Probabilistic Risk Assessment Methodology for Risk Management and Regulatory Applications

See-Meng Wong
Brookhaven National Laboratory
Bldg 130
Upton, New York 11973, U.S.A.
(516) 344-2111

Jeff E. Riley
Science Applications International Corp.
4920 El Camino Real
Los Altos, California 94022, U.S.A.
(415) 960-5965

Dana L. Kelly
Idaho National Engineering and Environmental Laboratory
Lockheed Martin Idaho Technologies
Suite 410
11428 Rockville Pike, Maryland 20852
(301) 816-7780

Abstract

This paper discusses the development and potential applications of a PRA methodology for risk management and regulatory applications in the U.S. nuclear industry. The new PRA methodology centers on the development of time-dependent configuration risk profiles for evaluating the effectiveness of operational risk management programs at U.S. nuclear power plants. Configuration-risk profiles have been used as risk-information tools for (1) a better understanding of the impact of daily operational activities on plant safety, and (2) proactive planning of operational activities to manage risk. Trial applications of the methodology were undertaken to demonstrate that configuration-risk profiles can be developed routinely, and can be useful for various industry and regulatory applications. Lessons learned include a better understanding of the issues and characteristics of PRA models available to industry, and identifying the attributes and pitfalls in the development of risk profiles.

Introduction

Since the publication of the landmark Reactor Safety Study (also known as WASH-1400) in 1975, the field of Probabilistic Risk Assessment (PRA) has made strong advances in both the nuclear and non-nuclear industries throughout the world. Improved formal methodologies have been developed to deal with several important aspects of PRA, such as uncertainties, external events, common cause failures, human reliability analysis, severe

accidents, and the role of expert judgment. There is a broad international consensus among vendors, operators, and regulators of nuclear power plants (NPPs) that PRA, also known as Probabilistic Safety Assessment (PSA), is a well-established technology to assist in decision-making on a wide range of design, operational, and regulatory issues [1]. In the United States, there is increasing use of PRA-based results to support decision-making concerning commercial nuclear plant operations and regulation.

Historical Perspective

After the 1979 accident at Three-Mile Island (TMI), PRA studies of many U.S. commercial nuclear power plants (NPPs) were performed to assess their contribution to overall public risk. In the late 1980's, the U.S. Nuclear Regulatory Commission (USNRC) sponsored PRA analyses of five selected NPPs which were documented in NUREG-1150. This NUREG-1150 study was performed to apply state-of-the-art PRA methods for evaluating plant risk as an aid to regulatory decision-making. As an outgrowth from the voluntary PRAs performed by U.S. utilities, the USNRC issued Generic Letter 88-20 which required all utilities to develop plant-specific Individual Plant Examinations (IPE) in order to examine severe accident vulnerabilities, and identify cost-effective plant improvements. The scope of analysis is a Level 1 PRA (including containment performance analysis) for "internal event" initiators such as loss of offsite power, or general plant transient events. Subsequently, a Supplement 4 to Generic Letter 88-20 was issued to request licensees (i.e., owners) of NPPs to develop IPEs for external events (IPEEE). Specifically, these IPEEE studies are performed to analyze risks attributed to seismic events, fires, tornadoes and high winds, external floods and transportation events. The IPE and IPEEE studies for each specific plant provide risk information concerning the plant design and operating features.

In contrast to the traditional PRAs which considered initiating events potentially occurring only during full-power operation, PRAs can be developed to address risks during other modes of operation. Specifically, "shutdown PRA" studies had been performed to assess relative risk and safety for all plant evolutions (including low power and power ascension/startup) throughout refueling and forced plant outages. Shutdown PRAs were performed for specific NPPs after operational experience had indicated that accidents during low power and shutdown could be significant contributors to risk.

As PRA methodology became an important technique to assess NPP safety, efficient computer software was needed to meet the demands from the PRA analysts and new areas of PRA applications. Emerging computer technology has led to the development of personal computer-based PRA software which allows rapid risk calculations of complex PRA models. Currently, the relative maturity of PRA methods and models, as well as the growing appreciation of the value of PRA as a risk management tool, has led to a shift towards risk-informed and performance-based regulation for the commercial nuclear power industry in the United States. As evidence of the fact that PRA technology can be used as a regulatory and risk management tool in a large number of applications, the USNRC issued a Policy Statement [2] on "the Use of PRA Methods in Nuclear Regulatory Activities" in August, 1995. This policy statement promotes the expanded use of PRA in all regulatory matters in a manner that complements the deterministic approach and supports the USNRC's traditional

defense-in-depth philosophy. This paper discusses the development and potential applications of a new methodology to supplement the deterministic approaches used in the regulatory activities.

Risk-Profile Methodology

In order to assess the effectiveness of risk-based technologies in the regulatory processes, a methodology for evaluating configuration-specific risk was developed for potential regulatory applications [3]. This new PRA methodology centers on the development of time-dependent configuration risk profiles. The main steps in the configuration-risk profile methodology, which could be applied to an operating NPP with an already completed PRA model, are listed below:

(1) Identify plant equipment-outage configurations from a review of plant operating records.

(2) Assess the modeling attributes of plant-specific PRA methodology (e.g., type of PRA model, mitigation and recovery rules, etc.), and determine appropriate quantification methods for risk calculations.

(3) Create a baseline risk model for quantifying a base case value to serve as a reference point for time-dependent variation of risk changes.

(4) Evaluate recovery actions for the out-of-service components and correlate each outage component to PRA-related basic events. Then, perform the risk calculations for each equipment-outage configuration to determine the conditional risk of each configuration.

(5) Assess the sensitivity and limitations of the risk model for configuration-risk calculations (e.g., effects of cutset truncation, human error rates, and common-cause failures on the configuration-risk estimates). Uncertainty calculations are also performed to determine the uncertainty distribution of risk estimates.

(6) Develop time-dependent configuration-risk profiles of selected risk measures (e.g., core damage frequency, core damage probability, or large early-release frequency).

An important aspect of developing the risk-profile methodology is to consider the types of PRA methods and software used in both the development and the application of PRA models at NPP sites. In addition, accurate plant operational data and a good understanding of the plant systems, support systems, and related dependencies coupled with risk modeling insights are needed. The risk profile reflects the risk variations due to changing configurations over time. As such, the methodology emphasizes the changes in risk with respect to time, as opposed to the absolute representation of plant risk at any given time.

Pilot applications of the methodology were undertaken to demonstrate that configuration-risk profiles can be developed routinely using existing and readily retrievable plant records, and can be useful for various industry and regulatory applications. Six nuclear power plants of different reactor designs with varying operating philosophies were selected for the trial applications. The pilot plants were South Texas Project Units 1 and 2, Comanche Peak Station Unit 1, Crystal River Nuclear Plant Unit 3, Brunswick Nuclear Plant Unit 2, Donald C. Cook Nuclear Plant Unit 1, and San Onofre Nuclear Generating Station Unit 2. The methodology was successfully tested and risk profiles were developed for all six U.S. plants. The risk profiles for a given plant site were developed by using different PRA software with generally consistent results, providing that care was taken to address the appropriate details of the risk model and all steps of the methodology were followed. Insights from the configuration-risk profiles were used on a trial basis for potential applications in current regulatory initiatives such as the integrated assessment of operational performance, and online maintenance risk assessment activities.

An important lesson learned from the visits to the pilot plants is the necessity of ensuring the quality of plant configuration-risk profiles. In order to produce appropriate and valid risk profiles, it is important to consider the details of the risk model. These considerations are the treatment of initiating event frequencies, system analysis, recovery actions, human reliability estimates, and common-cause failures. Also, a detailed knowledge about plant systems and plant operation is necessary to accurately interpret the observable elements of configuration-risk profiles. Other important lessons learned include using an efficient method to identify configurations, evaluating the consistency of outage records, properly translating outage events to PRA basic events, having a working knowledge of the PRA computer software and its limitations for computational purposes, and using appropriate truncation levels.

Potential Applications

Applications of the configuration-risk profile methodology can be categorized into two areas of use in (1) risk management of plant operations and (2) regulatory initiatives. For risk-management purposes, configuration-risk profiles can be used preoperationally, online for real-time applications, and postoperationally for analysis of plant performance. A preoperational application is the use of risk profiles for the planning and scheduling of maintenance to minimize plant risk (e.g., evaluating risk impacts of configurations in rolling maintenance schedules for online maintenance). An example of real-time applications is the use of risk profiles for monitoring the dynamic risk changes due to operational activities (e.g., surveillance testing) in combination with ongoing equipment failures. This provides timely information to operations staff to avoid specific critical configurations that can affect plant safety. Finally, an example of postoperational use is the evaluation of a long-term (e.g., six-month) configuration-risk profile to determine performance trends and risk-management practices. This type of evaluation can also provide bottom-line insights into the effectiveness of maintenance and corrective action programs.

Potential applications of the methodology were identified for use in new regulatory initiatives. The risk-profile methodology can be beneficial for the following applications:

- Risk-informed assessment of operational performance,
- Online maintenance risk assessment, and
- Guidance for improving Technical Specifications.

In particular, insights from configuration-risk profiles can be used to strengthen inspection planning in these regulatory activities. This is consistent with the USNRC's initiatives to develop guidance on integrating risk concepts and PRA into the largely deterministic, regulatory process. Other potential applications involve the use of risk profiles in risk ranking, event assessment, evaluation of operational performance, risk-based inspections, and review of licensing issues such as Justification for Continued Operation (JCO) or relief from technical specifications. Several of these applications were successfully tested during the pilot plant site visits.

Summary

The risk-profile methodology was developed to demonstrate its potential use for selected regulatory applications. Lessons learned from trial applications indicate that configuration-risk profiles can be developed routinely using existing and readily retrievable plant records of equipment outages. Configuration-risk profiles can be used for risk-management purposes in three ways for analysis of plant performance: (1) preoperationally, (2) online for real-time applications, and (3) postoperationally. Thus, the risk-profile methodology can be used extensively as a risk-information tool for evaluating operational management strategies and online monitoring of plant safety levels. As the shift towards risk-informed and performance-based regulation for the U.S. nuclear power industry continues to gain momentum, new PRA methodologies are being explored to meet the challenges of using PRA in regulatory activities. The successful application of new PRA methodologies would enhance their use in other engineering disciplines such as environmental and non-nuclear industrial applications.

REFERENCES

[1] P. Kafka, "PSA Technology - A Tool to Assist Decision Making on Complex Installations," PSA'95 - International Conference on Probabilistic Safety Assessment Methodology and Applications, Seoul, Korea (1995).

[2] "Use of Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities; Final Policy Statement," U.S. Federal Register, Vol. 60, p. 42622, Washington, D.C. (1995).

[3] S.M. Wong, G. Holahan, J. Chung, and M. Johnson, "Risk-Based Methodology for USNRC Inspections," PSA'95 - International Conference on Probabilistic Safety Assessment Methodology and Applications, Seoul, Korea (1995).