September 6, 1989

TO: ALL HOLDERS OF OPERATING LICENSES OR CONSTRUCTION PERMITS FOR NUCLEAR POWER PLANTS

SUBJECT: RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17, "SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS" (GENERIC LETTER 89-18)

This generic letter informs licensees and applicants of the final resolution of USI A-17, "Systems Interactions in Nuclear Power Plants." There are two enclosures which are provided for information.

Enclosure 1 outlines the bases for resolution of USI A-17.

Enclosure 2 provides a grouping of five general lessons learned from the review of the overall systems interaction issue. The review of this information will give licensees additional appreciation of the kinds of adverse systems interaction which have appeared in operating experience and can aid them in continuing evaluation of operating experience.

No specific action or written response is required by this letter. If you have any question about this matter, please contact the technical contact listed below or the Regional Administrator at the appropriate regional office.

Sincerely,

ORIGINAL SIGNED BY JAMES PARTLOW

James G. Partlow
Associate Director for Projects
Office of Nuclear Reactor Regulation

Technical Contacts:
D. Thatcher, RES
(301) 492-3935

Enclosures:
1. Bases for Resolution of Unresolved Safety Issue A-17
2. Summary Information Relevant to Operating Experience Evaluations
3. List of Recently Issued NRC Generic Letters

DISTRIBUTION
Central Files
NRC PDR
Branch Rdg File
MBoyle D. Thatcher

(F. Gillespie concurred in the A-17 resolution (including ltr. Murley fm Beckjord dtd. 08/08/89) prior to CRGR review.)

NRR	ADP/NRR	OGCB:DOEA:NRR
MBoyle:ps	JPartlow	C. BERLINGER CHB
9/6/89	9/6/89	9/6/89

9/6/89

8909070029 2A

ID TR-5
GENERIC
LTR

Enclosure 1

BASES FOR RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17

Introduction

The U.S. Nuclear Regulatory Commission (NRC) has concluded its resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." This document provides a summary of that resolution. More detailed background information is provided in References 1 and 2.

Adverse systems interactions (ASIs) involve subtle and often very complicated plant-specific dependencies between components and systems, possibly compounded by inducing erroneous human intervention. The staff has identified actions to be taken by the NRC to resolve USI A-17, and has made the judgment that these actions, together with other ongoing activities, should reduce the risk from adverse systems interactions.

The staff's judgment is not based on the assertion that all adverse systems interactions have been identified, but rather that the A-17 actions plus other activities by the licensees and staff, as discussed further below, give reasonable assurance that the more risk-significant interactions will be recognized and appropriate action taken.

Resolution

(1) Ongoing Actions by Licensees

(a) Water Intrusion and Flooding From Internal Sources

As part of the resolution of USI A-17, the staff has identified that water intrusion and flooding of equipment from internal plant sources may result in a risk-significant adverse systems interaction. Such events could cause a transient and could also disable the equipment needed to mitigate the consequences of the event. The appendix to NUREG-1174 (reference 1) provides insights regarding plant vulnerabilities to flooding and water intrusion from internal plant sources. It is expected that these insights will be considered in implementing Generic Letter 88-20 [Individual Plant Examinations (IPE)] which includes an assessment of internal flooding.

(b) Review of Events at Nuclear Power Plants

Licensees are expected to continue to review information on events at operating nuclear power plants in accordance with the requirements of Item I.C.5 of NUREG-0737. Such information is disseminated by the NRC in the form of information notices, bulletins, and other reports; by individual licensees in the form of licensee event reports; and by industry groups such as the Institute of Nuclear Power Operations (INPO). The NRC has an aggressive program of reviewing events at nuclear power plants. Each licensee is required to notify the NRC staff rapidly by telephone of any event that meets or exceeds the threshold defined in

10 CFR 50.72 and to file a written licensee event report for those events that meet or exceed the threshold defined in 10 CFR 50.73. Also, the NRC regional offices report events of significance every day. This information is reviewed daily by members of the NRC staff and followup efforts are assigned for events that appear to be potentially risk significant and/or are judged to be a possible precursor to a more severe event. A weekly meeting is held to brief NRC management on those events of significance. This ongoing process provides a great deal of assurance that any potentially significant event is brought to the attention of the appropriate NRC staff and management. Depending on the significance, further action may be taken to notify licensees or to impose additional requirements. The total process offers a high degree of assurance that precursors to potentially significant events, including those involving adverse systems interactions, are treated expeditiously. Attachment 2 summarizes the A-17 information relevant to these ongoing operating experience evaluations.

(2) Actions by the NRC Related to Adverse Systems Interactions

(a) Integration of Specific, Ongoing, Generic Issues Related to A-17

The NRC is considering certain aspects of potential interactions as part of the resolution of identified generic issues.

- USI A-46, "Seismic Qualification of Equipment

  Actions to resolve this issue have been sent to the licensees. The NRC and industry are working on detailed procedures that will be used to implement the requirements on a plant-specific basis. These implementation procedures will include walkdowns of individual plants to ensure that the systems needed to shut down the plant and maintain it in a safe condition for 72 hours can withstand a design-basis seismic event. The scope includes not only the systems needed to control reactivity and remove decay heat, but also the supporting power supplies, controls, instrumentation, and environmental control subsystems needed by those systems. The plant walkdown reviews include seismic systems interactions.

- Generic Issue 128, "Electric Power Reliability"

  The USI A-17 review of operating experience reemphasized the potential interactions stemming from the electric power system and, in particular, instrumentation and control (I&C) power supply failures. I&C power loss can cause significant transients and can simultaneously affect the operator's ability to proceed with recovery by disabling portions of the indications and the equipment needed for recovery. The events that have occurred were mostly limited to a single electrical division and therefore not strictly adverse systems interactions by the definition in the USI A-17 program. In addition, actions have already been taken by licensees to improve the operator's ability to cope with such events. As a separate activity, a number of generic issues involving electrical power supplies were integrated into one generic issue. This issue became GI 128, "Electric Power Reliability," and consists of the following specific electric issues:

- GI-48, "LCO for Class 1E Vital Instrument Buses in Operating Plants"

- GI-49, "Interlocks and LCOs for Redundant Class 1E Tie Breakers"

- GI-A-30, "Adequacy of Safety Related DC Power Supplies"

It was concluded that the additional information developed on USI A-17, (NUREG/CR-4470) should be used as an input to the GI-128 program. Therefore, that information was communicated to GI-128 for possible action.

(b) Define and Prioritize Other Issues

The Advisory Committee for Reactor Safeguards (ACRS) and other groups have identified concerns in the context of systems interactions. In many cases, the concerns are not considered to be within the scope of systems interactions as defined in the USI A-17 Task Action Plan. In some cases, these concerns have not been described specifically enough to permit the risk to be estimated. The NRC has undertaken a program [referred to as the Multiple System Responses Program (MSRP)] with Oak Ridge National Laboratory (ORNL) to define these concerns in sufficient detail so that they may be prioritized in accordance with NRC procedures.

Examples of concerns involve potential coupling of postulated plant events such as seismically induced fires and seismically induced flooding, and the attendant potential for multiple, simultaneous, adverse systems responses. These concerns are beyond the defined scope of USI A-17. If the definition, priority determination, and peer review processes identify one or more issues as having high or medium priority, the issue(s) will be assigned to the appropriate organization for resolution.

(c) Probabilistic Risk Analyses or Other Systematic Plant Reviews

- Existing Plants

The Commission's Severe Accident Policy, 50 FR 32128 (August 8, 1985), calls for all existing plants to perform a plant-specific search for vulnerabilities. Such searches, referred to as individual plant examinations (IPEs), involve a systematic plant review (which could be a PRA-type analysis). NRC is issuing guidance for performing such reviews. One subject area to be treated by the IPEs is common-cause failures (or dependent failures). USI A-17 recognizes that ASIs are a subset of this broader subject area and, therefore, is providing for the dissemination of the insights gained in the A-17 program for use in the IPE work.

- Future Plants

The Commission's regulations (10CFR50.52) require all future plants to perform a probabilistic risk assessment (PRA). NRC is issuing guidance on the content of PRA submittals for future light-water reactors (LWRs). As part of that guidance, A-17 is providing the insights gained in the A-17 program for the treatment of plant dependencies.

(d) Additional Considerations for Future Plants

The above actions acknowledge the fact that future plants will perform probabilistic risk assessments, and that such studies can uncover ASIs. The staff also recognizes that the continual review of operating experience will identify systems interactions, some of which may be ASIs. Further prioritization of issues defined by the MSRP may result in additional generic issues whose resolution may lead to requirements applicable to future plants.

Therefore, future plants should keep current on lessons learned from operating experience and continue to monitor the ongoing NRC process of developing, prioritizing, and resolving generic issues.

In addition, the staff plans to develop a standard review plan (SRP) for future plants. The SRP would include specific guidance regarding protection from internal flooding and water intrusion events.

Staff Findings

On the basis of the technical findings reported in NUREG-1174 and the regulatory analysis reported in NUREG-1229 the staff has concluded that these actions can further reduce the risk from ASIs. The staff does not recommend further broad searches for ASIs because such searches have not proved to be cost-effective, and in any case, there is no guarantee after such a study is performed that all ASIs have been uncovered. Although these actions complete the staff's work under the Task Action Plan for USI A-17, and constitute technical resolution of the issue as defined therein, the potential for systems interactions remains an important consideration in the design and operation of nuclear power plants.

References:

1. U.S. Nuclear Regulatory Commission, NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants."

2. ---, NUREG-1229, "Regulatory Analysis for Resolution of USI A-17."

Enclosure 2

SUMMARY INFORMATION RELEVANT TO OPERATING EXPERIENCE EVALUATIONS

I. SUMMARY OF USI A-17 FINDINGS

The U.S. Nuclear Regulatory Commission (NRC) has concluded its technical resolution of Unresolved Safety Issue (USI) A-17, "Systems Interactions in Nuclear Power Plants." This summary presents a portion of the results of that technical resolution for use in operating experience evaluations. More detailed background information is provided in References 1 and 2.

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 recognized that if the term 'systems interaction' was to be interpreted in a very broad sense, it became an unmanageable safety issue. Focusing was required to address 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 clearly defined and understood. Then, if other concerns still exist after completion of the program, they can be addressed as part of separate efforts as deemed necessary.

The information presented in this attachment is based on the following definitions:

(1) Systems Interaction (SI)

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 (i.e., that are hidden or unanticipated).

(2) Adverse Systems Interaction (ASI)

A systems interaction that produces an undesirable result.

(3) Undesirable Result (Produced by Systems Interaction)

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

(a) 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) of the Final Safety Analysis Report (FSAR) of the plant. (Note: This would violate the single-failure criterion.)

(b) Degradation of a safety system by a non-safety system. (Note: This result would demonstrate a breakdown in presumed "isolation.")

(c) Initiation of an "accident" (e.g., LOCA, MSLB) and (i) 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 (ii) 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.)

(d) Initiation of a "transient" (including reactor trip) and (i) 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 (ii) 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.)

(e) 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 when a suppression system is actuated).

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

(1) Functionally Coupled:

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

(2) Spatially Coupled:

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

(3) Induced Human-Intervention Coupled:

Those SIs in which 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 the A-17 program, these SIs are considered another example of functionally coupled ASIs. (Induced human-intervention-coupled systems interactions exclude random human errors and acts of sabotage.)

As a result of the staff's studies of adverse systems interactions (ASIs) undertaken as part of A-17 and reported in Reference 1, 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 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 tests 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.

(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) should 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 should 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 (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.

It should be noted that the staff has concluded that adverse systems interactions (ASIs) involve subtle, and often very complicated, dependencies. Therefore, total elimination of ASIs is unachievable. For these reasons, the staff is not recommending that each plant undertake a large, comprehensive study to uncover ASIs. Instead, the staff is recommending other, more cost-effective actions for reducing the frequency and impact of ASIs. Although these actions complete the staff's work under the task action plan for USI A-17, and constitute technical resolution of the issue as defined therein, the potential for ASIs remains an important consideration in the design and operation of nuclear power plants. The staff has, therefore, acknowledged the continuing importance of ongoing activities such as probabilistic risk assessments or other systematic plant evaluations and the continuing review and evaluation of the industry's operating experience.

The regulatory analysis (Reference 2) considered a number of alternatives for resolution, and based on that analysis, the staff has concluded that certain actions should be taken by NRC to resolve USI A-17. These actions are:

(1) Send a generic letter to all plants outlining the resolution of USI A-17 and providing information developed during the resolution of A-17.

(2) Consider the insights developed in the resolution of USI A-17 for flooding and water intrusion from internal sources in the Individual Plant Examinations (IPE).

(3) Consider systems interactions involving the electrical power systems in the integrated program on electrical power reliability.

(4) Provide information for use in future PRAs.

(5) Provide a framework for addressing those other concerns related to systems interactions which are not covered by the USI A-17 program.

(6) Acknowledge that the resolution of USI A-46 addresses aspects of systems interaction.

(7) Develop a standard review plan for future plants to address protection from internal flooding and water intrusion.

The following discussion addresses the first action. The second action is addressed in the IPE guidance documents. The remaining five actions involve staff actions.

II. INFORMATION RELEVANT TO OPERATING EXPERIENCE EVALUATIONS

A. Background

The adverse systems interactions (ASIs) sorted from the survey of experience appeared to be due to two general causes. Some of the ASIs resulted from obvious errors or failures to meet clearly specified design requirements and/or guidance. Others arose from more subtle causes such as the lack of sufficient consideration, or analysis, of all the significant failure mechanisms or modes and the associated event combinations and/or sequences.

In the case of older plants, the causes often are related to the fact that less design guidance and associated analyses were available and/or required when the plants were licensed.

Although no specific licensee actions are required, the staff concluded that it should communicate to industry certain highlighted concerns identified in the A-17 studies. The insights gained from this information should be beneficial to industry in their ongoing evaluations of operating experience.

B. Highlighted Concerns*

As part of the effort to provide a more focused approach for the resolution of A-17, a set of tasks was defined to accomplish a search of operating experience to accumulate a data bank on the types of common-cause events of concern. The major portion of this work was performed by the Oak Ridge National Laboratory (ORNL), and a summary of ORNL's findings is included in Reference 3.

The search emphasized events included in the LER (licensee event report) 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. The results of the ORNL experience review indicate 23 general categories of events (see Table 1) which have involved systems interactions.

*More details on the highlighted concerns and other ASIs are provided in References 1, 3, and 4, and those documents should be consulted for additional information.

Table 1 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	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

Review of these 23 general categories led to the identification of five areas of highlighted concerns. These are discussed below:

Electric Power System

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 the "Instrumentation and Control Power Supplies" heading below.

As outlined in References 3 and 4, concerns were highlighted in the area of electric power systems in Categories 1 and 13 (Table 1). 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 is not related to safety, various engineered safety feature 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. 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 (References 3 and 4) categorized the electric power system concerns into four areas:

- load sequencing/load shedding
- diesel generator failures caused by specific operating modes
- breaker failures due to loss of dc power
- 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, the A-17 investigation has focused on another concern. Specifically, some ASIs involve scenarios in which a non-safety-related load is supplied by a safety-related bus and is adequately isolated. The non-safety load is part of the normal plant operation and/or control. A failure in the safety-related portion can propagate and create a situation in which a plant transient occurs as a result of non-safety loads supplied by the safety-related bus and, simultaneously, significant safety-related equipment is unavailable because of the same failure.

The most significant events of this type appear to be those that involve the instrumentation and control power systems. As stated below in the discussion of these specific power supplies, the staff believes that current activities in the area of instrumentation and control power supplies should be integrated and should address this type of concern specifically. Accordingly, the staff has initiated an integrated program to review these issues.

Plant Support Systems

Although relatively few events of note were identified from the operating experience (Categories 13, 14, 18, and 22 of Table 1 and References 3 and 4), PRAs have consistently shown the potential importance of support systems. (Note: The electric power system, also a support system, was dealt with separately above.) This category includes other support systems such as component cooling water; service water; heating, ventilating, and air conditioning; lube oil; and compressed air.

As is the case for the electric power system, these support systems are often extensive and may be unique. These support systems can affect multiple frontline safety systems and can often affect systems not related to safety. As a result, failures in support systems can potentially initiate a transient and also can degrade other systems, some of which may have been designed to mitigate that very same event.

The support systems of concern often have interconnections between redundant divisions for operational flexibility or they may have interconnections to non-safety-related equipment. In some cases, single failures such as headers, drain lines, and vents are designed into the systems because the probability of a passive failure in conjunction with the need for the system is assumed to be low.

If the support system failure and the initiation of an event are coupled, a risk-significant situation could result from the failure of the support system (depending on other plant mitigating features).

Less attention may have been paid to the design and review of plant support systems than was paid to some of the frontline systems such as the ECCS. The

safety significance of event initiation coupled with limiting the capability for mitigation may not have been recognized.

Incorrect Reliance on Failsafe Design Principles

Protection systems at nuclear powers plant rely on the design principle of "failsafe" to varying degrees. There have been instances (see Category 18 in Table 1 and References 3 and 4) in which some failure modes were insufficiently analyzed because someone relied too much on the concept of failsafe.

The events to date have involved the scram system and its related support functions such as the air system and electric power system. Specifically, it was discovered that water could be in the scram discharge volume (SDV) of a BWR as a result of poor drainage or an air supply failure. Water in the SDV would inhibit the insertion of control rods. The failure involving the air system was of particular concern because it involved a system that had been considered a portion of the reactor protection system not related to safety. Action was taken at all boiling-water reactors to correct this problem.

This type of ASI may have resulted from the use of a design approach that actually requires of a number of non-safety-related features to function and, therefore, does not truly rely on failsafe principles. In the case of the air system, the system was assumed to fail safe, i.e., bleed off, and, as a result, a partial failure went unanalyzed. It was also noted that the electric supply system to this scram system had been modified previously because of a similar type of concern. Specifically, the electric power was originally assumed to fail safe (i.e., voltage going to zero) and, as a result, partial failure (such as low voltage or high voltage) went unanalyzed for a time.

The problems appear to have been created when portions of the systems were allowed to be classified as not related to safety because they were assumed to always fail safe.

Automated Safety-Related Actions With No Preferred Failure Mode

Another area of adverse systems interactions that was highlighted involved the inadvertent actuation of an engineered safety feature (ESF) (Category 6, "Inadvertent ECCS/RHR pump suction transfer"). The most significant characteristic of this area appears to be that, unlike a reactor trip, such a function does not have an "always preferred" failure mode. As a result, extra precautions may be needed to avoid (a) a failure to actuate when needed and (b) a failure that actuates the system when not required (i.e., inadvertently). The area of automatic ECCS switch to recirculation is the subject of a separate generic issue, Generic Issue 24.

Although the reported events involved only the automatic switchover to the sump in PWRs, some concern exists that individual plants may have other functions with the same characteristic. Some possible other functions include:

- containment isolation functions
- logic that selects a faulted steam generator to isolate it
- low-pressure-to-high-pressure system interlocks in the RHR system

Of particular note is the possibility that these types of functions will actuate inadvertently during testing or maintenance. It is a fairly common practice to put portions of the actuation logic in a trip or actuated state and to assume then that the plant is 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 functions that do not have an always preferred failure mode.

Instrumentation and Control Power Supplies

The ORNL review (NRC, 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 B&W plants, have already received significant attention as outlined in the ORNL assessment. Some residual concern was expressed 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 (reported in Reference 5). A significant number of I&C power supply events were noted, some of which involve ASIs. Although there is concern about the area of I&C power supplies, a significant amount of work (both at NRC and in the industry) has addressed this area. The A-17 resolution has not recommended any specific actions to deal with this area at this time, but has concluded that the existing efforts at NRC be coordinated to ensure that this critical area receives the proper emphasis. This is being done under Generic Issue 128, "Electric Power Reliability."

C. Recommendations

Ongoing industry reviews and evaluations of operating experience should consider the above types of events. It is further recommended that where utilities determine that specific evaluations (e.g., plant walkdowns, limited-scope accident safety analyses, or probabilistic risk assessments) are needed to address other safety concerns, awareness and recognition of potential adverse systems interactions such as highlighted above should be included in these evaluations.

D. References

1. U.S. Nuclear Regulatory Commission, NUREG-1174, "Evaluation of Systems Interactions in Nuclear Power Plants."

2. ---, NUREG-1229, "Regulatory Analysis for Resolution of USI A-17."

3. ---, NUREG/CR-3922, "Survey and Evaluation of System Interaction Events and Sources," January 1985.

4. ---, NUREG/CR-4261, "Assessment of System Interaction Experience in Nuclear Power Plants," June 1986.

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

Enclosure 3

LIST OF RECENTLY ISSUED GENERIC LETTERS

Generic Letter No.	Subject	Date of Issuance	Issued To
89-18	RESOLUTION OF UNRESOLVED SAFETY ISSUE A-17, "SYSTEMS INTERACTIONS IN NUCLEAR POWER PLANTS	09/06/89	ALL HOLDERS OF OPERATING LICENSES OR CONSTRUCTION PERMITS FOR NUCLEAR POWER PLANTS
89-17	PLANNED ADMINISTRATIVE CHANGES TO THE NRC OPERATOR LICENSING WRITTEN EXAMINATION PROCESS - GENERIC LETTER 89-17	09/06/89	ALL HOLDERS OF OPERATING LICENSES OR CONSTRUCTION PERMITS FOR PWRS AND BWRS AND ALL LICENSED OPERATORS
89-16	INSTALLATION OF A HARDENED WETWELL VENT (GENERIC LETTER 89-16)	09/01/89	ALL GE PLANTS
88-20 SUPPLEMENT 1	GENERIC LETTER 88-20 SUPPLEMENT NO. 1 (INITIATION OF THE INDIVIDUAL PLANT EXAMINATION FOR SEVERE VULNERABILITIES 10 CFR 50.54(f))	08/29/89	ALL LICENSEES HOLDING OPERATING LICENSES AND CONSTRUCTION PERMITS FOR NUCLEAR POWER REACTOR FACILITIES
89-15	EMERGENCY RESPONSE DATA SYSTEM GENERIC LETTER NO. 89-15 CORRECT ACCESSION NUMBER IS 8908220423	08/21/89	ALL HOLDERS OF OPERATING LICENSES OR CONSTRUCTION PERMITS FOR NUCLEAR POWER PLANTS
89-07	SUPPLEMENT 1 TO GENERIC LETTER 89-07, "POWER REACTOR SAFEGUARDS CONTINGENCY PLANNING FOR SURFACE VEHICLE BOMBS"	08/21/89	ALL LICENSEES OF OPERATING PLANTS, APPLICANTS FOR OPERATING LICENSES, AND HOLDERS OF CONSTRUCTION PERMITS
89-14	LINE-ITEMS TECHNICAL SPECIFICATION IMPROVEMENT - REMOVAL OF 3.25 LIMIT ON EXTENDING SURVEILLANCE INTERVALS (GENERIC LETTER 89-14)	08/21/89	ALL LICENSEES OF OPERATING PLANTS, APPLICANTS FOR OPERATING LICENSES, AND HOLDERS OF CONSTRUCTION PERMITS