NUREG-0493

A DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT OF THE RESAR-414 INTEGRATED PROTECTION SYSTEM

Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission

Available from
National Technical Information Service
Springfield, Virginia 22161
Price: Printed Copy $5.25; Microfiche $3.00

The price of this document for requesters outside of the North American Continent can be obtained from the National Technical Information Service.

NUREG-0493

A DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT OF THE RESAR-414 INTEGRATED PROTECTION SYSTEM

Manuscript Completed: January 1979
Date Published: MARCH 1979

Division of Systems Safety
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

CONTENTS

Contents (Cont'd)

Contents (Cont'd)

A DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT OF THE RESAR-414 INTEGRATED PROTECTION SYSTEM

1. INTRODUCTION AND SUMMARY

1.1 Background

One of the major innovations of the Westinghouse RESAR-414 design, as compared with previous designs, is its integrated protection system (IPS). This is described functionally in Chapter 7 of the RESAR (Ref. 1) and reviewed as to design criteria in the staff report (Ref. 2) to the Advisory Committee on Reactor Safeguards (ACRS). The ACRS subcommittee (July 24, 1978) and full committee (August 4, 1978) raised questions that dwelled especially on different aspects of the IPS design, with particular emphasis being given to the interconnections among the scram system, the control system, and the engineered safety features actuation system. Similar questions were raised by the staff. In addition, the ACRS report on RESAR-414, dated August 10, 1978 (Ref. 3), includes the recommendation "that the NRC staff give special attention in their review to testing procedures, to the safety problems associated with manufacturing and maintenance errors, and to the potential for adverse interaction between the control, scram, and engineered safety feature functions." This matter was discussed at ACRS subcommittee and full committee meetings.

The question that was to be investigated further is whether the design of the RESAR-414 IPS is satisfactory in view of the interconnections among the control, scram, and engineered safety features actuation systems, and the use of common shared signals for these systems. The concern is that certain classes of failures, which in other designs are likely to be tolerable, have the potential for serious consequences in this design.

The failures of potential concern are common-mode failures (CMF) of redundant elements. (We can adequately protect against independent failures.) The interconnections of the RESAR-414 design have the potential to propagate a CMF, if it were to occur, and to affect the functioning of systems other than the one in which the failure originated. The defense against such failures are, first, care in design, manufacture, and operation, and, second, the use of diversity in the design to provide alternate means of effecting the safety action.

The use of instrumentation systems to deal with control, scram, and engineered safety features functions is part of the defense-in-depth

principle of reactor safety. This principle is firmly established in the safety design of nuclear power plants and is discussed in Section 2 of this report. The present concern, therefore, can be characterized by the question of whether the RESAR-414 design has an adequate degree of defense in depth and includes adequate diversity.

Considering the significance of this concern, and the impact that the solution might have on the RESAR-414 design, the staff initiated a brief but intensive extension of its review of the IPS design (Ref. 4). This report is the result of the extended review effort. The staff studied both the defense-in-depth principle and its application to instrumentation systems in general and the IPS preliminary system architecture in particular. Several meetings were held by the staff with its consultants* and with Westinghouse personnel to discuss the issue (Refs. 5,6,7,8,9).

The staff sees significant benefits in using computers and other advanced technologies in reactor protection systems. Yet the regulatory requirements in this area (the regulations, guides, standards, and Standard Review Plan that form the basis for the staff review) were developed before the use of stored-program computers for reactor control or protection functions. (Appendix B of this report gives data related to defense in depth and to matters in NRC regulations, guides, and Standard Review Plans, and in IEEE standards.) These existing requirements and guides provided a basis for the extended review effort of the RESAR-414 IPS, but were of limited value in the detailed review process. In particular, they provided little guidance on systems interactions. As information on these systems has increased, it has become more evident that development of new regulatory criteria and guidance will be required to ensure that this increased sophistication is not accompanied by design changes that may degrade the defense-in-depth principle.

As a result of its study, the staff has set forth some guidelines for implementing a defense-in-depth analysis of the IPS and has evaluated the design bases and functional approach given by Westinghouse using these guidelines. This defense-in-depth analysis was in addition to the evaluation of conformance to all other requirements for reactor protection systems.

The guidelines developed in this report should be viewed as the initial step in the total development effort. Their application to the RESAR-414 IPS should likewise be viewed as one step of a process that, in the future, will involve the verification program, the RESAR-414 FDA review,

*Staff consultants for the IPS extended review effort were Mr. John L. Anderson and Mr. J. B. Bullock, Oak Ridge National Laboratory, and Mr. Ernest Siddall, Canatom, Ltd.

and construction permit (CP) and operating license (OL) reviews of individual plants using the IPS design. Each successive step in the development will require detailed participation by the industry and review by the NRC.

As a result of the extended review effort, including the application of the defense-in-depth guidelines, Westinghouse has made some changes in the system architecture of the IPS and stated its belief that the revised system meets the NRC staff guidelines.

In the report to the ACRS on RESAR-414 (Ref. 2), the staff concluded that the design criteria and design bases for the integrated protection system met the Commission's requirements and that the Westinghouse design verification program would provide the information to demonstrate that the final design met these criteria and bases. As a result of the extended review effort, the staff had determined that the Westinghouse design principles and the integrated protection system architecture are consistent with the defense-in-depth guidelines. Analyses and tests are required of Westinghouse to demonstrate that the final design will meet the defense-in-depth guidelines. On these bases, the staff concludes that the integrated protection system can meet the Commission's requirement and is acceptable for the preliminary design approval.

Section 2 of this report considers the concept of defense in depth and its application to instrumentation systems. The necessary concepts related to systems architecture and to independence and diversity of redundant subsystems are also defined and illustrated. Section 3 gives the defense-in-depth guidelines for instrumentation systems. Section 4 contains the staff's evaluation of the RESAR-414 IPS, including requirements imposed to provide assurance that the system final design will provide an adequate measure of defense in depth. Section 5 gives a summary of the extended review effort and a discussion of staff conclusions.

1.2 Definitions

The following definitions are used to provide an understanding of the report text, system architecture, and guidelines.

1.2.1 Defense in Depth

The defense in depth includes, as a general principle, design features providing for plant and public safety by the use of overlapping and redundant echelons of defense. For discussion, see Section 2.1.

1.2.2 Echelons of Defense

For reactor instrumentation systems, the echelons of defense are as follows:

1.2.2.1 Scram System

The scram system consists of sensors, signal processors, logic, and actuation initiation devices necessary to effect reactor trip or scram, including essential auxiliary systems. This echelon of defense performs a safety function. The scram system is also known as the reactor trip system.

1.2.2.2 ESF Actuation System

The ESF actuation system consists of sensors, signal processors, logic, and actuation initiation devices necessary to effect functioning of engineered safety features (for example, auxiliary feedwater, containment isolation, emergency core cooling, emergency power), including essential auxiliary systems.* This echelon of defense performs a safety function.

1.2.2.3 Control System

The control system consists of all instrumentation and control equipment not included in the scram or ESF actuation systems, including automatic and manual process controls, presentations of information to the operator (plant monitoring system), and plant computer(s) that are not part of scram or ESF actuation systems. This echelon of defense does not perform a safety function, but is nevertheless important to the defense-in-depth principle.

1.2.3 Channel

The channel is an arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity when single action signals are combined.

1.2.4 Instrumentation System

The reactor instrumentation senses various reactor parameters and transmits appropriate signals to the control systems during normal operation and to

*The scram system plus the ESF actuation system, taken together, are the "Protection System" defined in IEEE-279 and the General Design Criteria.

the scram systems and the engineered safety features actuation system during normal, abnormal, and accident conditions.

1.2.5 Diversity

Diversity is the design approach for achieving a reduced probability of functional failure as a result of postulated common-mode failures, by providing different equipment as redundant backup. The concept is discussed in Section 2.3.

1.2.6 Signal Diversity

Signal diversity is the use of different signals to initiate action, wherein either signal can independently sense the abnormal condition to be protected against, even if the other signal fails in a common-mode failure (CMF). For example, overpower can be independently measured by diverse signals such as neutron flux and reactor coolant temperature rise.

1.2.7 Equipment Diversity

Equipment diversity is the use of different equipment to perform safety functions. "Different" means sufficiently unlike as to decrease significantly the vulnerability to common-mode failures. Examples of equipment diversity are given in item 4.b. of section 2.3.

1.2.8 Common-Mode Failure

Common-mode failures are causally related failures of redundant or separate equipment; thus (1) CMF of identical redundant blocks in different channels or (2) CMF of different subsystems or echelons of defense. In this report, CMF embraces all causal relationships, including severe environments, design errors, calibration and maintenance errors, and consequential failures. This concept is discussed in Section 2.3.

1.2.9 Random Access Memory

The random access memory (RAM) is an on-line storage device into which information can be copied, which will hold this information, and from which the information can be obtained at a later time.

1.2.10 Read Only Memory

The read only memory (ROM) is a storage device that contains information that can be obtained, but not altered by, computer instructions.

1.2.11 Anticipated Operational Occurrences

"Anticipated operational occurrences mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of the turbine generator set, isolation of the main condenser and loss of offsite power" (10 CFR 50, Appendix A, Definitions and Explanations). In the Standard Format, Section 15, "Accident Analysis" (Ref. 11), the classification of transients is discussed. Initiating events are categorized according to their expected frequency of occurrences. Two of the categories are incidents of moderate frequency and infrequent incidents. These are defined as follows:

> "Incidents of moderate frequency - these are incidents, any one of which may occur during a calendar year for a particular plant."
>
> "Infrequent incidents - these are incidents, any one of which may occur during the lifetime of a particular plant."

Incidents within each of these categories are also known as anticipated operational occurrences.

Our review of the Westinghouse classification of postulated events is presented in our Safety Evaluations Report (Ref. 2). We note that Westinghouse has four categories of transients and of faults:

Condition I - Normal Operation and Operational Transients

Condition II - Faults of Moderate Frequency

Condition III - Infrequent Faults

Condition IV - Limiting Faults

Our review concluded (Section 15.3 of the Safety Evaluation Report (Ref. 13)) that Condition I and Condition II events plus the complete loss of coolant flow are anticipated operational occurrences.

1.2.12 Accidents

Accidents are defined as those conditions of abnormal operation that result in limiting faults. In the Standard Format, Section 15, "Accident Analysis" (Ref. 11), limiting faults are defined as follows:

> "These are occurrences that are not expected to occur but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material."

Our review of the Westinghouse classification of postulated events is presented in our Safety Evaluation Report (Ref. 13). We note that Westinghouse has four categories of transients and faults and that Condition IV is "Limiting Faults."

2. TECHNICAL DISCUSSION

2.1 General Principles

The principle of defense in depth is firmly established in the safety design basis of nuclear power plants. The basic idea is to provide several levels or "echelons" of defense so that failures in equipment and mistakes by people will be covered. Thus, the public safety is preserved in spite of failures.

One way to express defense in depth in general is to identify the following three echelons of defense:

1. Designing, building, and operating the plant correctly, with the operating parameters maintained within their normal ranges.

2. Providing protection systems to place the plant in a safe shutdown condition when the limits are exceeded.

3. Providing engineered safety features to maintain essential functions, like decay heat removal and containment isolation, under abnormal conditions.

As an example, consider the loss-of-coolant accident. If such an event were to occur, operation of the emergency core cooling system would be required to prevent unacceptable consequences. There is no echelon of defense provided to cover failure of this system if the accident were actually to occur. But, on the other hand, the design requirements of the reactor primary piping, its quality assurance during construction, periodic in-service inspection, and operation of continuous leak detection systems, all guard against having a loss-of-coolant accident in the first place. Thus we can say that a great deal of defense in depth exists relative to loss-of-coolant accidents, even though there is not another system specifically provided to deal with failure of the emergency core cooling system.

For reactor instrumentation systems, the three echelons of defense are the control system, the scram system, and the engineered safety features (ESF) actuation system.* These work in conjunction with the reactor control rods, fluid system pumps and valves, and so forth, to effect their functions.

*For definitions of these systems, see Section 1.2 of this report.

The scram system plus the ESF actuation system comprise the "protection system" as defined by the General Design Criteria and IEEE Standard 279. This equipment must be designed, fabricated, and tested to high standards and is reviewed in detail by the NRC. The reason for this regulatory emphasis is the importance to safety of the protection system; that is, its importance to the defense-in-depth approach. However, the requirements are specific and do not, in their present form, explicitly involve defense-in-depth considerations. The present review effort explicitly develops the defense-in-depth guidelines which supplement present requirements (single failure criterion, etc.) rather than replace them.

The control system, which includes all instrumentation and control equipment not part of the protection system, is not required to be "safety grade." Rather, the plant design basis includes postulated failures of the control system (as anticipated operating occurrences) for which the scram and ESF actuation systems must provide ample protection. Yet the control system, even though not safety grade equipment, plays an important role in defense in depth. Most disturbances are controlled without the need for action by the protection system. Therefore, it is mainly the control system that determines the frequency of challenges that the protection system has to meet. In an interconnected system like RESAR-414, it is important that transients or control system failures needing protection system action for safety not also induce protection system failure. This concern is expressed by GDC 24, "Separation of Protection and Control System," of 10 CFR 50 (Ref. 19) and within Section 4.7.4, "Multiple Failures Resulting From a Credible Single Event," of IEEE-279 (Ref. 18). This is the reason for involving the control system in this review of RESAR-414, even though it is not directly related to the plant safety systems.

The control system can fail in two ways: (1) the failure changes the controlled variable(s) so that a plant transient is induced; or (2) the system "freezes" so that no transient is induced by the failure but the control system cannot handle a transient when the system is in a failed condition.

Failures in the scram and ESF actuation systems, in general, do not induce transients or accidents but do render the failed system unable to provide the protection if it should be needed. Such failures are not the cause of accidents unless the event needing protection occurs prior to failure detection and repair.

Shared signals or other control-protection interconnections are therefore worthy of special scrutiny as potential agents causing the need for protection (via the control system) and failing the needed protection function.

2.2 Problem of Multiple Failures

If a system could be relied upon to function every time, defense in depth would not be required. In reality, however, such perfection is not attainable. Therefore, in addition to the high reliability required of safety-related systems, defense in depth is used to provide additional assurance of safety despite the imperfections. Most failures are tolerable because of the function of one or more of the other echelons of defense.

Defense in depth is not provided for every possible postulated failure in the control, scram, or ESF actuation system. For example, if the portion of the ESF actuation system that initiates the emergency core cooling system function were to fail during a loss-of-coolant accident, neither the control system nor the scram system could compensate for such a failure. Rather, the defense in depth for this contingency is to be found outside the instrumentation systems, in the piping design, quality assurance, etc., as discussed earlier in this section.

Defense in depth is, however, provided within the instrumentation system for many categories of postulated failures. If the control system fails, the scram and ESF actuation systems provide the needed protection. If the scram system fails, the control system forestalls most needs for scram protection, and the ESF actuation system initiates protection for the most probable events involving scram failure. Similarly, if the ESF actuation system fails, the control system and the scram system forestall the need for ESF actuation for most events. The lower probability events that do not have defense in depth provided by the control, scram, and ESF actuation systems are taken care of in other ways, such as the loss-of-coolant accident example discussed above. The defense-in-depth guidelines of Section 3.3 make these considerations more specific and quantitative.

Of course, the control system and, especially, the scram and ESF actuation systems are designed and operated to make such failures improbable. For the echelons of defense that perform safety functions -- scram and ESF -- severe design requirements, quality assurance, in-service testing, etc., are used to make each of the functions highly reliable.

In order that the defense in depth be effective where it is provided, the different echelons of defense must be available to provide the backup function. The combination of events of concern are, therefore,

the concurrent failures of different echelons of defense. This can, in principle, come about either randomly or causally.

Concurrent independent failures of more than one echelon of defense are not a significant hazard because each safety-related system is required to be designed, constructed, and operated to give adequate assurance that it will function as needed. A large fraction of licensing safety review is devoted to attaining such assurance. Independent multiple failures of safety-related systems are therefore so improbable that they can be ignored for the purpose of this report. The control systems not required for safety are acceptable if failures of control system components or total systems would not significantly affect the ability of plant safety systems to function as required, or cause plant conditions more severe than those for which the plant safety systems are designed (Ref. 20).

In general, we do not have numerical criteria for how low the probability of failure must be for the various systems important to safety. The technology of making such reliability calculations is still under development. As in the past, and for a period of time in the future, we must rely primarily on engineering judgment because of the lack of backup data. The problem of assuring the functioning of a single system is outside the scope of this review because of the concentration of this report on defense in depth and system interaction.

The possibility of causal failure of more than one echelon of defense is the primary concern in considering possible failure of defense in depth. In such events, failures in the different echelons of defense are causally related so that their occurrence is not just the random coincidence of multiple independent failures. This causal relationship can arise in a variety of ways, including an incorrect design, a hostile environment (such as fire or flood), incorrect human actions (such as misoperation), maintenance errors, or a failure in one system inducing failure in another via missiles, or power surges.

All these causal relationships are examples of some form of interdependence between the echelons of defense. An obvious cure would be complete independence of the different echelons. However, this is not possible. The different systems that comprise the different echelons of defense all form part of a single power plant - a single reactor. All their input signals come from a single physical system. All their components are located in the single plant, and many must be located in a single control room. The same operating and maintenance staff uses and cares for them. Their functions are effected in a single plant. These forms of interdependence are necessary and unavoidable. The problem then becomes one of specifying the degree of interdependence that is acceptable, and determining methods to maintain an acceptable level of safety in spite of the presence of that degree of interdependence.

2.3 Separation and Diversity of Instrumentation Systems

In some designs, the sensors for the different echelons of defense are separated from each other. There are nuclear power plants, for instance, where the control system sensors are separated from the scram system sensors. In other designs, these systems are interconnected by sharing of sensors with isolation devices to prevent certain types of failures from propagating from one system to the other.

The separation of control and safety received much attention in the late 1960s, and the following points were made:

1. Random independent component or subsystem failures are adequately mitigated by redundancy and are not, or should not be, an important part of the concern of control/safety interdependence.

2. Given adequate redundancy, the remaining concern is some sort of nonrandom multiple failure. For this discussion, this type of failure is called a common-mode failure (CMF). Included in this term are all the functional, environmental, and human events that can lead to causally related multiple failures.

3. Because the subject of concern is CMF, physical and electrical independence is the beginning, not the end, of the matter. For example, in some systems a signal from one power-range nuclear channel in the scram system is used as an input signal to the control system. The concern was that a failure in the equipment common to both control and scram systems could initiate a transient via the control system and impair the response of the scram system needed for safe shutdown of that transient. The failure would have to be a CMF to be of concern because, otherwise, the remaining unaffected channels in the scram system would be capable of providing the needed protection. An alternate design to avoid common equipment would be to provide a separate identical channel of instrumentation for the control function, which would be electrically independent of the scram system. However, such a condition does not indicate whether or not the postulated CMF would also fail the separate control channel because, being identical, it would perhaps be similarly affected. There are some CMF that would fail control and scram even with the separate identical channel; others would not do so.

4. These considerations lead to the conclusion that "independence" means something more than just using "separate" channels of instrumentation for the different echelons of defense. In the present state of the instrumentation art, two approaches are available to provide the needed independence: (1) designing, installing, and

operating the systems with great attention to the need for physical, electrical, and functional independence; and (2) judicious use of diversity. Both approaches are needed and both approaches are employed concurrently as appropriate. Approach (1) is the subject of many criteria, standards, and guidelines for safety-related instrumentation. Approach (2) is the principal additional provision considered in this report and is the main topic of the defense-in-depth guidelines of Section 3.3. Diversity is the design approach for achieving a reduced probability of functional failure, as a result of postulated common-mode failures, by providing different signals or equipment as redundant backup.

Various forms of diversity have been proposed:

a. Signal Diversity - Use of different signals to initiate action, such as neutron flux and reactor coolant temperature rise (ΔT). Either can sense the abnormal condition to be protected against (in this example, overpower), even if the other fails in a CMF.

b. Equipment Diversity - Use of different kinds of equipment to perform a function. Examples are relay vs solid-state logic, transistor vs magnetic amplifiers, and electrical vs pneumatic signal transmission.

c. Aspect Diversity - Use of different logic levels. An example is use of relays that pick-up to scram vs drop-out to scram.

d. People Diversity - Use of different groups of people to design or maintain different equipment.

5. It is difficult to define how much improvement in safety results from a given kind or degree of diversity. The CMF is principally concerned with those kinds that have not yet occurred and those that have not yet been thought about. The CMF that occurred may have been rectified or shown to be insignificant so one tries to provide against the possible consequences of unspecified CMF by adding some diversity. It is not possible, for an unknown CMF, to analyze or even to judge how much protection the diversity provides. The only available guide is intuition and experience as to what kinds of failures and errors have happened and what kinds of diversity have proved to be helpful. The guidelines in Section 3 of this report are based on the experience of the staff and the industry, as interpreted by the staff.

6. Requirements for separation and diversity are included in various NRC regulations, guides, and Standard Review Plans, and in IEEE Standards. Appendix B gives the texts of the requirements most relevant to the reconsideration of the RESAR-414 IPS. These texts and references show that CMF ("multiple failures resulting from a single event") and diversity are recognized by NRC requirements. However, it must also be stated that, for the last few years, industry and the NRC have generally relied on the earlier review summarized in this section and in the Westinghouse report WCAP-7306 (Ref. 10). That is, Westinghouse systems proposed prior to RESAR-414 were judged to be sufficiently like the one reviewed in WCAP-7306 so that reconsideration of defense in depth was not undertaken. The recognized increased complexity and interconnection of the RESAR-414 IPS led to this reconsideration and, therefore, to the defense-in-depth guidelines of Section 3 and the additional NRC staff positions related to RESAR-414.

2.4 Alternative Approaches

In developing guidelines related to defense in depth, the staff has considered two alternate approaches. The first approach is based on detailed evaluations of postulated CMF in hardware or software; the second is oriented toward specifying an acceptable degree of systems independence. Based on these studies and in the light of present knowledge of and experience with complex interconnected systems, the staff has chosen the second approach.

2.4.1 Approach Using Detailed Evaluation of Common-Mode Failure

In this approach, which is presently not being followed by the staff, the basic idea would be to require hypothesizing the CMF of hardware and/or software at various points in the system. Examples of such postulated CMF considered are loss of the following:

1. All detectors and signal processors associated with a single process variable.

2. All identical equipment modules.

3. All identical digital computer programs or program modules.

4. All data buses and memories controlled by a single computer.

5. All identical multiplex data transmission channels.

The guidelines for such an approach would specify that no credible CMF should cause unacceptable consequences.

Although this approach has strong intellectual appeal, the NRC staff is not pursuing it further at this time for the following reasons:

1. Both the nuclear industry and the NRC staff lack experience in designing and operating such systems in the context of reactor safety. This would cause great difficulty in specifying such things as the "credible CMF" that the designer would be required to postulate.

2. Application of such guidelines seems to involve much more detailed review of system design than is justified by the level of design information presently available, the level of approval involved (PDA), and the staff resources appropriate for the review.

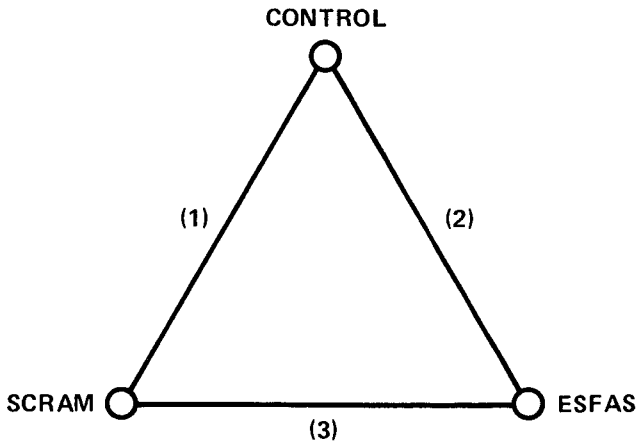
3. Given the lack of experience to date and the present limited information and resources, it seems likely that this approach would involve increasing the depth and detail of each review with time and would result in undesirable instability of requirements.

Instead of pursuing this approach, the staff is using the approach discussed in Section 2.4.2 in the belief that it is a valid way to provide the needed assurance of safety using a different analysis technique.

2.4.2 Approach Using a Specified Degree of System Separation

In view of the difficulties encountered with the approach using postulated specific CMF, the staff has chosen to approach the guidelines for defense in depth by specifying an acceptable degree of system separation. The broad principle is illustrated in Figure 1. The instrumentation of the IPS is subdivided into three functional systems associated with the three echelons of defense discussed in Section 2.1. The three functional systems are required to be sufficiently separated and diverse so that postulated CMF events (defined in the guidelines in Section 3) do not lead to unacceptable consequences. The required separation and diversity have been devised so that detailed hypotheses and analyses of individual CMF are not needed to evaluate acceptability.

The three systems -- control, scram, and ESFAS -- can be interconnected via the three paths marked (Refs. 1,2,3) in Figure 1. In a given design, one or more of these paths may be present, and in some designs each path on the diagram may represent one or more actual interconnections. Where an interconnection path is not present in a given design, the systems are to that degree separate, and defense in depth is maintained by such separation.



LEGEND:
(1), (2), (3) – INTERCONNECTION PATHS

Figure 1. Schematic Representation of an Interconnected Control, Scram, and Engineered Safety Features Actuation System.

The defense-in-depth analysis proceeds by postulating CMF events and defining their consequences; that is, determining if more than one echelon of defense is impaired. This analysis deals with the instrumentation systems, where the interconnections and shared signals are known to have the potential for CMF to influence more than one echelon of defense. Although safety equipment other than instrumentation is obviously part of the defense-in-depth principle, analysis of non-instrumentation equipment is outside the scope of the present review.

The CMF to be hypothesized for the defense-in-depth analysis are of three general kinds:

1. Some failures have the capability to induce plant transients for which scram and/or ESF function is needed. Defense-in-depth analysis requires that any credible failure of this type should not significantly impair the safety function. Interconnection paths of types (1) and (2) in Figure 1 are the ones to be considered for these failures. Diverse equipment or signals not impaired by the postulated CMF must be provided to effect the needed scram or ESF.

2. Alternatively, failures that do not indirectly cause plant transients requiring safety action could still impair the safety function. Such failures would persist in general until they were discovered and repaired. Such failures would have serious consequences only if an event needing safety action were to occur while the system was in the failed state, after the failure had occurred, and before the failure was discovered.

   The design, qualification, and in-service testing of safety systems is designed to minimize the probability of failures of all types, including this one. Moreover, the plant is designed so that challenges to the safety systems occur at a manageably low rate; this is why the first echelon of defense is important even though not directly related to safety.

   Insofar as defense-in-depth analysis is concerned, the only CMF events of this category to be analyzed are those involving scram failure where ESF are needed to mitigate the consequences. This interconnection is shown at interconnection path (3) in Figure 1. In RESAR-414, the mitigating systems for ATWS are auxiliary feedwater, power-operated relief valves, and turbine trip. Only for initiating events of moderate and high frequency (anticipated transients) is the interaction a concern. Postulated event sequences of this type, anticipated transients without scram (ATWS), are the subject of ongoing regulatory consideration as discussed in Appendix A to this report.

3. In addition to analyzing the consequences of postulated CMF in the preceding items 1 and 2, the staff has decided that a separate analysis should be made of the signal diversity For each anticipated operational occurrence in the design basis occurring in conjunction with a CMF, sufficient signal diversity should be provided in the design so that the plant can be brought to a stable hot standby condition. Long-term cooling should be available in the hot standby condition for bringing the plant to a cold shutdown. The plant response calculated using conservative analyses should not result in a non-coolable geometry of the core or violation of the integrity of the primary coolant pressure boundary or violation of the integrity of the containment

2.5 Block Concept

The concept of dividing the instrumentation systems into blocks (for definitions, see Figure 2 and Section 3.2) was devised as a systematic way to evaluate the defense in depth of a design. The blocks containing groups of components provide a mechanism for the analysis approach discussed in section 2.4.2. The guidelines of Section 3 and the evaluation of the RESAR-414 IPS design in Section 4 are based on the block concept. The basic idea is to aggregate the components and modules of the system into a manageably small number of functional units, or blocks, to systematize the postulation of CMF and the analyses of the consequences of these postulated CMF.

The simplest architecture would be a number of independent redundant channels, each with independent functional systems for control, scram, and ESF. Some systems look like this, but the IPS does not. The multiple use of signals in the IPS is contrary to the simple control/scram/ESF architecture, yet it is acceptable in principle as discussed in Section 2.3. In systems like IPS, then, the sensors and signal processors cannot be separated into functional systems.

Exceptions to the general separation are necessary, practical, and, in some instances, desirable. They are treated separately; for example:

1. Use of certain signals for more than one function.

2. Use of certain signals for post-accident monitoring.

3. Transmission of variables and system status (channel and system trips, bypasses, etc.) to the plant computer and the control boards.

The approach adopted by the staff for evaluation of defense-in-depth analysis for systems like IPS is to divide the sensors and signal processors into blocks, as defined in Section 3.2 and shown in Figure 2. All sensors are part of measured variable blocks (MVB). An MVB may also contain amplifiers, function generators, multipliers, etc., for signal processing. The equipment may be pneumatic, electric, analog, or digital.

Input signals for manual controls, calibration, and test signals are also permissible. The output signal(s) may be the value of a measured or derived variable and/or logic signals such as the output of a comparator.

An additional level of calculation is provided for by the use of derived variable blocks (DVB). The DVB accommodates the calculational dependencies of the Westinghouse RESAR-414 design within the block evaluation scheme. A DVB receives signals from two or more MVBs and provides additional signal processing.

Output signals from MVBs and DVBs as appropriate are sent to command blocks (CB) for further calculations as required and for logical manipulation. The CBs are also the foci of the intercommunication between redundant channels necessary to provide coincidence to the safety logic. The output signals from a CB go to the system whose operation is to be controlled or to the monitoring equipment.

Allowable and forbidden interconnections between blocks are given in the guidelines of Section 3. The guidelines present diversity requirements in terms of postulated CMF of the same block(s) in all redundant channels. It is the staff's belief that the application of these guidelines provides a conservative means of assessing the effects of common-mode failure. This conservatism arises from the postulated CMF of the block prescribed in the guidelines. In this way, the aggregation of equipment into blocks, plus the assumed failures of blocks, constitute a conservative CMF analysis of the entire system.

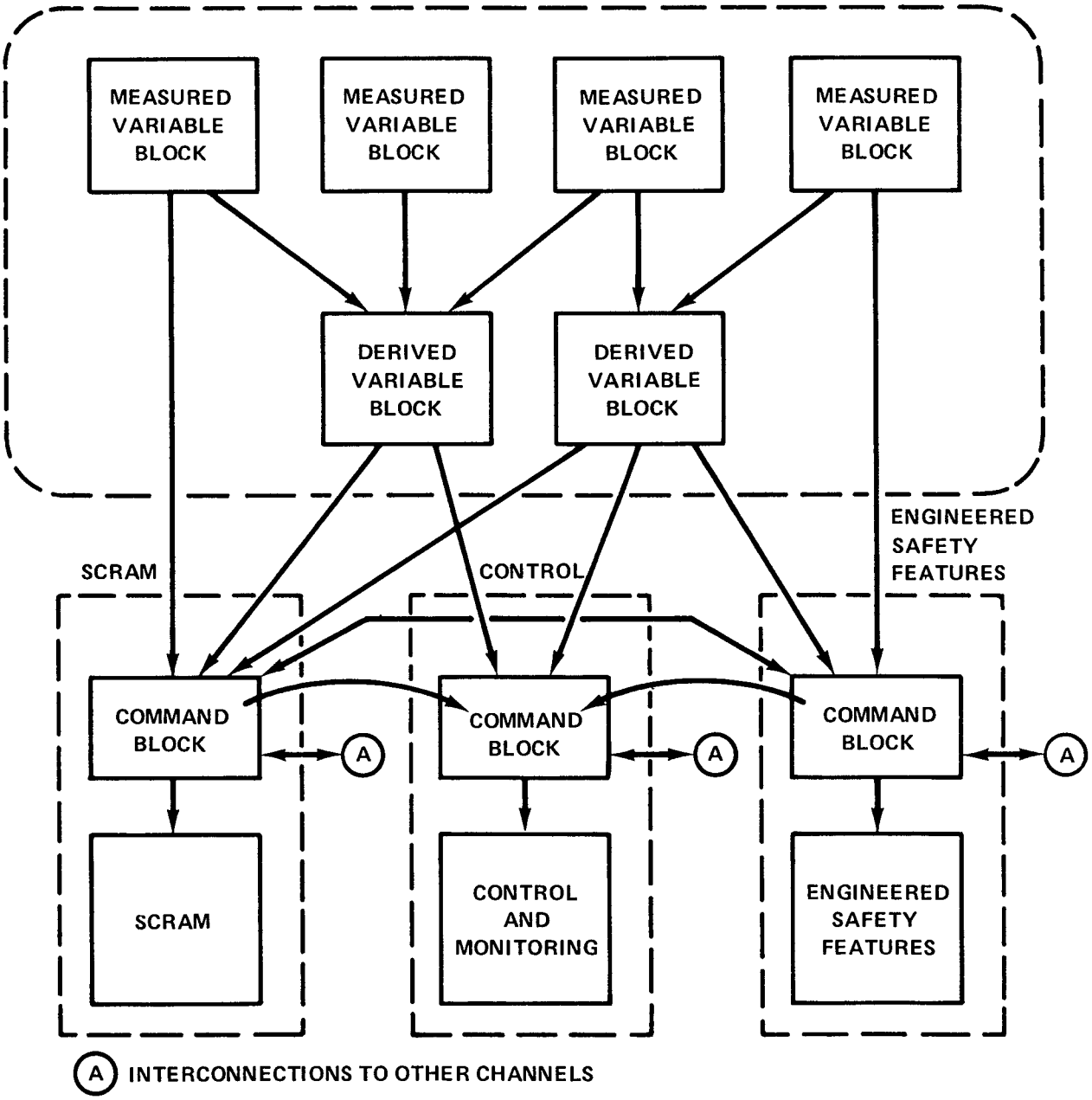


Figure 2. Basic System Architecture for Evaluation of Defense-in-Depth Principle.

3. GUIDELINES

3.1 Background

The defense-in-depth guidelines of this section are to be applied in addition to all other relevant and applicable requirements the instrumentation system must meet. They were developed based on the block concept, as described in Section 2.5.

These guidelines have been discussed with Westinghouse in various drafts during the RESAR-414 extended review effort. Westinghouse personnel offered many useful comments during these exchanges. Westinghouse representatives have verbally and informally stated their belief that RESAR-414 can meet guidelines like these, recognizing the fact that the guidelines are still evolving. Westinghouse does not agree that the guidelines are necessary or that they represent final guidelines for separation and diversity of instrumentation for the design of the RESAR-414 IPS. The staff has nevertheless used these guidelines in the extended review effort of RESAR-414, and has established staff requirements for the RESAR-414 FDA review as given in Section 4 of this report.

3.2 Definition of Blocks

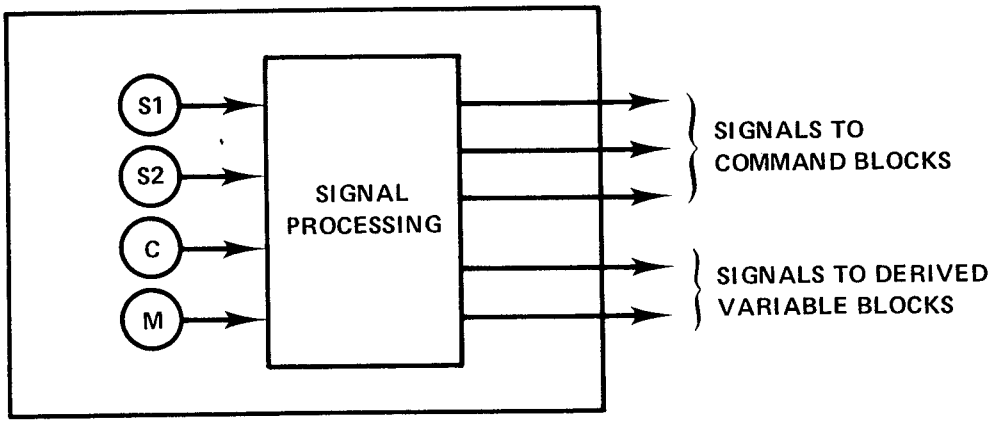
To conduct a defense-in-depth analysis, components of the system architecture must be defined. A block is a functionally separate group of equipment or software that is (and is in some guidelines required to be) considered as a unit in defense-in-depth analysis. This concept is discussed in Section 2.5. The different types of blocks are defined in the following sections.

3.2.1 Measured Variable Block (MVB)

INPUTS: One or more sensors (S); manual (M); calibration and testing (C); each sensor in one block only.

OUTPUTS: To one or more derived variable block(s) and/or command block(s). MVB output signals may not be used as input signals for other MVBs.

MISSION: Receive and process sensor, calibration and manual signals, and initiate control, scram, and/or ESF command blocks. May also provide input signals to DVBs.

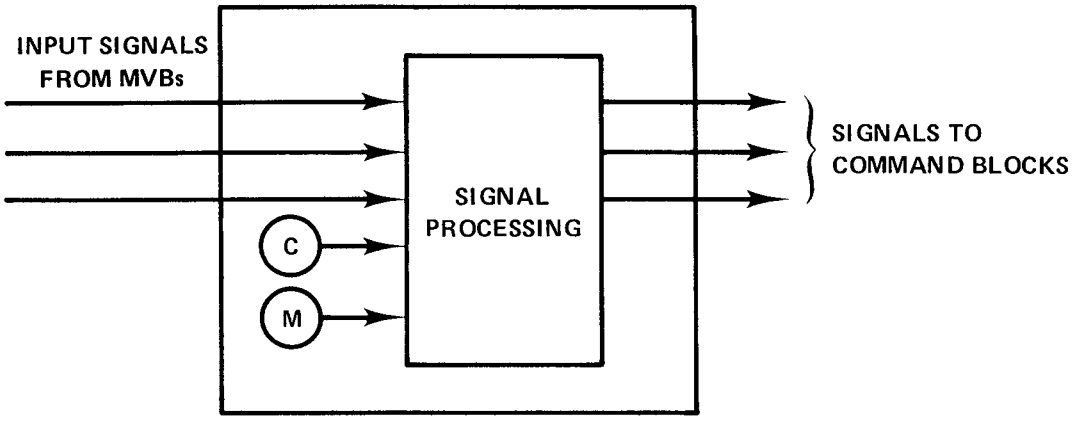


3.2.2 Derived Variable Blocks (DVB)

INPUTS: One or more MVBs and/or DVBs; manual (M); calibration and testing (C).

OUTPUTS: One or more command blocks.

MISSION: Receive MVB signals and provide signals to one or more command blocks.

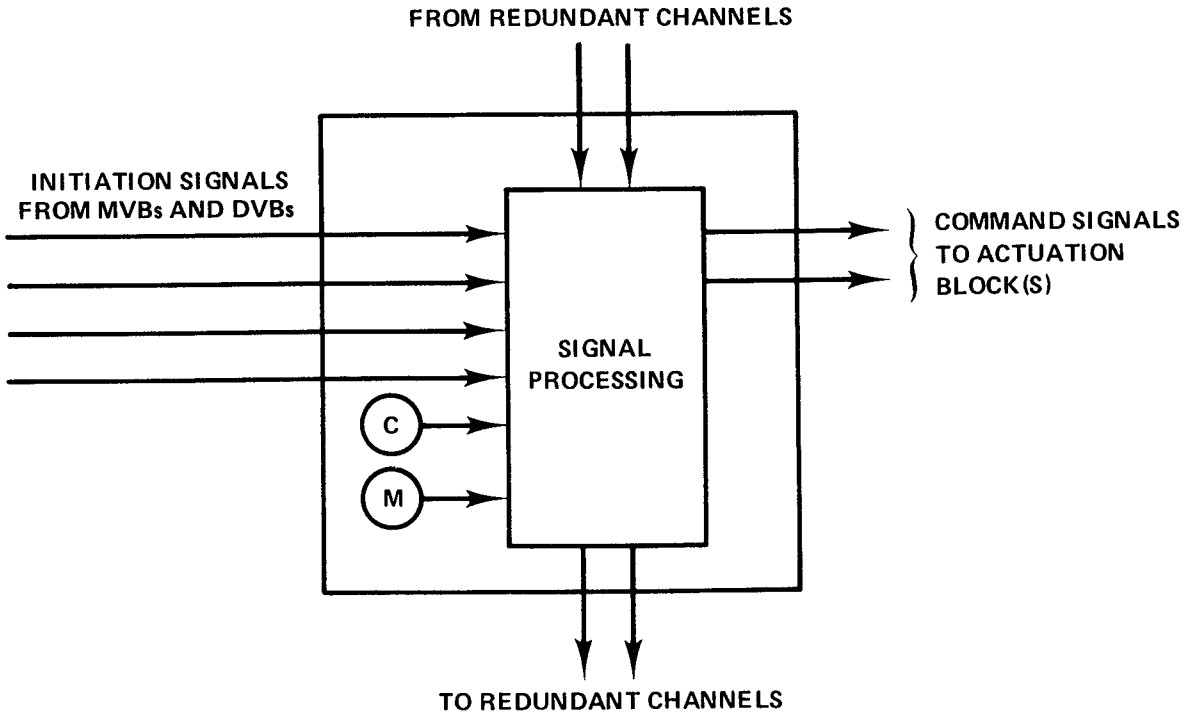


3.2.3 Command Block (CB)

INPUTS: Signals from one or more MVB(s) and/or DVB(s); manual (M); calibration and test (C); and from its counterparts in redundant channels.

OUTPUTS: Signals to actuate block; and to its counterparts in redundant channels.

MISSION: Receive and process signals and provide command signals to its actuation block and to its counterpart(s) in redundant channels.



3.2.4 Functional Independence

For a defense-in-depth analysis, an output signal of block Y is functionally independent from block X if the hypothesized failure of block X does not impair the functional capability of the given output signal of block Y.

3.3 Guidelines

3.3.1 Guideline 1 - General Requirement

The instrumentation system should provide three echelons of defense in depth: control, scram, and ESF. The design Guidelines 2 through 9 are intended to provide the assurance that an adequate degree of defense in depth is provided. The classes of postulated failures to be included in the defense-in-depth analysis are defined, and the diversity requirements are stated. These guidelines are to be applied in addition to all existing criteria, standards, and guidelines related to the design, construction, and operation of reactor protection systems and safety-related instrumentation.

3.3.2 Guideline 2 - Method of Evaluation

The instrumentation system should be subdivided into redundant channels, and each channel should be analyzed as consisting of blocks as defined in Section 3.2 and Figure 2, and discussed in Section 2.5. Each block should be analyzed as a multiple "black box," so that any failure required to be postulated to occur within the block fails all output signals. The output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences when analyzed in accordance with Guideline 7. Justification for the failure assumed must be provided.

3.3.3 Guideline 3 - Postulated Common-Mode Failure of Blocks

Analysis of defense in depth should be performed by postulating concurrent failures of the same block or blocks in all redundant channels. The output signals of the blocks thus postulated to fail should be in accordance with Guideline 2. Subject to Guidelines 4, 5, and 6, concurrent failure of the same single block in all channels should be postulated, with each single block being selected in turn. The analysis then consists of postulated failures of all blocks, taken one by one.

3.3.4 Guideline 4 - Use of Identical Hardware and Software Modules

To limit the postulated CMF to a single block in all redundant channels, the likelihood of CMF among different blocks in the same channel should be shown to be acceptably low. A numerical standard has not been developed. Acceptability will be based on programs of qualification, design verification, system validation and testing, and on the depth and breadth of experience with the equipment. Special attention is required for (1) novel hardware, software, or application; (2) design and programming errors and common maintenance or modification errors; (3) severe environmental conditions, including abnormal conditions such as electromagnetic interference, temperatures, pressures, humidity, wetting, mechanical forces, which must be considered as possible causes of CMF; (4) cables, piping, and other interconnecting paths; and (5) common facilities such as shared power supplies in the various echelons.

3.3.5 Guideline 5 - Effect of Other Blocks

The analysis should include propagation of the postulated CMF in the single block in each channel via its output signals to all the other blocks influenced by these signals, directly or indirectly. Subject to Guidelines 4 and 6, these other blocks may be assumed to function correctly, in accordance with the true and false input signals they receive.

3.3.6 Guideline 6 - Output Signals

Each block should be designed so that it cannot be significantly influenced by any credible change or failure of equipment to which its output signal or signals are connected. For cases in which a single block has more than one output signal, no output signal should be significantly influenced by any credible change or failure of equipment to which any other output signal is connected. This guideline includes any signal transmission path involving a shared memory. For cases in which compliance with this guideline cannot be demonstrated, concurrent failure of the interconnected blocks should be postulated rather than the single failure of Guideline 3.

3.3.7 Guideline 7 - Diversity for Anticipated Operational Occurrences

Sufficient diversity should be provided in the design so that, for each anticipated operational occurrence in the design basis* (Ref. 11) occurring in conjunction with each single CMF postulated in accordance with Guide-

*For RESAR-414, these are the Conditions I and II plus complete loss of coolant flow as specified by Section 15.3 of the Safety Evaluation Report (Ref. 13).

lines 3 through 6, the plant response calculated using conservative analyses should not result in a non-coolable geometry of the core or violation of the integrity of the primary coolant pressure boundary or violation of the integrity of the containment.

3.3.8 Guideline 8 - Diversity Among Echelons of Defense

3.3.8.1 Control/Scram

When a CMF postulated in accordance with Guidelines 3 through 6, can result in a plant response that requires scram and also can impair the scram function, diverse means, which are not subject to or failed by the postulated CMF, should be provided to effect the scram function and to ensure that the plant response calculated using conservative analyses should not result in a non-coolable geometry of the core or violation of the integrity of the primary coolant pressure boundary or violation of the integrity of the containment.

3.3.8.2 Control/ESF

When a CMF postulated to occur in accordance with Guidelines 3 through 6 can result in a plant response that requires ESF and can also impair the ESF function, diverse means not subject to or failed by the postulated CMF should be provided to effect the ESF function to ensure that the plant response calculated using conservative analyses should not result in a non-coolable geometry of the core or violation of the integrity of the primary coolant pressure boundary or violation of the integrity of the containment. The diverse means may include manual operator action under the following conditions:

1. The postulated CMF and its effects do not impair any related aspect of the manual action; and

2. Sufficient information is available to the operator; and

3. Sufficient time is available for operator analysis, decision, and action; and

4. Sufficient information and time are available for the operator to detect, analyze, and correct reasonably probable errors of operator function.

3.3.8.3 Scram/ESF

Interconnections between scram and ESF (for interlocks providing for scram initiation if certain ESF are initiated, or ESF initiation when a scram occurs, or operating bypass functions) are permitted, provided that all guidelines are satisfied, with special attention being given to Guidelines 5 and 6.

The interaction between the scram system and the ESF actuation system is considered in the "Technical Report on Anticipated Transients Without Scram for Light Water Reactors" (Ref. 12). The staff has recommended rulemaking on this issue, as described in Appendix A herein. Further guidance will be developed as a result of that rulemaking.

3.3.9 Guideline 9 - Plant Monitoring

Signals may be transmitted from the scram and ESF actuation systems to the control system for plant monitoring purposes, provided that all guidelines are met, with special attention being given to Guidelines 5 and 6.

Connections and software that are used to enable the plant monitoring system to maintain surveillance of the scram and/or ESF actuation systems should not significantly reduce the reliability of, nor add significantly to, the complexity of the scram and/or ESF actuation systems.

The design should be such that failure of the plant monitoring system does not directly influence the functioning of the scram or ESF actuation systems. The design should also address the possibility that failure or misoperation of the plant monitoring system might cause the operating staff to make adjustments in the scram and/or ESF actuation systems, or in-plant operating parameters, that could cause or allow plant operation to be outside the safety limits or to be in violation of the limiting conditions for operation.

4. APPLICATION OF DEFENSE-IN-DEPTH GUIDELINES TO RESAR-414 INTEGRATED PROTECTION SYSTEM

4.1 Introduction

In the NRC staff report to the ACRS on RESAR-414 (Ref. 2), the staff concluded that the integrated protection system was acceptable for preliminary design approval. This conclusion was based on staff review of the design criteria and design bases for the system in conjunction with the assessment of the functional requirements, specifications, design, development, testing, and quality assurance programs during the design verification program. However, during the ACRS meetings on RESAR-414 and in the subsequent ACRS report (Ref. 3), questions were raised in regard to several design aspects of the integrated protection system. In particular, the potential for adverse interaction between the control, scram, and engineered safety features functions was questioned. Testing procedures and safety problems associated with manufacturing and maintenance errors were identified as an area for which special review attention was recommended. As noted in Sections 7.1 and 7.7 of the report to the ACRS (Ref. 2), the staff also recognized these as key areas for review.

Considering the significance of these matters and the impact that their resolution might have on the RESAR-414 design, we concluded that our preliminary design approval review of the integrated protection system should be extended and additional review completed and the results reported in the staff safety evaluation report on RESAR-414 (Ref. 13). The objectives of this additional review effort were (1) to develop more specific design guidelines for using digital computer and other advanced tehnologies in safety systems and to ensure that this increased sophistication would not degrade the principle of defense in depth by increasing interactions between control, scram, and engineered safety features functions; (2) to evaluate the architecture of the RESAR-414 integrated protection system with respect to these guidelines; and (3) to identify any design modifications and/or additional analyses required to address these concerns.

The defense-in-depth guidelines have been presented in Section 3 for the instrument systems. The results of our evaluation of the architecture of the integrated protection system and additional required modifications and analyses are presented in the following sections.

4.2 RESAR-414 Instrumentation and Control System Architecture

Our evaluation of the design of the RESAR-414 integrated protection system is presented herein. A description of the system and a summary

of Westinghouse's preliminary evaluation of defense in depth for the system is also presented.

4.2.1 Description of Integrated Protection System Design

The RESAR-414 integrated protection system is a distributed process microcomputer based system. The following description of the system design is based on information provided to the staff by Westinghouse. The information consisted of block diagrams, schematics, design bases, design criteria, and descriptive material in supplement to RESAR-414, and was presented to the NRC staff during a series of meetings with Westinghouse (see References 5, 6, 7, 8, 9 and 21).

The major elements of the RESAR-414 instrumentation systems and their interrelationships are shown in Figure 3. The instrumentation system is considered to consist of three sequential portions: the "sense" portion, the "command" portion, and the "execute" portion.

The sense portion transduces process parameters into signals for use by the command system. The command portion operates on signals from the sense portion and generates output signals that direct the execute portion. The execute portion consists of the mechanical and electrical equipment that is actuated by signals from the command system. As also shown in Figure 3, the instrumentation system is divided into two parts, the safety system and the nonsafety system (IEEE-603). The nonsafety system includes the sensors, integrated control cabinets, integrated control logic cabinet, and control actuators (such as motors, valves, and breakers) that perform the sense, command, and execute functions of the integrated control system. The safety system includes the sensors, integrated protection cabinet, integrated logic cabinet, and reactor protective actuators. The reactor protective actuators are the scram breakers that provide a reactor trip and the motors, valves, and breakers that provide the engineered safety features. The integrated protection cabinet houses the equipment that develops the sense and command signals for reactor trip. The integrated protection cabinet also provides sense and command signals for use by the integrated logic cabinet in generating engineered safety features commands and for use by the integrated control system in developing control system commands.

The integrated protection cabinet architecture has been developed as shown in Figure 4. The sense features of the integrated protection cabinet are accomplished by two types of modules: measured variable conditioner, and derived variable calculators. The measured variable conditioner consists of the equipment, including the sensor, that transduces process variables into signals for use by derived variable calculators or for use by the command subsystems. Derived variable calculators consist of the equipment that operates on one or more signals from measured variable conditions for use by the command subsystems.

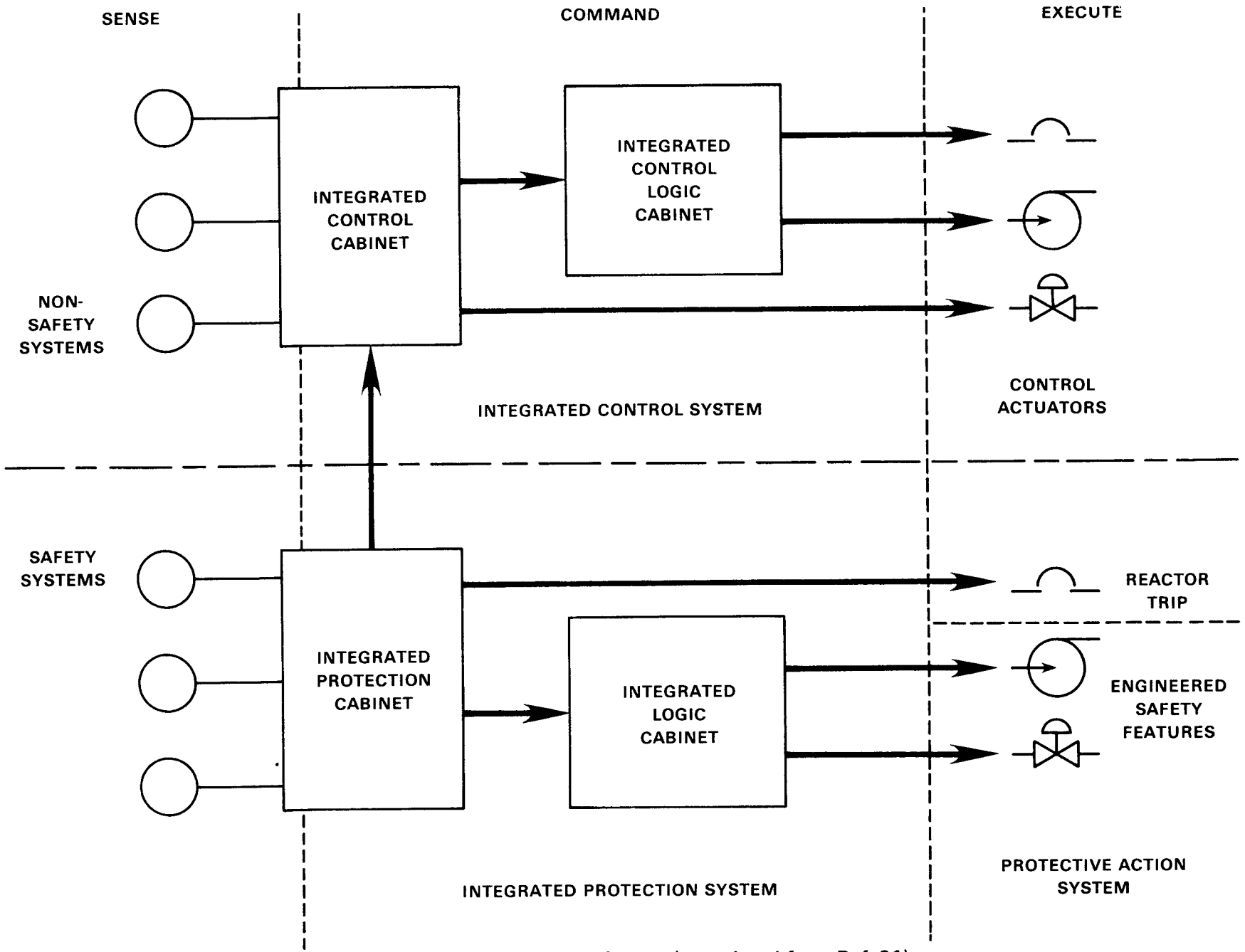


Figure 3. Westinghouse Safety System (reproduced from Ref. 21).

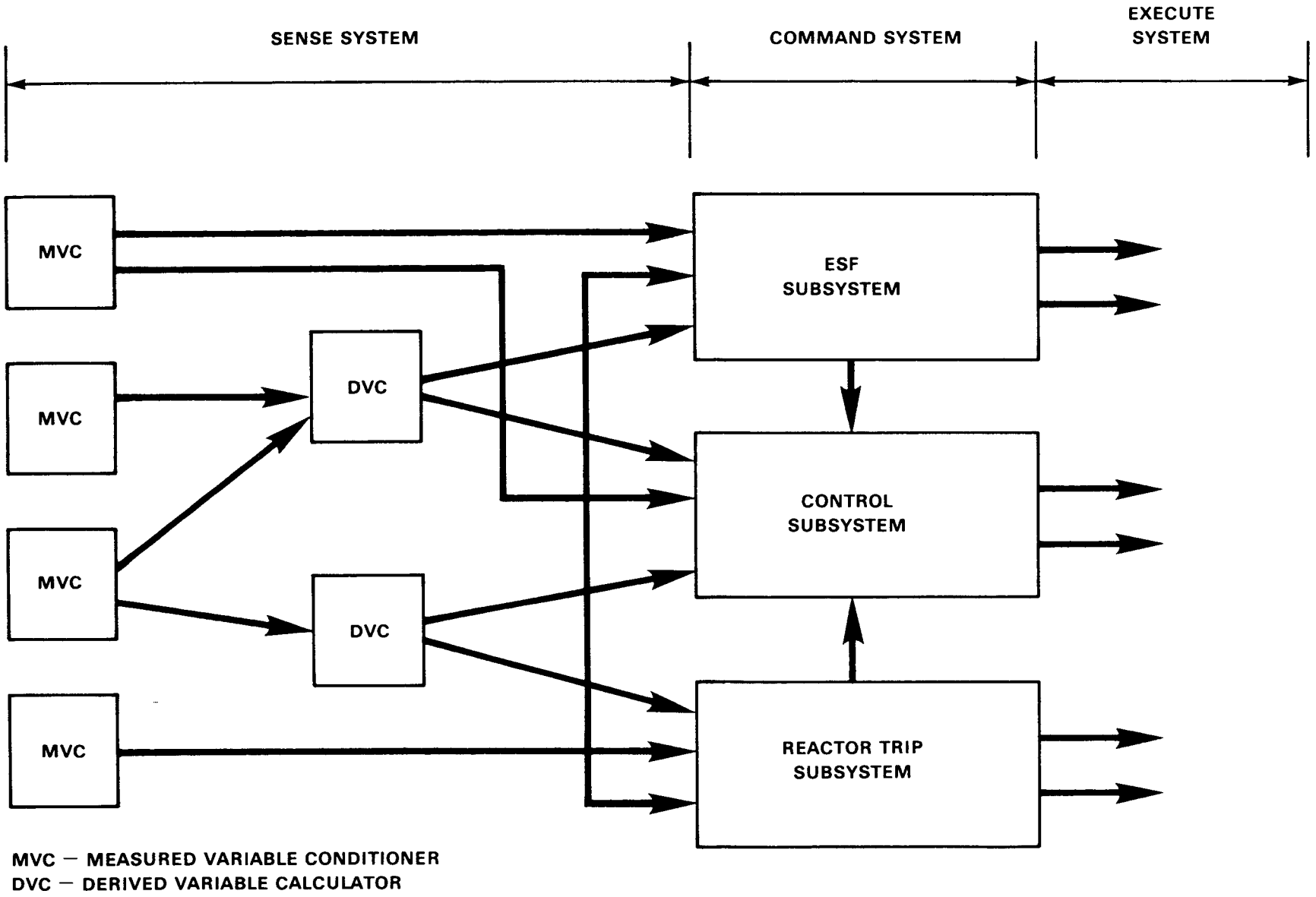


Figure 4. Westinghouse Instrumentation and Control System (reproduced from Ref. 21).

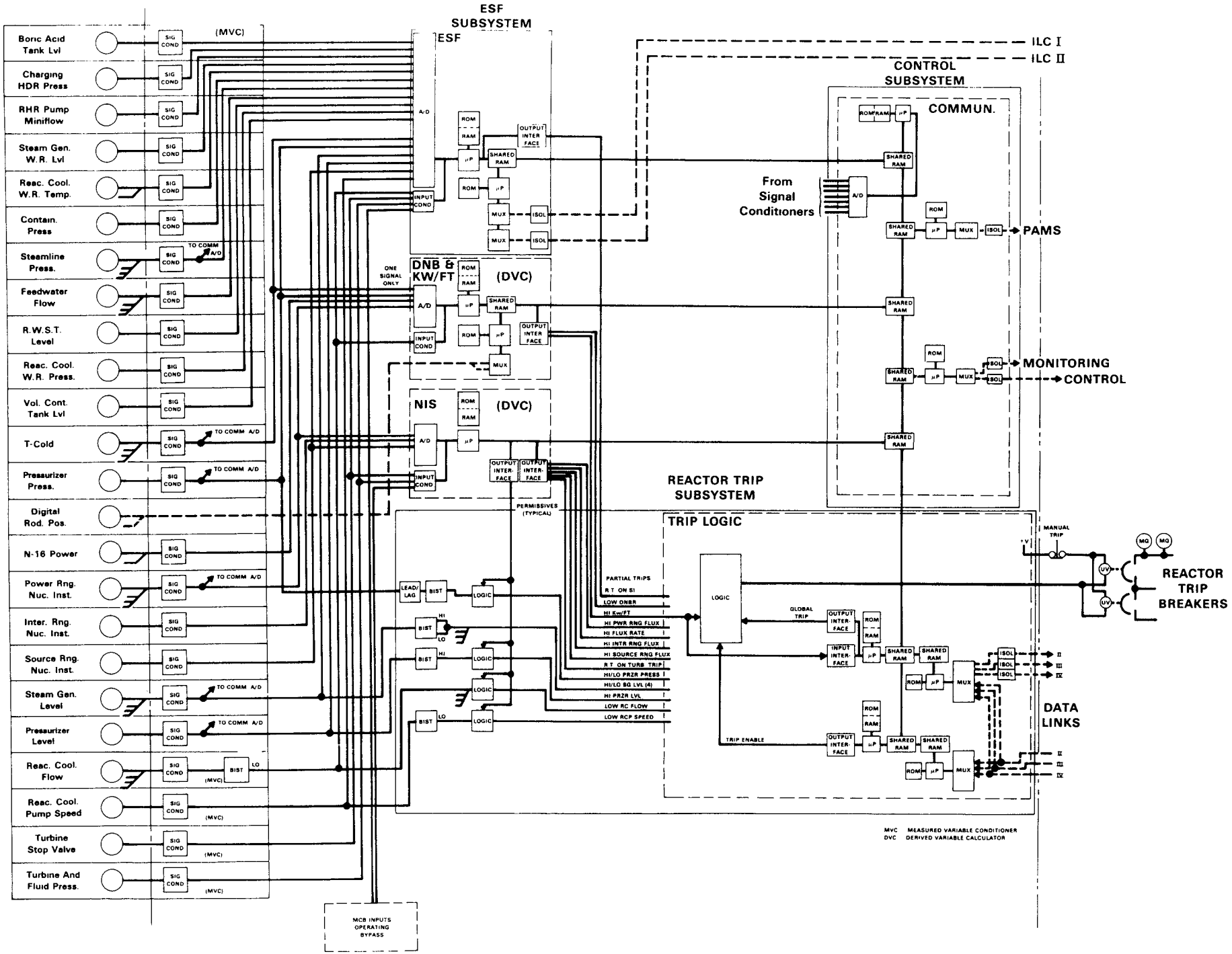
The command portion of the integrated protection cabinet is provided by three modular subsystems: the engineered safety features subsystem, the control subsystem, and the reactor trip subsystem. The three subsystems receive signals from measured and derived calculators and output command signals as follows: (1) the engineered safety features subsystem generates command signals for use by the integrated logic cabinet in developing commands to execute engineered safety features systems functions; (2) the control subsystem generates command signals for use by the integrated control system in developing commands to execute control functions; and (3) the reactor trip subsystem generates command signals for actuating a reactor trip by deenergizing the control rod trip breakers. The three command subsystems are allowed to communicate to each other as follows: (1) the reactor trip and engineered safety features subsystems provide surveillance information signals to the control subsystem for monitoring and recording by the plant computer and post-accident monitoring system; and (2) the reactor trip and engineered safety features subsystem provide interlock information signals between each other such as reactor trip on safety injection and operating bypass permissives.

4.2.2 Westinghouse's Preliminary Evaluation of Defense in Depth

Westinghouse has stated (see Refs. 1 and 21) that the architecture of the RESAR-414 instrumentation and control systems, including the integrated protection system and the use of signals from the integrated protection system for control does not violate the principles of defense in depth. Westinghouse performed a preliminary evaluation of the integrated protection system design using an approach similar to the block concept and guidelines described in Sections 2 and 3 of this report. The evaluation approach used by Westinghouse is presented in Reference 21.

Based on an initial review of the integrated protection cabinet using the proposed criteria presented in Reference 21, Westinghouse modified the preliminary architecture to improve the separation and independence between the three command subsystems. The architecture of the integrated protection cabinet, as modified, is shown in Figure 5. Westinghouse has stated that diverse signals are provided in the sensing portions of the integrated protection cabinet. The diverse signals will independently provide protective actions to adequately mitigate the consequences of the common-mode failure followed by a transient. In addition, the signals from the integrated protection cabinet to the execute portion of the reactor trip and to the command portions of the integrated control system and the engineered safety features are stated by Westinghouse to be separated and generated independently of each other.

Westinghouse has stated that, based on the architecture in Figure 5, the integrated protection system provides diversity to protect against


ESF SUBSYSTEM
ESF
(MVC)
Boric Acid Tank Lvl
Charging HDR Press
RHR Pump Miniflow
Steam Gen. W.R. Lvl
Reac. Cool. W.R. Temp.
Contain. Press
Steamline Press.
Feedwater Flow
R.W.S.T. Level
Reac. Cool. W.R. Press.
Vol. Cont. Tank Lvl
T-Cold
Pressurizer Press.
Digital Rod. Pos.
N-16 Power
Power Rng. Nuc. Inst.
Inter. Rng. Nuc. Inst.
Source Rng. Nuc. Inst.
Steam Gen. Level
Pressurizer Level
Reac. Cool. Flow
Reac. Cool. Pump Speed
Turbine Stop Valve
Turbine And Fluid Press.
SIG COND
TO COMM A/D
DNB & KW/FT
(DVC)
NIS
ONE SIGNAL ONLY
MCB INPUTS OPERATING BYPASS
ILC I
ILC II
CONTROL SUBSYSTEM
COMMUN.
From Signal Conditioners
PAMS
MONITORING
CONTROL
REACTOR TRIP SUBSYSTEM
TRIP LOGIC
PERMISSIVES (TYPICAL)
PARTIAL TRIPS
R.T. ON SI
LOW ONBR
HI Kw/FT
HI PWR RNG FLUX
HI FLUX RATE
HI INTR RNG FLUX
HI SOURCE RNG FLUX
R.T. ON TURB TRIP
HI/LO PRZR PRESS
HI/LO SG LVL (4)
HI PRZR LVL
LOW RC FLOW
LOW RCP SPEED
GLOBAL TRIP
TRIP ENABLE
MANUAL TRIP
REACTOR TRIP BREAKERS
DATA LINKS
MVC MEASURED VARIABLE CONDITIONER
DVC DERIVED VARIABLE CALCULATOR

common mode failures similar to that demonstrated in Topical Report WCAP-7306 (Ref. 10). Westinghouse has noted that the analysis to verify this statement has not been performed for the RESAR-414 instrumentation system and that the following assumptions are also included by Westinghouse as part of its proposed basis (reproduced from Ref. 21):

1. "These criteria are limited to defense-in-depth considerations which deal with interdependence between control and reactor trip and interdependence between control and engineered safety features.

2. "The approach to design and analysis documented in WCAP-7306 is acceptable for RESAR-414 for interdependence between control and reactor trip and interdependence between control and ESF. The acceptance criteria for the diverse (backup) protective actions are less restrictive than those for the primary protection actions and shall be bounded by 10 CFR 100 on a best estimate basis. In this regard the probability of CMF's are considered to be lower than the probability for failures which establish the requirements for the primary protective actions.

3. "The consideration of CMF's as addressed by these criteria are based on system design and operation errors. CMF's associated with components (both hardware and software components) are not considered a credible cause for interdependence between the three echelons of defense because they can be adequately dealt with by design verification and qualification testing programs. For example, the use of shared memory is permitted provided the verification program results are acceptable.

4. "Manual actuation of protective functions is acceptable as a backup to automation actuation provided the manual actuations meets specific established criteria.

5. "Interdependence between reactor trip and ESF is outside the scope of this review of RESAR 414 because this is identical to the ATWS issue which is being treated as a separate generic issue."

Westinghouse has commented on the guidelines presented in Section 3 of this report, which are included in Reference 21. In providing these comments, Westingouse states that this does not constitute an agreement on the part of Westinghouse that the guidelines are either necessary or that they represent final guidelines for separation and diversity of instrumentation and control for the design of the RESAR-414 integrated protection system.

4.2.3 Staff Evaluation of the RESAR-414 Integrated Protection System for Defense-in-Depth Principle

In our review of the RESAR-414 instrumentation system architecture for the application of the defense-in-depth principle, we identified our concern that a common-mode failure in the integrated protection cabinet could result in the loss of all three of the defense-in-depth functions. That is, the failure could result in a control system transient and, at the same time, disable the reactor trip and/or engineered safety features designed to mitigate the consequences of that transient.

We have reviewed the integrated protection system architecture based on the defense-in-depth guidelines identified in Sections 2 and 3. Based on our review, we conclude that the architecture, as shown in Figure 5, is acceptable for preliminary design approval. The preliminary design approval is predicated on the satisfactory completion of analyses, tests, and resolution of concerns stated herein. We have reasonable assurance that Westinghouse can satisfactorily complete this additional work. The basis of our preliminary design approval and the conditions of our approval are discussed in the following paragraphs.

The staff made an evaluation of the architecture of the integrated protection system presented in Figure 5. The evaluation was based on Guidelines 1 and 2 of Section 3. We note that the architecture presented in Figure 5 provides for three echelons of defense consisting of control, scram, and ESF. Also from Figure 5 and the definitions provided in Reference 21, the following blocks in the terminology of Section 3 of this report are:

Measured Variable Blocks	Associated System
1. Boric Acid Tank Level	ESFAS
2. Charging Header Pressure	ESFAS
3. Steam Generator Water Level	ESFAS
4. Reactor Coolant Water Temperature	ESFAS
5. Containment Pressure	ESFAS
6. Steamline Pressure	ESFAS, Control
7. Feedwater Flow	ESFAS, Control
8. Recirculating Water Storage Tank Level	ESFAS
9. Reactor Coolant Water Pressure	ESFAS
10. Volume Control Tank Level	ESFAS
11. T-Cold	ESFAS, Scram, Control
12. Pressurizer Pressure	ESFAS, Scram, Control
13. Digital Rod Position	Scram
14. N-16 Power	Scram, Control
15. Power Range Nuclear Instrument	Scram, Control
16. Intermediate Range Nuclear Instrument	Scram

Measured Variable Blocks (cont.)	Associated System (cont.)
17. Source Range Nuclear Instrument	ESFAS, Scram
18. Steam Generator Level	ESFAS, Scram, Control
19. Pressurizer Level	ESFAS, Scram, Control
20. Reactor Coolant Flow	ESFAS, Scram
21. Reactor Coolant Pump Speed	ESFAS, Scram
22. Turbine Stop Valve	ESFAS, Scram
23. Turbine and Fluid Pressure	ESFAS, Scram

Derived Variable Blocks	Associated System
1. DNB & kW/ft	Scram and Control
2. NIS	Scram and Control
3. Each Analog Bistable	Scram

Command Blocks	Associated System
1. Trip Logic	Scram
2. Communication	Control
3. ESF	ESFAS

From this analysis, we conclude that the architecture, at this point in its development, is not in conflict with the guidelines presented in Section 3. We also conclude that, for a preliminary design approval, the proposed architecture of the integrated protection system is acceptable.

For a final design approval, we require that the design of the as-built integrated protection system conform to the guidelines stated in Section 3 of this report in addition to all other reactor protection system design criteria, such as the General Design Criteria of 10 CFR 50, Regulatory Guides, and Industry Standards. The additional analyses required to illustrate conformance to the guidelines of Section 3 are to be conducted with conservative estimates of parameters of the design. The additional tests to demonstrate that the design conformance to the guidelines of Section 3 may be provided by an amendment to the design verification program. In summary, we require that Westinghouse propose a program of analyses and tests with the objective of demonstrating that the design of the RESAR-414 integrated protection system conforms to the guidelines of Section 3 of this report. After review and approval by the staff, the program is to be executed, results analyzed, and a program report submitted for staff review.

4.3 Signal Selector

4.3.1 Summary for the Signal Selector Device

The staff review of the signal selector, a control system device, was conducted by means of an audit. Our audit concentrated upon evaluating the safety significance of the interconnection between protection and

control as well as the consequences of failure of the signal selector. In the audit, we did not conduct a detailed review of the algorithms that are to be stored and executed in digital devices within the signal selector.

For the purposes of a preliminary design approval, we find the proposed design of the signal selector acceptable. However, our review did identify several concerns that Westinghouse must resolve to our satisfaction prior to the issuance of an OL or FDA safety evaluation of the signal selector. These concerns are expressed in Sections 4.3.3.1 through 4.3.3.4.

4.3.2 Description

The control system on the RESAR-414 plant will derive some of its inputs from signals that are present in the integrated protection system. A criterion of the plant design is that no single random failure in the protection system should cause an adverse control action and also prevent proper action of the protection channel needed to protect against that adverse action.

The signals from the protection system to the control system are limited to digital signals transmitted over multiplexed optical data links. The transmission of the signals is unidirectional, from protection to control. The optical data links serve as electrical isolation devices. The digital signals received from each channel of the protection system are gathered and digitally processed in the signal selector using pre-stored algorithms to establish valid measured signals for the control system (Refs. 14 and 15). The protection signals used for control are as follows:

1. Reactor inlet temperature (T_{cold})
2. Power range ex-core nuclear detectors
3. Reactor power (N-16)
4. Margin to trip on departure from nucleate boiling ratio and margin to trip on linear power density
5. Steam generator water level (each of four loops)
6. Feedwater flow (each of four loops)

7. Pressurizer pressure

8. Pressurizer water level

9. Reactor power output of rod drop track/store units (this information is required to determine negative period in a rod position event)

Physically, two signal selector devices are provided although they share the same signal input sources and are also operated from the same power supply. Each signal selector is composed of microprocessors and ROMs and RAMs for processing of the digital signals. Furthermore, the outputs of the two signal selectors are compared and alarmed in the event of a detected discrepancy.

Westinghouse states that the reason for having two signal selectors is to service the needs of the redundant control systems and independent interlocks. Two control systems, the power control system and the feedwater control system, are redundant because they are crucial to plant availability and their failure would result in plant shutdown. Also, the pressurizer level and pressure control system have independent interlocks on key valves to prevent unwanted system depressurization.

Westinghouse has given two reasons for the placement of the signal selectors in the control system. First, no single protection channel set has enough information to determine if the electrical signal for a given process variable is valid. Second, the selectors provide defense against common-mode failure. If the selection devices were located in one of the integrated protection cabinets, a single event, such as extreme temperature, could cause the signals to process erroneous data to both the signal selector and protection cabinet.

4.3.3 Evaluation

4.3.3.1 Signal Diversity

Based on the review of the topical report describing the signal selector (Refs. 14 and 15) and information obtained in recent meetings with Westinghouse (Refs. 5,6,7,8,9), we have concluded that the proposed design of the signal selector is conditionally acceptable. The basis for the conclusion and the conditions of the acceptance are discussed as follows.

The signal selector, as previously discussed, is a device connecting the protection system and control system in the RESAR-414 design. The control system in the design derives certain of its inputs from signals that are present in the protection system. Our review indicated that there were no signals from the control system that were transmitted

through the signal selector (or through any other path) to the protection system.

The connection of protection and control systems is a concern to the staff. General Design Criterion 24 addresses the interconnection of protection and control and requires that connections be limited to assure that safety is not significantly impaired. It is the Westinghouse design philosophy that the plant be controlled from the same measurements with which it is protected; thereby, the control system will function to maintain margins between operating conditions and safety limits and reduce the likelihood of spurious trips. We have approved previous Westinghouse designs containing a connection from protection to control based on their demonstration of insignificant impairment to safety. (This issue was addressed by Westinghouse for previous designs in Reference 10.)

A main function of the signal selector is to prevent a single random failure in the protection system from causing an adverse control action and also to prevent proper action of the protection channel needed to protect against the adverse action. This is based on the principle that the single random failure will be detected by the signal selector when a comparison of like signals is made. The algorithm used in the signal comparison process is classified proprietary by Westinghouse. In this role, the signal selector is then a functional isolator; that is, it isolates the control system from a single random failure in the protection system.

As a functional isolator between protection and control, the signal selector need not be Class 1E equipment and part of the protection system as required of electrical isolators in IEEE Standard 279. The signal selector is located downstream of the electrical isolation devices between the protection system and control system. Based on qualified electrical isolation devices, it is reasonable to expect that the failure of the signal selector will not impede the ability of the protection system to respond to a challenge. We conclude that the signal selector need not be part of the protection system.

The signals used for protection and control have been previously defined. Protection system components used to generate and transmit these signals serve both protection and control functions. We are concerned with the possibility of systematic, nonrandom, concurrent failures of these redundant components in protection resulting in the loss of both protection and control. For example, a common-mode program error in a shared component can result in the loss of protection and control. We have discussed these concerns in both Sections 2.4 and Appendix B of this report. Our requirements for the resolution of these concerns are presented in Section 3.3. We would find the signal selector acceptable

provided that the system is in conformance with the guidelines of Section 3.3.

Position - Westinghouse has not demonstrated that the common loss of shared signals between protection and control has an insignificant impact upon safety as required by General Design Criterion 24. We require that Westinghouse demonstrate by analysis and/or by test that the loss of any shared signal between the protection system and control system will not have a significant impact on safety. The demonstration must consider the possibility of systematic, nonrandom, concurrent failures of the shared signals or provide a basis for the exclusion of this consideration. Furthermore, we require that this be demonstrated by test and analyses for each type of signal shared between the protection and control system (see Section 4.3.2). The tests and analyses shall also demonstrate that the signal selector performs no protection function.

4.3.3.2 Signal Selector Operation - Limiting Case

The signal selector must be capable of rejecting a single erroneous signal caused by a random failure in the protection system. In addition, Westinghouse states (Refs. 14 and 15) that it must be able to perform this function even when one of the protection channels is bypassed or removed from service for test or maintenance. It is also stated that this criterion must be met even if the failure and an unrelated transition into the test mode occur simultaneously (within the same execution cycle of the algorithm). This criterion is the single random failure requirement of Section 4.7.3 of IEEE-279.

The integrated protection system is designed to allow the concurrent bypassing of two out of four channels measuring any given process variable. Although the signal selector would reject the two bypassed signals, it would be unable to isolate an erroneous signal between the two remaining signals. Thus, when only two channels of valid signal remain in the signal selector, an alarm is provided to inform the operator, and administrative action is required to place controls derived from those channels into a manual mode of operation.

The staff is concerned with the transition to and operation of the signal selector in the limiting case when only two valid signals remain. In this case, the coincident logic for the trip system is modified to a one-out-of-two logic for the subject protection function. Because the signal selector in the control system and the bypass logic in the protection system are new designs with a high degree of operational flexibility, the staff is concerned with failures that will impact both protection and control. This concern is most important when the limiting case of operation is achieved; that is, where the same two signals are used for protection and control. A shared-component failure or an inadequate design basis could result in the loss of both protection and control.

Position - We require that Westinghouse demonstrate the adequacy of the signal selector to achieve and sustain limiting case operation. We require that Westinghouse evaluate the safety consequences resulting from the partial and total failure of the signal selector devices during limiting case operation. Furthermore, we require that Westinghouse establish administrative and surveillance procedures for limiting case operation.

4.3.3.3 Failure Consequences of Signal Selector

In the topical reports (Refs. 14 and 15), Westinghouse has not evaluated the consequences resulting from the failure of the signal selector. Our concern is that the failure of the signal selector may, for example, by including malfunctions of more than one controller, cause plant conditions that are more severe than those for which the plant safety systems are designed. From the preliminary information on the signal selector, it is not evident that a single failure will be confined to one of the redundant devices because they are interconnected. Westinghouse has not established the safety consequences resulting from loss of the signal selector.

Position - We require that Westinghouse define and evaluate the credible failure modes of the signal selector and their effects, including the possibility of systematic, nonrandom current failures of the two devices. Our concern is that plant conditions more severe than the design basis of the safety system may result from failure of the signal selector. Modifications of the design will be required for those failure consequences resulting in plant conditions more severe than those for which the plant safety systems are designed.

4.3.3.4 Signal Selector Design Bases

The design bases of the signal selector, as stated in the Westinghouse topical report (Refs. 14 and 15), are incomplete. The design bases do not address transient operation of the plant and, in particular, asymmetries resulting from spatial variations in measured process variables and operational variations in measured process variables. Westinghouse has not demonstrated that the design bases of the signal selector are adequate with respect to the intended functions and service environment.

Position - We require that Westinghouse demonstrate, by test and/or analysis, that the operation of signal selector will not result in a challenge to the safety system during operation of the plant.

4.4 Verification and Validation

A new design trend in safety systems has been initiated with the use of digital computers in protection systems. The design trend contains the potential for an increase as well as a degradation in nuclear safety. The increase to safety stems from the flexibility to directly synthesize trip variables, such as DNBR. Also, through signal diversity and distributed processing, the potential for improved system reliability exists.

The potential for degrading nuclear safety through the use of digital computers also exists. For example, a common-mode software error in redundant safety channels can result in the loss of the safety function. To guard against the potential for degrading safety in the design of digital computer based safety systems, the Nuclear Regulatory Commission staff is presently developing the guidance for Independent Verification and Validation Programs for instrumentation system design.

The purpose of an Independent Verification and Validation Program is to minimize errors. Precedent exists for the use of this type of program when a highly reliable digital computer system is required. For example, the U.S. Air Force has used this type of program to achieve a highly reliable system in the MINUTEMAN III and the TITAN II projects. NASA has used the program to achieve a highly reliable system in the VIKING project. Reference 16 describes the characteristics of an Independent Verification and Validation Program as required by the U.S. Air Force.

The NRC staff expects to establish guidelines for an Independent Verification and Validation Program in the near future. However, Westinghouse has docketed a topical report that addresses program verification (Ref. 17). The review of this report is incomplete at this time. Our plans are to complete the review subsequent to the establishment of NRC Independent Verification and Validation Program guidelines. At that time, we will evaluate all verification and validation activities associated with the design, development, and qualification of the RESAR-414 safety system.

4.5 On-Line Testing

4.5.1 Periodic Testing

The on-line testing features for the RESAR-414 integrated protection system consists of two types of systems. The first type is the periodic channel test system that is manually initiated and then proceeds automatically to complete all tests of one protective channel. To test a second channel, a manual master selector switch is used that inhibits testing more than one channel at a time. The channel tests are expected

to be executed approximately on a monthly basis, commensurate with the anticipated mean time between failures of the overall system. The testing devices, including hardware and software, are redundant and contained within each respective channel, except for the selector switch that provides enabling power to the testers, one at a time. Once initiated, the test automatically imposes a channel bypass and removes all input signals. Test signals are then substituted in a logical progression to test many channel functions. Status information is fed back to the tester from the channel data outputs for test confirmation. When a channel test sequence is completed, the input signals are automatically restored, and, after a delay for stabilization of transients, the bypass is removed.

Functionally, the tester has the capability to completely disable a channel by, for example, failing to restore the input signals. An undetected common-mode failure of either hardware or computer program in the tester has the potential for disabling all channels of all signals fed to the integrated protection system involving all levels of defense in depth.

An additional factor affecting the basis for acceptance of the system design at a later stage in its development is the confirmation that the test itself is valid. It is conceivable that a design error in the tester could overlook a failure to danger in the protection system and continue to give an indication of successful test. Since the operator has little opportunity or access to make an independent overview, this could also occur as a common-mode failure with the attendant loss of defense in depth. An accumulation of single failures of the untested tester could have the same result. It is the staff's intent to evaluate this concern during the design verification phase of the RESAR-414 review.

Position - We require that Westinghouse develop the periodic test system in a manner that will minimize common-mode errors. An independent verification and validation program for the development of the test system (Section 4.5) would be acceptable to the staff. Furthermore, we require that, upon completion of a periodic test, a positive means be provided to assure the operator that the channel has been properly reconfigured with respect to process signals. Finally, the confirmation of the validity of the test shall be demonstrated during system qualification for each test in the periodic test program. This shall include tests to confirm that the tester will detect all failures for which it has been designed.

4.5.2 On-Line Validity Checking

The second type of on-line testing is the continuous validity checking incorporated in the protection system computer programs. The need for such checks in data transfers where noise can be a problem is understandable. The need for continuous, millisecond time-scale checks of other software or hardware features is not obvious. Moreover, extensive on-line testing can degrade safety through unnecessary complexity.

Position - We require that on-line testing be limited to the detection of gross failures. Thus, the use of watch-dog timers and block checksums for detection of gross failures are acceptable. The extensive use of on-line test that may be achieved with digital computers can degrade safety. We require that Westinghouse establish the failure basis for each on-line test used in the design.

5. SUMMARY AND CONCLUSIONS

The guidelines to evaluate the degree of defense in depth provided by an interconnected instrumentation system are presented in Section 3. We have reviewed the RESAR-414 integrated protection system architecture for conformance to the design requirements for reactor protection systems such as the general design criteria, regulatory guides, industry standards, and, in addition, the guidelines presented in Section 3. Based on the results of our evaluation, presented in Section 4.2.3, we conclude that, for purposes of a preliminary design approval, the RESAR-414 integrated protection system is acceptable.

The analyses and tests, which will provide information to demonstrate that the defense-in-depth principle has been implemented in the integrated protection system final design, are summarized in the following sections. We require that these tests and analyses be completed and found acceptable by the staff before approval of an FDA for RESAR-414.

5.1 Defense-in-Depth Analysis

We require that Westinghouse conduct a design analysis of the integrated protection system in accordance with the defense-in-depth guidelines. We also require a test program to demonstrate that the integrated protection system performs as analyzed. These tests and analyses are to be defined in a program plan which is to be submitted for staff evaluation. After review and approval by the staff, the program is to be executed, results analyzed, and a program report submitted for staff review.

5.2 Signal Selector

Based on our review of the topical reports (Refs. 10,14,15,17), we have concluded that the proposed design of the signal selector is acceptable for preliminary design approval. However, our review of the preliminary design did define several concerns in which Westinghouse will be required to perform analyses and tests to demonstrate that the defense-in-depth principle has been implemented in the integrated protection system final design. These positions are summarized as follows:

1. We require that Westinghouse demonstrate by analysis and test that the loss of any signal shared by control and scram or ESF does not significantly affect safety.

2. We require that Westinghouse demonstrate the adequacy of the signal selector for limiting situations (such as one signal failed and one bypassed), for transient operation of the plant, and for spatial asymmetries in process variables. Furthermore, we require that Westinghouse establish administrative and surveillance procedures for operation of the signal selectors under limiting situations.

3. We require that Westinghouse define and evaluate the credible failure modes of the signal selector and their effects, including the possibility of systematic, nonrandom concurrent failure of the two devices. Our concern is that plant conditions more severe than the design basis of the safety system may result from failure of the signal selector. Modifications of the design will be required for those failure consequences resulting in plant conditions more severe than those for which the plant safety systems are designed.

4. We require that Westinghouse demonstrate by test and/or analysis that the operation of the signal selector will not result in a challenge to the safety system during operation of the plant.

5.3 Testing

5.3.1 Periodic Testing

The detailed design will be subject to confirmation in the Verification Program. We require that a positive means be provided to assure the operator that, upon the completion of a test sequence in one channel, the channel has been restored to operating condition including re-initialization.

5.3.2 On-Line Validity Checking

We require that continuous validity checking included in the software be limited to necessary functions such as watch-dog timers and block check-sums, and that Westinghouse establish the failure basis for each on-line test.

5.4 Verification and Validation

To guard against the potential for degrading safety in the design of digital computer based safety systems, the Nuclear Regulatory Commission staff is presently developing the guidance for Independent Verification and Validation Programs for instrumentation system designs.

The NRC staff expects to establish guidelines for an Independent Verification and Validation Program in the near future. However, Westinghouse has docketed a topical report that addresses program verification (Ref. 17). The review of this report is incomplete at this time. Our plans are to complete the review subsequent to the establishment of NRC Independent Verification and Validation Program guidelines. At that time, we will evaluate all verification and validation activities associated with the design, development and qualification of the RESAR-414 safety system.

6. REFERENCES

1. Westinghouse Electric Corporation, "Reference Safety Analysis Report (RESAR)," Amendment 16 to RESAR-414, Docketed by letter from J. D. McAdoo, Westinghouse, to S. Vargas, NRC, Docket STN 50-572, July 10, 1978. Available in NRC PDR for inspection and copying for a fee.

2. U.S. Nuclear Regulatory Commission, Staff Report to Advisory Committee on Reactor Safeguards (ACRS), "Westinghouse Electric Corporation Reference Safety Analysis Report-414," July 1978. Available in NRC PDR for inspection and copying for a fee. (See also Reference 13.)

3. Letter from S. Lawroski, ACRS, to Honorable J. M. Hendrie, NRC, Subject: Report on Westinghouse Electric Corporation Safety Analysis Report, RESAR-414, dated August 10, 1978. Available in NRC PDR for inspection and copying for a fee.

4. Letter from R. S. Boyd, NRC, to T. M. Anderson, Westinghouse, Subject: Consideration of RESAR-414 Integrated Protection System, September 1, 1978. Available in NRC PDR for inspection and copying for a fee.

5. Summary of Meeting on September 6, 1978, to Discuss the Additional Review Effort for the RESAR-414 Integrated Protection System, Docket STN 50-572. Available in NRC PDR for inspection and copying for a fee.

6. Summary of Meeting on September 11, 1978, to Discuss the Additional Review Effort for the RESAR-414 Integrated Protection System, Docket STN 50-572. Available in NRC PDR for inspection and copying for a fee.

7. Summary of Meeting on September 18, 1978, to Discuss the Additional Review Effort for the RESAR-414 Integrated Protection System, Docket STN 50-572. Available in NRC PDR for inspection and copying for a fee.

8. Summary of Meeting on September 26, 1978, to Discuss the Additional Review Effort for the RESAR-414 Integrated Protection System, Docket STN 50-572. Available in NRC PDR for inspection and copying for a fee.

9. Summary of Meeting on October 3, 1978, to Discuss the Additional Review Effort for the RESAR-414 Integrated Protection System, Docket STN 50-572. Available from NRC PDR for inspection and copying for a fee.

10. T. W. Burnett, "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," Westinghouse Electric Corporation, Topical Report WCAP-7306, April 1969.

11. U.S. Nuclear Regulatory Commission, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants, LWR Edition," USNRC Report NUREG-75/094 (Reg. Guide 1.70, Rev. 2), Chapter 15, "Accident Analyses," September 1975. Available for purchase from National Technical Information Service, Springfield, Virginia, 22161.

12. U.S. Nuclear Regulatory Commission, "Anticipated Transients Without Scram for Light Water Reactors," USNRC Report NUREG-0460, Vols. 1 and 2, April 1978; Vol. 3, December 1978. Available for purchase from National Technical Information Service, Springfield, Virginia, 22161.

13. U.S. Nuclear Regulatory Commission, "Safety Evaluation Report on Westinghouse RESAR-414," USNRC Report NUREG-0491, November 1978. Available for purchase from National Technical Information Service, Springfield, Virginia, 22161.

14. B. M. Cook, "Westinghouse Model 414 Control Systems Signal Selection Device," Westinghouse Electric Corporation, Topical Report WCAP-8899 (Proprietary), May 1977.

15. B. M. Cook, "Westinghouse Model 414 Control Systems Signal Selection Device," Westinghouse Electric Corporation, Topical Report WCAP-8899, Rev. 1 (Proprietary), August 1978.

16. "Management Guide to Avionics Software Acquisition," Volume 1 - "An Overview of Software Development and Management," Aeronautical Systems Division, Air Force Systems Command, ASD-TR-76-11, June 1976.

17. Westinghouse Electric Corporation, "414 Integrated Protection System Prototype Verification Program," Topical Report WCAP-9153 (Proprietary), August 1977.

18. The Institute of Electrical and Electronics Engineers, "Criteria for Protection Systems for Nuclear Power Generating Stations." IEEE Standard 279-1971. Available from the Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017. Copyrighted.

19. Code of Federal Regulations, Title 10, "Energy," Part 50 (10 CFR 50), Revised as of January 1, 1978. Available from public library or the U.S. Government Printing Office.

20. U.S. Nuclear Regulatory Commission, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants - LWR Edition," USNRC Report NUREG-75/087, September 1975.

21. Transmittal from Westinghouse NES, October 2, 1978 (Rewrite of 5th Transmittal); October 4, 1978 (Final Version of the 5th Transmittal) to J. Joyce, NRC (Division of System Safety, Instrumentation and Control Systems Branch), Subject: "Application of Defense in Depth Principle to Reactor Instrumentation Systems," received October 6, 1978. Available in NRC PDR for inspection and copying for a fee.

APPENDIX A

ANTICIPATED TRANSIENTS WITHOUT SCRAM

"ATWS" is an acronym for "anticipated transients without scram." The first part of ATWS (anticipated transients) is concerned with deviations from normal operating conditions that might occur one or more times during the service life of a plant.* The other part of ATWS (without scram) is concerned with the reactor protection system. In the event of an occurrence of an anticipated transient, the control rods (which are part of the reactor protection system) are automatically inserted into the reactor core to shut down the nuclear reaction - the "scram." If, in spite of all the care built into the reactor protection system design, a scram should not result following an anticipated transient, then an ATWS event would occur.

In September 1973, the Atomic Energy Commission regulatory staff published the "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors" (WASH-1270, Ref. 1) establishing acceptance criteria for anticipated transients without scram (ATWS). These criteria were developed because of the staff belief that a fully satisfactory methodology for analyzing the reliability of protection systems from the standpoint of common mode failures was not available at that time, that elements of these types of failures had occurred in protection systems, and that the potential consequences of some postulated anticipated transient without scram were calculated to be hazardous to the public. Subsequent to the publication of WASH-1270, the AEC staff met with Westinghouse and other reactor vendors on a regular basis and reviewed their evaluation models, the results of analyses of anticipated transients without scram, the diversity of the systems relied upon to mitigate the consequences of ATWS, and the susceptibility of the reactor protection system to common mode failure. Westinghouse, in conformance with the requirements of Section II-B of Appendix A to WASH-1270, submitted an analysis of anticipated transients without scram (Ref. 2).

The NRC staff review of the Westinghouse ATWS analyses included the anticipated transients expected to occur, the initial conditions and system parameters assumed in the analyses, the reliability of systems, analytical techniques, the results of analyses of ATWS, and the design of the reactor protection system. Using the requirements of WASH-1270 as a guideline, the staff reviewed each relevant aspect of the Westinghouse model and analysis. The details of the staff review are provided in the "Status Report on Westinghouse Analyses of Anticipated Transients Without Scram," December 9, 1975 (Ref. 3).

*The Code of Federal Regulations, 10 CFR 50, Appendix A, defines Anticipated Operational Occurrences as those conditions of operation expected to occur one or more times during the life of the nuclear power unit.

Since the publication of the 1975 status report (Ref. 3), additional information relevant to ATWS has been developed by the industry and the NRC. Based on review of this information and discussions with Westinghouse and others, the NRC Division of Systems Safety published a report entitled "Anticipated Transients Without Scram for Light Water Reactors," NUREG-0460, in April 1978 (Ref. 4). NUREG-0460 concludes that features to mitigate consequences of ATWS events are needed. More recently, Volume 3 of NUREG-0460 (published in December 1978) gives ATWS guidelines for Westinghouse plants including RESAR-414.

In view of the differing opinions on ATWS, a recommendation is made in NUREG-0460 that an ATWS rulemaking proceeding be initiated. That proposal is currently under review by the Office of Nuclear Reactor Regulation and the Advisory Committee on Reactor Safeguards. If the current staff proposal leads to initiation of rulemaking by the Commission, any rule adopted would include an implementation plan for all classes of plants. The RESAR-414 class of plants would be required to provide any needed plant modifications in conformance with ATWS criteria and schedule requirements provided in the rule.

These modifications would assure that the ESF needed to mitigate a postulated ATWS event would not be impaired by the postulated scram system failure. Conformance with Guideline 8 of Section 3 of this report (see main text of this report) provides this assurance.

The staff requires a commitment to provide an ATWS solution for the RESAR-414 design. This requirement should be considered in context with the NRC's planned deliberations on the need for ATWS provisions in general. The recent sequence of actions within the NRC is as follows:

1. In April 1978, NUREG-0460 was published by the NRC. The recommendations included design requirements and recommended rulemaking to establish such criteria. Volume 3 to NUREG-0460 was published in December 1978.

2. The report is presently being reviewed (March 1979) by the Advisory Committee on Reactor Safeguards and the Office of Nuclear Reactor Regulation. After completion of the review, now estimated to be May 1979, the Director, NRR, will forward his recommendations to the Commission.

3. After deliberation, the Commission will act on the matter. Whether it will agree to rulemaking is speculative at this time. If rulemaking is initiated by the Commission, we would expect that any rule adopted would include an implementation plan for all classes of plants. The RESAR-414 class of plants would be required to provide plant modifications in conformance with ATWS criteria and schedular requirements provided in the rule.

Although these deliberations are ongoing, we are concerned that the RESAR-414 design might progress to a point over the coming months that could preclude full implementation of the design modifications to satisfy acceptance criteria in NUREG-0460 should they eventually be adopted by the Commission, either with or without rulemaking.

Therefore, the NRC staff believes that Westinghouse should commit that the design and construction of plants referencing RESAR-414 will not preclude implementing RESAR-414 modifications necessary for ATWS. The type of design modifications that may be required to satisfy NUREG-0460 criteria are minor, and would be accomplished by conforming with defense-in-depth Guideline 8 of Section 3.

REFERENCES

1. Atomic Energy Commission, "Technical Report on Anticipated Transients Without Scram for Water-Cooled Power Reactors," WASH-1270, September 1973. Available for purchase from National Technical Information Service, Springfield, Virginia 22161.

2. Westinghouse Electric Corporation, "Anticipated Tansient Without Trip Analysis," Topical Report WCAP-8330, August 1974. Available in NRC PDR for inspection and copying for a fee.

3. U.S. Nuclear Regulatory Commission, "Status Report on Westinghouse Analyses of Anticipated Transients Without Scram," December 9, 1975. Available in NRC PDR for inspection and copying for a fee.

4. U.S. Nuclear Regulatory Commission, "Anticipated Transients Without Scram for Light Water Reactors," Vols. 1 and 2, USNRC Report NUREG-0460, April 1978; Vol. 3, USNRC Report NUREG-0460, December 1978. Available for purchase from National Technical Information Service, Springfield, Virginia 22161.

APPENDIX B

RULES, CRITERIA, SRP REFERENCES

Consideration of defense in depth, CMF and diversity in instrumentation and control systems is included in NRC regulations and guides, and in IEEE Standards.

(1) The General Design Criteria, 10 CFR Part 50, Appendix A, include the following statements:

> "The development of these General Design Criteria is not yet complete....Some of the specific requirements...have not as yet been suitably defined. Their omission does not relieve any applicant from considering these matters in the design of a specific facility and satisfying the necessary safety requirements. These matters include...(4) Consideration of the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems...."
>
> (Introduction)
>
> "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." (Criterion 22)
>
> "Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired." (Criterion 24)
>
> "No single failure results in the loss of the protection system." (Criterion 21)
>
> "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." (Criterion 22)
>
> "The protection and reactivity control systems shall be designed to assure an extremely high probability of accomplishing their safety functions in the event of anticipated operational occurrences." (Criterion 29)

(2) 10 CFR 50.55a requires that protection systems meet the requirements of IEEE-279. (10 CFR 50.55a(h)). IEEE-279-1971 (the edition currently effective) includes the following clause:

> "4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required."
>
> "4.6 Channel Independence. Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce the likelihood of inter-actions between channels during maintenance operations or in the event of channel malfunction."
>
> "4.7.4 Multiple Failures Resulting from a Credible Single Event. Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, one of the following must be met.
>
> "4.7.4.1 Alternate channels, not subject to failure resulting from the same single event, shall be provided to limit the consequences of this event to a value specified by the design bases. In the selection of alternate channels, consideration should be given to (1) channels that sense a set of variables different from the principal channels, (2) channels that use equipment different from that of the principal channels to sense the same variable, and (3) channels that sense a set of variables different from those of the principal protection channels using equipment different from that of the principal protection channels. Both the principal and alternate protection channels shall meet at all the requirements of this document.
>
> "4.7.4.2 Equipment, not subject to failure caused by the same credible single event, shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment shall meet all the requirements of this document."

IEEE-603-1977 includes a similar clause:

> "5. Protection System Functional and Design Requirements
>
> In addition to the functional and design requirements in Section 4, the following shall apply to the protection system.

"5.1 Interaction Between the Protection System and Other Systems.

"5.1.1 Where a single credible event, including all direct and consequential results of that event, can cause a nonsafety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those protection systems channels designated to provide principal protection against the condition, one of the following shall be met:

"(1) Alternate channels and equipment, not subject to failure resulting from the same single event, shall be provided to detect the event and limit the consequences of this event to a value specified by the design basis. In the selection of alternate channels, consideration should be given to:

"(a) Channels that sense a set of variables different from the principal channels.

"(b) Channels that use equipment different from that of the principal channels to sense the same variable.

"(c) Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.

"Both principal and alternate channels shall be a part of the protection system.

"(2) Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the protection system."

"5.1.2 Provisions shall be included so that the requirements in 5.1.1 can still be met in conjunction with the requirements of 5.4 if a channel is in maintenance bypass. Acceptance provisions include reducing the required coincidence, defeating the nonsafety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel."

(3) The Standard Review Plan implements these requirements.

"Table 7-1, 'Acceptance Criteria for Instrumentation and Control Systems', lists the criteria currently applicable to safety-related

instrumentation and control systems...Conformance to these criteria does not necessarily establish the adequacy of the functional performance and reliability of these systems." (SRP 7-1, pp. 1-2)

Table 7-1 includes IEEE-279.

"Section 4.7 - Control and Protection system interaction involves more than examining their electrical isolation and interconnection. The functional performance of control systems must be reviewed to the extent that it is determined that a control system cannot prevent proper action of a protection system. This section of IEEE Std 279, with regard to isolation devices and multiple failures resulting from a credible single event, is explained by example in the document." (SRP 7.2, p.16)

"Section 4.7 - The interaction of control systems and the ESFAS involves more than examining the electrical interconnection of control systems with the ESFAS. Compliance with the diversity requirements of subsection 4.7.4.1 is a requirement for the initiation of engineered safety features and the interlocks for valves between the reactor coolant system and low pressure systems. In addition, the functional performance of appropriate control systems must also be reviewed to determine whether their effect on plant conditions can indirectly affect the performance of the ESFAS or the ESF. For example, if a cooling water system is used to supply both safety and nonsafety equipment, the controls for the cooling water system must be examined to determine whether failure could lead to insufficient cooling water being supplied to the ESF or the ESFAS during an accident. (Also see Regulatory Guide 1.106.)

"Note that if failure of a system serving both safety and nonsafety systems can lead to a condition requiring action by the safety system, then in addition to the failure creating the need for safety action, the ESFAS must be designed to withstand any other simultaneous single failure." (SRP 7.3, pp. 9-10)

NRC FORM 335 (7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER *(Assigned by DDC)*
NUREG 0493

4 TITLE AND SUBTITLE *(Add Volume No., if appropriate)*
A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System

2. *(Leave blank)*

3 RECIPIENT'S ACCESSION NO.

7 AUTHOR(S)

5. DATE REPORT COMPLETED
MONTH | YEAR

9 PERFORMING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Office of Nuclear Reactor Regulation
Division of Systems Safety
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

DATE REPORT ISSUED
MONTH | YEAR

6 *(Leave blank)*

8 *(Leave blank)*

12 SPONSORING ORGANIZATION NAME AND MAILING ADDRESS *(Include Zip Code)*
Office of Nuclear Reactor Regulation
Division of Systems Safety
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO

11 CONTRACT NO

13 TYPE OF REPORT
Technical Report

PERIOD COVERED *(Inclusive dates)*

15 SUPPLEMENTARY NOTES

14 *(Leave blank)*

16 ABSTRACT *(200 words or less)*

This report discusses the defense-in-depth and diversity principles as they apply to safety related instrumentation and presents guidelines which can be used to assess the degree to which the designs of complex, interconnected safety systems conform to these principles. These guidelines are based on the use of the block concept, an approach in which the components and modules of the system are aggregated into a small number of functional units, or blocks, to simplify the analysis. It is believed that the use of the block concept and the guidelines will result in a conservative assessment of the capability of such systems to function when subjected to postulated to common-mode failures.

A preliminary assessment of the RESAR-414 Integrated Protection System by means of the guidelines is also presented. The results of this assessment support the conclusion that, for purposes of a preliminary design approval, the RESAR-414 Integrated Protection System is acceptable. However, the assessment, has also resulted in requirements for additional analyses and tests, the results of which must demonstrate conformance to the guidelines prior to the issuance of a Final Design Approval.

17 KEY WORDS AND DOCUMENT ANALYSIS

17a DESCRIPTORS

17b IDENTIFIERS/OPEN-ENDED TERMS

18 AVAILABILITY STATEMENT
Unlimited Availability

19. SECURITY CLASS *(This report)*

21 NO. OF PAGES

20 SECURITY CLASS *(This page)*

22 PRICE
$