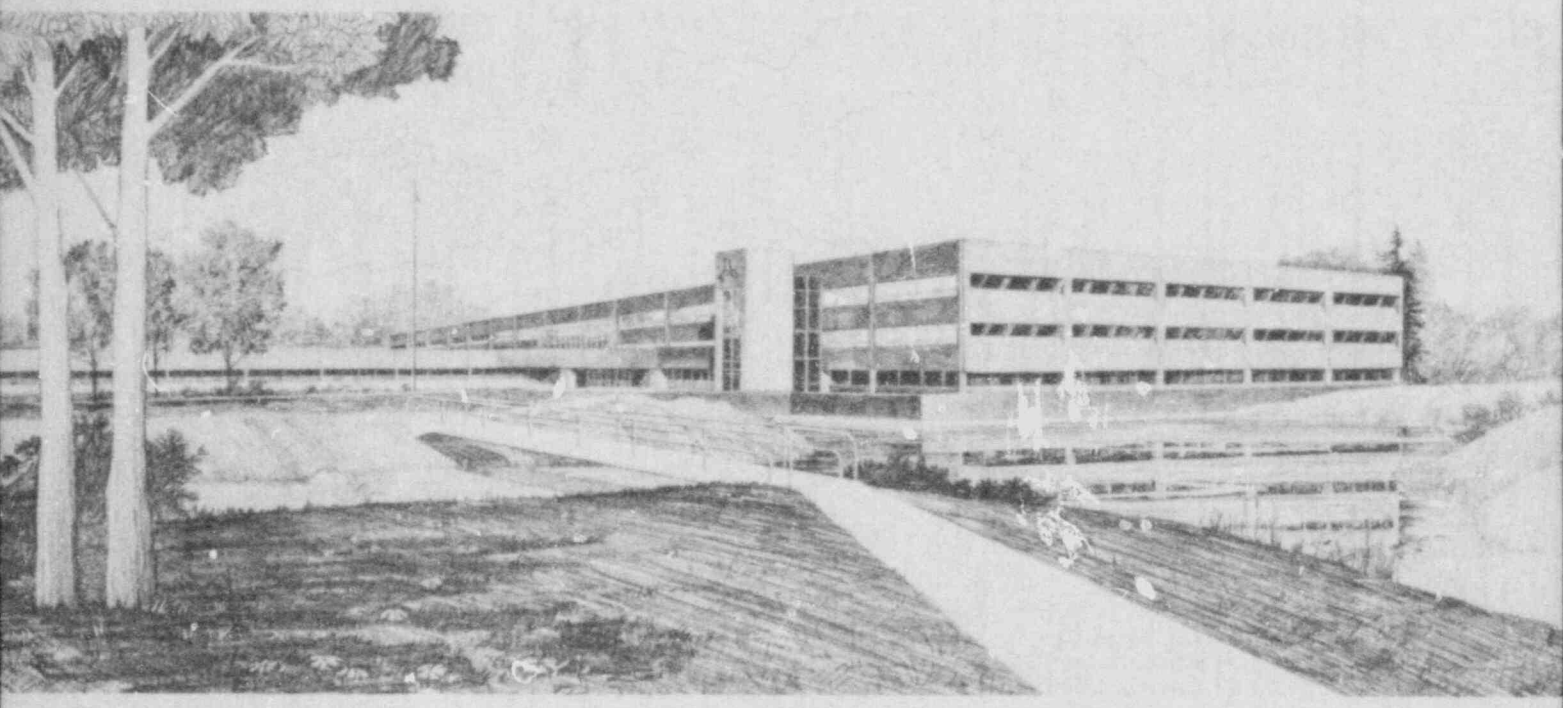
NUREG/CR-4017
EGG-2348



Idaho National Engineering Laboratory
Operated by the U.S. Department of Energy

Interim Criteria for the Use of Programmable Digital Devices in Safety and Control Systems

Dennis M. Adams
John M. Svoboda

December 1984

Prepared for the
U.S. Nuclear Regulatory Commission
Under DOE Contract No. DE-AC07-76IDO1570

EG&G Idaho

Available from

GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-4017
EGG-2348
Distribution Category: R2

INTERIM CRITERIA FOR THE USE OF PROGRAMMABLE DIGITAL DEVICES IN SAFETY AND CONTROL SYSTEMS

Dennis M. Adams
John M. Svoboda

Published December 1984

EG&G Idaho, Inc.
Idaho Falls, Idaho 83415

Prepared for the
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under DOE Contract No. DE-AC07-76IDO1570
FIN No. A6370

ABSTRACT

Proposed criteria for the application of stored program, digital computers in commercial nuclear power plants is presented. This report emphasizes recommendations for the design of computer systems and recommends a method for the regulatory review of computer system designs. More restrictive requirements are made for protection systems than control systems or other plant computer systems. In making these recommendations, the study team reviewed current regulations, past Nuclear Regulatory Commission reviews of computer systems, the work done by other government agencies, and the work done by many other countries. The results of this study provide a classification of systems, a recommended design method, and a specification of design issues to be resolved during the design and development of digital computer systems. Also included is a recommendation of subject areas that need further research activity. This report is part of a larger program to research computer system design issues, to develop design criteria (hardware and software) for Safety Parameter Dispiay Systems, to research software quality assurance, to provide a comparative risk assessment of digital technology, and to develop electrical isolation criteria.

FIN No. A6370—Research to Assess Microprocessor Based System Design and Plant Control and Associated Isolation Devices

SUMMARY

This report defines a set of recommended requirements for stored program computers used in the protection and control systems of commercial nuclear power plants. The requirements are designed to take advantage of computer capabilities and, at the same time, ensure that precautions are engineered into these systems to minimize their disadvantages. To achieve this purpose, a review was made of the current criteria including the Code of Federal Regulations, Regulatory Guides, NUREGs, and industry standards. It was concluded that although these criteria were developed before the maturation of computer technology, these criteria do not restrict the use of computers. Furthermore, the design fundamentals expressed in these criteria are sound.

In this report, computer systems are grouped into three classes according to the importance of the system to safety. These classes are then used to restrict interclass communications for the purposes of independence, separation, and diversity. A design method is described as a phase-by-phase recommended development process. Each phase briefly describes what should be included. As a review method, we recommend that each of the design issues (the major headings include Defense-in-Depth, Susceptibility of Computers, and Reliability) be audited at each design phase. Furthermore, recommendations and requirements are given for each class of computer system and each design issue.

Finally, there are subject areas in the body of this report that require more research. These subject areas are identified and summarized at the end of the report.

CONTENTS

ACRONYMS

A/D	Analog to digital
ANS	American Nuclear Society
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
CFR	Code of Federal Regulations
CPU	Central processing unit
D/A	Digital to analog
DOD	Department of Defense
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EMP	Electromagnetic pulse
ESF	Engineered safety features
ESFAS	Engineered safety features (actuation) system
FMEA	Failure modes and effects analysis
IEEE	Institute of Electrical and Electronics Engineers
ISA	Instrument Society of America
MIL-SPECS	Military specifications
NQA	Nuclear quality assurance
NRC	United States Nuclear Regulatory Commission
RAM	Random access memory
RFI	Radio frequency interference
ROM	Read only memory
RTS	Reactor trip system
SO	System operational (testing)
SPDS	Safety parameter display system

INTERIM CRITERIA FOR THE USE OF PROGRAMMABLE DIGITAL DEVICES IN SAFETY AND CONTROL SYSTEMS

1. SCOPE

This document defines interim design criteria, recommended by EG&G to the Nuclear Regulatory Commission (NRC), for the design and review of stored program digital computers (hence referred to as computers) in commercial nuclear power plants. These criteria, although designed primarily for protection and control systems, express fundamental design issues that are applicable to most computer systems.

Computer technology, when properly used,[1] can improve nuclear power plant protection and control systems and thus enhance the safety of these plants. Computer technology can also provide new capabilities and improve the reliability of these systems, but may also introduce new problems. The scope of this document is to define these new potential problems and recommend criteria for their solution. Background research work for this report is contained in a related report.[2] This previous report examines typical computer hardware and software capabilities in a process control environment, identifies safety issues, and summarizes the NRC's reviews of two major computer control and protection systems.

1.1 Purpose

The purpose of this document is to outline criteria for computer technology in commercial nuclear power plants by: not restricting or specifying functional requirements of systems, where possible; advocating computer designs that exploit the capability of this technology; requiring that computer systems be designed to minimize the adverse effects due to the disadvantages of digital technology; minimizing cost; and providing a guide for the design of computer systems to aid both the engineering design community and the NRC licensing staff. To accomplish these goals, this report develops a comprehensive set of recommended practices formulated with respect to a design method and design issues. The design method (Section 4.1) is a statement of typical engineering design steps used during development. The design issues (Sections 4.2, 4.3, and 4.4) are those items normally resolved during each of the steps in the design method. The NRC may choose to audit a system's design through the investigation of one or all of the design issues in each step of the design method. A thorough review of computer systems by the NRC is probably not possible. It is hoped that a definitive, technical statement can both inform the industry as to expected requirements and serve as a guide to the NRC staff during a review. This report does not focus on the mechanics of the review cycle but, rather, makes recommendations at the engineering and design levels. The mechanics of the review cycle is left to the NRC staff.

1.2 Current Criteria

Instrumentation and control system design standards are governed in law by the Code of Federal Regulations (CFRs) (primarily 10 CFR 50, including Appendix A and B).[3] Further clarification and guidance can be found in NRC's Regulatory Guides, NRC's Branch Technical Positions, American National Standards Institute (ANSI) Standards, Instrument Society of America (ISA) Standards, American Society of Mechanical Engineers (ASME) Standards, American Nuclear Society (ANS) Standards, and Institute of Electrical and Electronics Engineers (IEEE) Standards. Appendix A contains a list of relevant criteria-related documents.

Although many of these standards and guides were written prior to the maturation of computer technology, a careful review of these standards and guides establishes that they do not prohibit the use of computers. The concepts and engineering development methods expressed in these documents are fundamentally sound and for the most part independent of the technology used to formulate the concept. These standards and guides establish

the reliability and defense-in-depth concepts at a general or overall level of detail. The scope of this research effort is to clarify these standards and guides for computer technology at lower levels of detail.

While, it is not the purpose of this document to restate all existing standards, certain standards and requirements will be emphasized because of their importance to computers. In addition, assertions will be made to alleviate the uncertainty associated with using computers in protection and control systems.

This document references military specifications (MIL-SPECS) in several places. The Department of Defense (DOD) has developed and established extensive manufacturing and testing requirements for microelectronic components. DOD maintains a large data base on the reliability of these components. The MIL-SPECS reflect this effort. Furthermore, the microelectronic industry already understands and manufactures components to MIL-SPECS requirements. The use of selected MIL-SPECS should enhance the reliability of nuclear systems, provide data for reliability analysis of systems, and minimize difficulties in specifying hardware and software. We recommend that a formal effort be made to determine which portions of the MIL-SPECS are applicable to microelectronic components used in nuclear power plant applications.

1.3 Format of Report

Certain lines and paragraphs in the remainder of this report are marked with a "*TBC*" or a "*HOLD*." The "*TBC*" indicates that this subject is "To Be Completed" at a later date and that a significant amount of additional work will be required to formulate a justifiable position on the subject. The "*HOLD*" indicates that the stated position represents current thinking, but EG&G reserves the right to do additional research in this area.

2. DEFINITIONS AND TERMINOLOGY

The following are definitions of terms used in this report. These terms represent common usage and are derived from relevant standards given in Appendix A. Several terms require additional discussion, namely the definition of "safety related," "nonsafety related," and "important to safety."

Equipment "important to safety" is commonly referred to as "safety related" (which NRC interprets as essentially "Class 1E" equipment defined in IEEE 323-1974).[a] Safety-related structures, systems, and components are those relied upon to remain functional during and following design-basis events (see definition below).

Also of significance in this report is "nonsafety-related" electric equipment.[b] Nonsafety-related electric equipment is a part of the non-1E equipment group where a failure, under postulated environmental conditions, could prevent the satisfactory accomplishment of required safety functions by safety-related equipment. Typically, nonsafety-related equipment can: (a) inhibit a safety function, (b) give rise to a situation that challenges a safety-related system, (c) be a part of a system necessary to maintain a safe shutdown and, (d) be associated with the operation of safety systems but not be included in IEEE 603 or 308.

Finally, according to current NRC definitions, the term "important to safety" represents a broader category of equipment such that nonsafety-related equipment may still be "important to safety."

Work is continuing at Brookhaven National Laboratory and within the IEEE (P-827) concerning the definitions of safety and the development of a "2E" classification of equipment. In this report, we choose not to use the 2E designation since work is ongoing in this area. Instead, we have adopted a designation of Class I, Class II, and Class III systems to provide a graded approach to requirements for computer systems as used in nuclear power plants. These designations are defined in the alphabetical listing of terminology at the end of this section.

---

a. Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants, 10 CFR 50, Federal Register Vol. 48, No. 15 January 21, 1983 Rules and Regulations.

b. ibid.

These classifications (Class I, II, and III) are similar in purpose to the three categories used in Regulatory Guide 1.97. However, the 1.97 categories are written for accident variable monitoring instrumentation, and qualification of equipment.

Also, note that the Safety Parameter Display System (SPDS), under the conditions imposed by the NRC [SECY-82-111, March 11, 1982, and Supplement 1 to NUREG-0737, *Requirements for Emergency Response Capability* (Generic Letter No. 82-33)], is used in addition to the basic instrumentation components and serves to aid and augment these components. According to the NRC, the SPDS need not meet requirements for the single-failure criteria and it need not be qualified to meet Class 1E requirements.

The following is an alphabetical listing of the terminology as used in this report:

- ***Aliasing***—A folding of frequency spectra in a sampling system which prevents the original signal spectrum from being completely reclaimed from the sampled data. This is usually a problem when the sampling rate is low compared with the sampled signal bandwidth.

- ***Architecture***[4]—The interrelationship of the components (registers, memory, accumulators, CPUs, clock, etc.) and the bus structure organization of a stored program computer or several stored program computers.

- ***Availability***[5]—The characteristic of an item expressed by the probability that it will be (functionally) operational at a randomly selected future instant in time.

- ***Bus***—A standard protocol for the electrical signals interconnecting the components of a computer system.

- ***Class I System(s)***—Electric equipment "related to safety" that is required for the safe shutdown of a nuclear reactor. Class I systems are typically 1E systems as defined in IEEE 323-1974.

- ***Class II System(s)***—Equipment defined as nonsafety-related (but important to safety) whose failure under postulated environmental conditions could (a) prevent the satisfactory accomplishment of required safety functions by safety-related (Class I equipment, important to safety) equipment, or (b) equipment that could give rise to a situation (state of the reactor) that challenges a Class I system.

- ***Class III System(s)***—Equipment which includes those components that (a) are used in the development or testing of either Class I or Class II systems, or (b) may impact or inhibit the satisfactory operation of a Class II (or a Class I) system.

- ***Code***—A term used synonymously with computer programs.

- ***Common-Mode Failure***—Multiple failures attributable to a common cause; causally related failures of identical, redundant blocks in different channels, or of different subsystems with common elements in different echelons of defense. Common-mode failures may include failures due to severe environment, design errors, implementation errors, calibration, training, design-basis events, maintenance, etc. (see Reference 5).

- ***Computer***—As used in the text, computer refers to a stored program digital computer.

- ***Computer Family***—A group of computer devices or systems related by common characteristics or properties, usually developed by one company. For example, the Intel 8008, 8080, 8086, and probably the 80286 constitute a computer family.

- ***Computer Security*** –Protection against threats or perturbations that may affect safety.

- ***Configuration Management***—A design issue that ensures the integrity of the system components.

- ***Control System***—Equipment (defined as nonsafety-related but important to safety) provided to maintain variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to ensure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, and the containment and its associated systems. These systems are typically Class II systems as defined in this report. Class I systems may control plant variables in the classical sense but are called protection systems since they are more important to safety and defined as related to safety.

- ***Central Processing Unit (CPU)***—The registers and logic required to perform the basic logical and arithmetic operations which constitute a program.

- ***Defense-in-Depth***[6]—The defense-in-depth includes, as a general principle, design features providing for plant and public safety by the use overlapping and redundant echelons of defense [sic].

- ***Design-Basis Events***—Conditions or normal operation, including anticipated operational occurrences, design-basis accidents, external events and natural phenomena for which the plant must be designed to ensure the functions of "safety-related" equipment and systems (see definition of safety-related).

- ***Direct Memory Access***—Memory which can be accessed by input/output (I/O) devices without utilization of the CPU in order to increase system performance.

- ***Diversity***—The design approach for achieving a reduced probability of functional failure as a result of (postulated) common-mode failures by providing different equipment or methods as redundant backup.

- ***Electromagnetic Interference (EMI)***—The coupling of unwanted electromagnetic signals (conducted or radiated) that penetrate systems and produce undesirable effects.

- ***Electromagnetic Compatibility (EMC)***—The capability of electronic equipment or systems to be operated in the intended operational electromagnetic environment at designed levels of efficiency.

- ***Engineered Safety Features (Actuation) System (ESFAS)***—A system consisting of sensors, signal processors, logic and actuation-initiation devices necessary to effect functioning of engineered safety features (e.g., auxiliary feedwater, containment isolation, emergency core cooling, emergency power), including essential auxiliary systems. This echelon of defense performs a safety function.

- ***Equipment***—System components that may include both hardware and software.

- ***Error-Correction Code***—The use of an algorithm that detects and corrects errors in arithmetic processors as well as errors caused by faulty transmissions. Many algorithms exist, typically two bit error detection and single bit error correction.

- ***Fault Tolerant***—A computing system having the built-in capability (without external assistance) to preserve the continued correct execution of its programs and I/O functions in the presence of a certain set of operational faults.

- ***Fold-Over***—An undesirable condition where the output signal from a device decreases from full scale as the input signal continues to increase beyond full scale.

- ***Isolation***—The electrical and information (signal) separation between redundant systems, the trip system, the control system, and the engineered safety system ensuring independence and integrity of function.

- ***Nonsafety-Related (but important to safety)***—Those systems that are a part of the non-1E group (not Class I) whose failure under postulated environmental and operational conditions could prevent the satisfactory accomplishment of required safety functions by safety-related systems. Nonsafety-related equipment can typically (a) inhibit a safety function, (b) give rise to a situation that challenges a safety-related system, (c) be a part of a system necessary to maintain a safe shutdown, or (d) be associated with the operation of safety systems but not be included in IEEE 603 or 308.

- ***Operational Fault***—An unspecified (failure-induced) change in the value of one or more logic variables in the hardware of the system. It is the immediate consequence of a physical failure event. The event may be a permanent component failure, a temporary or intermittent component malfunction, or externally originating interference with the operation of the system.

- ***Operations Monitor***—An independent device that performs the function of determining the integrity of the system.

- ***Program (Computer Program)***—A set of ordered instructions and data that specify logical operations in a form suitable for execution by a stored program computer. Also called "code."

- ***RAM***—Random access memory.

- ***Redundancy (a redundant system)***—A system that duplicates the essential function of another system to the extent that either may perform the required function regardless of the state of operation or failure of the other system.

- ***Register***—A hardware device (usually flip-flops) that can be set and reset to high or low values used by the CPU to perform operations on computer words.

- ***Reliability***—The characteristic of an item expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.

- ***ROM***—Read only memory.

- ***Safety Group***[7]—A given minimal set of interconnected components, modules, and equipment that can accomplish a safety function.

- ***Safety-Related***—Those equipment or systems related to safety, commonly called "1E safety systems" ("Class 1E" equipment defined in IEEE 323-1974); Class I systems as used in this report. Equipment and systems that are relied upon to remain functional during and following design-basis events to ensure:

  - The integrity of the reactor coolant pressure boundary

  - The capability to shut down the reactor and maintain it in a safe shutdown condition

  - The capability to prevent or mitigate the consequences of accidents which could result in potential off-site exposures comparable to the 10 CFR 100 guidelines.

- ***Security***—Those design practices and administrative procedures/controls ensuring that the availability of the computer system is not jeopardized through malevolent, unintentional, or unauthorized access and/or perturbation.

- ***Software Practices***—Those design practices, standards, and guidelines which are followed to ensure that the developed software is acceptably error free, maintainable, responsive to requirements, structured, and changeable. Software practices typically include selecting programming languages, establishing design procedures, structure, plausibility checks, coding details, and testing provisions.

- ***Stored Program Computer***—A computer that executes programmed instructions from a stored medium as opposed to dedicated logic (function is fixed at the design stage using combinational and sequential circuits) and analog (linear) circuits.

- ***Susceptibility of Digital Systems***—The design and successful operation of stored program digital systems is dependent on several design issues that need to be addressed in each of the design phases to ensure safe system operation.

- ***System***—A functionally related group of hardware and software elements; the entire assembled equipment.

- ***Virtual Memory***—A hardware and software scheme allowing large programs to execute on small machines by maintaining only the most recently used program sections in the computer's limited memory. The least useful sections are left on disk until they are needed.

3. CLASSIFICATION OF SYSTEMS

The following classifications, defined in Section 2, "Definitions and Terminology," ensure that more stringent requirements are applied to systems related to safety. These classifications are also used to relax requirements or avoid overspecification of systems that are not as important to safety (e.g., Class II systems).

The classifications listed below provide a graded approach for establishing safety requirements with respect to the function performed and the potential impact on safety systems (the intent of General Design Criterion 1). These classifications are also consistent with the recommendations made by the President's Commission on the Accident at Three Mile Island (October 1979). The Commission's recommendations include (a) that a set of rules be developed which delineates the significance of various components and systems for the overall safety of the plant, and (b) that the discrepancy in regulations between those systems which are safety related and those systems which are not safety related is inappropriate.

Also, the January 1980 report, "Three Mile Island, An NRC Report to the Commissioners and to the Public," states that:

> "The current classification of systems and equipment into 'safety-related' and 'nonsafety-related' is especially unsatisfactory."

The report goes on to state:

> "The process is not good enough to pinpoint many design weaknesses or to address all relevant design issues. Some important accidents are outside or not adequately assessed within the 'design envelope'; key systems are not 'safety-related' ..."

For these reasons, this report attempts to provide a systems approach for the design and utilization of computers in commercial nuclear power plants. To meet the needs of this approach and the above recommendations, we developed the following three classifications and formulated rules in each class.

3.1 Class I

Class I systems are those systems that are safety related and required for the safe shutdown of the plant (see further definitions in Section 2). These systems typically include the Reactor Trip System (RTS) and Engineered Safety Feature (Actuation) Systems (ESFAS).

3.2 Class II

Class II systems represent non-1E equipment, nonsafety related but important to safety, that can affect the satisfactory operation of a Class I system (see definitions in Section 2). Class II equipment, for example, may effect reactivity, neutron flux, coolant temperature, and turbine load.

3.3 Class III

Class III systems are not important to safety and include those components that (a) were used in the development or testing of either Class I or Class II systems, (b) may impact or inhibit the satisfactory operation of a Class II (or a Class I) system, or (c) had applications that use computers but are not Class II systems. Equipment in this category typically does not perform a control or safety function and may include, for example, data logging, special purpose computer development systems, compilers, linkers, assemblers, graphics packages, test data (input and output), and equipment used to calculate calibration parameters and operational data sets for Class I, II, and III systems.

3.4 Safety Parameter Display Systems

The SPDS logically fits within our Class II designation since it is not important to safety and need not meet 1E requirements. The only current guidelines for the SPDS can be found in (a) SECY-82-111, March 11, 1982, and (b) Supplement 1 to NUREG-0737, *Requirements for Emergency Response Capability* (Generic Letter No. 82-33). Our requirements, as stated in the

remainder of this report, constitute recommendations to the NRC for the development, review, and use of computer-based systems in control and protection, including SPDS equipment.

3.5 Inter-Class and/or Channel Communications

Associated with the classification of systems are the requirements established for interclass communications or transfer of data. These requirements maintain the integrity of class designations and meet the intent of defense-in-depth requirements. The method and characteristics of the communication shall follow a standard protocol and be specified in the System Specification phase of the Design Method (Section 4.1).

In Figure 1, the arrows indicate acceptable communication paths and directions of allowed data transfer (or instruction transfer) under normal operating conditions. Other bus structures may exist within Class II and III, but are not shown. The numerics on the restricted buses refer to the paragraphs in the text. The isolation lines in the figure refer to minimum electrical isolation requirements. The communication restrictions constitute information isolation requirements. Figure 1 shows a typical reactor configuration that separates reactor trip functions from engineered safety features. Note: no interchannel communication is allowed, and an operations monitor is required for each Class 1 channel. The three dimensionality of this figure amplifies the requirements for independence and redundancy.

3.5.1 Class I to Class I. No interchannel (Figure 1) or intersafety group communication between Class I channels is allowed. Only one-way data transfer to coincidence logic is allowed.

3.5.2 Class I to Class II. There are no restrictions on communication from Class I to Class II channels, provided that timing requirements of the Class I channels or safety groups are not impaired by such communication.

3.5.3 Class II to Class I. Class II to Class I channel communication is allowed only in one channel or safety group at a time. Such communication requires administrative control, manual initiation, and bypass indication to the operators. Data and instructions transferred will be qualified by pretesting, editing and verification, and will be described in the System Requirements Specification (see Section 4.1.1).

3.5.4 Class II to Class II. No restrictions on communications are required for Class II to Class II channel communication other than imposed by the design considerations of Section 4.

3.5.5 Class II to Class III. No restrictions on communications from Class II to Class III systems are required, provided that the timing and functional requirements of the Class II systems are met.

3.5.6 Class III to Class II. There are no restrictions on communications from Class III to Class II systems, provided that the System Specification is met and that the operation of Class II systems is not impaired.

3.5.7 Class III to Class III. There are no restrictions on communications within this class.

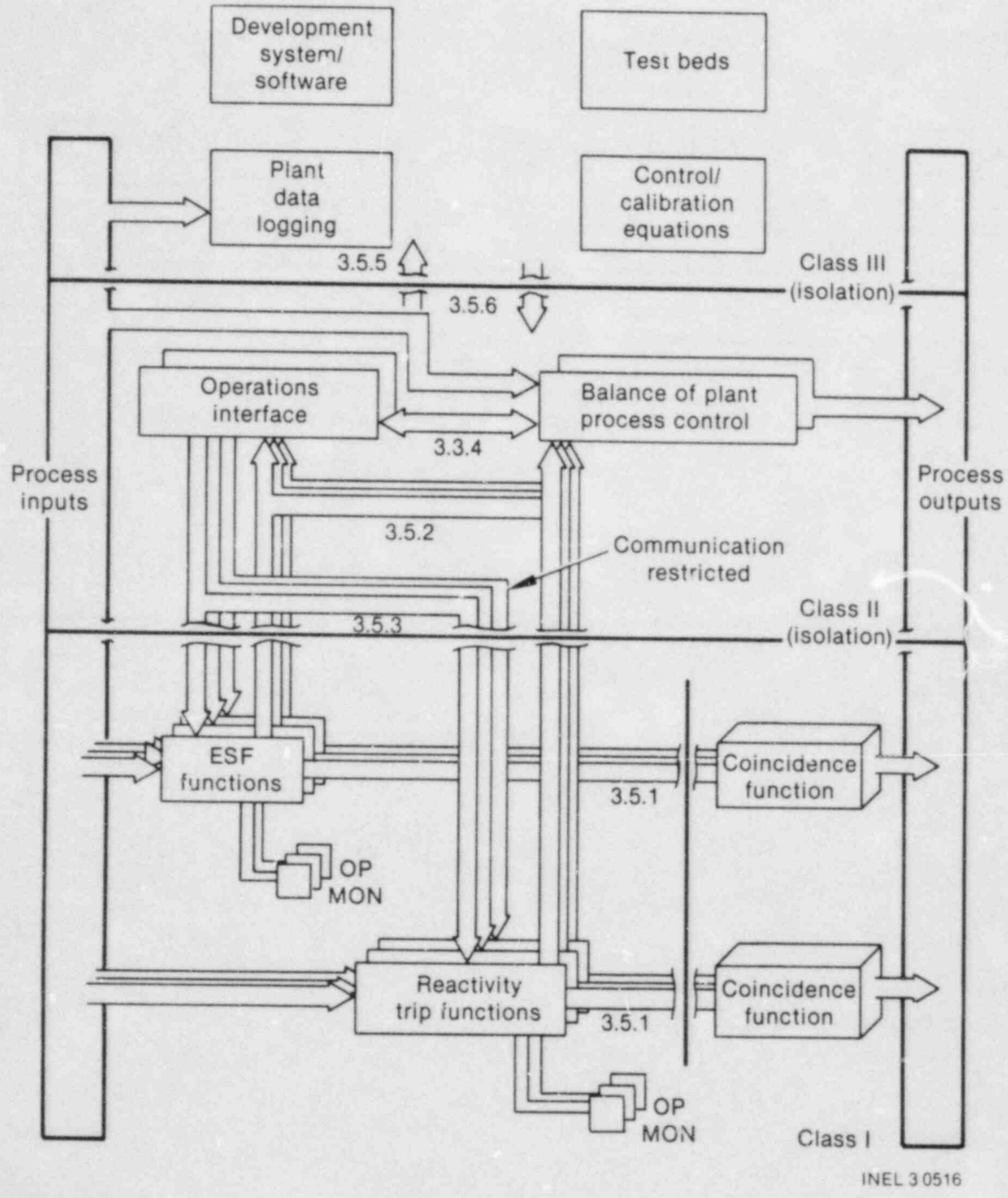


Figure 1. Typical Communication Paths.

4. DESIGN AND REVIEW REQUIREMENTS

The design of real-time computer systems for use in commercial nuclear power plants requires that numerous design issues be analyzed and, if necessary, precautions and/or constraints be engineered into the system to minimize the impact of these design issues. The issues important to the review of digital computers are grouped in the following sections under the major subject headings of 4.2 Defense-in-Depth, 4.3 Susceptibility of Computers, and 4.4 Reliability. These issues can be resolved by analysis, but when possible, actual tests are preferred. The paragraphs of Section 4.1 specify a typical design method for resolving design issues. The design method shall provide information to audit the design process, demonstrate the functional requirements of the system, and demonstrate the resolution of design issues.

We recommend that the NRC, as a review method for digital computers, review or audit each of the design issues in Section 4.2 (Defense-in-Depth), Section 4.3 (Susceptibility of Computers), and Section 4.4 (Reliability) at each phase of the Design Method in Section 4.1. The NRC, using discretion, may choose, however, to audit only one or two design issues in each step of the design method.

4.1 Design Method

A design method shall be used that meets the requirements of the following subparagraphs or their intent. The design method shall provide documentation of successes and failures and the resolution of all issues and design problems. The design method shall provide for system operation during all phases of plant operation (including design-basis events, startup, core changeout, emergency situations, and operational anomalies) throughout the life of the plant. The design method shall specify: the functional requirements of the system, the system interfaces, the standards used, requirements for integration with existing equipment, requirements for human factors, and the system concepts and constraints. The design method shall not separate the development of hardware and software since real-time systems rely on the highly interrelated aspects of both hardware and software. The purpose of the structured design method, among other things, is to provide the NRC with a documented, development history to judge completeness and quality of the product. The following recommended design steps include both hardware and software and shall include explicit provisions for the design issues in Sections 4.2, 4.3, and 4.4.

4.1.1 System Requirements Specification. This phase of the design process defines the attributes and scope of the hardware and software system to be developed and the design-basis requirements the system must meet. It is a major effort since the remaining design phases depend heavily on the system functional requirements and their realization. Typically, this phase defines "what is needed," the functions to be performed, the details of "what is needed," and a ranking of those needs. This phase should also define the organization and responsibilities of the management, the responsibilities of the designers, the requirements for the verification and validation team, and the organization and responsibilities of the quality assurance group.

4.1.2 Engineering Design Alternatives. This design phase typically evaluates the above requirements, the system constraints, and the reasons why the design should proceed in a given direction for both hardware and software. The design alternatives typically may be based on engineering analysis, comparable experience with a given reactor instrumentation design or with computer components (or families of components), test equipment or test facilities for a microcomputer family, EMI compatibility, and reliability. The purpose of this phase is to evaluate the best way to realize the system requirements and perhaps eliminate unnecessary or ambiguous requirements.

4.1.3 System Specification. This phase of design defines as many details as possible of the system to be developed and the design, engineering, verification and validation, and test methods to be used. This phase is the product of the two previous phases. It specifies the operating environment, the design philosophy, the interfaces, and the maintenance procedures to be used. The System Specification should include a list of Class I, II, and III systems, the expected process and control dynamics, the hardware components (both development and final hardware components), the software

components (both development and final software components), the calculations to be performed, the tests to be conducted, and the test data to be used.

4.1.4 Development. This design phase includes the steps and activities necessary to produce and/or procure the hardware and software components and the tests required to develop and to verify the system. Typically, this phase will also include the development of prototypes or "breadboards," the documentation of problems and their resolution, and the development of an audit trail for both hardware and software module testing. The methods used shall be those defined in the previous development phases with all exceptions documented. The verification and validation team shall design, develop, and execute tests independently in accordance with the System Requirements Specification.

4.1.5 System Qualification. This phase (sometimes referred to as the certification phase) is that validation activity which merges the actual hardware and software in a test environment for system-level testing prior to installation. The system qualification shall include a review of the hardware environmental tests designed to meet the anticipated design-basis events for the system, a demonstration of all functional requirements, and system component interactions, when possible. The requirements for the System Qualification phase shall be defined in the previous development phases and exceptions shall be documented.

4.1.6 Installation. This phase includes the actual installation of the system in the plant, including all interfaces to other hardware. This phase also includes comprehensive testing to show conformance to the Specification, recording of test data, demonstration of maintenance procedures, and training. Formal System Operation (SO) testing will be part of this activity. The verification and validation team shall specify and audit SO testing.

Post-Installation Review. This phase examines the effectiveness of the system design and performance after installation. The review shall be performed periodically for the lifetime of the plant and shall include verification of the system using installation and development tests, analysis of system discrepancies, recommendations for changes in the system, and evaluation of these recommended changes. The verification and validation team shall participate in the post-installation review and initiate activities and define requirements for changes or redevelopment.

4.2 Defense-in-Depth

The defense-in-depth principle is firmly established in the safety design of nuclear power plants. Defense-in-depth is implemented by providing overlapping and successive echelons of defense systems. Fundamental to the defense-in-depth concept is the reliance on diversity, redundancy, and independence as means of improving system reliability and avoiding common-mode failures.

4.2.1 Diversity. The Code of Federal Regulations (10 CFR 50, Appendix A, Criterion 22), states that:

> "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."

Class I systems shall be diverse in both hardware and software. Some acceptable types of diverse designs are given below.

- *Class I.* Independent software design groups can design code from a mutually developed functional requirements document. The number of independent design groups shall be consistent with coincidence logic such that the system shall never rely on only one software design. The code will run on different families of computers (different manufacturers with substantially different instruction sets) and will be developed using different compilers and test beds. Verification and validation can be met by an exchange of designs at the end of development, each design group testing and reviewing the other group's development.

- *Class I.* Systems can be made diverse by using technologies other than stored program computers on some channels, provided that redundancy and independence requirements can also be met.

- *Class I.* Systems can be designed and not be diverse provided that the functions being performed are simplistic in nature, and the number of executable statements and hardware components are minimized and proven so that significant confidence in the system can be developed through actual

testing. Statistical techniques can be used to characterize and qualify the system. An upper limit on the number of program statements is on the order of 1000 to 2000 statements with the number of program loops minimized.

- *Class II.* Computers should perform *all* reactor protection functions in a diverse and redundant mode from Class I computers. Class II computers must *not* execute software on hardware that is similar in instruction sets, compilers, and developed code. The same computer design group shall not develop the protection system code for both Class I and Class II systems. The restrictions of paragraph 3.5.3 shall apply.

- *Class II, III.* Diversity in Class II and III systems is not required.

4.2.2 Redundancy

- *Class I, II.* Redundancy for these computer systems is required to meet (a) the functional requirements of the system, (b) system operating bypasses and maintenance bypasses (IEEE Std 603 and 10 CFR 50, Appendix A, Criterion 21), and (c) the reliability and availability requirements of each class of system (also Criterion 21). The capability for manual control of all major Class I and Class II functions is also required.

- *Class III.* Redundancy is not required for Class III systems.

4.2.3 Independence

- *Class I, II.* The independence of Class I and Class II systems is required as specified by (a) Criterion 24 (10 CFR 50, Appendix A), Separation of Protection and Control Systems, and (b),as indicated in Section 3.5 (Interclass and/or Channel Communications). Electrical isolation shall be used between Class I and Class II systems in each direction and between Class II and Class III systems in each direction. Electrical isolation is recommended between major components in each class. No electrical connections are allowed between Class I channels.

- *Class I, II.* Information independence of Class I shall be maintained by restricting communication. Class II to Class I communications are allowed only in one channel at a time and require manual initiation and bypass indication to the operator. Data transferred shall be qualified by pretesting, editing, and verifying as defined in the System Specification (Section 4.1.3).

4.3 Susceptibility of Computers

The term susceptibility identifies a group of properties that are important for the design of real-time computer systems. The issues identified in the following paragraphs shall also be identified in the design methods of Section 4.1. Identification will be such that the steps taken to design for (and mitigate) problems related to these issues can be audited and reviewed at each design step.

4.3.1 Electromagnetic Compatibility (EMC). Computers shall be designed to operate in a prescribed electromagnetic environment and shall be compatible with other equipment in that environment for all system states, including design-basis events. A methodology shall be developed to define credible electromagnetic interference (EMI) threats, develop methods to minimize the threat, and test to show EMI threats can be tolerated. Table 1 lists the areas important in the design of computer systems for electromagnetic compatibility (EMC) which should be evaluated with respect to the equipment used.

4.3.1.1 Electromagnetic Interference (EMI). EMI is defined as the coupling of unwanted electromagnetic signals[8] (conducted or radiated) which may penetrate systems and produce undesirable effects. EMI includes radio frequency interference (RFI), and electromagnetic pulse (EMP) which includes static discharge. Computers, in general, are susceptible to EMI of virtually all bandwidths given energy of enough magnitude. The bandwidth to which the digital system is most sensitive depends on the type of logic used. Furthermore, the degree of sensitivity is also dependent on how and where it is applied to the logic elements, including the signal inputs, signal outputs, power inputs, and grounds. The susceptibility of logic circuits to EMI is a function of geometry as determined by component layout, signal path loop area, conductor lengths, lead routing, and location.

4.3.1.2 EMC Criteria. It shall be shown through testing, analysis, or examination that the following requirements are met:

- *Class I, II, III*—All digital systems shall not exceed radiation emissions as specified by FCC Docket 20780.
- **Hold* Class I*—Digital systems shall meet the specifications of Military Standard 461 and 462.
- *Class I, II*—A procedure to qualify computer systems for all anticipated EMI conditions shall be developed and used at installation. The procedure will also be used to requalify the system periodically.

4.3.2 Radiation. Depending on the anticipated nuclear radiation environment, computer systems shall be designed using packaging and/or shielding techniques and using digital logic that is resistant to radiation such that:

- *Class I, II.* Short term—flux density does not cause a loss of function in Class I and Class II systems.
- *Class I, II.* Long term—the devices shall be replaced before the projected integrated dose rate predicts failures.

4.3.3 Configuration Management. Configuration management shall be provided using both administrative and automated techniques to ensure that the correct, verified, and validated hardware and software is in place, is operational, and cannot be modified without following established procedures. The following items are required:

4.3.3.1 Hardware

- *Class I, II*—Keyed circuit cards and cable connectors shall be used such that each connector and card or type of card has a unique orientation, connection, and location within an enclosure.
- *Class I, II *Hold**—Cards shall be hardware labeled such that the computer can read and verify these labels for hardware revisions. The system must identify incorrect revisions and not operate unless the proper labels are read. Data to be included may contain manufacturing identification number, calibration number and date, integrated circuits (ICs), fabrication site, mask set number, and parity check sum values for error detection purposes.
- *Class I, II*—No development activities are allowed on these systems
- *Class I, II*—If second source hardware is used, proof of compatibility is required in the verification and validation procedures
- *Class I*—Off-site communication shall not be allowed by modems or any other device.
- *Class II*—Off-site communication is restricted to a "read only" mode, from the Class II systems to the off-site location, provided that the timing requirements and functions of the Class II systems are not impaired by such activity.
- *Class III*—There is no specific provision for off-site communication in this class.
- *Class I, II, III*—Spares shall be handled under strict administrative and environmental control.
- *Class I, II, III*—Any changes and/or upgrades to the system shall be documented and under strict administrative control.

4.3.3.2 Software

- *Class I, II, III*—Strict control over all software (including test case input and output data) used in the development of the system shall provide an audit trail.
- *Class I, II, III*—No revisions or changes shall be allowed to the editor, compiler, linker, locator, or libraries after verification and validation of the system, without a formal prescribed revision, and reverification and revalidation process.
- *Class I, II*—Data may be changed by the operator only if the data variables and ranges are prescribed as normal, planned changes in the System Requirements Specification.

Table 1. Subjects important in design of computer systems for electromagnetic compatibility, conditions and equipment to be evaluated, and areas to be evaluated

Line Power Conditioning Equipment

- Primary-to-secondary voltage isolation levels
- Primary-to-secondary and secondary-to-primary conducted EMI rejection characteristics
- EMI emission levels

dc Power Supplies Linear Design

- Input-to-output conducted EMI characteristics
- Input-to-output voltage isolation

Switching Design

- Input-to-output and output-to-input conducted EMI rejection
- Input-to-output voltage isolation
- Radiated EMI

Enclosures

- Radiated EMI attenuation (both electrostatic and magnetic)
- Degradation of EMI gasketing because of maintenance, time, corrosive environment, vibration and shock
- Conducted EMI attenuation at enclosure penetration

System Component Emissions

- Display devices (CRTs, printers-electrostatic, plotters, keyboards)
- Inherent EMI rejection of the system

Special Design Effort

- Decouple signal and power lines penetrating shielded enclosures, and
- Isolate process signals from other equipment (use of filtering and isolation techniques)
- Minimize lengths and loop areas of signal conductors
- Use systematic and recognized grounding and shielding philosophy.

- *Class I, II, III*—All accepted and operational revisions shall be saved for historical and backup purposes.

4.3.4 Security—*TBC*. Security is defined as those design practices and administrative procedures and/or controls that ensure the availability of the computer system is not jeopardized through malevolent, unintentional, or unauthorized access and/or perturbation. Security practices shall be defined in the System Requirements Specification and used throughout the life of the plant. In general, these practices should include:

- ***Class I, II, III.*** Distribution of access responsibility (hardware and software keys) among several individuals.

- ***Class I, II, III.*** Use of "need to know criteria" with respect to the hardware and software keys, and the details of how the system operates with respect to job responsibilities.

- ***Class I, II, III.*** Classification and marking of all data and disposal control of all detailed information about the system being developed or in use.

- ***Class I.*** No modem access to the system is allowed.

- ***Class I.*** No operator data input is allowed directly into a Class I system.

- ***Class II.*** All operator data input to the system requires an online edit for integrity checking prior to acceptance and use.

- ***Class I, II.*** Restrictions are placed on portable electrical equipment that may be brought in proximity to the computers and not previously tested for EMI generation.

- ***Class I, II.*** Once data entry is initiated, data entry shall be completed or the system will revert to previous data set.

4.3.5 Software Practices. Software practices are those design practices, standards, and guidelines which are followed to ensure that the developed software is acceptably error free, maintainable, responsive to requirements, and changeable. Software practices typically include: selection and use of computer languages, establishment of design procedures, use of error codes, structure of the code, plausibility checks, coding details, and testing provisions. The development of software practices is influenced by the characteristics of the hardware selected for use, including the hardware word length, addressing modes, cycle time, architecture of the system, and the availability of supporting hardware. Typical supporting hardware may include: memory management modules, graphics devices, error-correction chips, bus management modules, communications devices, and mathematics processors. The development of software practices is also influenced by the development hardware, the available software for both the development system (test beds), and the end product. Development software typically includes operating systems, compilers, assemblers, linkers, loaders, editors, graphics packages, and specification languages.

Unfortunately, there does not exist a standard set of software practices that, if used in a particular application, will guarantee that error-free, reliable software will be written. The state of the art is such that code development must be written using top down design, structured, and modular development techniques. The following requirements and/or recommendations are made for software practices.

- ***Class I, II, III.*** A software standard shall be written for the system being developed in conjunction with the design phases of Section 4. The standard will emphasize modularity, simplicity, and auditability as follows:

  - Tests shall be designed such that both input and expected output are defined prior to use for each module and functional requirement. Tests will also be designed to ensure that bad data is rejected and appropriate action taken.

  - Practices shall be defined to allow each team (development teams or verification and validation teams) independent access to the code being developed.

  - Group reviews and audit procedures shall be defined.

  - Methods shall be defined to ensure that the code meets the System Requirements Specification and the code is simple to understand.

- Methods shall be defined to establish the file management techniques and access methods used to manage the system development.

- ***Class I, II, III.*** Assembly language code should be avoided. Strongly typed high-level languages shall be used with three exceptions: (a) timing requirements are such that assembly code is required; (b) the functions or utilities are not readily achievable in the high-level language; and (c) upgrades to existing systems written in an older language.

- ***Class I.*** A certified or verified compiler and/or operating system shall be used. Certification may be done in parallel with system development by system developers.

- ***Class I.*** The use of interrupts shall be minimized.

- ***Class II.*** A controlled compiler and/or operating system shall be selected and used based on applicability to the problem, maturity of the software, and available support.

- ***Class I, II, III.*** It shall be shown that the assumptions made in the reliability analysis (fault trees, failure modes, effects analysis) and defense-in-depth requirements are preserved in the software.

4.3.6 Signal Conditioning. A standard, mature protocol (bus) will be used. The bus structure shall be selected based on the functional and hardware requirements. Communications design shall include consideration for the following:

4.3.6.1 Analog Input Signal Interface

- ***Class I, II, III***—The Analog-to-Digital (A/D) conversion units shall not exhibit fold-over for an input differential or common mode overvoltage condition. The A/D units must withstand the maximum credible voltage (and frequency) associated with their location and use.

- ***Class I, II, III***—The bandwidth of the A/D converter and computer combination shall be of a value sufficient to reconstruct the signal to the accuracy specified in the System Specification.

- ***Class I, II, III***—The A/D converters shall exhibit a long-term stability greater than the time between re alibration and/or scheduled maintenance.

- ***Class I, II***—Calibration of the A/D converters should not require removal of wires from terminal blocks (connectors are acceptable) or modules from equipment racks.

- ***Class I, II, III***—The A/D resolution, accuracy, and linearity shall be equal to or better than that specified in the System Specification.

4.3.6.2 Discrete Input Signals

- ***Class I, II, III***—A method shall be provided in hardware or software to effectively debounce contact state transitions, or it shall be demonstrated that these transitions have no detrimental effect.

4.3.6.3 Analog Output Signal Interface

- ***Class I, II, III***—Digital-to-Analog (D/A) conversion devices shall have their outputs sufficiently filtered to prevent noise (typically from high-speed switching) from causing spurious output.

- ***Class I, II, III***—The D/A converters shall exhibit long-term stability greater than the time between recalibration and/or scheduled maintenance.

- ***Class I, II, III***—The D/A converters' resolution, accuracy, and linearity shall be equal to or better than that specified in the System Specification.

- ***Class I, II***—Common mode, overvoltage, and/or frequency applied to the output of the D/A shall be isolated from the digital side.

- ***Class I, II***—The bandwidth of the D/A shall be consistent with the phase and timing requirements of the process being controlled.

- ***Class I, II***—Calibration of the D/A converters shall not require the removal of wires from terminal blocks (connectors are acceptable) or removal of modules from equipment racks.

4.3.6.4 Discrete Output Signal Interface

- *Class I, II*—The power-down failure mode shall be consistent with the System Requirements Specification.

- *Class I, II*—The output circuits drive capability, threshold levels, isolation levels, and delay shall be compatible with the interfacing equipment.

4.3.7 Timing. Timing is a critical issue in the design and response of any real-time system because that system must perform functions in response to stimuli within a specified time frame. A single computer system which typically executes functions in a sequential, time multiplexed manner differs from its analog counterpart which typically executes functions in parallel and continuously. This means that satisfying the system level requirements using a digital computer imposes new areas of concern that are dependent on both hardware and software characteristics. The following requirements for timing are divided into three groups where timing is critical.

4.3.7.1 Process and/or Function Level Timing

- *Class I, II*—The System Specification shall specify timing requirements for each function required for the system.

- *Class I, II*—It shall be demonstrated through testing and, if necessary, through analysis that the system will meet the specified timing requirements. This analysis shall include determination of system bandwidth including worst-case software cycle time, sample period, and response time.

- *Class I, II*—It shall also be demonstrated that the bandwidth of the signal conditioning and filters is compatible with the timing requirements for each signal and system bandwidth; this will eliminate signal aliasing due to discrete sampling.

- *Class I, II*—System timing reference shall not be derived from sources subject to common mode or single point failure. System timing shall not be derived from a reference power grid source frequency.

- *Class I, II*—If external interrupt handlers cannot be successfully completed, the design will allow control to be returned in order that other functions can be processed within required time limits.

4.3.7.2 Intercomputer Module Timing

- *Class I*—If intercomputer synchronization (only allowed in the coincidence logic between channels) is employed, it is required that synchronization errors or loss of synchronization shall not result in the loss of a protective function.

- *Class I, II*—During Class I to Class II communication, communication errors or loss of communication shall not result in the loss of a protective function.

- *Class I, II, III*—Standard protocols shall be used.

- *Class I, II, III*—We recommend asynchronous computing module operation.

4.3.7.3 Internal Computing Module Timing

- *Class I*—A simple loop structure is required that minimizes the number of paths and branches necessary to define the software cycle time.

- *Class I*—A bus contention time-out feature with error handling shall be used to prevent processor latch-up and to detect addressing errors.

- *Class II*—The preceding paragraph is recommended.

4.3.8 Single Failure

- *Class I, II*—As required in 10 CFR 50, Appendix A, Criterion 21:

  > "(1) no single failure (shall result) in loss of the protective function and (2) removal from service of any component or channel does not result in the loss of the required minimum redundancy..."

  As applied to computer systems, the single failure applies to both hardware and software components.

4.3.9 Power. Digital computer systems are susceptible to power-line noise, power loss, ac and/or dc voltage fluctuations, and ac frequency deviations. The requirements of a power system are a function of the System Requirements Specification, and the hardware and software selected to realize the requirements.

4.3.9.1 Class I, II—ac Power Conditioning. It is recommended that isolation/regulation transformers be used. Care should be exercised in the selection and use of the transformer. Single cycle loss "ride through," line frequency versus regulation, line regulation, load regulation, isolation breakdown, and transient rejection (frequency response) shall be analyzed.

4.3.9.2 Class I, II—dc Power Supplies. Similar characteristics apply for both ac and dc power systems and shall be analyzed. Also, for dc power systems, the nonvolatile memory requires additional stored energy capacity for purposes of graceful power-down. This additional requirement shall be proven through test and analysis.

4.3.9.3 Class I, II—Power-Up/Down Detection Circuitry. Care should be exercised in the selection of power-up and/or power-down detection circuitry. The circuitry shall be capable of handling the following power perturbations: a partial power up, then power down, full power up, a partial power down, then power up, and a full power down. The specific requirement is stated as follows:

The digital computer system's power source, in conjunction with the System Requirements Specification, the software design, and the hardware (vital bus, uninterruptible power supply, line voltage regulators, line filters, and dc power supplies), shall be capable of providing power such that Class I systems shall continue to operate in the presence of a design-basis power perturbation without the loss of a safety function.

4.4 Reliability

Reliability describes a fundamental design principle that includes the selection of components, specification of component interaction, and the establishment of procedures necessary to minimize risks to the completed computer system. Certainly, most of the design issues previously discussed under the headings of Defense-in-Depth and Susceptibility of Computers (Sections 4.2 and 4.3, respectively) can contribute to the development of a reliable system. Reliability is defined as the characteristic of a component expressed by the probability that it will perform a required mission (function) under stated conditions for a stated mission time (IEEE Std 352). Perhaps a more important characteristic is the availability of the system to perform the required function. Availability is defined as the characteristic of a component expressed by the probability that it will be operational at a randomly selected future instant in time (IEEE Std 352). The following is a statement of reliability requirements followed by requirements for design issues that affect the reliability of computer systems, including error detection and/or corrective action, quality assurance, verification and validation, maintenance, system architecture, and obsolescence.

4.4.1 General Reliability Requirement

- *Class I, II.* A reliability analysis must be performed during the early phases of design (typically during the Engineering Design Alternatives phase). This study will be conducted in accordance with the techniques described in IEEE Std 352 (*General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems*) for both hardware and software. The reliability analysis shall be used as a design guide throughout the remaining design phases and shall constrain the system design for both hardware and software. The assumptions made in the Failure Mode and Effects Analysis shall be demonstrated by test for both the hardware and software.

- *Class I, II.* If the fault tree indicates that a software function is only dependent on a group of functions, tests will be made to zero all common block variables, data inputs, and all other subroutines not in the dependent group to verify that the reliability analysis is valid and constraints are being observed. Similar tests are required for hardware. These tests can be performed by the development team and shall be performed by the verification and validation team.

4.4.2 Error Detection and/or Corrective Action. Error detection and/or corrective action (sometimes called fault-tolerant computing) represents a significant advantage of digital computers over analog

systems because fault-tolerant techniques[9] can be used to perform substantial real-time checking of both hardware and software. On the other hand, although fault-tolerant techniques are recommended (even required for Class I systems), the overuse or extensive use (for example the synchronization of computer modules between channels) tends to become overly complicated if these techniques are not carefully designed. Note that detection of a failure or error (and, therefore, corrective action) is implicit in the application of the single-failure criterion.[a] Fault-tolerant techniques shall be used within the design constraints previously discussed, including timing requirements, interclass communication requirements, hardware speed, and software practices. The following requirements are made for fault-tolerant computing:

- *Class I*—Fault-tolerant techniques shall be used to mitigate the consequences of both hard and soft errors and to perform analytical checks necessary to provide confidence that each function of the Class I system is performing normally or as designed. An independent system monitor is required for each channel in the Class I system to monitor the status of the system, the bus activity, and take corrective action if necessary. Also, as a minimum, single bit correction is required for memory data and instructions.

- *Class II, III*—The use of real-time hardware and software techniques to verify the integrity of the control function is strongly recommended. The use of recovery blocks, limit checks, error correction (single bit correction with two bit detection or even two bit correction), bus tests, memory checks, and recovery methods are recommended as appropriate for the design of the system being developed.

4.4.3 Quality Assurance. 10 CFR 50, Appendix B states:

> "Quality Assurance comprises all those planned and systematic actions necessary to provide adequate confidence that a ... system, or component will perform satisfactorily in service ...."

This definition and the further supporting material in *Quality Assurance Program Requirements for Nuclear Power Plants*, ANSI/ASME NQA-1-1979 shall apply for hardware and software equipment. The additional requirements as specified in this document shall be included in the quality assurance program. Additional quality assurance requirements are as follows:

- *Class I *HOLD**. Microelectronic components and circuits (microprocessors, isolation devices, and memories) shall be manufactured and tested in accordance with military specifications. The applicable military specifications are to be determined.

- *Class I, II *HOLD**. Lead personnel on the design teams, the verification and validation team, and the quality assurance team shall have a minimum of five years hands-on design experience.

4.4.4 Verification and Validation. Verification is the comparison of the step-by-step requirements for software and hardware development to determine that there has been a faithful translation from requirements of one design step to the requirements of the next design step. Validation is the determination of the correctness of the final system, that the integrated hardware and software product meets the System Requirements Specification as installed in the plant. The specific requirements for verification and validation are as follows:

- *Class I, II, III*. A verification and validation team or group shall be organized and operate independently from the design group with administrative authority to (a) require that specific test hardware and software be purchased, and (b) to hire consultants necessary to perform the verification and validation function. Resolution of design issues or differences of opinion with respect to meeting the design requirements shall be resolved by the order of the verification and validation team.

- *Class I, II, III*. The verification and validation team shall develop, design, and, if necessary, purchase hardware and software components (test beds) required to perform independent tests.

a. ANSI/IEEE Std 379-1977, "IEEE Standard Application of the Single Failure Criterion for Nuclear Power Generating Station Class 1E Systems."

- *Class I.* The methods used by the verification and validation team shall be consistent with the type of hardware and software diversity used in the design.

- *Class I, II, III.* A verification and validation plan shall be developed independently (with respect to the development activity) and shall be consistent with the design steps specified in Section 4.1 (Design Method).

- *Class I, II, III.* The verification and validation team shall certify through test and analysis at each design step that the requirements have been met.

- *Class I, II, III.* Verification and validation shall include interaction and testing during software development.

- *Class I, II, III.* The verification and validation team shall certify that a software design standard is developed, is satisfactory, and followed. They shall also certify that the implications and restrictions imposed on the design, due to the reliability analysis [(fault trees, failure modes and effects analysis (FMEA)] have been followed.

- *Class I, II, III.* The verification and validation team shall conduct static and dynamic tests to ensure that the system performs according to the System Requirements Specification. Tests shall be configured to ensure that the system operates correctly with "good" data and that it also rejects "bad" data.

- *Class I, II, III.* The verification and validation team shall determine the level of detail necessary to requalify the system after changes or maintenance have been made. It is anticipated that a substantial number of tests will be executed during the system development, and that most of these tests will be repeated after the changes are made. The results of these tests will be compared to previous results.

- *Class I, II, III.* All software maintenance, validation test software, and validation test data input and output shall be under administrative change control.

4.4.5 Maintenance. Maintenance has two definitions. First, when applied to hardware, maintenance means the execution of diagnostics and tests to detect problems and keep the hardware operational and within specifications. Second, when applied to software, maintenance is the phase in the software life cycle, following development, where repairs and improvements to operation are made. The following requirements are necessary for maintenance of both hardware and/or software:

- *Class I, II.* A manual override shall be available, as defined in IEEE Std 603, to bypass (or to inhibit) the capability of a portion of the hardware or software system for accomplishing a safety function. This shall only be permitted under administrative control.

- *Class I, II.* Only those hardware maintenance procedures shall be allowed as indicated in the System Specification.

- *Class I, II, III.* In accord with the requirements for Error Detection and/or Corrective Action (Section 4.4.2), we recommend that extensive use be made of real-time diagnostics for detecting problems and for verifying the system after routine maintenance (during normal operation).

- *Class I, II, III.* Maintenance shall be performed periodically with a period determined by the component design life, duty cycle, reliability, failure modes, environmental stress, and component or system history. This period shall be reviewed and adjusted as necessary.

- *Class I, II, III.* Hardware maintenance shall be performed to maintain each component and system within its specifications.

- *Class I, II, III.* All changes to the hardware and software not included in the System Requirements Specification or the System Specification shall require a reverification and revalidation. The level of detail required for the reverification and revalidation shall be commensurate with the class of the system, the magnitude of the change, and the relative importance of the functions being modified. Major changes may require a total redevelopment, reverification, and revalidation.

4.4.6 Architecture. The term "architecture" is used to discuss the interrelationship of the components of the system; the functional modules that provide error correction, virtual memory capabilities, extended mathematical calculations, direct memory access control, and data communications. The term "architecture" typically refers to the internal architecture of the CPU's memory, registers, accumulators, etc. The architecture of the computing hardware can enhance the reliability of the system being designed, increase the throughput of the system (speed of calculations), and enhance the functionality of the system. The architecture of the system is also a determining factor in what the software is required to accomplish. The following requirements shall be imposed on the architecture of a computer protection and control system:

- ***Class I, II, III.*** The system shall be configured to meet the interclass communications requirements of Section 3.5.

- ***Class I, II.*** The system architecture shall be configured to meet the diversity, redundancy, independence, and reliability analysis requirements.

- ***Class I.*** Each Class I channel shall have an operations monitor.

4.4.7 Obsolescence. Obsolescence is the process of phasing a component or system out of use because of outmoded design or construction, excessive maintenance, or new operational requirements. The computer industry utilizes a rapidly changing technology whose components may experience a short production time. Although most components are upward compatible with the next generation of components, the expected life time of computer components is about 10 to 15 years. This lifetime depends on the duty cycle and environment in which the components are used. Nuclear power plants are expected to last about 30 to 40 years, but they will probably be in use for a greater period of time since it may be easier to refurbish an existing plant than to license and construct a new plant. From a regulatory point of view, computer systems should be designed in anticipation of obsolescence of the hardware, and possibly the software, which ultimately may not be supported by the manufacturer. As a minimum, the following recommendations are made:

- ***Class I, II, III.*** We recommend flexibility of design, with provision for change, and adherence to standard practices for both hardware and software.

- ***Class I, II, III.*** We recommend high-level languages whose definition includes primitives for real-time, and multitasking operations.

- ***Class I, II, III.*** We recommend that a sufficient inventory of computer components be maintained for the expected life of the plant.

- ***Class I, II, III.*** We recommend that software be developed in a portable fashion, isolating the system dependancies in one or two modules.

5. RECOMMENDATIONS FOR ADDITIONAL STUDIES

In several places in this report, indications are made that additional work needs to be done in particular subjects or issues. These subject areas include (a) diversity of hardware and software, (b) criteria for EMC, (c) requirements for computer security, and (d) quality assurance issues. In addition, due to the state of the art in computer systems, additional studies should be conducted to establish reliability goals for each class of computer equipment, to evaluate software quantitatively, to determine fault-tolerant computer architecture and techniques applicable to Class I and Class II computers, and to evaluate military specifications for use in nuclear power plant computer systems.

6. REFERENCES

1. N. Wilde, *A Preliminary Reliability Analysis of Hard-Wired Circuits Versus Programmable Computers in Safety and Control Systems*, EGG-DE-6323, June 1983.

2. D. M. Adams and R. R. Rohrdanz, *Preliminary Assessment of Design Issues Related to the Use of Programmable Digital Devices for Safety and Control Systems*, EGG-EE-6102, December 1982.

3. U.S. Nuclear Regulatory Commission, *Code of Federal Regulations, Title 10, Part 50, Appendix A and B*, Washington, D.C.: GPO, 1981.

4. C. C. Foster, *Computer Architecture*, Second Edition, Cincinnati: Van Nostrand Reinhold Company, 1976.

5. ANSI/IEEE Standard 352-1975, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems.*

6. U.S. Nuclear Regulatory Commission, *A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System*, NUREG-0493, March 1979.

7. IEEE Standard 603-1980, *Standard Criteria for Safety Systems for Nuclear Power Generating Stations.*

8. M. O. Fryer, *Electromagnetic Compatibility of Computer Systems With Nuclear Power Plants*, EGG-NTP-6702, October 1984.

9. G. H. Chisholm, *Full-Authority Fault-Tolerant Reactor Control System Feasibility Study*, ANL-ACK 85010, Argonne National Laboratory, April 1984.

APPENDIX A

CURRENT CRITERIA

APPENDIX A

CURRENT CRITERIA

Licensing for construction and operation of a Nuclear Power Plant is based on numerous codes, guides, and standards. Because the use of computers in safety systems is a relatively new application, there are few documents which specifically address their use. The following lists include documents which relate to Plant Protection and Safety Systems. These documents presently are used to evaluate the application of computers in Safety Systems.

1. Law

As related to Plant Protection and Safety Systems, a licensee, *by law*, must meet the requirements of NRC's 10 CFR 50, including Appendix A and Appendix B. These systems are designed, built, qualified, installed, tested, and operated in conformance with the requirements of 10 CFR 50. Some of the Regulatory Guides, Regulations, and Industry Standards listed in Sections 2 and 3 of this Appendix must also be met by law because they are required by 10 CFR 50 or the NRC.

NRC—10 CFR 50, 1981	Domestic Licensing of Production and Utilization Facilities.
NRC—10 CFR 50 Appendix A, 1981	General Design Criteria for Nuclear Power Plants
NRC—10 CFR 50 Appendix B, 1981	Quality Assurance Program Requirements for Nuclear Power Plants

2. Regulatory Guides and Regulations

To assist those in this industry in determining compliance to 10 CFR 50 and to provide detailed guidance, numerous Regulatory Guides (RG), NUREGs, and Branch Technical Positions have been prepared by the NRC. The purpose of these documents is to assist those in the industry in understanding the position taken by the NRC on various issues as related to 10 CFR 50. The licensee is required by law to meet some, but not all, of the criteria in these documents. However, since these documents reflect the NRC's recommendations for conformance to 10 CFR 50, and since it is incumbent on the licensee to conform to 10 CFR 50, it is often easier and quicker for the licensee to obtain NRC approval (a license) by following the guides and regulations rather than to propose designs or methods which depart from them. More formally, NUREG-0800 states:

> "Regulatory Guides amplify specific regulations, describe acceptable methods for meeting requirements and provide guidance to applicants. Industry codes and standards set forth requirements and recommended practices applicable to I and C systems for nuclear power plants. These standards, as modified by the regulatory guides which endorse them, also provide acceptable methods for meeting the requirements of the regulations."

NRC RG 1.22-1979	Periodic Testing of Protection System Actuation Functions
NRC RG 1.28-1979	Quality Assurance Program Requirements (Design and Construction)
NRC RG 1.29-1978	Seismic Design Classification
NRC RG 1.33-1978	Quality Assurance Program Requirements (Operation)
NRC RG 1.47-1973	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
NRC RG 1.53-1973	Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems

NRC RG 1.62-1973	Manual Initiation of Protective Actions
NRC RG 1.68-1978	Initial Test Programs for Water-Cooled Nuclear Power Plants
NRC RG 1.75-1978	Physical Independence of Electric Systems
NRC RG 1.89-1974	Qualification of Class 1E Equipment for Nuclear Power Plants
NRC RG 1.97-1980	Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident
NRC RG 1.100-1977	Seismic Qualification of Electric Equipment for Nuclear Power Plants
NRC RG 1.105-1976	Instrument Set Points
NRC RG 1.118-1978	Periodic Testing of Electric Power and Protection Systems
NRC RG 1.131-1977	Qualification Tests of Electric Cables, Field Splices, and Connections for Light-Water-Cooled Nuclear Power Plants
NUREG-0308 1977	Safety Evaluation Report Related to Operation of Arkansas Nuclear One, Unit 2
NUREG-0491-1978	Safety Evaluation Report Related to the Preliminary Design of the Standard Reference System RESAR-414
NUREG-0493-1979	A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System
NUREG-0588-1979	Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment
NUREG-0696-1981	Functional Criteria for Emergency Response Facilities
NUREG-0737-1981	Clarification of TMI Action Plan Requirements
NUREG-0800-1981	U.S. NRC Standard Review Plan (Formerly NUREG-75/087)
BTP ICSB—12[a]	Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service
BTP ICSB—13[a]	Design Criteria for Auxiliary Feedwater Systems
BTP ICSB—14[a]	Spurious Withdrawals of Single Control Rods in Pressurized-Water Reactors
BTP ICSB—16[a]	Control Element Assembly (CEA) Interlocks in Combustion Engineering Reactors
BTP ICSB—20[a]	Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode
BTP-ICSB—21[a]	Guidance For Application of RG 1.47
BTP-ICSB—22[a]	Guidance for Application of RG 1.22

a. BTPs are located in NUREG-0800.

3. Industry Standards

Professional societies and institutes which have expertise related to the Nuclear Power Industry have prepared numerous Industrial Standards which are endorsed by the NRC. These organizations include the Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), American Nuclear Society (ANS), Instrument Society of America (ISA), and American Society of Mechanical Engineers (ASME). Some of these standards must be met by law because of a requirement by 10 CFR 50 (e.g., IEEE Std 279) or by the NRC. As stated previously, it is usually easier for the licensee to obtain NRC approval by complying to the applicable standards rather than deviating from them. The NRC has made interpretations of some of these standards with Regulatory Guides. This has been done to modify and clarify these standards when needed.

ANSI C37.90-1978	Relays and Relay Systems Associated with Electric Power Apparatus
ANSI/ANS-4.1-1978	Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations
ANSI/IEEE-ANS-7-4.3.2-1982	Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations
ANSI/ASME NQA-1-1979 (Supersedes ANSI/ASME N45.2-1977)	Quality Assurance Program Requirements for Nuclear Power Plants
IEEE 279-1971	Criteria for Protection Systems for Nuclear Power Generating Stations
IEEE 308-1980	Criteria for Class 1E Electric Systems for Nuclear Power Generating Stations
IEEE 323-1974	Qualifying Class 1E Equipment for Nuclear Power Generating Stations
IEEE 336-1977	Installation, Inspection, and Testing Requirements for Instrumentation and Electric Equipment During the Construction of Nuclear Power Generating Stations
IEEE 338-1977	Criteria for the Periodic Testing of Nuclear Power Generating Station Safety Systems
IEEE 344-1975	Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations (Modified by NRC Regulatory Guide 1.100)
IEEE 352-1975	Guide for General Principles for Reliability Analysis of Nuclear Power Generating Station Protection Systems
IEEE 379-1977	Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems
IEEE 381-1977	Criteria for Type Tests of Class 1E Modules Used in Nuclear Power Generating Stations
IEEE 383-1974	Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connections for Nuclear Power Generating Stations (Modified by NRC Regulatory Guide 1.131-1977)

IEEE 384-1980	Criteria for Independence of Class 1E Equipment and Circuits (Modified by NRC Regulatory Guide 1.75-1978)
IEEE 420-1973	Trial-Use Guide for Class 1E Control Switchboards for Nuclear Power Generating Stations
IEEE 467-1980	Quality Assurance Program Requirements for the Design and Manufacture of Class 1E Instrumentation and Electrical Equipment for Nuclear Power Generating Stations
IEEE 472-1974/ ANSI C37.90a-1974	Guide for Surge Withstand Capability (SWC) Tests
IEEE 494-1974	Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations
IEEE 497-1981	Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations
IEEE 566-1977	Recommended Practice for the Design of Display and Control Facilities for Central Control Rooms of Nuclear Power Generating Stations
IEEE 577-1976	Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations
IEEE 603-1980	Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 627-1980	Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations
IEEE 729-1983	IEEE Standard Glossary of Software Engineering Terminology
IEEE 730-1981	Standard for Software Quality Assurance Plans (Provides general guidance; not approved by IEEE for Nuclear Power Generating Stations)
ISA-RP55.1	Recommended Practice, Hardware Testing of Digital Process Computers.

A2348

NRC FORM 335 (2.84) NRCM 1102, 3201, 3202

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

SEE INSTRUCTIONS ON THE REVERSE

1. REPORT NUMBER (Assigned by TIDC add Vol. No., if any)
NUREG/CR-4017
EGG-2348

2. TITLE AND SUBTITLE
Interim Criteria for the Use of Programmable Digital Devices in Safety and Control Systems

3. LEAVE BLANK

4. DATE REPORT COMPLETED
MONTH: December
YEAR: 1984

5. AUTHOR(S)
Dennis M. Adams
John M. Svoboda

6. DATE REPORT ISSUED
MONTH: February
YEAR: 1985

7. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
EG&G Idaho, Inc.
P.O. Box 1635
Idaho Falls, ID 83415

8. PROJECT/TASK/WORK UNIT NUMBER

9. FIN OR GRANT NUMBER
A-6370

10. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

11a. TYPE OF REPORT
Final Technical

b. PERIOD COVERED (Inclusive dates)

12. SUPPLEMENTARY NOTES

13. ABSTRACT (200 words or less)

Proposed criteria for the application of stored program, digital computers in commercial nuclear power plants is presented. This report emphasizes recommendations for the design of computer systems and recommends a method for the regulatory review of computer system designs. More restrictive requirements are made for protection systems than control systems or other plant computer systems. In making these recommendations, the study team reviewed current regulations, past Nuclear Regulatory Commission reviews of computer systems, the work done by other government agencies, and the work done by many other countries. The results of this study provide a classification of systems, a recommended design method, and a specification of design issues to be resolved during the design and development of digital computer systems. Also included is a recommendation of subject areas that need further research activity. This report is part of a larger program to research computer system design issues, to develop design criteria (hardware and software) for Safety Parameter Display Systems, to research software quality assurance, to provide a comparative risk assessment of digital technology, and to develop electrical isolation criteria.

14. DOCUMENT ANALYSIS - a. KEYWORDS/DESCRIPTORS

b. IDENTIFIERS/OPEN-ENDED TERMS

15. AVAILABILITY STATEMENT
Unlimited

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

17. NUMBER OF PAGES
33

18. PRICE

120555078877 1 1AN1R3
US NRC
ADM-DIV OF TIDC
POLICY & PUB MGT BR-PDR NUREG
W-501
WASHINGTON DC 20555

EG&G Idaho, Inc.
P.O. Box 1625
Idaho Falls, Idaho 83415