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

WGRISK Task 2007-2

Digital I&C Risk:

Recommendations on the methods and information sources for quantitative evaluation of digital system reliability in PSA

Kevin A. Coyne, Chief
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
March 25-27, 2009

Outline

- Objectives
- Scope
- Milestones
- Results
- Conclusions and Recommendations

Objectives

- Make **recommendations regarding current methods and information sources** used for quantitative evaluation of digital system reliability for PSA applications

- **Identify**, where appropriate, the near and long term **developments** that would be **needed** in order to improve reliability assessments

Scope

- **Discussion** of **current experiences** with reliability modeling and quantification of digital systems
- **Development** of **recommendations**
- Project focuses on Level 1 PSA (internal events) for operating reactors and those which will be constructed in the next 5 years
- Topics include:
  - Actual risk assessment applications
  - Data used
  - How any limitations in methods or data were addressed
  - Recommendations for future research

Milestones

- **Planning and Nominations for task group**
  Spring - Summer 2007 [completed]
- **First Planning Meeting**
  September - October 2007 [completed]
- **Working Meeting**
  Originally scheduled Spring 2008 [completed October 2008]
- **Report to CSNI**
  Originally scheduled December 2008 [provide to PRG in April 2009 and to CSNI in May 2009]
  (Provide recommendations in the areas of methods and data)

Results

- Useful forum for sharing and discussing respective experiences
- Spectrum of opinions on methods for modeling DIC systems
- Wide variation in terms of scope and level of detail for existing models of DIC systems
- General agreement on need to account for software failures
- General agreement on need to address scarcity of probabilistic data
- General agreement on need to continue research to address technical challenges

Conclusions and Individual Participant Recommendations (1 of 2)

- **Method development**
  - Develop a taxonomy of digital component failure modes for common use
  - Develop methods for quantifying software reliability, capturing benefits of fault tolerant features, and addressing human-system interfaces unique to digital systems
  - Evaluate the need and approaches for addressing dynamic interactions
- **Data collection and analysis**
  - Create clearinghouse for collecting hardware data that guarantees anonymity of the data sources
  - Not practical to use operating experience as the only source for estimating software failure rates or probabilities

Conclusions and Individual Participant Recommendations (2 of 2)

- **International cooperation**
  - Joint development of methods on software modeling, common cause failure, and human reliability analysis
  - Sharing of failure data
  - Benchmark study to compare methods
- **Mechanisms for cooperation**
  - Publish technical documents, such as “CSNI Technical Opinion Papers”
  - Share approaches, methods, probabilistic data, results, and insights gained from relevant projects among NEA members