Coffman

10

DRAFT

INITIAL GUIDANCE FOR THE PERFORMANCE OF SYSTEMS INTERACTION ANALYSES AT SELECTED LWRS

(GUIDANCE FOR INTERIM USE AND COMMENT)

Reliability and Risk Assessment Branch
Division of Safety Technology
Office of Nuclear Reactor Regulation

U.S. Nuclear Regulatory Commission
Washington, DC 20555

DRAFT

CONTENTS

CONTENTS (Continued)

Page

APPENDICES

1 INTRODUCTION

1.1 Purpose

This report is issued to provide guidance that the Office of Nuclear Reactor Regulation believes should be followed during the systems interaction analysis at a selected LWR. Compliance with this report is not a regulatory requirement and it is not a substitute for the regulations. This report defines both the minimum general ingredients for an acceptable systems interaction analysis and ~~an~~ two illustrative, specific procedures. We encourage the use of improvements to the specific procedures and the application of different procedures. However, an application of a different procedure will be accepted only where it complies with the minimum general ingredients described in 5.~~1~~2.

The objective of a systems interaction analysis is to assure that safe operation of the plant is not compromised by adverse systems interactions. The assurance is provided through both the conduct and the documentation of the systems interaction analysis. The documentation provides evidence of the extent to which the plant was analyzed for dependent faults that will fail one of four systems interaction criteria (to be described in Chapter 4).

The byproducts of a systems interaction analysis include the discovery of hidden dependencies as improvements to event and fault sequences ~~defined for~~ used in reliability and risk assessments, the discovery of adverse systems interactions ~~identification of safety issues~~ that are potentially generic to other plants, and the alerting of design, manufacturing, and operations personnel to the hazards that compose adverse systems interactions.

1.2 Background

The staff's systems interaction program was initiated in May 1978 with the definition of USI A-17 (Systems Interaction in Nuclear Power Plants) and was intensified by TAP (NUREG-0660) Item II.C.3 (Systems Interaction). The concern arises because the design, analysis and installation of systems are frequently the responsibility of teams of engineers with functional specialties--such as civil, electrical, mechanical, or nuclear. Experience at operating plants has led to questions of whether the work of these functional specialists is sufficiently integrated to enable them to minimize adverse interactions among systems. Some adverse events that occurred in the past might have been prevented if the teams had assured the necessary independence of safety systems under all the conditions of operation.

Generally, the nuclear power industry is without a comprehensive program that separately evaluates all structures, systems, and components important to safety for the three categories of adverse systems interactions, i.e., spatially coupled, functionally coupled, and humanly coupled. However, there is piecemeal assurance that LWRs can be operated without endangering the health and safety of the public. Each licensed plant has been evaluated against licensing requirements that are founded on the principle of defense-in-depth. Adherence to this principle results in requirements such as physical separation and independence of redundant safety systems, and protection against hazards such as high energy line ruptures, missiles, high winds, flooding, seismic events, fires, human factors, and sabotage. Many of these design provisions are subject to review against the Standard Review Plan (NUREG-75-087) which requires interdisciplinary reviews of safety-grade equipment and address different types of potential systems interactions. Also, the quality assurance program which is followed during the design, construction and operational phases ior each plant contributes to the prevention of introducing adverse systems interactions. Thus, the licensing requirements and procedures provide piecemeal evidence of an adequate degree of plant safety.

The NRC staff's current procedures assign primary responsibility for review of various technical areas to specific organizational units and assign secondary responsibility to other units where there is a functional interface. Designers follow somewhat similar procedures and provide for the analyses of systems and for interface reviews. The Office has been developing methods that could identify adverse systems interactions which were not considered by current review procedures. The first phase of this study began in May 1978 and was completed in February 1980 by Sandia Laboratories under contract to the NRC staff.

The Phase I investigation was structured to identify areas where interactions are possible between systems and have the potential of negating or seriously degrading the performance of safety ~~functions~~ actions. The study concentrated on commonly caused failures among systems that would violate a safety ~~function~~ action. The investigation was to then identify where NRC review procedures may not have properly accounted for these interactions.

The Sandia Laboratories used fault-tree analysis on one design to identify component failure combinations (cut-sets) that could result in loss of a safety function. The minimal cut-sets were further reduced by incorporating six linking systems failures into the analysis. The results of the Sandia effort indicated a few potentially adverse systems interactions within the limited scope of the study. The staff reviewed the interactions for safety significance and generic implications. The staff concluded that no corrective measures needed to be implemented immediately except for the potential interaction between the PORV and its block valve. This interaction had been separately identified by the evaluations of the TMI-2 accident while Sandia was performing their study. Since corrective measures were already being implemented, no separate measures were needed under USI A-17.

The "NRC Action Plan Developed as a Result of the TMI-2 Accident," NUREG-0660, provides for a systems interaction follow-on study, Section II.C.3, "Systems Interactions." Since April 1980, the Office of Nuclear Reactor Regulation has intensified the effort both by broadening the study of methods to identify potential systems interactions and by preparing this guidance for ~~audit~~ analysis ~~reviews~~ of selected plants for systems interactions. Our recent experience provides a basis from which we ~~developed~~ are developing a more efficient review process for ~~potential~~ adverse system interactions. The process will provide for a resolution of USI A-17, assimilate operating reactor experience, and rank identified systems interactions by their relative importance to safety.

As a part of our responsibility and preparatory to the development of regulatory guidance addressing systems interactions, we conducted a ~~review~~ survey and evaluation of the state-of-the-art of methods that might be applicable for near-term analyses ~~of~~ for systems interactions. Three laboratories (Battelle Memorial Institute, Brookhaven National Laboratory, and Lawrence Livermore National Laboratory) aided in performing the ~~review~~ survey and evaluation and their final reports with recommendations are documented in References ~~10~~ 1, ~~11~~ 2, and ~~12~~ 3. The laboratory reports address both near-term and long-term analysis capabilities and needs. This report makes extensive use of the results of the laboratory ~~reviews~~ surveys as well as information gained from other reports and discussions with experts in the field both within and outside of the NRC.

It is expected that the development of systematic ways to ~~identify~~ discover, rank, and evaluate systems interactions will go further to reduce the likelihood of intersystem failures resulting in the loss of plant safety functions. A comprehensive program is expected to employ analytical methods, visual inspections, experience feedback, and simulator dependencies experiments. ~~The LWR industry's current experience with systems interaction analyses is fragmented.~~ Experience like that gained by the Phase I study is an essential ingredient to the staff's considerations of a comprehensive systems interaction program. After the systems interaction analys~~i~~es ~~is~~ are performed on ~~a~~ the selected LWR, we will decide whether separate analyses for systems interaction ~~analyses~~ must be performed on all LWRs.

1.3 Implementation

Implementation of the Systems Interaction Initial Guidance is a critical prerequisite to a general licensing requirement since the Nuclear Industry's experience with systems interactions analysis of LWRs is fragmented. Since the Initial Guidance includes the details of both the analysis process and the techniques to be used during the analysis, implementation will provide the experience feedback necessary to demonstrate that both the analysis process and the proposed techniques can identify all three types of systems interactions. The implementation will establish the applicability of the ~~interim~~ initial guidance for the identification and ranking of systems interactions, and identify any modifications to the guidance that should be made prior to issuing a final Systems Interactions Guidance to all applicants and licensees.

An expected benefit from the initial implementation will be the identification of the feasible range of ~~all types of~~ systems interactions at plants that have different combinations of NSSS and BOP designs. Specifically, there are three types of systems interactions of interest to the staff: spatially coupled, functionally coupled, and humanly coupled systems interactions. The Crystal River-3 event of February 1980 is a good example, where a single failure in a nonsafety-grade power supply resulted in the stuck open PORV and a small LOCA. This event includes the functionally coupled systems interactions where the reactor power, turbine control valve position, and feedwater controls are functionally dependent upon the integrated control system which is fed by the nonsafety-grade power supply buses. A humanly coupled systems interaction was also involved in this event in that one operator was following the correct procedures by balancing high pressure injection flow between the loops while he was unaware that one HPI flow indicator had failed in the mid-scale position (which resulted from the nonsafety-grade power supply failure). Thus, the real potential existed for the operators to take inappropriate action (even though he followed procedures correctly) affecting more than one system because of erroneous readouts on ~~the~~ a main panel.

An example of a spatially coupled systems interaction~~s~~ is the Browns Ferry-1 fire which resulted in closure of the main steam isolation valves and hindrance of the supply of makeup cooling water in Unit 1 for the decay heat removal function.

Although specific plants have been suggested by the ACRS and other~~s~~ groups for the initial implementation of the Systems Interaction ~~Interim~~ Initial Guidance, several optional approaches to the implementation were explored. Each option was evaluated against important items such as NRR manpower, resources, and schedule, cost to the utility, and the usefulness to the development of regulatory guides and SRPs. A detailed discussion of the specific implementation to be performed is discussed in Chapter 3.

Chapter 4 describes the elementary terminology of systems interaction analyses. Chapter 5 provides the guidelines for conducting the systems interaction analysis at ~~a~~ one of the selected LWR and Chapter 6 describes the guidelines for the review of the program results.

1.4 Coordination

A systems interaction analysis is aimed at searching for hidden intersystems dependencies that can jeopardize past assumptions of systems independence, whether those assumptions were either stated or implicit.

Nuclear power plant systems have been designed against "the single failure criterion." The degree to which the design of specific systems complies with the single failure criterion remains the responsibility of the chartered technical review branches. The systems interaction analysis is not intended to duplicate such evaluations. Because intersystems dependencies could cross any system's boundary, the systems interaction analysts will share some concerns with ~~the~~ some technical review branches and other ongoing programs.

One of the ongoing programs is the performance of a Probabilistic Risk Assessment. Risk assessments also treat dependent faults by relying upon the analysts knowledge of the plant a failure rate data to quantify the probabilistic effects of hidden dependencies. By contrast, systems interaction analyses model the plants ir a systematic way to discover hidden dependencies. The result of a PRA is consistent ranking of the main risk contributors to be used by management to allocate resources. The result of a systems interaction analysis is a phenomenologically determined systems problem to be corrected by the responsible technical review branches. Together, PRAs and systems interaction analyses are supplementary in assuring the reliability of LWR safety functions.

Significant systems interactions are often coupled by "Human Errors," and we intend to search for some of these hidden dependencies. The results of our search will be closely coordinated with the Division of Human Factors Safety. Some Latent Human Errors due to improperly written procedures, or inadequate training can be the common cause in an adverse systems interaction. However, our reviews are not expected to concentrate on these types of Human Errors; rather, we rely upon the Division of Human Factors to identify and evaluate Latent Human Errors.

2 OVERVIEW (EXECUTIVE SUMMARY)

The NRC's systems interaction program was initiated in 1978 with the definition of an Unresolved Safety Issue 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, installation, and maintenance of systems is frequently the responsibility of teams of engineers with specialities. Experience at operating plants led to questions whether the work of these engineering specialists is sufficiently integrated to minimize adverse interactions among systems. For example, ~~last year~~ in 1980 at Crystal River-3, 40,000 gallons of primary coolant inventory were lost from a short to ground in a nonsafety-grade 24 VDC power supply during normal operations. Such adverse events might have been prevented if the specialist teams assured the necessary independence of safety functions under all conditions of operation. The staff is considering the issuance of a regulatory requirement for separate reviews for adverse systems interaction.

2.1 Terminology

The terminology given here is fundamental to the review for adverse systems interactions and serves to introduce the specific emphasis of the approach.

To avoid unacceptable reactor core damage and a release of unacceptable levels of radioactivity to the site environs, the following systems safety actions can be specified:

To maintain the primary coolant inventory.

To transfer the heat from the reactor to the ultimate heat sink.

To render and keep the entire core subcritical.

To maintain the integrity of the containment and control radioactivity releases.

A condition that will degrade the performance or exceed the capability of a system associated with ~~the~~ these systems safety actions constitutes the failure of a safety criterion.

If a systems safety criterion is failed, then it is likely that it was caused by more than one component failure. ~~Multiple failures can result from either independent or dependent causes.~~ Independently caused multiple failures occur by remote coincidence. Dependently caused multiple failures result from the influence of a coupling. Because we are concerned with multiple, dependent failures, the second essential characteristic of a systems interaction is the coupling that causes the failures to be dependent. ~~effects.~~

During any scenario from an initiating event to the failure of a systems 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 simultaneously effect intentionally "independent" systems is it possible to fail a systems 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 simultaneously influenced.

An intersystems dependency simultaneously 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.

The systems interactions of interest 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 coupling between systems, including electrical, hydraulic, pneumatic, and mechanical.

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. The domain over which a coupling can realistically occur will vary depending upon the nature of the barriers in the plant.

Humanly coupled systems interactions are special since the operators could influence all systems in the plant. To better focus the reviews, we excluded inadvertent human error. Systems interaction reviews will assume the operator follows procedure when influencing a system and the procedure is correct.

2.2 The Analysis Process

The staff conducted a survey 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, 1, 2, and 3.

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. The three-step process is:

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

2. Search the selected combinations of systems, and

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

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

Although systems interactions can be conveniently categorized by their 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 dependencies is a prerequisite to the identification of systems interactions. The search for spatial or human couplings best proceeds with a basic understanding of the plant's design dependencies.

A systematic approach must be taken because the plant is too complex and the ~~deficiencies~~ dependencies are too subtle for the reviewer to understand without the use of a logical systems modelling technique. Thus, a logic model for the plant is developed which describes the functional dependencies among systems required to fulfill the systems safety actions.

In modelling the plant all the systems that serve the systems safety actions 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 structural support for all these systems. The less-than-obvious functional coupled systems interactions 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. The selection must be congruent with operating experience. Thus, professional judgment could modify the final selection of the combinations of systems for detailed analysis.

The second step, the search, should now proceed by modelling the functional couplings of the selected systems through multiple tiers of dependencies toward the subsystems and components.

At times the detailed modelling 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.

The identification of spatial couplings is based upon a search of plant arrangements by performing a systematic visual inspection. Where they exist, plant specific reviews (e.g., seismic) supplement and can facilitate the visual inspection. It is not the intent of systems interaction reviews to duplicate existing reviews, rather to draw on these reviews.

The actual visual inspection must use a multidisciplinary team to provide joint, immediate judgment on the feasibility of each systems interaction. This vital ingredient provides a focus on the inductive "what if" questions. The multidisciplinary-team inspection provides the rationale upon which to base the selection of specific combinations of faults.

Control rcom simulators appear to be an effective tool to search for humanly 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 that perform the systems safety actions. 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.

The emphasis in the reviews is on the search for adverse systems interactions, not on corrective action. Until specific criteria to evaluate the systems interactions are developed, adverse systems interactions will be evaluated to assure compliance with current requirements. The utility on its own may choose to take corrective actions.

An important interface exists between the analyses ~~reviews~~ defined here and PRAs since both efforts treat dependent faults. A PRA provides a means of weighing the relative importance of two or more dependent faults while a Systems

Interaction ~~Review~~ Analysis is aimed at finding the preconditions that cause faults to be dependent. Thus, the results of a systems interaction ~~review~~ analysis are important enough by themselves. Additionally, it is important that a PRA assimulate the design dependencies described in the results of an ~~SI~~ systems interaction analysis.

3 SCOPE AND SCHEDULE

Some implementation of the Systems Interaction ~~Interim~~ Initial Guidance is a critical prerequisite to a general licensing requirement since the Nuclear Industry's experience with systems interactions analysis of LWRs is fragmented. Since the Initial Guidance includes the details of both the analysis process and the techniques to be used during the analysis, some implementation will provide the experience feedback necessary to demonstrate that both the analysis process and the proposed techniques can search and ~~identify~~ discover all three types of systems interactions.

The implementation will ~~establish~~ demonstrate the applicability of the initial guidance for the search and evaluation of systems interactions, and identify any modifications to the guidance that should be made prior to issuing a final Systems Interactions Analysis Requirement for all applicants and licensees.

There are three types of systems interactions of interest to the staff: spatially coupled, functionally coupled and humanly coupled systems interactions. The Crystal River-3 event of February 1980 is a good example where a single failure in a nonsafety-grade power supply resulted in the stuck open PORV and a small LOCA. This event includes the functionally coupled systems interactions where the reactor power, turbine control valve position and feed water controls are functionally dependent upon the integrated control system which is fed by the nonsafety-grade power supply buses. A humanly couple systems interaction was also involved in this event in that one operator was following the correct procedures by balancing high pressure injection flow between the loops while he was unaware that one HPI flow indicator had failed in mid-scale position which resulted from the nonsafety-grade power supply failure. Thus, the real potential existed for the operators to take inappropriate action (even though he followed procedures correctly) affecting more than one system because of erroneous readouts on ~~the~~ a main panel.

An example of a spatially coupled systems interactions is the Browns Ferry-1 fire which resulted in closure of the main steam isolation valves and hinderance of the supply of makeup cooling water in Unit 1 for decay heat removal purposes. An expected benefit of the initial implementation process will be to ascertain the feasible range of all types of systems interactions at plants that have different combinations of NSSS and BOP designs.

Although specific plants have been suggested by the ACRS, ~~the~~ and other~~s~~ groups for the implementation of the Systems Interaction Initial Guidance, several optional approaches to the implementation were explored.(6) Each option was evaluated against the major important items such as NRR manpower resources and schedule, cost to the utility, and the usefulness to the development of regulatory guides and SRPs.

The best option ~~is~~ was to select a few plants on the basis of the importance criteria, apply the existing Initial Guidance in each plant, and review the results (the review criteria will consist of current licensing requirements). There are many advantages to this option. These include:

1. Only 2 to 3 NRR professional staff years will be needed to monitor these initial reviews.

2. Since only a few plants are involved, the major emphasis will be put on a detailed search for all types of systems interactions and suggested methods to efficiently identify these systems interactions.

3. The expected period of the systems interaction analysis of an LWR and its review is about 18 months. This is consistent with the schedule proposed to the Commissioners for the development of a Regulatory Guide for systems interaction analysis of LWRs.

4. A systems interaction analysis of an LWR includes site specific hazards, such as the Midland-2 process steam interface with the Dow Chemical Plant or high population sites as mentioned in NRC Report SECY 81-25 dated Jan. 12, 1981. Thus, the systems interactions analysis of an LWR can

provide added assurance for public health and safety at plants selected because of their site specific hazard.

5. This option allows resolutions of USI A-17 and TMI Action Plan Item II.C.3 without adding new licensing requirements.

6. The results of a systems interaction analysis of a generic group of plants has little value to a specific plant because equipment arrangements are specific to each plant. The results obtained at the end of implementing the guidance on a specific plant will be directly applicable to the specific plant selected and no additional systems interaction analysis should be needed.

The only disadvantage with this option is that the costs will be borne by the selected utility (estimated $2 million). However, the utility costs could be reduced if they effectively coordinate the systems interaction ~~review~~ analysis with other related programs at the selected facility, such as their fire program, flood analysis, high energy pipebreak effects analysis, "~~2~~ II over ~~1~~ I" assessment (nonseismic ~~system~~ Component effects on seismic ~~systems~~ components), failure mode and effects analysis of electrical and electronic equipment, equipment qualification program and specific site hazard analyses.

4 TERMINOLOGY

The objective of this section is to describe the important terms and concepts of systems interaction analyses in LWRs. The term "Systems Interaction" has had ~~a~~ many ~~broad range of~~ usages. The usage described here is fundamental to the approach for the near-term evaluation of LWR's susceptibilities to adverse systems interactions and serve to introduce the specific emphasis of the approach. The terms presented here are both rigorous enough to proceed with the Systems Interaction Program and flexible to allow for further development, if needed. Figure 1 is included to provide orientation as the reader proceeds to understand the fundamental terms of the Systems Interaction Program.

4.1 Systems Safety Actions and Systems Safety Criteria

The safety philosophy behind the design of a nuclear reactor plant is that of providing several barriers between the fission products and the environment ~~in order~~ to make the release of radioactivity to the environment an extremely unlikely event. To support these barriers, in the event of an accident, a number of vital safety actions should be performed by various systems. In designing these systems, care has been taken to provide several independent ways in which a safety action can be performed. Generally, this care is expressed as ~~expressed in terms of~~ redundancy and diversity so that, ideally, several independent system failures are necessary to have degradation or failure of a safety action.

The intended systems safety of an LWR design is to provide assurance against unacceptable reactor core damage and a release of unacceptable levels of radioactivity to the site environs.

In order to have unacceptable reactor core damage and a release of unacceptable levels of radioactivity to the site environs two things must happen: a) an accident must be initiated, e.g., Loss of Coolant Accident (LOCA) initiator or a transient initiator must occur; and, b) one or more vital safety action must degrade or fail. The Systems Interaction Program is currently focused on the following systems safety actions:

1. Keep coolant on the core.
2. Keep the path for heat to move from the core to the ultimate heat sink.
3. Keep the ability to shut down the core.
4. Keep the engineered safety features operational.

We define a "failure of a systems safety criterion" as a condition that results in the degraded independence of two or more systems associated with the systems safety actions. The term "degraded independence" refers to a systems action that can be influenced by another system whose influence should have been outside the design specifications. Correspondingly, failure of a safety criterion means either a complete inability to meet the corresponding safety action or a reduced assurance that the safety action will be met. The systems safety criteria are:

1. The systems relied upon to maintain the primary coolant inventory shall be unimpaired.

2. The systems relied upon to transfer decay heat from the reactor to the ultimate heat sink shall be unimpaired.

3. The systems relied upon to render and keep the entire core subcritical shall be unimpaired.

4. The Engineered Safety Features, including those for the control radioactive material, shall be unimpaired.

The satisfaction of each of these systms safety criteria contributes to the satisfaction of the general safety objective. The systems of interest to a system interaction analysis include necessary front line systems and support systems (nonsafety-grade systems are not excluded). The actions of ~~a~~ safety-grade system~~s~~ caused by an influence from nonsafety-grade system~~s~~ that was outside the design specification should be deemed a failure of a systems safety criterion.

4.2 Terms

Systems Interaction

Notwithstanding that many intersystems dependencies are intended by design, the connotation of an adverse intersystem dependency is inherently part of the use of "systems interactions."

If a condition in the plant exists that affects the safety of the plant in a way not intended by the design, it could be that a systems interaction exists. The presence of a system interaction increases the likelihood of an unacceptable accident, by increasing the likelihood of failure of the systems safety actions. A systems interaction exists if multiple faults occur in systems that were intended in the design to independently serve at least one systems safety action.

Two comments are relevant at this point.

a) The possibility that the dependent faults may exist in the same system seems to contradict the term system~~-~~interaction (which implies different systems). Since there is no standard grouping of the components of a nuclear power plant into systems, some analysts could "define out" important problems by grouping faulted components into the same system. ~~This~~ Such grouping subverts public safety.

b) The phrase "intended in the design" is necessary because there exists ~~dependent faults~~ intersystems dependencies that are known and are intended. For example, all the components of one train of a fluid system or the components of one channel of an electrical system are connected in series and, therefore, completely dependent. A valve failed in the closed position results in a fault of the pump of the same train. Yet, this dependency is known and intended both by the design and review procedures. On the other hand, a dependence between two faults in redundant trains or in different safety-grade systems are not intended and thus constitutes a system interaction.

A common cause failure is a group of multiple, dependent, concurrent failures, i.e., faults that have been combined because they share the same initiator. In casual usage, there is little practical distinction between a common cause failure and a systems interaction. Like a systems interaction, a common cause failure results only when the plant possesses a precondition that allows concurrent, dependent effects to be propagated from a single cause.

There are four nuances in the more rigorous usage of the term "systems interaction" in contrast with the term "common cause failure." First, the tendency in the usage of "common cause failure" is to identify separately the specific failure that created concurrently other failures. Compare this with the usage of "systems interaction" where the tendency is to identify collectively the initiating failure, the entire sequence of failures, and the specific failure that created concurrently other failures. Second, the usage of "common cause failure" leads us to thinking that the effected multiple failures resulted simultaneously from a single failure. Whereas, the usage of "systems interaction" includes our experience where the multiple faults resulted from a combination of both sequential and simultaneous failures. Next, the term "common cause failure" can apply to resultant failures that are all contained within one system. The term "systems interaction" applies to resultant failures that have crossed systems boundaries. Finally, the term "common cause failure" is used frequently without a suggestion of its ultimate consequence. By comparison, the term "systems interaction" inherently connotes an adverse consequence, i.e., the systems interaction initiating failure results in the failure of a ~~basic~~ systems safety criterion.

Failure (event): The inability of a system or part of a system to perform its intended function due to an internal state.

Fault (event): The inability of a system, or part of a system to perform its intended function due to an external state.

Independent events: Events that do not influence each other.

Dependent events: Events that influence the occurrence of each other.

Initiating event: An event upon which the occurrence of subsequent events may depend. Usually, no analysis had been performed on the events that led to the initiating event. In that sense, the initiating event is a random event (ie., no causal relationship has been analyzed).

4.3 Types of Systems Interaction

A review of operating reactor experience indicates that there are different types of systems interactions. The state-of-the-art ~~reviews~~ surveys (Ref 1, 2, & 3) show that some me~~n~~thods more efficiently search for certain types of systems interaction then other methods. There are many ways to classify the types of systems interactions. However, the classification of systems interactions by coupling is most useful to guide the analyst in matching the methods to the particular evaluation. Systems interactions have occurred through couplings between systems and subsystems. Then there is a cascading effect of the system affecting another via this coupling. Normally, several systems will be involved via various couplings in any given systems interaction. These couplings fall into three catogories:

1. Functional coupling
2. Spatial coupling
3. Human coupling

Functional couplings have resulted either from the sharing of components between systems or through physical connections between systems including electrical, hydraulic, pneumatic and mechanical connections. For example, the electrical connection from the 4160V engineered safety features bus to the safety injection pump in a CE PWR constitutes a functional coupling.

Spatial couplings have resulted 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 in the concept of a spatial coupling is the spatial domain associated with the various spatial couplings involved. Typical spatial couplings involve water, steam, fire, explosion, radiation or pipe whip. The domain over which a coupling can realistically occur will vary with the design features of the plant. For example, water leaking from a line in one room may affect equipment in adjoining rooms. But breakage of a high pressure pipe followed by pipe whip will affect only systems in the room within reach of that pipe (provided the walls of the room realistically define the spatial domain for that pipe). Each type of spatial coupling has its own realistic domain. The domain concept is inherent to identifying these spatial couplings.

Human couplings are a special case which can link all systems in a plant. That is, the action in one system can trigger the plant operator to initiate action in another otherwise independent system. The operator has coupled the two systems and has become part of the overall systems interaction.

Furthermore, if human error is considered, virtually any system design is susceptible to an adverse systems interaction. The actions of the "human coupling" tend to be the least predictable of any system in the plant, and the human has the greatest freedom to interact throughout the plant.

At this point it is necessary to touch upon a fundamental feature of systems interaction analyses. A systems interaction analysis is directed toward the search for the plant conditions that couple effects to their causes. The analysis presumes that the means exist both to determine and to describe such cause-effect relationships. Regarding humanly coupled systems interactions, this presumption is only true where the effect and its causes are related either (a) by an operator fastidiously following a written procedure or (b) by a saboteur following a malevolent purpose with knowledge of a plant's vulnerability. There remain a large number of error-likely conditions where the relationships between the causal influences and the effects cannot be determined and described. For such conditions where there are many combinations of influences on the human and his predisposal penchants, there are other NRC efforts based upon ergonomics and applications of probability theory. Thus, a system interaction analysis is necessarily constrained to search only for those plant conditions for which a unique cause-effect relationship can be determined.

4.4 Characteristics of Systems Interactions

Notwithstanding that many intersystems dependencies are desired by design, the connotation of an adverse intersystems dependency is inherently part of the use of the term "systems interaction."

The failure of at least one of these systems safety criteria is the first essential characteristic of an adverse systems interaction. Hypothetically, a ~~basic~~ systems 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 use of 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 assure the systems safety actions. Yet, the potential that these independent systems might be vulnerable to hidden dependencies has created the need for a Systems Interaction Program.

It is more likely that a systems safety criterion could be failed by the existence of more than one failed component in the LWR. Multiple failures can result from either independent or dependent causes which are separately treated in a probabilistic risk assessment (PRA) 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 rate data. Dependently caused multiple failures result from the influence of a coupling in the plant and their joint occurrence has a higher probability than the value obtained assuming independent failures. Because we are concerned with commonly caused multiple failures, the second essential characteristic of a systems interaction is the couplings that cause the failures to be dependent. An effect, whether or not it is a failure, that was caused by another failure is termed a "fault."

During any scenario from an initiating event to the failure of a systems safety criterion, the multiple dependent failures (faults) could occur either as parallel effects (simultaneously) or as serial effects (sequentially). Only when the plant possesses a precondition that can simulaneously affect intentionally "independent" systems which perform a systems safety action is it possible for a licensed LWR to fail a systems 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 simultaneously influenced. The systems must be such that ~~they both~~ at least on system assures a basic safety criterion and the systems were designed to be independent.

Thus, we can state that an adverse systems interaction is a precondition within the plant that would fail a systems safety criterion as a consequence of both an intersystems dependency and an initiating malfunction. An intersystems dependency simultaneously transmits the effects of an initiating failure to more than one system. Systems interactions that were not intended by design, i.e., not explicitly included in the design descriptions, can be referred to as hidden dependencies.

The relative safety importance among systems interactions is determined primarily by the degree of impairment of systems safety actions. Two considerations bear on the degree of impairment: (1) the specific state of the plant, and (2) the initiating failure. The relative safety importance of systems interactions is discussed further in Section 5.3.

5 GENERAL GUIDELINES FOR PERFORMING A SYSTEMS INTERACTION ANALYSIS

This section defines the general guidelines that the utility should observe in performing the ~~pilot~~ initial systems interaction analysis. A Systems interaction analysis is a three-step process: (1) the selection of the combination of systems for detailed analysis, (2) the search for adverse systems interactions, and (3) the assessment of the identified systems interactions. Additionally, this section describes the potential usefulness of simulation. Specific procedures that the utility may want to consider in performing the analysis are given in the appendices.

The systems interaction analysis is aimed at the identification of those couplings between systems which will lead to an adverse system interaction when the necessary initiating failure occurs. As described in Section 4.2, the existence of those couplings (a hazard) constitutes a latent adverse systems interaction.

Thus, the following sections provide guidelines for identifying those couplings which are the basis for latent adverse system interactions. While the sections are organized by type of coupling, i.e., functional, spatial, and human, it is important to maintain an overall perspective on the search 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 of the design by modeling it is a prerequisite to the search for systems interactions. The search for spatial or human couplings cannot proceed without this basic understanding of the plant's systems.

5.1 Guidelines for the Selection of the Combinations of Systems for Detailed Evaluation

To proceed with this first step, the combinations of systems most important to the systems safety actions must be systematically separated from among all the plant's systems. The plant's functional couplings (intersystems dependencies) must be evaluated to grade their relative importance among the plant's systems. The most important systems should be those selected to begin Step 2 (5.1.2).

The first step in the identification of functional couplings is the modeling of the physical connections among the plant systems. This step is essentially the same as that in a reliability or risk assessment. ~~(Results from such an assessment, preferably plant-specific, would facilitate this step and should be employed if available.)~~ A systematic approach should be taken in this first step. The plant is too complex and the relationships are too subtle for the analyst to evaluate without the assistance of systems modeling techniques.

Reliability and risk assessments are of interest since they highlight specific combinations of systems failures that have particularly high consequences or probabilities. When identifying dominant accident sequences (combinations of systems failures), the plant modelling aspect of a risk assessment might be useful in the systems interaction analysis.

However, care should be taken lest too much significance be attached to a few dominant accident sequences. In risk assessments performed to date, the dominant accident sequences owe their significance to the large consequences associated with them. They are not the most probable core melt sequences. The PRAs conducted to date indicate that a small number of sequences tend to dominate the accident risk for any given plant design. Since there can be a large number of other accident sequences of lower risk significance but higher probability, a small number of dominant sequences may not give much insight into the plant's weaknesses that could lead to severe accidents. To the extent that the dominant accident sequences represent potential vulnerabilities in the plant, they should be utilized during the search for functional couplings. But the analysis also should include consideration of other than the dominant sequences.

The final selection of the combinations of systems for detailed analysis, at the completion of Step 1, must be congruent with past LWR experience. Thus, professional judgment based upon operating experience could modify the final selection of the systems upon which detailed analyses will be performed.

One way to select the combinations of the systems for detailed analysis is to utilize distinctions between safety-grade and nonsafety-grade systems. Almost all the systems in an LWR are given detailed considerations by the designers during the design and installation processes. However, past licensing reviews of LWRs led to an emphasis on safety-grade systems. The less-than-obvious functional couplings are expected to lie in nonsafety-grade support systems. Much more attention has been given to the front-line and safety-grade systems such that fewer functional couplings of concern are expected to be found in these systems. 5

Initially, we performed the Diablo Canyon program~~[16]~~ [5] by searching for common-cause failures originating in nonsafety-grade systems resulting from a seismic event. It should be clear that this extension of safety reviews into nonsafety-grade systems extended past licensing practice in the performance of 10 CFR safety reviews. However, the methods being developed will not be restricted by the distinction between safety-grade and nonsafety-grade systems.

5.2 Guidelines for the Search for Systems Interactions

Step 2 in the process is to perform a detailed review of those systems that were graded as most important to safety from Step 1 (5.1.1). The main objective of the entire review process is to identify those systems interactions that jeopardize the independence of redundant trains of systems performing the systems safety actions.

5.2.1 The Search for Functionall} Coupled Systems Interactions

This section provides the guidelines for the search for functionally coupled, spatially coupled, and humanly coupled systems interactions. The use of simulation is also discussed as it could be used to identify systems interactions in selected systems.

To perform such a search, the analysts will need to proceed through multiple tiers of dependencies into the details of subsystems to the component* level. The analysts should now proceed to model the functional couplings of the selected systems in more detail. The level of detail should be limited to the highest level at which a specific functional coupling is first ~~modeled~~ discovered. Once this functional coupling has been identified, the systems interaction should be characterized to complete this step in the review process.

To characterize the systems interaction the following should be included:

1. The random failure that will initiate the systems interaction scenario.

2. The type of coupling (electrical, hydraulic, pneumatic, mechanical, structural) that compromised the intended independence of systems.

3. The systems that were combined by the coupling.

4. A brief summary of the systems interaction scenario including the cascade paths that will result from the functional couplings, the systems affected by the scenario, and the operational mode of the plant.

5. The systems safety consequences of the scenario including the degree of impairment of front-line systems.

An itemization of the information to be reported to the NRC staff review is given in Section 6.0.

*A component is a basic element of the system. For systems interaction reviews the component level is the level of resolution of the system description or analysis.

At times the analysts will proceed with the detailed modeling of the functional couplings of the selected combinations of systems to the point where there is confidence that no functional coupling exists. The analysts will terminate the modeling of the functional couplings and provide a brief justification for this judgment. It remains that such systems will be evaluated for both humanly and spatially coupled systems interactions.

5.2.2 The Search for Spatially Coupled Systems Interactions

The initiating events that are a part of spatially coupled systems interactions are extreme conditions, e.g., earthquakes, fires, floods, pipe breaks. When the spatial domain of an initiating event is larger than the distance between components from different systems, then the conditions for a primary spatial coupling exist. When the response of a component directly affected by the initiating event has a spatial domain that envelopes another component in a different system, then the conditions for a secondary spatial coupling exist. The guidelines for identifying spatially coupled systems interactions that are presented in this section address both primary and secondary couplings.

Generally, the identification is based upon a review of plant arrangements by performing a systematic visual inspection of the plant. To the extent that they exist, prior studies should be employed to facilitate this visual inspection. Plant-specific studies, such as seismic, environmental qualification, and fire reviews serve as improved starting points. Some architect-engineering firms have computer programs defining the locations of all components in a plant and such lists could substantially aid the preparations for the visual inspection. The components location from all systems important to the systems safety actions should be indicated. Additionally, the components locations of those systems previously combined with other systems because of functional couplings should be indicated. The indicated locations should be the areas for particular attention during the actual visual inspection.

The actual visual inspection must use a multidisciplinary team of experts to provide joint, immediate judgement on (1) whether the spatial coupling appears to meet the definition of an adverse systems interaction, and (2) to provide

Table 5.1 Extreme Conditions (Generic Causes of Spatially Coupled Failures)

Extreme Condition (Generic Cause)		Example of Source	Spatial Coupling
1.	Corrosion or other chemical reactor	Acid, water, or chemical agent attack	Shared location, pneumatic, hydraulic
2.	Moisture	Condensation, pipe rupture, rainwater, floods	Shared location, pneumatic, hydraulic
3.	Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances, crystallized boric acid from control system	Shared location, pneumatic, hydraulic
4.	Impact	Pipe whip, water hammer, missiles, structural failure, earthquakes	Shared location, hydraulic structural mechanical
5.	Vibration	Machinery in motion, earthquake	Structural mechanical
6.	Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuits	Shared location, pneumatic, hydraulic, mechanical
7.	Electromagnetic interference	Welding equipment, rotating electrical machinery, lightning power supplies, transmission lines	Electrical (inductive)
8.	Electronically conductive medium	Conductive gases	Shared location, pneumatic
9.	Pressure	Explosion, out-of-tolerance system changes (pump overspeed), flow blockage	Shared location, pneumatic, hydraulic mechanical
10.	Radiation	Neutron sources and charged particle radiation	Radiation

the initial importance ranking of the adverse systems interactions. The first purpose is the vital step in searcn for spatially coupled interactions since it provides for a focus on the creative "what if" questions. The multidisciplinary team inspection provides the rationale upon which specific combinations of faults in nonconnected systems can be based.

Spatially coupled interactions are due to the existence of extreme conditions that simultaneously affect more than one system. Table 5.1 provides a list of extreme conditions that can affect more than one system along with examples of sources of such conditions and the spatial couplings through which they propagate.

The actual visual inspection should produce a list of spatially coupled systems interactions. The following records are needed to complete the evaluation of each interaction.

1. The plant location at which the spatial coupling was identified.

2. The initiating event.

3. The type of extreme condition that caused the first failures, e.g., impact, temperature, moisture, pressure, radiation.

4. The type of spatial response of the first failure that affected a different system, if a secondary spatial coupling is identified, e.g., vibration, impact, moisture, pressure, corrosion, spurious current.

5. The systems that were combined by the spatial coupling.

6. A brief summary of the systems interaction scenario including the cascade paths that will result from the initiating event, the systems affected by the scenario, and the operational mode of the plant.

7. The systems safety consequences of the scenario including the degree of impairment of front-line systems.

Again, an itemization of the information to be reported to the NRC is given in Section 6.0.

5.2.3 The Search for Humanly Coupled Systems Interactions

Significant systems interactions can be coupled by reactor operators. Some latent human errors (as noted in Section 4.2) due to improperly written procedures or inadequate training can be the common cause in an adverse systems interaction. However, our reviews are not expected to concentrate on these types of human couplings; rather, we rely upon the Division of Human Factors to identify and evaluate written operating procedures and operator training.

Our ~~reviews~~ analyses concerning human couplings will concentrate on systematically searching for potential dynamic human errors that are part of the dependent effects in a systems interaction scenario. These are the types of human couplings that propagate some initiating failure across systems that should have remained independent. We want to predict only those human errors where the operator's actions are motivated by the plant's response to a failure. The best examples are from the machine-to-man transmission interface (the displays). Thus, we will treat the operator as a secondary coupling, i.e., the operator has the potential to be induced to connect systems that are normally independent.

A systems interaction anslysis is necessarily constrained to search only for those plant conditions for which a unique cause-effect relationship can be determined. Thus, the reactor operator is assumed to fastidiously follow procedures and the procedures are assumed to be correct. Based on these simplifying assumptions, the human couplings for a system interaction analysis are defined by the normal operating and emergency operating procedures. We expect that the emergency operating procedures appear more likely to induce those human couplings that will lead to an adverse systems interactions.

Typically an indicating symptom from an abnormal condition triggers the operator to take actions by procedure involving other systems. A false indication could induce operator action (a human coupling) that leads to an adverse systems interaction. Even if two or more indicators are required for operator action, one failure (e.g., instrument power, low voltage) could cause both the triggering and the corroborating indication.

We recognize the significant differences among emergency procedures at the various plants. Some utilities use event-oriented procedures where operators make an initial diagnosis of the event taking place and select the emergency procedure to use for the event. Other utilities use symptom-oriented procedures where the procedure is based on the nature of the indications received by the operator; no diagnosis of the specific event is required. Both the industry (via the Institute for Nuclear Power Operations) and the NRC are developing guidelines for standardizing emergency procedures based on a symptom orientation.

On the other hand, the abnormal condition could be valid but a failure in the indicators the operator uses to corroborate the condition could fail leading to an adverse systems interaction. For example, PWR pressurizer level instrument could give the appearance of an adequate level when, in fact, further action was required to establish the proper reactor level.

Specifically, a utility should utilize the following procedure in searching for human couplings during this initial analysis:

1. All emergency procedures should be reviewed to select those procedures applicable to the scope of this initial an~~s~~alysis. The rationale for discarding any procedure at this stage should be noted.

2. All normal operating procedures should be reviewed to select those applicable to the scope of this initial analysis*

*It is not anticipated that normal operating procedures will be a significant source for future SI reviews. This step is included in the initial analysis to test that hypothesis.

3. Each procedure selected for further analysis should be reviewed then to identify each indication that induces an operator action on a system other than the indication-generating system. The identification should include definition of the specific alarms, displays, instruments or other initiating indications and the corroborating indications required for each of the operator actions.

4. Each indication should be analyzed to determine both whether the initiating indication and the corroborating indication share a common dependency and whether the initiating indication and the emergency condition share a common dependency.*

At the conclusion of the search for humanly coupled systems interactions, those identified should be characterized by the following features:

1. The random nonhuman failure that will initiate the systems interactions.

2. The operator actions that ~~would~~ will adversely couple otherwise independent systems or adversely intervene in otherwise desired systems interactions.

3. The systems that were combined adversely by the operator actions.

4. A brief summary of the systems interaction scenario including the cascade paths that will result from the functional couplings (nonhuman), the systems affected by the scenario, and the operational mode of the plant.

5. The procedures that will lead the operator to act as a coupling.

*Note that the operator is assumed to act according to procedure and the procedure itself is correct. By this assumption, if the instrumentation and other components involved in the procedure function properly, the human coupling can only be a beneficial or mitigating link in a systems interaction. Therefore, for a systems interaction analysis, only human couplings involving instrumentation, component, or other "nonhuman" problems are of interest.

6. The functional safety consequences of the scenario including the degree of impairment of the front-line systems and the safety functions served.

5.2.4 The Use of Existing Simulators

It appears that control room simulators have been underutilized in the search for machine-to-man adverse systems interactions (specifically, those systems interactions initiated by control systems malfunctions or by power supply failures). A control room simulator is ~~a~~ control panels ~~which~~ That duplicate~~s~~ all the switches, controllers, instruments, recorders, annunciators, of a nuclear power plant. The only difference between the plant's main control room panels and the control room simulator panels is that the panel components are driven by computers instead of the plant. In the simulator's computer, all the plant systems that have direct interfaces with the control room have been modeled sufficiently to represent most normal, many transient, and some accident conditions of the plant. The mathematical modeling of systems includes the plant's functional couplings, operator controls, and displays. The details of the control and protection systems logic that were developed using ~~fault trees and success trees~~ Boolean algebra already exists in the simulator. Fluid systems and core physics have also been modeled to represent intrasystem behavior.

~~It appears that~~ Control room simulators have ~~are~~ not been ~~being~~ used to search for adverse systems interactions that combine both functional and human couplings. Simulators might be used ~~This can be accomplished~~ by simulating an initiating failure and looking for the resultant impairment of systems important to the basic safety functions including the possible corrective actions. The most frequently observed failures identified from an ongoing reliability program and operating experience feedback could be selected as the initiating failure at the simulator.

The advantage of the simulator in systems interaction analysis is that it allows the immediate observation of the effects of failures by monitoring key parameters and setpoints. Thus, it seems that this might very well be the equivalent of "evaluating" large groups of cut-sets by simply monitoring the parameters-of-interest (e.g., safety system setpoints) without giving attention to individual cut-sets one at a time. A unique advantage of the simulator is that the plant response can be studied at speeds other than real time.

There are some limitations to the use of existing simulators to search for systems interactions. The type of simulator needed for a systems interactions analysis is one in which the interconnections among plant systems are simulated extensively and accurately. In other words, an "engineering" type simulator would be more suitable than a purely "training" type simulator in which known plant response is preprogrammed and simply played back to the trainee. The benefit of the "training" type simulator is in the mind of the trainee (which is not easy for us to search). Also, existing simulators do not simulate some "nonsafety" systems of interest to systems interactions analyses. Finally, control panel support hardware such as switches, breakers, relays, and instruments have not been simulated even though they are essential to the realistic simulation of control system and power supply failures.

At the present time, control room simulators seem to have a potential to search for systems interactions resulting from power supply failures, control system malfunctions, and the loss of panel displays. The extent of interface modeling determines the extent to which the simulator is useful in the search for intersystem dependencies because it determines the accuracy of the plant response to an initiating failure. Also, to be totally useful, some special provision for introducing failures in an isolated manner will be necessary in addition to the existing list of preprogrammed malfunctions and their effects. Such a provision should include the facility to set the simulated variable to a desired value for some period.

5.3 Guidelines for Assessing the Identified Systems Interactions

~~Furthermore,~~ The NRC will not require corrective action for ~~identified~~ discovered adverse system interactions unless it is needed under existing NRC requirements. At a minimum, an assessment will have to be made to the extent required to assure compliance with current regulatory requirements. The utility may choose on their own to take corrective actions based on this initial analysis to improve plant performance and system safety.

Adverse systems interactions are already important simply because of the failure of a systems safety criterion (Section 4.1). Yet the failure of a systems safety criterion covers a range of importance because each criterion allows a range of system impairments. The systems safety criteria were chosen from a conservative perspective to guide the search of a plant ~~to identify~~ for systems interactions.

In the past, the ranking of safety issues has been needed because corrective actions at plants continued to reflect a balance between maximum safety and other contravening purposes. Thus, we expect that future corrective actions on identified systems interactions will be graded by their safety significance for both any interim patch and the final fix. The most systematic means of grading relative safety significance is built upon the notion of risk. Formal PRAs constitute only one specific application of the risk notion. Less formal applications may be acceptable that emphasize features such as (a) the number of ~~functions~~ actions lost, (b) the degree of degradation of a ~~basic~~ systems safety ~~function~~ action, and (c) the urgency for human amelioration. However, any risk-based assessment is not complete by itself and is normally modified by legal constraints and obligations among ~~interfacing~~ responcible organizations.

6 GUIDELINES FOR REVIEWING PROGRAM RESULTS

The initial analyses will provide the experiential basis upon which the NRC can both (1) complete considerations for the issuance of a requirement that all LWRs perform a separate analysis ~~evaluation~~ for systems interactions, and (2) demonstrate the feasibility of the guidance on a limited scope. To achieve this, the utility must report its results and provide its recommendations concerning a broadly scoped application of the initial guidance. This section describes the needed report from the utility and discusses the staff's intended use of the reported information.

6.1 Guidelines for the Utility Report

Those adverse systems interactions discovered ~~identified~~ by a utility that require action under current NRC regulations will be processed by existing NRC procedures (10 CFR 21). Note that these systems interactions along with recommended corrective actions should have been reported to the NRC through normal channels at the time they were first discovered. The utility's final report must include these systems interactions only to provide a complete description of all the adverse systems interactions discovered ~~identified~~. No separate action should be required by the NRC. As stated previously, the NRC will not require action on any systems interaction unless it is already required by existing regulatory ~~regulations~~ requirements.

The type of information needed for an adequate evaluation of the feasibility of the initial guidance is centered around those adverse systems interactions that were identified. Specifically, the utility should report:

1. The engineering characterizations, as previously itemized for each adverse systems interaction that is functionally coupled (5.2.1), spatially coupled (5.2.2), and humanly coupled (5.2.3).

2. A discussion of the search process and the assessment criteria used by the utility to rank the systems interactions or groups of interactions by their relative importance to safety.

3. A brief description of those systems interactions resolved because they would exceed current NRC requirements. Also, the resolution should be described.

4. A brief description of those systems interactions resolved because the utility judged the resolution beneficial. The basis for the judgment should be included if it were not already described as part of item 2 above. Also, the resolution should be described.

5. The coordination with other ongoing programs that occurred during the search, the ranking, and any resolution should be described. The description should specify the redundant or the supplemental nature of the coordination between another ongoing program and the systems interaction analysis.

The type of information to complete the NRC considerations of the need for a requirement that all LWRs perform a separate systems interaction ~~review~~ analysis is centered around the efficacy of these initial analyses. Thus, we look for the utility to report:

1. Alternative methodologies and techniques that comply with the general guidelines of Section 5.1 but differ from the illustrative procedures of Appendices C and D. The staff considers the dependency matrix-directional graph based technique described in Appendix D to have the potential to more efficiently perform the steps described in 5.1 and 5.3.

   An alternative might be founded ~~more substantially~~ upon the use of simulation as discussed in Section 5.4, or upon evaluations of operating experience. The description of the alternative methodology should be sufficiently complete to demonstrate its feasibility. The completeness needed is reflected in the level of detail required for the feasibility objective of the pilot effort as listed above. This level of detailed information will be needed even where the utility considers their ongoing programs the ~~adequate~~ alternative methodology.

2. The overall scope of the analysis including fiscal resources, duration, and the timing of the review during the plant's life cycle.

3. Any other category of comments that address the need for a requirement for a separate systems interaction analysis.

6.2 Guidelines for the NRC Review

The NRC will prepare a final report on the utility program that summarizes the results and recommendations made by the utilities and synthesizing these findings into an overall summary and conclusions concerning systems interaction analyses. This report should be reviewed with the utilities involved prior to final issoance.

The report will address the content of both the analyses and and the utility's report from the perspective of the need for a separate requirement for adverse systems interactions analyses. Specifically, the report would address:

1. The adequacy of the scope of the analysis.

2. The adequacy of the criteria used for both searching and importance ranking of adverse systems interactions. This would include a contrast of these criteria against current criteria like the single failure criterion and the acceptance criteria of related SRP sections (NUREG-0800).

3. The impact that a separate requirement would have on an overall reliability assessment of the plant.

Finally, the NRC will develop a final regulatory position, as appropriate, for separate systems interaction analyses utilizing the experiences and recommendations of the utilities involved in this program. If a requirement is deemed necessary, these guidelines will be prepared and issued following standard NRC procedures, including allowance for public comment. Prior to the public comment stage, the draft guidelines should be reviewed with the utilities involved in this program.

7 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.

4. I. Papazoglou, Brookhaven National Laboratory, "Contribution to the Initial Guidance for the Performance of Systems Interactions Reviews," USNRC REPORT NUREG/CR-____, 1982.

5. U.S. Nuclear Regulatory Commission, "Safety Evaluation Report Related to the Operation of Diablo Canyon Nuclear Power Plant, Units 1 and 2," USNRC Report NUREG-0695, Supplement 11, October 1980.

6. Memorandum from H. Denton, NRR, to R. Fraley, ACRS, Subject: Seismic-Induced and Other Interactions Between Non-safety and Safety Systems," November 20, 1981.

APPENDIX A

SYSTEM INTERACTION INFORMATION
DOCUMENTS AND ACTIVITIES

Documents

1. System manuals for all front-line systems and support system: these include all the equipment details about structural support, lubrication, and cooling. Also it should include all the operating modes and setpoints.

2. Systems flow diagram: it includes ~~all~~ the information on functional couplings with other systems.

3. P&IDs: this is applicable to both front-line and support systems.

4. Electrical drawings: these include details of ~~all~~ buses (vital and nonvital) motor control centers, distribution panels, raceway and conduit drawings, interlocks between circuit breakers.

5. I&C drawings: these include details of instrumentation, wiring diagram for ~~all~~ equipment, and shutdown logic.

6. Plant procedural manuals: these include plant testing, maintenance, normal operations, and emergency procedures.

7. Selected topical and plant-specific reports: these include specific topics such as pipe break effects, fire hazards, loss of offsite power, loss of ultimate heat sink, computer code user's manuals (e.g., GO, SETS, BACFIRE and specific reports such as plant startup reports, preoperational programs, probabilistic risk assessment reports, and reliability assessment reports).

8. Plant operator training manuals.

9. Facility hazard characteristics: these include high seismic zone, frequent tornados, and chemical facility interfaces.

10. Final Safety Analysis Report.

Activities

1. Facility visual inspections: this is a kind of activity where a team consisting of members from appropriate disciplines perform the walkdowns of systems and walk-throughs of various compartments and buildings and identify spatial couplings between systems.

2. Review of LERs: this includes review of all Licensee Event Reports for a specific or a similar facility. Emphasis on the review of LERs on power supply failure and instrumentation and control systems malfunctions.

3. Plant operator interviews.

4. Topical meetings.

5. Review of Operating Reactor Experience of a specific or similar facility.

Special Items

1. Engineering analyser/control room simulator: in order to effectively use an analysis or a simulator to identify systems interactions, the extent and accuracy of modeling of both front-line and support systems must be adequate. Particularly, the extent of interface modeling determines the usefulness of the present simulators to identify the intersystem dependencies and thus predict accurately the plant response to initiating malfunctions.

APPENDIX B

SUMMARY SHEET OF EXAMPLE SYSTEMS INTERACTION EVENT

Event Title: Primary Coolant Discharge to Containment

Date of Event: February 26, 1980

Plant: Crystal River Unit 3

Date of Latest Entry: August 12, 1980

Reference Documents

1. NUREG-0667, "Transient Response to Babcock & Wilcox - Designed Reactors," May 1980.

2. NSAC-3/INPO-1, "Analysis and Evaluation of Crystal River - Unit 3 Incident," March 1980.

3. Memorandum from K. R. Wichman (ORAB) to R. W. Reid (ORB #4), "Crystal River - 3: Evaluation of Proposed Corrective Actions Subsequent to February 26, 1980, Incident (TAC 12961)," dated July 2, 1980.

4. Letter from J. A. Hancock, Florida Power Corp., to H. R. Denton, NRC, dated March 12, 1980, Subject: "Crystal River Unit 3, Docket No. 50-302, Operating License No. DPR-72."

5. Letter from J. P. O'Reilly, NRC, to Florida Power Corp., dated March 28, 1980.

Safety Significance

1. Type of Event: Transient-induced LOCA.

2. Criteria Penetrated: Uncontrolled loss of primary coolant.

Description of Event

1. Systems Design

Crystal River Unit 3 is a B&W-designed NSSS with OTSGs. This design leaves the primary system very sensitive to perturbations in the secondary system. To accommodate the sensitivity, the Integrated Control System (ICS) uses a complex feed-forward system to control the reactor, the feedwater controls, and the turbine controls. The Non-Nuclear Instrumentation (NNI) systems provide input values of process parameters to the ICS. Additionally, the NNI provides indications of plant variables to the main control board and provides control signals to other plant actions including PORV operation. Once opened, the PORV controller holds the PORV open over a 70 psi range.

2. Root Cause

The primary system interaction hazard leading to this event was the functional dependencies of the ICS input, the PORV position, the instruments used for manual control, and the entire NNI-X power supply upon one +24 VDC line within the NNI-X power supply. Additional systems interaction hazards are (a) the functional dependencies of the reactor power, the turbine CV position, and the FW controller upon the ICS, and (b) the dependence of the NNI-Y indicators upon the NNI-X power supply.

The initiator for this adverse systems interaction was the loss of the +24 VDC within the NNI-X power supply. Three intrasystems deficiencies led to this system interaction initiator. First, less than adequate procedures existed for installing buffer subassemblies into the power monitor modules after surveillance testing. Second, less than adequate QA procedures failed to detect an improperly installed subassembly. Third, the improper installation 2 weeks earlier shorted one +24 VDC supply line to ground and resulted in damaging the printed circuit wiring of the module.

3. Pertinent Scenario

The known scenario considered pertinent to systems interaction concerns is tabulated beginning with the systems interaction initiator and ending with the worst consequence attained during the accident. The attached cause-effect chart shows the relationship of the events.

t=0: One +24 VDC supply line of the NNI-X system was lost causing the control circuit to open and hold open the PORV, and the start of a 1/2-second timer that delays tripping the entire NNI-X power supply. Simultaneously NNI began supplying spurious inputs to the ICS.

t=1/2 second: The timer delay was satisfied permitting the protective monitor to trip the entire NNI-X power supply. The total loss of the NNI-X increased the number of erroneous inputs to the ICS resulting in a slight opening of the turbine CV, a slight increase in reactor power, and a significant decrease in feedwater flow. The total loss of the NNI-X eliminated the ability to signal closure of the PORVs. Thus, the PORVs opened and remained open. The total loss of the NNI-X affected over half of the NNI-Y instrument on the main board because of dependence upon NNI-X inputs for signal conditioning, compensations, buffer amplification, and readouts. About 80% of the instruments used for manual control displayed erroneous readouts.

t=25 seconds: The undercooling transient occurred from the combination of decreased feedwater flow and increased reactor power. The reactor scrammed on high reactor pressure.

t=3-1/2 minutes: The combination of reactor scram and stuck open PORVs depressurized the reactor to well below the safety injection setpoint for HPI. The HPI system started.

About this time the drain tank disk ruptured and primary coolant was dumped into the containment ~~from~~ via the PORVs.

t=10 minutes: The code safety valves opened as the primary system went water-solid. Primary coolant and borated HPI coolant were dumped into the containment from the Code safety valves. (Since most of his instruments were erroneous, and consistent with TMI-2 B&Os advice, the operator chose not to stop the HPI.)

4. Stable Condition Attained

From the worst consequences attained during this accident the overall plant was brought to a stable condition by the following actions. The operator closed the PORV block valves to stop the LOCA through the PORVs. An instrument technician restored the NNI-X power supply and the operators then followed emergency procedures to bring the plant to normal hot shutdown. While attaining a stable condition one OTSG was dryed out and the feedwater was isolated.

Analysis of Event

The intent of this section is to explore what criteria could have been penetrated in the light of what criteria were penetrated during the accident. Since there was an uncontrolled loss of coolant to the containment along with a release of some radioactivity to the environment prior to closure of the purge valves, any additional malfunction would have significantly increased the likelihood of a serious accident.

Because the conditions of the event did not include a degradation of the automatic functioning of the ESF and RPS, I judge it unlikely that the containment would have been breached by an additional failure in the ESFs or RPSs.

Following TMI-2, emphasis was placed upon operating procedures that could allow bypassing the containment, e.g., continued pumping from containment sump to auxiliary building. Although the containment vents were initially open they automatically closed on high containment pressure. The operator immediately verified containment isolation per procedures. Thus, I judge it unlikely that the containment would have been bypassed by inattention to procedures.

However, I judge the likelihood to be significantly high that inappropriate operator action across systems could have exacerbated the accident. The operator did not know which instruments on the main control board were accurate. For example, one operator was following procedures by balancing HPI flow between the loops while he was unaware that one flow indicator had failed in the mid-scale position. Thus, the real potential existed for the operators to take inappropriate action affecting more than one system because of erroneous readouts in the main board.

Actions Taken

The licensee has proposed and taken many actions to preclude recurrence of many of the adverse consequences experienced during the event of February 26, 1980. A safety evaluation was prepared for issuance concerning the proposed actions. Some of the actions are pertinent to the adverse systems interactions experienced during the event.

Regarding the loss of operator information, the licensee proposed to install two new, electrically separate channels of indications for 23 key plant variables. Each channel will be uniquely dependent upon either the NNI-X or NNI-Y power supply. Additionally, an indicator light will be used to identify the operable NNI system. The new systems will meet the single failure criterion.

Regarding the erroneous opening of the PORVs, the licensee proposed to add an interlock, independent of the NNI power monitor module, to preclude automatically opening a PORV upon loss of either the +24 or -24 VDC.

Regarding the plant upset due to the ICS, the B&W Reactor Transient Response Task Force (Ref. 1) recommended (Recommendation 2.2(5)(d)) that the ICS should have provisions for detecting failures and taking defensive action to preclude substantial plant upsets whenever a control system or input signal fails. One defensive action suggested was reverting to manual control. By "plant upsets" the Task Force meant an occurrence requiring action by ESFs or code safety valves.

Disposition

All of the adverse systems interaction hazards identified by the investigations of the Crystal River Unit 3 accident appear to have been identified and corrective actions proposed. Given that the proposed corrective actions are implemented on all B&W NSSS plants and designs, no further action is necessary by the Systems Interaction Branch.

Figure 1 Systems Interaction Aspects of Crystal River-3 Accident on February 26, 1980

Figure 2 24VDC Power Supply and Monitor for NNI-X

Figure 3 PORV Controller

APPENDIX C

AN ILLUSTRATIVE PROCEDURE (EVENT TREE/FAULT TREE)

The guidelines discussed in Chapter 5 define the ingredients for an initial analysis for systems interactions. They were general in nature to encourage specific improvements by the utilities performing the initial analysis. However, the staff endorses the specific procedure described in this appendix as consistent with the more general guidelines and illustrative of the intent of the guidelines given in Chapter 5.

The proposed procedure for identifying important system interactions is a combination of existing methods, including methods proceeding in time from cause to effect as in Failure Modes and Effects Analysis and methods regressing in time from effect to cause as in Fault Tree Analysis. This illustrative procedure is based on a synthesis of the Event Tree/Fault Tree methods, where information from Failure Modes and Effects Analysis, visual inspections, and the feedback of operating history experience are used to assist in the complete construction of the Event Trees and the Fault Trees.

More specifically, the procedure can be distinguished into the three steps described in Chapter 5.

1. Selection of the combinations of systems for detailed evaluation (see 5.1).

2. The search for system interactions (see 5.2).

3. Assessing the identified system interactions (see 5.3).

Each of these steps can be divided into further steps as described in this appendix. This illustrative procedure is similar to the initial steps used in a Probabilistic Risk Assessment or a Reliability Assessment. The detailed steps of the procedure need not be executed in exact sequence within the three major steps; instead, there exists a parallel/feedback relationship. The emphasis is upon the deterministic modeling of the plant by the Event Tree/Fault Tree courses of reasoning. Quantitative analysis using probability is not necessary to accomplish the primary objective of the search for systems interactions.

This section is organized as follows. Section A.1. describes the selection of the combinations of systems for detailed evaluation. Section A.2. gives the procedure for systematically searching for interactions among the identified systems. Section A.3. presents a method to assess the identified system interactions.

The procedure described throughout Appendix C has been separately described in more detail in reference 4. The reference includes the classification of accidents by the mitigations required, the list of accident initiators for PWRs, examples of PWR functional event trees, the assignment of FLS and support systems to safety functions in a PWR, example dependency tables, and examples of systemic event trees.

A.1 Selection of the Combinations of Systems for Detailed Evaluation

The first major step of the procedure results in the selection ~~identification~~ of systems among which a system interaction potentially exists. This selection ~~identification~~ is not a mere listing of these systems, but includes a modeling of their operating modes as well as the system interactions that result from functional couplings.

The first major step of the review can be accomplished by the following five steps.

Step 1 Familiarization with Plant Design and Operating History

In this step, the analysts gather pertinent information about the plant and establishes lines of communication with the designers and operators who are more able to answer specific questions.

Step 2 Development of Functional Event Trees

The four ~~basic~~ systems safety actions (Section 4.1) are analyzed into subactions to generate the functional Event Trees.

The functional Event Trees can be kept generic in nature by reactor type (PWR and BWR).

Step 3 Assignment of Systems to the Event Trees

The safety actions identified in the functional Event Trees are performed by engineered systems designed specifically for ~~this~~ the purpose. The operations of these systems completely determine the course of an abnormal event. These systems are called front-line systems (FLS). Once the actions of the functional event trees are replaced by the front-line systems, the resulting event trees are called systemic event trees.

To successfully perform their function, the front-line systems depend on the output of support systems. Support systems affect the response of a plant only through their effect on the FLS.

To identify the support systems for each front-line system, the following ~~systems~~ substeps can be followed:

Substep 3.1 The operation of the front-line system is searched in detail, identifying all the necessary inputs as well as all of its outputs. If, for example, the FLS is a fluid system, all potential sources of the fluid should be identified. All the systems with which the FLS interact directly (as discharge points) or indirectly (as secondary sides of heat exchangers) should be identified.

Substep 3.2. The power sources necessary for the operation of the active components, e.g., electric power and steam, should be identified.

Substep 3.3. The modes of controlling the system must be identified, in particular, whether the system is controlled automatically or by operator action. In both cases the indications necessary to initiate control system or operator action must be identified. The possiblity of manual overriding of automatic control should also be considered. In the case of automatic control, the type of the controlling system should be identified (e.g., electrical, pneumatic) along with the systems associated with each type (e.g., power supply, instrument air).

Substep 3.4. The cooling systems of the various components of the FLS should be identified.

Substep 3.5. The lubrication systems (if any) of the various components of the FLS should be identified.

Substep 3.6. The location and structural dependence of the FLS should be established.

The identification of the support systems that contribute to the initiating event is described in Step 5.

Step 4 Development of "Systemic Event Trees"

The use of Systemic Event Trees simplifies the search for system interactions in two important ways. First, Systemic Event Trees provide a systematic way for eliminating combinations of system that are immaterial for the abnormal sequence under analysis. Second, Systemic Event Trees collate accident sequences with their consequences. Thus, they provide the necessary framework for the assessment of the identified system interactions.

Another type of simplification results from the combination of abnormal sequences (tree paths) that lead to the same consequences. The abnormal scenarios that are equivalent with respect to their consequences can be combined by Boolean algebra. The simplification reduces the number of combinations of systems that need to be searched for system interactions.

Step 5 Develop Fault Trees for the Initiating Event

This step identifies the systems and associated failures that would precede the initiating event. A coupling between such systems or associated failures and the Front-Line Systems and their support systems constitutes a system interaction. For example, a breach of the primary pressure boundary is a LOCA initiator; at the same time, however, it can flood a certain area impairing one or more FLS or SS. Another example, short circuit might create a power failure that will initiate a transient; at the same time it can start a fire that would affect other systems. Also, an earthquake might cause the failure of water storage tank generating a local flood.

For each initiating event, all effects should be identified and a list of the effects compiled. Later, this list will be compared to a list of failure causes for front-line and support systems in the search for hidden dependencies.

A.2 The Search for System Interactions

A.2.1 General Description of the Second Major Step

The second major step of the procedure contains the steps necessary to search for interactions among the combinations of systems selected in the first major step.

In the second major step, the systems will be modelled in more detail by Fault Trees. The smallest combinations of component failures will be generated (minimal cut sets), and a search for an interaction will be performed for the minimal cut sets. It is more efficient to proceed by successively resolving the systems into finer and finer detail by first searching for interactions at a system level, then proceeding to a redundant train level, next to a subsystem level, and finally to a component level. A system interaction uncovered at a general level preempts further analysis at this time of the systems involved in that interaction. However, a potential problem with this procedure is that certain failure modes of a system that adversely influence other systems cannot be identified before a Failure Modes and Effects Analysis (FMEA) at the subsystem or the component level is completed. The impact of this problem will be assessed during the actual application of the procedure in the initial analyses.

A.2.2 The Steps of Major Step 2

The search for systems interactions can be divided into the following steps. It should be emphasized that there exists a feedback relationship among these steps.

Step 6 Perform Cascade Failure Analysis

The purpose of this analysis is to determine the different failure modes of the combinations of systems selected from major step 1 and the influences of these modes on other systems. The failure modes, the causative factor(s), the effects of the failure on other systems, and the resulting indications available to the operator should be documented. The failure modes of the system need not be limited to total failures (e.g., partial failures corresponding to degraded or excessive operation may be included). To determine the influence on other systems, the dependencies modelled in Step 3 should be used. It should be emphasized, however, that the search for possible influences of a certain system's failure need not be limited to the systems with which the failure is associated through the dependency modelling. In assessing the indications available to the operator for a system failure, special care should be given to whether the provided indication is sufficient to unambiguously specify the particular failure mode of the system. A special note should be made if one type of indication covers several failure modes.

The column of operators' indications should be searched for indications from different failure modes of the system. A special note should be made when such cases are identified.

Step 7 Develop the System Fault-Trees

Each front-line system associated with an abnormal sequence on the Systemic Event Trees (determined in Step 4) defines the top event for the Systemic Fault

Tree. Initially, these top events should be developed to the point where local faults are distinguished from the support system faults identified in the cascade failure analysis of Step 6. Other support system faults form the top events for the support System Fault Trees. The development of the Fault Trees will proceed in levels as was mentioned in Section A.1.

Step 8 Generate Minimal Cut Sets

Using the information obtained from the cascade failure analysis (Step 6), the Systemic Event Trees (Step 4) are reexamined to eliminate immaterial ~~abnormal~~ sequences. Next, each ~~abnormal~~ sequence is characterized by the consequences in which it will result if realized (see Step 4).

This reduced number of combinations of systems based upon the improved description of ~~abnormal~~ sequences is then searched for systems interactions. First, the analyst should look for double system failures; that is, for ~~abnormal~~ sequences involving the failure of only two systems. Next, we look for triple system failures, etc. The search for system interactions will start from the double system failures (if any) and it will continue on with increasing numbers of systems. This classification has the potential of reducing the size of the required effort for the following reason. A triple system failure contains three double failures. If all these double failures have been examined and no interactions have been found, no interaction exists in the triple failure. Of course, this is true only if the success criteria for the systems involved are the same in the double failures as in the triple. If an interaction has been found in a double combination, one could only determine whether this interaction extends into the third system.

At this point of the analysis the ~~abnormal~~ sequences (Event Tree paths) have been identified and ordered in terms of the number of front-line system failures they contain.

Starting with the first ~~abnormal~~ sequence in this list, the Systemic Fault Trees, the Support Systems Fault Trees, and the Initiating Event Fault Trees are under an AND gate. Then, the minimal cut sets are generated.

Step 9 Search for Completion of Interactions in the Minimal Cut Sets

Each minimal cut set is searched for functional, spatial, or human interactions.

Functional interactions due to shared hardware can be identified by careful examination of the Systemic Fault Trees and Support Systems Fault Trees. The appearance of the same hardware in different places of a fault tree is an indication of systems interaction. After searching for interactions due to shared hardware, a search is made for functional interactions due to functional couplings among the elements of the cut set. The failure mode lists developed in Step 6 are useful at this point. For every element of the cut set, the failure effects are searched to discover any influenced systems that may be part of the same cut-set. Also, each of the element's failure modes are searched to discover one element's failure mode that may be common to another element's failure effects.

Spatially coupled interactions can be identified through a process similar to that for process couplings. If such common features exist, the next step consists in examining whether a single cause of such a feature can affect the elements of the cut set simultaneously. This common cause will be possible where elements of one cut set are coupled together.

The search for spatial couplings will be best performed through plant visual inspections. The coupled elements of the cut set are recorded as candidates for examination in an actual visual inspection for this particular generic cause.

Humanly coupled interactions can be identified by searching the cut-set elements for any condition where one of the failures would induce an operator action that will influence at least one other system represented in the same cut-set. A search is made for human couplings between more than one element in the cut-set.

It should be emphasized that during this part of the procedure that the analysts' accumulated experience (LERs, observed system interactions) become important for completeness. Steps 6 through 9 should have been repeated for each redundant train and subsystem.

Each interaction identified in Step 9 is characterized as described in Sections 5.2.1, 5.2.2, and 5.2.3.

A.3 Assessing the Identified of System Interactions

Assessing the identified system interactions could be done with different degrees of formalism. A rather formal method is described here. However, the assessment of the relative importance among identified systems interactions is not essential for these initial analyses. The NRC will not require corrective action for identified adverse systems interactions unless it is needed under existing NRC requirements.

Each minimal cut-set generated after the last iteration in the search phase can be associated with a single path of the Systemic Event Tree and hence with a consequence (usually amount, mode, and timing of radioactivity release). The minimal cut sets containing the systems involved in a given interaction are identified and grouped by equivalent consequences. The probability of occurrence of each minimal cut-set is estimated and the contribution to the risk of these minimal cut-sets is reestimated after removing the interaction and the new contribution to the risk is calculated. The difference of the contributions to the risk of the minimal cut-sets before and after the removal of the interaction represents the risk reduction achieved by removing the interaction and constitutes the measure of importance of the interaction.