NUREG–1174

Evaluation of Systems Interactions in Nuclear Power Plants

Technical Findings Related to Unresolved Safety Issue A–17

U.S. Nuclear Regulatory Commission

Office of Nuclear Regulatory Research

Dale Thatcher

NUREG–1174

Evaluation of Systems Interactions in Nuclear Power Plants

Technical Findings Related to Unresolved Safety Issue A–17

Manuscript Completed: April 1989
Date Published: May 1989

Dale Thatcher

Division of Safety Issue Resolution
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, DC 20555

ABSTRACT

This report presents a summary of the activities related to Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants," and also includes the NRC staff's conclusions based on those activities. The staff's technical findings provide the framework for the final resolution of this unresolved safety issue. The final resolution will be published later as NUREG-1229.

CONTENTS

CONTENTS (cont.)

TABLES

ABBREVIATIONS

ACRS	Advisory Committee on Reactor Safeguards
ADS	automatic depressurization system
AEC	Atomic Energy Commission
AEOD	Office for Analysis and Evaluation of Operational Data
AFW	auxiliary feedwater
ANS	American Nuclear Society
ASI	adverse systems interaction
ATWS	anticipated transient without scram
BNL	Brookhaven National Laboratory
BTP	branch technical position
BWR	boiling-water reactor
CCC	common-cause candidate
CCW	component cooling water
CFR	*Code of Federal Regulations*
CPCo	Consumers Power Company
DMA	digraph matrix analysis
ECCS	emergency core cooling system
EPRI	Electric Power Research Institute
ESF	engineered safety features
FMEA	failure modes and effects analysis
FSAR	Final Safety Analysis Report
GDC	general design criterion/criteria
GI	generic issue
HELB	high-energy line break
HPSI	high-pressure safety injection
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control
IE	Office of Inspection and Enforcement, NRC
IEEE	Institute of Electrical and Electronics Engineers
INPO	Institute of Nuclear Power Operations
IP3	Indian Point Station, Unit 3
IREP	Interim Reliability Evaluation Program
LER	licensee event report
LLNL	Lawrence Livermore National Laboratory
LOCA	loss-of-coolant accident
MSLB	main steamline break
NPRDS	Nuclear Plant Reliability Data System
NRC	U.S. Nuclear Regulatory Commission
NSSS	nuclear steam supply system
NYPA	New York Power Authority
ORNL	Oak Ridge National Laboratory
PASNY	Power Authority of the State of New York
PG&E	Pacific Gas & Electric Co.
PRA	probabilistic risk assessment
PWR	pressurized-water reactor
RCPB	reactor coolant pressure boundary
RHR	residual heat removal
RSS	Reactor Safety Study
RSSMAP	Reactor Safety Study Methodology Applications Program
RTS	reactor trip system
SEP	Systematic Evaluation Program
SETS	Set Equation Transformation Systems
SI	systems interaction
SISIP	Seismically Induced Systems Interaction Program
SRP	Standard Review Plan
TAP	Task Action Plan
TMI	Three Mile Island Nuclear Station
TMI-2	Three Mile Island Nuclear Station, Unit 2
USI	unresolved safety issue

EXECUTIVE SUMMARY

The U.S. Nuclear Regulatory Commission (NRC) has concluded its technical evaluation of Unresolved Safety Issue (USI) A–17, "Systems Interactions in Nuclear Power Plants." This report summarizes the results of the technical activities used by the NRC staff to formulate the final resolution of USI A–17. The regulatory analysis for the proposed resolution of USI A–17 will be published later as NUREG–1229.

Because of the complex, interdependent network of systems, structures, and components that constitute a nuclear power plant, the scenario of almost any significant event can be characterized as a systems interaction. As a result, the staff determined that if the term "systems interaction" were interpreted in a very broad sense, it became an unmanageable safety issue. To begin to address perceived safety concerns within this potentially broad subject area requires some focusing. One way to focus such an effort is to develop a working set of definitions based on the perceived safety concerns. It is recognized that by the very nature of such a focusing effort, all concerns that one may characterize as systems interactions may not be addressed. It is therefore extremely important that the scope and boundary of the focused program be as clearly defined and understood as possible. Then, if other concerns still exist after completion of the program, they can be addressed as part of other efforts as deemed necessary.

The technical findings and conclusions presented in this document are based on the following definitions.

Systems Interaction (SI)

An action or inaction (not necessarily a failure) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and *propagation* to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between an SI and a classic single-failure event is in those hidden or unanticipated aspects of the initiating failure and/or its propagation.

Adverse Systems Interaction (ASI)

A systems interaction that produces an undesirable result.

Undesirable Result (Produced by SIs)

This was defined by a list of the types of events that were to be considered in USI A–17:

- Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and analysis (Chapter 15) of the Final Safety Analysis Report (FSAR) of the plant. (*Note:* This would violate the single-failure criterion.
- Degradation of a safety system by a system that is not safety related. (*Note:* This result would demonstrate a breakdown in presumed "isolation.")
- Initiation of an "accident" [e.g., loss-of-coolant accident (LOCA), main steamline break (MSLB)] *and* (a) the degradation of *at least one* redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) *or* (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect action. (*Note:* This includes failure to perform correct actions because of incorrect information.)
- Initiation of a "transient" (including reactor trip) *and* (a) the degradation of *at least one* redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) *or* (b) sufficient degradation of critical operator information to cause the operator to perform unanalyzed, unassumed, or incorrect action. (*Note:* This includes failure to perform correct actions because of incorrect information.)
- Initiation of an event that requires plant operators to act in areas outside the control room (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes based on the way they propagate:

Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

Induced Human-Intervention Coupled

Those SIs that result when a plant malfunction (such as failed indication) inappropriately induces an operator action, or a malfunction inhibits an operator's ability to respond. As analyzed in A–17, these SIs are considered another example of functionally coupled ASIs. (*Note:* Random human errors and acts of sabotage are excluded.)

As a result of the staff's studies of ASIs undertaken as part of its search for a solution to the USI A–17 safety issue, the staff has concluded the following:

(1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task and therefore incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the A–17 program utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.

(2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and test and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.

(3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.

(4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.

(5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.

(6) Induced human-intervention-coupled interactions as defined in A–17 are a subset of the broader class of functionally coupled SIs. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.

(7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of flooding and water intrusion events and more recent operating experience indicates that these types of events are continuing to occur (see the Appendix for additional information).

(8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.

(9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.

(10) For existing plants, a properly focused, systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.

(11) The area of electric power, and particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could provide a more effective approach in this area.

(12) For future plants, additional guidance regarding ASIs could benefit safety.

(13) The concerns raised by the Advisory Committee on Reactor Safeguards (ACRS) on A-17, but which have not been addressed in the staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.

UNRESOLVED SAFETY ISSUE A-17: SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS

1 INTRODUCTION

In 1978, the NRC identified the area of systems interactions as an unresolved safety issue (USI) and designated it as USI A-17, "Systems Interactions in Nuclear Power Plants."

The origins of the concerns with systems interactions go back to 1974 when the Advisory Committee on Reactor Safeguards (ACRS, November 8, 1974) expressed its belief that the staff should give "attention to the evaluation of safety systems and associated equipment from a multidisciplinary point of view to identify potentially undesirable interactions between systems."

It should be noted that the original concerns were raised in the context of standard plants (ACRS, November 8, 1974). It was felt that with the prospect of many "identical" plants, significant additional efforts should be focused on uncovering potential problems that may arise because a nuclear power plant is designed by groups of engineers and scientists who belong to separate engineering and scientific disciplines. It was recognized that some interdisciplinary reviews were performed to ensure the compatibility of the plant's structures, systems, and components; however, there remained some question regarding the adequacy of these reviews. For standardized plants, it was believed that the additional effort could provide significant benefits. In addition to the original ACRS concern, some potentially significant events at operating nuclear power plants have been traced to, or have been postulated to be the result of, a single common cause (as opposed to multiple independent causes). As a result, the required independence among the plant safety systems and the independence of the safety systems from the systems not related to safety have been questioned. Because of the original ACRS concern and because some significant operating events took place as a result of unexpected interdependencies among the various plant systems, components, and structures, USI A-17 was developed to address the area of systems interactions. (*Note:* The program designed to address systems interactions will not address all events resulting from a single common cause.) For further clarification, see Sections 2 and 3 of this report.

In 1979, an accident at the Three Mile Island Nuclear Station, Unit 2 (TMI-2) led to issuance of NUREG-0660, "NRC Action Plan Developed As a Result of the TMI-2 Accident," which identified TMI Action Plan Item II.C.3, "Systems Interaction," for the purpose of coordinating and expanding the staff's work on systems interactions (USI A-17) and to incorporate that work into an integrated plan for addressing the broader question of systems reliability in conjunction with IREP (Interim Reliability Evaluation Program) and other efforts. The TMI-2 Action Plan also stated: "As these programs go forward, there will be a conscious effort to coordinate these activities, including possible combination of resources, to eliminate unnecessary duplication." As stated in the Task Action Plan (TAP) for USI A-17 (NUREG-0649), the resolution of USI A-17 has considered the activities described in Item II.C.3.

The A-17 program has been designed to establish whether or not there are significant generic safety concerns in the area of systems interactions, and then if there are such concerns, to develop ways to identify these concerns and address them.

2 BACKGROUND

The term "systems interaction" has never been precisely defined, and, as a result, the investigation into the concern has suffered from a lack of a clear focus. At times, A-17 was becoming a "catch all" category for almost all significant events that occurred at operating reactors. The term has often been used interchangeably with other terms such as "dependent failures," "propagating failures," "common-cause failures," and "common-mode failures." To address what was perceived to be the original concern, and to address some of the significant types of events that have occurred, the A-17 program has been provided with a set of working definitions (see Section 3, "Definitions and Scope").

The definitions attempt to clarify the specific types of phenomena or events that are of interest in A-17 and to separately classify other phenomena or events considered outside the scope of A-17.

3 DEFINITIONS AND SCOPE

One of the largest efforts in focusing all of the various tasks related to systems interactions was in the development of a workable set of definitions. The definitions, and associated clarifications, were drawn from the large amount of information previously developed in A-17 (before 1983). The definitions attempt to clarify the specific types of phenomena or events that are of interest, i.e., those that represent unanticipated, adverse interactions among "systems" where systems can be structures, systems, or components. The definitions also attempt to separately classify other types of events which, although they may be significant, are not addressed in A-17. Table 1 is included to summarize the scope and bases of the USI A-17 issue.

Table 1 Scope of USI A–17, "Systems Interactions"*

Concerns	Covered by	Clarification
(1) Recognized/analyzed single failures directly propagate to other equipment/systems within the same safety division	Existing regulations • Single failure defined in the GDC	Not analyzed in A–17
(2) Single failures subtly propagate to cause plant transients/accidents and/or degrade the required safety systems. Includes: • Subtle spatial inter-ties • Subtle functional inter-ties	USI A–17 definition of adverse systems interactions	
(3) Common failure of redundant safety systems due to commonalities such as: • Same manufacturing defect • Same testing error • Same maintenance error	Improvements in maintenance and test procedures, ATWS rule, A–44 proposed rule	Not analyzed in A–17
(4) Operator errors that disable redundant safety systems	Improvements in operator training	Not analyzed in A–17
(5) Events that could cause multiple plant problems simultaneously: • Particularly earthquakes • Also fire and pipe break/flooding	USI A–46 plus current licensing requirements cover earthquakes Appendix R deals with fire Equipment qualification rule (10 CFR 50.49) deals with design-basis pipe breaks None of these programs deals with multiple, simultaneous events. Therefore, this area is to be further evaluated under the Multiple System Responses Program.	Not analyzed in A–17, except for internal flooding/water intrusion events occurring one at a time

*General subject area involves system failures which are due to system dependencies.

The definitions presented here parallel those in the NRC Task Action Plan (NUREG–0649); however, the term "common-mode failure" has been dropped and further clarifications have been added. In developing the definitions, the main objective was to acknowledge that a great amount of concern exists regarding events in which a scenario progresses to an undesirable set of circumstances and the cause can be traced to a single common cause (common-cause events), involving an equipment malfunction or failure and its propagation.

After tracing the origins of the systems interaction concern as expressed by the ACRS and then also considering the changes that have been taking place in the nuclear industry over the last 10 years, it was decided that a classification needed to be created to make the problem of "systems interactions" more tractable and also to take credit for other activities which will cover areas that one might argue should be included in A–17. Some of the changes that have been acknowledged include

(1) greater attention to human factors or the man/machine interface in all aspects of nuclear power plant design and operation

(2) use of probabilistic risk assessments (PRAs) in safety analysis

(3) increased attention to operating events.

The resulting classification scheme outlines a number of different types of common-cause events, only one set of which was defined to involve "adverse systems interactions." The other single-cause events involve mostly common characteristics of the equipment (e.g.,

single manufacturer, common maintenance practices and personnel, common testing practices and personnel).

3.1 Systems Interactions

The definition used here is: Actions or inactions (not necessarily failures) of various systems (subsystems, divisions, trains), components, or structures resulting from a single credible failure within one system, component, or structure and *propagation* to other systems, components, or structures by inconspicuous or unanticipated interdependencies. The major difference between this type of event and a classic single-failure event is in those aspects of the initiating failure and/or its propagation that are not obvious (that are hidden or unanticipated).

Systems interactions (SIs) also can involve systems related to safety and systems not related to safety. A large part of the problem in addressing SIs stems from the fact that, in any nuclear power plant, many systems are intended to interact and are so designed. For example, one division of the safety-related component cooling water system is designed to interact with (i.e., cool) a number of other safety-related systems in that division as well as possibly some systems not related to safety. Similarly, one division of the Class 1E electric power system is designed to interact with a number of safety-related systems in that same division as well as possibly with some equipment not related to safety. If these support-type systems do fail, the supported system will also most likely fail or at least will operate improperly.

Although these examples involve interaction of systems and even could be considered adverse systems interactions, they are not the kinds of interactions of concern in USI A-17, because this type of interaction is expected and the potential for such failure propagation is within the typical analysis and assumptions for a single failure. To differentiate among all the potential "systems interactions," the A-17 Task Action Plan added the aspect of "adverse" to further pinpoint the issue.

3.2 Adverse Systems Interactions

The definition used here is: A systems interaction that produces an undesirable result, as defined by a list of the types of events to be considered in the A-17 program (see list that follows).

The list was created on the basis of perceived safety concerns in the broad area of systems interactions for the purpose of capturing *potential* adverse systems interactions, and therefore terms such as "undesirable" instead of "unacceptable" and "degradation" instead of "failure" were used.

(1) Degradation of redundant portions of a safety system, including consideration of all auxiliary support functions. Redundant portions are those considered to be independent in the design and accident analysis (Chapter 15, FSAR analyses) of the plant. (*Note:* This would violate the single-failure criterion.)

(2) Degradation of a safety system by a system not related to safety. (*Note:* This result would demonstrate a breakdown in presumed "isolation.")

(3) Initiation of an "accident" [e.g., loss-of-coolant accident (LOCA), main steamline break (MSLB)] *and* (a) the degradation of *at least one* redundant portion of any one of the safety systems required to mitigate that event (Chapter 15, FSAR analyses) *or* (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (*Note:* This includes failure to perform correct actions because of incorrect information.)

(4) Initiation of a "transient" (including reactor trip) *and* (a) the degradation of *at least one* redundant portion of any one of the safety systems required to mitigate the event (Chapter 15, FSAR analyses) *or* (b) degradation of critical operator information sufficient to cause the operator to perform unanalyzed, unassumed, or incorrect actions. (*Note:* This includes failure to perform correct actions because of incorrect information.)

(*Note:* Undesirable results 3 and 4 are included because of the concerns regarding possible breakdowns in defense-in-depth principles. If a link is found between the initiation of an event and the systems designed to mitigate that event, then the probability of an event sequence progressing to core melt may be greater than originally believed.)

(5) Initiation of an event that requires plant operators to act in areas outside the control room area (perhaps because the control room is being evacuated or the plant is being shut down) and disruption of the access to these areas (for example, by disruption of the security system or isolation of an area when fire doors are closed or a suppression system is actuated).

The intersystem dependencies (or systems interactions) have been divided into three classes, based on the way they propagate:

Functionally Coupled

Those SIs that result from sharing of common systems/components; or physical connections between systems, including electrical, hydraulic, pneumatic, or mechanical.

Spatially Coupled

Those SIs that result from sharing or proximity of structures/locations, equipment, or components, or by spatial inter-ties such as heating, ventilation, and air conditioning (HVAC) and drain systems.

Induced Human-Intervention Coupled

Those SIs that result when a plant malfunction (such as failed indication) inappropriately induces an operator action, or when a malfunction inhibits an operator's ability to respond. As analyzed in the study of USI A-17, these SIs are considered another example of functionally coupled ASIs. (*Note:* Random human errors and acts of sabotage are excluded.)

3.3 Other Common-Cause Events

Multiple failures resulting from a single common cause and typically characterized by the failure of identical components in redundant safety systems will not be addressed in the A-17 study. Such multiple failures can be traced to external events, manufacturing and installation errors, or to operation, testing, and maintenance errors.

The usual design practice for safety systems is to satisfy the single-failure criterion by providing identical, redundant safety systems which are subjected to common environmental events and made, installed, operated, tested, and maintained in common. Therefore, the potential for these types of "failures" results from a recognized compromise in independence (see 10 CFR Part 50, Appendix A, "Introduction to the General Design Criteria") and is addressed in a number of ways, and in some cases without specific identification. Some of the ways in which this other class of failures/errors is addressed are discussed in the four paragraphs that follow.

To obtain protection from possible failures induced by a component's environment, including failures resulting from external events, the components of the safety systems are designed, qualified, and installed to be immune to such anticipated challenges.

To obtain immunity to failures, including failures resulting from manufacturing and installation errors, the safety-related systems, structures, and components are subjected to various quality control and quality assurance programs which include comprehensive testing requirements at all phases of construction and pre-operation. Major improvements in the area of quality assurance have been made at the utilities.

Protection from failures attributed to errors by operators, technicians, and maintenance personnel can be obtained through adequate training and good procedures for all aspects of operation, testing, and maintenance. The staff is instituting major programs to address all of these areas (see NUREG-0985).

Other provisions may be utilized for protection against these types of common-cause failures. One design technique which is utilized is diversity. An example of such an application by the staff is a portion of the requirements which resulted from the Salem anticipated transient without scram (ATWS) event (NUREG-1000). As part of the resolution, it was concluded that consideration should be given to providing a diverse breaker trip scheme. Although such cases have been addressed on an individual basis, the concept of diversity is cited in the regulations [e.g., General Design Criterion (GDC) 22].

3.4 Clarifications

Some additional clarifications are included here to address the areas that tend to be the hardest to classify. First, events induced by operator error will be discussed and then events involving external phenomena and other major plantwide events will be discussed. Classic single failures vs. adverse systems interactions will be discussed. Also, the concept of frontline and support systems will be presented.

3.4.1 Operator Error

For purposes of studying USI A-17, plant operators and their procedures were assumed to be perfect. This assumption allowed the staff to focus on only the area of the adequacy of the information presented to the operator by the plant display systems, as outlined in induced human-intervention-coupled SIs. Therefore, the operator was treated as a hardwired link that performed perfectly. As stated earlier, other programs involving human factors were considered more suited to addressing the possibility of operator error, test and maintenance errors, and procedure deficiencies (see NUREG-0985).

3.4.2 External Events

One of the most difficult areas to classify for purposes of studying USI A-17 is external events. In general, external events such as tornadoes and earthquakes are not addressed in the A-17 program. It is recognized that external events could initiate other common-cause failures, as stated in Section 3.3 above.

It is also recognized that, with respect to non-seismically qualified or non-safety-related equipment, an external event such as an earthquake could be the cause of the single initiating failure in an adverse systems interaction sequence. In that limited sense, external events were considered. The group engaged in the A-17 program did not consider the potential for an external event to cause simultaneous multiple initiating failures and systems responses. For more discussion of major plantwide events

and the potential for multiple systems responses, see Section 3.4.3 which follows.

3.4.3 Major Plantwide Events and the Potential for Unanalyzed, Nonconservative, Multiple Systems Responses

During discussions with the ACRS, some disagreements over the scope of the A–17 program were noted (ACRS, May 13, 1986).

In later discussions with the ACRS, the concerns were developed further. The analysis for plant events (such as earthquakes, fires, LOCAs, and floods) involve a number of assumptions. These assumptions often include certain aspects which the ACRS believes may not be conservative. The first aspect involves the assumptions that the events themselves are not linked, that is an earthquake does not start a fire, a fire does not cause a LOCA, etc. The ACRS is concerned that such assumptions are neither realistic nor conservative.

The second aspect involves the assumption that if a component is not specifically required to function for the mitigation of an event, then it is assumed to be disabled or inoperable. Again, the ACRS is concerned that such assumptions are not conservative because if the specific failure modes of the component are considered, the component could spuriously perform some detrimental action which could affect the ability to mitigate the event and/or to achieve safe shutdown.

The above concern involving specific failure modes includes the added aspect that systems and components are generally assumed to be either fully operable or totally inoperable, as if only two possible states existed. As a result, ACRS believes that there is also the potential that partial failures that do not result in total loss of function could lead to some unanalyzed systems action which in turn may adversely affect the event mitigation and/or the ability to achieve safe shutdown. The ACRS believes that failures or partial failures could occur simultaneously in multiple systems, if the initiating event is of a sufficiently broad nature, such as an earthquake, fire, or flood.

The staff studying USI A–17 has not addressed the potential for major events causing other events nor has it addressed the multiple failure concerns expressed by the ACRS. It is recommended that these issues be addressed as separate potential generic issues.

3.4.4 Single Failures vs. ASIs

An important aspect of the A–17 group's definition of SIs and ASIs is the unanticipated or hidden nature of the dependency. It is acknowledged (and therefore *not* "unanticipated") that certain design features do not have redundancy. Examples are the reactor vessel itself and the refueling water storage tank at some pressurized-water reactors (PWRs). Clearly, a failure of these could lead to an undesirable result; however, A–17 does not intend to deal with these common causes because they are not *hidden* or *unanticipated.* The other important aspect involves a similar problem area. A problem arose because once an ASI is identified, it looks like a classic single failure and one could then argue that it is, therefore, not an ASI, just a single failure. This aspect was very critical in the operating experience search. That part of the program relied heavily on the consensus of a number of people familiar with operating events and plant design and, therefore, keenly attentive to "surprises" such as unanticipated couplings or dependencies. This "judgment" aspect has led to at least one noted disagreement involving power sources and the results that one would anticipate or expect from a single failure in a Class 1E power source. An analyst or engineer familiar with nuclear power plant systems, and particularly with the instrumentation and control power systems and electric power systems, may expect one set of results (which would meet all other aspects of the ASI definition); another analyst or engineer may find the results unexpected. Therefore, some events involving loss of instrumentation and control power supplies may not have been captured during the initial screening of the licensee event report (LER) data base. Because of its possible importance, as outlined in related Generic Issue (GI) 76 (NUREG–0933, Rev. 2) and as stated by the NRC staff (NRC memorandum, September 18, 1984), further specific work was undertaken in this area (see Section 5.4).

3.4.5 Frontline and Support Systems

During the review and evaluation of systems interactions, the group studying USI A–17 acknowledged that there may be a difference in the way the frontline systems, such as emergency core cooling and reactor protection systems, are treated and the way the support systems, such as component cooling water and heating and ventilating systems, are treated. The frontline systems usually receive thorough scrutiny in the licensing process because of the number of specific criteria that are clearly applicable and also because these areas of the plant tend to be more standardized among plants (at least regarding any specific nuclear steam system supplier).

The support systems, on the other hand, are often less standardized and in many cases are more complex and pervasive, so that they not only interface with multiple frontline safety systems and other safety-related support systems, but also may interface with functions not related to safety. As a result, support systems may require greater scrutiny for adverse systems interactions.

3.5 Summary and Conclusions

Resolution of USI A–17 involves those types of common-cause events which are classified as adverse systems interactions subject to the above definitions and classifications.

On the basis of all work that has been and is being performed in the resolution of A–17 and with the objective of resolving A–17 in a defined time frame, the staff concluded that a working set of definitions was crucial to the A–17 program. Therefore, the staff focused its A–17 task on certain types of phenomena and scenarios and left other areas to other programs and issues.

4 AVAILABLE METHODS FOR IDENTIFYING SYSTEMS INTERACTIONS

As a related effort to the investigation of the nature and potential safety significance of adverse systems interactions, the group engaged in the A–17 program explored a number of methods that appeared to offer the potential for finding ASIs. The purpose of this part of the program was to determine the effectiveness and the resource requirements of potential ASI search methods and to make recommendations regarding possible search methods if it was concluded that a search was necessary.

Some of the information on methods is reported in other sections of this report (e.g., digraph matrix analyses, Section 5.3; interactive fault tree and failure modes and effects analyses, Section 5.3; operating experience search, Sections 5.1.1, 5.2.3, 5.2.5, 5.2.6, and 5.4; onsite inspections, Sections 5.1 and 5.6; and PRAs, Section 5.5). This section of the report also addresses some of these methods, combinations of these methods, and other methods, and then draws some general conclusions.

ORNL (NUREG/CR–4261) reviewed and identified four classes of qualitative analyses techniques that can be used to identify possible systems interactions. Each class of techniques would be appropriate for different aspects of a systems interaction search (see Table 2). In addition, there are distinct advantages and disadvantages in performing each class of techniques. The four basic classes are

(1) operating experience reviews

(2) onsite inspections

(3) analysis by parts

(4) graph-based analyses

Each class of techniques is composed of one or more different analysis methodologies. Each class of techniques is discussed below, and information is provided about the individual methodologies in the class. (For a list of some associated references for each technique, see NUREG/CR–4261.)

Some combination of these analysis techniques could be used to perform a systems interaction study or could be incorporated into a systematic study such as a probabilistic risk assessment (PRA) to identify functional, spatial, or induced human-intervention-coupled systems interactions.

4.1 Operating Experience Reviews

The NRC staff currently requires operating experience review "programs" for each nuclear power plant licensee (TMI Action Plan Item I.C.5). The NRC and industry also sponsor their own reviews of operating experience (see Section 5.4). The objective of all of these programs is to learn from events that have already occurred, or have the potential to occur, at operating nuclear power plants. The history of events at plants under construction is also reviewed. The potential benefit of operating experience reviews is to eliminate recurring problems. For systems interaction purposes, this may allow previously unanticipated dependencies to be identified before any serious safety consequences occur.

To benefit from the review of operating experience, reliable sources of data on events must be available. For a specific plant, this includes both onsite sources (deficiency reports, operating logs, work orders, etc.) and documents prepared for submittal to outside agencies [licensee event reports (LERs), significant event reports, Nuclear Plant Reliability Data System (NPRDS) failure reports, etc.] The data sources that contain information on events from many plants include the NRC's LER files, Institute of Nuclear Power Operations (INPO) operating experience systems, and various other industry working groups (vendors, technical societies, etc.).

Once a source of operating experience is chosen, proper review requires the services of experienced personnel. The reviewers need to be familiar with the facility for which the review is conducted; reviewers also need to be cognizant of the similarities and differences between that facility and those facilities at which the events occurred. This knowledge is essential in determining whether the events apply to the plant for which the review is being performed.

A key to performing effective operating experience reviews is to carry the evaluation beyond simply asking, "What would happen in our plant if the exact same conditions occurred?" It requires the personnel to consider two other questions:

Table 2 Analysis methodologies available to identify types of systems interactions

Analysis methodologies available to identify systems interactions	Types of systems interactions identified by methodologies		
	Functional	Spatial	Induced human-intervention-coupled
Operating experience review	X	X	X
Plant walkthrough		X	
Preoperational testing	X		
Failure modes and effects analysis	X	X	X
Design review	X	X	X
Decision table	X		X
System state enumeration	X		
Binary matrix	X	X	
Digraph matrix	X	X	X
Event tree analysis	X		
Fault tree analysis	X	X	X
GO methodology	X	X	
Sneak-circuit analysis	X		
Generic analysis	X	X	

(1) Can this systems interaction occur at our facility under any conditions?

(2) If such an event occurred at our facility, are the consequences unacceptable?

If the answer to both these questions is "yes," then further evaluation (and subsequent resolution) of the potential problem is required.

Operating experience reviews can examine the potential for certain systems interactions (i.e., those interactions that have occurred previously). Since the NRC requires ongoing operating experience reviews, it would be simple and inexpensive to include the identification of systems interactions as one of the objectives of the reviews. The recognized shortcomings of operating experience reviews are that the reviews (1) are not fully predictive and (2) are very dependent on the experience and training of the review staff. Operating experience reviews can provide insights into functional, spatial, and induced human-intervention-coupled systems interactions.

4.2 Onsite Inspections

Onsite inspections are used to identify differences between the as-built conditions and the design conditions. They can also examine undesirable situations (i.e., proximity, seismic interaction, etc.) that may not be apparent from design documentation. This class of techniques incorporates the experience and knowledge of plant personnel into the analysis. Onsite inspections can also be used to identify areas in which the environmental conditions within the plant are hazardous to equipment or in which adverse changes have been made in the plant's equipment configuration (because of maintenance or upgrading). Two types of onsite inspection methodologies were identified: plant walkthroughs and preoperational testing.

4.2.1 Plant Walkthroughs

Plant walkthroughs are used to identify potential spatial systems interactions and to visually inspect safety-related components and systems in their as-built configuration. Consequently, walkthroughs are used to identify those systems interactions that were overlooked during plant design or that were generated during plant construction.

Consumers Power Company developed a plant walkthrough program at its Midland Nuclear Power Plant, Units 1 and 2 (Consumers Power Company, June 1983) to determine the potential for spatial systems interactions. The program consisted of: (1) combined proximity for seismic Category I and II components, systems, and structures, (2) high-energy line break hazards, (3) internal missiles, and (4) flooding. The function and team composition for each of these walkthroughs were varied to be appropriate for each specific type of systems interaction. Consumers Power Company also developed a supplemental walkthrough program that addressed (1) fire protection, (2) stress, (3) thermal growth, (4) system or

area turnover walkthroughs, and (5) potential concerns discovered during preoperational testing of systems.

Plant walkthroughs to identify potential systems interactions have also been performed at Diablo Canyon Nuclear Power Plant; San Onofre Nuclear Generating Station, Units 2 and 3; Zion Nuclear Plant; and Indian Point Station, Unit 3. These walkthroughs were structured to identify spatial systems interactions.

The advantages of plant walkthroughs include: (1) They can focus on bad design, construction errors, maintenance errors, and conditions for common failure and (2) They utilize the knowledge of experienced plant personnel.

4.2.2 Preoperational Testing

Preoperational testing is used to demonstrate the operability of the nuclear steam supply systems, the auxiliary systems, and related secondary systems. All licensees are required to successfully complete a preoperational testing program before a full-power license can be issued. This testing program demonstrates the capability of items of equipment (and systems) to meet their design performance and safety criteria. However, preoperational tests can specifically test how systems interact (in some cases existing tests already do this). For example, a diesel generator operability test should include sequencing the diesel generators onto the emergency power buses. There are many cases in which a test specifically designed to test for systems interactions could confirm the absence of unacceptable interactions during specific operating modes.

The advantages of preoperational testing include: (1) The tests can provide a baseline of operating data from which future operational anomalies may be identified, (2) They provide further confidence in the analytical results and functional capabilities of the systems, and (3) They have the potential to identify functional interactions.

A disadvantage is that they cannot typically identify spatially coupled interactions.

4.3 Analysis by Parts

The third class of techniques available for identifying systems interactions is analysis by parts. Analysis-by-parts techniques are more analytically oriented than the previously discussed classes of techniques, but they are also less comprehensive than the graph-based analyses discussed in Section 4.4. Five methodologies were identified as analysis-by-parts techniques:

(1) failure modes and effects analysis

(2) design reviews

(3) decision tables

(4) system state enumeration

(5) binary matrices

Analysis by parts requires the analyst to examine the causes of a given event or to develop credible conditions under which an undesirable event could occur. Consequently, a problem is not evaluated from a total system perspective. Instead, direct causes of subsystem or component failures are identified and the consequences of these failures are examined. Since these techniques are used to look for direct causes, they are not exhaustive in that regard.

Several advantages of this class of techniques are: (1) They require less effort to perform than the graph-based analyses (at the price of less complete coverage), (2) They are relatively simple to perform, (3) They are useful for detecting local effects, and (4) They require the analyst to look systematiically at the failure of each component. Disadvantages of this class include: (1) They usually capture only local effects, (2) They depend on the creativity of the analyst, (3) They have a limited amount of predictive strength, and (4) They are generally used in support of other classes and frequently address the same type of systems interactions as the graph-based methods. Each of the methodologies is discussed below.

4.3.1 Failure Modes and Effects Analysis

Failure modes and effects analysis (FMEA) is an inductive analysis method that is generally applied at the component level. As such, it examines a component to determine how it would fail (mode) and what would result (effect). An FMEA generally does not examine the causes of the failure extensively but may be employed to identify failure modes whose effects are severe enough to warrant further analysis.

The FMEA identifies failure modes for components of concern and traces their effects on other components, subsystems, and systems. Emphasis is placed on identifying the problems that result from such problems as hardware failures and operator errors. Typically, a column format is employed in an FMEA. Specific entries for the columns include descriptions of the component, its failure modes, possible failure causes, possible effects, and actions to reduce the failures and their consequences. By further examining the causes of the failures, possible common-cause mechanisms may be identified.

An FMEA is traditionally developed at the component level. However, an FMEA can also be applied at the subsystem or system level to trace interactions and their effects on plant safety functions and, eventually, on plant

safety itself. In addition, the effects of the failure modes (whether at the component or system level) must be considered for all plant operational modes and the analyst must also consider the possibility of other components undergoing test and maintenance.

4.3.2 Design Reviews

Design reviews are performed to ensure that the safety system independence and functional design criteria have been met or exceeded. The procedures for performing them vary, and are specific to the design organization. Design reviews are generally performed by a diversified group of experienced designers called a design review team. Using the design criteria or specifications for the systems, the team reviews available documentation such as control schematics, layout drawings, as-built drawings, and piping and instrumentation diagrams. The team then identifies design deficiencies, including potential systems interactions. The team also recommends actions or design changes that may correct the design deficiencies and eliminate potential systems interactions. An advantage of using design reviews to identify potential systems interactions is that they can provide early identification. One disadvantage is that as-built drawings are frequently not available or are not up to date. Also, it is difficult to ensure the comprehensiveness of design reviews.

4.3.3 Decision Tables

Decision tables are used to describe each possible output state of a component. The output states are a function of the inputs and internal states (operational or failed states) of the components. Decision tables can handle binary and nonbinary logic (i.e., components with two or more states).

To construct a decision table, the analyst divides the system into levels of components or subsystems. Once the system has been divided into levels, the analyst needs to perform three basic steps:

Step 1 The analyst constructs the decision tables beginning with the components of the lowest levels (i.e., the simpler components of the system).

Step 2 The outputs of the tables from Step 1 constitute the inputs of the decision tables for the next higher level.

Step 3 Step 2 is repeated for each higher level until the decision table of the system is formed.

This methodology can be used to identify common-cause failures, since they are the inputs that are carried through several levels.

One advantage of constructing decision tables is that they not only model hardware failures, but model human actions and interactions as well. However, decision tables are not a stand-alone method and are generally used to aid in constructing fault trees.

4.3.4 System State Enumeration

In a system state enumeration analysis, all of the system states are generated and recorded in a table format by considering all possible combinations of component states. After this is completed, each system state is individually examined for dependencies between component states. From a qualitative point of view, this analysis is equivalent to an event tree analysis.

An advantage of system state enumeration is that it is a fairly complete qualitative method. However, a complete qualitative system analysis would include an FMEA for each state. Also, for complex systems, enumerating all potential component states can be an overwhelming task.

4.3.5 Binary Matrices

Binary matrices use hierarchies to portray the dependencies between components. A binary entry in each intersection of the matrix indicates whether or not the components are dependent upon each other. The binary entry indicates that the component on the left of the matrix (row) is dependent upon (receives support from) the component listed at the top (column). The matrix is not limited to components. The entity of interest could be maintenance, a physical location, a system train, and so forth. A set of binary matrices that represent more than one independent system is used to generate digraph matrices.

One advantage of binary matrices is that the analyst need only supply direct relationships between individual items (components, subsystems, etc.). A computer code can then be used to deduce subsequent relationships. A second advantage of binary matrices is that the components can be listed in any order in the matrix. In addition, the use of binary matrices forces the analyst to identify all supporting systems or components. This aids the analyst in developing fault trees, digraph matrices, and such techniques.

4.4 Graph-Based Analyses

The last class of analysis techniques is graph-based analyses. Graph-based analyses are comprehensive within a given set of boundary conditions and are used to represent the logical relationship among those components (or systems) whose failure can lead to a specific undesired event. These relationships are captured in the graphic model. All of the potential failure modes (within the scope of the analysis) are then identified by using computers to generate the combinations of component and human failures that contribute to the undesired event.

Advantages of this class of techniques include: (1) the ability to cover low-frequency events systematically, (2) the ability to deal with complex systems, (3) the ability to evaluate shared support systems, and (4) the ability to identify common-cause failures. Disadvantages of these techniques include: (1) their limited ability to analyze human interface, (2) their complexity, and (3) their expense when performed at a detailed level (probably the level needed for an ASI study).

Six methodologies were identified as graph-based analysis techniques:

(1) digraph matrix analysis

(2) event tree analysis

(3) fault tree analysis

(4) GO methodology analysis

(5) sneak-circuit analysis

(6) generic analysis

4.4.1 Digraph Matrix Analysis

Digraph matrix analysis (DMA) utilizes a success tree that includes all systems and/or components (elements) involved in an accident sequence. This success tree includes subsystems and support systems as elements. A binary matrix (known as an adjacency matrix) is produced from the success tree that contains information about the relationship between these elements. This binary matrix is then converted to a dual-digraph matrix by changing all "or" gates to "and" gates and "and" gates to "or" gates. Cutsets or failure combinations are then obtained from the dual digraph. The cutsets are then evaluated for systems interactions. The steps involved in performing a DMA are:

First, the analyst selects the combinations of systems of interest for a detailed evaluation. (This is equivalent to the PRA event tree analysis designed to find accident sequences.)

Next, the analyst constructs a single-digraph model for each accident sequence. This is a graphic approach that allows the analyst to develop a binary matrix (adjacency matrix) of elements that have direct influence on an element of higher order.

The analyst can then partition digraph models into independent subdigraphs to find the cutsets. Computer codes are available that identify the cutsets.

Finally, the analyst can evaluate cutsets on the basis of probability and display answers for both top event and cutset probabilities.

Some advantages of a digraph matrix analysis include:

(1) The construction of the logic model is performed directly from plant schematics (piping and instrumentation diagrams, electrical schematics, safety logic diagrams, etc.). The resulting model can be overlaid on the plant schematics; thus, the model can be readily understood, reviewed, and corrected.

(2) The digraph can represent physical situations that are cyclic.

(3) DMA computer codes can process very large models. An entire accident sequence consisting of several safety systems and their support systems is modeled as a single digraph.

(4) The binary matrix indicates all levels of subordination, but only direct first-level relationships must be provided. Computer codes deduce any consequent levels of subordination.

(5) An element of the matrix can be any entity of interest (e.g., an entire system, a system function, component, or maintenance crew). Elements of any level of detail can be intermixed.

Disadvantages of a digraph matrix analysis include:

(1) There are few trained analysts and few available computer codes that can be used to develop and subsequently apply the analysis.

(2) For certain types of logic diagrams, the analyst's attempt to be more complete can lead to computer limitations.

4.4.2 Event Tree Analysis

Because nuclear power plant systems are so complex, it is not feasible to write down by inspection a listing of important accident sequences. Therefore, a systematic and orderly approach is required to properly understand and identify the many factors that could influence the course of potential accidents. This approach involves developing an event tree. An event tree is an inductive logic model that sequentially models the progression of events (both failure and success) from some initiating event to a series of logic consequences. An event tree begins with an initiating failure, and it maps out a sequence of events of the system level that forms a set of branches. Each of the branches represents a specific accident sequence. A complete event tree analysis requires the identification of all possible initiating events and the development of an event tree for each event.

Event trees are normally used to model events having binary failure states. These events usually correspond to total success or failure of a system. Event tree analysis is a useful tool for systems interaction analysis when used with other techniques such as fault tree analysis.

4.4.3 Fault Tree Analysis

Fault tree analysis is a deductive failure analysis that focuses on an undesired event and provides a method for determining causes of this event. The undesired event constitutes the top event in a fault tree diagram. Careful choice of the top event is important to the success of the analysis. A fault tree analysis describes an undesired state of the plant or system (usually an undesired state that is critical from a safety viewpoint) and analyzes the plant or system to find all credible ways in which the undesired event can occur. The fault tree is a graphic model of the combinations of faults that will result in the occurrence of the undesired event. The faults can depict hardware failure, human error, system failures, external events (e.g., earthquakes or internal fires), or other events that can lead to the undesired event.

A fault tree is not a model of all possible plant or system failures or all possible causes for failure. A fault tree is tailored to its top event and includes only those faults that contribute to the top event. The fault tree is not quantitative; however, the results can be evaluated quantitatively. In fact, the fault tree is a convenient model to quantify and, along with event trees, has formed the structure for almost all of the PRA studies performed for the nuclear industry. As a result, a large number of people in the nuclear industry are experienced in developing and/or using fault trees.

A formalized combination of event trees and fault tree analyses is called a cause-consequence analysis. The event trees are used to determine the sequence of events that can lead to the consequences of interest. Event trees are developed for several different initiating events (usually LOCAs and transients). The fault trees are then used to model the causes of the event sequences. The causes of the event sequence failures can be modeled as system failures or component failures. However, if failure data are lacking on the system level, the causes would be modeled on the component level where such data are usually available. Hence, the results of a cause-consequence analysis are both qualitative and quantitative.

Two advantages of performing a cause-consequence analysis are: (1) the method is better suited for identifying potential system dependencies on the component level than is the event tree alone and (2) for fault trees alone, the dependencies are shown on separate trees. However, the consequence diagram includes all of them within a single logic structure.

4.4.4 GO Methodology

The GO methodology is a success-oriented technique that is generally used for quantitative analyses. However, this methodology can be used to identify component failure combinations that can lead to system failure, and to construct event trees. Completed GO models resemble system schematic or process flow charts and tend to be more compact than equivalent fault tree models (albeit with correspondingly less failure mode information). Seventeen logical operators are used to model a process. From these models, functional, spatial, and induced human-system interactions can be identified.

Specific advantages of the GO methodology include: (1) The system models follow the normal process flow (as does a digraph matrix analysis), (2) Modeling of most component and system interactions and dependencies is explicit, (3) Models are compact and easy to validate, (4) Model evaluations can represent both success and failure states of systems, and (5) It is uniquely adaptable to analyses in which many levels of system availability are to be considered, since it has the ability to handle multiple system states (i.e., partial failure or degraded conditions can be modeled).

Disadvantages of the GO methodology include: (1) Fewer analysts are familiar with the GO methodology than with fault tree/event tree analyses and (2) The GO methodology has been used extensively for probabilistic studies of individual systems but has not been employed to any great extent as the primary technique for a full-scope PRA.

4.4.5 Sneak-Circuit Analysis

Sneak-circuit analyses are normally applied to electrical systems and were originally designed to identify unplanned modes of operation, unexplained problems, and unrepeatable anomalies. However, this type of analysis can also be applied to fluid systems, since fluid systems can be represented by electrical system analogs.

A sneak-circuit analysis will identify latent signal paths or circuit conditions in systems that may cause undesired events to occur, or may inhibit the occurrence of a desired function. The problems identified in the analysis are called sneak circuits and are characterized by their ability to escape detection during most standardized tests. In addition, sneak circuits are not dependent on component failures, although many erroneous responses of system failures occur because of component failures. Sneak circuits can be subdivided into four types:

(1) sneak paths, which cause current or energy to flow along unexpected paths

(2) sneak timing, which may cause or prevent the flow of current of energy to activate or inhibit a function at an unexpected time

(3) sneak indications, which may cause an ambiguous or false display of system operating conditions

(4) sneak labels, which may cause incorrect stimuli to be initiated through operator error

An advantage of sneak-circuit analyses is that problems caused by latent signal paths that are not contingent on component failures can be identified. These signal paths can cause undesired events to occur, or inhibit a desired function from occurring. The main disadvantages of sneak-circuit analyses are the lack of documentation explaining the methodology. Additionally, only one company was found that had experienced and qualified analysts able to perform such analyses.

4.4.6 Generic Analysis

A generic analysis reviews the basic events in each minimal cutset for susceptibilities to generic causes (dependencies). The minimal cutsets can be determined from fault tree analysis or similar analyses. When a generic cause is common to all members of a minimal cutset, and the location of the minimal cutset components offers no protection from that generic cause of failure, the minimal cutset is called a common-cause candidate (CCC). Generic causes for failure that are often considered in such analyses are:

(1) mechanical/thermal generic causes

impact
vibration
pressure
grit
moisture
stress
temperature
freezing

(2) electrical/radiation generic causes

electromagnegic interference
radiation damage
conducting medium
out-of-tolerance voltage
out-of-tolerance current

(3) chemical/miscellaneous generic causes

corrosion (acid)
corrosion (oxidation)
other chemical reactions
carbonization biological

(4) other common links

energy source
calibration
installations
maintenance
operator or operation
proximity
test procedure
energy flow paths

Although a major portion of this technique is qualitative, it follows an analysis procedure such as fault trees rather than preceding it, as other qualitative methods usually do. This approach differs from most common-cause analyses because it deals directly with the minimal cutsets instead of adding secondary failures to the logic model. Thus, only component failures that result in system failure are considered.

A generic analysis is a helpful methodical way to identify spatial systems interactions. It has been implemented in a number of computer programs and is extensively used in dependent-failure analyses in the nuclear industry.

4.5 Oak Ridge National Laboratory's Conclusions and Recommendations

ORNL concluded (NRC, NUREG/CR-4261) that there are many different and varied methodologies available that can identify systems interactions. However, no one methodology by itself can adequately identify functional, spatial, and induced human-intervention-coupled systems interactions. Therefore, several different analysis techniques should be used.

Determining the most appropriate combination of analysis techniques for identifying systems interactions requires consideration of several factors—time, scope, costs, benefits, and such. However, a review of the methodologies available made several insights apparent. First, any systems interaction program should utilize operating experience reviews, design reviews, and preoperational testing. These three methodologies are already required to be performed, and minimal modifications to the existing programs could be required to identify all three types of systems interactions. Second, expanding the scope of PRAs to include the identification of systems interactions should simplify the problem (with respect to starting an independent evaluation), since the analysts would already be familiar with the systems and their responses. Last, the resulting combination of methodologies must be able to adequately identify all three types of systems interactions—spatial, functional, and induced human-intervention coupled.

The manpower required to perform a PRA that includes a systems interaction analysis should be within the bounds provided in the "PRA Procedures Guide" (NUREG/CR-2300). The "PRA Procedures Guide" indicates that 19 to 38 man-months are required for sequence and system modeling, with another 18 to 24 man-months required for external event analysis. It is not possible to separate the amount of modeling required for independent and dependent failure modes. However, it should be recognized that to do an adequate job of analyzing systems interactions requires experienced analysts and adequate time to examine and incorporate all the potential dependencies that can arise from systems interactions. For this reason, the upper estimates provided in the guide may be more appropriate to ensure that adequate analysis of systems interactions can be included.

In summary, the methodologies discussed in this report can be applied to identify systems interactions. However, the problem in conducting a systems interaction analysis is not a problem with methodology as much as it is a problem with scope and level of detail.

4.6 Staff Conclusions

All methods appear to have some advantages and disadvantages. The major conclusions based on the above review are:

(1) The global application of any method or combination of methods is costly.

(2) The choice of method may not be as important as the scope and depth of the study performed.

(3) It is, therefore, probably most cost effective to limit studies to specific areas and to increase the level of detail in modeling and analysis in those areas.

5 DESCRIPTION OF RESULTS AND STAFF CONCLUSIONS

NRC defined a number of tasks in the revised Task Action Plan (TAP) for USI A-17 (NUREG-0649) to address the area of systems interactions. Although all the tasks defined in the TAP were completed, this section of the report is not organized into the same set of tasks. Rather, this report is organized around the task results and recommendations which were then used as input for the technical resolution of USI A-17.

The tasks outlined for studying the A-17 issue were developed to utilize a combination of existing information, ongoing work, and new work with the objective of focusing the various efforts to resolve the generic issue as defined in the revised TAP scope and definitions.

5.1 Utility Studies of Systems Interactions

A number of utilities performed systems interaction studies of their own plant(s) as part of the operating license review process. The staff has considered some of these programs in the resolution of A-17.

5.1.1 Zion Nuclear Plant Study

In a June 17, 1977 letter, the NRC Advisory Committee on Reactor Safeguards (ACRS) recommended that Commonwealth Edison conduct a study of possible systems interactions related to the Zion Nuclear Plant's shutdown heat removal capability. The ACRS also referenced additional guidance contained in its letter of November 8, 1974. Possible approaches to a systems interaction study were discussed with a number of consultants and with the NRC staff.

As a followup to these discussions, Commonwealth Edison performed an experience survey utilizing LERs (Commonwealth Edison Company, June 16, 1978). The study was divided into three phases. Phase 1 consisted of a review of more than 9000 LERs which were generated in the operation of U.S. commercial nuclear power plants between 1969 and 1977.

The LERs were used to identify events that have occurred at operating power plants that involve systems interactions which had a potential for reducing the effectiveness of shutdown cooling systems under nonaccident conditions. The review covered not only four-loop PWRs but all pressurized-water, boiling-water, and gas-cooled reactor LERs.

The Zion screening criteria as quoted from the report were formulated to include the following types of events:

- Events which demonstrated that the action of any system degraded or resulted in loss of the effectiveness of any of the following systems:

  reactor coolant

  instrumentation power

  residual heat removal

  chemical and volume control

  component cooling

  auxiliary feedwater

  service water

  portions of main steam

  auxiliary power
- The action which initiated the event could have been a normal control function, a malfunction, or operator induced. The single-failure criterion was not

extended; however, a detailed review was made to determine its applicability.

- As an example, the failure of an RHR [residual heat removal] pump to start due to an electrical fault in the motor would not have been considered a systems interaction. However, if the motor failure was due to excessive humidity and temperature in the RHR cubicle, it was considered an undesirable systems interaction.
- It was noted that personnel action can result in maintenance errors or operator errors which will have a direct effect on a system or piece of equipment, but this was not considered to be an interaction between systems. For example, the loss of an instrument bus due to placing a grounded test instrument on the bus results in the loss of a large amount of equipment, as expected. If, alternatively, the load from the bus was not correctly shed from the electrical system and resulted in faults in other parts of the electrical system, it would be considered an undesirable interaction.

The second phase of the study, which was conducted by Fluor Pioneer, Inc., involved detailed analysis and investigations of each identified event to determine how and why the event occurred and its effect on the originating plant.

For the third phase, an assessment was made of the possibility of the occurrence of an identical or similar event at the Zion plant. If it was found that a similar event could occur at the Zion plant, corrective action options were evaluated. The evaluation criteria included consideration of safety, constructability, operability, maintainability, and cost. While the range of possible corrective options was being review and analyzed, the utility assessed the benefits of the options.

On the basis of the evaluation criteria and the benefits assessment, the utility concluded that for Zion, the generic studies requested by the NRC and the implementation of conclusions and recommendations involving such items as fire protection, pipe break, and low-temperature primary system overpressure have resulted in modifications that substantially reduce the possibility of the occurrence of a majority of the events studied. In addition, about five specific investigations and/or plant modifications were recommended in the study.

It should be noted that there is not a good correlation between the LERs highlighted by Commonwealth Edison and the LERs contained in the ORNL review of operating experience (see Section 5.4). To some degree, this occurred because of differences in definitions of what constitutes an adverse systems interaction event. Nevertheless, the Zion study was reviewed by ORNL as part of the review of operating experience (see Section 5.4) for possible SI events which met the definition offered in the current A-17 Task Action Plan.

5.1.2 Diablo Canyon Nuclear Power Plant Seismically Induced Systems Interaction Program

Pacific Gas and Electric Co. (PG&E) established a systems interaction program (PG&E, May 7, 1984) which was intended to establish confidence that if a seismic event of the severity of the postulated Hosgri event* occurred, structures and equipment important to safety will not be prevented from fulfilling their safety functions because of seismically induced failure or motion of structures or equipment not related to safety. Also, the Seismically Induced Systems Interaction Program (SISIP) was instituted to establish confidence that safety-related systems will not fail to meet the single-failure criterion because of seismically induced interactions.

PG&E defined the following two terms to clarify its postulation of potential systems interactions:

(1) *Targets* are (a) structures and equipment needed to take the plant to safe shutdown and maintain it at safe shutdown; (b) certain accident-mitigating systems such as containment isolation, main steam isolation, and containment spray; and (c) the manual fire suppression equipment.

(2) *Sources* are any other equipment whose seismically induced failure or motion could interact with a target and prevent or inhibit a target from accomplishing its safety function.

On the basis of these definitions, a large number of potential interactions were postulated. PG&E utilized four ways to resolve postulated interactions. These were: (1) resolution by field inspection in which the interaction team could by inspection or simple field analysis show that either the source would not fail, the occurrence of the interaction was not credible, or the consequences of the interaction, if it occurred, would not adversely affect target operations; (2) resolution by engineering analysis in which PG&E could show either that the interactions would not occur or, if they did occur, that the consequences would not affect target operations; (3) resolution by an expedient modification in which PG&E decided it was more cost effective to resolve the interaction by modifying the plant than to justify the configuration by analysis; and (4) resolution by necessary modification in which further analysis showed that plant modification is the only means for resolving the interaction. Because the last two involved plant modification, PG&E combined resolutions 3 and 4 and only reported three resolution groups.

*The Diablo Canyon seismic design basis was upgraded after the potential for severe earthquakes originating from the Hosgri Fault (a branch of the San Andreas Fault) was reappraised.

The problem in assessing the Diablo Canyon program comes from the fact that the safety significance of the modifications (both expedient and necessary) cannot be readily established.

Information developed as a result of this program has been utilized in the A-17 program (see Section 5.6).

5.1.3 Indian Point Station, Unit 3 Utility Study

The Indian Point Station, Unit 3 (IP3) systems interaction report was prepared by the Power Authority of the State of New York (PASNY, November 1983) in conjunction with Ebasco Services Inc. and consists of 25 volumes. The objectives of this study were: (1) to develop a methodology and evaluation criteria to be used to identify and evaluate systems interactions and (2) to apply these criteria to a systems interaction review of 23 identified systems.

For purposes of this study, the utility decided to define systems interactions as those events that affect the safety of the plant by one system acting on one or more other systems in a manner not intended by design, with emphasis on interactions in which systems not related to safety (non-safety systems) act on safety-related systems.

The analysis then involved: (1) the systematic search for hidden or inadequately analyzed interconnections or couplings that link safety and non-safety systems in the reactor plant and (2) the evaluation of the effects of a non-safety-system failure (or maloperation) propagated into the safety system by such interconnections/couplings. (*Note:* It was assumed for purposes of that study that the safety systems satisfied the single-failure criterion and that redundant safety systems do not possess dependencies so that one malfunction cannot disable redundant safety systems.)

On the basis of these premises, a number of potentially adverse interactions between non-safety systems and safety systems were identified through a series of dependency tables, logic diagrams, failure mode and effect analysis, event trees/fault trees, review of previous reports, and walkthroughs (onsite reviews). Only one of these resulted in a reportable condition (LER) as determined by the licensee. This involved a nonseismic pipe connection to a seismic system with inadequate isolation. The resolution involved maintaining a manual isolation valve in a closed position.

A number of potential adverse systems interactions were identified and resolved. The utility concluded that the program increased the level of safety for IP3; however, the contribution to core damage probability from the postulated non-connected seismically initiated systems interactions was less than 4 percent of the overall core-melt frequency at the design-basis earthquake level (Atomic Industrial Forum, Inc., October 8, 1985). Information developed as a result of this program has been utilized in the A-17 program (see Section 5.6).

5.1.4 Midland Nuclear Power Plant, Units 1 and 2 Program

In January 1983, Consumers Power Company (CPCo) initiated a program to address systems interactions (CPCo, June 6, 1983). The program consisted of three parts to address the three classes of systems interaction: functional, spatial, and induced human-intervention-coupled.

The functional interaction portion of the program was to rely heavily on existing plant procedures for design control and preoperational checkout and testing. The design control task involved an interdisciplinary review of plant design to ensure that potential interactions generated by the interface between activities of the various engineering groups were identified and corrected. The program was to include preoperational testing to demonstrate the capability of required safety systems to meet design performance and safety criteria. Additional methods for use in identifying and evaluating functional dependencies included probabilistic risk assessment (PRA), control systems failure evaluation, and licensing department reviews of industry operating experience through nuclear steam supply system (NSSS) vendor reports, Institute of Nuclear Power Operations (INPO) reports, and licensee event reports (LERs).

Onsite reviews (walkthroughs) of safety-related structures, systems, and components were employed to address spatially coupled SIs. These onsite reviews identified potential interactions arising from proximity, location of non-seismically qualified equipment over safety equipment, high-energy line break (HELB), internal missiles, and flooding. Additional reviews also addressed the areas of pipe stress, fire protection, and thermal growth for potential spatial interactions. CPCo was incorporating many inplace programs into the spatial SI studies to avoid unnecessary duplication of efforts. For example, a program had been in place to address the seismic "Class II over Class I" issue per Regulatory Guide 1.29 requirements.

To address the induced human-intervention-coupled class of ASIs, the CPCo SI program incorporated design reviews and other tasks implemented to improve operator response to plant events. Other tasks included a human factors review of control room design and procedures, review of control room operating experience, and increased operator training, including the use of simulators.

Although the Midland project has been terminated, the available results, particularly with regard to the seismically induced systems interactions have been utilized in the A-17 program (see Section 5.6).

5.1.5 Staff Conclusions

Although the licensee programs discussed above contributed to an increase in safety, the utilities did not perceive the amount of increase to be significant. What was clear was that each program cost the utility millions of dollars.

On the basis of these preliminary conclusions, the staff defined a task to examine the three utility studies (Diablo Canyon, Indian Point 3, and Midland) in greater detail to attempt to better optimize the cost/benefit ratio.

For the results and conclusions of this additional work, refer to Section 5.6.

5.2 Other Related Studies, Programs, and Issues

As part of earlier NRC programs to address the issue of systems interactions, national laboratories did a number of studies. In addition, many other ongoing NRC programs are directly related to the work on A-17.

5.2.1 Sandia Laboratory Study of Watts Bar Nuclear Plant

From 1978 through 1980, NRC contracted with Sandia Laboratory to utilize a method of reviewing nuclear power plant systems for potential interactions that was different from the review process being used by NRC in its Standard Review Plan (SRP) (NUREG-0800).

The method was the fault tree method using the Set Equation Transformation Systems (SETS) computer code for evaluating the fault trees to identify the potentially interactive cutsets. The resulting report (NUREG/CR-1321), also assessed the SRP to show where the potential interactions revealed by this independent method may not be specifically discussed in the SRP sections on review, review procedures, or acceptance criteria.

The scope of the study was restricted to allow the methodology to be developed and demonstrated in a timely fashion. The interactions addressed were limited to those arising from physical connections and common locations.

Three plant functions were included: decay heat removal, reactor subcriticality, and reactor coolant pressure boundary integrity. The range of environmental conditions, plant modes, and plant occurrences was also restricted.

The first step of the study was to develop a methodology for reviewing the SRP that could also be used to evaluate specific facilities. The underlying premise of the methodology is that potential interactions can effectively be found by identifying the commonalities between systems.

The methodology uses fault trees to model plant functions from which the analysis is performed. The SETS computer code and subsequent analysis identifies and highlights the important commonalities based on input plant information. Commonalities found between components whose unavailability could lead to loss or significant degradation of an important plant function are pursued in greater detail.

The principal product of this study was to be the development of a systematic and disciplined methodology for the identification and evaluation of a range of potential systems interactions.

The methodology was applied to a facility that had recently gone through the licensing process (Watts Bar) to achieve two goals: (1) to provide a basis for comparison to the SRP-type review and (2) to demonstrate the methodology itself. In general, it was concluded that application of the methodology should not be limited to those systems explicitly identified in the SRP as safety related. In addition to this general conclusion, several weaknesses were identified in the SRP. These met all of the following criteria: (1) A potential cause of an interaction could be identified, (2) If an interaction occurred, it would increase the likelihood of core damage, and (3) The potential cause of an interaction was not explicitly covered in the SRP.

The weakness identified was the absence of explicit assurances in the SRP or its supporting documents that: (1) the reactor coolant pressure boundary integrity will not be lost as a result of interactions stemming from a common location or common actuation of the pressurizer power-operated relief valves and their isolation valves, (2) the decay heat removal function will not be lost as a result of interactions stemming from a common location or common cooling between trains of the auxiliary feedwater system, (3) positive pressure control will not be lost as a result of interactions stemming from common power sources between pressurizer heater channels, and (4) the inventory makeup necessary to maintain decay heat removal will not be lost as a result of interactions stemming from the common location of the refueling water storage tank output valves.

Although the Sandia work was considered a major portion (Phase I) of the NRC program to address systems interactions, subsequent revision to the A-17 Task Action Plan somewhat deemphasized this work by Sandia because ongoing PRA work (see Section 5.5) and the Brookhaven

application on Indian Point 3 (see Section 5.3) were similar to the Sandia work.

The staff concluded that fault trees and other PRA techniques could be used in the investigation of systems interactions. For more on PRA and its relationship to systems interactions see Section 5.5.

5.2.2 Systems Interactions State-of-the-Art Reviews

The NRC requested three national laboratories to conduct a review of the state of the art in the area of systems interactions in 1980.

Each laboratory produced a report as follows:

- NUREG/CR-1859, "Systems Interaction: State-of-the-Art Review and Methods Evaluation," prepared for NRC by Lawrence Livermore National Laboratory, January 1981
- NUREG/CR-1896, "Review of Systems Interactions Methodologies," prepared for NRC by Battelle Columbus Laboratories, January 1981
- NUREG/CR-1901, "Review and Evaluation of Systems Interaction Methods," prepared for NRC by Brookhaven National Laboratory, January 1981

The broad objective of these reports was to develop methods that held the best potential for further development and near-term use by industry and NRC on systems interaction evaluations for future as well as operating plants. More specifically, the objectives of the work were to include:

(1) development of a definition of systems interaction and corresponding safety failure criteria

(2) review and assessment of current systematic methods that have been used, or are considered feasible for use, on any complex system comparable to a light-water reactor plant

(3) provision of an inventory of a range of systems interaction scenarios with emphasis on actual operating experience to

  (a) better focus on the definition of systems interaction

  (b) serve as a basis for evaluating the ability of the various methodologies to predict these examples

(4) recommendation of a methodology or alternatives that have the best potential for further development and near-term use by industry and the NRC on systems interaction evaluations

(5) application of candidate methodologies to actual occurrences to demonstrate their ability to predict systems interactions effects

The staff concluded that the recommendations of the three studies would be considered as part of the A-17 resolution if a study was required of all utilities. For more on state of the art see Section 4, on methods.

5.2.3 Advisory Committee on Reactor Safeguards Concerns

As stated in the introduction to this report (Section 1), the ACRS was credited with identifying the original concerns. In addition to the original identification, the ACRS has also been instrumental in subsequent investigations in the area of systems interactions. The utility studies at Zion, Indian Point, and Diablo Canyon were all the subject of ACRS discussions (see Sections 5.1.1, 5.1.2, and 5.1.3, respectively).

In addition, in September 1979, ACRS consultants completed NUREG-0572, "Review of Licensee Event Reports (1976-1978)," in which they identified a class of events as "systems interaction." The report concluded that a number of LERs reveal unusual and often unpredicted interactions among various plant systems. The report went on to state that it is not surprising that interactions exist, since a nuclear power plant is an extensive and complex facility; however, the nature of these interactions is often quite unexpected. When interactions involve degraded performance of systems required for vital functions, such as shutdown heat removal, there can be significant safety implications. The ACRS acknowledged that the NRC staff is studying systems interactions through Generic Task No. A-17.

Regarding the use of the LERs the report stated:

> Redundancy and defense in depth are widely used in essential reactor systems to assure their availability. Implicit in such usage is the assumption that a high degree of independence exists between the redundant elements (or the various echelons of defense in depth). Occasionally an LER discloses an unintentional or previously unrecognized interdependence between such elements. In such cases, interdependence reflects one type of systems interaction problem. Although there are few LERs that directly reveal such problems, there are many that hint at deficiencies of this nature. Because of the potentially serious implications of such situations, more attention needs to be directed to seeking them out. Careful review of

LERs can uncover such design errors, if they are consciously sought out.

Reference is then made to three sections of the Appendix that include some examples. The first section is entitled "Systems Interactions" and describes three separate events, all of which involve the plant electrical systems. These specific events do not meet the definition and screening criteria of the current TAP for A-17 and therefore were not included in the ORNL list. However, it should be noted that the ORNL LER study (see Section 5.4) does highlight the area of electrical systems as a potentially significant area from the viewpoint of adverse systems interactions.

The second section is entitled "Failures That Indicate Interdependence of Redundant Elements" and describes four separate events.

- The first of these events involves redundant battery chargers for a fire pump and would not meet the TAP definition of systems interaction because (1) the fire system is not typically a system needed to achieve and maintain safe shutdown and (2) the chargers were not truly redundant in the same sense of engineered safety features (ESF) Trains A and B equipment.
- The second event involves the loss of both makeup pumps at Davis-Besse Nuclear Power Station. It is the staff's understanding that the makeup pumps at Davis-Besse are not considered safety related and therefore such an event does not meet the TAP definition which includes degradation of safety-related equipment.
- The third event involves a boron dilution event at Surry Power Station, Unit 2. Although this event involved some unexpected interaction between systems and temporarily blinded the operator, none of the systems involved were safety related and the consequences were very minimal. The consequences were limited by the inherent design of the system because the system could only deliver a maximum of 150 gpm which could not reduce the boron concentration below acceptable levels between the required sampling intervals.
- The fourth event occurred at Three Mile Island Nuclear Station, Unit 1 (TMI-1) and involves a miscalibration of all four power range flux monitors as a result of a faulty test pressure transmitter. Although this event does demonstrate a common-cause effect or dependency, it is not an adverse systems interaction but rather fits in the class of other common-cause failures according to the TAP definitions.

The third section of the Appendix is entitled "Adverse Interactions of Safety System and the Influence of Human Errors" and involves one event at Arkansas Nuclear One, Units 1 and 2. The event involved a number of adverse systems interaction aspects and has also been included in the list of events compiled by ORNL. It was noted that the ACRS report and the ORNL report both seem to indicate the potential for adverse systems interactions in the highly complicated electrical power supply and its control systems.

Some other ACRS questions and concerns were documented in the form of recommendations to the staff and, in at least three cited utility studies, in the form of guidance to the utilities. Of particular note is the guidance in the ACRS October 12, 1979 letter on Indian Point Station, Unit 3. This guidance was issued in response to questions about what constitutes "reasonably appropriate study of systems interactions at Indian Point 3." In that letter, the ACRS expressed specific concerns in two separate areas. One area involved "possibility of systems interactions within an interconnected electrical and mechanical complex." The ACRS expressed concerns with the consideration of other than usually assumed failures, that is, partly failed or other than normally assumed failed states. The ACRS was also concerned that this type of failure would probably not be revealed by LERs and that a failure mode and effects analysis (FMEA) was required. The second area involved "possibility of interactions between non-connected systems due to the physical arrangement or disposition of equipment." Again, ACRS expressed its belief that LERs would not reveal these unique interactions and recommended a physical inspection of the plant and the "formation of a small but competent interdisciplinary team."

Over the years, ACRS has stated its belief that the staff should require all utilities to do a systems interaction type of analysis and that because such an analysis could be done with little NRC guidance, the requirement should be issued without further investigations and delay. Over the same time period, the NRC staff took the position that such a general requirement would not resolve the issue because of the lack of any consensus about what, if anything, needed to be done. The staff continued to pursue an approach for resolution, searching for an overall cure in the form of what "acceptable" methods should be applied. At this time and on the basis of further review, the staff has concluded that the concerns expressed by the ACRS in the October 12, 1979 letter are some of the central issues that need to be addressed by the resolution of USI A-17.

Regarding the ACRS report (NUREG-0572), the staff concluded that although many of the events cited there were not "adverse systems interactions" as defined in the present A-17 TAP, the overall conclusions of the report regarding power systems and their control remain valid. In addition, the general type of concerns expressed in the report regarding compromise in redundancy and/or levels of defense in depth also remain valid and have been

explored further in the work on A-17 (see Sections 3, 5.4, and 5.6).

On the basis of further review, the staff concludes that (1) walkthroughs similar to walkthroughs suggested by ACRS but with much narrower focus could achieve a cost-effective safety improvement at some plants and (2) although the pursuit of so-called partial failures (leading to functionally coupled ASIs) may uncover uniquely plant-specific scenarios, there is not sufficient evidence to show that they are safety significant enough to justify the type of analyses required to uncover them. In addition, with respect to the failure modes of control systems, USI A-47 (NUREG-0649) is also addressing this area. The staff will provide information to the utilities regarding the types of problems uncovered in the electrical power systems (one area that was highlighted for partial failure investigation), and other types of problems regarding failure modes (see Section 5.4). The ACRS has also expressed concern (ACRS, May 13, 1986) over the scope of the A-17 program. This was discussed previously in Sections 3.4.2 and 3.4.3.

5.2.4 Post-TMI-2 Actions, Including Human Factors Issues

After the accident at TMI-2, a significant amount of attention was focused on the operators and on so-called human factors issues. The USI A-17 TAP (NUREG-0649) recognizes all the activity in this area and attempts to limit the overlap of concerns between the systems interaction issue and those other efforts. As a result, the A-17 studies focused on the hardware or hardwired aspects of the operators' indication systems and left the human engineering and, specifically operator error, to NUREG-0985, "Human Factors Program Plan."

The A-17 area of concern was, therefore, limited to the possibility of misleading an operator by means of malfunction (that was not readily detectable) in a plant indication system during an event. This was the induced human-intervention-coupled adverse systems interaction referred to in Section 3. After the accident at TMI-2, a significant amount of attention was focused on this aspect of plant indications. Specifically, requirements were implemented through NUREG-0737, Supplement 1, which improved monitoring information (Regulatory Guide 1.97, "Instrumentation for Light-Water-Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident," and added operator aids such as the safety parameter display system.

The staff engaged in the A-17 program concluded that plant personnel (operators, maintenance personnel, test technicians, etc.) can have a significant impact on plant response, both negative and positive; however, events initiated by personnel error should not be classified as systems interactions. The potential for indication systems misleading the operator has been reduced by other actions mentioned above. Furthermore, the actions in the area of operator information and training should improve response to and recovery from ASI-type events.

5.2.5 NRC Office for Analysis and Evaluation of Operational Data Activities

As a result of the TMI-2 accident, the NRC formed the Office for Analysis and Evaluation of Operational Data (AEOD) with the intent to pay closer attention to current operating experience and to learn from past experience. AEOD has reported on a number of events that meet the TAP definition of systems interaction, although the events may not have been labeled "systems interactions." In some cases, the staff has formulated new generic issues based on the AEOD reports (see Section 5.2.7). As part of the resolution of A-17, the staff took a separate look at operating experience. The AEOD reports were one of the reference sources for this work (see NUREG/CR-3922 and Section 5.4 for more information on operating events).

The staff has concluded that since the formation of AEOD, operating events at plants receive much greater scrutiny than at the time when the systems interaction issue first surfaced. It should be recognized that the implementation by NRC and the industry, through organizations such as INPO, of such scrutinizing analyses addresses some concerns that could be called SIs and as such contributes to a reduction in concerns with systems interaction.

5.2.6 Office of Inspection and Enforcement Activities

The former NRC Office of Inspection and Enforcement (IE) had the responsibility for notifying all utilities about significant operating events through a system of bulletins and information notices. Several of the events that were screened from the operating experience, by the work on A-17, were the subject of an IE bulletin or notice. In those cases, this information was included as a reference source (see NUREG/CR-3922 for more information). In addition, as part of the decisionmaking process to possibly implement new requirements, those regulatory actions already required by IE were considered (for more information see Section 5.4).

Over the years, IE has notified the industry about significant operating occurrences. In some cases, the occurrences involve systems interactions. As was concluded for AEOD, the staff concludes that the IE mechanisms of bulletins and notices addressed significant experience, including systems interactions.

5.2.7 Other Generic Issues

In November 1983, the NRC published NUREG–0933, "A Prioritization of Generic Safety Issues." The report presents the priority rankings for a number of generic safety issues related to nuclear power plants. The purpose of these rankings is to assist in the timely and efficient allocation of NRC resources for the resolution of those safety issues that have a significant potential for reducing risk.

The prioritized issues include TMI Action Plan items under development; previously proposed issues covered by task action plans, except issues designated as unresolved safety issues (USIs) which had already been assigned high priority; and newly proposed issues.

The safety priorities, ranked as high, medium, low, and drop, have been assigned on the basis of risk significance estimates, the ratio of risk to costs, and other impacts estimated to result if resolution of the safety issues were implemented.

A number of the issues identified in NUREG–0933 can be called adverse systems interactions and, therefore, there is significant overlap between some issues listed there and the general categories resulting from the ORNL experience search (Section 5.4). This could be expected since the NUREG–0933 issues often arise from the same sources that ORNL used (e.g., LERs and AEOD reports). In some cases, a potential area of concern highlighted from an A–17 systems interaction perspective will have been cited, and possibly addressed, but on a more specific basis.

The resolution of A–17 has considered the safety priority ranking given to the corresponding issues (when available). The A–17 resolution then also recommends further action if necessary (for more information see Section 5.4).

Three issues included in NUREG–0933 warrant special discussion: Issue II.C.3, "Systems Interactions"; Issue C–13, "Non-random Failures"; and Generic Issue 77, "Flooding of Safety Equipment Compartments by Backflow Through Floor Drains." As stated in the TMI Action Plan, the purpose of Issue II.C.3 was "to coordinate and expand ongoing staff work on systems interaction (USI A–17) so as to incorporate it into an integrated plan for addressing the broader question of system reliability in conjunction with IREP [Interim Reliability Evaluation Program] and other efforts."

When the A–17 Task Action Plan was revised in January 1984, it was decided to include in issue A–17 the activities described under Issue II.C.3.

Issue C–13, "Non-random Failures," is an issue that was credited to ACRS in NUREG–0471. Although this issue was formerly referred to as "common mode failure of identical components exposed to identical or nearly identical conditions or environments" (as evidenced by reference to issues such as A–9, A–30, A–35, B–56, and B–57), it was expanded to include other types of failures and, as a result, a reference to USI A–17 is made in NUREG–0933. It should, therefore, be kept clear that the term "non-random failures" can include more than "systems interactions" and that a resolution of A–17 does not resolve all non-random failures (for additional information see Section 3).

GI–77 was given a high priority and was also qualified insofar as the lack of plant-specific details. In this regard, the group studying the resolution of USI A–17 considered these in its resolution.

The mechanism in place for identifying and prioritizing generic safety issues provides an avenue for handling all types of issues, including systems interaction-type issues. On the basis of the treatment of a general type of issue such as C-13, that is by handling it as a class and dealing with individual identified parts, the staff concludes that this is the best mechanism for dealing with any remaining or future SI concerns after the resolution of A–17. This is consistent with the need to clearly define any proposed safety issue in order to prioritize it.

5.2.8 Other Unresolved Safety Issues

The Task Action Plan for USI A–17 acknowledges that a relationship can exist with USI A–47, "Safety Implications of Control Systems" (NUREG–0649). This is primarily based on the understanding that control systems do interact with many plant systems and, therefore, if the control systems interactions lead to possible degradations in safety systems, such a concern could also be labeled an adverse systems interaction.

As the resolution of A–17 progressed, a close relationship between A–46 (NUREG–0649) and part of A–17 was acknowledged. Part of A–17 deals with possible seismic-induced spatial interactions between the non-seismic structures, systems, and components and the seismic structures, systems, and components. A–46 deals with the seismic qualification of certain equipment in older plants. The resolution of A–17 reflects this relationship.

Although USI A–45, "Shutdown Decay Heat Removal Requirements" (NUREG–0649) is not directly related to A–17, it is recognized that if the resolution of A–45 were to be an independent shutdown system, then such a resolution could substantially reduce the safety benefit of pursuing some ASIs.

As the resolution of A–17 has progressed to the point of focusing on certain areas, the relationships to other unresolved safety issues have been considered. The proposed

resolution of A–17 acknowledges relationships with USI A–45, USI A–46, and USI A–47.

5.2.9 Systematic Evaluation Program

The Systematic Evaluation Program (SEP) was initiated by the NRC to review the designs of older operating nuclear reactor plants to reconfirm and document their safety. The review provided (1) an assessment of the significance of differences between current technical positions on safety issues and those that existed when a particular plant was licensed, (2) a basis for deciding how these differences should be resolved in an integrated plant review, and (3) a documented evaluation of plant safety.

The review focused on 137 different "topic" areas (NUREG–0824). Although topics that were being reviewed under other programs, such as unresolved safety issues, were generally deleted from consideration in the SEP, some topics that were evaluated under the SEP are related to USI A–17. Therefore, the information developed in these topic areas was used in the A–17 study.

Of specific applicability were topics that were related to potential spatially coupled interactions.

These topics included:

- III-4.C Internally Generated Missiles
- III-5.A Effects of Pipe Break on Structures, Systems, and Components Inside Containment
- III-5.B Pipe Break Outside Containment

On the basis of its review of the general SEP findings on these topics (SECY-84-133), the staff concluded that:

(1) Plants typically provide significant protection against internally generated missiles.

(2) The flooding reviews performed in response to the Atomic Energy Commission (AEC) generic letter of September 26, 1972, may not have adequately covered some significant areas of concern.

This information was used to develop the focus of spatially coupled ASIs (see Section 5.6).

5.2.10 Standard Review Plan

The Commission's Standard Review Plan (SRP) (NUREG–0800) is the document that defines the acceptance criteria and review guidance used in the licensing process. The SRP has evolved over a number of years and has typically addressed areas of concern that can be considered adverse systems interactions.

One alternative considered in the A–17 program was the possibility of revising the SRP or related guidance documents such as regulatory guides to improve the evaluation of ASIs for future plant reviews. Some of the SRP sections that already address systems interaction concerns are listed in Table 3.

5.2.11 NRC's Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants

The NRC has published a policy to resolve safety issues related to reactor accidents more severe than design-basis accidents (NUREG–1070). Its main focus is on the criteria and procedures the Commission intends to use to certify new standard designs for nuclear power plants; however, it also provides guidance on decision and analytical procedures for the resolution of severe-accident issues for *other* classes of future plants and for existing plants (operating reactors and plants under construction which have applied for operating licenses). Severe nuclear accidents are those during which substantial damage is done to the reactor core, whether or not there are serious offsite consequences. Specifically the policy states:

> The Commission plans to formulate an integrated systematic approach to an examination of each nuclear power plant now operating or under construction for possible risk contributors (sometimes called "outliers") that might be plant specific and might be missed absent a systematic search.

The investigation into USI A–17, "Systems Interactions," highlighted a number of nuclear power plant systems or areas that appear to be the ones that are most likely to contain potential adverse systems interactions.

ASIs (both functionally coupled and spatially coupled) are most often caused by a design feature and/or a set of operating conditions peculiar to a particular plant; the consequences of an ASI are similarly determined by features peculiar to a particular plant and by the operator's response. Therefore, the resolution of A–17 can add to the formulation of any systematic evaluation of plants by providing aid in focusing the search for "outliers."

The areas of concern should include aspects that are discussed in the review of operating experience (see Section 5.4) and the review of seismic/spatially coupled SI programs (see Section 5.6). These are:

Table 3 SRP sections that deal with spatially and functionally coupled ASIs

Source	SRP Section(s) (NUREG–0800)
Spatially coupled ASIs	
Earthquake	3.6.2, 3.7.3, 3.9.2, 3.10, 3.11, 6.7, 9.1.3, 9.2.1-9.2.3, 9.2.6, 9.3.1, 9.3.3 9.3.5, 9.4.1-9.4.5, 10.3, 10.4.7, 10.4.9
Internal flood	3.4.1, 3.6.1, 9.3.3, 10.4.5
Internal fire	9.5.1
High-energy line break	3.6.1
Internal missiles	3.5.1.1-3.5.1.3, 9.1.4, 9.1.5
Functionally coupled ASIs	
Reactor protection/engineered safety features	7.2, 7.3
Safe shutdown	7.4
Control system	7.7
Station service water	9.2.2
Electric power systems	8.2, 8.3

Functionally Coupled ASIs

(1) electric power systems

(2) support systems

(3) overreliance on "fail-safe" design principles

(4) automatic actions with no preferred failure mode for all stations

(5) instrumentation and control power supplies

Spatially Coupled ASIs

(1) non–seismically qualified equipment effects on seismically qualified equipment

(2) internal plant flooding of safety-related equipment

5.2.12 Electric Power Research Institute's "Systems Interaction Identification Procedures"

As the technical resolution of USI A–17 was proceeding, the Electric Power Research Institute (EPRI) published EPRI NP-3834, Volumes 1–5, "Systems Interaction Identification Procedures." The staff asked Oak Ridge National Laboratory to review and assess the report's impact on the proposed resolution of USI A–17.

ORNL prepared a draft letter report dated February 10, 1986, concluding that both the proposed resolution for USI A–17 and the EPRI report explored numerous methodologies for identifying SIs. Both assessments conclude that no one methodology by itself can adequately identify functional, spatial, and induced human-intervention-coupled interactions. Therefore, several different analysis techniques could and should be used.

None of the methods presented in the EPRI assessment provided a quicker, easier, or more comprehensive means of identifying SIs. It was, therefore, concluded that the EPRI work brought no new information to the technical resolution of A–17.

5.3 Indian Point Station, Unit 3 Laboratory Demonstration Study

The staff initiated a laboratory demonstration study on the Indian Point 3 plant in mid-1983 through Brookhaven National Laboratory (BNL) and Lawrence Livermore National Laboratory (LLNL). The purpose of the study was to test and compare two potentially useful search methods and to compare the results with the study made by the utility. One method, the digraph matrix method, was applied by LLNL (for further information see NUREG/CR–2915, NUREG/CR–3593, NUREG/CR–4179, and LLNL's report of June 1983) and the other method, the interactive fault tree/failure mode and effect analysis, was applied by BNL (for further information see NUREG/CR–4207). Both studies concentrated on functionally coupled events.

By placing the same $1 million limit on each study, a meaningful comparison was anticipated.

There was no shortage of postulated intersystems dependencies that could be counted among the possible causes of safety malfunctions (NRC memorandum, March 20, 1985). From the impressively large number of cutsets generated by both groups of analysts, surprisingly few were safety significant.

Two cutsets contributed an estimated core damage frequency as high as 6×10^{-6} per reactor-year. The next likely cutset contribution was not greater than about 5×10^{-9} per reactor-year. The estimated frequencies of occurrence are highly biased by a pessimistic treatment of recovery actions available to the operators. Therefore, a very small fraction of the intersystems dependencies (which are possible to postulate) were even modestly safety significant.

The only safety-significant systems interaction highlighted by BNL was the unavailability of station battery 32 coincident with a safeguards systems actuation signal. This postulated event would leave both low-pressure injection recirculation pumps and other vital equipment unavailable. The loss of station battery 32 does not meet General Design Criterion (GDC) 35 (PASNY, LER 84-010-00, Docket 05000286, July 16, 1984). The postulated event could lead to core damage with an estimated frequency as high as 2×10^{-6} per reactor-year. The plant was modified and is not now vulnerable to this postulated event.

The first significant systems interaction highlighted by LLNL is a misalignment of preselected service water pumps and valves coincident with a loss of offsite power. Without rapid operator intervention, this postulated event could lead to a reactor coolant pump seal failure and hence a small LOCA and the loss of both core heat removal paths. The postulated event could lead to core damage with an estimated frequency as high as 4×10^{-6} per reactor-year. (*Note:* Although this was presented by LLNL as an adverse systems interaction, it does not truly fit the TAP definition.)

The other significant systems interaction highlighted by LLNL is a mechanical failure of the linkage within an interlocking breaker coincident with a loss of offsite power. Without rapid operator intervention, this postulated event could lead to damage to the emergency diesels and the subsequent failure of reactor coolant pump seals LOCA and loss of core-heat-removal paths. It was estimated that this postulated event could lead to core damage with a frequency only as high as 5×10^{-9} per reactor-year.

On the basis of the evaluation of the results of the two demonstration analyses, the staff concludes that there is no one method that alone could serve as a mechanism for resolving concerns regarding adverse systems interactions; in other words, there is no panacea. Significant resources were expended by the two national laboratories and the results indicate that few, if any, risk-significant, functionally coupled systems interactions were uncovered. At least one interaction was uncovered that violated the plant's design basis.

Furthermore, it appears that the ability of one method or another to identify certain systems interactions is often more a function of the skill of the analyst and the modeling detail, than it is a function of a particular method. From this, the staff concluded that there is no one solution to the systems interaction issue and, therefore, focused on a more limited type of analyses. The basis for this was the possibility that a more directed effort, by any number of methods, may be cost effective if it can be determined that certain areas are more prone to significant adverse systems interactions. To this end, the operating experience search was intended to highlight such areas (see Section 5.4). The Indian Point 3 demonstration did point out that the electrical power system, or portions of it, may be such an area. In particular, the study provides some indication that electrical distribution systems sometimes are not designed with total redundancy and channelization and usually include significant non-safety/safety interfaces which make them prone to hidden dependencies.

5.4 Search for Common-Cause Events in Operating Experience

As part of the effort to provide a more focused approach for the resolution of A-17, a set of tasks was defined to search operating experience in order to accumulate a data bank on the types of common-cause events of concern.

The major portion of this work was performed by ORNL, and a summary of ORNL's findings is included in NRC's document, NUREG/CR-3922.

The search emphasized events included in the LER files and involved a screening of those events based on the Task Action Plan definition. On the basis of the characteristics or attributes of the systems interaction events, a group of general categories of SI events was developed. In this manner, it was anticipated that generic areas of concern could be highlighted for possible further action. The results of the ORNL experience review indicate 23 general categories of events that have involved systems interactions. Those categories are listed in Table 4.

Table 4 Event categories involving systems interactions

Category No.	Title	No. of events
1	Adverse interactions between normal or offsite power systems and emergency power systems	34
2	Degradation of safety-related systems by vapor or gas intrusion	15
3	Degradation of safety-related components by fire-protection systems	10
4	Plant drain systems allow flooding of safety-related equipment	8
5	Loss of charging pumps due to volume control tank level instrumentation failures	6
6	Inadvertent ECCS/RHR pump suction transfer	4
7	HPSI/charging pumps overheat on low flow during safety injection	6
8	Level instrumentation degraded by HELB conditions	21
9	Loss of containment integrity from LOCA conditions during purge operations	10
10	HELB conditions degrading control systems	3
11	Auxiliary feedwater pump runout under steamline break conditions	2
12	Waterhammer events	4
13	Common support systems or cross-connects	18
14	Instrument power failures affecting safety systems	5
15	Inadequate cable separation	8
16	Safety-related cables unprotected from missiles generated from HVAC fans	3
17	Suppression pool swell	3
18	Scram discharge volume degradation	2
19	Induced human interactions	4
20	Functional dependencies from failures during seismic events	5
21	Spatial dependencies from failures during seismic events	13
22	Other functional dependencies	21
23	Other spatial dependencies	30

From these categories, the staff sought to establish possible safety significance (NUREG/CR–4261). This involved consideration of completed or ongoing related regulatory action. In this manner, it was anticipated that some areas would need no further action and any remaining areas of concern could then be evaluated for potential safety significance. In general, where extensive regulatory action was involved, such as IE bulletins or vendor notifications, the event and action taken could be shown to involve other than plant-specific features. The categories for which little regulatory action was taken often involved scenarios that were specific to a particular plant.

The staff then reviewed all the categories to see if some generic aspects related to adverse systems interaction concerns should be identified for action on all plants. The areas are summarized below on the basis of the type of coupling exhibited, that is, functional, spatial, or induced human intervention. ORNL also looked at the general

adequacy of the ongoing evaluations of operating experience.

5.4.1 Functionally Coupled Type

Electric Power System

For purposes of this work, the electric power system includes the offsite sources, the switchyard, the power distribution buses and breakers, onsite generating equipment, and the control power and logic to operate the breakers and start and load the diesel generators. Some of the lower voltage (typically 120-V ac and 125-V dc) power supply portion of the system is also dealt with under Section 5.4.1.5.

As outlined in NUREG/CR-3922 and NUREG/CR-4261, concerns were highlighted in the area of electric power systems in Categories 1 and 13 (Table 4). Three important factors appear to contribute to the possible significance of this area:

(1) It is one of the most (if not the most) extensive support systems in a plant. Power is supplied from various sources including the offsite network, the main plant turbine-generator, and in certain situations, the safety-related diesel generators. Power is then distributed to various items of equipment for normal plant control which are not related to safety, various engineered safety features equipment which is safety related, and various items of equipment for shutdown and decay heat removal.

(2) Given these system demands, the power system is therefore an inherently complex system. A large number of normal operating modes at the plant, as well as transient and accident situations, must be accommodated. Interfaces are created between redundant safety-related equipment as well as between non-safety-related equipment and the safety-related equipment. In addition, the power system itself relies on a number of other support systems such as HVAC and cooling water.

(3) Because of individual plant requirements and situations (a number of significant events occur when the system is in any abnormal temporary alignment), each power system tends to have some unique aspects. Very few specific ASIs can be stated to be generically applicable; however, the staff believes that general classes of electric power events can be potentially generic.

ORNL (NUREG/CR-3922 and NUREG/CR-4261) categorized the electric power system concerns into four areas:

(1) load sequencing/load shedding

(2) diesel generator failures caused by specific operating mode

(3) breaker failures due to loss of dc power

(4) failures that propagate between the safety-related portion and the non-safety-related portion of the power systems

With respect to these four areas of concern, the staff noted that although regulatory practice has allowed non-safety-related equipment to be powered from safety-related buses, this practice has created the potential for a number of undesirable interactions. In such situations, the isolation devices protect the safety-related equipment. These isolation devices have been the subject of much concern, both in the main power supply area (such as breakers that open on fault current or "accident" signals) and in the instrumentation and control power supply area (such as isolation transformers and other devices). In some cases, the "isolation" devices do not isolate the full range of undesirable events. In addition, there are other concerns that the investigation into the A-17 issue has focused on. The ASIs of note involve scenarios in which a non-safety- related load is supplied by a safety-related bus and the non-safety-related load is part of important plant operation and/or control. As a result, a failure in the *safety-related* portion can create a situation in which a plant transient event occurs and, simultaneously, significant safety-related equipment is unavailable because of the same failure. The most significant types of events appear to be those that involve the instrumentation and control power system. As stated below in the discussion of those specific power supplies, the staff believes that ongoing activities in the area of instrumentation and control power supplies should be integrated and should also address this type of concern.

Plant Support Systems

Concerns related to the area of support systems were noted in Categories 1 (as stated, the electric power system is an extensive support system), 13, 14, 18, and 22 (Table 4). Since the electric power system was dealt with separately, the support systems considered here include cooling water systems; heating, ventilation, and air conditioning systems; lube oil systems; air supply systems; and instrumentation and control systems. As was pointed out for the electric systems, these types of support systems tend to be plant unique to some extent.

The main general concern with some of the support systems involves the potential for them to initiate an event and also degrade the systems necessary to mitigate that event. This potential breakdown in the defense-in-depth philosophy can exist in some plants; however, the safety significance is highly dependent on other plant mitigating features such as remaining independent trains of equipment.

Because the loss of these support systems (including the electrical power system) does not lead to events such as a large LOCA or an MSLB which require immediate operator action, the staff concludes that, except for catastrophic failures (see Section 5.4.2), the potential for recovery of these systems is very great. In conjunction with the conclusions regarding induced human-intervention-coupled SIs (see Section 5.4.3), the staff has not recommended a regulatory action in this area, except for spatially coupled interactions. The staff will, however, communicate to the industry this information on support systems.

Incorrect Reliance on Failsafe Design Principles

One area of adverse systems interactions involved reactor protection (scram) systems, Category 18. The staff recognized that such ASIs could be significant because of the time response demanded of a trip system. An argument similar to the argument given above (that the operator could have the time to fix a problem) does not apply.

The staff believes that the types of ASI identified in the studies were the result of use of a design approach which actually requires the functioning of certain features (for instance, a BWR discharge volume had to be empty) and, therefore, an incorrect reliance on failsafe principles. In fact, the concern with the air system was due to reliance on incorrect failsafe principles. In that case, the air system was assumed to fail safe (i.e., bleed off) and, as a result, a partial failure, at some low pressure, went unanalyzed. Action was taken at all BWRs to correct this problem. In addition, it was noted that the electrical supply system to this scram system also had been previously modified because of similar concerns. Specifically, the electrical power was assumed to fail safe, that is, voltage going to zero and, as a result, partial failure such as low voltage or high voltage went unanalyzed for a time.

Although the staff is concerned with such scenarios, the concern focuses on the reactor trip system and it is acknowledged that the resolution of A-9, "Anticipated Transient Without Scram (ATWS)," should resolve the concerns in the area of the reactor trip system (RTS). The staff acknowledges that there may be other areas of the plant in which incorrect use of failsafe principles has occurred, but in all cases except the RTS, it is concluded that the safety significance would be less because of the greater time available for the operator to take corrective action. The only exception may be during a large LOCA; however, the probability of a large LOCA occurring in conjunction with these types of partial failures should be low. The staff will, however, communicate to the industry this information on the use of failsafe principles.

Automated Safety-Related Actions With No Preferred Failure Mode

Another area of adverse systems interactions which was highlighted involved the inadvertent actuation of an engineered safety features (Category 6), inadvertent emergency core cooling system/residual heat removal (ECCS/RHR) pump suction transfer. The most significant characteristic of this area appears to be that such a design feature does not have an "always" preferred (failure) mode. As a result, extra precautions may be needed to avoid: (1) a failure to actuate when needed and (2) a failure that actuates the system when not required (i.e., inadvertently). Of particular note is the possibility of inadvertent actuation of these types of functions during testing or maintenance. It is fairly common practice to put portions of the actuation logics in a trip or actuated state and assume that the plant is then in a "safe" condition. Although this may be true for functions that have a preferred (failure) mode, it may not be a conservative assumption for these other functions that do not have an always preferred (failure) mode. The specific area of automatic ECCS switch to recirculation is the subject of a generic issue (GI) that is scheduled for prioritization, GI-24 (NUREG-0933, Rev. 2).

GI-24 will consider the aspect of possible untimely, inadvertent ECCS/RHR pump suction transfer; therefore, the staff concludes that further specific action as part of the A-17 resolution is not warranted. The task manager for A-17 will make the staff responsible for NUREG-0933 aware of the information developed in the ORNL study.

There is some additional concern that other ESF systems may similarly not always have a preferred failure mode. In general, almost all of these systems have been analyzed for inadvertent actuation from a functional standpoint. The staff will, however, communicate to the industry this information on the concern (regarding functionally coupled ASIs) for systems that do not have an always preferred failure mode.

Instrumentation and Control Power Supplies

The ORNL review (NUREG/CR-3922) highlighted several events related to instrumentation and control (I&C) power supplies (Category 14). The events at all plants, and specifically at Babcock & Wilcox plants, have already received significant attention as outlined in the ORNL assessment (NUREG/CR-4261). As stated in Section 3.4.3, there was some concern that the potential for a significant event related to I&C power supply interactions may still exist. Because of this concern, further review work at ORNL was identified.

ORNL completed this work and summarized it in a report entitled, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events"

(NUREG/CR–4470). The report included a number of I&C power supply failures, some of which led to initiation of a plant transient and partial disabling of a safety system or operator indication.

On the basis of the additional work performed by ORNL and the staff's further review of the area of I&C power, the staff concluded that a significant number of issues and industry efforts were already under way in this area. The results of the A–17 work in this area will be communicated to the industry for information. However, the conclusion that significant activity is already under way in this area has led the A–17 resolution to include a recommendation that all the issues related to I&C power be combined under one task action plan to better expedite and coordinate the work in this critical area. In addition, the ORNL report should be utilized in this combined task.

5.4.2 Spatially Coupled Type

Spatial dependencies appeared in a number of categories, including 3, 4, 8, 10, 15, 16, 21, and 23 (Table 4). This information was used in conjunction with the review of the utility studies in the spatial area.

See Section 5.6 for the staff's conclusions regarding spatially coupled interactions.

5.4.3 Induced Human-Intervention-Coupled Type

The limited treatment of the operator in the study of the A–17 issue (i.e., as a hardwire link) resulted in only a few events in this specific area (Category 19) and, actually, these events could also be classified as another form of functional coupling. Of related interest are those events related to instrument and control power losses (Category 14), since such losses can also lead the operator to a false conclusion.

On the basis of actions taken independently of the A–17 issue in the area of operator indication, and particularly the implementation of Regulatory Guide 1.97 and the issuance of IE Bulletin 79–27, the staff concludes that no additional action should be required for adverse systems interactions of this type at this time. The A–17 investigation will supply any additional information uncovered as a result of instrumentation and control power supply investigations as input to GI–76 (NUREG–0933, Rev. 2).

5.4.4 Adequacy of Ongoing Evaluations of Operating Experience

ORNL reviewed (NUREG/CR–4261) the existing programs for the reporting, evaluation, and dissemination of significant operating experience. This review included the activities considered by AEOD (Section 5.2.5) and IE (Section 5.2.6) and efforts by the industry. On the basis of this review, ORNL concluded that adequate provisions are in place to continue to monitor the operating experience for adverse systems interactions regardless of whether they are specifically labeled as such.

The staff agrees with the ORNL conclusion and is, therefore, considering taking no action in the area of evaluation of operating experience, except for the one-time dissemination of the information from the ORNL study for ASIs (NUREG/CR–3922 and NUREG/CR–4261).

5.4.5 Undesirable Results of Systems Interaction Events

Part of the effort to focus USI A–17 involved a set of definitions which included a set of undesirable results (see Section 3.2). Although no conclusion was reached as to the relative consequences or frequency of the various results (except for undesirable result 5—see below), a closer evaluation of the nature of the events which involve these results led to certain observations.

Undesirable result 1 involves breakdowns in the independence of redundant safety systems, divisions, trains, etc. This is a clear violation of the single-failure criterion, and these events often result from errors such as design or installation errors. Although they sometimes involve subtle couplings, they are still caused by errors that probably cannot be rectified by providing additional guidance on the application of the single-failure criterion.

Undesirable result 2, which addresses the degradation of a safety-related system by a system not related to safety, involves a similar observation: Independence or isolation is clearly required for these cases and typically errors, rather than subtle couplings, cause the problems.

Undesirable results 3 and 4, on the other hand, involve coupling of any plant accident or transient event and the degradation of any safety system including operation information. This aspect of breakdowns in levels of defense in depth has not typically been the subject of as much guidance as the area of independence between safety systems and non-safety systems. One exception may be in regard to the potential for a LOCA or MSLB to result in an environment that can impact safety-related equipment. This area has been the subject of a large effort to qualify the plant equipment to survive these environments.

ASIs of note that were identified as a result of the A–17 study were events that involved a single failure, such as loss of a power supply or other support system which led to a transient and also led to the loss of a train of some mitigative feature.

Undesirable result 5 was included in the A–17 issue to address events that may involve plant features such as

locked doors or inaccessible areas. The search of operating experience uncovered only a few events of this type (NUREG/CR-3922). In addition, a prioritization (NUREG-0933) of a related area, GI-81, "Impact of Locked Doors and Barriers on Plant and Personnel Safety," concluded that the issue should be dropped from further consideration. Therefore, the staff did not consider this type of adverse systems interaction further.

5.5 Probabilistic Risk Assessments

The following is extracted from the Introduction to NUREG/CR-3852, "Insight Into PRA Methodologies."

> In 1975, a new approach to evaluating reactor reliability and risk—Probabilistic Risk Assessment (PRA)—was presented in the Reactor Safety Study (RSS), WASH-1400 [renumbered NUREG-75/014]. This approach is based upon the concept of defining reactor system functions required for specific challenges (event trees) and estimating the probability of failure of system and functional requirements (fault trees). Since the completion of the RSS, reliability and risk assessment methods have been slowly evolving to the degree that they have become generally accepted for providing a reasonable analysis of the safety of a nuclear power plant. During the mid to late 1970s, the Reactor Safety Study Methodology Applications Program (RSSMAP) developed the concept of dominant accident sequences to simplify the construction of detailed event and fault trees. Following RSSMAP, the Interim Reliability Evaluation Program (IREP) sponsored five reliability assessments to determine plant differences by utilizing a variety of probabilistic assessment methods and implementation techniques. In addition to these NRC-sponsored studies, the nuclear power industry has conducted a number of reliability and risk studies. Examples include the Zion, Indian Point, Oconee, and Limerick PRAs. These studies have also made significant advances to the state of the art in probabilistic analysis.
>
> At the present time about 20 probabilistic safety analyses on specific nuclear power plants have been completed. All of the studies are primarily based on the methods developed in the Reactor Safety Study. However, most of the studies have attempted to improve upon the original probabilistic concepts.

Many of the studies, to one degree or another, address some aspects of the general subject area of systems interactions. Adverse systems interactions constitute a small subset of the general area referred to as "dependencies" in a PRA. The dependencies related to systems interactions involve topic areas such as Modeling of AC Power Systems and Modeling of Logic (Actuation) Systems. There are many other dependencies dealt with which are not systems interactions. Among these are evaluation of human error and common-mode analysis.

Reports published on probabilistic risk assessment (NUREG-1050, NUREG/CR-2300, and NUREG/CR-2815) have consistently identified the area of dependencies as critical to the accuracy of the studies. The failure to adequately treat dependencies, including adverse systems interactions, will repeatedly cause the results to underestimate overall risk.

In terms of probabilities, cutsets include independent events so that $P_{AB} = P_A \cdot P_B$. However, where there is some dependency, P_{AB} is greater than $P_A \cdot P_B$. Clearly, by A-17 definitions, not all such dependencies are due to adverse systems interactions because a dependency such as could arise from common maintenance practices (e.g., the case of the Salem A and B scram breakers, NUREG-1000) would also be such a dependency. If a PRA would, through very detailed modeling, include *all* the system and initiating event dependencies (including functional and spatial dependencies), then it would address all concerns for systems interactions.

No PRA to date has been able to make this sort of claim; however, many have highlighted significant system dependencies that are related to the systems interaction issue.

Additional work has been performed in the general subject area of common-cause event analysis. A guide (NUREG/CR-4780) has been prepared to aid in performing a common-cause analysis as part of a risk or reliability analysis. The guide reflects many years of research by the authors and others in the treatment of dependent failures in reliability and risk studies. As such, it references much related work by organizations such as the Electric Power Research Institute and Pickard, Lowe, and Garrick, Inc.

During its study leading to the resolution of USI A-17, the staff considered both the PRA methods used in these areas and significant systems interactions highlighted by individual studies.

5.5.1 PRA Methods

ORNL reviewed the relationship of systems interactions to PRAs (NUREG/CR-4261) and concluded that there are three keys to adequately model systems interaction dependencies in a PRA:

(1) The model must provide adequate detail about the systems. This detail is required to identify functional

interactions that occur because support systems fail and is also necessary for examining spatial interactions.

(2) The model must utilize extensive plant-specific information. This information includes the location of safety-related equipment and its proximity to both redundant equipment and to items that could affect its safety function. Through the use of such plant-specific information, the spatial systems interactions could be identified. Plant-specific information is also needed for identifying functional interactions that can occur in support equipment such as cooling water and electric power systems.

(3) The models must consider off-normal (i.e., other than anticipated) modes of operation. A number of the systems interactions identified in an operating experience review (see Section 5.4) involved off-normal conditions during which equipment failed because the designer did not anticipate all conditions.

One of the greatest advantages of this type of plant modeling may be found in the process itself: By following patterns of investigation dictated by application of the techniques, the analyst takes a systematic look at plant design and operation. This can provide more insights than just those gained in the traditional design-review process.

To provide a reasonably accurate estimate of the probabilities of accident sequences, a PRA must consider dependencies between the systems and initiating events in the sequence. In some cases this has been done through system failure probabilities (which are derived from failure data that include such things as support system failure) and in other cases explicit detailed modeling has accounted for them.

In either case, the process must include the normal, recognized, systems interaction (e.g., where Train A cooling water supports Train A high-pressure injection through bearing cooling). To resolve issue A-17, a PRA would also have to address the adverse systems interactions. The problem (with respect to A-17) is that the dependencies of concern (referred to as adverse systems interactions) are sometimes so hidden or subtle that the analyst would not recognize them and, therefore, would not account for them either in the failure probabilities or through the modeling process.

The staff has concluded that it is not necessary (or even logical) to perform a separate, full-plant-scope study, such as a PRA, solely for the purpose of addressing adverse systems interactions. However, if for other reasons a PRA is performed, the A-17 program results provide the following guidance.

With respect to future PRAs, the staff concludes that numerous methods are available for identifying the adverse systems interactions, but it is more a question of the amount of effort (and therefore dollars) one can expend. Therefore, contrary to the expectation expressed in NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," the staff does *not* endorse one methodology. On the other hand, the staff reinforces the conclusions reached in NUREG/CR-2815 regarding functional dependencies and physical dependencies.

Specifically, NUREG/CR-2815 concludes:

(1) Functional Dependenc[i]es

All functional dependenc[i]es should in principle be identified at the FMEA phase and/or included in a correctly drawn fault tree. A fault tree should contain in particular all the shared-hardware and direct-process-coupling types of dependenc[i]es. Additional functional dependenc[i]es could be identified if the basic events in the fault trees are further decomposed to simpler events. The level of resolution in a fault tree depends on *whether the analyst believes* that a dependence could possibly exist at lower levels and on the relevant significance of such dependenc[i]es.

In this last regard, the A-17 program has highlighted a number of areas of concern which should be the focus of such resolution by the analyst (see Section 5.4).

(2) Physical Dependenc[i]es

A search of physical dependenc[i]es generally consists of generating minimal cutsets and examining whether the elements of these sets are susceptible to the same generic causative factor and in addition are connected by an "environmental" conductor that will allow such a dependence to be created by a single source. Computer-aided search procedures have been developed for this purpose and are described in Section 3.7.3.9 of the ANS/IEEE, "PRA Procedures Guide" [NUREG/CR-2300].* In applying these techniques, the information generated during the FMEA and put in the form of generic causative factors list is extremely useful.

Special caution should be exercised if codes that generate minimal cutsets using cutoff probabilities are employed, in order to avoid missing important dependenc[i]es contained in the rejected cutsets.

*Prepared for NRC under auspices of ANS/IEEE.

For certain physical dependenc[i]es the search within minimal cutsets can be combined with the PASNY* approach of identifying "targets" and "sources" for these interactions. If critical combinations of "targets" to be examined during "walkthroughs" are defined on the basis of the minimum cutsets, then the efficiency of the "walkthrough" procedure will improve substantially.

As concluded elsewhere (see Section 5.6 on spatial interactions), the staff believes that a focused walkthrough review could be beneficial to safety. If a specific plant PRA is available, the targets and sources could be identified on the basis of the minimal cutsets and the procedure could be improved substantially.

5.5.2 ASIs Identified From Review of PRA Results

The following ASIs were identified from a review of a number of PRAs (NRC memoranda, December 3, 1984, and May 31, 1985) based on the description of the events as compared to the definitions in the A-17 Task Action Plan.

Support Systems

(1) Direct-current bus supplies actuation power to the turbine-driven emergency feedwater pump and to a diesel generator breaker. Therefore, a single dc bus failure (the breaker connecting the bus fails to close) disables two emergency feedwater pumps in the event of a loss of offsite power.

(2) Stripping vital loads from the safety buses on a safety injection signal (even though offsite power has not been lost) and then reloading them sequentially on the bus reduces the reliability of the safety function.

(3) Direct-current bus faults can cause a reactor trip initiating event with concomitant failure of multiple core and containment cooling system trains.

(4) Failures in the component cooling water (CCW) system have been identified as extremely important support system failures which have the potential of being an initiating event along with disabling mitigative systems required for that sequence. These aspects are discussed together in the next section, "Initiating Events."

(5) A pipe failure in an air supply system results in failure of all automatic depressurization system (ADS) valves.

*Power Authority of the State of New York, now called New York Power Authority (NYPA).

Initiating Events

(1) A CCW system pipe break causes loss of cooling to the reactor coolant pump seals and to the charging pumps which provide seal injection flow. Loss of seal cooling and injection flow may result in seal failure (i.e., small LOCA). Core melt may ensue because the high head safety injection pumps (ECCS) also fail when CCW system cooling is lost. Thus, a single initiating event (loss of CCW) may directly result in core melt.

(2) Loss of cooling to reactor pump seals for short periods of time (30-60 minutes) may result in seal failure even when the reactor coolant pumps have been tripped.

These examples indicate that PRAs have indeed uncovered some adverse systems interactions. These examples of ASIs occur in the areas of support systems and initiating events coupled with mitigating system failures. They tend to reinforce the areas highlighted by the review of operating experience.

5.6 Study of Seismic/Spatially Coupled Systems Interactions

As the review of operating events and the review of utility SI studies progressed, it became apparent that a very large number of spatial interactions were possible. To attempt to understand these phenomena, a separate effort was defined to review this area. The approach for the review of SI studies was to compare the results of the IP3 study and the Diablo Canyon study, and from this information to draw conclusions about the possible safety significance of the interactions postulated and the costs associated with conducting a more focused program.

The major portion of this work was performed by Mark Technologies Corp. under subcontract to ORNL. That report (NUREG/CR-4306) addresses four major aspects of the programs. These aspects are the targets, the scope of the postulated initiating events, the postulated source failures, and the resulting documentation.

5.6.1 Target Scope

The programs reviewed had broad target scopes. They considered most safety systems and one included refueling and fire-protection components. The differences in scope in each of the programs appeared to have been based on plant-specific licensing and documentation considerations rather than on any cost/benefit or risk-based criteria. The target scope is the most important factor in the level of effort and cost for all of the programs reviewed.

5.6.2 Initiating Events

A review of the programs shows that greater risk significance is associated with those initiators capable of

challenging the plant support functions. The greatest risk-significant initiators for the reactor coolant pressure boundary include seismic events and fires. Auxiliary feedwater and other frontline systems have significant risk only for plantwide events which are capable of challenging multiple frontline functions simultaneously (e.g., seismic, fire, flood, and possibly tornado winds). Tornado missiles, local internal missiles, and pipe failure (not seismically induced) do not pose significant plant risk outside the plant support systems.

5.6.3 Source Failures

All three programs have postulated large numbers of source failures for which limited historical data are available and even less quantitative evaluation has been performed. The program scopes of source failures included low-frequency initiating events such as high-energy line breaks, tornado missiles, plantwide floods, and low-probability seismically initiated component failures such as failure and falling of piping, raceways, and HVAC equipment. In addition to the low-frequency initiating failures, the programs postulated interactions with safety components such as large mechanical equipment and piping which could be capable of surviving some impacts. Other areas of source failure appear to have been less extensively covered. These include, most notably, the effects of water spray on electrical equipment. The postulation and treatment of water as a source was inconsistent in the documentation of both the walkdown and the flooding study portions of the programs. Limiting the study to only the most credible source initiators and the resulting credible interactions can produce reductions in cost and optimize risk benefit.

5.6.4 Documentation

Documentation of the three programs on an individual source/target basis took a lot of engineering and administrative time. Individual documents were generated, revised, edited, controlled, tracked, and sorted in the interests of ensuring traceability and unique identification of the thousands of potential, but in many cases, clearly low-probability, low-risk events. A streamlined and focused program could be developed with a level of documentation commensurate with the level of risk associated with the events being investigated.

5.6.5 Analysis of Spatially Coupled Systems Interactions

Each interaction is typically characterized by an initiating event or failure, a coupling or transmission of the failure effects, and a disabling of a target component, system, and so forth. Of particular note is the uncertain nature of each one of these characteristics. Unlike functionally coupled ASIs, in which a failure usually propagates directly through the connected systems and causes other failure in spatially coupled events, failure propagates through less direct paths and, as a result, other failures are less certain.

On the basis of its review, Mark Technologies Corp. outlined a relative ranking of the targets based on the perceived risk significance of the target groupings.

With respect to the targets, the support systems and controls were noted to be of greatest significance. The basis for this conclusion involves the fact that support systems and controls can potentially affect multiple frontline systems as well as possibly initiate a plant transient. In addition, controls (instrumentation, electrical devices, etc.) tend to be very sensitive to the type of spatial phenomena (e.g., seismic, flood, spray) which are of concern. These are followed in decreasing importance by the reactor coolant pressure boundary, the auxiliary feedwater (AFW) system and controls, and the other frontline systems.

With respect to the source or initiating event scope, the programs considered a number of initiators which included seismic events, flood, fire, missiles, pipewhip, and tornado, depending on the target system involved.

The report (NUREG/CR–4306) discusses a simplified search methodology which could be applied to these target groupings and initiating events and provides cost estimates for such searches.

5.6.6 Staff Conclusions

The staff generally agrees with the conclusions of NUREG/CR–4306.

The staff believes that for any future SI reviews, the target scope should be limited to the support systems and controls for the systems required for safe shutdown, the safe-shutdown systems themselves, and the reactor coolant pressure boundary.

The staff does not believe that further review for spatially coupled interactions in the area of the ECCS is justified. These areas received a lot of review in the past. The review of the ECCS has not focused on all of the areas listed as concerns, but the need for this equipment is predicated on the occurrence of a LOCA which has a relatively low frequency of occurrence. In addition, the reactor coolant pressure boundary (RCPB) would be evaluated as a target system (both as the RCPB itself and under controls such as relief valves) and, therefore, the potential for a seismically induced LOCA caused by a spatially coupled ASI should be low.

Furthermore, the staff believes that the initiating events to be considered should include only those related to seismic events and fluid-related failures such as flooding

and water intrusion, including spray from low- or moderate-energy piping. On the basis of other previous or ongoing activities, each of the other potential initiating events is believed to be adequately covered.

With respect to flooding, actions were taken at all plants as a result of the event at Quad Cities in 1972 (AEC letter, September 26, 1972). The actions taken should have addressed these areas of concern. (See also SRP Section 3.6.1 and Branch Technical Position (BTP) ASB 3-1.) However, there is some evidence that not all flooding and water-intrusion interactions were evaluated. Specifically, both the Diablo Canyon and Indian Point studies, as well as some of the SEP reviews (e.g., NUREG-0824) under Topic III-5.B, "Pipe Break Outside Containment," highlighted some potential interactions. In addition, operating experience has highlighted a number of events that have involved flooding and water intrusion (see Section 5.4.2). On the basis of these findings, the staff developed a number of insights in the area of flooding and water intrusion from internal sources (see the Appendix for additional information).

The area of fire protection has received significant attention as the result of action taken in response to Appendix R of 10 CFR Part 50. The overall fire reviews include the type of considerations identified in the Mark Technologies Corp. report. Because of this, the staff is recommending taking no further action related to fire as a hazard. However, the fire-suppression system itself may be a source for flood or spray.

(1) Turbine missiles and (2) tornadoes and tornado missiles have been the subject of a number of proposed generic issues, namely A-37 and A-38, respectively. These issues were prioritized "drop" and "low," respectively. In addition, the SEP group reviewed the area of internal missiles under Topic III-4.C and generally concluded that plants had adequate protection from internal missiles. On this basis, the staff is not recommending that these sources be pursued.

As a result of the above considerations and the spatially coupled ASIs uncovered by the operating experience review (see Section 5.4), the staff concludes that a focused search for certain spatially coupled systems interactions and appropriate corrective measures could benefit safety for some operating plants.

6 SUMMARY OF STAFF CONCLUSIONS

The resolution of any safety issue requires that the nature of the concern be clearly described. Concerns described as general subject areas, such as common cause, systems interactions, and dependent failure, can prove so broad that almost every conceivable safety issue could fall within the concern, and therefore the issue itself would prove unmanageable.

Therefore, to proceed with a resolution of the concerns expressed as "systems interactions," the NRC staff developed a set of definitions to attempt to give the safety concern narrower focus. As part of developing this definition, it was decided to take advantage of many ongoing efforts, so that if some aspects that might be considered systems interactions were better addressed by other efforts, the definitions would direct the A-17 effort away from those areas. As a result, a workable set of definitions was developed for the A-17 issue. Many other concerns were left to be addressed outside A-17. These definitions are crucial to the understanding of the issue and its resolution.

On the basis of the definitions, a number of tasks were defined. These tasks were structured to: (1) make use of operating experience and other sources of actual or postulated events, (2) take maximum advantage of previous systems interaction studies, (3) evaluate the safety significance of systems interactions, and (4) evaluate the safety benefit and cost effectiveness of potential corrective measures.

Because systems interactions events are for the most part plant specific, the quantification of the potential safety significance was extremely difficult. Therefore, the safety benefit is based mostly on qualitative insights rather than quantitative analysis.

As a result of the investigation into adverse systems interactions the staff concluded the following:

(1) To address a subject area such as "systems interactions" in its broadest sense tends to be an unmanageable task incapable of resolution. Some bounds and limitations are crucial to proceeding toward a resolution. Considering this, the staff studying the A-17 issue utilized a set of working definitions to limit the issue. It is recognized that such an approach may leave some concerns unaddressed.

(2) The occurrence of an actual ASI or the existence of a potential ASI is very much a function of an individual plant's design and operational features (such as its detailed design and layout, allowed operating modes, procedures, and test and maintenance practices). Furthermore, the potential overall safety impact (such as loss of all cooling, loss of all electric power, or core melt) is similarly a function of those plant features that remain unaffected by the ASI. In other words, the results of an ASI depend on the availability of other independent equipment and the operator's response capabilities.

(3) Although each ASI (and its safety impact) is unique to an individual plant, there appear to be some characteristics common to a number of the ASIs.

(4) Methods are available (and some are under development) for searching out SIs on a plant-specific basis. Studies conducted by utilities and national laboratories indicate that a full-scope plant search takes considerable time and money. Even then, there is not a high degree of assurance all, or even most, ASIs will be discovered.

(5) Functionally coupled ASIs have occurred at a number of plants, but improved operator information and training (instituted since the accident at Three Mile Island) should greatly aid in recovery actions during future events.

(6) Induced human-intervention-coupled interactions as defined in A-17 are a subset of the broader class of functionally coupled systems interactions. As stated for functionally coupled SIs, improvements in both operator information and operator training will greatly improve recovery from such events.

(7) As a class, spatially coupled SIs may be the most significant because of the potential for the loss of equipment which is damaged beyond repair. In many cases, these ASIs are less likely to occur because of the lower probability of initiating failure (e.g., earthquake, pipe rupture) and the less-than-certain coupling mechanisms involved. However, past operating experience highlighted a number of flooding and water intrusion events and more recent operating experience indicates that these types of events are continuing to occur (see the Appendix for additional information).

(8) Probabilistic risk assessments or other systematic plant-specific reviews can provide a framework for identifying and addressing ASIs.

(9) Because of the nature of ASIs (they are introduced into plants by design errors and/or by overlooking subtle or hidden dependencies), they will probably continue to happen. In their evaluations of operating experience, NRC and the nuclear power industry can provide an effective method for addressing ASIs.

(10) For existing plants, a properly focused systematic plant search for certain types of spatially coupled ASIs and functionally coupled ASIs (and correction of the deficiencies found) may improve safety.

(11) The area of electric power, particularly instrumentation and control power supplies, was highlighted as being vulnerable to relatively significant ASIs. Further investigation showed that this area remains the subject of a number of separate issues and studies. A concentrated effort to coordinate these activities and to include power supply interactions could prove an effective approach in this area.

(12) For future plants, additional guidance regarding ASIs could benefit safety.

(13) The concerns raised by the Advisory Committee on Reactor Safeguards on A-17, but which have not been addressed in the staff's study of A-17, should be considered as candidate generic issues, separate from USI A-17.

7 REFERENCES

Advisory Committee on Reactor Safeguards, Letter dated November 8, 1974, to the Director of Regulation of the AEC, "Systems Analysis of Engineered Safety Systems."

———, Letter dated June 17, 1977, to Chairman of the NRC, "Report on the Zion Station, Units 1 and 2."

———, Letter dated October 12, 1979, to Executive Director of Operations of the NRC, "Systems Interactions Study for Indian Point Nuclear Generating Unit No. 3."

———, Letter dated May 13, 1986, to Executive Director of Operations of the NRC, "ACRS Comments on Proposal Resolution of USI A-17, "Systems Interactions in Nuclear Power Plants."

Atomic Energy Commission, Letter dated September 26, 1972, from R. C. DeYoung to licensees, "Flooding Event at Quad Cities, Unit 1."

Atomic Industrial Forum, Inc., Letter dated October 8, 1985, from M. R. Edelman to V. Stello, "Unresolved Safety Issue A-17 Systems Interactions"

Commonwealth Edison Company, "Zion Station Interaction Study," Docket 50-304, June 16, 1978.

Consumers Power Company, "Program Manual Spatial Systems Interaction Program/Seismic Midland Energy Center," Revision 1, June 6, 1983.

Electric Power Research Institute, "Systems Interaction Identification Procedures," EPRI NP-3834, Vols. 1-5, July 1985.

———, EPRI NP-5613, see NRC, NUREG/CR-4780.

Lawrence Livermore National Laboratory/Analytic Information Processing, Inc., "Preliminary Systems Interaction Results From the Digraph Matrix Analysis of the Watts Bar Nuclear Power Plant Safety Injection Systems," UCID-19707, June 1983.

Oak Ridge National Laboratory, ORNL/Letter Report, "Summary and Assessment of EPRI Report NP-3834 on 'Systems Interaction Identification Procedures'," February 10, 1986.

Office of Inspection and Enforcement, NRC, Bulletin 79-27, "Loss of Non-Class 1E Instrumentation and Control Power Systems Bus During Operation," November 30, 1979.

Pacific Gas and Electric Company, "Diablo Canyon Seismically Induced Systems Interaction Program," Dockets 50-275 and 50-323, May 7, 1984.

Power Authority of the State of New York, "Systems Interaction Study, Indian Point 3," Docket 50-286, November 1983.

———, LER 84-010-000, Docket 50-286, July 16, 1984.

U.S. Nuclear Regulatory Commission, Memorandum dated September 18, 1984, from R. Kendall to D. Thatcher, "Comments on ORNL Draft NUREG/CR-3922."

———, Memorandum dated December 3, 1984, from H. R. Denton to Division Directors, "Insights Gained From Probabilistic Risk Assessments."

———, Memorandum dated March 20, 1985, from A. Thadani to K. Kniel, "RRAB Inputs to the USI A-17 Program."

———, Memorandum dated May 31, 1985, from A. Thadani to K. Kneil, "RRAB Input to USI A-17 Resolution."

———, NUREG-75/014, "Reactor Safety Study—An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," October 1975.

———, NUREG-0471, "Generic Task Problem Descriptions (Categories B, C, and D)," June 1978.

———, NUREG-0572, "Review of Licensee Event Reports (1976-1978)," September 1979.

———, NUREG-0649, "Task Action Plans for Unresolved Safety Issues Related to Nuclear Power Plants," September 1984.

———, NUREG-0660, "NRC Action Plan Developed As a Result of the TMI-2 Accident," May 1980.

———, NUREG-0737, Supplement 1, "Clarification of TMI Action Plan Requirements: Requirements for Emergency Response Capability," January 1983.

———, NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," July 1981.

———, NUREG-0824, "Integrated Plant Safety Assessment Systematic Evaluation Program—Millstone Nuclear Power Station, Unit 1," February 1983.

———, NUREG-0933, "A Prioritization of Generic Safety Issues," revised frequently.

———, NUREG-0985, "Human Factors Program Plan," August 1983; Rev. 1, September 1984.

———, NUREG-1000, "Generic Implications of ATWS Events at the Salem Nuclear Power Plant," April 1983.

———, NUREG-1050, "Probabilistic Risk Assessment (PRA) Reference Document," Final Report, September 1984.

———, NUREG-1070, "NRC Policy on Future Reactor Designs," July 1985.

———, NUREG-1229, "Regulatory Analysis for Proposed Resolution of USI A-17," to be published.

———, NUREG/CR-1321, "Final Report—Phase I, Systems Interaction Methodology Applications Program," Sandia National Laboratories (SAND80-0884), April 1980.

———, NUREG/CR-1859, "Systems Interactions: State-of-the-Art Review and Methods Evaluation," Lawrence Livermore National Laboratory, January 1981.

———, NUREG/CR-1896, "Review of Systems Interaction Methodologies," Battelle Memorial Institute, January 1981.

———, NUREG/CR-1901, "Review and Evaluation of Systems Interactions Methods," Brookhaven National Laboratory, January 1981.

———, NUREG/CR-2300, "PRA Procedures Guide," Vols. 1 and 2, January 1983.

———, NUREG/CR-2815, "Probabilistic Safety Analysis Procedures Guide," Brookhaven National Laboratory, January 1984.

———, NUREG/CR-2915, "Initial Guidance on Digraph Matrix Analysis for Systems Interaction Studies," Lawrence Livermore National Laboratory (UCID-19457), March 1983.

———, NUREG/CR-3593, "Systems Interaction Results From the Digraph Matrix Analysis of a Nuclear

Power Plant's High Pressure Safety Injection Systems," Analytic Information Processing and Lawrence Livermore National Laboratory, July 1984.

———, NUREG/CR–3852, "Insight Into PRA Methodologies," August 1984.

———, NUREG/CR–3922, "Survey and Evaluation of Systems Interaction Events and Sources," Oak Ridge National Laboratory, January 1985.

———, NUREG/CR–4179, "Digraph Matrix Analysis for Systems Interactions at Indian Point Unit 3, Abridged Version," Vol. 1, January 1986, Vols. 2-6 will be available in the NRC Public Document Room, 2120 L Street, N.W., Washington, D.C., Lawrence Livermore National Laboratory.

———, NUREG/CR–4207, "Fault Tree Application to the Study of Systems Interactions at Indian Point 3," Brookhaven National Laboratory, April 1985.

———, NUREG/CR–4261, "Assessment of System Interaction Experience in Nuclear Power Plants," Oak Ridge National Laboratory, June 1986.

———, NUREG/CR–4306, "Review and Evaluation of Spatial System Interaction Programs," Oak Ridge National Laboratory, December, 1986.

———, NUREG/CR–4470, "Survey and Evaluation of Vital Instrumentation and Control Power Supply Events," August 1986.

———, NUREG/CR–4780, "Procedures for Treating Common Cause Failures in Safety and Reliability Studies: Procedural Framework and Examples," January 1988.

———, SECY-84-133, "Results of SEP," Enclosure 4, "SEP Phase II Safety Lessons Learned," March 23, 1984.

APPENDIX
INTERNAL FLOODING AND WATER INTRUSION INSIGHTS

Operating events have demonstrated the susceptibility of individual plant components to water intrusion and flooding from internal plant sources. Flooding, as discussed here, includes flooding of equipment by large volumes of water (i.e., equipment submergence) and other forms of water intrusion, including water spraying, dripping, or splashing on sensitive equipment. Examples of these types of events can be found in an operating experience review (References 1 and 2) conducted by the NRC and in individual NRC information notices (References 3–9). A key point apparent from these events is that the quantity of the water involved is not necessarily a measure of the problems that the water can create; the *location* of the water is much more significant. For example, a small leak that drips down through electrical equipment can have a more severe impact on the plant than an 8-foot flood in a pump compartment. Also, Generic Issue 77, "Flooding of Safety Equipment Compartments by Back-Flow Through Floor Drains," has received a high priority ranking (Reference 10) because of the possibility that plant designs have overlooked backflow through floor drains as a flooding pathway.

All plants should have conducted some flooding-type studies as part of demonstrating conformance to various requirements. These requirements were typically focused on large volumes of water and the potential for submerging equipment.

(1) The general design criteria (10 CFR Part 50, Appendix A) address the area of flooding. Specifically:

- GDC 3, "Fire protection," states: "Fire fighting systems shall be designed to assure that their rupture or inadvertent operation does not significantly impair the safety capability of these structures, systems and components designated as important to safety."

- GDC 4, "Environmental and dynamic effects missile design bases," states: "Structures, systems, and components important to safety shall be designed to accommodate the effects of and to be compatible with...normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. These structures, systems and components shall be appropriately protected against dynamic effects, including the effects of missiles, pipe whipping, and discharging fluids, that may result from equipment failures and from events and conditions outside the nuclear power unit. However, dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping."

(2) As part of environmental qualification requirements of 10 CFR 50.49, submergence was evaluated for certain equipment for water associated with design-basis events.

(3) Generic letters issued to licensed facilities in 1972 required additional review based on an event at the Quad Cities plant.

(4) For more recently licensed plants, the Standard Review Plan (Reference 11) cites the generic letters of 1972, and therefore, flooding-type analysis should have been performed as part of the licensing process.

In addition, all plants should have developed programs for the review of operating experience per the requirements of Item I.C.5 of NUREG–0737 (Reference 12). These reviews should include consideration of NRC information notices and other industry documents such as those issued by the Institute of Nuclear Power Operations (INPO). Both of these have included events involving flooding and water intrusion.

The staff has concluded that existing requirements lack specific guidance regarding water intrusion events that may involve small amounts of water and subtle paths of communication of water or moisture to sensitive equipment.

The staff also recognizes that it may not be possible to identify all subtle pathways and sources. However, the staff believes that risk could be reduced significantly by conducting a focused review that includes:

(1) reviewing actual industry operating experience involving water intrusion for applicability to the licensee's plant

(2) considering action such as sealing conduit or providing shields for sensitive equipment, and

(3) examining safe-shutdown equipment specifically focusing on the potential for water intrusion problems. Safe-shutdown equipment for a flooding or water intrusion event would typically include the equipment needed to perform the following functions:

- Bring the plant to hot shutdown and establish heat removal.

- Maintain support systems necessary to establish and maintain hot shutdown.
- Maintain control room functions and instrumentation and controls necessary to monitor hot shutdown.
- Provide alternating current and/or direct current emergency power as needed on a plant-specific basis to meet the above three functions.

[*Note:* In addition to the above equipment, a review should include electrical equipment that could cause inadvertent actuation of components which in turn could hinder the ability to perform these functions (e.g., logic cabinets that actuate the automatic depressurization system).]

On the basis of a large amount of industry experience, the staff has determined that a flooding (including water intrusion) analysis should address the aspects listed below. Water intrusion includes all forms of water or moisture release from water sources internal to plant structures (e.g., leaks or ruptures of water or steam sources or from fire-suppression system actuation). Regardless of the means of release, the failure mechanism is intrusion of water or moisture to sensitive equipment (e.g., electrical cabinets).

(*Note:* If an analyses has been performed to demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping (i.e., per revised GDC 4), then fluid discharge associated with that rupture may be excluded from further consideration.)

Water Intrusion Considerations

Sources

The water can and has been released by failure (e.g., leaks, ruptures), by system actuation (e.g., fire-suppression system), or by special plant situations during maintenance or testing. Actual operating experience has demonstrated problems that emanate from:

- domestic water systems (toilets, sinks, eye-wash stations, etc.)
- fire-suppression equipment
- moderate-energy piping systems such as circulating water
- maintenance actions (e.g., draining, venting)
- low-pressure steam and condensate leakage

Pathways

Operating experience has demonstrated that separate rooms do not necessarily provide protection because of

- drain systems that may be plugged or allow backflow
- heating and ventilation ducts and penetrations between rooms
- unsealed doors
- unsealed or inadequately sealed electrical conduit and penetrations (either by design or from inadequate maintenance)
- unusual maintenance situations (temporary drain lines, water barriers)

Operating Experience

Collective industry experience has been described in:

- NRC Information Notice 83–41, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Equipment," June 22, 1983
- NRC Information Notice 83–44, "Potential Damage to Redundant Safety Equipment As a Result of Backflow Through the Equipment and Floor Drain Systems," July 1, 1983
- NRC Information Notice 85–85, "Systems Interaction Event Resulting in Reactor System Safety Relief Valve Opening Following a Fire-Protection Deluge System Malfunction," October 31, 1985
- NRC Information Notice 86–106, Supplement 2, "Feedwater Line Break," March 18, 1987
- NRC Information Notice 87–14, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Ventilation Equipment," March 23, 1987
- NRC Information Notice 87–49, "Deficiencies in Outside Containment Flooding Protection," October 9, 1987
- NRC Information Notice 88–60, "Inadequate Design and Installation of Watertight Penetration Seals," August 11, 1988

REFERENCES

1. U.S. Nuclear Regulatory Commission, NUREG/CR–3922, "Survey and Evaluation of System Interaction Events and Sources," Vols. 1 and 2, January 1985.

2. ———, AEOD/C402, "Operating Experience Related to Moisture Intrusion in Electrical Equipment at Commercial Power Reactors," June 1984.

3. ———, Information Notice 83–41, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Equipment," June 22, 1983.

4. ———, Information Notice 83–44, "Potential Damage to Redundant Safety Equipment As a Result of Backflow Through the Equipment and Floor Drain Systems," July 1, 1983.

5. ———, Information Notice 85–85, "Systems Interaction Event Resulting in Reactor System Safety Relief Valve Opening Following a Fire-Protection Deluge System Malfunction," October 31, 1985.

6. ———, Information Notice 86–106, Supplement 2, "Feedwater Line Break," March 18, 1987.

7. ———, Information Notice 87–14, "Actuation of Fire Suppression System Causing Inoperability of Safety-Related Ventilation Equipment," March 23, 1987.

8. ———, Information Notice 87–49, "Deficiencies in Outside Containment Flooding Protection," October 9, 1987.

9. ———, Information Notice 88–60, "Inadequate Design and Installation of Watertight Penetration Seals," August 11, 1988.

10. ———, NUREG–0933, "A Prioritization of Generic Safety Issues," December 1983.

11. ———, NUREG–0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," LWR edition, July 1981.

12. ———, NUREG–0737, "Clarification of TMI–2 Requirements," September 1980.

NRC FORM 335 (2-84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE.

1. REPORT NUMBER *(Assigned by TIDC, add Vol. No., if any)*
NUREG-1174

2. TITLE AND SUBTITLE
Evaluation of Systems Interactions in Nuclear Power Plants
Technical Findings Related to Unresolved Safety Issue A-17

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: April YEAR: 1989

5. AUTHOR(S)
Dale Thatcher

6. DATE REPORT ISSUED
MONTH: May YEAR: 1989

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Division of Safety Issue Resolution
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Same as 7, above.

11a. TYPE OF REPORT
Technical

b. PERIOD COVERED *(Inclusive dates)*

12. SUPPLEMENTARY NOTES

13. ABSTRACT *(200 words or less)*

This report presents a summary of the activities related to Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants," and also includes the NRC staff's conclusions based on those activities. The staff's technical findings provide the framework for the final resolution of this unresolved safety issue. The final resolution will be published later as NUREG-1229.

14. DOCUMENT ANALYSIS – a. KEYWORDS/DESCRIPTORS
Unresolved Safety Issue A-17
Systems Interactions

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

16. SECURITY CLASSIFICATION
(This page) Unclassified
(This report) Unclassified

17. NUMBER OF PAGES

18. PRICE

☆U. S. GOVERNMENT PRINTING OFFICE:1989-241-590:00080