENCHMARK #1

- Developed Markov and DFM methods for use
- Developed a method to integrate model/results into a traditional PRA (dynamic event tree, using cell to cell mapping and post processing)
- Applied Markov and DFM to benchmark #1 to provide proof-of-concept
- Assessed capabilities and limitations of each method
- Prepared, peer reviewed, and will publish NUREG/CR
- Quantification to be provided in next NUREG/CR (draft to peer review in May, 2007)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DEVELOP BENCHMARK # 2

- RPS (Reactor Trip/ ESF) system based on the TELEPERM platform
- Based on a proposed industry configuration
- Benchmark 2 goal is to permit a more thorough examination of:
  - High quality development processes (software)
  - Extensive internal/external communication
  - Less external interactions with the process
  - Redundancy/Defense-in-depth/Diversity
  - Current safety system design strategies
  - Failure modes

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

APPLY TO BENCHMARK #2

- Apply Markov and DFM to benchmark #2
- Compare and assess capabilities and limitations
- Quantify system reliability
- Examine limitations highlighted from benchmark #1 to determine if they have been addressed
- Examine proof-of-principle issues and demonstrate practicality
- Peer review
- Publish NUREG/CR

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

INTEGRATION OF DYNAMIC METHODS INTO PRAs

- Use SAPHIRE as an example event tree/fault tree PRA tool
- Ensure both the dynamic methods and the base PRA account for dependencies (support systems, human errors, input sensors, software, etc.)
- Develop of uncertainty estimation and propagation methods
- Ensure risk important measures work with dynamic methods

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

TRADITIONAL METHODS RESEARCH

- Review of reliability methods and data (Complete)
- Traditional methods selection
- Candidate method illustration
- Apply methods to Benchmark # 1
- Apply methods to Benchmark # 2
- Integration into PRA

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

REVIEW OF RELIABILITY METHODS AND DATA

- Review of reliability methods and data used by non-nuclear industries
- Evaluation and comparison of failure parameter databases
- Review of digital system/software-induced failure experience
- Development of a basis and framework for modeling software failures in terms of failure rates and probabilities
- Failure modes and effects analysis and dependency analysis of Benchmark #1

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

TRADITIONAL METHODS SELECTION

- Review (applications of) traditional methods (e.g., new reactor PRAs and reliability models from other industries)
- Develop criteria for evaluating traditional methods
- Apply criteria to identify candidate methods
- Engage technical community
  - Public meeting (March 2007)
  - Phenomena Identification and Ranking Table (PIRT)-like review process (April 2007)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

CANDIDATE METHOD ILLUSTRATION

- Illustrate how the candidate traditional methods can account for digital system features
- Identify types and sources of data for model quantification
- Refine candidate traditional methods
- Illustrate how models can be integrated into existing PRAs
- Consider reliability quantification methods provided by industry, if any
- Complete draft NUREG/CR (June 2007)
- Conduct peer review of draft NUREG/CR (July 2007 – Sept. 2007)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

APPLY TRADITIONAL METHODS TO BENCHMARK #1

- Apply each candidate traditional method to the benchmark #1
- Quantify system reliability models
- Compare methods in terms of capabilities and limitations
- Consider reliability quantification methods provided by industry, if any
- Complete draft NUREG/CR
- Conduct peer review of draft NUREG/CR

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

APPLY TRADITIONAL METHODS TO BENCHMARK #2

- Apply each candidate traditional method to benchmark #2
- Quantify system reliability models
- Compare methods in terms of capabilities and limitations
- Consider reliability quantification methods provided by industry, if any
- Complete draft NUREG/CR
- Conduct peer review of draft NUREG/CR

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

INTEGRATION INTO PRA

- Illustrate and/or develop methods for integrating reliability models into existing PRAs
- Use SAPHIRE as an example event tree/fault tree PRA tool
- Ensure PRA models account for dependencies (support systems, human errors, input sensors, etc.)

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

POSSIBLE SHORT TERM ACTIVITIES

- NRC is investigating what current digital system risk insights can be derived from current information
  - New reactor reviews
  - Operating reactor reviews
  - Other industries
- NRC is investigating ways to incorporate risk insights into current reviews

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SUMMARY

- NRC has reviewed the most promising available methods and tools for risk and reliability modeling of digital systems
- NRC is develop the most promising methods (both traditional and dynamic) to the point where then can be used in a proof-of-concept application
- NRC is benchmarking these methods (both traditional and dynamic) using a digital protection system and a digital control system to demonstrate their practicality
- Industry is providing put and peer review of the RES products
- NRC is use the information gather as part of the development of the methods to support development of regulatory guidance
- In the short term NRC is investigating ways to incorporate risk insights into digital system licensing reviews