Thermal-Hydraulic Level 1 Probabilistic Risk Assessment (PRA) Success Criteria Activities

Background

The NRC’s Standardized Plant Analysis Risk (SPAR) models are used to support a number of risk-informed initiatives. The fidelity and realism of these models is ensured through a number of processes, including cross-comparison with industry models, review and use by a wide range of technical experts, and confirmatory analysis. An ongoing activity exists to use one of the agency’s mature accident simulation tools (MELCOR) to perform analyses that can be used to confirm, or support the update of, specific aspects of the SPAR models. The aspects under consideration are the so-called, “success criteria,” as well as the timing of certain key events (e.g., the depletion of a water source) that affect the estimation of the probability of success for operator actions.

Examples of the type of issues that have been investigated to date include the following:

- Small-break loss of coolant accidents – dependency on aligning the emergency core cooling system water source to the containment sump
- Feed and bleed decay heat removal – the minimum number of pressurizer power operated relief valves and high-head pumps needed
- Spontaneous steam generator tube rupture – time available for operators to mitigate the accident prior to core damage
- Station blackout – time available to recover power
- Medium and large loss of coolant accidents – minimum equipment needed to prevent core damage

Approach

Using a mixture of in-house and contractor capabilities, specific modeling aspects are identified, scoped and analyzed. These analyses are then used as the technical basis for making changes (as needed) to the PRA models themselves. The high-level framework for this process is depicted in the figure on the following page.

Ongoing & Future Plans:

As of Fall 2010, ongoing and near-term plans include:

- Development of a NUREG documenting analyses performed for a BWR Mark I and a 3-loop Westinghouse plant with a subatmospheric containment
- Implementation of the first round of analyses in to the SPAR models
- Development of an additional MELCOR input model for a 4-loop Westinghouse plant with a large, dry containment for future success criteria analyses
- Investigation of Level 1 PRA end-state issues, such as the relative conservatism in common core damage surrogates (e.g., core uncoverage versus peak clad temperature of 1204 degrees Celsius (2200 degrees Fahrenheit))
- Increased collaboration with external stakeholders

For More Information
Contact Don Helton, RES/DRA, at 301-251-7594 or Donald.Helton@nrc.gov
High-Level Overview of Success Criteria Process

This figure shows the basic steps in the analysis, which include the translation of the actual plant design and operating features to a computer model representation, the performance of analytical studies and the generation of results, and the distillation of these results into findings that can be used to confirm or alter the PRA model representation of the plant.
Advancing Modeling Techniques in Level 2 and Level 3 Probabilistic Risk Assessment (PRA)

Background

As part of its strategic long-term research planning efforts, the agency has identified Level 2 and Level 3 PRA (see text box below) as an area that would benefit from examination of advanced methods.

The levels of PRA:
Level 1 PRA – initiating event to the onset of core degradation or achievement of a safe state
Level 2 PRA – onset of core degradation to the release of fission products to the environment
Level 3 PRA – offsite consequences

In 2009, the project began with an internal scoping study to evaluate both methodological and implementation-oriented issues associated with the advancement of Level 2/3 PRA modeling techniques. The scoping study created a taxonomy of methods approach classes, which is depicted in the figure below. This effort included a meeting with targeted external stakeholders, and was fully documented in a May 2009 report entitled, “Scoping Study on Advancing Modeling Techniques for Level 2/3 PRA” (ADAMS Accession No. ML091320454).

Objective

The objective of this activity is to investigate the feasibility of using advanced methods to achieve specific improvements in the current state-of-the-practice in Level 2 and Level 3 PRA. The specific attributes of a desirable advancement would include:

- Reduces reliance on unnecessary modeling simplifications and surrogates (i.e., more phenomenological)
- Addresses methodological shortcomings identified by the State-of-the Art Reactor Consequence Analyses (SOARCA) project
- Improves treatment of human interaction and mitigation
- Makes process and results more scrutable
- Leverages advances in computational capabilities and technology developments, but is computationally tractable
- Allows for ready production of uncertainty characterizations

The Spectrum of Approach Classes

This figure depicts four classes of approaches and provides thoughts as to how the migration across this spectrum affects the key characteristics.

Approach

Following on the heels of the 2009 scoping study, the next phase of work has begun with the initiation of a methods development project at Sandia National Laboratories. This phase of the work, which started in July 2009, focuses on a dynamic event tree approach that utilizes the MELCOR accident analysis program in conjunction with a dynamic operator response model. To accomplish this, NRC and Sandia are collaborating with the University of Maryland and the Ohio State University. The initial method development effort, including the approaches application to a demonstration problem is scheduled to be completed in 2011.

For More Information

Contact Don Helton, RES/DRA, at 301-251-7594 or Donald.Helton@nrc.gov
The building blocks:

MELCOR (not an acronym) – a NRC-developed computer code that deterministically models the progression of severe accidents in nuclear power plants

MACCS2 (MELCOR Accident Consequence Code System 2) – a NRC-developed offsite consequence computer code that models the atmospheric transport and dispersion of radioactive material and the associated health effects

ADS-IDAC (Accident Dynamics Simulator using Information, Decisions, and Actions in a Crew Context) – a discrete dynamic event tree computer code developed by the University of Maryland that dynamically treats accident evolution, in concert with a simulator such as MELCOR, with a focus on the cognitive representation of the operators

ADAPT (Analysis of Dynamic Accident Progression Trees) – a discrete dynamic event tree computer code developed by The Ohio State University that dynamically treats accident evolution, in concert with a simulator such as MELCOR, with a focus on component and phenomenological behavior

Sample High-Level Code Coupling Scheme

This figure illustrates a potential scheme for combining existing computer programs in a manner that facilitates dynamic accident simulation.
Digital Instrumentation and Control Probabilistic Risk Assessment

Background

Nuclear power plants (NPPs) have traditionally relied on analog systems for their monitoring, control, and protection functions. With a shift in technology to digital systems with their functional advantages, existing plants have begun to replace current analog systems, while new plant designs fully incorporate digital systems. Since digital instrumentation and control (I&C) systems are expected to play an increasingly important role in nuclear power plant safety, the NRC has developed a digital I&C research plan that defines a coherent set of research programs to support its regulatory needs.

The current licensing process for digital I&C systems is based on deterministic engineering criteria. In its 1995 policy statement on probabilistic risk assessment (PRA), the Commission encouraged the use of PRA technology in all regulatory matters to the extent supported by the state of the art in PRA methods and data (60FR42622). Although many activities have been completed in the area of risk-informed regulation, the risk-informed analysis process for digital I&C systems has not yet been satisfactorily developed. Since, at present, no consensus methods exist for quantifying the reliability of digital I&C systems, one of the programs included in the NRC digital I&C research plan addresses risk assessment methods and data for digital I&C systems. The objective of this research is to identify and develop methods, analytical tools, and regulatory guidance to support (1) NPP licensing decisions using information on the risks of digital systems and (2) inclusion of models of digital systems in NPP PRAs.

Approach

Previous and current RES projects have identified a set of desirable characteristics for reliability models of digital systems and have applied various probabilistic reliability modeling methods to an example digital system (i.e., a digital feedwater control system [DFWCS]). Several NUREG/CR reports, which have received extensive internal and external stakeholder review, document this work. The results of these “benchmark” studies have been compared to the set of desirable characteristics to identify areas where additional research might improve the capabilities of the methods. One specific area currently being pursued by RES is the quantification of software reliability. To examine the substantial differences in PRA modeling of software (versus conventional NPP components), in May 2009, RES convened a workshop involving experts with knowledge of software reliability and/or NPP PRA. At the workshop, the experts established a philosophical basis for modeling software failures in a reliability model. RES is now reviewing quantitative software reliability methods and plans 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, they will then be applied to an example software-based protection system in a proof-of-concept study.

![Condensed Markov state transition model for quantifying DFWCS failure frequency due to hardware failures](image)

The results of the benchmark studies have also highlighted the following areas where enhancement in the state of the art for PRA modeling of digital systems is needed:

- approaches for defining and identifying failure modes of digital systems and determining the effects of their combinations on the system
- methods and parameter data for modeling self-diagnostics, reconfiguration, and surveillance, including using other components to detect failures
- better data on hardware failures of digital components, including addressing the potential issue of double-crediting fault-tolerant features, such as self-diagnostics
• better data on the common-cause failures (CCFs) of digital components

• methods for modeling software CCF across system boundaries (e.g., when there is common support software)

• methods for addressing modeling uncertainties in modeling digital systems

• methods for human reliability analysis associated with digital systems

• determining if and when a model of controlled processes is necessary in developing a reliability model of a digital system

Even if an acceptable method is established for modeling digital systems in a PRA and progress is made in the above areas, (1) the level of effort and expertise required to develop and quantify the models will need to be practical for vendors and licensees and (2) the level of uncertainty associated with the quantitative results will need to be sufficiently constrained so that the results are useful for regulatory applications.

International Collaboration

In October 2008, RES staff led a technical meeting on digital I&C risk modeling for the working group on risk (WGRisk) of the Organization for Economic Cooperation and Development, Nuclear Energy Agency, Committee on the Safety of Nuclear Installations. The objectives of this meeting were to make recommendations regarding current methods and information sources used for quantitative evaluation of the reliability of digital I&C systems for PRAs of NPPs, and identify, where appropriate, the near- and long-term developments necessary to improve modeling and evaluation of the reliability of these systems. While the meeting did not produce specific recommendations of the methods or information sources that should be used for quantitative evaluation of the reliability of digital I&C systems for PRAs of NPPs, it did provide a useful forum for the participants to share and discuss their experience with modeling these systems. The report documenting the meeting is available on the NEA web site (http://www.nea.fr/nsd/docs/2009/csni-r2009-18.pdf). A follow-on WGRisk activity is now getting underway that will focus on development of a failure mode taxonomy for digital I&C systems for use when incorporating digital I&C systems into NPP PRAs.

For More Information
Contact Alan Kuritzky, RES/DRA, at 301-251-7587 or Alan.Kuritzky@nrc.gov
SPAR Model Development Program

**Background**

For assessing public safety and developing regulations for nuclear reactors and materials, the NRC traditionally used a deterministic approach that asked "What can go wrong?" and "What are the consequences?" Now, the development of risk assessment methods and tools allows the NRC to also ask "How likely is it that something will go wrong?" These risk tools also allow the NRC to consider multiple hazards and combinations of equipment and human failures that go beyond what is traditionally considered. By making the regulatory process risk-informed (through the use of risk insights to focus on those items most important to protecting public health and safety), the NRC can focus its attention on those design and operational issues most important to safety.

In the reactor safety arena, risk-informed activities occur in five broad categories: (1) rulemaking, (2) licensing process, (3) operating reactor oversight process, (4) regulatory guidance, and (5) development of risk analysis tools, methods, and data. Activities within these categories include revisions to technical requirements in the regulations; risk-informed technical specifications; a new framework for inspection, assessment, and enforcement actions; guidance on risk-informed in-service inspections; and improved standardized plant analysis risk models.

The Standardized Plant Analysis Risk (SPAR) models, Systems Analysis Programs for Hands-on Integrated Reliability Evaluation (SAPHIRE) software and the Risk Assessment Standardization Project (RASP) Handbook, developed by the NRC’s Office of Nuclear Regulatory Research (RES), provide the staff with the Probabilistic Risk Assessment (PRA) tools to support these risk-informed activities.

**Objective**

**SPAR Model Applications**

SPAR models and the SAPHIRE software are used to support the following activities:

- **Inspection Program** (e.g., Significance Determination Process (SDP) Phase 3)

Determining the risk significance of inspection findings or of events to decide the allocation and characterization of inspection resources, the initiation of an inspection team, or the need for further analysis or action by other agency organizations.

- **Management Directive 8.3, “NRC Incident Investigation Program” (MD 8.3)**

Estimating the risk significance of events and conditions at operating plants so that the agency can analyze and evaluate the implications of plant operating experience in order to compare the operating experience with the results of the licensees’ risk analysis, identify risk conditions that need additional regulatory attention, identify risk insignificant conditions that need less regulatory attention, and evaluate the impact of regulatory or licensee programs on risk.

- **Accident Sequence Precursor (ASP) Program**

Screening and analyzing operating experience data in a systematic manner in order to identify those events or conditions which are precursors to severe accident sequences.

- **Generic Safety Issues**

Providing the capability for resolution of generic safety issues, both for screening (or prioritization) and conducting more rigorous analysis to determine if licensees should be required to make a change to their plant or to assess if the agency should modify or eliminate an existing regulatory requirement.

- **License Amendment Reviews**

Enabling the staff to make risk-informed decisions on plant-specific changes to the licensing basis as proposed by licensees, and provide risk perspectives in support of the agency’s reviews of licensees’ submittals.

- **Performance Indicators Verification** (e.g., Mitigating System Performance Index (MSPI) NUREG-1816)

Assisting in the identification of threshold values for risk-based performance indicators and in the development of an integrated performance indicator.

- **Special Studies** (e.g., Loss of Offsite Power and Station Blackout, NUREG/CR-6890 volumes 1 & 2)

Performing various studies in support of regulatory decisions as requested by the Commission, Nuclear Reactor Regulation and other NRC Offices.
**Approach**

The SPAR models and the SAPHIRE software are used by NRC staff in support of risk-informed activities related to the inspection program, incident investigation program, license amendment reviews, performance indicator verification, accident sequence precursor program, generic safety issues, and special studies. These tools also support and provide rigorous and peer reviewed evaluations of operating experience, thereby demonstrating the agency's ability to analyze operating experience independently of licensees’ risk assessments and enhancing the technical credibility of the agency.

The SPAR models integrate systems analysis, accident scenarios, component failure likelihoods, and human reliability analysis into a coherent model that reflects the design and operation of the plant. The SPAR model gives risk analysts the capability to quantify the expected risk of a nuclear power plant in terms of core damage frequency and the change in that risk given an event or an anomalous condition or a change in the design of the plant. More importantly, the model provides the analyst with the ability to identify and understand the attributes that significantly contribute to the risk and insights on how to manage that risk.

Currently, 78 SPAR models representing the 104 operating commercial nuclear plants in the United States are used for analysis of the core damage risk (i.e., Level 1 analysis) from internal events at operating power. The Level 1 SPAR model includes core damage risk resulting from general transients (including anticipated transients without scram), transients induced by loss of a vital alternating current or direct current bus, transients induced by a loss of cooling (service) water, loss-of-coolant accidents, and loss of offsite power. The SPAR models use a standard set of event trees for each plant design class and standardized input data for initiating event frequencies, equipment performance, and human performance, although these input data may be modified to be more plant- and event-specific, when needed. The system fault trees contained in the SPAR models are generally not as detailed as those contained in licensees’ PRA models.

In fiscal year 2010, the 78 SPAR models were revised and augmented to take advantage of the new features and capabilities of SAPHIRE Version 8. SAPHIRE Version 8 was made available to the staff in April 2010. This new version of the SAPHIRE software provides enhanced user interface tools, as well as improved modeling and analysis methods that support the development and use of the SPAR models. Model enhancements included improved modeling of common-cause failure events, handling of recovery rule linking, analysis documentation, and parameter data updates.

![Example Significance Determination Process Analysis Results with SAPHIRE Version 8](image)

To more accurately model plant operation and configuration and to identify the significant differences between the licensees’ PRA and SPAR logic, detailed cut-set level reviews have been accomplished on all 78 models. In addition to the internal event at-power models, the staff has developed 15 external event models based on the licensee responses to Generic Letter 88-20, Supplement 4 “Individual Plant Examination of External Events (IPEEE) for Severe Accident Vulnerabilities” (1991), 7 low power/shutdown models, and 3 extended Level 1 models supporting large early-release frequency (LERF) and Level 2 modeling. The external event models were recently used to identify and evaluate severe accident sequences for the consequential steam generator tube rupture project in support of the NRC’s Steam Generator Action Plan.

One significant upcoming activity is the incorporation of internal fire scenarios from the National Fire Protection Association 805, “Performance-Based Standard for Fire Protection for Light Water Reactor Electric Generating Plants,” pilot applications into the SPAR models. In addition, the staff continues to provide technical support for SPAR model users and risk-informed programs. The staff also completes approximately a dozen routine SPAR model updates annually.

The staff is also developing design-specific internal events SPAR models for new reactor designs. The AP1000 model was completed in February 2010. The model has been optimized for SAPHIRE Version 8 and has been transitioned to a routine maintenance status. A first draft of the Advanced Boiling-Water Reactor (ABWR) model has been provided to the Office of New
Reactors (NRO) for review. The staff also plans to initiate work on developing a design-specific internal events SPAR model for the US Advanced Pressurized Water Reactor. Because design standardization is a key aspect of the new plants, it should only be necessary to develop one SPAR model for each of the new designs.

A formal SPAR model quality assurance plan was implemented in September 2006. Limited scope validation and verification is accomplished by comparison to licensee PRA models (as available), and comparisons to NRC NUREGs and analyses. Limited scope peer reviews consist of internal QA review by NRC contractors, NRC PRA staff, and Regional Senior Reactor Analysts (as available). The user feedback from staff, peer reviews from licensees, and insights gained from special studies such as identification of threshold values during Mitigating Systems Performance Index (MSPI) reviews and the Loss of Off Site Power and Station Blackout study result in improvements to the models on a continuing basis. In 2007, NRC entered into a cooperative effort with the Electric Power Research Institute (EPRI) to improve PRA quality and address several key technical issues common to both the SPAR models and industry models. This cooperative effort resulted in the joint publication of EPRI Report 1016741, “Support System Initiating Events: Identification and Quantification Guideline,” in 2008. This report documents current methods to identify and quantify support system initiating events used PRAs. In addition, the staff, with the cooperation of industry experts, performed a peer review of a representative boiling-water reactor SPAR model and pressurized-water reactor SPAR model in accordance with American National Standard, ASME RA-S-2002, “Standard for Probabilistic Risk Assessment for Nuclear Power Plant Applications,” and Regulatory Guide 1.200, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment Results for Risk-Informed Activities.” The staff has reviewed the peer review comments and has initiated projects to address these comments, where appropriate. The staff is also re-evaluating certain success criteria in the SPAR models using state-of-the-art thermal hydraulic modeling tools.

**Example Loss of Offsite Power SPAR Model Event Tree Display with SAPHIRE Version 8**

**For More Information Contact:**
- Peter Appignani, RES/DRA, at 301-251-7608 (Internal Events)
- Selim Sancaktar, RES/DRA, at 301-251-7572 (External Events & LPSD models)
- Michelle Gonzales, RES/DRA, at 301-251-7591 (New Reactor models and Routine SPAR model updates)
- Daniel O’Neal, RES/DRA, at 301-251-7599 (SAPHIRE)
- Jeffery Wood, RES/DRA, at 301-251-7588 (SAPHIRE)