Recommendations for a Proposed Standard for Performing Systems Analysis

Jeffrey LaChance,[1] Donnie Whitehead,[2] and Mary Drouin[3]
[1]Science Applications International Corporation
[2] Sandia National Laboratories
[3]U.S. Nuclear Regulatory Commission

1. Introduction

In August 1995, the Nuclear Regulatory Commission (NRC) issued a policy statement proposing improved regulatory decisionmaking "by increasing the use of PRA [probabilistic risk assessment] in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data." A key aspect in using PRA in risk-informed regulatory activities is establishing the appropriate scope and attributes of the PRA. In this regard, ASME decided to develop a consensus PRA standard. The objective is to develop a PRA Standard such that the technical quality of nuclear plant PRAs will be sufficient to support risk-informed regulatory applications. This paper presents example recommendations for the systems analysis element of a PRA for incorporation into the ASME PRA Standard.

2. Systems Analysis Recommendations

System unavailability or unreliability during accidents is evaluated in the systems analysis portion of a PRA. Although there are different techniques that may be used in a systems analysis, fault trees are the preferred method since they are deductive in nature and, if properly constructed, can identify potential failure modes of a system and can be used to calculate the system unavailability/unreliability. Because of the prevailing use of fault trees in systems analysis, this paper focuses on a proposed standard for fault tree analysis. However, the proposed standard is also applicable for other systems analysis methods.

The recommendations focus on the technical standard for the content of the system models and address recommendations for updating, documenting, and peer reviewing the systems analysis. An overview of these

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

DISCLAIMER

recommendations is presented followed by specific example recommendations for the technical standard in Table 1.

2.1 Technical

The technical standard addresses the key portions of a systems analysis beginning with the understanding of how the systems work. The major attributes of a systems analysis is that the system model should reflect the as-built, as-operated system. This can only be accomplished by reviewing pertinent plant information sources on the design and operation of the system supplemented by information obtained through analysis of operational data, walkdowns, and interviews.

The key element determining system model content and structure is system success criteria. Success criteria should be based upon realistic engineering analyses (e.g., experiments, tests, or thermal-hydraulic analyses) applicable to the plant. Using the required system success criteria, the model boundaries and interfaces should be identified. The system model should include components required for system operation, support systems required for actuation and operation of the system components, and other components whose failure can degrade or fail the system. The system model should include the relevant and possible failure modes for each component required for system operation. This includes hardware failures, test and maintenance unavailabilities, common-cause failures, and human failures that can occur both before and during an accident. Screening of components, particular component failure modes, and support systems can be performed when the component/system can be shown to have little or no impact on the required system operation or model results.

2.2 PRA Update

If used in risk-informed applications, the systems analysis should be updated on a periodic basis such that each system model continue to reflect the as-built, as-operated plant. Updates are recommended at least every two years or when a plant change affects a system model such that any decisions made with the system model is impacted.

2.3 Documentation

A systems analysis should be clearly documented such that it can be peer reviewed. A key element is a workplan that establishes how the systems analysis was performed. The workplan should indicate if and how the technical requirements for a systems analysis have been incorporated into the system models. The documentation should also include the sources of information used in the analysis, a discussion of any assumptions and limitations made in the analysis, and the results.

2.4 Peer Review

A peer review of the systems analysis against the technical requirements can provide an important basis for the acceptance of the PRA for use in risk-informed applications. The peer review is accomplished in part by reviewing the workplan used in the systems analysis against the technical requirements. A detailed or limited review of all generated systems models is performed depending on whether the workplan addresses all of the technical requirements. The review should be performed by a team of personnel independent of those who generated the system models and should have substantial experience in PRA particularly in the area of systems analysis.

Table 1. Example recommendations for a systems analysis standard.

Function	Example Recommended Standard
System Understanding	• Review plant information sources on system design and operation to allow construction of a model that reflects the as-built, as-operated plant. • Review system operating experience. • Perform procedurally-guided system walkdowns. • Conduct interviews.
System Model Selection	• Use different model types as appropriate. • Use screening to simplify a model as appropriate. • If appropriate, a single data value may be used to represent a system.
Success Criteria	• Determine system success criteria using realistic engineering analyses. • Include the impact of aging when understood. • Incorporate dependency into the system model.
Model Boundaries and Interfaces	• Include all components required for system operation. • Components may be excluded if their aggregate unavailability is less than a predefined value (e.g, 1%). • Do not include component failures that would be beneficial to system operation. • Make sure component boundaries are consistent with the definitions used to establish component failure data. • Model shared portions of a component separately to account for dependencies. • Include automatic signals required to actuate the system. • Include conditions needed for automatic system actuation in the model. • Include human response actions. • Identify support systems required for system operation. • Include motive and control power required for component operation. • Include other support systems unless exclusion is supported by plant-specific engineering analyses. • Do not use procedularized recovery actions to eliminate support systems from the model, included the actions in the model. • Include conditions that cause the system to isolate, trip, or fail. • Unless supported by evidence, assume equipment fails if it is operated beyond its design.

Table 1. Example recommendations for a systems analysis standard.

Function	Example Recommended Standard
Component Failure Modes	• Unless screened, include all component hardware failures. • Do not include repair of hardware failures unless justified by an appropriate analysis. • Include unavailability due to planed and unplanned test and maintenance. • Ensure that combinations of maintenance events are based on plant experience. • Model intra-system common-cause failures. • Model inter-system common-cause failures when supported by data. • Include pre- and post-initiator human actions. • Review interactions caused by changes in the operating environment, conditions related to plant design or operational features, or other factors for inclusion in the model. • Exclude component failure modes only if the aggregate failure probability is less than a specified value (e.g., 1%).
Integrated Model Construction	• Use a consistent event naming scheme. • For fault trees, break circular logic where it first occurs. For support states, ensure that the support states account for each support system dependency. • Grouping of component failure events is discouraged.