November 2, 1989

MEMORANDUM FOR: Scott Newberry, Chief
Instrumentation and Control Systems Branch
Division of Engineering and Systems Technology

FROM: Theodore S. Michaels, Senior Project Manager
Non-Power Reactor, Decommissioning and
Environmental Project Directorate
Division of Reactor Projects - III,
IV, V and Special Projects

SUBJECT: REVIEW OF DRAFT ANSI/ANS 15.20 - CRITERIA FOR THE REACTOR AND SAFETY SYSTEMS FOR RESEARCH REACTORS

A Working Group has been formed to rewrite ANS 15.15 - Criteria for the Reactor Safety Systems of Research Reactors (1978:R86), which will be withdrawn when the new standard, ANS 15.20 is ready for approval. The new standard will include digital control systems.

A draft "strawman" has been developed for review (Enclosure 1). Also enclosed are draft inputs to go into the standard under the Hardware and Software sections (Enclosures 2 & 3). Your assistance is requested in reviewing these sections and the draft of ANS 15.20 (Enclosure 1).

Your comments/concurrence are requested by November 24, 1989. If you will be unable to meet this date, please notify me at x21102 within 10 days of the date of this memorandum.

Original signed by:

Theodore S. Michaels, Senior Project Manager
Non-Power Reactor, Decommissioning and
Environmental Project Directorate
Division of Reactor Projects - III,
IV, V and Special Projects

Enclosures:
As stated

cc: A. Adams

DISTRIBUTION
Docket File
PDNP r/f
WTravers
TMichaels

[TM M2 SNEWBERRY]

DFX2

PDNP:PM
TMichaels:dmj
11/ /89

PDNP:LA
SWeiss
11/ /89

RD-7-3
DJD-7
ANS

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

November 2, 1989

MEMORANDUM FOR: Scott Newberry, Chief
Instrumentation and Control Systems Branch
Division of Engineering and Systems Technology

FROM: Theodore S. Michaels, Senior Project Manager
Non-Power Reactor, Decommissioning and
Environmental Project Directorate
Division of Reactor Projects - III,
IV, V and Special Projects

SUBJECT: REVIEW OF DRAFT ANSI/ANS 15.20 - CRITERIA FOR THE REACTOR AND SAFETY SYSTEMS FOR RESEARCH REACTORS

A Working Group has been formed to rewrite ANS 15.15 - Criteria for the Reactor Safety Systems of Research Reactors (1978:R86), which will be withdrawn when the new standard, ANS 15.20 is ready for approval. The new standard will include digital control systems.

A draft "strawman" has been developed for review (Enclosure 1). Also enclosed are draft inputs to go into the standard under the Hardware and Software sections (Enclosures 2 & 3). Your assistance is requested in reviewing these sections and the draft of ANS 15.20 (Enclosure 1).

Your comments/concurrence are requested by November 24, 1989. If you will be unable to meet this date, please notify me at x21102 within 10 days of the date of this memorandum.

Theodore S. Michaels

Theodore S. Michaels, Senior Project Manager
Non-Power Reactor, Decommissioning and
Environmental Project Directorate
Division of Reactor Projects - III,
IV, V and Special Projects

Enclosures:
As stated
cc: A. Adams

ENCLOSURE 1

1 DRAFT ANSI/ANS 15.20

2 November 1989

3 Criteria for the Reactor and Safety Systems

4 for Research Reactors

FOREWORD

(This foreword is not a part of American National Standard Criteria for the Control and Safety Systems of Research Reactors, ANSI/ANS-15.20-19XX)

The American Nuclear Society Standards Secretariat established subcommittee ANS-15 in the fall of 1970 with the task of preparing a standard on the operation of research reactors. In January 1972 this charter was expanded to the multiple tasks of preparing all standards for research reactors. To implement this enlarged responsibility, a number of subcommittee working groups has been established to develop standards for consideration and complementary action by subcommittee ANS-15.

In 1978, a standard dealing with reactor safety systems at research reactors was published; ANSI/ANS-15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors." In 1987, subcommittee ANS-15 decided that the standard should be revised in light of the advent and use of computer technology in research reactors which could potentially affect the relationship of control and safety systems associated with research reactors. Accordingly, a new working group, ANS-15.15, was established in the fall of 1987 under the chairmanship of Dr. Robert C. Nelson of the United States Air Force with the task of developing an updated standard for control and safety systems at research reactors. The final work group draft was completed and reviewed by ANS-15 on _____. The standard was approved by ANS-15 on _____ and presented for processing by N-17 on _____. The standard has been redesignated as ANSI/ANS-15.20-19XX, "Criteria for the Reactor Safety Systems for Research

Reactors."

The membership of ANS-15.20 at the time of completion of the revised standard was:

Robert C. Nelson, Chairman, United States Air Force
John Bernard, Massachusetts Institute of Technology
Bill Hyde, General Atomics
Robert Walston, U.S. Department of Energy
Jenaid Rasvi, General Atomics
Frank DiMigglio, Rhode Island Atomic Energy Commission
Phil Middleton, MIDCO, Inc.
, Sandia National Laboratories
, Los Alamos National Laboratory
, Nuclear Regulatory Commission

Several of the requirements of this standard are based on the collective judgment and experience of the work group as applied to this class of reactors. The composition of the work group offers a broad spectrum of expertise in research reactor operation, control, and safety system development and engineering. They represent a wide variety of research reactors, large and small, and come from universities, national laboratories, government, and private industry. Therefore, the requirements specified in the standard represent a reasonable and responsible approach to the design of control and safety systems for research reactors.

In preparing this standard, the intent has been to specify objectives which:

a. Describe a systematic approach to establishing requirements for the control system of a new research reactor which is commensurate with the risks involved.

b. Describe a systematic approach to establishing requirements for the Reactor Safety System (RSS) of a new research reactor which is commensurate with the risks involved.

c. Ensure that important items such as safety interlocks are given proper attention with the greatest degree of latitude given the designer that safety permits.

In this process of creating standards against the background of established and varied practices in many operating facilities, it is important to consider that:

a. It is not intended that the standard be used as a demand model for backfitting purposes.

b. It should be a vital aid for existing and new owner-agency.

c. It should be helpful for the facility undergoing change/modification.

d. Its thoughtful use by industry should ease the burden of regulatory agencies.

The family of standards and task assignments include:

ANS-15.1 Development of Technical Specifications for Research Reactors

ANS-15.2 Quality Control for Plate-Type Uranium-Aluminum Fuel Elements

ANS-15.4 Selection and Training of Personnel for Research Reactors

ANS-15.7 Research Reactor Site Evaluation

ANS-15.8 Quality Assurance Program Requirements for Research Reactors

ANS-15.10 Decommissioning of Research Reactors

ANS-15.11 Radiological Protection of Research Reactor Facilities

ANS-15.14 Physical Security for Research Reactors

ANS-15.16 Emergency Planning for Research Reactors

ANS-15.17 Fire Protection Criteria for Research Reactors

ANS-15.19 Shipment and Receipt of Special Nuclear Material (SNM) by Research Reactor Facilities

ANS-15.20 Criteria for the Reactor Safety Systems for Research Reactors

The membership of Subcommittee ANS-15 at the time of its approval of this standard was:

W. J. Richards, Chairman, McClellan Air Force Base

L. C. Brinkerhoff, U.S. Department of Energy

W. J. Brynda, Brookhaven National Laboratory

B. L. Corbett, ORNL, Martin Marrietta Energy Systems, Inc.

A. F. DiMeglio, R. I. Nuclear Science Center

J. P. Farrar, University of Virginia

D. E. Feltz, Texas A & M University

T. F. Luera, Sandia National Laboratory

G. W. Nelson, University of Arizona

R. C. Nelson, United States Air Force

D. P. Pruett, Argonne National Laboratory - West

T. M. Raby, U.S. National Institute of Standards and Technology

E. Roybal, U.S. Department of Energy

L. S. Rubenstein, U.S. Nuclear Regulatory Commission

R. R. Walston, U.S. Department of Energy

M. H. Voth, Pennsylvania State University

W. L. Whittemore, General Atomics

The American National Standards Committee N-17, Research Reactors, Reactor Physics, and Radiation Shielding had the following membership at the time it reviewed and approved this standard:

R. S. Carter, Chairman

T. M. Raby, Secretary

Organization	Representative
American College of Radiology	M. M. Ter Pogossian
American Institute of Chemical Engineers	D. Duffey
American Nuclear Society	R. S. Carter
American Physical Society	H. Goldstein
American Public Health Association	W. A. Holt
Health Physics Society	S. H. Brown
	A. G. Johnson (alt)
National Institute of Standards & Technology	T. M. Raby
U. S. Department of Energy	P. B. Hemming
	J. W. Lewellen (Alt)
U. S. Nuclear Regulatory Commission	L. I. Kopp (ANS-10)
	L. S. Rubenstein
McClellan Air Force Base	W. J. Richards (ANS-15)
ORNL, Martin Marietta Energy Systems, Inc.	D. K. Trubey (ANS-6)
Union Carbide Corp (retired)	A. D. Callihan (ANS-1)

1	U. S. Army, White Sands Missile Range	A. DeLaPaz (ANS-14)
2	Individual Members	J. D. Buchanan
3		W. L. Whittemore
4		R. E. Carter
5		J. E. Olhoeft
6		A. Weitzberg

Criteria for the Control and Safety Systems of Research Reactors.

1. SCOPE

This standard documents the criteria from which design requirements are established for the reactor safety system of an individual research reactor.

2. PURPOSE

This standard is intended to serve the research reactor community for establishing criteria for control and safety systems. Its application should be in lieu of ad hoc application of part or all of any similar standards for power reactors.

3. DEFINITIONS

The following terms are defined in order to establish their usage in this standard and to document the meaning of terms used frequently in the community. The definitions of several terms (such as Safety Limit, Limiting Safety System Setting, Engineered Safety Feature, Safety Analysis Report, and Restricted Area) are not included because they are generally well known or are readily available in other documents such as Title 10, Code of Federal Regulations, Part 20, "Standards for Protection Against Radiation;" Title 10, Code of Federal Regulations, Part 50, "Licencing of Production and Utilization Facilities;" and American National Standard for the Development of Technical Specifications for

Research Reactors.

bypass. The deliberate inhibition of the capability to provide a protective action; for example, the application of a short circuit across the contacts of low-flow trip relay either in order to perform a test of the channel or to operate in a natural convection mode.

credible. A postulated event or condition is considered credible unless it has been shown to have a probability of occurrence that is so infinitesimal that there is virtually no chance that it will occur. (Usually taken to be an event probability > 10^{-6}.)

Design Basis Event (DBE). Anticipated operational occurrence (such as the loss of coolant flow or a reactivity excursion) which is used to determine the specific design requirements for the reactor safety system.

negligible-risk research reactor. A research reactor for which, in the postulated event of the complete failure of the reactor safety system coincident with the occurrence of the most adverse Design Basis Event, the radiological consequences with respect to Public Health and Safety would be negligible. Negligible radiological consequences are taken to be an exposure/release of radioactivity, in one day due to an accident, in a quantity which would not exceed the limit permitted to be released over a year due to routine operations. Specifically, the consequences could not exceed:

(1) the exposure of the whole body[1] of an individual in an unrestri ted area to 0.5 rem of radiation or the exposure of "any other organ" of such an individual to 1.5 rem of radiation; or

(2) the exposure of the whole body of an individual located at an allowed position in a restricted area of the reactor facility to 5 rem of radiation or the exposure of "any other organ" of such individual to 15 rem of radiation; or

(3) the release of radioactive materials in concentrations at a point where a member of the public could be located which, if averaged over a period of 24 hours, would exceed 365 times the limits specified for such materials in Title 10, Code of Federal Regulations, Part 20, Appendix B, "Concentrations in Air and Water above Natural Background," Table II.

operable. Capable of performing the intended function (providing the protective action when required) in an acceptable manner.

protective action. The initiation of a signal or the operation of equipment within the reactor safety system in response to a variable or condition of the reactor facility having reached a limit specified in the Design Basis.

(1) At the protective instrument channel level, protection action is the generation and transmission of a trip signal indicating that a reactor variable has reached the specified limit.

(2) At the protective instrument subsystem level, protection action is the generation and transmission of a trip signal indicating that the decision has been made that a Design Basis Event has occurred.

---

[1]The "whole body" value shall also apply to the active blood-forming organs, gonads, fetuses, and lenses of eyes.

Note: Protective action at this level would lead to the operation of the safety shutdown equipment.

(3) At the protective instrument system level, protection action is the generation and transmission of the command signal for the safety shutdown equipment to operate.

(4) At the reactor safety system level, protective action is the operation of sufficient equipment to immediately shutdown the reactor.

protective instrument channel. That combination of discrete modules and interconnections necessary to sense one reactor variable related to a Design Basis Event and to initiate and transmit a protective signal if and when that variable reaches the specified limit.

protective instrument subsystem. The combination of protective instrument channels and any decision logic units (e.g., two-out-of-three) necessary to determine that one of the Design Basis Events has occurred and to transmit the necessary protective signals.

shall, should, and may. The word "shall" is used to denote a requirement; the word "should" to denote a recommendation; and the word "may" to denote permission, neither a requirement nor a recommendation.

unsafe failure. Any malfunction such that the unit (i.e., module, channel, subsystem, system, or piece of equipment) is no longer operable. A malfunction which results in the immediate execution of the protective action of the unit is not an unsafe failure.

4. DESIGN BASIS

The reactor control system (RCS) and reactor safety system (RSS) shall have a documented design basis, which shall be kept available to facilitate a determination of the adequacy of the RCS and RSS design, including design changes. Appropriate sections of the safety analysis report may serve this purpose.

4.1 CONTROL SYSTEM.

4.2 SAFETY SYSTEM.

For each mode of operation of the research reactor, the design basis shall address and discuss in appropriate detail at least the following items:

(1) Each Design Basis Event for which the RSS must function; the limits of allowable facility conditions for each event.

(2) The decision criteria for determining which events have consequences capable of transcending the RSS and therefore are to be accommodated by either safety interlocks or engineered safety features.

(3) Safety interlocks to be provided and the specific function of each.

(4) Those protective actions which must be automatic; those which may be solely manual.

(5) The reactor variables to be monitored to detect the occurrence of each Design Basis Event: for those variables that have spatial dependence, the minimum number and locations of sensors needed for safety purposes.

(6) The limiting values of the setpoints at which protective actions must be

initiated; requirements to change setpoints to accommodate different modes of operation of the reactor.

(7) The protective instrument subsystem intended to monitor the reactor variables associated with each Design Basis Event; the number of channels required in each subsystem; the required separation between both the units of and interconnections for redundant channels; any required decision logic.

(8) Minimum performance requirements for each protective instrument subsystem including such items as range, accuracy, and response time.

(9) The required characteristics of the safety shutdown equipment including such items as response time and interface with the protective instrument system.

(10) The ranges of external conditions (both steady-state and transient; normal, abnormal, and accident cases) throughout which the RSS must remain operable.

Note: External conditions include such items as the supply power, temperature, humidity, vibration, radiation, fire, explosion, earthquake, flood, lightning, missiles, and wind.

(11) The conditions having the potential for functional degradation of the RSS and for which provisions must be incorporated to retain the capability for protective actions.

(12) Bypass capability needed for any part of the RSS; the permissive conditions associated with the use of each bypass; and related special precautions.

(13) Any design reliability goals for the RSS; the need for test provisions during reactor operations; objectives, methods, and acceptance limits; recommended intervals for checks, tests, and calibrations.

(14) Beyond those normally provided, any quality assurance requirements needed

to accommodate any unusual or unique aspects of the design of the RSS.

(15) The administrative controls necessary to satisfy the requirements of this standard in conjunction with the physical features of the RSS.

5. DESIGN CRITERIA

5.1 SINGLE FAILURE

5.1.1 **Statement of the Criterion**: The reactor safety system (RSS) design shall provide a level of reliability and redundancy such that the RSS can, as a minimum, perform the required protective actions in the presence of any single failure within the RSS concurrent with:

(1) the occurrence of all failures caused by the single failure and

(2) all failures caused by the Design Basis Event.

Specifically the protective actions required are:

(a) those for each safety interlock.

(b) the intended automatic detection of each Design Basis Event and the immediate execution of the safety shutdown of the reactor.

(c) the manual execution of safety shutdown of the reactor.

5.1.2 **Application**: Except as provided below, the single failure criterion stated above shall be applied to the design of the RSS for each research reactor.

(1) A probabilistic assessment of the RSS may be used to eliminate certain postulated failures from consideration on the basis that such failures are shown not to be credible.

(2) For negligible-risk research reactors, compliance with the single failure criterion for protective actions (a) and (b) of 5.1.1 is not mandatory.

(3) For pulse reactors, compliance with the single failure criterion for protective action (b) in 5.1.1 is not mandatory for those portions of the RSS which function only for reactivity excursion-type events. A pulse reactor is a reactor that has been specially designed with an inherent shutdown mechanism sufficient to allow the reactor to accept large reactivity insertions without exceeding any safety limit.

(4) If trustworthy failure rate data are available, reliability analysis may be used to demonstrate that the RSS satisfies such sufficient reliability goals that exemption from compliance with the single failure criterion for protective actions (a) and (b) in 5.1.1 is justified. The minimum level of reliability considered generally acceptable for this purpose is that equivalent to 95% confidence that operation without the needed protective action for a Design Basis Event will occur no more often than once in the operating life of the research reactor and 95% confidence that such a failure of the RSS will be detected prior to or during the startup for the next day of operation.

(5) As an alternative to compliance with the single failure criterion for protective actions (a) and (b) in 5.1.1, the RSS may include methods that promptly detect unsafe failures and alert the reactor operator, provided that:

(a) the composite reliability of the basis portion of the RSS and its associated fault detection method is comparable to that which would be attained by direct compliance.

(b) the fault detection methods do not introduce a credible common failure mode.

(c) written administrative controls are provided which include appropriate specific actions to be taken when a failure is detected.

5.2 REDUNDANCY.

The following types of redundancy shall be considered. To the extent advantageous and practical, the indicated order of preference shall be incorporated:

(1) Functional diversity - monitoring different reactor variables related to the Design Basis Event.

(2) Equipment diversity - monitoring the same reactor variable using equipment with different principles of operation.

(3) Simple redundancy - monitoring the same reactor variable using duplicate equipment.

5.3 INDEPENDENCE.

Where the application of the single failure criterion is mandatory, the following are also required.

5.3.1 Redundant channels and subsystems shall be physically separated from each other either by suitable barriers or by distances sufficient to accommodate the external conditions detailed in the design basis.

5.3.2 Where signals from redundant units are necessarily brought together, such as at the inputs of logic units, the RSS shall include sufficient isolation to prevent an unsafe failure in one unit from causing an unsafe failure in a redundant unit.

5.3.3 Attention shall be given to the situation where a credible single failure could both initiate a Design Basis Event and cause the loss of the corresponding protective action at the channel or subsystem level. One such situation is where a control system input signal is derived from a protective instrument channel (a neutron-level channel, for example).

For any such situation, additional redundancy shall be provided to the extent necessary to assure that loss of protective action at the system level is not credible. The additional units shall themselves satisfy 5.1.2 along with the other requirements of this standard.

5.4 FAIL-SAFE DESIGN.

A design objective shall be that no malfunction within the system, caused solely by the variations of external conditions within the ranges detailed in the design basis, will result in an unsafe failure.

5.5 SETPOINTS.

The RSS shall include physical features that assure that the proper setpoints are automatically made active or include features that facilitate administrative controls to verify the proper setpoints, or both, with the operating mode of the reactor is changed.

5.6 MANUAL INITIATION.

Simple and direct means shall be provided for the reactor operator to immediately activate the safety shutdown equipment.

5.7 BYPASSES.

5.7.1 The design of the CS and RSS shall provide bypass capability only where necessary to accommodate essential functions such as: changes in the operating mode of the reactor or periodic testing which must be conducted during reactor operation.

5.7.2 Bypass of manual initiation provisions of the RSS shall not be allowed.

5.7.3 The RSS shall include features which either physically provide for or facilitate administrative controls to:

(1) prevent unauthorized use of bypasses.

(2) limit the types and number of simultaneous bypasses for each mode of operation to that shown to be acceptable in the design basis, and

(3) prevent bypasses being inadvertently left active.

5.7.4 The initiation of any bypass during operation shall be immediately announced both audibly and visually. Thereafter, continuous indication of each active bypass shall be provided in the normal and immediate field of vision of the reactor operator.

5.7.5 Bypasses of a part of the RSS to perform periodic testing during reactor operation shall be allowed only when the remainder of the RSS satisfies 5.1.2 and 5.3.4.

For one-out-of-two portions of the RSS: when a bypass is necessary for a brief time to perform periodic testing, compliance with 5.1.2 is not mandatory if the reliability of the portion remaining active has been shown to be acceptable. For example, the time permitted for the bypass has been shown to be so brief that the probability that the active portion might fail during the bypass time is commensurate with the probability that the one-out-of-two system might fail during the normal operating time between tests.

5.6 COMPLETION OF PROTECTIVE ACTIONS.

5.8.1 Each channel shall indicate in a distinctive manner when it is in the tripped state.

5.8.2 Once tripped, the RSS shall remain in the tripped state at the system level and shall indicate the protective instrument subsystem initiating the shutdown until deliberate action is taken by the reactor operator.

The manual reset mechanism shall not be capable of preventing the initiation of protective action. The manual reset mechanism for the RSS shall be physically and electrically separate from mechanisms for any acknowledgement and reset for alarms that are not part of the RSS

5.9 SURVEILLANCE.

5.9.1 The RSS shall include capability for periodic checks, tests and calibrations.

5.9.2 In the event that the disabling of a channel (for example, by the disconnection of a detector) is necessary to conduct a surveillance activity, the RSS shall include either features which physically assure that operability is restored before allowing any operation of the reactor for which the operability is required or features which facilitate administrative controls which specifically accomplish the same function; for example, a prestart instrument checklist.

5.9.3 Where on-line periodic testing is necessary, such testing shall not reduce the capability of the RSS below that required by 5.7.5.

5.10 ACCESS CONTROL.

5.10.1 The RSS shall include physical provisions, such as a keyswitch, to prevent the unauthorized use of the reactor controls.

5.10.2 The RSS shall include physical means, such as recessed screwdriver adjustments or protective covers, to limit access to setpoint and calibration adjustments to the extent necessary to prevent inadvertent misadjustments.

5.11 CLASSIFICATION AND IDENTIFICATION

5.11.1 Any unit that is used both to perform protective actions of the RSS and nonsafety actions shall be classified as part of the RSS.

5.11.2 All RSS equipment, including interconnections, shall be physically marked in a manner that is obvious and is distinctively indicative of RSS equipment. When components or modules are mounted within assemblies that are clearly marked as being part of the RSS, the marking of individual components or modules is not required.

5.11.3 RSS features on drawing, design change documents, etc. shall be distinctively identified. All RSS drawings shall be kept current.

1 6. QUALITY ASSURANCE.

2 6.1 The quality assurance requirements for the RSS are to be satisfied through
3 the overall quality assurance program approved for the reactor facility.

4 6.2 The quality of components and modules shall be commensurate with the degree
5 of their safety importance and any reliability goals of the RSS. Where the use
6 of one-of-a-kind or unproven designs becomes necessary, such cases are to be
7 identified and supported by special quality assurance measures.

8 7. HARDWARE.

9 8. SOFTWARE.

10 9. REFERENCES.

ENCLOSURE 2

HARDWARE

Issues that shall be reviewed for hardware are as follow:

a. Environmental and Seismic Qualification

The hardware should be built and designed to withstand the environmental and seismic background in which the system will operate.

b. Electromagnetic Interference (EMI) Environment

Provisions for precluding or minimizing EMI should be provided. Features such as optical isolation, shielding, bypass filters and signal conditioners should be provided.

c. Power Supplies

The power supplies for the system should be buffered to reduce the possible impact of minor power line fluctuations. Random access memories should be backed-up by battery power. Scram circuits should scram when power is lost to them and self-diagnostic circuits should scram the reactor when fault conditions are detected.

d. Failure Modes and Effects

Probability risk assessment techniques may be used to predict failure to scram for various failure modes. Failure modes such as the following should be considered:

1) Physical System Failure (wire breaks, shorts, ground fault circuits)

2) Limiting Safety System Setting Failure (failure to detect)

3) System Operable Failure (loss of monitoring)

4) Computer/Manual Control Failure (automatic and manual scram).

SOFTWARE

An approved verification and validation (V&V) plan for the development of software which performs a safety function shall be provided. Use of Standard ANSI/IEEE-ANS-7-4.3.2-1982 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations" is an appropriate standard for use in V&V of research reactor software except as noted below in Section d.

V&V Plan

Verification and validation (V&V) are two separate but related activities that follow the development of software. Verification determines whether the requirements of one phase of the development cycle have been consistently, correctly, and completely transformed (fulfill the requirements) to the subsequent phase of the cycle. Validation is the testing of the final product to ensure that performance conforms to the requirements of the initial specification. The need for V&V arose because software is very complex, and prone to human errors of omission, commission and interpretation. V&V provides for an independent verifier to work in parallel with, but independent of, the development team to ensure that human errors do not hinder the production of safety software that is reliable and testable.

In executing V&V, certain principles have proven over time to be very effective in software development programs. These principles can serve as a comprehensive reference base for applying the applicable criteria for software evaluations of Class 1E safety systems.

a. Well defined systems requirements expressed in a well written document including a functional specification which lists in detail the functions that are to be performed by the digital safety system.

b. A development methodology to guide the production of software. The primary specification for the software provides the foundation for not only sound development but also of effective verification and validation activities. The individual requirements in the specification for any software system describe how the software is to behave in any circumstance. The specification must be reliable and testable. A reliable specification exhibits the following characteristics:

- Correct - Each requirement of the safety function has been stated correctly.
- Complete - All of the requirements for the safety function are included.
- Consistent - The requirements are complementary and do not contradict each other.
- Feasible - The requirements can be satisfied with available technology.
- Maintainability - The requirements will be satisfied for the lifetime of the equipment.

- Accuracy - The requirements include the acceptable bounds of operation.

c. Comprehensive testing procedures should be developed which validate the specific functions that the digital control system and its software are to perform. The organization that tests these functions shall acknowledge that each of these functions have been tested.

d. A key ingredient in an effective V&V process is the independence of the V&V team from the development organization. The level of independence shall be such that the V&V team shall at least report to a different supervisor than the development organization. This requirement differs from the requirements of Section 4 of Supplement 3S-1 of NQA-1-1979 referred to in ANSI/IEEE-ANS-7-4.3.2-1982 in Section 7.1. In Supplement 3S-1 the V&V team and the development team can report to the same supervisor.