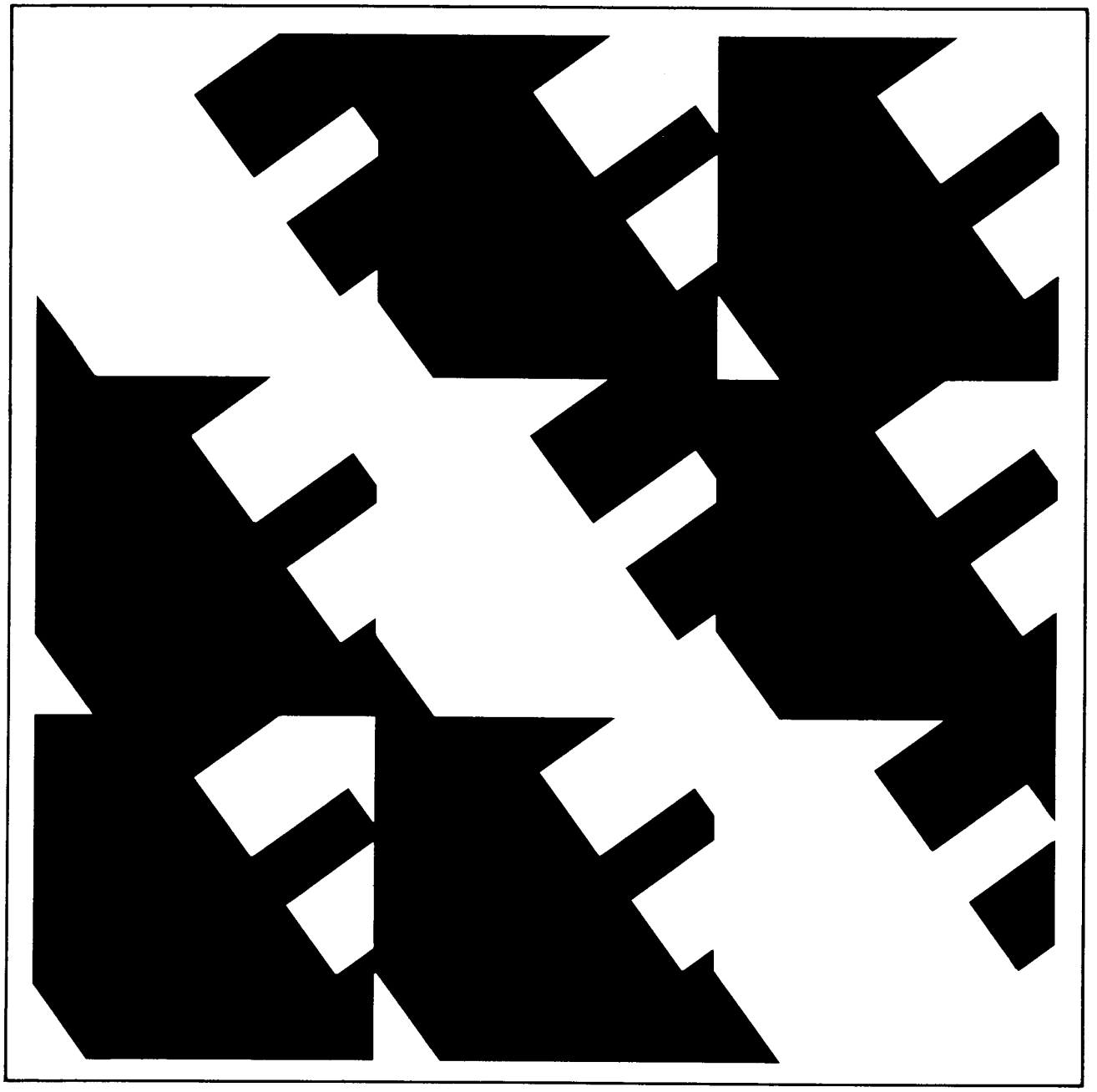
ANSI/IEEE Std 497-1981
(R
AMERICAN NATIONAL STANDARD
Approved January 20, 1983
American National Standards Institute

IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations



IEEE Std 497-1981

Published by The Institute of Electrical and Electronics Engineers, Inc. 345 East 47th Street, New York, New York 10017

March 31, 1981

SH08193

IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations

1. Scope

This standard applies to the design of instrumentation provided for the control room operator to monitor variables required to determine accident conditions within nuclear power generating stations. The criteria apply to accident monitoring instrumentaton required during the period from accident initiation, through the point in time when personnel access is possible to commence activities in parts of the plant that require inspection, repair, or replacement.

Instrumentation addressed by this standard is the minimum necessary for the control room operator to: (1) take the preplanned manual actions to accomplish and maintain safe plant shutdown for design basis accident events; (2) assess the processes of accomplishing and maintaining critical safety functions (that is, reactivity control, core cooling, reactor coolant system integrity, primary reactor containment integrity, and radioactive effluent control); and (3) monitor the extent to which those variables which have the potential for causing a breach of the primary reactor containment have exceeded the design basis values, or that the in-core fuel cladding, the reactor coolant pressure boundary, or the primary containment may have been breached.

The scope of the standard is limited to on-site environmental and process monitoring.

2. Purpose

The purpose of this standard is to provide the minimum design criteria for instrumentation used to meet the accident monitoring requirements of ANSI/ANS-4.5-1980 [1].[1] This standard provides that information required to consolidate existing standards into a cohesive set for application to accident monitoring.

[1]The numbers in brackets correspond to the references listed in Section 4 of this standard.

3. Definitions

The user of this standard should familiarize himself with the terminology defined in ANSI/ANS-4.5-1980 [1].

3.1 Terms defined in ANSI ANS-4.5-1980 [1].

accident
accident phases
controlled condition
critical safety functions
design basis accident events
variable types A, B, and C

NOTE: The term **critical safety function** (defined in ANSI/ANS-4.5-1980 [1]) pertains to a subset of *safety functions.* That subset is distinguished by the words *direct and immediate threat to the health and safety of the public.* This term is used in the definition of type B variables in ANSI/ANS 4.5-1980 [1].

3.2 Other terms used in this document:

components. Discrete items from which a system is assembled.

divisions. The designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

module. Any assembly of interconnected components which constitutes an identifiable device, instrument, or piece of equipment. A module can be disconnected, removed as a unit, and replaced with a spare. It has definable performance characteristics which permit it to be tested as a unit. A module could be a card, a drawout circuit breaker, or other subassembly of a larger device, provided it meets the requirements of this definition.

power sources. The electrical and mechanical equipment and their interconnections necessary to generate or convert power.

redundant equipment or system. A piece of equipment or a system that duplicates the essential function of another piece of equipment

or system to the extent that either may perform the required function regardless of the state of operation or failure of the other.

NOTE: Redundancy can be accomplished by use of identical equipment, equipment diversity, or functional diversity.

safety function. One of the processes or conditions (for example, emergency negative reactivity insertion, post accident heat removal, emergency core cooling, post accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limit established for a Design Basis Event (DBE).

safety system. Those systems (the reactor trip system, and an engineered safety feature, or both, including all their auxiliary supporting features and other auxiliary features) which provide a safety function. A safety system is comprised of more than one safety group of which any one safety group can provide the safety function.

information display channel. An arrangement of electrical and mechanical components or modules, or both, from measured process variable to display device as required to sense and display conditions within the generating stations.

information display channel failure. A situation where the display disagrees, in a substantive manner, (that is, the maximum error within which the information must be conveyed to the operator has been exceeded), with the conditions or status of the plant.

4. References

[1] ANSI/ANS-4.5-1980 Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors[2]

[2] ANSI/IEEE Std 344-1975 (R1980), IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations

[3] ANSI/IEEE Std 379-1977, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E Systems

[4] ANSI/IEEE Std 494-1974, IEEE Standard Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations

[5] ANSI/IEEE Std 577-1976, IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Nuclear Power Generating Stations

[6] IEEE Std 308-1980, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations

[7] IEEE Std 323-1974 (R1980), IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations

[8] IEEE Std 384-1981, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits

[9] IEEE Std 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

[2]ANSI documents are available from The American National Standards Institute, 1430 Broadway, New York, N.Y. 10018.

5. Design Basis

A specific design basis for accident monitoring instrumentation shall be established for each nuclear power generating station. The design basis information thus provided shall be available, as needed, for making judgements on the adequacy of design of the accident monitoring instrumentation.

The design basis shall document, as a minimum, those items which are required by Section 5 of ANSI/ANS-4.5-1980 [1] and the following:

(1) The type A variables provided for manually controlled actions for which no automatic control is provided and which are required for the safety systems to accomplish their safety functions. These manual actions are defined in the safety system design basis in accordance with IEEE Std 603-1980 [9].

(2) The range of transient and steady-state conditions of the power sources (for example: voltage, frequency) for which provisions must be incorporated to ensure adequate performance when required.

(3) The postulated conditions having the potential for functional degradation of accident monitoring instrumentation performance and for which provisions must be incorporated to retain the capability for performing the accident monitoring functions (for example: mis-

siles, pipe breaks, fires, loss of ventilation, spurious operation of fire supression systems, operator error, failure in non-safety-related systems).

(4) For instrumentation to provide the alarming function for type C variables specified by 6.3 of ANSI/ANS-4.5-1980 [1], the alarm limits applicable to each measured variable or combination of variables; the increments allotted for inaccuracies, calibration uncertainties, and errors (increment between alarm limit and setpoint allowable value); and the increments allotted for drift during the interval between calibration verification tests (increment between setpoint allowable value and alarm setpoint).

(5) The range of environmental conditions imposed on the operator during accident conditions throughout which he is expected to observe the accident monitoring displays.

(6) The methods to be used to determine that the reliability of the accident monitoring instrumentation design is appropriate for each accident monitoring function and any qualitative or quantitative reliability goals which may be imposed on the system design.

6. Design Criteria

This section provides design criteria for the minimum set of accident monitoring instrumentation required for type A, B, and C variables as defined in ANSI/ANS-4.5-1980 [1]. Included in the instrumentation provided for type A variables is that required for manually controlled actions for which no automatic control is provided and which is required for the safety systems to accomplish their safety function (see 4.8.1 of IEEE Std 603-1980 [9]). This subset of instrumentation for type A variables is part of the related safety system and is Class 1E. Additional general criteria for information display channels to monitor type A, B, and C variables and design guidance for information display channels used to monitor type B and C variables are given in ANSI/ANS-4.5-1980 [1].

6.1 System Design Criteria

6.1.1 Failure Criteria. The following is an expansion on the single failure criterion of 6.1.7 of ANSI/ANSI 4.5-1980 [1].

The accident monitoring instrumentation shall be capable of providing the information required for the operator to perform his role in bringing the plant to and maintaining it in a safe condition during an accident in the presence of: (1) any single detectable failure within the accident monitoring instrumentation concurrent with all identifiable but nondetectable failures; (2) all failures occurring as a result of the single failure; and (3) all failures and spurious system actions which cause or are caused by the accident requiring the accident monitoring function. Any systems or components which provide services (for example, cooling, illumination, and energy supply) which are required by the accident monitoring instrumentation to perform its function shall be included in the single failure analysis of the accident monitoring instrumentation it supports. ANSI/IEEE Std 379-1977 [3], provides guidance on the application of the single failure criterion.

Where the failure of one of two redundant information display channels could result in information ambiguity (that is, the redundant displays disagree and the operator cannot readily deduce which channel has failed) which could lead the operator to defeat or fail to accomplish a required safety function, additional information shall be provided to allow the operator to deduce the actual conditions so that he may properly perform his role. For example, this may be accomplished by providing the capability, if sufficient time is available, for the operator to perturb the measured variable and determine which channel has failed by observation of the response on each instrumentation channel or by cross checking with an independent channel which monitors a different variable which bears a known relationship to the multiple channels (addition of a diverse channel), or by providing an additional independent channel of instrumentation on the same variable (addition of a replicate channel).

NOTE: Within each redundant division of a safety system, redundant instrumentation display channels are not required.

This failure criterion shall apply as a minimum to that accident monitoring instrumentation provided for type A and B variables. The failure criterion does not apply to that accident monitoring instrumentation provided for type C variables. See 6.1.7 of ANSI/ANS-4.5-1980

[1]. For those systems for which either quantitative or qualitative reliability goals have been established, analysis of the design shall be performed in order to confirm that such goals have been achieved.

Systems required to meet the failure criteria of this section are permitted to violate the single failure criterion during channel maintenance, test or calibration provided that acceptable operation can be otherwise demonstrated. For example, the time interval required for a test, calibration or maintenance operation could be shown to be so short so as to have no significantly detrimental effect on overall availability of the accident monitoring instrumentation system.

The performance of a probabilistic assessment of the accident monitoring instrumentation may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment, in this case, is intended to eliminate consideration of events and failures that are not credible.

A probabilistic assessment may be used in lieu of meeting the single failure criterion for accident monitoring instrumentation for those type A variables not meeting Section 5(1) and for type B variables provided that:

(1) Quantitative reliability goals are established and justified consistent with the role of the instrumentation in accident monitoring and are included in the design bases per Section 5(6)

(2) The techniques used to show compliance with the reliability goals meet the requirements of ANSI/IEEE Std 577-1976 [5], and are included in the design basis per Section 5(6)

(3) Reliability data used in calculations to show compliance with the reliability goals are documented and justified for their applicability.[3]

6.1.2 Integrity. Information displays channels shall meet the performance requirements of the design basis, under the conditions specified, during the time period which the particular information display channel is required. If justified by the design basis, different performance requirements may be applicable to different extremes of conditions.

6.1.3 Rate and Trend Analysis. Where rate of change of a variable or variable trending is essential for accident monitoring, instrumentation shall be provided to display information in sufficient time and over a suitably realistic time base to fulfill the design basis requirements.[4]

6.1.4 Maintenance and Repair. Accident monitoring instrumentation shall be designed to facilitate maintenance, repair, and adjustment. Consideration shall be given to potential inaccessibility during the accident period in determination of equipment selection and location.

6.1.5 Channel Identification. In order to provide assurance that the channel independence requirements of 6.2.5 can be applied during the design, construction, maintenance, and operation of the plant, type A and B accident monitoring instrumentation shall be identified distinctively. In the installed equipment, components and modules mounted in assemblies that are clearly identified as to channel within the accident monitoring system do not themselves require identification. In the association of information display channels with safety system channels common identification may be used.

In addition, accident monitoring instrumentation for type A and B variables shall meet the following requirements:

(1) The instrumentation shall be distinctly identified for each redundant section of the accident monitoring instrumentation in accordance with the requirements of IEEE Std 384-1981 [8]

(2) Identification of accident monitoring instrumentation shall be distinguishable from any identifying markings placed on equipment for other purposes (for example, identification

[3]ANSI/IEEE Std 352-1975 (Appendix A) discusses reliability data sources and ANSI/IEEE Std 500-1977 (Appendix A) defines reliability data collection and display system requirements and presents, as an appendix, an acceptable set of failure rate data for instrumentation, electronic, and electrical equipment.

[4]Continuous recording, for example, strip chart, may be desirable where general trend information is required by the operator. Recording or nonrecording, or both, indication may be desirable where instantaneous rate indication is required. Periodic, nonindicating recording, for example, magnetic tape in conjunction with an on-line computer based information processing system, may be desirable for sampled information which requires calculations to yield significant information.

of fire protection equipment, phase identification of power cables)

(3) Identification of accident monitoring instrumentation and its divisional assignment shall not require frequent use of reference material

(4) The associated documentation shall be distinctly identified in accordance with the requirements of ANSI/IEEE Std 494-1974 [4]

(5) Instrumentation for those type A variables identified in accordance with Section 5(1) must be identified as part of the applicable safety system

Refer to 6.3.2 for identification requirements for accident monitoring displays.

6.1.6 Auxiliary Features

6.1.6.1. Systems or components which provide services which are required for the accident monitoring instrumentation to accomplish its functions shall be considered part of the accident monitoring instrumentation and shall meet all applicable requirements of this standard. Auxiliary features for accident monitoring instrumentation provided for those type A variables identified in accordance with Section 5(1) are part of the related safety system and must meet applicable requirements.

NOTE: An example of a component providing required service for accident monitoring instrumentation is a cabinet cooling fan required to maintain signal conditioning modules within design range temperature.

6.1.6.2. Other components, equipment, and systems that (1) perform a function that is not required for the accident monitoring instrumentation to provide required information to the operator, and (2) are part of the accident monitoring instrumentation by association (that is, not isolated from the accident monitoring instrumentation) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the accident monitoring instrumentation below an acceptable level as specified by the design basis.

6.1.7 Power Source(s). The accident monitoring instrumentation power source(s) shall be capable of providing adequate service to the accident monitoring instrumentation for the fulfillment of the signal interruptability criteria set forth in ANSI/ANS-4.5-1980 [1], Table 6.1-1, coincident with loss of off-site power.

The power source(s) used to power the accident monitoring instrumentation is a supporting system for the accident monitoring instrumentation for which design criteria are given in 6.1.6.

Class 1E power sources shall be used for instrumentation to monitor those type A variables identified in accordance with Section 5(1).

NOTE: *Electric Power Sources.* Where Class 1E Power Sources are used refer to IEEE Std 308-1980 [6] for the requirements that apply.

6.1.8 Equipment Qualification. Accident monitoring equipment shall be qualified in accordance with IEEE Std 323-1974 (R1980) [7] to meet the requirements of 6.1.1, 6.1.2, and 6.3.6 of ANSI/ANS-4.5-1980 [1]. The seismic qualification specified by 6.1.1, ANSI/ANS-4.5-1980 [1], shall be in accordance with ANSI/IEEE Std 344-1975 [2].

6.1.9 Control of Access. The design shall permit the administrative control of access to information display channel calibration adjustments, test points, and controls used to remove a display channel from service. These administrative controls shall be supported by provisions within the accident monitoring instrumentation system, by provisions in the generating station design; or by a combination thereof.

6.2 Information Display Channel Design Criteria

6.2.1 Quality of Components and Modules. Accident monitoring instrumentation shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Information display channel equipment for type A and B variables shall be designed, manufactured, inspected, installed, operated, and maintained in accordance with an acceptable quality assurance program.[5] The level of Quality Assurance to be applied to display channel equipment for type C variables shall be selected by the designer to assure that the specified performance requirements are met.[6]

6.2.2 Interaction Between Information Display Channels and Other Systems

6.2.2.1 Classification of Equipment. Information display channels that are used for

[5] See ANSI NQA-1-1979 (Appendix A).

[6] Refer to Table 6.1-1 of ANSI/ANS-4.5-1980 [1].

both accident monitoring display and for other operations and which are not part of a safety system shall be classified as accident monitoring equipment, and shall meet, as a minimum, the requirements of this standard.

6.2.2.2 Isolation. The transmission of signals between accident monitoring equipment and any system not meet the minimum design requirements stated herein shall be through isolation devices which shall be classified as part of the accident monitoring equipment and shall meet all the requirements of this standard. No credible failure external to the accident monitoring instrumentation shall be transmitted through the isolation device in such a way as to prevent the accident monitoring channel from meeting the performance requirements specified in the design basis. A failure of an isolation device is evaluated in the same manner as a failure of other equipment in the accident monitoring instrumentation. Isolation devices shall meet the requirements of IEEE Std 384-1981 [8].

6.2.3 Capability for Test and Calibration. Information display channels shall have the capability for testing and calibration on a periodic basis to verify availability and performance capabilities to the extent necessary to meet the system availability goals. The periodic test and calibration shall follow a predetermined method and results shall be documented.

6.2.3.1 Channel Availability Test. Capability shall be provided for testing the operational availability of each information display channel during plant operation. This may be accomplished in various ways, for example:

(1) By observing the effect of perturbing the monitored variable

(2) By observing the effect of introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable

(3) By cross-checking between channels that bear a known relationship to each other

6.2.3.2 Calibration. Capability shall be provided for calibration of each information display channel during normal plant power or shutdown operation or both as determined by the required interval between calibrations.

During the accident period, means shall be provided for validating the required information. This may be accomplished in various ways. For example:

(1) Recalibration

(2) Specifying a calibration interval to ensure that the period during which the channel is needed will fall within the equipment's qualified calibration interval

(3) Selection of equipment that does not require periodic calibration

(4) Cross-calibration with other channels that bear a known relationship to the information display channel

6.2.3.3 Test Methods. A specific test method shall be developed to include the following:

(1) A procedure to check display channel performance, accuracy, and where required, response time

(2) Minimum acceptance tolerances beyond which calibration or repair must be done

(3) A test interval which establishes the time between tests. The test interval shall consider equipment specifications, scheduled plant operating cycles, system design basis test interval, and historical experience

(4) A method of documentation of the testing or calibration in an orderly manner to facilitate maintaining historical records of equipment which are part of an information display channel

6.2.4 Instrumentation Characteristics. The performance characteristics of the information display channel for type A and B variables (for example, range, accuracy, and response time) shall be selected to allow for the uncertainties in the analysis and errors in the instrumentation itself (for example: temperature and voltage effects drift). Section 6.3 of ANSI/ANS-4.5-1980 [1] recommends certain allowances (termed *margin*) for instrument ranges for type C variables.

6.2.5 Channel Independence. The information display channels for type A and B variables shall be independent and physically separated in accordance with the following criteria:

(1) Redundant sections shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the accident monitoring function during and following any design basis accident event requiring that function

(2) Accident monitoring equipment required to monitor a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event to the de-

gree necessary to retain the capability to meet the requirements of this standard

(3) Instrumentation provided for type A and B variable shall be physically separated from non-safety system equipment and circuits to the degree necessary to assure that a failure in, or spurious action by, such equipment will not prevent the accident monitoring equipment from meeting the requirements of this standard, and

(4) Instrumentation provided for those type A variables identified in accordance with Section 5(1) shall meet the requirements of IEEE Std 384-1981 [8].

These requirements do not preclude the association of these information display channels with safety system channels, provided this association does not compromise the ability of the safety system channel to meet the requirements of IEEE Std 603-1980 or the ability of the information display channel to meet the requirements of this standard.

6.2.6 Derivation of Information Display Channels. To the extent feasible and practical, information display channels shall directly measure the desired variable. (See 6.1.3 of ANSI/ANS-4.5-1980 [1]).

6.3 Display Requirements

6.3.1 Sharing Displays. The same displays may be used for accident monitoring as are used for the normal operations of the plant provided that these displays meet accident monitoring requirements.

6.3.2 Display Location and Identification. In addition to the criteria of 6.1.6 of ANSI/ANS-4.5-1980 [1], permanently installed type A accident monitoring displays which enable the operator to determine when conditions exist that require specified manual actions, or to monitor the results of those actions, shall be located in the vicinity of the control stations used to effect the actions.

6.3.3 Alarms for Type C Variables. The alarms provided for type C variables to meet the requirements of 6.3.2.1, 6.3.3.1, and 6.3.4.1 of ANSI/ANS-4.5-1980 [1] are part of the accident monitoring instrumentation and shall meet the requirements for instrumentation provided for type C variables.

6.3.4 Indication of Bypasses. If the information display channel for those type A variables listed in accordance with Section 5(1) have been bypassed, or deliberately rendered inoperative, for any purpose, continued indication of this fact for each affected safety group shall be provided in the control room.

6.3.4.1. This display instrumentation need not be part of the safety systems.

6.3.4.2. This indication shall be automatically actuated if the bypass or inoperative condition is: (1) expected to occur more frequently than once a year, and (2) expected to occur when the affected system is required to be operable.

6.3.4.3. The capability shall exist in the control room to manually activate this display indication.

6.4 Installation. In addition to the criteria of 6.1.5 of ANSI/ANS-4.5-1980 [1] portable instrumentation used for accident monitoring shall meet the following:

6.4.1. Portable instrumentation used for accident monitoring shall meet the requirements of this standard with the exception of 6.1.1, 6.1.5, 6.1.8, 6.2.5, and 6.3.2.

6.4.2. The design and application of portable instrumentation as part of the accident monitoring instrumentation shall not compromise redundant, permanent instrumentation through process, power supply, or display interconnection.

6.4.3. Where portable instrumentation is to be used, the design shall provide for the administrative control of storage and access to ensure compliance with the criteria necessary to meet the performance requirements of the design basis.

Appendix A

Bibliography

ANSI NQA-1, 1979, Quality Assurance Program Requirements for Nuclear Power Plants

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

ANSI/IEEE Std 500-1977, IEEE Guide to the Collection and Presentation of Electrical, Electronic, and Sensing Component Reliability Data for Nuclear Power Generating Stations