BNL-47162
Conf-911106--87

RELIABILITY ASSURANCE FOR REGULATION OF ADVANCED REACTORS*

R. Fullwood, R. Lofaro and P. Samanta
Brookhaven National Laboratory
Engineering Technology Division, Department of Nuclear Energy

BNL--47162
DE92 010138

Summary

The advanced nuclear power plants must achieve higher levels of safety than the first generation of plants. Showing that this is indeed true provides new challenges to reliability and risk assessment methods in the analysis of the designs employing passive and semi-passive protection. Reliability assurance of the advanced reactor systems is important for determining the safety of the design and for determining the plant operability. Safety is the primary concern, but operability is considered indicative of good and safe operation. This paper discusses several concerns for reliability assurance of the advanced design encompassing reliability determination, level of detail required in advanced reactor submittals, data for reliability assurance, systems interactions and common cause effects, passive component reliability, PRA-based configuration control system, and inspection, training, maintenance and test requirements. Suggested approaches are provided for addressing each of these topics.

Background

The Congressional hearings on advanced reactors (AR) concluded that an AR, by definition, has substantially less risk than the current generation of reactors, where substantially less is taken to mean less by an order of magnitude or more. Presently, there is little experience on which to base a determination that shows this to be true. Furthermore the current generation of nuclear power plants has carried risk reduction, using redundant active components and systems, to the extent that reactor complexity is believed to be a contributor to risk. Common cause interactions in active redundant systems impose further constraints on safety achieved by redundancy.

To achieve the order of magnitude risk reduction required of ARs a combination of the following are used:

- Inherent safety – physical impossibility for an undesired event to occur. This is the most desirable form of safety.
- Passive safety – systems or components that do not require actuation to prevent an undesired event. Experience has demonstrated that equipment without moving parts is more reliable than active equipment.
- Active safety – systems or components requiring actuation to prevent an undesired event. The reliability of active components is often enhanced using several systems, one to backup the other (redundant).

Incorporated in the several vendor designs are:

- Passive systems,
- Semi-passive systems,
- Digital control, and
- Advanced control rooms.

These present new challenges to Probabilistic Safety Assessment (PSA) by requiring:

- Accuracy at high confidence while dealing with systems having an order of magnitude less probability of failure than current systems.
- Analysis of protection from common cause.
- Modeling of new components and systems.
- Reliability calculations for which there is little experience base.
- Assuring the accurate modeling of test, training, replacement and repair to assure that reliability is being maintained.
- Human factors in operation, organization and maintenance.

From these, several tasks have been identified and are discussed below:

1) Reliability Assurance of the Advanced Designs,
2) PSA-Based Prioritization of Level of Detail in Licensing Submittals,
3) Data Collection Based on the Needs for Risk Calculation
4) System Interactions and Common-Cause Effects,

*This work was performed under the auspices of the U.S. Department of Energy.

5) Analysis of Passive Component Reliability,

6) PRA-Based Configuration Control System, and

7) Inspection, Training, Maintenance and Test Requirements.

These will now be discussed:

1. RELIABILITY ASSURANCE OF THE ADVANCED DESIGNS

Discussion

Reliability models of the safety systems and other systems with which they interact, such as the man-machine interface, are constructed in the conventional PRA frame-work with extensions to the new systems. Determination of reliability assurance of a design containing both passive and active components depends on the accident environmental envelope in which they must operate. This environment affects the reliability of the passive systems by temperature, radiation, residual stress and cyclic stress. Moreover, the reliability of active components degrades with environment according to its stress history, and the test and maintenance that is performed upon it. Active systems, operating in redundancy are subject to various common causes of failure that degrade the independence of the systems. A major cause of active failure is the man-machine interface at organizational, operating, testing and maintaining levels.

As the risk of the plant is reduced to meet AR goals, it may be that accident initiators that previously had been insignificant must be addressed. Advanced reactors will require a reassessment of accident initiators to determine if there are new initiators, and if initiators in hot and cold shutdown and refueling as well as mis-assembly and foreign material entry into the primary system are being properly considered.

Upon assembly of this quantitative information, including uncertainties, the reliability of the AR design may be estimated. This reliability assessment will not solely depend on models of the AR but will draw to as large an extent as practical on experience gained with the current generation of nuclear power plant – the experience base and the lessons learned. The results of evaluating the licensing application is conveyed to the applicant for clarification and possible design rectification or component quality upgrade. This may result in revisions to the design and/or procedures to assure the highest possible level of safe operation.

Approach

a) Utilization of Existing Resources

A design will be carefully examined and compared with its PRA (if available) and previous modeling to determine the adequacy of existing work. Work that must be done to assure the reliability of new systems and components, and to determine the reliability of the various systems working together to achieve plant safety will be identified.

b) Passive System Reliability Analysis

Passive systems are those with no separate control, i.e. in electrical parlance two terminal networks. As such, the concerns are primarily with envelope degradation due to stress, stress cycles, radiation and chemical effects.

A basic approach to passive system reliability is Stress-Strength modeling. This method overlaps a probability density function for the stresses, such as those just named, onto a probability density function for the strength, including test and maintenance. The area of overlap is the probability of failure. Another approach, used by BNL in support of the Advanced Neutron Source reactor being designed by ORNL, embodies probabilistic fracture mechanics calculations in a "C" personal computer language program which has been used for pipe leak and break estimates and guidance for a robust design. Using a "tool kit" of approaches, the reliability of passive systems is initially scoped using quick approximate methods for reliability prioritization to identify components/systems for detailed analyses as needed.

c) Semi-Passive Reliability Analysis

The term "semi-passive" is used to mean a two terminal network, i.e., no external control but involving mechanical elements such as check valves.

The purely passive parts of the system are analyzed, as described in b). The non-reciprocal, mechanical element is likely to dominate the system unreliability and be the focus of analysis, which may use methods such as Failure Modes, Effects, and Criticality Analysis (FMECA) with a matrix of failure initiators to examine the ways the component can fail, the mitigation of failure and the detection of failure. This would include considerations of training, test, maintenance and mitigating factors.

d) Active Reliability Analysis

The methods used for active reliability analysis are conventional, embodying a combination of FMECA

and fault tree analysis, but with careful consideration of common cause system interactions for redundant systems.

e) Systems Reliability

Upon completion of the reliability analysis of components and subsystems, the results are assembled into system and plant analyses using fault tree construction and the analyses of uncertainties in quantifying the results. These results provide the bases for importance ranking as an aid in focussing improvements in the analyses, as well as gasing recommendations for improvements in design or component quality.

2. PSA-BASED PRIORITIZATION OF LEVEL OF DETAIL IN LICENSING SUBMITTALS

Discussion

The requirements for the level of detail required in licensing submittals for design certification are expected to be significant. As noted previously, the advanced designs use a number of new design features to achieve the desired level of risk reduction. The new features employ new components and systems, for which there is little accumulated experience or detailed engineering information to base licensing decisions. Admittedly, evaluation of the advanced reactor designs should focus on the risk-significant aspects and, as such, detailed information is required for those aspects of a design. Advanced reactors will have probabilistic safety assessments (PSAs) performed for the "paper design" and the PSAs can be used to prioritize the design features. This prioritization will provide the basis for the level of detail required in licensing submittals. In general, the level of detail will be less for less risk-significance. In the absence of a PSA, qualitative risk and reliability insights may be used to obtain this prioritization. This process will not only help to reduce the licensee's burden, but it also will focus the NRC-review effort upon appropriate areas to improve overall plant safety.

Approach

Specific activities for PSA-based determination of submittal detail are summarized as:

a) Process for Prioritization

Available risk-importance measures provide the primary basis for prioritizing the level of detail. Prioritization will be defined for systems, components, design features, and for specific failure mechanisms/categories relevant for advanced reactors. The intent of the process will not be to obtain detailed rankings, but to obtain groupings based on PSA evaluations.

b) Criteria for Defining Prioritization Categories

Criteria will be defined to delineate the various groups of detail. Both numerical criteria using quantified risk analyses, and qualitative criteria using deterministic guidelines will be used.

c) Level of Detail Information

The various levels of detailed information to be associated with different categories will be scoped/defined. As stated earlier, the most risk-significant aspects will require the most detailed information.

d) Demonstration Analysis

Using an available PSA, the above process will be applied to demonstrate the process. In the absence of available experience with the new systems, sensitivity analyses will be used. Specific guidelines for these sensitivity analyses will be defined.

3. DATA COLLECTION BASED ON THE NEEDS FOR RISK CALCULATION

Discussion

All utilities are required to record data related to the operation and maintenance of the various systems and components in the plant. This information is typically used at the plant level to evaluate performance, and to determine repair and refurbishment frequencies. It is also used outside of the plant to verify and quantify reliability assessments of the various systems and components. These data provide the means for calculating the mathematical models of reliability and risk, and provide the ultimate basis for calculating plant risk. Clearly, a comprehensive data collection program must be in place to provide the type of information required to support these analyses.

Approach

Brookhaven National Laboratory has extensive experience in performing risk and reliability studies, as well as research into the causes and effects of nuclear plant aging. Common to studies of this nature are requirements on availability and quality of data to support the calculations. In most cases, accurate data are very difficult to obtain. Data that are available are typically incomplete or do not address parameters relevant to the determination of risk and reliability. Many of the national data bases, along with actual plant records have

been extensively reviewed and analyzed to extract useable information. This has provided BNL with in-depth familiarity with the types of data recorded, and with the deficiencies existing in current data bases.

Consideration should be given to the design and development of a comprehensive data management program instituted at plant startup. The objective of such a program is to support activities and decision making at the plant level, while making data available for evaluating the safe operation of the plants. Key to this program is a data base designed for these purposes. In order to assure this, consideration should be given to the type of data needed, format used, frequency of recording, and definition of terminology used in the recording. Each category should address specific components and systems.

In light of the previous discussion, a task should be undertaken to develop guidelines for reliability-based data recording requirements. These guidelines may be used to aid in the design and development of plant data bases for assuring that information needed to support risk and reliability analyses is available as needed. Specific areas to be addressed as part of this task include the following:

- Identification of the types and frequency of data to be recorded for use in risk and reliability analyses.
- Reliability based prioritization of components and systems to determine the importance of reporting requirements,
- Definition of consistent terminology for describing events in relation to risk and reliability analyses.

The guidelines will address the recording of normal operating data, corrective and preventive maintenance data, and surveillance test data. With the implementation of these guidelines, sufficient information will be available for predictions of advanced reactor component and system reliabilities, and plant risk.

4. SYSTEM INTERACTIONS AND COMMON CAUSE EFFECTS

Discussion

Advanced nuclear power plants will embody risk-reducing designs which will tax the ability of risk assessment to evaluate. The lower risk will place greater emphasis on effects which had been minor contributors in the earlier designs due to the elimination or risk reduction of the previously dominant contributors. Underlying the design of plants is the independence of systems. If there are system interactions (including common cause/common mode) that violate independence, system operability may not be as intended. These interactions may arise from many different mechanisms: design, quality control, environment, externalities, support systems, control systems, and human factors, and require investigation from each perspective.

Attempts have been made to estimate these effects on a phenomenological basis by attempting to infer, by mathematical models, the common cause coupling by relating observations made on one system to another. This approach is neither complete nor physically based.

Approach

Failure Modes, Effects and Criticality Analysis (FMECA) is a detailed, realistic method for identifying the ways of component failure. It may be systematically applied for each of the mechanisms listed above to determine design robustness. Currently this method is being used for evaluation and risk reduction in the design of the Advanced Neutron Source (ANS) reactor and facility at Oak Ridge National Laboratory. FMECA is useful for detecting various types of weaknesses including system interactions. Once identified, recommendations may be made for modification or correction, or this knowledge may be used for probabilistic evaluation purposes to determine if the plant risk is within guidelines.

5. ANALYSIS OF PASSIVE COMPONENT RELIABILITY

Discussion

Advanced reactors are expected to make greater use of passive systems than the earlier designs. These passive systems are basically envelopes and supports for coolant which, under gravity or other natural laws, flows to perform its design function. Questions regarding failure devolve on material failure such cyclic fatigue, stress corrosion cracking, corrosion, or radiation. Protection against these effects is provided by samples, nondestructive testing and inspection. Models analyzing passive degradation begin with probability distributions of manufacturing defects in the materials, consider the probability of defect detection in pre-service inspection, and apply various defect growth models according to failure mechanisms that are operative. For example, the Paris model is commonly used for cyclic fatigue growth. Other models are used for stress corrosion cracking, corrosion and radiation. Whatever causes the defect growth to take place, the result is a probability distribution of defect sizes. The probability of defect detection under in-service inspection is applied. When the defect has grown through the wall, it is a leak; when it has grown to, say 2/3 of the circumference, it is called a break. Leak-before-break criteria may be applied to determine the probability of repairing the defect before reaching break size.

This is one example for modeling passive reliability. Other types of passive components would require different types of modeling. For example, failures that are basically diffusion processes may use Arrhenius modeling, while electrical breakdown may use empirical power-law formulae.

Approach

Advanced reactor designs will be reviewed to identify passive systems important to determining the plant risk, the criticality of their performance, mitigating systems and mechanisms. Failure mechanisms for these systems will be identified and their passive reliability estimated by the appropriate current technology. This will result in a preliminary estimate of the reliability of the passive systems and insights into the analysis methodology when applied to these systems to give rise to recommendations for improvement.

6. PRA-BASED CONFIGURATION CONTROL SYSTEM

Discussion

One important way to assure the operational safety of a plant is to control the maintenance and testing effect on the plant such that failures are promptly detected and the components are restored to operational status without undue impact on the risk. Current surveillance requirements and allowed outage times are considered unduly burdensome while not significantly improving plant safety in many cases. Indeed, current requirements which focus on individual components are silent on many risk-significant multiple component outages. Development of a PRA-based operational configuration control system for an advanced reactor can address many of the problems discussed above and will bring in the experiences from the present generation of nuclear plants, thus resulting in safer operation of the newer plants.

Approach

A system is proposed for development that will base the relevant technical specification on risk rather than the current engineering judgment. The specific activities to be carried out in developing a PRA-based operational configuration control system may be summarized as follows:

a) Feasibility and Scope of the System

This feasibility task uses the PRA for an advanced plant to study the risk implications of the outage configuration to define how the system can be effective in preventing occurrences of high risk levels, and also how the system can be used to transfer to low risk levels when the operational risk level has been identified as being high. Initially, plant-specific data will not be available, thus requiring the use of the most appropriate alternative data sources. This task will also study and identify the portion of the technical specifications applicable to specific systems of the advanced reactor.

b) Criteria for an Operational Configuration Control System

Numerical criteria for the operational configuration control system are defined and implemented in this task. Criteria will be devised in such a way that both the objectives of risk control and of operational flexibility are achieved.

c) Guidelines for Developing the System

Specific guidelines for developing an effective risk-based operational configuration control system will be delineated for use in developing the system. These guidelines will include test and maintenance planning and scheduling to avoid high risk levels, and control outage durations. They will also include guidelines for extensions, testing of functionally alternative equipment to assure success paths and feedback of information in deciding future actions.

d) Reliability Assurance Activities

The use of such a system will provide a capability to audit and monitor the plant performance. Such auditing capabilities can be used to monitor and to institute reliability assurance activity. This task will develop guidelines for analyzing plant operational data and how such information should be used to institute specific reliability engineering activities.

7. INSPECTION, TRAINING, MAINTENANCE AND TEST REQUIREMENTS

Discussion

The inspection, surveillance, monitoring, and maintenance (ISM&M) practices used at a plant can directly affect the reliability of components and systems, as well as plant risk. To ensure reliable system performance, ISM&M practices are needed that can effectively detect and mitigate degradation before failures result. In recent BNL studies related to nuclear plant aging, it was found that current ISM&M practices are not always capable of controlling degradation. As a result, component failures have been found to increase with time, resulting in a decrease in system availability. Efforts are now under way to identify those ISM&M practices that are

effective at detecting and mitigating degradation in the older plants. The experience gained in this work is applicable to avoiding similar degradation processes in the advanced reactors.

The identification of effective ISM&M practices is based on reviews of the various systems and components to identify the degradation processes that can potentially result in failures and adversely affect plant risk. Once this is accomplished, suitable ISM&M practices are selected to maintain an acceptable level of reliability. Since many of the systems used in the advanced reactors have components and functions that are similar to those used in current reactors, much of the experience and knowledge gained from current studies will be applicable.

Approach

Based on the above discussion, a task will be implemented to review the design and expected models of operation of the various systems in the advanced reactors and identify effective ISM&M practices for properly controlling risk and reliability. This work will consist of the following subtasks:

- Review of advanced reactor system designs to identify the most important systems and components in terms of system reliability and plant risk.
- Review of operating conditions and operating environment to identify degradation processes that will be active.
- Selection of ISM&M practices that will be most effective at detecting and mitigating the identified degradation processes.
- Development of guidelines for the inclusion of ISM&M practices in plant technical specifications.

SELECTED BIBLIOGRAPHY

[1] M.A. Azarm, et al., "Evaluation of Reliability Technology Applicable to LWR Operational Safety," NUREG/CR-4618, BNL-NUREG-51995, August 1988.

[2] M.A. Azarm, R.A. Bari, T-L. Chu and L. Oliveria, "Level-1 Internal Event PRA for the High Flux Beam Reactor," Volumes 1 & 2, Rev. 1, Brookhaven National Laboratory, July 1990.

[3] M.A. Azarm and W.E. Vesely, et al., "System Unavailability Indicators: Summary Report," Volume 1 & 2 Draft NUREG/CR, March 1991.

[4] J.L. Boccio, W.E. Vesely, M.A. Azarm, et al., "Validation of Risk-Based Performance Indicators: Safety System Function Trends," NUREG/CR-5323, BNL-NUREG-52186, October 1989.

[5] R.R. Fullwood, 1988, "Review of Pipe-Break Probability Assessment Methods and Data for Application to the Advanced Neutron Source Project for Oak Ridge National Laboratory," (internal preliminary report, final report in preparation).

[6] R.R. Fullwood and R.E. Hall, "Projection of Future Technological Needs of the U.S. Nuclear Regulatory Commission over the Next Decade," Letter report to J.J. Lazenick, USNRC, November 1989.

[7] R.R. Fullwood and R.E. Hall, 1990, "PRAISDPD: An Aging Pipe Reliability Analysis PC Code," in The Role of Personal Computers in Probabilistic Safety Assessment and Decision Making, Elsevier, London.

[8] R.R. Fullwood, D. Selby (ORNL) and F. Peretz (ORNL), 1988, "PRA in Preconceptual Design," TANSAO, 56, 1-626, pp 338-339.

[9] W.E. Gunther, "Power Electronic Switching Devices: Their Role in the Nuclear Industry," BNL Technical Report, April 1990.

[10] R.E. Hall, R.R. Fullwood and J.L. Boccio, "Preliminary Program Plan for the Heavy Water Moderated and Cooled Production Reactor: Reliability, Availability, Maintainability and Inspectability," BNL-NPR-HWR-1, May 1990.

[11] E. Lofgren et al., 1988, "Guidance for Using Reliability Programs to Defend against Common-Cause Failures," BNL Technical Report A3282-6-16-88.

[12] E. Lofgren, et al., 1991, "Issues and Approaches for Using Equipment Reliability Alert Levels," NUREG/CR-5611, BNL-NUREG-52251, (in publication).

[13] P.K. Samanta, et al., "Evaluation of Risks Associated with AOT and STI Requirements at the ANO-1 Nuclear Power Plant," NUREG/CR-5200, BNL-NUREG-52024, August 1988.

[14] P.K. Samanta, et al., "Study of Operational Risk-Based Configuration Control," Draft NUREG/CR-5461, BNL-NUREG-52261, September 1990.

[15] W.E. Vesely, et al., "Evaluation of Diesel Unavailability and Risk-Effective Surveillance Test Intervals," NUREG/CR-4810, BNL-NUREG-52022, May 1987.