POLICY ISSUE
(Information)

September 16, 1991

SECY-91-292

For: The Commissioners

From: James M. Taylor
Executive Director for Operations

Subject: DIGITAL COMPUTER SYSTEMS FOR ADVANCED LIGHT WATER REACTORS

Purpose: To inform the Commission on the major regulatory issues associated with the application of digital computer technology to instrumentation and control (I&C) systems that are important to safety and the NRC staff's actions to resolve these issues. These issues include the effect of evaluated experiences, the continuing rapid changes in digital computer technology, and the establishment and maintenance of the new regulatory review process for I&C systems important to safety consistent with Subpart B of Part 52 of Title 10 of the Code of Federal Regulations (10 CFR Part 52).

Background: The evolutionary and passive advanced light water reactor (ALWR) designs incorporate instrumentation and control (I&C) systems using digital computer technology to implement the monitoring, control and protection functions. The Electric Power Research Institute (EPRI) Utility Requirements Document (RD) also addresses the use of digital computer technology for I&C systems and man-machine interface systems (M-MIS).

To ensure that digital systems are implemented safely in nuclear power plants, the staff is reviewing the designs with an approach that considers existing regulatory requirements, the development of requirements where none exist, the lessons learned in the U.S. and other countries, and the guidelines provided in the EPRI RD.

Contact:
M. Chiramal, NRR/DST
492-0845
J. Gallagher, NRR/DST
492-0823

NOTE: SENSITIVE INFORMATION - LIMITED TO NRC UNLESS THE COMMISSION DETERMINES OTHERWISE

NOTE: ENCLOSURE 1 REMOVED TO ALLOW PUBLIC RELEASE OF PAPER

The use of digital computer technology in protection and control systems raises a concern that the software and hardware for these computer systems could be vulnerable to design and programming errors that could lead to safety-significant common mode failures.

The staff reviewed Chapter 10 of the EPRI RD, "Man-Machine Interface Systems," and concludes that, in general, the EPRI requirements are acceptable from the point of view that they do not violate existing NRC criteria. The EPRI RD provides high-level design goals that address many of the key issues discussed herein. There are, however, certain open issues and confirmatory items that require resolution before the EPRI RD can be considered complete, even at this relatively high level of design requirements.

Significant work remains to resolve all issues such that the ALWR designs can be certified. In reviewing the advanced boiling water reactor (ABWR) design, the staff concluded that the ABWR safety analysis report does not include a sufficiently complete design and does not reference many of the standards included in the EPRI RD. The staff will continue to communicate with the applicant, the General Electric Company (GE), to address these open issues.

Discussion: EXPERIENCE

There is a wide range of experience with the application of digital computer technology for monitoring, control, and protection systems in various industrial applications; land, sea, and air transportation systems; communication systems; defense systems; fossil power plants; and nuclear power plants.

The most successful digital systems applications have been in industrial processes to automatically control, monitor, and protect major components. Certainly the recent Patriot Missile and telephone system experience demonstrate, however, that these systems can fail.

The U.S. nuclear industry has limited operational experience with digital computer system technology. Core Protection Calculators (CPCs) were reviewed by the NRC in the late 70's and are installed in all later Combustion Engineering (CE) plants. Several U.S. plants have retrofitted digital systems to replace selected analog systems, however, complete replacement of all plant analog systems with digital systems has not been performed.

Plants using safety-related digital computer systems are being designed and constructed in Canada, the United Kingdom, France, and Japan. The NRC staff communicates regularly with these countries to monitor activities involving digital systems applications in these plants. This is especially important given the international nuclear industry's difficulties with implementing computer systems applications that were designed without a structured process and the use of formal verification and validation (V&V) procedures. ~~Enclosure 1 provides details of some of these experiences.~~ (ENCLOSURE 1 REMOVED TO ALLOW PUBLIC RELEASE)

MAJOR REGULATORY ISSUES

Instrumentation and Control (I&C) systems help to ensure that the plant operates safely and reliably by monitoring, controlling, and protecting critical plant equipment and processes. The digital computer based I&C systems for ALWRs differ significantly from the analog systems used in operating nuclear plants. Because of the greater information content of digital signals compared to analog signals and the increased information processing capability of digital equipment compared to analog equipment, the change to digital computer based I&C systems provides the potential for improvements in the safe and reliable operation of nuclear power plants. This potential is achievable through the implementation of highly reliable digital I&C systems for all service conditions of operation of the equipment. This requires special constraints on the system architectural designs and features, and the application of a high level of discipline to the processes associated with the life cycle phases of design, manufacture, installation, operation, maintenance, and modification of the I&C system. Such requirements, however, must allow for flexibility in the application of the evolving digital computer technology.

The digital I&C system has a greater degree of sharing of data transmission, functions, and process equipment compared to the analog system. Although this sharing forms the bases for many of the advantages of the digital system it also raises a key concern with respect to its reliability. The concern is that a design using shared data bases and process equipment has the potential to propagate a common cause or common mode failure of redundant equipment. Another key concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure.

The goal of the requirements for the digital I&C systems is to limit the probability of the occurrence of common cause and common mode failures and, since some failures will still occur,

limit the extent of loss of functions of the I&C systems. These requirements are in addition to the existing requirements that are based primarily on analog technology. Enclosure 2 discusses these issues and development of requirements for digital systems.

The staff is reviewing the EPRI Utility Requirements Document (RD) for the evolutionary and passive ALWRs and two applications for design certification: the GE ABWR and the ASEA-Brown Boveri/Combustion Engineering, Incorporated (ABB/CE) System 80+.

To review the I&C systems for the ALWRs, the staff is using current regulatory requirements, guides, and industry standards in the SRP, and national and international standards not currently endorsed by the NRC. Information from other elements, such as lessons learned from operational and design experience, participation in codes and standards committees, staying current with evolving technology through technical information exchanges, conferences and meetings, and input from research efforts, will also be integrated into the review of the ABWR, ABB/CE System 80+, and passive ALWRs, as well as the updated SRP. Enclosure 3 discusses additional details of the staff's review efforts.

Conclusion: There is a general consensus within the international nuclear community that the proper use of digital computer technology in the design of monitoring, control and protection systems will improve the safety and performance of nuclear power plants. The President's Commission on The Accident At Three Mile Island reached a similar conclusion regarding improving the collection and understanding of information on the state of plant processes and equipment and thereby improving the safety and performance of the plant.

Digital computer technology is changing in a way that provides a much wider range of tools to assist in the engineering activities to develop and verify the designs of advanced I&C systems. This change in technology has the potential to provide improved hardware and software to implement the design. The international community is expending a significant amount of resources, most of which are outside the nuclear industry, to formulate guidelines and standards to improve the proper use of this technology.

However, much of this technology is being developed without consensus standards, as the technology available for design is ahead of the technology that is well understood through experience and supported by application standards. This is a challenge to which the NRC must respond, especially in light of the design certification process.

Enclosure 2 addresses the effect that the use of digital computer technology has on current requirements which primarily address analog I&C technology. Enclosure 2 describes the need for additional requirements and describes how Chapter 10 of the EPRI RD can provide a frame of reference to assist in developing new requirements and acceptance criteria. The enclosure also proposes a means for reviewing proposed designs and developing requirements and acceptance criteria in an environment of change. A graded set of requirements based on the importance to safety of the functions being performed with respect to reduction in the potential for radiation exposure could be adopted. The functions with the highest level of importance to safety, and thus with the most stringent requirements, are less likely to be affected by equipment changes than those functions with lower levels of importance to safety, such as, information systems.

Because of its safety importance, the staff expects to expend the most effort in the modification or development of requirements and acceptance criteria for digital computer technology-based monitoring, control, and protection systems. Particular emphasis will be placed on defense against propagation of common mode failures within and between functions. In this regard, the staff currently intends to require some level of diversity such as a reliable analog backup.

The staff shares in the consensus that these I&C systems can improve safety; however, the international operating and regulatory experience, the developmental nature of consensus U.S. standards and the significant interdependence of these

systems, require that ALWR applicants submit sufficient design information for certification for the staff to ensure that open issues are adequately resolved.

~~NOTE: Because Enclosure 1 discusses sensitive information about foreign experience, the staff recommends that this paper not be made publicly available.~~ (ENCLOSURE 1 REMOVED TO ALLOW PUBLIC RELEASE)

James M. Taylor
Executive Director
for Operations

Enclosures:
~~1. Nuclear Plant Experience With Digital Computer Application~~ (ENCLOSURE 1 REMOVED TO ALLOW PUBLIC RELEASE)
2. Requirements for Digitial Systems
3. Staff Review of ALWRs

DISTRIBUTION:
Commissioners
OGC
OCAA
OIG
GPA
LSS
REGIONAL OFFICES
EDO
ACRS
ACNW
SECY

ENCLOSURE 1 REMOVED TO ALLOW

PUBLIC RELEASE OF PAPER

ENCLOSURE 2

REQUIREMENTS FOR DIGITAL SYSTEMS

PURPOSE

This enclosure discusses the differences between analog and digital instrumentation and control (I&C) systems, the need for requirements for reducing the probability and consequences of common mode failures in digital I&C systems, and a process for developing new regulatory requirements and acceptance criteria.

INTRODUCTION

Instrumentation and Control (I&C) systems help to ensure that the plant operates safely and reliably by:

- monitoring the state of the plant processes and plant equipment to assist the operating staff in making decisions
- controlling plant processes, in both automatic and manual modes
- protecting critical plant equipment to maintain the integrity of barriers to the release of radioactive materials or to control radioactivity releases if one or more of the barriers are breached.

Because of the greater information content in digital signals compared to analog signals and the increased information processing capability of digital equipment compared to analog equipment, the change to digital computer based I&C systems provides the potential for improvements in the safe and reliable operation of nuclear power plants. The use of digital computer technology to provide information to help plant operators prevent or cope with accidents was one of the principal recommendations in the report of the President's Commission on The Accident at Three Mile Island. The realization of this potential is, of course, dependent on the implementation of highly reliable digital I&C systems for all the service conditions of operation of the equipment. The achievement of high levels of reliability for these systems requires special constraints on the system architectural designs and features and a high level of discipline applied to the processes associated with each life cycle phase of the I&C system. However, the requirements for the life cycle phases of design, manufacture, installation, operation, maintenance and modification of these I&C systems must not arbitrarily constrain application of digital computer system technology.

DIFFERENCES BETWEEN THE ARCHITECTURE OF ANALOG AND DIGITAL I&C SYSTEMS

As discussed below there is a major difference in the optimum architectural configuration of digital computer based I&C systems when compared to analog systems.

An analog I&C system is a collection of primarily single parameter configurations. Analog I&C systems usually have direct wire connections between the components that comprise each of these single parameter configurations. These are usually referred to as "hard-wired configurations." Often the only installed common items between such configurations are the cable routing fixtures and the power supplies for the equipment that make up these configurations.

The processing functions for control algorithms, linearization of sensor measurements, logic relationships, etc., have been traditionally implemented with analog equipment by the use of built-in circuits dedicated to a particular math or logic task. Programming for these functions is usually limited to adjustments in setpoints and pre-selected coefficients by changing potentiometer settings and rearranging highly visible built-in patch connectors.

A digital I&C system usually consists of a collection of individual input/output circuit boards connected to the plant equipment (sensors and actuators) through direct wire connections. These boards are connected to a multiplexed data link or data highway so that a single electrical wire or optic fiber carries signals from many sensors including information about the state of the sensors and actuators and the quality of the signals. This wire or fiber also carries control commands for many separate actuators. This data link or highway is connected to a set of equipment that uses a shared computer that can sequentially perform the algorithmic numerical and logic computations for several controllers according to the inputs from their respective sensors and actuators. The ingress, transmission, and egress of data on the multiplex data links or data highway is usually controlled by a protocol that within itself has shared functions. Consequently the data link (highway) protocol could result in a high degree of interdependence with respect to the equipment connected to the data link.

The shared computer can be

1) a mini (mainframe) computer that uses a multi-task operating system to perform many processing functions using the application software programs and the same hardware and executive operating system software to control the operation of that hardware or,
2) a set of microcomputers, individually connected to the highway, each running asynchronously using embedded software with limited multi-tasking capability for the operating system and application software modules that may be identical for different redundant hardware sets of equipment.

Consequently, the shared processing equipment can have a wide range of interdependence with respect to the functions performed; i.e., from one computer that performs many functions to separate computers that perform different functions but use common software modules for these separate functions.

POTENTIAL PROBLEM CAUSED BY SHARING RESOURCES

It is this resource sharing that forms the bases for many of the advantages of digital computer technology over analog technology. However, this sharing raises a key concern with respect to the reliability of I&C systems based on digital computer technology. The root cause of this concern is that the use of

shared data bases and processing equipment can result in a design that has the potential to propagate a common mode failure of redundant equipment. The resulting loss in functions would be greater than for an analog I&C system; thereby, resulting in a system that is less safe than the analog system. That is, the consequences of a common mode failure can be a loss of defense in depth.

Another key concern is that software programming errors can defeat the redundancy achieved by the hardware architectural structure. A software error is a common mode failure that can simultaneously defeat the functioning of all redundant channels or trains of the protection system, even if the protection system design has minimized the sharing of databases and digital processing equipment.

The goal for the requirements is to both limit the probability of the occurrence of common mode failures associated with digital computer technology and, since some failures will still occur, limit the extent of loss of functions in the monitoring, control and safety systems. These requirements are in addition to the existing requirements for I&C systems that are based primarily on analog technology and, therefore, place emphasis on single random failures in hardware and stress incorporation and maintenance of redundancy in equipment. These additional requirements are being developed by the staff for applicability to ALWR designs.

The challenge in the achievement of this goal of limiting the occurrences and consequences of common mode failures, is to reach the proper balance between control over the extent and means of information sharing and the potentially adverse effects that this control might have on the benefits from the application of digital technology, with its attendant potential for improvements in safety and operation of the plant.

This challenge is further complicated by the duration of the validity of Design Certification that results through compliance with these requirements, vis-a-vis the rapid rate of technology advancements in the electronics and information management fields. Regulatory requirements should not unduly impede the orderly introduction of improved technologies that address the goal for advanced reactor man machine interface (M-MI) systems: to improve the performance of the personnel involved in the operational activities of the plant (operations, maintenance, and surveillance of both plant processes and equipment).

DEFENSE IN DEPTH

The principle of defense in depth is to provide several levels or echelons of defense to challenges to plant safety, so that failures in equipment and human

errors will not result in an undue threat to public safety. The echelons of defense provided by M-MI I&C systems are as follows:

1) the monitoring and diagnostic surveillance systems that provide information to the plant operations personnel regarding the state of plant processes and plant equipment
2) the control systems that regulate plant process variables within specified normal ranges
3) the protection systems that place the plant in a safe shutdown condition when specified limits are exceeded
4) the engineered safety features systems that provide essential functions to either maintain the integrity of barriers to the release of radioactive materials or to mitigate the consequences of failures in these barriers in order to control the release of radioactive materials to acceptable limits

The foundational purpose of the requirements for the M-MI I&C system is to achieve an acceptably low probability that common mode failures caused by equipment or people will result in the loss of more than one echelon of defense in depth.

DEFENSE AGAINST COMMON MODE (COMMON CAUSE) FAILURES

The nuclear industry and the staff carefully evaluate and seek ways to improve human activities performed throughout the plant life cycle because such activities are the primary cause of common cause failures. A recent International Atomic Energy Agency (IAEA) safety practices document, Safety Series No. 50-P-1, "Application of the Single Failure Criterion," contains a section in which common cause failures are arranged by category and a general framework is provided to defend against these failures. These categories are identical to those developed by the United Kingdom Atomic Energy Authority (UKAEA) Safety and Reliability Directorate in SRD R 196, "Defenses Against Common-mode Failures in Redundancy Systems." Figure 1 (from IAEA 50-P-1) provides the categories of common mode failures. The percentages given in Figure 1 are obtained from INPO Report 85-027, "Analysis of Root Causes of Significant Event Reports," which presented the analysis of significant event reports for 1983 and 1984. This figure shows that design, maintenance, and operations activities are the major contributors to common cause failures.

The IAEA report contains the following statement:

> In the defense against common mode failures, quality, segregation and diversity are of fundamental importance. There are two basic forms of preventing common cause failures in a system; either the causal influences on the system can be reduced, or the ability of the system to resist those influences can be increased. The reduction of causal influences can be related to all the causes of failure shown in [Figure 1] and the overall defense strategy can be as shown in [Figure 2].

The various aspects of quality, especially those associated with quality assurance, to provide discipline in the design, manufacture, installation, operation, and maintenance of systems important to safety, assist in minimizing common cause failures due to human error.

The main purpose of segregation is to provide and maintain independence between redundant components so that a common influence cannot cause a common mode failure. Segregation can be regarded as a form of diverse location and environment. Many of the requirements for redundancy are directed to achieving an acceptable degree of segregation to restrict the propagation of failures between redundant channels. Segregation requirements are primarily concerned with the hardware configuration of M-MI I&C systems.

In addition to quality and segregation, there is a need for adequate diversity in human activities for the M-MI I&C system life cycle phases, and the application of the equipment (hardware and software) used in realizing the M-MIS design. The practice of diversity includes functional diversity, hardware and/or software diversity, and human diversity.

When diversity is considered for a particular application, care should be exercised to ensure that the diversity actually achieves the desired increase in reliability of the implemented design. If diverse components or systems are used, there should be reasonable assurance that such additions are of overall benefit, taking into account any disadvantages, such as additional complications in operating, maintenance and test procedures, or the consequent use of equipment of lower reliability.

One of the more effective means of achieving diversity is to require some form of diversity between preselected sets of functions (functional diversity) to ensure that common mode failures of M-MIS equipment do not degrade the performance of more than one set of these functions. The concept of functional diversity is discussed in NUREG-0493, "A Defense In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System," March 1979. In that assessment, the preselected sets of functions were control, including general monitoring functions; reactor trip; and engineered safety features. A block concept was introduced to provide a mechanism for systematically analyzing the effect of common mode failures on the defense in depth of the I&C system. The block concept aggregates the equipment (components and modules) of the system into a manageably small number of functional blocks. The staff chose three such blocks: measured variable, derived variable and command blocks. These blocks provide the equipment structure for the preselected sets of system level functions. The resulting block structure is used for the analysis of the consequences of postulated common mode failures. Figure 3 shows the block structure.

Since its initial introduction, this approach has been refined (on the U.K. Sizewell B design) to provide for some level of diversity within both the reactor trip system and the engineered safety features (ESF). This diversity will provide assurance that common mode failures of software or hardware will not defeat all the reactor trip or ESF functions.

The EPRI ALWR Utility Requirements Document uses a similar approach to establish general requirements that provide some level of protection against common mode failures in major control and monitoring functions and between the reactor trip system and the ESF. EPRI termed this approach segmentation of major functions.

In addition to the above, the staff is considering the following M-MIS regulatory requirements:

1) Requirements for the engineering activities that are used for the development of the design, manufacture, installation, operation and maintenance features of the man machine interface systems with emphasis placed on reduction in the probability of common mode failures, and
2) Requirements for the implementation of the design with emphasis on the hardware and software architectural configurations (including diversity) used to reduce the probability of the occurrence or propagation of common mode failures

SAFETY CLASSIFICATION OF I&C SYSTEMS

The present method for safety classification of I&C systems and equipment is highly deterministic in that, with a few exceptions, the I&C systems are either members of the protection system or not members, and the equipment is either Class 1E or non-safety grade.

This classification method has two major problems:

1) I&C equipment not included in the protection system is considered as non-safety equipment, although operating experience has shown it to be quite important with respect to the safe operation of the plant. Many events that resulted in a significant deterioration in the echelons of defense in depth have occurred because of failures or misoperation of equipment in monitoring or control systems that are outside of the protection systems.
2) All I&C equipment considered important to safety is also considered as part of the protection system and, therefore, must meet the criteria for protection systems as stated in IEEE-279 (10 CFR 50.55a(h)). This means that the equipment used in these systems must be Class 1E, independent of the level of importance to safety of the function performed by that system. The result can be a potentially significant first cost and overhead cost burden on utilities without the accompanying benefit justification and consequently lead to the exclusion of equipment and systems that could contribute to an improvement in plant safety.

The problem with such a limited classification method was a subject of both the findings and the recommendations in the President's Commission report on The Accident at Three Mile Island.

The Institute of Electrical and Electronic Engineers (IEEE) Nuclear Power Engineering Committee (NPEC) had initiated activities in the U.S. to develop a new classification method for I&C systems and equipment important to safety. This classification method was based on graded requirements commensurate with the importance of the involved safety function (similar to that for mechanical equipment). These activities were terminated because of what appeared to be two major concerns by the IEEE NPEC Members. One was the perception of a resultant significant increase in the complexity and number of items and, therefore, the overhead burden, for the plant I&C equipment list covered by the requirements of 10 CFR 50, Appendix B. The second was the conviction that, since there is no quantitative measure for level of importance to safety or an agreement between industry and the NRC with respect to meaningful differences in EQ (equipment qualification) and QA requirements for different levels of importance to safety, any equipment added to this graded classification would, in effect, be considered by the NRC as Class 1E, with the attendant significant increase in life cycle costs.

The international situation is different. In 1984, the IAEA issued safety guide 50-SG-D8, "Safety-Related Instrumentation and Control Systems for Nuclear Power Plants," which recommended all plant I&C systems important to safety be placed in one of three categories according to their importance to safety. The requirements for these systems are to be based on their importance to safety as established by these three categories. This safety guide, together with Safety Guide 50-SG-D3, "Protection Systems and Related Features in Nuclear Power Plants," establish distinctions between the safety systems (i.e. those systems provided to assure the safe shutdown of the reactor and heat removal from the core and to limit the consequences of anticipated operational occurrences and accident conditions), and safety related I&C systems (i.e. those systems important to safety that are not included in the safety systems.) Figure 4 depicts the relationship between these systems. Of special interest for the use of this approach in the design of the M-MIS are the graded requirements for reliability, equipment qualification, testing, design, and qualification (V&V) of software for computer and multiplexed systems, and the reliability of the computer and multiplexed systems based on the importance of the associated safety functions.

The methodology used for determining the importance to safety of a particular I&C system is based on the methodology in the IAEA Safety Guide 50-SG-D1, "Safety Function and Component Classification for BWR, PWR and PTR." In this methodology, safety functions are ranked in order of importance by the combination of:

1) the consequence of failure of that safety function (based on magnitude of potential increase in radiation exposure upon failure of that safety function), and
2) the probability that the safety function would be required.

The assignment of safety class design requirements for the equipment that performs the safety function needs a third factor that accounts for the confidence that the safety system(s) will perform as expected. That is:

3) the probability that the safety function would not be accomplished when required.

The product of these three factors must be acceptably low for all I&C systems that are important to safety. IAEA Safety Guide D8 has further subdivided this third factor to include specific factors that deal with alternative actions for accomplishing the safety function and time considerations for initiation of the safety function and for reconfiguration or repair of safety systems and equipment. Safety Guide D8 also includes general guidance for key design requirements as they relate to three categories of importance to safety: highest, intermediate, and lowest.

The International Electrotechnical Commission (IEC), Subcommittee 45A, Reactor Instrumentation, is developing an international standard "The Classification of Instrumentation and Control Systems Important to Safety for Nuclear Power Plants," which is based on IAEA Safety Guide D8.

The IEC standard presents the following:

1) A definition of the three categories of importance to safety of functions and the associated systems and items of equipment
2) Criteria for assignment of functions and associated systems and items of equipment to one of the three categories and a procedure for performing this assignment
3) Key requirements for the functions and associated systems and items of equipment important to safety for each of the three categories

These requirements are the design criteria for assuring functionality, performance, reliability, environmental durability and quality assurance of the functions and associated systems and items of equipment.

The need for a graded safety classification of I&C digital based systems is addressed by several of the requirements given in Chapter 10, "Man-Machine Interface Systems" of the EPRI Utility Requirements Document. For example, subsection 6.1.3.14 contains the following statement:

> The M-MIS functions of protection, control, alarm, and display shall be based on digital technology (instrument display formats and sensor signal conditioning exempted). This technology shall have the following characteristics [three of which were selected for this example]:
>
> - software shall be capable of being verified and validated
> - a standard software structure shall be used in all processors which provide RPS or safety system functions
> - a continuous-loop, non-interruptible software structure is preferred

Experience has shown that V&V of software has several levels of completeness that are dependent, amongst other factors, on the design attributes and operating characteristics of the computer system that the software resides

in. Mainframe systems that require multitasking to be effective cannot be verified to the same level of completeness as distributed microprocessor systems that use the preferred software structure cited above. Consequently, the assurance of reliability for the achievement of a safety function is not as high for a mainframe based system when compared to a microprocessor based system (the probability that the safety function would not be performed is higher for the mainframe system). One would, therefore, expect requirements for both deterministic hardware and software structures for I&C systems associated with safety functions whose consequence of failure would be either a significant release of radioactivity or a lower level of release but with a higher probability of occurrence.

Control room displays also perform a safety function. They assist the operator in monitoring plant operation to ensure that process variables are being maintained within the limits assumed in the safety analysis of the plant. However, the failure of the control room displays are of lesser consequence because of the functions of the automatic protection systems. Therefore, the degree of completeness one normally expects to get from a V&V program for software resident in a multitasked based mainframe (mini) computer system, commonly used for the control room displays, would be acceptable.

REQUIREMENTS FOR ENGINEERING ACTIVITIES

The requirements the NRC presently uses to determine the acceptability of an I&C design for a system or component that is important to safety concentrate primarily on the implementation of the design. For matters related to the design process, reliance is placed on references to more general requirements generated from 10 CFR 50, Appendix B: quality assurance criteria. There are also some specific requirements for the qualification of equipment, seismic testing, and the reference to the V&V process in the ANSI/IEEE computer standards.

In contrast, Chapter 10 of the EPRI Utility Requirements Document contains policy statements that form the basis for requirements for both the design of the ALWR M-MIS and the process by which this design is achieved. These statements are directed to the production of a quality design, provided that the accompanying requirements and appropriate acceptance criteria are met.

The policy statements specifically address the design process for those aspects of the design that can reduce the probability of human error, if properly specified. The human factors engineering activities include task analysis for selection and allocation of tasks between human and machine including the appropriate level of automation for each monitoring, control, and protection function.

The following are important requirements for controlling the engineering activities that follow from these policy statements:

- discipline in the design process
- verification & validation of common mode failure prone design activities (such as software development)

- diversity of skills within specified engineering teams
- documentation and configuration management
- testing, both as part of the design process (rapid prototyping) and for qualification of equipment
- the use of formal methods to specify the software functional requirements
- the use of automatic tools for both design and V&V

The requirements in the EPRI document address a range of topics governing engineering activities. However, staff review of the document finds that it does not define acceptance criteria needed to determine if these requirements have been properly implemented.

REQUIREMENTS FOR DESIGN IMPLEMENTATION

The requirements presently referenced in the standard review plan address primarily the single failure criteria and redundancy. Therefore, new requirements are needed to address the potential common mode failure sources that are more likely to exist in digital I&C systems. In some cases, additional requirements may be needed to clarify existing requirements in order to cover features of digital computer technology.

The sources of major complexities in the requirements for digital I&C systems arise from the additional configuration dimensions dealing with the system software structures (which are in addition to the hardware structures) and the need for separation between redundant function sets (because of the increased emphasis on common mode failures).

Several organizations are developing requirements for separation between redundant functions sets. The EPRI document addresses segmentation of major control and monitoring functions and other design features that reduce the probability of common mode failures. As discussed previously, NUREG-0493 presents guidelines for functional diversity between different echelons of defense in depth to address common mode failures. A consensus agreement of the types of diversity that achieve acceptable separation in the context of the different potential sources of common mode failures has not yet been achieved.

While requirements have also been developed that address specific aspects of the software structure that are potential sources of common mode failure, (for example, IEC 880, "Software for Digital Computers in Safety Systems," recommends against the use of operating systems, interrupts, etc.) there has been almost no development of requirements for system software architecture. Furthermore, the requirements addressing the system hardware architecture are almost totally from the view of independence between redundant channels or trains.

A requirement could call for a set of diagrams of system software architecture that would show the software functional configurations at the subsystem level, with designators as to the particular category of software used to perform each

function - that is; operating system software, application specific software, or embedded software. This software functional configuration could show not only the software directly associated with the monitoring, control or safety functions, but also the software support functions needed to operate the application software functions or to transfer data between subsystem. A mapping of the system software architecture into the system hardware architecture could show any overlap of software functions within hardware modules, and thereby identify areas where separation of functions for protection against potential common mode failures may not have been maintained. The system software architecture can also be used in developing requirements for software structures similar to the use of the system block architecture in Figure 3 to develop the guidelines for the blocks shown in that diagram.

Additionally, requirements could also be developed for the following:

- diversity; functional, equipment, and software
- fault tolerance
- reliability of software (There is disagreement amongst software design experts with respect to quantitative versus qualitative claims for the reliability of software. Consequently, the staff has initiated a program to address software reliability and provide the basis for a regulatory position on this method.)

Since the EPRI RD does contain requirements for digital system engineering and design implementation, the staff intends to use it to assist in the development of requirements and acceptance criteria for the different classes of I&C systems that are important to safety.

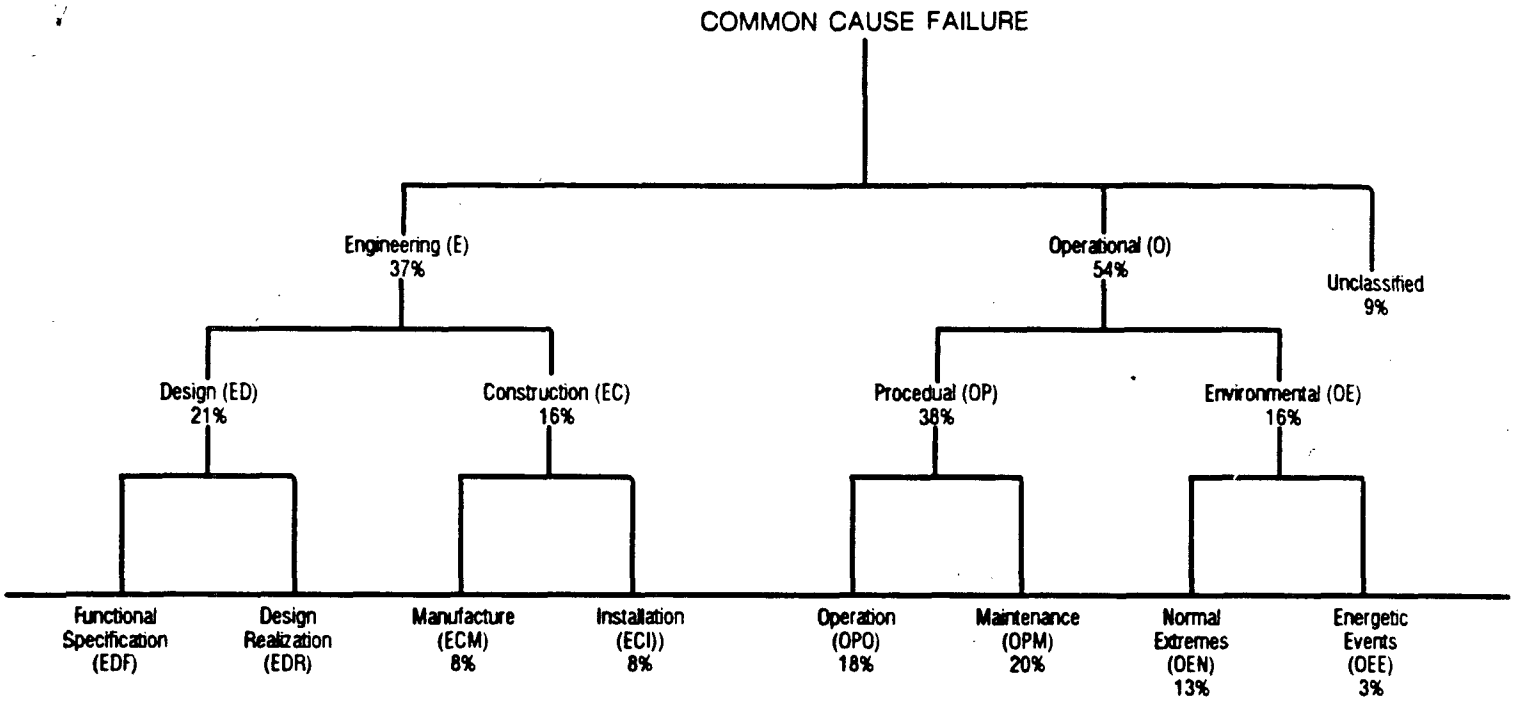


Figure 1. Categories common mode failures.

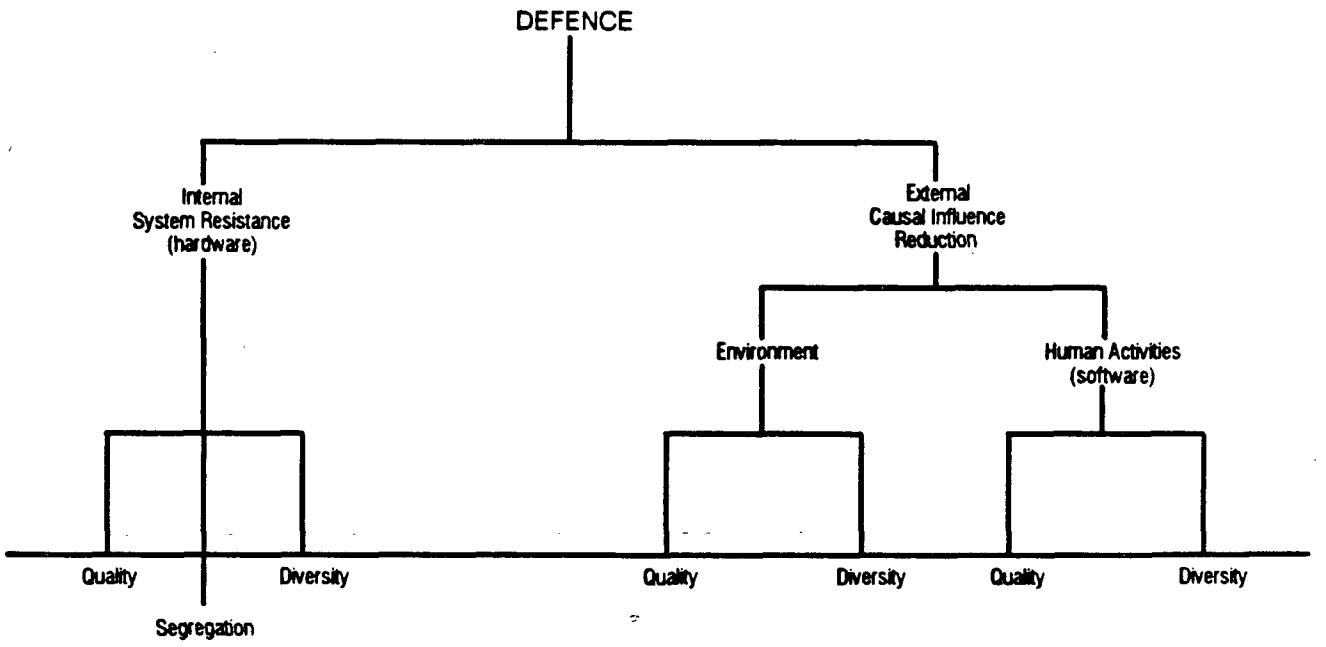


Figure 2. Common cause defence structure.

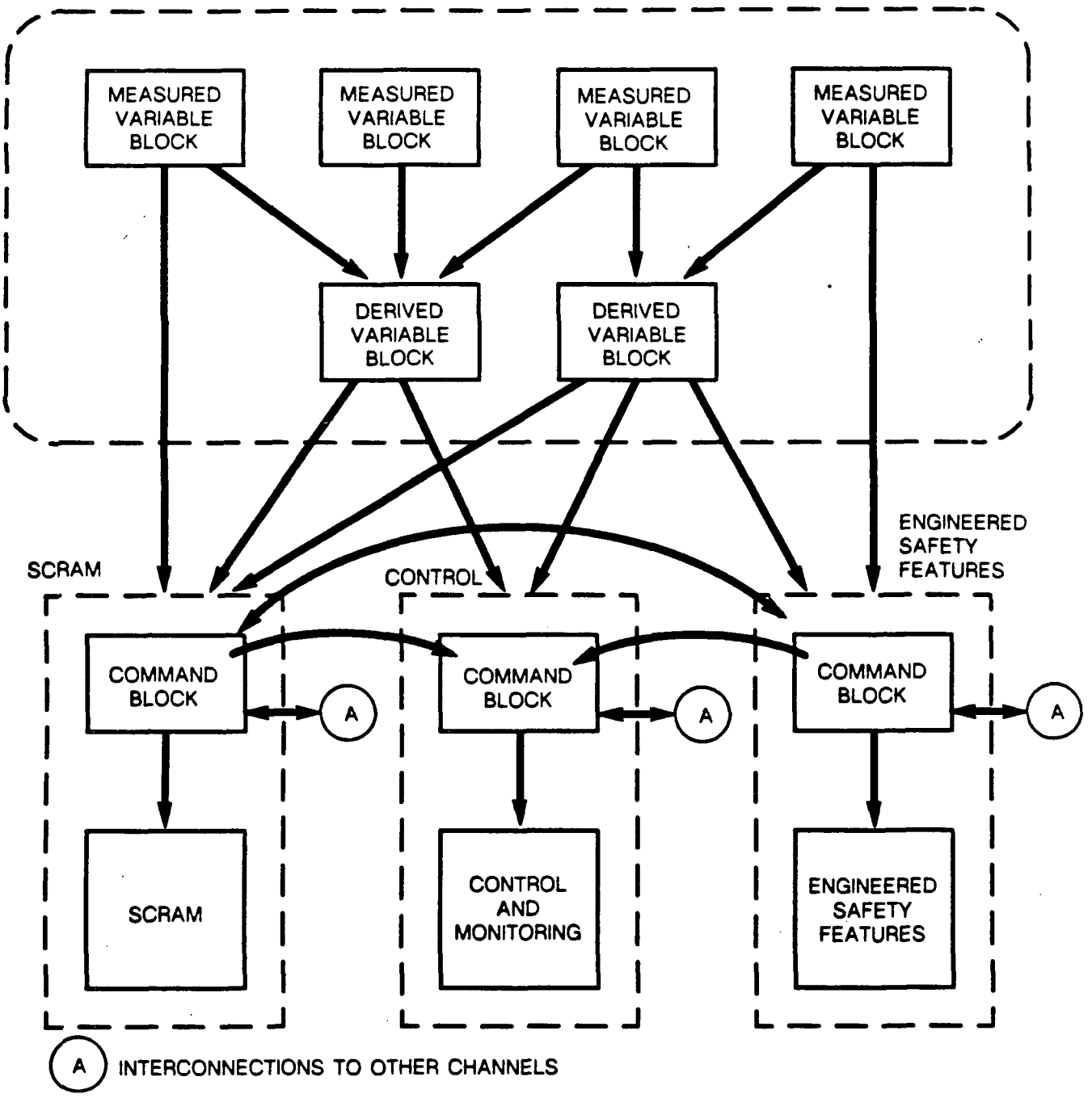
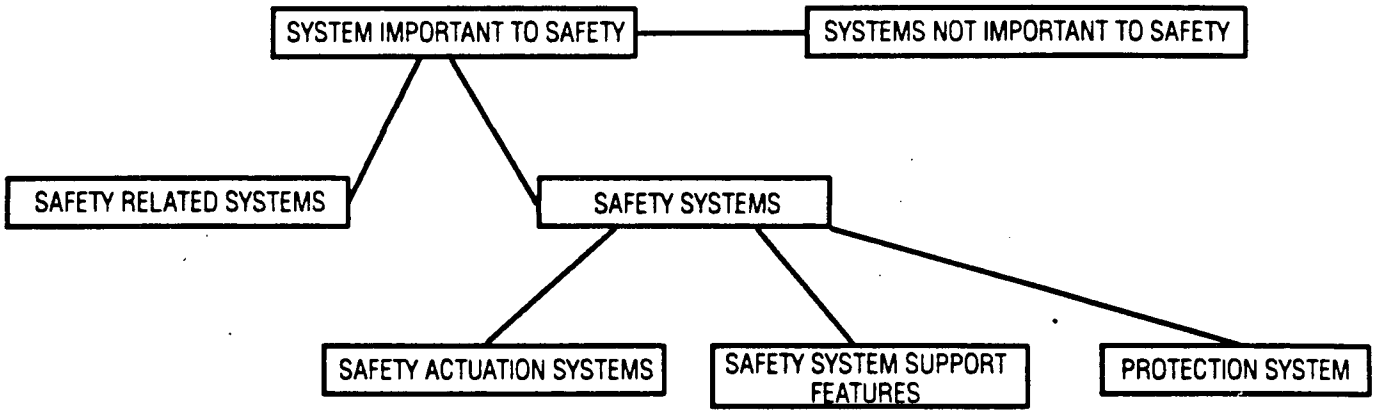


Figure 3. Basic Block Architecture for Evaluation of Defence-in-Depth Principle.



Examples*:

Fire detection and extinguishing system I&C

Fuel handling and storage I&C

I&C associated with operation of safety system

I&C for monitoring I&C

Communication equipment

Control room I&C

Utimate heat sink I&C

Power regulating system

Reactor coolant system pressure I&C

Reactor coolant system flow I&C

Access control system

Examples:

Actuation I&C for:

- Reactor trip
- Emergency core cooling
- Decay heat removal
- Containment isolation
- Containment spray
- Containment heat removal

Examples:

I&C for emergency power supply

Examples:

Initiation I&C For:

- Reactor trip
- Emergency core cooling
- Decay heat remoal
- Containment isolation
- Containment spray (pressure suppression)
- Containment heat removal

← GENERAL GUIDANCE IN IAEA Safety Guide 50-SG-D8 →

← LIMITED GUIDANCE IN IAEA Safety Guide 50-SG-D3 →

← MAIN GUIDANCE IN IAEA Safety Guide 50-SG-D3 →

* The necessary actuation devices to perform control actions may be included within the boundaries of these I&C systems.

Figure 4. Examples of I&C systems important to safety. (Examples are given for illustration. Some systems are listed in one column only although some I&C of these systems may belong to another column also, e.g. control room I&C.)

ENCLOSURE 3

STAFF REVIEW OF ALWRs

The staff is reviewing the EPRI RD for the evolutionary and passive ALWRs and two applications for design certification: the GE ABWR and the ASEA-Brown Boveri/Combustion Engineering, Incorporated (ABB/CE) System 80+.

The Standard Safety Analysis Report (SSAR) submitted for the GE ABWR does not contain sufficient design detail, as required by 10 CFR 52 and clarified by the February 15, 1991, staff requirements memorandum. The level of detail available for review is not adequate for the staff to resolve all safety questions. The staff requested the applicants to provide additional information and will continue to work with the applicants to resolve any open issues. The prototype testing required for the design certification of the microprocessor based monitoring, control and protection system, in accordance with 10 CFR Part 52, paragraph 52.47 (b) (2) (i) (B) and (2) (ii) is currently under review. This item is a major factor in establishing the level of detail required or design certification. Based on the information currently available, the staff believes that prototypes will be needed to demonstrate acceptable performance of new technology.

The staff is also reviewing the SSAR for the ABB/CE System 80+ evolutionary design. The staff's preliminary conclusion is that the ABB/CE System 80+ design submittal is more complete than the other submittal, but additional information is needed for a design certification.

The EPRI RDs contain design process requirements and system requirements beyond current regulatory requirements. The staff will use the EPRI RD to assist in identifying and resolving key issues for both the evolutionary and passive ALWRs. Enclosure 2 discusses these key issues and the development of requirements for digital systems. During the review process, the staff will inform the Commission of resolution of these issues since they may result in a significant extension to current requirements.

The staff has established a section in the Instrumentation and Control Systems Branch in the Division of Systems Technology, NRR, dedicated to the review of I&C systems of ALWRs. The staff is establishing a multi-disciplianry contractor team with technical expertise and skills to help the staff resolve the diverse and complex ALWR issues elated to the I&C systems. As requirements and positions are finalized, they will be integrated into the review process and incorporated in the updated Standard Review Plan (SRP). The Pacific Northwest Laboratories and the Lawrence Livermore National Laboratory will participate in these activities.

The NRC staff is also participating in the development and revision of both national and international standards that address the development and implementation of digital computer technology for I&C systems. The staff has members on the working groups for ANSI/IEEE-ANS-7-4.3.2., "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," and the International Electrotechnical Commission (IEC) Standard 880, "Software for computers in the safety systems of nuclear power stations."

The Office of Nuclear Reactor Regulation (NRR) staff has requested the Office of Nuclear Regulatory Research (RES) to provide support in a number of areas of advanced digital I&C systems for passive plants. The results of this effort will also support the staff in reviewing passive ALWRs.