N6124
DIGITAL SYSTEM DEPENDABILITY PERFORMANCE

Presentation
For
Commissioner Merrifield

June 8, 2006

By
William E. Kemper, Chief
Instrumentation and Electrical Engineering Branch
Division of Fuel, Engineering, and Radiological Research,
Office of Nuclear Regulatory Research

OVERVIEW

- BACKGROUND
- OBJECTIVE
- DIGITAL SYSTEM DEPENDABILITY PERFORMANCE PROJECT OVERVIEW
  - PROCESS
  - OUTCOMES
- RISK-INFORMING DIGITAL I&C REVIEWS
- SUMMARY

BACKGROUND

- NRC has approved several digital, computer-based systems for safety-related (SR) service in nuclear power plants
- These Digital Instrumentation and Control (I&C) systems are installed in operating plants
- Advanced plants will use highly integrated digital instrumentation and controls systems
- Many challenging issues facing NRC
  - Significant increase in complexity
  - Failures of software quality assurance programs (i.e., Palo Verde)
  - Embedded inter-channel communications (i.e., breakdown in separation of redundant channels)
  - Embedded communications between safety and non-safety processors (i.e., breakdown in safety/non-safety separation)
  - Un-quantified failure modes (e.g., software common-mode failures, microprocessor, communication, peripheral components)

OBJECTIVE

- Provide an independent assessment methodology for quantifying digital system safety (including software-hardware interactions) in a risk context that can be directly applicable to probability risk assessments

PLANNED ASSESSMENT OVERVIEW

- NRC will supply Contractor with a safety system as government furnished equipment
  - Potential for vendor-supplied equipment (collaborative arrangement)
- Based on safety assessment method developed by the University of Virginia (UVA) through funding from many contributors
  - NRC has collaborated with UVA since 1998 to develop this method
  - National Science Foundation, Federal Railroad Administration, NASA, Boeing, Lockheed-Martin, Maglev, Union Switch & Signal, others

PLANNED ASSESSMENT OVERVIEW, cont.

- Safety assessment method
  - Develop models representing both “safe” and “unsafe” failures
  - Perform fault-injection experiments on a model of the system (a hardware prototype, a software model, or a combination) to learn system failure characteristics
  - Analyze the results to quantify system and safety reliability
- Average of 12 months per system evaluation
  - Intent is to replicate actual nuclear plant hardware/software configuration(s) to the extent possible (one channel at most)
  - One option is the Oconee RPS/ESF, but this project is not coordinated with the NRC application review schedule

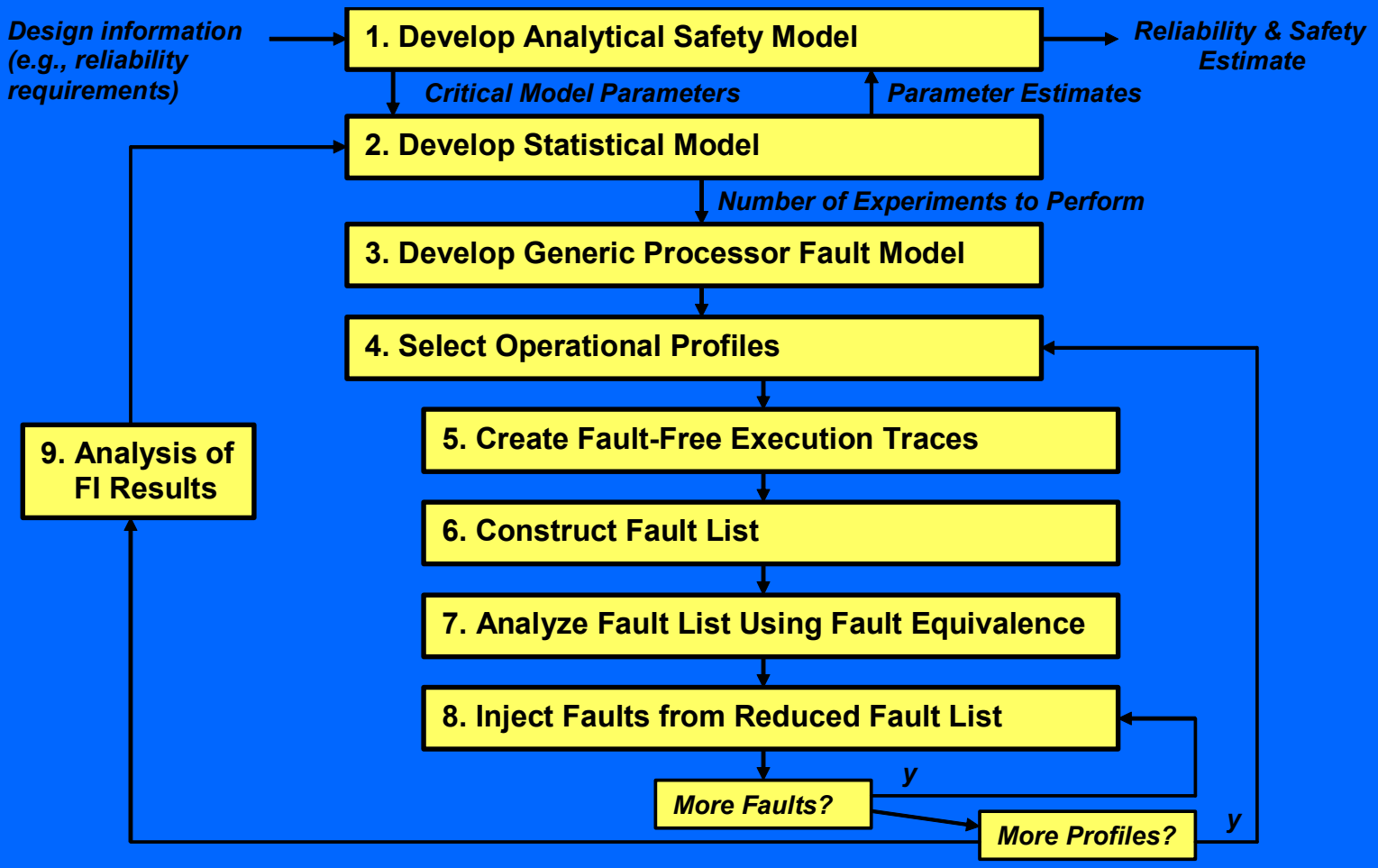
N6124, DIGITAL SYSTEM DEPENDABILITY PERFORMANCE

- TELEPERM XS (TXS) is the first test case
- General Services Administration has issued the purchase order to the vendor for the TELEPERM XS safety system
  - Engineering workstations for system development/operation
  - Gateways (Linux and Windows 2000)
  - TELEPERM XS safety processor (chassis, processor modules, communications modules, some input/output modules)
  - Spare modules
  - Must configure the system prior to testing
    - Work with Oconee and/or AREVA-NP to obtain nuclear application software
    - Engineering workstations will allow NRC to develop custom configurations to support various applications

N6124, DIGITAL SYSTEM DEPENDABILITY PERFORMANCE, cont.

- Status
  - Chairman has concurred on project acquisition memo dated May 16, 2006
  - Source Evaluation Panel is preparing its recommendation on contract award for the Contracting Officer; final decision on vendor pending
  - Expect to award the contract for this project (N6124) by end of July
- Schedule
  - Vendor has begun building the TELEPERM XS system (ordered parts, etc.) June 2006
  - Delivery of TELEPERM XS system ~ October 2006
  - Dependability Performance testing starts January 2007
  - First system assessment completed January 2008

N6124: PROCESS



N6124: OUTCOMES

- Understand better:
  - The behavior of hardware/software systems under the influence of internal and external faults
  - Analysis of consequent errors that might produce system failures
- Analyzed and properly characterized system(s) for:
  - Performance
  - Reliability/Availability quantification
  - Failure modes under anticipated operating conditions
  - Subsystem and system interconnection safety
  - Risk-based failure information for probabilistic risk assessments
- Obtain a tool that can support independent assessment and validation of digital system performance

RESEARCH ON RISK-INFORMING DIGITAL SYSTEM REVIEWS

- NRC research is focused on development of
  - Regulatory Guidance to support risk-informed review of digital systems
    - Development of 1.174 series Regulatory Guide for digital system reviews
  - Detailed models of digital systems and development of reliability modeling methods that can integrate these models into traditional probabilistic risk assessments
    - Review of available modeling methods
    - Development of both traditional and dynamic methods
    - Investigate what models are acceptable
    - Benchmarking results

SUMMARY

- The Digital System Dependability research will augment and supplement the current regulatory process by:
  - Characterizing significant hardware, software, and interface errors;
  - Understanding potential failure modes and the criteria for detecting these failure modes;
  - Modeling of digital systems that could be used to provide empirical evidence of system reliability;
  - Identifying or developing methods and data that enable the NRC to establish the risk important aspects of digital safety systems; and
  - Modeling of digital systems that could be used to support probabilistic risk assessments
- RES plans to evaluate each digital platform approved by the NRC using the selected safety assessment method

BACKUP SLIDE: REFERENCES

- ACRS and NAS recommendations
- PSAM paper laying out the issues (2004)
- NUREG/CR-6901 “Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments” (February 2006)
- Draft NUREG/CR-XXXX “Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk ” (Currently undergoing peer review)
- Letter Report, “Review of Software-Induced Failure Events in Different Industries to Identify Failure Modes and Mechanisms/Causes”
- Draft Regulatory Guide DG-XXXX “An Approach for Plant-Specific, Risk-Informed Decisionmaking: Digital Systems” (scheduled to be sent out for public comment December 2006)