IEEE Std 497™-2002
(Revision of IEEE Std 497-1981)

IEEE Standards

497™

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

IEEE Power Engineering Society

Sponsored by the
Nuclear Power Engineering Committee

IEEE

Published by
The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

30 September 2002

Print: SH94992
PDF: SS94992

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

IEEE Std 497™-2002
(Revision of IEEE Std 497-1981)

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

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society

Approved 13 May 2002

IEEE-SA Standards Board

Abstract: Criteria for variable selection, performance, design, and qualification of accident monitoring instrumentation are established in this standard. Included requirements for display alternatives for accident monitoring instrumentation, documentation of design bases, and use of portable instrumentation.
Keywords: accident monitoring, display criteria, selection criteria, type variables

---

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2002 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 30 September 2002. Printed in the United States of America.

Print: ISBN 0-7381-3277-2 SH94992
PDF: ISBN 0-7381-3280-2 SS94992

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

(This introduction is not part of IEEE Std 497-2002, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, but is included for information purposes only.)

In the aftermath of an incident at a United States nuclear power plant in March of 1979, a more rigorous approach to developing an accident monitoring system occurred in the United States. This approach culminated in three major sources of requirements for such a system namely:

— ANSI/ANS Std 4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors (provided selection and performance criteria)
— IEEE Std 497-1981, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations (provided design criteria)
— Regulatory Guide (RG) 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Rev 3, May 1983 (prescribed a detailed list of variables to monitor and specified a comprehensive list of design and qualification requirements to be met)

The prescriptive and regulatory-driven nature of RG 1.97 resulted in its becoming the de facto standard for accident monitoring. Although containing many useful approaches and guidance for designing an accident monitoring system, both IEEE Std 497-1981 and ANSI/ANS Std 4.5-1980 became little used and were eventually withdrawn as active standards.

More recently, a need for developing a more flexible consolidated standard arose. The impetus for this need was the desire for increased use of microprocessor based instrumentation systems in both old and the next generation of advanced design nuclear power plants. A need also developed for additional flexibility while modifying past designs and addressing design basis issues. In response to this need, in November of 2000 the Nuclear Power Engineering Committee of IEEE's Power Engineering Society directed its Working Group 6.1 to prepare a new revision of IEEE Std 497-1981.

The new revision was to provide a consolidated source of post-accident monitoring requirements and bases for a new generation of advanced nuclear plant designs. This revision was to also contain guidance and allow a flexible basis for making changes to such systems in older plants. In essence, the revision was to integrate and incorporate applicable requirements from IEEE Std 497-1981, ANSI/ANS Std 4.5-1980, and RG 1.97, as well as to consider state-of-the-art digital design techniques for accident monitoring displays and user feedback from review and use of these three source documents.

Based on this direction, the working group elected to develop an approach to accident monitoring that is both simpler and less prescriptive in nature. That is, instead of providing a list of instrument variables to monitor, the intention would be to provide criteria for how the variables would be selected. Also, instead of up to three possible design and qualification category requirements for each variable type, the intent was to standardize the requirements based on level of importance of the variable type. The result of this effort is IEEE Std 497-2002.

A valuable aspect of this current revision is the criteria provided for advanced instrumentation system designs and design modifications based on modern digital technology. With current technology there are many possibilities for accident monitoring channel configurations that acceptably meet the criteria of this standard. Figure 2 of this standard identifies options from analog signal channels to various combinations of digital signal processing, data validation processing and display afforded by, but not limited to, today's technology. The definitions associated with Figure 1 of this standard are helpful in understanding the options shown in Figure 2. It was also the working group's intention to address the control room displays of information using computer generated displays and calculated values. The criteria presented in this standard provide useful guidance in this area without limiting the types of displays that can be made available to the control room operator.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Std 497-2002 is arranged to provide six types of accident monitoring criteria as follows:

— How to select and categorize variables. (Clause 4)

— What performance requirements must be met. (Clause 5)

— What design features need to be considered. (Clause 6)

— What aspects of seismic and environmental qualification must be met for each variable type. (Clause 7)

— What display requirements to assure control room operators are properly informed. (Clause 8)

— What quality assurance requirements should apply. (Clause 9).

In addition, an informative annex providing guidance on establishing instrument accuracy requirements has been included.

The following discussion provides guidance and clarification on the use of this standard in the areas of variable selection, establishing design requirements in a simplified way based on level of importance, and qualification clarifications based on function and need.

The selection criteria in this standard allow the defining of five variable types similar to RG 1.97. Type A is accident specific and needed for preplanned operator action, Type B and Type C allow a supervisory overview approach to accident monitoring by allowing a review of critical high level safety functions, Type C additionally allows extended range monitoring of defense-in-depth variables. Type D and Type E allow monitoring of performance of appropriate safety and radiation monitoring systems. The selection criteria, if properly imposed, would result in a list of variables similar to that required by RG 1.97. However, other approaches to implementation of the criteria allow the possibility of other equally acceptable variations. Thus an optimum combination of accident monitoring variables is now more likely and can be defended.

Accident monitoring variable selection must be consistent with the plant specific emergency operating procedures (EOPs) and abnormal operating procedures (AOPs). The variables selected from these procedures need to be the minimum set to assess that safety-related functions are performed and safety systems operate acceptably. It is not intended that the standard apply to instrumentation for contingency actions listed in the EOPs. Also, instrumentation for shutdown from outside the main control room (i.e., remote shutdown) is outside the scope of this standard.

The EOPs derive from Emergency Procedure Guidelines (EPGs), which are developed by the Nuclear Steam Supply System (NSSS) Vendor Owners' Group. For example, such EPGs include functional restoration EPGs or Plant Critical Safety Function Status Trees (depending on which NSSS vendor) for technical emergency procedure input. The working group attempted to use terminology from multiple NSSS vendors for improved universality in this standard.

Accident monitoring instrumentation monitors a large number of variables with a wide variation in the level of importance to the operators. Because of this variation, it would not be reasonable to require that all of the instruments be designed and qualified for all aspects of Class 1E equipment, nor to exclude all instruments from all requirements. Recognizing the potential value to the user, the working group has established the design, display, qualification, and quality requirements for accident monitoring instrumentation in a manner that is consistent with the level of importance of the variables that are being monitored.

The design, display, qualification, and quality criteria of this standard differ from the approach detailed in RG 1.97, which specifies design and qualification requirements for each variable in terms of one of three possible design and qualification categories, that is, Categories 1, 2 and 3. In developing this revision, the working group adopted a philosophy where the qualification requirements for all variables within a type group are either: completely consistent within the group or; consistent with the individual variable's assigned accident monitoring function. This philosophy results in all Type B and Type C variable instruments having the same design, display, qualification, and quality requirements. Type B and Type C

Copyright © 2002 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

variables do not have any accident specific functions, but instead have the same function for all accidents. For variables categorized as Type A, Type D, or Type E, the design requirements are consistent within each respective group. The qualification (environmental and seismic) requirements applicable to a variable are based on individual variable functional needs and postulated accident conditions at the installed location. Note: Reviews performed by the Working Group confirm that this more simplistic approach (eliminating the need for three design and qualification categories separate from the five variable type groups) results in no new design and qualification requirements above that in place at nuclear plants, which presently comply in an acceptable manner with RG 1.97.

The working group also considered and adopted “lessons learned” from established equipment qualification programs. For example, this standard recognizes that equipment used for accident monitoring may have different qualification requirements based on the time duration relied upon during the accident, the environmental effects present during the postulated accident or the need for that instrument for a particular accident. To illustrate this philosophy, three examples are offered:

Example 1: The plant safety analysis identifies that a Type A variable is required to initiate a specific planned manually-controlled action to support a safety-related function for only one specific accident in which no post-accident harsh environment exists. The instrumentation does not have a Type A function for other accidents that produce a harsh environment at the instrument location. The instrumentation for this variable does not require environmental qualification to a harsh environment by the criteria of this standard. However, those Type A variables that are needed to terminate or mitigate an accident producing a harsh environment shall be environmentally qualified for the worst case applicable accident environment.

Example 2: High Pressure Coolant Injection (HPCI) system flow rate is a Type D variable used by boiling water reactory (BWR) plant control room operators to indicate and assess the operation of the HPCI system after an accident. The HPCI flow sensor is located in the same room as the HPCI pump, the pump’s steam turbine prime mover, and the associated supply steam piping. The room also contains temperature sensors for steam leak detection. If for illustration purposes, it is assumed that the only source of steam flooding in the room is a pipe break that disables the HPCI pump steam turbine, then it is not necessary to environmentally qualify the HPCI flow sensor instrumentation located in that room for that pipe break steam environment. This conclusion is arrived at by observing that the HPCI system is not required to operate during this accident scenario (because it is disabled) and, as a result, there is no performance to assess. Additionally, the room’s leak detection system provides information on the system’s availability and status.

Example 3: A Type E radiation monitor is mounted on a non-seismically designed plant effluent vent. This vent path can be isolated further upstream by a seismically designed and constructed damper and the position of this damper is indicated in the control room. The requirements of this standard may not require that this Type E variable instrumentation be seismically qualified.

In conclusion, although written primarily for new plant designs, existing plants may also find useful guidance and applicable criteria in this standard. The use of applicable plant procedures to determine the requirements of the accident monitoring instrumentation provides the necessary flexibility for useful design criteria. This standard can be used to address the necessary changes to the plant configuration that inevitably occur over the operating life of any plant. This standard also offers some advantages in clarifying when environmental and seismic qualification would be required and establishing design criteria for digital equipment upgrades involving accident monitoring instrument channels.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Future Work

As the use of computers in the nuclear plant is a dynamic area of design, the working group intends to keep this area as one of its ongoing future tasks.

The treatment of accident monitoring instrumentation for severe accidents should be incorporated into this standard in the future. It is the working group's philosophy that sufficient instrumentation should exist to inform operators of the status of the three fission product barriers at all times. Instrumentation needed to monitor plant conditions during a severe accident must perform its function for the time period needed in the best-estimate (using realistic assumptions) environmental conditions of the severe accident (e.g., pressure, temperature, humidity, radiation) for which the instrument is relied upon to function.

Another area that the group believes should be incorporated into the standard in the future is the instrumentation that is used for determining plant emergency classification levels (such as notification of unusual event, alert, site area emergency, and general emergency).

--`,,`-`-`,,`,,`,`,,`---
Copyright © 2002 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Participants

This standard was prepared by Subcommittee 6 Working Group 6.1 (Post Accident Monitoring) of the Nuclear Power Engineering Committee of IEEE's Power Engineering Society. At the time this standard was balloted, Working Group 6.1 had the following membership:

Glenn E. Lang, *Chair*

Daryl L. Harmon
David A. Horvath
Joseph P. Joyce
Peter M. Kelly
Barry S. Marcus
Ifti Rana

At the time this standard was prepared, Subcommittee 6 (Safety Related Systems) under the Nuclear Power Engineering Committee had the following membership:

Paul L. Yanosy, *Chair*
David A. Horvath, *Secretary*

Wesley W. Bowers
Robert Copyak
John J. Disosway
Britton P. Grim
Randy C. Jamison
James T. Keiper
Tom Klein
Glenn E. Lang
Evangelos C. Marinos
Mike H. Miller
Charles C. Roslund
John B. Waclo
David J. Zaprazny

At the time this guide was balloted, the Nuclear Power Engineering Committee had the following membership:

Neal P. Smith, *Chair*
John P. Carter, *Vice Chair*
John J. Disosway, *Secretary*

Satish K. Aggarwal
George Attarian
Farouk D. Baxter
Vincent P. Bacanskas
Brij M. Bharteey
Wesley W. Bowers
Daniel F. Brosnan
Salvatore P. Carfagno
Robert C. Carruth
Robert Copyak
Pat Duggan
Surin K. Dureja
Joseph K. Fragola
Wilmer C. Gangloff
Britton P. Grim
Robert E. Hall
Gregory K. Henry
David A. Horvath
Paul R. Johnson
Sonny Kasturi
James T. Keiper
John MacDonald
Scott Malcolm
Alexander Marion
Wolfgang W. Michel
Gerald L. Nicely
Roger D. Parker
Barry Skoras
James E. Stoner
Peter Szabados
James E. Thomas
Gary J. Toman
T. J. Voss
John B. Waclo
Raymond Weronick
Paul L. Yanosy
David J. Zaprazny

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Satish K. Aggarwal
Vincent P. Bacanskas
Farouk D. Baxter
Wesley W. Bowers
Daniel F. Brosnan
John P. Carter
Robert Copyak
Guru Dutt Dhingra
Randall Groves
Gregory K. Henry
Paul R. Johnson
John MacDonald
Scott Malcom
Gary Michel
James Ruggieri
James E. Thomas
David J. Zaprazny

When the IEEE-SA Standards Board approved this standard on 13 May 2002, it had the following membership:

James T. Carlo, *Chair*
James H. Gurney, *Vice Chair*
Judith Gorman, *Secretary*

Sid Bennett
H. Stephen Berger
Clyde R. Camp
Richard DeBlasio
Harold E. Epstein
Julian Forster*
Howard M. Frazier
Toshio Fukuda
Arnold M. Greenspan
Raymond Hapeman
Donald M. Heirman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Peter H. Lips
Nader Mehravari
Daleep C. Mohla
William J. Moylan
Malcolm V. Thaden
Geoffrey O. Thompson
Howard L. Wolfman
Don Wright

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Alan Cookson, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Michelle Turner
IEEE Standards Associate Project Editor

Copyright © 2002 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

1. Overview 1

1.1 Scope 1
1.2 Purpose 1
1.3 Application 1

2. References 2

3. Definitions 2

4. Selection criteria 5

4.1 Type A variables 5
4.2 Type B variables 5
4.3 Type C variables 6
4.4 Type D variables 6
4.5 Type E variables 6
4.6 Documentation of selection bases 6

5. Performance criteria 8

5.1 Range 8
5.2 Accuracy 8
5.3 Response time 8
5.4 Required instrumentation duration 9
5.5 Reliability 9
5.6 Performance assessment documentation 9

6. Design criteria 9

6.1 Single failure 9
6.2 Common cause failure 10
6.3 Independence and separation 11
6.4 Isolation 11
6.5 Information ambiguity 11
6.6 Power supply 12
6.7 Calibration 12
6.8 Testability 12
6.9 Direct measurement 13
6.10 Control of access 13
6.11 Maintenance and repair 13
6.12 Minimizing measurements 13
6.13 Auxiliary supporting features 13
6.14 Portable instruments 13
6.15 Documentation of design criteria 13

7. Qualification criteria 14

7.1 Type A variables 14
7.2 Type B variables 14
7.3 Type C variables 14

--`,,`-`-`,,`,,`,`,,`---

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS

Not for Resale

7.4 Type D variables 14
7.5 Type E variables 15
7.6 Portable instruments 15
7.7 Post event operating time 15
7.8 Documentation of qualification criteria 15

8. Display criteria 15

8.1 Display characteristics 15
8.2 Trend or rate information 17
8.3 Display identification 17
8.4 Type of monitoring channel display 17
8.5 Display location 17
8.6 Information ambiguity 17
8.7 Recording 17
8.8 Digital display signal validation 17
8.9 Display criteria documentation 17

9. Quality assurance 18

Annex A (informative) Accident monitoring instrument channel accuracy 19

Annex B (informative) Bibliography 20

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

1. Overview

1.1 Scope

The criteria contain the functional and design requirements for accident monitoring instrumentation for nuclear power generating stations. This standard is intended for new plant designs. The guidance provided in this standard may also prove useful for operating nuclear power stations desiring to perform design modifications or design basis evaluations.

This standard contains guidance for the selection of variables and establishes design and performance requirements. Guidance on the use of portable instrumentation and defining various display alternatives for accident monitoring instrumentation is also included.

1.2 Purpose

The purpose of IEEE Std 497™-2002 is to direct the user in selecting and categorizing post accident monitoring variables; establishing design requirements; and establishing performance requirements. It provides guidance on the use of portable instrumentation and various display alternatives for accident monitoring instrumentation.

1.3 Application

This standard applies to accident monitoring instrumentation intended for use during the following control room operations:

a) As required for preplanned operator action related to accident mitigation
b) For assessing plant conditions, safety system performance and making decisions related to plant response to abnormal events
c) For achieving and maintaining safe shutdown following an accident

This standard does not apply to accident monitoring instrumentation that is intended solely for historical recording or solely for maintenance purposes. This standard also does not apply to instrumentation used to support contingency actions in emergency operating procedures or to instrumentation required to support plant shutdown from outside the control room.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

2. References

This standard shall be used in conjunction with the following publications. When the following standards are superceded by an approved revision, the revision shall apply.

ASME NQA-1-2001, Quality Assurance Requirements for Nuclear Facility Applications.[1]

IEEE Std 7-4.3.2™-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations. [2, 3]

IEEE Std 308™-2001, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.

IEEE Std 323™-1983 (R1996), IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 344™-1987 (R1993), IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

IEEE Std 352™-1987 (R1999), IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Stations.

IEEE Std 379™-2000, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

IEEE Std 384™-1992 (R1998), IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits.

IEEE Std 577™-1976 (R2001), IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations.

IEEE Std 603™-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

IEEE Std 1023™-1988, IEEE Guide for Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.

3. Definitions

The following definitions apply specifically to this standard. For other definitions, see *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition [B4].[4]

3.1 accident analysis licensing basis: The portions of the licensing basis documentation that describe the design basis events (including anticipated operational occurrences), the thermal-hydraulic response of the plant, and the subsequent response of the safety systems.

[1]ASME publications are available from the American Society of Mechanical Engineers, 22 Law Drive, Fairfield, NJ 07007, USA.

[2]The IEEE standards or products referred to in Clause 2 are trademarks owned by the Institute of Electrical and Electronics Engineers, Incorporated.

[3]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

[4]The numbers in brackets correspond to those in the bibliography in Annex A.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

3.2 accuracy: A measure of the degree by which the actual output of a device approximates the output of an ideal device nominally performing the same function.

3.3 anticipated operational occurrence (AOO): Those conditions of normal operations that are expected to occur one or more times during the life of the nuclear power unit and include, but are not limited to, loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power (see Title 10 CFR, Part 50 [B10]).

3.4 auxiliary supporting features: Systems or components that provide services (such as cooling, lubrication, and energy supply) required for the safety systems to accomplish their safety functions.

3.5 common cause failure: Multiple failures of structures, systems, or components as a result of a single phenomenon.

3.6 contingency actions: Alternative actions taken to address unexpected responses of the plant or conditions beyond its licensing basis (for example, actions taken for multiple equipment failures).

3.7 critical safety functions: Those safety functions that are essential to prevent a direct and immediate threat to the health and safety of the public. These are accomplishing or maintaining of:

- Reactivity control
- Reactor core cooling
- Reactor coolant system integrity
- Primary reactor containment integrity
- Radioactive effluent control

3.8 current value: That magnitude of a variable that is associated with the present time and is available for display within the response time limits of an information display channel.

3.9 design basis event (DBE): Postulated events specified by the safety analysis for the station to establish the acceptable performance requirements of the structures and systems.

3.10 display channel: An arrangement of electrical and mechanical components or modules, or both, from the measured process variable to the display device as required to sense, process, and display conditions within the generating station (see Figure 1).

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

3.12 display segment: The electrical components or modules in an information display channel that receive the processing electronics output and process the signal for input to the applicable display device. The display segment may include data validation algorithms, storage of digital display graphics, and analog or digital display devices (see Figure 1).

3.13 electrical power source: The electrical and mechanical equipment and their interconnections necessary to generate or convert power. Specific criteria unique to the Class 1E power system are given in IEEE Std 308-1991.[5]

3.14 execute features: The electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and

[5]Information on references can be found in Clause 2.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

command features. The scope of the execute features extend from the sense and command features output to and including the actuated equipment-to-process coupling.

3.15 licensing basis documentation (LBD): The set of U.S. Nuclear Regulatory Commission (NRC) requirements applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant specific licensing basis (including all modifications and additions to such commitments over the life of the license) that are documented and in effect (see Title 10 CFR, Part 54 [B11]).

The LBD consists of:

— The latest version of the Final Safety Analysis Report (FSAR), the Updated Safety Analysis Report (USAR), or the Standard Safety Analysis Report (SSAR)
— NRC Safety Evaluation Reports
— Operating License, Final Design Certification, including the Technical Specifications, and
— Correspondence between the NRC and the licensee that contains licensing requirements or commitments for the design or operation of the nuclear power plant or standard plant design.

3.16 precision: The degree of mutual agreement between individual measurements, namely repeatability and reproducibility.

3.17 processing segment: The electrical components or modules in an information display channel that receive the sensing segment outputs and perform various conversions and compensation on the sensed signal. The processing electronics may include sensor power supply, analog-to-digital (A/D) conversion, signal compensation, electrical to engineering unit conversion, digital-to-analog (D/A) conversion, and electrical isolation devices for signal interfacing between safety systems and other systems (see Figure 1).

3.18 rate: The first time derivative of the current value.

3.19 response time: The time required for the output to reach 90 percent of the final output value in response to a step input.

3.20 safety-related function: A function that is relied upon during or 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, and (the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to Title 10 CFR Part 100 guidelines [B9]).

3.21 safety system: A system 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, or the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to Title 10 CFR Part 100 guidelines [B9].

3.22 sense and command feature: The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions. The scope of the sense and command features extends from the measured process variables to the execute features input terminals.

3.23 sensing segment: The electrical and mechanical components or modules in an information display channel from measured process variable to the input of the processing electronics (see Figure 1).

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

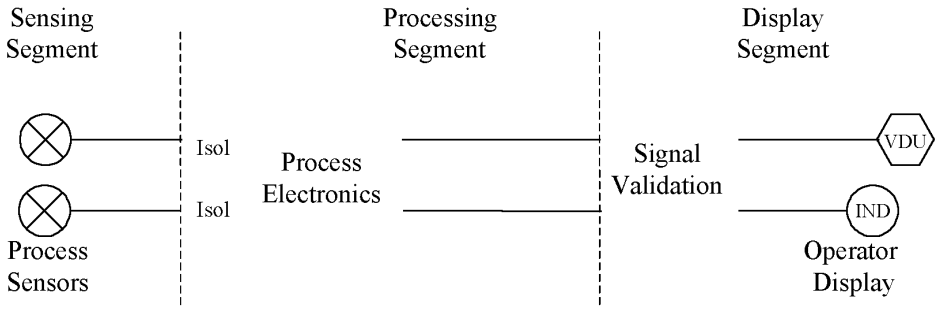


Figure 1—Display channel

3.24 trend: The general tendency of the current value (i.e., increasing, constant, or decreasing).

4. Selection criteria

This clause provides criteria for identifying the plant specific variables for accident monitoring. The variable types will be referred to as A, B, C, D, and E. Criteria for the selection of each type of variable are given below and summarized in Table 1.

4.1 Type A variables

Type A variables are those variables that provide the primary information required to permit the control room operating staff to:

a) Take specific planned manually-controlled actions for which no automatic control is provided and that are required for safety systems to perform their safety-related functions as assumed in the plant Accident Analysis Licensing Basis.
b) Take specific planned manually-controlled actions for which no automatic control is provided and that are required to mitigate the consequences of an AOO.

Type A variables provide information essential for the direct accomplishment of specific safety-related functions that require manual action. These variables are a subset of those necessary to implement the plant specific emergency procedure guidelines (EPGs) or the plant specific emergency operating procedures (EOPs) or the plant abnormal operating procedures (AOPs). Type A variables do not include those variables that are associated with contingency actions that may also be identified in written procedures.

4.2 Type B variables

Type B variables are those variables that provide primary information to the control room operators to assess the plant critical safety functions.

Any plant critical safety functions addressed in the EPGs or the plant specific EOPs that are in addition to those identified above shall also be included.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

The Type B variables shall be those necessary to implement the plant functional restoration EPGs, plant specific EOPs, and the plant critical safety function status trees, if applicable.

4.3 Type C variables

Type C variables are those variables that provide primary information to the control room operators to indicate the potential for breach or the actual breach of the three fission product barriers (extended range): fuel cladding, reactor coolant system pressure boundary, and containment pressure boundary.

The selection of these variables represents a minimum set of plant variables that provide the most direct indication of the integrity of the three fission product barriers and provide the capability for monitoring beyond the normal operating range.

4.4 Type D variables

Type D variables are those variables that are required in procedures and LBD to:

a) Indicate the performance of those safety systems and auxiliary supporting features necessary for the mitigation of design basis events.
b) Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition.
c) Verify safety system status.

The Type D variables shall be based upon the Plant Accident Analysis Licensing Basis and those necessary to implement the following procedures (as applicable to the plant design):

a) Event specific EPGs or plant specific EOPs
b) Functional restoration EPGs or plant specific EOPs
c) Plant AOPs

4.5 Type E variables

Type E variables are those variables required for use in determining the magnitude of the release of radioactive materials and continually assessing such releases.

The selection of these variables shall include, but not be limited to, the following:

a) Monitor the magnitude of releases of radioactive materials through identified pathways (e.g., secondary safety valves, and condenser air ejector).
b) Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature).
c) Monitor radiation levels and radioactivity in the plant environs.
d) Monitor radiation levels and radioactivity in the control room and selected plant areas where access may be required for plant recovery.

4.6 Documentation of selection bases

Documentation shall be developed and maintained for the selection bases of the accident monitoring variables consistent with the plant LBD.

--`,,`-`-`,,`,,`,`,,`---
Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 1—Summary of accident monitoring variable types/source documents

Referenced clause in standard	Selection criteria for the variable type	source Documents
4.1	Type A — Planned manually controlled actions for accomplishment of safety-related functions for which there is no automatic control.	— Plant Accident Analysis Licensing Basis — EPGs or plant specific EOPs — Plant AOPs
4.2	Type B — Assess the process of accomplishing or maintaining plant critical safety functions.	— Functional restoration EPGs or plant specific — Plant critical safety functions related EOPs — Plant critical safety function status trees
4.3	Type C — Indicate potential for a breach of fission product barriers — Indicate an actual breach of fission product barriers	— Plant Accident Analysis Licensing Basis — Design basis documentation for the fission product barriers — EPGs or plant specific EOPs
4.4	Type D — Indicate performance of safety systems — Indicate the performance of required auxiliary support features — Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition — Verify safety system status	— Plant Accident Analysis Licensing Basis — Event specific EPGs or plant specific EOPs — Functional restoration EPGs or plant specific EOPs — Plant AOPs

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 1—Summary of accident monitoring variable types/source documents *(continued)*

Referenced clause in standard	Selection criteria for the variable type	source Documents
4.5	Type E — Monitor the magnitude of releases of radioactive materials through identified pathways — Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways — Monitor radiation levels and radioactivity in the plant environs — Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery	— Procedures for determining radiological releases through plant identified pathways — Procedures for determining plant environs radiological concentration — Procedures for determining plant habitability

5. Performance criteria

5.1 Range

The range of a monitoring channel shall be established to ensure that it covers the transients identified in the plant LBD.

The range for Type C variables shall encompass, with margin, those limits that would indicate a breach in a fission product barrier. For example, measurement of reactor pressure shall include the capability of measuring, with margin, up to Level D service limits of the reactor vessel (see American National Standard Boiler and Pressure Vessel Code [B1]).

5.2 Accuracy

The required accuracy of accident monitoring instrument channels shall be established based on the assigned function. See Annex A for useful guidance.

5.3 Response time

Accident monitoring instruments shall be designed to provide real time and timely information. Typically, the displayed information will lag behind actual conditions because of sensor location, thermal heat transfer time lag, information processing cycle times, degree of severity of environmental conditions, and other potential effects on instrument response times.

In general, these response times are not as critical as in the case when the instrument provides a signal for automatic Reactor Protection System or Engineered Safeguard System action.

For computer driven displays, the indicated variable will additionally lag real time conditions depending on the update frequency of the display. The update frequency shall be fast enough to avoid the potential of

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

misleading the operator with respect to plant conditions. It is considered prudent that this update period be approximately one to two seconds.

5.4 Required instrumentation duration

The post event operating time for each variable shall be defined and addressed in the development of the qualification program.

a) The post event operating time for Type A variable instrument channels shall be the duration for which the measured variable is required by the plant's LBD.
b) The post event operating time for Type B variable instrument channels shall be at least the duration associated with the longest-duration design basis event for that variable.
c) The post event operating time for Type C variable instrument channels shall be at least 100 days for instrument channels monitoring the fission product barriers:
    1) Fuel cladding
    2) Reactor coolant system pressure boundary
    3) Containment pressure boundary

    The qualification duration for other Type C variable instrument channels shall be the duration for which the measured variable is required by the plant's LBD.
d) The post event operating time for Type D and Type E variable instrument channels shall be based on the plant's LBD.

A shorter post event operating time may be acceptable if equipment replacement or repair can be accomplished within an acceptable out-of-service time, taking into consideration the location and accessibility of the equipment.

5.5 Reliability

For those systems for which either quantitative or qualitative goals have been established, appropriate analysis of the design shall be performed to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for performing the reliability analysis.

5.6 Performance assessment documentation

An assessment for each of the performance criteria shall be conducted. This assessment shall be done to assure the as-designed performance meets or exceeds the performance criteria. The results of this assessment shall be documented and shall consider:

a) Allowances for calibration uncertainties, loop errors, and drift (consistent with the methodology given in ANSI/ISA Std 67.04.01-2000 [B3]).
b) The magnitude and direction of errors imposed on the accident monitoring instrumentation by environmental and/or seismic conditions during and after the postulated event.

6. Design criteria

6.1 Single failure

Accident monitoring instrument channels for Type A, Type B, and Type C variables shall satisfy the single failure requirements of IEEE Std 379-2000.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

The accident monitoring instrumentation shall be capable of providing the information required for the operators to perform their role in bringing the plant to, and maintaining it in, a safe condition during an accident in the presence of the following:

a) Any single detectable failure within the accident monitoring instrumentation concurrent with all identifiable but non-detectable failures.
b) All failures occurring as a result of the single failure.
c) All failures and spurious system actions that cause or are caused by the accident requiring the accident monitoring function.

Any systems or components that provide services (for example, cooling, illumination, and energy supply) that are required by the accident monitoring instrumentation to perform their function shall be included in the single failure analysis of the accident monitoring instrumentation they support. IEEE Std 379-2000 provides guidance on the application of the single failure criterion.

Systems required to meet the single failure criterion of this clause are not required to meet the single failure criterion during channel maintenance, test or calibration provided the duration of such testing satisfies the applicable requirements of the LBD. For example, the time interval required for a test, calibration, or maintenance operation could be shown to be so short that it would have an insignificant effect on overall availability of the accident monitoring instrumentation system.

6.2 Common cause failure

Design of instrumentation using microprocessor based sensors, data acquisition, or display equipment for Type A, Type B, and Type C variables, shall address concerns over the possibility that the use of computer software could result in a common cause failure. Common cause failures for the instrumentation channels shall be addressed at the variable level.

The use of identical software in redundant instrumentation channels is acceptable provided one of the following design features can be demonstrated:

a) If channel diversity exists using components not subject to a software common mode failure.
b) If an analysis is conducted which demonstrates that defense-in-depth exists against the consequences of a software common mode failure.

If an analysis does not confirm either channel diversity or defense-in-depth, then a diverse design is required. Examples of how a diverse design may be accomplished include the following:

a) If two diverse display channels are used, both shall meet the same design criteria applicable to the variable.
b) If two redundant (but not diverse) display channels are used, a third diverse processing and display segment shall be used. In this case, the diverse channel segment does not need to meet the design criteria of Type A, Type B, and Type C variables (e.g., a plant computer display).

For instrumentation using microprocessor-based computers, guidance to address common cause failures can be found in IEEE Std 7-4.3.2-1993.

System interaction between accident monitoring microprocessor-based instrumentation systems and other systems that may be served by the data acquisition and display system shall be considered as part of the common cause failure evaluation.

 Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.3 Independence and separation

The accident monitoring instrument channels for Type A, Type B, and Type C variables shall be independent and physically separated in accordance with the following criteria:

a) Instrumentation 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.
b) Redundant segments shall be independent of, and physically separated from, each other to the degree necessary to retain the capability of accomplishing the accident monitoring function during and following any design basis event requiring that function. This shall also include data communication independence described in 5.6 of IEEE Std 7-4.3.2-1993.
c) 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 extent practical to retain the capability to meet the requirements of this standard.
d) Separation shall meet the requirements of IEEE Std 384-1992 and 10 CFR Part 100 [B9].

These requirements do not preclude the association of accident monitoring instrument 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 603-1998 or the ability of the accident monitoring instrument channels to meet the requirements of this standard.

Subclause 5.5 of IEEE Std 7-4.3.2–1993 provides guidance on electromagnetic capability (EMC) compatibility.

6.4 Isolation

The transmission of signals between accident monitoring instrumentation and any system not meeting the minimum design requirements stated herein shall be through isolation devices. These isolation devices shall be classified as part of the accident monitoring instrumentation 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. 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 384-1992.

6.5 Information ambiguity

For Type A, Type B, and Type C variables, the failure of an accident monitoring instrument channel shall not result in information ambiguity that could lead the operator to defeat or fail to accomplish a required safety-related function (for example, the redundant displays disagree and the operator cannot readily deduce which channel has failed). If analysis shows that credible failures can result in information ambiguity, a signal validation technique should be employed. If the signal validation process cannot be automatically accomplished, additional information shall be provided to allow the operators to deduce the actual conditions so that they may properly perform their role.

Examples of how this may be accomplished are:

a) Having the capabilities of being able to perturb the measured variable and determine which channel has failed by observing the instrument channel.
b) Cross checking the value with an independent channel that monitors a different variable that bears a known relationship to the multiple channels (addition of a diverse channel).
c) Providing an additional independent channel of instrumentation on the same variable (addition of a replicate channel).

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

6.6 Power supply

The electrical power supplies for accident monitoring instrumentation shall be considered an auxiliary supporting feature. The power supply for instrumentation that monitors Type A, Type B, and Type C variables shall be Class 1E. Each instrumentation channel power supply shall be designed to be continuously available during plant transients unless short interruptions are evaluated and found acceptable in the plant's licensing basis.

Class 1E or non-Class 1E power supplies may be used for instrumentation to monitor Type D and Type E variables. If an interruption in power is not tolerable, a continuously available source of power shall be used for Type D and Type E variables.

Instruments that obtain their power from the process, such as potential transformers, current transformers and some instruments in a two-wire instrument loop, shall be exempted from this requirement.

The power supplies for the accident monitoring instrument channels shall be capable of providing power with the necessary voltage, frequency and duration to allow the accident monitoring channels to perform with the required accuracy and reliability. Power supplies shall be designed to prevent transients that would adversely impact a monitoring channel from performing its required function or the monitoring channel's accuracy.

Where Class 1E power supplies are used, refer to IEEE Std 308-1991 for the requirements that apply. Batteries are acceptable power supplies for use in portable instrumentation (see 6.14 of IEEE Std 308-1991).

6.7 Calibration

Capability shall be provided for calibration of each accident monitoring instrument channel during normal plant power or shutdown operation or both as determined by the required interval between calibrations.

Means shall be provided for maintaining instrument calibration during the accident. One or more of the following may accomplish this:

- Recalibration
- Specifying a calibration interval to ensure the duration the channel is needed will fall within the equipment's qualified calibration interval
- Selection of equipment that does not require periodic calibration
- Cross-calibration with other channels that bear a known relationship to the information display channel

6.8 Testability

Accident monitoring instrument channels shall have testing capability to verify, on a periodic basis, operability requirements in accordance with the plant's LBD. The periodic test shall follow a predetermined method and results shall be documented.

Capability shall be provided for testing the operability of each accident monitoring instrument channel during plant operation. Examples of how this may be accomplished follow:

a) By observing the effect of perturbing the monitored variable
b) By observing the effect of introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable
c) By cross-checking between channels that bear a known relationship to each other
d) By automatic on-line diagnostics of channel availability

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

6.9 Direct measurement

To the extent practical, a direct variable shall be selected to monitor the related function. A less direct variable may be substituted for the most direct variable if justified by analysis. The analysis shall account for misinterpretation of the less direct variable as well as availability of reliable instrumentation for the more direct variables.

6.10 Control of access

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

6.11 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 in determination of equipment selection and location.

6.12 Minimizing measurements

To the practical extent, the same variables and displays shall be used for accident monitoring as are used for normal operation of the plant to enable the plant operators to use, during an accident situation, variables and displays with which they are most familiar.

6.13 Auxiliary supporting features

Systems or components that provide services that are required for the accident monitoring instrumentation to accomplish its functions shall meet all applicable requirements of that instrumentation. Auxiliary supporting features for accident monitoring instrumentation provided for those variables identified in accordance with Clause 4 are part of the related display channel and shall meet applicable criteria.

For example, a cabinet cooling fan required to maintain signal conditioning modules within design temperature range is an auxiliary supporting feature.

Other components, equipment and systems that perform a function that is not required for the accident monitoring instrumentation to provide required information to the operator, and 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 capability of the accident monitoring instrumentation to function.

6.14 Portable instruments

When required, as part of an EOP or an AOP, portable instruments may be used to obtain data. In such cases, the instruments, the means of communicating data to the control room, and the means of analyzing data to obtain information shall be considered part of the accident monitoring channels. The equipment that forms part of this accident monitoring instrumentation shall meet the criteria for the applicable variable type.

6.15 Documentation of design criteria

Documentation shall be developed and maintained for the design criteria for the accident monitoring variables.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

7. Qualification criteria

The requirements for equipment qualification (seismic and environmental qualification) of accident monitoring instruments shall be consistent with the assigned function of that variable during and following a design basis event or following a seismic event.

7.1 Type A variables

Instrument channels that are required for a planned manual operator action, needed directly or indirectly as a result of a seismic event, shall be seismically qualified. Guidance for seismic qualification is provided in IEEE Std 344-1987.

Instrument channels required for planned operator action to terminate or mitigate an accident shall be environmentally qualified for that accident's postulated environment at the installed location in accordance with the plant's LBD and IEEE Std 323-1983.

7.2 Type B variables

These instrument channels shall be seismically qualified. Guidance for seismic qualification is provided in IEEE Std 344-1987.

Instrument channels shall be environmentally qualified for the worst-case postulated accident environment at the installed location of the equipment in accordance with the plant's LBD and IEEE Std 323-1983. Environmental qualification of instrument channels shall consider performance testing to the maximum process conditions, while subjected to the worst-case postulated accident environment.

7.3 Type C variables

These instrument channels shall be seismically and environmentally qualified in accordance with IEEE Std 344-1987 and IEEE Std 323-1983.

Instrument channels shall be environmentally qualified for the worst-case postulated accident environment at the installed location of the equipment in accordance with the plant's LBD and IEEE Std 323-1983. In addition, environmental qualification of instrument channels shall consider performance testing to the full range of the instrument channels while subjected to worst-case postulated harsh environmental conditions in accordance with the plant's LBD.

NOTE—The above environmental qualification requirements for extended range instrument channels does not account for steady-state elevated levels that may occur in other environmental parameters associated with the extended range. For example, a sensor measuring reactor pressure must be qualified for the measured process variable range (i.e., Level D Service Limit of the reactor vessel) (see American National Standard Boiler and Pressure Vessel Code [B1]), but the corresponding ambient temperature is not mechanistically linked to that pressure. Rather, the ambient temperature value is the bounding value for design basis events analyzed in Chapter 15 of the plant's FSAR or USAR. The extended range requirement is to provide confidence that the equipment would continue to provide information if conditions degrade beyond those postulated in the safety analysis. Since extended ranges are non-mechanistically determined, extension of associated environmental parameter levels is not justifiable and has, therefore, not been required. Proof of performance of instrumentation that provides information to the operator for severe accident mitigation may be done by design only.

7.4 Type D variables

Instrument channels that monitor systems that are expected to be operable following a seismic event shall be seismically qualified in accordance with IEEE Std 344-1987.

Instrument channels shall be environmentally qualified for the particular accident's postulated environment at the installed location in accordance with plant's LBD and in accordance with IEEE Std 323-1983.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7.5 Type E variables

Instrument channels that monitor systems are not required to be environmentally or seismically qualified.

If an instrument channel that is used to determine the magnitude of a radiological release meets the selection criteria of Type A, Type B, Type C, or Type D, then that instrument channel must meet the qualification requirements for that particular type of variable.

7.6 Portable instruments

Portable instruments are excluded from seismic qualification requirements. Administrative controls of storage and access to portable instruments shall ensure compliance with the criteria necessary to meet the performance requirements of the design.

7.7 Post event operating time

Accident monitoring instrumentation shall be qualified, as a minimum, for the length of time their function is required (see 5.4).

7.8 Documentation of qualification criteria

The basis for the selection of the instrument channels that will be qualified shall be established and documented as part of the equipment qualification program.

8. Display criteria

8.1 Display characteristics

8.1.1 Information characteristics

The basis for display characteristics for accident monitoring variables shall include the results of an analysis of the system functions required to respond to an accident and analysis of the tasks required of the operator to implement those functions during design basis events. Display characteristics shall be identified that include, as a minimum; range, instrument accuracy, precision, display format (e.g., status, value, or trend), units, and response time, consistent with the performance characteristics of Clause 5.

8.1.2 Human factors

Accident monitoring displays shall be designed through application of accepted human factor methods and principles per the guidance provided in IEEE Std 1023-1988. Guidance for detailed display design of computer driven displays is provided in IEEE Std 1289-1998 [B6] and ISO 9241-3-1992 [B7].

8.1.3 Anomalous indications

The design of accident monitoring instrumentation shall not cause indications on meters, annunciators, recorders, or video display units to give anomalous readings, which are misinformative and potentially confusing to operators.

8.1.4 Continuous vs. on-demand display

At least one redundant display segment for Type A and Type B accident monitoring variables shall be a continuous real-time display of either a validated digital display or a dedicated analog display (see Figure 2)

Other redundant displays for Type A and Type B accident monitoring variables and displays for other accident monitoring variables may be displayed on demand.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

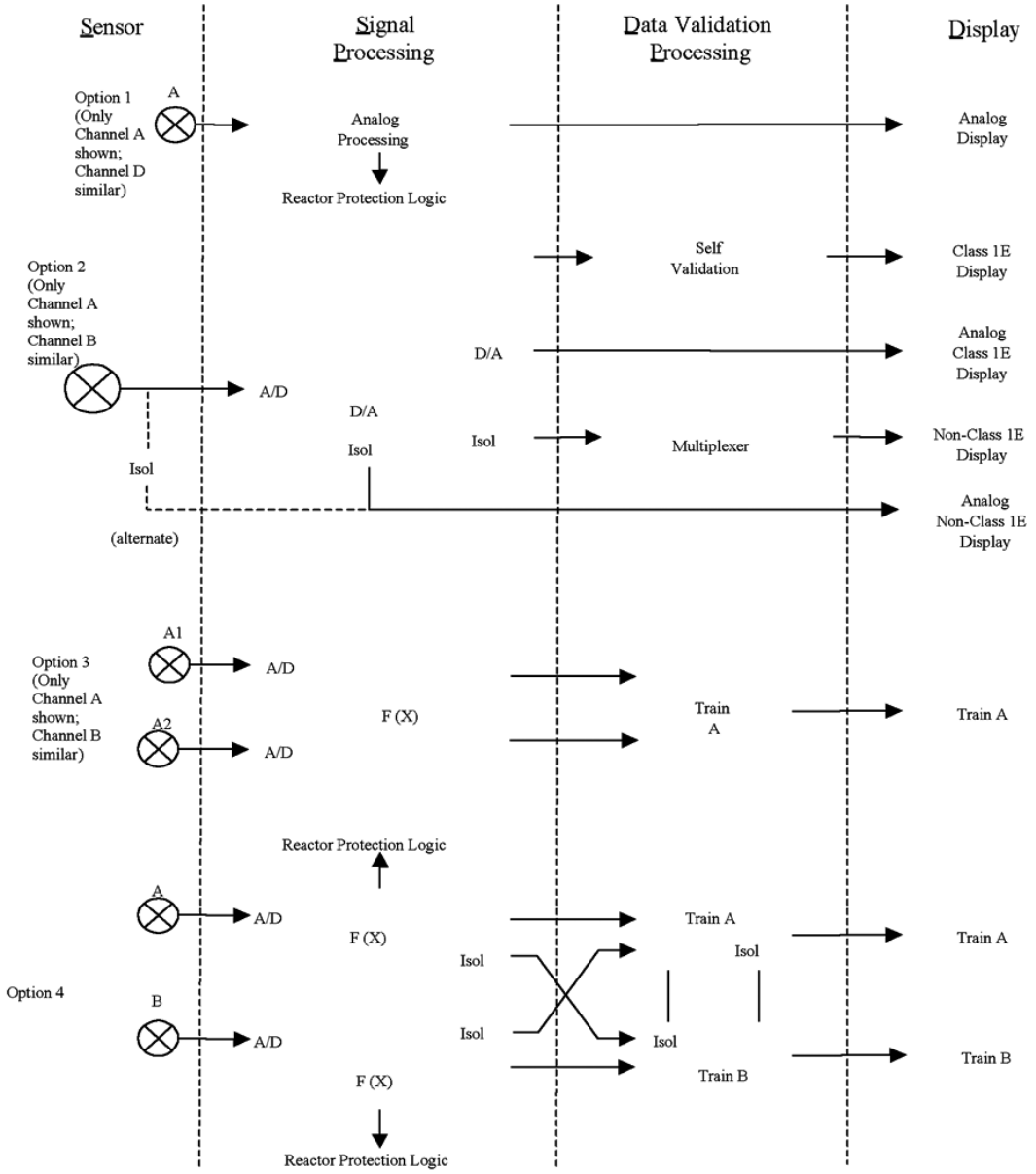


Figure 2—Examples of monitoring channel displays

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

8.2 Trend or rate information

If direct or immediate trend or rate information is essential for operator action, the trend information shall be continuously available on dedicated trend displays (with corresponding recording device) and selectively available on another redundant trend display (with corresponding recording device). The display shall have the capability of providing at least 30 minutes of data.

8.3 Display identification

Control board indication (both conventional indicators and computer based video display unit presentations) of Type A, Type B, and Type C variables shall be uniquely identified as accident monitoring variables with a characteristic designation so that the operator can easily discern information intended for use under accident conditions. On a multi-variable video display, accident monitoring variables should be specifically identified, not the entire video display unit. Type D and Type E variables do not require unique identification.

8.4 Type of monitoring channel display

Monitoring channel displays may use several configurations to provide the display channel information to the operator (see Figure 2).

8.5 Display location

Displays on control board indicators or computer based video display presentations should be placed in appropriate function or system related locations. The basis for display locations should include functional task analysis results and accepted human factors principles.

To the extent practical, the same accident monitoring displays shall be used to monitor normal plant operations.

8.6 Information ambiguity

Displays, which are provided for the sole purpose of resolving information ambiguity, are not required to be of the same type and not required to be continuously displayed.

8.7 Recording

Recording shall be provided for at least one channel of each Type A, Type B, and Type C variable. Recording shall also be provided for Type E variables (other than where portable instruments are used).

Accident monitoring data records may be continuously updated, stored in computer memory and displayed on demand. This function may be performed using non-safety related computers that may not meet the requirements given in IEEE Std 7-4.3.2-1993. Recording capability shall be provided for at least 30 minutes pre-event and 12 hours post-event.

8.8 Digital display signal validation

Signal validation may use normal sensor channels of accident monitoring variables. This provides operators with the most valid information available, if the validation result is verified consistent with corresponding accident monitoring instrument channels. If signal validation is used, the validity of the indication shall be provided as part of the display, for example, through use of unique color coding.

8.9 Display criteria documentation

Documentation shall be developed and maintained for the display criteria for the accident monitoring variables.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

9. Quality assurance

Accident monitoring instrumentation for Type A, Type B, and Type C variables shall be designed, manufactured, inspected, installed, operated, and maintained in accordance with ASME NQA-1-2001. The level of quality assurance to be applied to accident monitoring instrumentation for Type D and Type E variables shall be selected and documented by the designer to assure that the specified performance requirements are met.

Microprocessor based instrumentation development including software validation and verification shall be in accordance with the requirements of IEEE Std 7-4.3.2-1993.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

(informative)

Accident monitoring instrument channel accuracy

A.1 Introduction

As stated in 5.2 the required accuracy of an accident monitoring instrument channel is established based on the channel's assigned function.

A.2 Accuracy requirement groupings according to usage

In general, accident monitoring instrument variables fall into one or both of the following groups according to how the displayed function is to be used by control room personnel.

The first group consists of those variables where the corresponding channel accuracy is specified in the plant's safety analysis or licensing basis. Typically a tight (narrow band) accuracy will have been established to assure that operator action occurs in a timely fashion.

The second group consists of those variables that provide trend or plant stability information (i.e., it is of primary importance for the operator to know whether the monitored variable is increasing, decreasing, or constant). It is of secondary importance to know the exact value of the variable.

A.3 Typical accuracy requirements

For the first group of variables, the level of importance of the monitored information will dictate the required accuracy to be achieved. Typically, this accuracy can be on the order of ± 1 percent or even as high as ± 10 percent of full span. The assumptions made in developing the plant's safety analysis/licensing basis will govern the value to be met. Historically, the required accuracy for instrument channels relied upon to monitor containment pressure and hydrogen concentration has been ± 10 percent of full span.

For linearly derived display instruments (i.e., display range is two decades or less) within the second group of variables, the typical required accuracy, based on historical use, has been ± 20 percent. For instruments with a logarithmic scale this required accuracy has been ± 50 percent of the reading or alternatively plus/minus a half decade.

For instrument variables that fall into both groups, the more restrictive accuracy requirements would apply.

Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B

(informative)

Bibliography

[B1] American National Standard Boiler and Pressure Vessel Code, Section III, Nuclear Power Plant Components, Subsection NCA, General Requirements for Division 1 and Division 2, Section 2142.

[B2] ANSI/ANS Std 4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors.

[B3] ANSI/ISA Std 67.04.01-2000, American National Standard Setpoints for Nuclear Safety-Related Instrumentation.[6]

[B4] IEEE 100™, The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition.[7]

[B5] IEEE Std 497-1981, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations.

[B6] IEEE Std 1289™-1998, IEEE Standard Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.

[B7] ISO 9241-3:1992, Visual Display Terminals (VDTs) Used for Office Tasks Ergonomics Design-Part 3: Visual Display Requirements.[8]

[B8] Regulatory Guide (RG) 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Rev 3, May 1983.

[B9] Title 10, Energy Code of Federal Regulations (CFR), Part 100, Reactor Site Criteria.[9]

[B10] Title 10, Energy Code of Federal Regulations (CFR), Part 50, Appendix A, General Design Criteria for Nuclear Power Plants.

[B11] Title 10, Energy Code of Federal Regulations (CFR), Part 54.3(a), Requirements for Renewal of Operating Licenses for Nuclear Power Plants—Definitions.

[6]ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[7]The IEEE standards or products referred to in Annex B are trademarks belonging to the Institute of Electrical and Electronic Engineers, Inc.

[8]ISO publications are available from the ISO Central Secretariat, Case Postale 56, 1 rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iso.ch/). ISO publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[9]The Code of Federal regulations is available from the United States Government Printing Office, Washington DC 20401-4302, USA.

 Copyright © 2002 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale