On the Modeling and Review of Digital Systems in DC/COL PRAs

May 30, 2007

Todd Hilsmeier
PRA Licensing Branch
Division of Safety Systems and Risk Assessment
Office of New Reactors

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

INTRODUCTION

- Purpose
- Problem Statement 1
- Project Plan
- Overview of how digital systems were modeled in the AP1000/ESBWR PRAs
- Overview of how digital systems were reviewed as part of the design certification review/approval efforts of AP1000/ESBWR

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

PURPOSE

- Provide a high-level overview of how digital systems were modeled in the AP1000/ESBWR PRAs
- Provide a high-level overview of how digital systems were reviewed as part of the design certification review/approval efforts of AP1000/ESBWR

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

Problem Statement 1

- "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."

- Deliverables
  - Issue interim guidance addressing use of current methods in modeling of digital systems for design certification and COL application PRAs.
  - In the longer term, update regulatory guidance as needed (SRP, Regulatory Guides, etc.).

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

Project Plan

Problem Statement 1 Milestones, Assignments and Deliverables	Due date 2007 or as noted
Major Activity: Develop interim guidance on the use of current PRA methods to properly model digital systems in PRAs for design certification applications or license applications (COL) under part 52.	
1a) Industry provides technical paper that discusses lessons learned and proposed guidelines associated with modeling of digital systems for DC and COL applications.	May
1b) Evaluate industry white paper - identify key principles and methods and document evaluation in a white paper.	August
1c) Review and document in a white paper NRC staff PRA risk-insights and lessons learned, including key principles and methods used in past evaluations of digital systems as part of design certification review/approval efforts (i.e., AP1000, ESBWR, ABWR as applicable).	July
1d) Review and document in a white paper NRC completed digital system research on digital I&C technology including risk-insights, lessons learned, key principles and methods.	August
1e) Review and document in a white paper NRC completed digital I&C operating reactor retrofit experience using digital technology including risk-insights, lessons learned, key principles and methods.	August
1f) Consolidate NRC and industry findings (Tasks 1b, 1c, 1d, and 1e) to establish interim draft guidance and acceptance criteria to evaluate digital systems using risk-insights in DC and COL reviews. Ensure integration of TWG resolutions with TWG#3 interim guidance. Document type to be determined.	September
1g) Complete final draft of interim guidance and acceptance criterion, which incorporates internal NRC review comments. Document type to be determined.	November
Milestones 1h to 1n: - Issue final draft of interim guidance for public review and comment. - Receive public comments. - Finalize guidance recommendations and acceptance criteria. - Issue final interim guidance. Document type to be determined.	December 2007 to June 2008

high-level, preliminary overview will be presented

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

High-Level Overview of How Digital Systems Were Modeled in the AP1000/ESBWR PRAs *

1) Evaluated impact of digital systems on initiating events

Included consideration of the following:

- Identification of initiating events caused by digital systems (e.g., PMS could cause spurious reactor trip, ESF actuation)
- Quantification of impact that digital systems have on initiating event frequency, including the handling of uncertainties in these frequencies
- Identification of initiating events that impact availability of digital systems (e.g., Loss of 120 VAC causes DAS failure)

* More detail information on this topic to be developed by July 2007

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

2) Captured impact of digital systems on PRA success criteria and accident timing

3) Developed system analysis and dependency modeling for digital systems

   Included consideration of the following:

   - Modeling method (e.g., traditional fault tree analysis)
   - Level of detail of modeling, for example:
     - Software: only common cause failures of software modeled
     - Hardware: circuit board level (e.g., power interface boards, analog input boards, output boards)
   - Identification of failure modes (e.g., failure modes identified at the circuit board level for hardware)

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

3) System analysis (continued)

- Basis for assumptions and simplifications made in modeling the digital system
- Recovery actions (e.g., manual actuations in event of digital system failure)
- When is a digital system considered diverse (e.g., PMS and DAS assumed diverse by using different architecture, hardware implementations, and different software)
- The physical and logical dependencies captured in the digital system model, for example:
  - Support systems (e.g., vital ac buses, cooling fans, and HVACs that are needed to support the digital components)
  - Shared components (e.g., power supplies, voters, sensors, and testers)
  - The potential impacts of test and maintenance unavailabilities.(e.g., automatic testing, online self-diagnostic testing, surveillance testing)

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

4) **Modeled digital system common cause failures (CCF) for both hardware (HW) and software (SW)**

Included consideration of the following:

- Basis for identifying potential HW and SW CCF (e.g., considered CCF for those circuit boards with similar hardware and similar software)
- Level of detail at which HW and SW CCF are modeled, for example:

  Software CCF:
  - CCF of "common functions" SW were modeled (e.g., processor functions, I/O processing, communications)
  - CCF of "application" SW were modeled (e.g., SW controlling algorithms, protective/actuation functions)

  Hardware CCF:
  - CCF considered for circuit boards within a system and for board across systems
- Basis for the HW and SW CCF failure probabilities, including the handling of uncertainties in these CCF probabilities

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

5) Estimated the parameters of digital system events (e.g., basic events) modeled in the PRA

Included consideration of the following:

- Source(s) of failure data to estimate failure parameters of digital system events (e.g., operating experience, testing data during design and development, generic databases)
- Basis for computing failure parameters of digital system events from the data sources, including how discrepancies in component boundary/failure modes were handled
- Assessing uncertainties in data

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

6) Captured digital systems in human reliability analysis (e.g., timing issues, manual actuations, etc...)

7) Modeled dependencies across echelons of defense (e.g., sharing of sensors and processors among control systems, reactor trip system, ATWS mitigation systems, and ESFAS) in accident sequence analysis

   Included consideration of the following:

   - Dependencies between initiating events and digital systems (e.g., modeled initiating event by a fault tree or created a specific event tree for the initiating event)
   - Dependencies between systems (e.g., fault trees) caused by digital systems (e.g., traditional link FT/ET method)

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

How Digital Systems Were Modeled in the AP1000/ESBWR PRAs (Continued)

8) Evaluated the impact of digital systems, including their associated uncertainties, on plant risk

Included consideration of the following:

- Basic event importance measures with respect to digital system unavailability (e.g., software CCF, hardware CCF)
- Propagation of parameter uncertainties related to digital systems (e.g., CCF parameters of digital components) in uncertainty analyses of initiating event frequency, system unavailabilities, CDF and LERF
- Sensitivity calculations using alternative assumptions to determine potential risk impacts

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

High-Level Overview of how Digital Systems Were Reviewed as Part of the Design Certification Review/Approval Efforts of AP1000/ESBWR *

1) Evaluated the PRA modeling of digital systems

   - Information on the level of detail and depth of this evaluation to be provided later

* More detail information on this topic to be developed by July 2007

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

Digital System Reviews (Continued)

2) Evaluated digital systems using risk insights from the PRA

- Use of importance/sensitivity studies to show that digital systems have adequate defense-in-depth:
  - Importance measures of basic events in the digital system PRA models (e.g., software CCF, hardware CCF) were reviewed to evaluate the impact that the unavailabilities of these events have on plant risk.
  - Sensitivity studies were performed to assess the impact of uncertainty in software/hardware CCF failure probabilities
  - Evaluation of cutset results containing digital system basic events
- Risk insights have confirmed the importance of diversity in limiting the uncertainties (i.e., software) when implementing digital I&C systems (adequate defense-in-depth)

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

Conclusion

Problem Statement 1 Milestones, Assignments and Deliverables	Due date 2007 or as noted
Major Activity: Develop interim guidance on the use of current PRA methods to properly model digital systems in PRAs for design certification applications or license applications (COL) under part 52.	
1a) Industry provides technical paper that discusses lessons learned and proposed guidelines associated with modeling of digital systems for DC and COL applications.	May
1b) Evaluate industry white paper - identify key principles and methods and document evaluation in a white paper.	August
1c) Review and document in a white paper NRC staff PRA risk-insights and lessons learned, including key principles and methods used in past evaluations of digital systems as part of design certification review/approval efforts (i.e., AP1000, ESBWR, ABWR as applicable).	July
1d) Review and document in a white paper NRC completed digital system research on digital I&C technology including risk-insights, lessons learned, key principles and methods.	August
1e) Review and document in a white paper NRC completed digital I&C operating reactor retrofit experience using digital technology including risk-insights, lessons learned, key principles and methods.	August
1f) Consolidate NRC and industry findings (Tasks 1b, 1c, 1d, and 1e) to establish interim draft guidance and acceptance criteria to evaluate digital systems using risk-insights in DC and COL reviews. Ensure integration of TWG resolutions with TWG#3 interim guidance. Document type to be determined.	September
1g) Complete final draft of interim guidance and acceptance criterion, which incorporates internal NRC review comments. Document type to be determined.	November
Milestones 1h to 1n: - Issue final draft of interim guidance for public review and comment. - Receive public comments. - Finalize guidance recommendations and acceptance criteria. - Issue final interim guidance. Document type to be determined.	December 2007 to June 2008