THE DEVELOPMENT OF INTERIM GUIDANCE ON SYSTEMS INTERACTIONS

F. Coffman*, B. Atefi**, R. Bari**, E. Chelliah*, J. Conran*, P. Cybulskis***, R. Galluci***, I. Papazoglou**, P. Pelto***, and R. Widrig***

*U.S. Nuclear Regulatory Commission
**Brookhaven National Laboratory
***Battelle Memorial Institute

ABSTRACT

The Office of Nuclear Reactor Regulation is developing interim guidance to direct the systematic evaluations of LWRs for adverse systems interactions. The guidance establishes a three-step review process and provides basic definitions, deterministic safety criteria, a classification of the types of adverse systems interactions, and descriptions of the formal methodology applicable for disciplined evaluations including the ranking of interactions by their relative importance to safety. The guidance provides for accommodating lessons learned from operating experience and relates systems interactions to Human Errors and Probabilistic Risk Assessments.

INTRODUCTION

The purpose of this paper is to summarize current staff thinking on the approach to be taken by the Systems Interaction Program within the Office of Nuclear Reactor Regulation for the evaluation of adverse systems interactions in LWRs. This approach will be documented in the "Interim Guidance for the Performance of System Interaction Pilot Review" that is being developed with technical assistance from Battelle Memorial Institute and Brookhaven National Laboratory. The objective of the interim guidance is to provide a mature plan for the conduct of pilot reviews. The pilot reviews are a useful exercise prior to a general licensing requirement since the nuclear industry's experience with systems interactions review is fragmented.

The staff's systems interaction program was initiated in May 1978 with the definition of an Unresolved Safety Issue on Systems Interaction in Nuclear Power Plants and was intensified by the NRC Action Plan developed as a result of the TMI-2 accident. The concern on systems interaction arises because the design, analysis and installation of systems is frequently the responsibility of teams of engineers with specialities--such as civil, electrical, mechanical, or nuclear. Experience at operating plants led to questions whether the work of these engineering specialists is sufficiently integrated to minimize adverse interactions among systems. Some adverse events that occurred in the past might have been prevented if the teams assured the necessary independence of safety systems under all conditions of operation. The staff is considering

the issuance of a regulatory requirement that separate reviews for systems interaction be performed on operating reactors and LWR designs when a substantial portion of construction is completed. The plants would be reviewed for common cause failures that could jeopardize the independent systems needed to perform basic safety functions.

TERMINOLOGY

This section discusses the important terms and concepts of systems interaction reviews. The terminology given here is fundamental to the near-term review of a LWR for adverse systems interactions and serves to introduce the specific emphasis of the approach.

Basic Safety Functions and Associated Systems

The general safety objective of a nuclear plant design can be stated: "to avoid unacceptable reactor core damage and release of unacceptable levels of radioactivity to the site environs."

To avoid unacceptable reactor core damage and a release of unacceptable levels of radioactivity to the site environs, there must be either no accidents or no multiple failures of the vital combinations of systems that serve basic safety functions. Given the possibility of accidents, or transients combined with systems failures, the following basic safety functions can be specified:

1. To maintain the primary coolant inventory.
2. To transfer the heat from the reactor to the ultimate heat sink.
3. To render and keep the entire core subcritical.
4. To maintain the integrity of the containment and control radioactivity releases.

The systems of interest to a system interaction review are those that are either directly or indirectly associated with the basic safety functions. The failure of a safety criterion is a condition that will degrade the performance or exceed the capability of a system associated with the basic safety functions. The term "degrade the performance" refers to the inability of a system to operate according to design specifications.

Systems Interactions

Notwithstanding that many intersystems dependencies are intended by design, the connotation of an adverse intersystem dependence is inherently part of the definition of a systems interaction. The failure of at least one of the basic safety criteria is the first essential characteristic of an adverse systems interaction.

Hypothetically, a basic safety criterion could be failed where only one component failed within all the systems of an LWR. Although not a likely state,

this failed state is mentioned here to show contrast in our terms. Already, the licensing process requires specific functions at plants to meet a single failure criterion; but excluded from this criterion is consideration of the failure of passive components in fluid systems. To comply with the single failure criterion, LWR designs use independent systems and components to provide the basic safety functions. Yet, the potential that these "independent" systems might be vulnerable to dependent failures has created the need for a Systems Interaction Program.

If a basic safety criterion is failed, then it is more likely that it was caused by more than one component failure. Multiple failures can result from either independent or dependent causes which are separately treated in a Probabilistic Risk Assessment once the causes are determined. Independently caused multiple failures occur by remote coincidence and their joint probability can be easily calculated for feasible combinations of failures given suitable failure data. Dependently caused multiple failures result from the influence of a coupling among systems in the plant and their joint occurrence has a higher probability than the value obtained assuming independent failures. The incremental difference in probabilities is a measure of the relative importance among combinations of multiple, dependent failures. Because we are concerned with multiple, dependent failures, the second essential characteristic of a systems interaction is the coupling that causes the dependent effects.

During any scenario from an initiating event to the failure of a basic safety criterion, the multiple, dependent failures could occur either as parallel effects (simultaneously) or as a serial effect (sequentially). Only when the plant possesses a precondition that can jointly effect intentionally "independent" systems associated with a basic safety function, is it possible for a licensed LWR to fail a basic safety criterion from the occurrence of one initial failure. Thus, the third characteristic of a systems interaction is a precondition that allows systems to be jointly influenced that were intended to be independent.

An adverse systems interaction exists where a dependent fault occurs in at least one system that was intended by design to independently serve a basic safety function. An intersystems dependency simultaneiously transmits the effects of a fault to more than one system. Systems interactions that were not intended by design, i.e., not explicitly included in the design description, are referred to as hidden dependencies.

2.4. Types of System Interactions

Our review of adverse events show that there are different types of system interactions. The state-of-the art survey showed that some methods more efficiently identify specific systems interaction types than other methods. Thus, the classification of systems interaction by type is useful to guide the analysts in matching the method(s) best suited to the particular evaluation. Systems interactions of interest to the systems interaction review can be conveniently categorized by the nature of the coupling between the systems:

Functionally coupled systems interactions result either from the sharing of components between systems or through physical connections between systems including electrical, hydraulic, pneumatic and mechnical.

Spatially coupled systems interactions result from the proximity of systems to one another within the plant. For example, a steam leak could short out an electrical junction box across the room from the steamline. A systems interaction results based on this spatial coupling. Inherent to a spatial coupling is the concept of spatial domain. Typical spatial couplings involve water, steam, fire, explosion, radiation, or pipe whip. The domain over which a coupling can realistically occur will vary depending upon the barriers in the plant. For example, water leaking from a line in one room may affect equipment in adjoining rooms. But a high pressure pipe whip will affect only systems in the room within reach of that pipe.

Humanly coupled systems interactions are special since the operators could influence all systems in the plant. To better focus the reviews, the guidance excludes human error and sabotage from systems interaction reviews. Systems interaction reviews will assume the operator follows procedure when interacting among systems and the procedure is correct. The focus is a fault within one system that induces the operator to influence another, otherwise independent system in the unsafe direction. To illustrate let us postulate a failure with a power supply that causes instruments to disply spurious readings to the operator who is misled into influencing another system.

3.0 The Systems Interaction Review Process

The staff conducted a survey of the state-of-the-art of methods that could be employed for systems interaction reviews. Three laboratories (Batelle Memorial Institute, Brookhaven National Laboratory, and Lawrence Livermore National Laboratory) aided in performing the survey, and their final reports with recommendations are documented in the References. During the survey a range of methods were evaluated including Fault Trees, Event Trees, Cause-Consequence Diagrams, GO Methodology, Failure Modes and Effects Analysis, Walk-Downs, Operational Survey, Markov Modeling, Phased Mission Analysis, Diversion Path Analysis, and Generic Cause Analysis. Analysts discipline their reviews by these formalized courses of reasoning.

The survey concluded that no single method is presently available in a form that can be immediately used to perform an adequate review for adverse systems interactions and recommended an approach using different combinations of methods; each combination will screen out adverse systems interaction by following a stepwise review process. It appears beneficial to iterate between steps 1 and 2 to adequately complete a review.

The three-step process is:

1. Model the plant to select the combinations of systems for detailed evaluation;

2. Search the selected systems to identify system interactions; and

3. Evaluate the systems interactions against criteria for corrective action.

A comprehensive review is expected to employ analytical methods, visual inspections, experience feedback, and simulator dependencies-experiments.

The systems interaction review is aimed at the identification of those couplings between systems which will lead to an adverse system interaction when the necessary initiating event occurs. Although systems interactions can be conveniently categorized by type of coupling, it is important to maintain an overall perspective on the identification process. Any adverse systems interaction could involve a number of different types of couplings in the cascading of effects among systems.

Functional couplings are especially important and a basic understanding by modeling of the design is a prerequisite to the identification of systems interactions. The search for spatial or human couplings cannot proceed without this basic understanding of the plant's systems.

3.1 Model the Plant to Select the Combination of Systems for Detailed Evaluation

The first step is akin to that in a reliability or a risk assessment. Plant specific results from such an assessment will facilitate this step. A systematic approach must be taken because the plant is too complex and the dependencies are too subtle for the reviewer(s) to evaluate without the use of a formal systems modelling technique. In subsequent steps, there is the possible need to analyze the systems in detail. Detailed analyses could burden the review by the magnitude of the numbers of components. A set of identifiers are needed to tract the various systems, subsystems, and components identified in the modelling process. These identifiers should permit the addition of potential couplings that are identified in the next step of the review. Thus, a logic model for the plant is developed which relates the functional dependencies among systems required to fulfill the basic safety functions.

In modelling the plant <u>all</u> the systems that serve the basic safety functions must be considered, e.g., the maintenance of reactor coolant inventory in an operating PWR requires not only the charging pumps with a supply of water, but also motive power, instrument power, component cooling, lubrication, as well as environmental control and structual support for all these systems. The less-than-obvious functional couplings are expected to lie at these support levels.

To complete the first step the analysts must select the combinations of systems for detailed analysis based upon the logic model. It appears the systems having the largest number of couplings to the basic safety functions are most likely to reveal systems interactions. The selection must be congruent with operating experience. Thus, engineering judgment could modify the final selection of the combinations of systems for detailed analysis.

3.2 Search the Selected Systems to Identify Systems Interactions

The guidance for this second step is discussed below by the type of systems interaction.

Functionally coupled: The search should now proceed by modelling the functional couplings of the selected systems through multiple tiers of dependencies toward the subsystems and components. The detail should be truncated at the highest level at which a specific hidden dependency is first modelled. Having identified a hidden dependency, the systems interaction should be characterized.

The following charaterizes a systems interaction:

1. The random failure that will initiate the scenario.

2. The type of physical coupling that compromised the intended independence.

3. The systems that were combined.

4. A brief summary of the scenarios including the cascade paths, the other affected systems, and the plant operating mode.

5. The functional safety consequences including the degree of impairment of the basic safety functions.

At times the detailed modelling of the functional couplings will proceed to where there is confidence that no hidden dependency exists. It remains that such systems will be reviewed for both spatially and humanly coupled systems interactions.

Spatially coupled: The identification is based upon a search of plant arrangements by performing a systematic visual inspection. Where they exist, plant specific reviews (seismic, environmental qualification, fire) supplement and can facilitate the visual inspection. It is not the intent to duplicate existing reviews, rather it intends to draw on these reviews for completeness.

The actual visual inspection must use a multidisciplinary team of experts to provide joint, immediate judgment on the feasibility of each systems interaction. This vital step provides a focus on the inductive "what if" questions. The multidisciplinary-team inspection provides the rationale upon which specific combinations of fault can be based.

Humanly coupled: Control room simulators appear to be an effective tool to search for humanly coupled (and potentially functionally coupled) systems interactions resulting from power supply, control system, and instrumentation failures. This can be done by simulating selected failures and searching for an impairment of the systems associated with the basic safety functions.

Alternatively, the sets of signals to the operator identified in the emergency procedures form sets of associated equipment with functional couplings that can be searched for hidden dependencies.

3.3 Evaluate the Systems Interactions Against Criteria for Corrective Action

The emphasis in the pilot reviews is on identifying adverse systems interactions, not on corrective action. Until specific criteria to evaluate the systems interactions are developed, the adverse systems interactions will be evaluated to assure compliance with current requirements. The utility may choose to take corrective actions based on this pilot review effort in order to improve plant performance and systems safety.

4.0 Systems Interaction Reviews and PRAs

An important organizational interface exists between the System Interactions Review defined here and Probabilistic Risk Assessments since both efforts treat dependent faults. In a PRA the analysts need the joint probability of two or more dependent faults to assess their relative importance; while a Systems Interaction Review is aimed at a description of the preconditions that cause the faults to be dependent. The results of a Systems Interaction Review will be fully characterized system interactions (mechanistically defined system problems describing the systems and the couplings between them) to be evaluated by the responsible technical organizations. Conceptually such fully characterized systems interactions could be by-products of a PRA; pragmatically, PRA's and Systems Interactions Reviews are complementary in assuring the reliability of LWR safety functions.

References

1. A. Buslik, I. Papazoglou, R. Bari, Brookhaven National Laboratory, "Review and Evaluation of Systems Interaction Methods," USNRC Report NUREG/CR-1901, January 1981.

2. P. Cybulskis, et al., Battelle Memorial Institute, "Review of Systems Interaction Methodologies," USNRC Report NUREG/CR-1896, January 1981.

3. J. Lim, R. McCord, and T. Rice, Lawrence Livermore National Laboratory, "Systems Interaction: State-of-the-Art Review and Methods Evaluation," USNRC Report NUREG/CR-1859, January 1981.