U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital I&C PRA Research

Kevin Coyne, Chief
Probabilistic Risk Assessment Branch
Division of Risk Analysis
Office of Nuclear Regulatory Research
(301-251-7586, Kevin.Coyne@nrc.gov)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Outline of Presentation

- Background
- Objective
- Previous research
- Current and near-term activities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background

- Current licensing process for digital systems is based on deterministic engineering criteria
- Commission's 1995 probabilistic risk assessment (PRA) policy statement encourages use of PRA to the extent supported by the state-of-the-art
- Risk-informed analysis process for digital instrumentation and control (DI&C) systems has not yet been satisfactorily developed

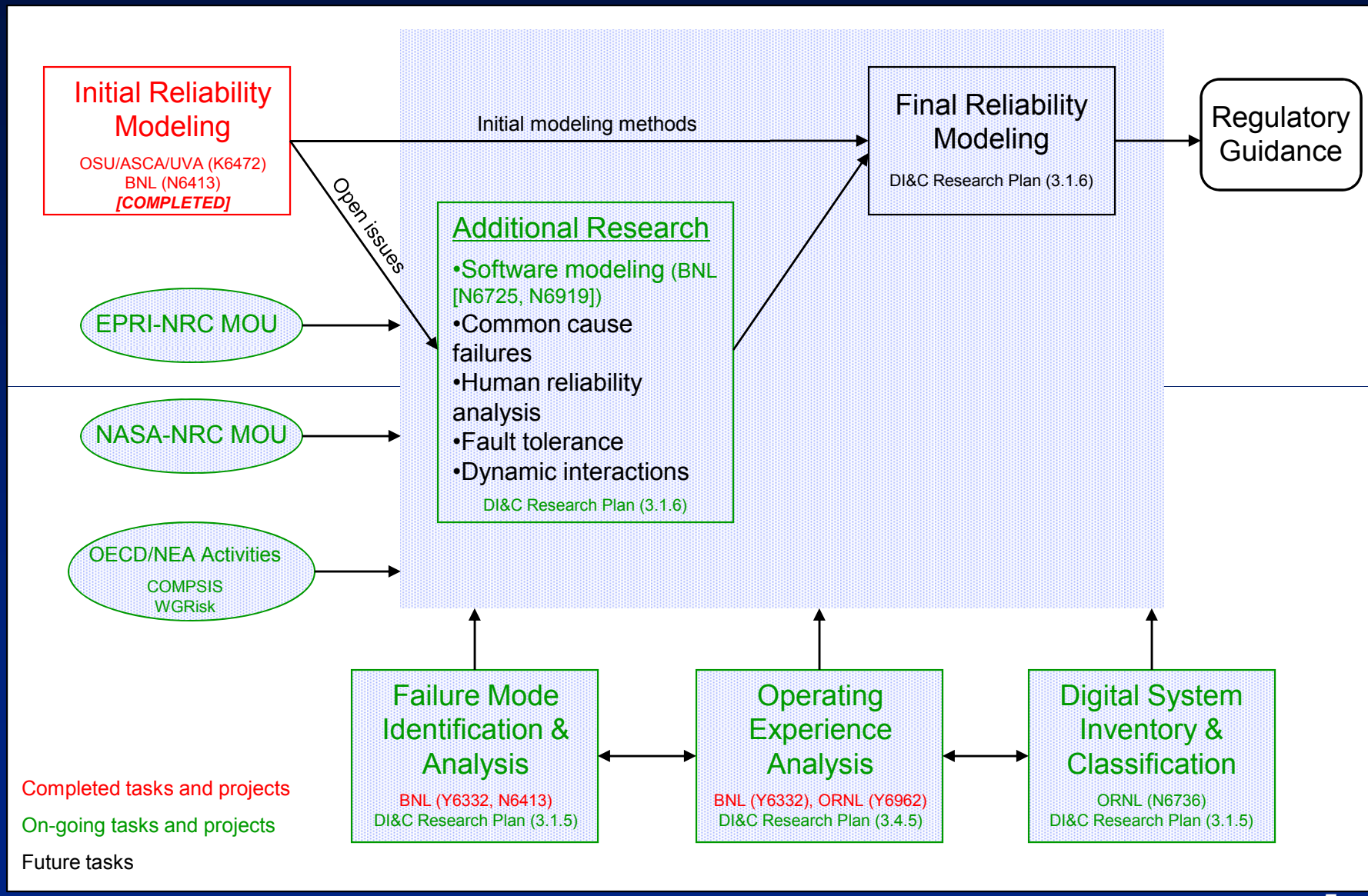
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Objective

- Identify and/or develop methods, analytical tools, and regulatory guidance for:
  - Including digital system models into nuclear power plant (NPP) PRAs
  - Using information on the risks of digital systems to support NRC's risk-informed licensing and oversight activities

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital System Risk Modeling



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Previous Research (1 of 2)

- Failure mode identification and analysis
  - Brookhaven National Laboratory (BNL) (Y6332/N6413) – Failure modes and effects analysis of a digital feedwater control system (DFWCS) (NUREG/CR-6962 [2008], NUREG/CR-6997 [2009])
- Initial reliability modeling
  - Ohio State University/ASCA/University of Virginia (K6472) – Dynamic reliability modeling methods applied to a DFWCS (NUREG/CR-6901 [2006], NUREG/CR-6942 [2007], NUREG/CR-6985 [2009])
  - BNL (Y6332/N6413) – Traditional reliability modeling methods applied to a DFWCS (NUREG/CR-6962 [2008], NUREG/CR-6997 [2009])

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Previous Research (2 of 2)

- Operating experience analysis
  - BNL (Y6332)
    - Study of reliability methods and data used by non-nuclear industries (internal letter report)
    - Collection of failure data and development of database for probabilistic modeling of digital systems (proprietary letter report, though information on Hierarchical Bayesian Method is included in NUREG/CR-6962)
    - Review of software-induced failure experience (Appendix C to initial draft version of NUREG/CR-6962; modified version will be made publicly available in Summer 2010)
  - Oak Ridge National Laboratory (ORNL) (Y6962)
    - Review of operational experience data to identify generic DI&C system failure modes and failure mechanisms and to obtain generic insights (Letter report undergoing review – will be made publicly available)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Current and Near-Term Activities (1 of 3)

- NRC/BNL currently pursuing incorporating software failure into digital system reliability models
  - Workshop on philosophical basis (completed)
    - Basis was established for modeling software failures probabilistically
    - Publicly available BNL report (ADAMS ML092780607)
  - Review of quantitative software reliability methods (QSRMs) (completed)
    - Desirable characteristics for QSRMs for use in PRAs
    - Identification of QSRMs
      - NRC-sponsored research
      - NASA-sponsored research
      - Research performed at international organizations (e.g., VTT and Halden Reactor Project)
      - Open literature research
    - Major categories of reviewed QSRMs
      - Software reliability growth methods
      - Bayesian belief network methods
      - Test-based methods
      - Other methods
    - Publicly available BNL report (ADAMS ML102240566)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Current and Near-Term Activities (2 of 3)

- NRC/BNL currently pursuing incorporating software failure into digital system reliability models (continued)
  - Plan to develop one or two technically sound approaches to modeling and quantifying software failures in terms of failure rates and probabilities
  - Assuming such approaches can be developed, plan to apply them to an example software-based protection system in a proof-of-concept study
- Initiate research to address other “gaps” in the state-of-the-art
  - Data, data, data
  - Common cause failures
  - Fault tolerant features
  - Dynamic interactions
  - Human reliability analysis

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Current and Near-Term Activities (3 of 3)

- Activities that support DI&C PRA
  - Digital system inventory and classification (ORNL – N6736)
    - Preliminary classification/categorization structure of digital systems in current and future NPPs
    - Inventory of digital systems and components used in current and future NPPs
  - Failure mode identification and analysis
    - Electric Power Research Institute (EPRI)-NRC Memorandum of Understanding (MOU) – Failure analysis guideline
    - National Aeronautics and Space Administration (NASA)-NRC MOU – Technical Interchange Meeting (Summer 2010)
    - Organisation for Economic Cooperation and Development (OECD) Nuclear Energy Agency (NEA) Working Group on Risk Assessment (WGRisk) – Failure mode taxonomy
    - NRC Digital System Research Plan FY 2010-FY 2014 – Task 3.1.5 (Analytical Assessment of DI&C Systems)
  - Operating Experience Analysis
    - OECD/NEA – Computer-based Systems Important to Safety (COMPSIS) project
    - NRC Digital System Research Plan FY 2010-FY 2014 – Task 3.4.5 (Operating Experience Analysis)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

BACKUP SLIDES

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Development of Desirable Characteristics of QSRMs

- The desirable characteristics were developed based on the perceived need for reliability models of digital systems in a PRA and the knowledge and experience of the study team in performing research and literature reviews on modeling of digital systems.
- They are expected to address the general guidelines provided in the American Society of Mechanical Engineers (ASME) standard for PRA for NPP applications.
- The desirable characteristics can be used in evaluating available QSRMs and their applications to determine if the characteristics are satisfied.
- Although an itemized evaluation of the methods against the desirable characteristics is beyond the scope of this study and is planned to be included in the next phase of the research, the QSRM review report is useful in performing such an evaluation.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Software Reliability Growth Models

- SRGMs have been used to estimate software reliability measures, such as failure rates, based on test data and to determine whether the software should be released.
- In an SRGM:
  - The occurrence of software failures is modeled as a Non-Homogeneous Poisson Process (NHPP).
  - It is usually (but not always) assumed that, during testing, the detected software faults are fixed perfectly and instantaneously such that the software failure rate decreases and reliability increases with time.
  - How the failure rates decrease is determined by the empirical formula of the SRGM.
- Both continuous- and discrete-time SRGMs* exist.

* Discrete SRGMs will be addressed in the next phase of this work.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Continuous-Time SRGMs (1)

- Continuous-time SRGMs can be categorized into Exponential NHPP, Non-exponential NHPP, and Bayesian models.
- Unification schemes for various NHPP SRGMs have been developed by, e.g., expressing the accumulated number of software faults in similar forms.
- For exponential NHPP models:
  - It is assumed that software failure rate is proportional to the remaining fault content, which is analogous to the rate of radioactive decay of an isotope being proportional to the inventory of the isotope.
  - Effectively, the software failure rate decreases exponentially with time.
  - Exponential NHPP models include Musa's Basic model, Schneidewind's model, Goel's NHPP model, the Generalized Exponential model, Shooman's Exponential model, and Jelinski-Moranda's model, etc.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Continuous-Time SRGMs (2)

- For Non-exponential NHPP models:
  - It is assumed that software failure rate follows the shape of a probability density function of a different distribution, e.g., a Gamma distribution.
  - Non-exponential NHPP models include Musa's Logarithmic Poisson Execution Time Method, Duane's model, (delayed or inflection) S-shaped reliability growth models, etc.
- For Bayesian SRGM models:
  - It is assumed that the failure rate decreases probabilistically/ stochastically with time.
  - The models essentially are an exponential NHPP model that explicitly includes the uncertainty of the failure rate in the model.
- Parameter estimation of SRGMs
  - Maximum likelihood method, Least-square method, and Moment-matching method are commonly used.
  - Usually only point estimate of model parameters is performed but there exists no inherent difficulty in determining the associated uncertainties.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on Continuous-Time SRGMs

- SRGMs are the most popular software reliability methods/models.
- There exists no single SRGM that is universally superior to others, because all are based on assumed empirical formulas that are not applicable to all situations.
- In real applications, the assumptions for individual models are often violated; still, many models were demonstrated empirically to be robust.
- Demonstrations are needed to show that the estimated failure rates fit actual operational experience well considering the fact that test inputs do not necessarily reflect operational environment well.
- Since SRGMs are driven by test-failure data, it may not be possible to use these models to demonstrate very high reliability.
- Continuous-time SRGMs can be directly applied to estimate software failure rates. If failure probability per demand is of interest, continuous-time SRGMs can still be used but not in a straightforward manner, i.e., it may be possible to generate demand-based results by including the frequency of demands in the failure rate estimation of an SRGM, or re-interpret the time-based failure data used in an SRGM as demand-based data.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Bayesian Belief Network Models

- A BBN is a probabilistic graphical model depicting a set of random variables and their conditional independencies via a directed acyclic graph.
- A basic assumption for BBNs is that a node is conditionally independent of its non-descendent nodes, given its parent nodes.
- For a BBN, Jensen [*Bayesian Networks and Decision Graphs*, Springer, 2002] proved that the joint distribution of all variables $\{V_i\}$ is

$$P(V_1, V_2, \cdots, V_n) = \prod_{i=1}^{n} P(V_i \mid parents(V_i)).$$

- Bayesian inference is performed by updating the above equation using the acquired evidence; there exists a spectrum of software tools for the inference.
- Building BBNs is application specific and there exists no general guideline to guarantee the correctness of dependencies in the BBN.
- Usually, a BBN model is built by a group of experts in domains of both BBN and specific applications based on information or evidence from experts' knowledge and statistical data.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on the BBN Method

- The principal strength of the BBN method is its capability of incorporating both experts' subjective opinion (qualitative evidence) and quantitative evidence in a single BBN application model.
- Another advantage of the BBN method is the relative simplicity of the BBN chain rule, compared with full dependency among the random variables.
- However, characterizing the dependence between nodes, which is a fundamental concept of the BBN method, is heavily dependent on analyst judgment and knowledge, and can be difficult to verify, which can lead to large uncertainty in the resultant estimates.
- Other challenges in developing a BBN that takes full advantage of the method's capabilities include:
  - The substantial development effort needed
  - The necessary expertise of the BBN developers and any elicited experts
  - The availability of documentation of the software development activities
  - The need to quantify the qualitative evidence (e.g., the impact of software development quality on software reliability)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Test-Based Models

- All QSRMs use test data to some degree and thus are subject to many of the limitations of test-based methods.
- Test-based models apply standard statistical methods to analyze software testing results and/or software operational data to obtain software reliability.
- Two types of testing may be performed, namely
  - White-box (or glass-box or gray-box) testing: account for internal structure and paths of software execution paths,
  - Black-box testing: frequentist approach and Bayesian approach.
- Implementation of a test-based method consists of (1) generating test cases based on the expected "operational profile" of the software; (2) performing the test; and (3) quantifying the software reliability.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on Test-Based Models

- For software, test cases should be generated from the operational profile, which may not be well known.
- A software with a fault removed during test is considered a modified version of the original software and the previous testing results may not be directly applicable.
- Testing may not uncover incorrect requirements or specifications of software.
- A large number of tests may be required to obtain statistical confidence in a probabilistic parameter with a low value.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

A Correlation Method Using Software Development Practices

- "Frestimate" is a software tool implementing a method which:
  - Includes a proprietary database of software development practices (e.g., use of coding standards) of past projects obtained by surveying software managers and engineers,
  - Uses a regression analysis to estimate the defect density (number of defects per thousand lines of code) of a target software system based on system-specific practices, and
  - Converts number of defects to a failure rate using an empirical formula.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on the "Frestimate" Method

- The general concept of performing correlation/regression analyses using past software development experience is reasonable.
- However, because of the unavailability of detailed information on the past software development projects and the correlation/ regression analyses used to construct the predictive model, this methodology could not be evaluated in detail and may not be appropriate for use where transparency and understanding of both data and modeling assumptions are required to permit sufficient levels of peer review and quality assurance.
- Additional potential limitations include:
  - If data from past projects mostly involved software for normally operating control systems, the data may not be applicable to the types of software typically used in NPP protection systems
  - Subjectivity in the responses to the survey of software development practices
  - Large uncertainties associated with the process for determining the ratio between inherent defects and failure rate

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Context-based Software Risk Model

- CSRM is an integrated risk-modeling approach that incorporates hardware, software, and the static or dynamic interactions between them.
- It is based on the concept of “context-dependent” software risk scenarios, essentially identification of hardware failures or other off-normal conditions that require the software to operate under conditions that may not have been thought of by the system and software designers.
- CSRM is not a specific approach for generating software failure rates or probabilities, though it can be used in conjunction with quantitative estimation processes.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on the CSRM Method

- CSRM does not have its own/new quantification method for software failure rates and probabilities, but relies on existing QSRMs.
- A principal advantage of CSRM is that it decouples the estimation of the rate at which a given system may enter a context-forcing condition from the frequency or probability that the digital system does not respond correctly given the occurring system condition or "context," thereby greatly reducing the testing burden.
- Potential limitations include
  - The context-based evaluation has to be carried out for each software-related failure scenario that involves a combination of software and hardware failures, and it is not clear from the publicly-available information what amount of time and resources would be required to accomplish this for a complex NPP protection system.
  - The context-based, risk-informed testing approach is not meant to be applied to scenarios that occur under nominal conditions, since, as CSRM's developers state, these types of scenarios can be quantified using existing software reliability estimation models.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Other QSRMs

- Metrics methods (NUREG/GR-0019, NUREG/CR-6848): Software reliability was estimated using a few reliability prediction systems (RePSs), each based on a "root" software engineering measure (SEM) and possibly some supporting measures (the root SEMs were identified and ranked by a set of experts).
  - The REPSs were developed by applying available methods, concepts, and empirical formulas, and do not represent new innovative methods.
  - The root SEMs were applied in an orthogonal, independent manner and the available documentation does not indicate that any work was done on development of metrics methods that combine some or all highly ranked SEMs.
- Rule/standard based methods: International Electrotechnical Commission (IEC) Standard 61508 specifies requirements of software and hardware systems and provides guidance on assigning safety integrity levels (SILs).
  - The relationship between the SILs' qualitative requirements and the associated quantitative requirements/targets is assigned subjectively, and needs to be validated.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary and Principal Findings (1)

- Most of the existing QSRMs were not developed specifically for supporting quantification of software failure rates and demand failure probabilities to be used in reliability models of digital systems. However, they do estimate software failure rates or probabilities, and use them in supporting decision-making during software development.
- Many of the QSRMs (i.e., the SRGMs, Frestimate method, and metrics methods) use empirical formulas that are not mathematical laws, and therefore, their general applicability is limited.
- Most applications of QSRMs only considered failure of the software system as a whole, not broken down by software failure mode.
- BBN methods have the advantages that they allow aggregation of disparate information about a piece of software and they include parameter uncertainties as a part of the modeling. However, to fully realize all of the benefits of the BBN approach requires expert judgment to characterize the dependence between nodes, and this can lead to large uncertainty in the resultant estimates.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Summary and Principal Findings (2)

- The test-based methods use standard statistical methods with software testing and, conceivably, with operating data if available. Limitations of the methods are also applicable to any other methods that use test data.
- Frestimate may be difficult to use due to the unavailability of detailed information on the past software development projects and the correlation/ regression analyses used to construct the predictive model.
- CSRM identifies contexts for performing tests, but does not provide a new method for quantifying software failure probabilities.
- The metrics methods apply available methods, concepts, and empirical formulas, and do not represent new innovative methods.
- Assignment of quantitative requirements/targets in IEC Standard 61508 remains to be validated.

For the next phase of this research, we are currently leaning towards proof-of-concept application of BBN and discrete-SRGM.