

IEEE STANDARDS
ARCHIVES
DO NOT REMOVE

Draft American National Standard

Publication of this draft standard for comment and criticism has been approved by the Institute of Electrical and Electronics Engineers. Distribution of this draft standard for comment shall not continue beyond 12 months from the date of publication. It is expected that following this 12 month period, this draft standard, revised as necessary, shall be submitted to the American National Standards Institute for approval as an American National Standard. Suggestions for revision should be directed to the Secretary, IEEE Standards Committee, 345 East 47th Street, New York, N. Y. 10017.

IEEE Trial-Use Standard Criteria for Safety Systems for Nuclear Power Generating Stations

August 15, 1977

SH06940



PUBLISHED BY

THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Inc.
345 EAST 47 STREET, NEW YORK, N. Y. 10017



Documents

Document Sharing Hub

Draft American National Standard

**IEEE Trial-Use Standard
Criteria for Safety Systems for
Nuclear Power Generating Stations**

Sponsor
Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society

© Copyright 1977 by

The Institute of Electrical and Electronics Engineers, Inc

*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.*

Approved March 3, 1977

IEEE Standards Board

William R. Kruesi, *Chairman*

Irvin N. Howell, Jr., *Vice Chairman*

Ivan G. Easton, *Secretary*

William E. Andrus
Jean Jacques Archambault
Mark Barber
Edward J. Cohen
Warren H. Cook
Louis Costrell
R. L. Curtis
David B. Dobson

R. O. Duncan
Charles W. Flint
Jay Forster
Ralph I. Hauser
Joseph L. Koepfinger
Irving Kolodny
Benjamin J. Leon
Thomas J. Martin

Donald T. Michael
Voss A. Moore
William S. Morgan
William J. Neiswender
Ralph M. Showers
Robert A. Soderman
Leonard W. Thomas, Sr.
B. W. Whittington

Foreword

(This foreword is not a part of IEEE Std 603-1977, Trial-Use Standard Criteria for Safety Systems for Nuclear Power Generating Stations.)

This standard establishes functional and design criteria for nuclear power generating station “safety systems,” that is, that collection of systems required to minimize the probability and magnitude of release of radioactive material to the environment by maintaining plant conditions within the allowable limits established for each design basis event. These criteria are established to provide a means of promoting safe practices for design and evaluation of safety system performance and reliability. The criteria herein represent an acceptable basis for ascertaining the adequacy of safety system performance and reliability. Adherence to these criteria does not necessarily fully establish the adequacy of safety system functional performance and reliability. However, omission of any of these criteria will, in most instances, be an indication of safety system inadequacy.

The safety system encompasses both the protection system (a sense and command aspect) and protective action system (execute aspect). The safety system also encompasses the reactor trip system, engineered safety features, and auxiliary supporting features. Fig 1 has been provided to clarify the interrelationships among protection and protective action systems as well as the reactor trip system, engineered safety features, and auxiliary supporting features.

Application

The safety system criteria established herein are to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design basis events. However, this standard does not necessarily apply to all of the safety related systems, structures, and equipment required for complete plant safety. Although the scope is limited to those systems which perform to mitigate the consequences of design basis events, that is, safety systems, many of the underlying principles may be applicable to equipment provided for safe shutdown, post-accident monitoring display instrumentation, preventive interlock features, or any other systems, structures, or equipment related to safety, or all of the preceding.

To determine which systems are subject to these criteria, an analysis of the overall plant response to postulated design basis events must be performed. A detailed presentation of analytical techniques that can be used in such an analysis is contained in Ref [C4] of Appendix C. Good engineering judgment must be exercised in this assessment to assure that adequate margin exists in the design while not imposing unduly restrictive criteria such that the goal of protecting the public health and safety is replaced by one of protecting every plant component.

Interdisciplinary Approach

The safety system criteria herein are established using a “systems approach” to the design of the power, instrumentation, and control portion of the safety system, as opposed to a specific engineering discipline approach (that is, electrical, mechanical, or civil). It must be recognized that the protective functions cannot be accomplished without mechanical as well as electric equipment and circuitry. Therefore, the design by other than electrical engineering disciplines, primarily mechanical and nuclear engineering, is also affected by these criteria. In order for the safety system to meet the requirements of this standard and the supportive standards, the aggregate design of the safety system (without regard to discipline) may be constrained. Such constraints are implicit interface requirements imposed upon the individual constituent parts to enable the entire safety system to meet these requirements.

While this standard does take a systems approach to the design of the power, instrumentation, and control portion of the safety system, it does not attempt to establish new and different criteria for mechanical equipment or components. Such an attempt by a user is a misapplication of the standard. Nor does this standard attempt to establish the system level requirements which may be required by mechanical or civil equipment; for example, inservice inspection of piping is intentionally excluded. This standard is to provide criteria for the safety system without conflicting with existing standards. This standard is not intended to duplicate or conflict with component design requirements such as the ASME Boiler and Pressure Vessel Code. Rather, this standard is to complement and interface with such documents. This standard and others (for example, Refs [C1] and [C4] in

Appendix C) establish “system level” criteria while other codes and standards establish such detailed design requirements as deemed necessary to assure the functional adequacy of the individual constituent parts of the safety system.

Evolution

This standard evolved by expanding the scope of IEEE Std 279-1971, Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI N42.7-1972). Work was initiated in 1971 to establish criteria for the actuator system (now termed the protective action system). It was decided, after many draft revisions, to assign a new number to the expanded scope, and due to the codification of IEEE Std 279-1971 in Federal Regulation 10CFR50.55a(h), to temporarily retain the existing number 279 for the protection system scope. Following the trial-use period, this standard will be issued as a full standard replacing IEEE Std 279-1971. Therefore, this standard represents the third Subcommittee 6 publication of a systems level criteria document: first, IEEE Std 279-1968 as a trial-use protection system standard; second, IEEE Std 279-1971 as a full protection system standard; and now IEEE Std 603-1977 as a trial-use safety system standard. The significant modifications accomplished with this standard over IEEE Std 279-1971 are as follows:

(1) The scope of this standard has been expanded from the protection system (IEEE Std 279-1971) to the safety system (IEEE Trial-Use Std 603-1977). The safety system encompasses both the protection and protective action systems. The protection system scope has been clarified as the system providing the “sense and command” aspects of the protective function. In contrast, the protective action system has been established as the system providing the “execute” aspects of the protective function. Fig 1 has been added to clarify the interrelationships among protection, protective action, and safety systems as well as the reactor trip system, engineered safety features, and auxiliary supporting features.

(2) The requirements in the former Section 4 of IEEE Std 279-1971 were the primary bases for establishing the requirements contained in Sections 4, 5, and 6 of this standard. Section 4 of this standard contains the functional and design requirements applicable to both the protection and protective action systems. Those additional requirements unique to the sense and command aspects are contained in Section 5 of this standard, while those requirements unique to the execute aspect are contained in Section 6. A conscious attempt was made to establish most of the requirements in Section 4 — stating these requirements broadly enough to apply to both the protection and protective action systems, yet with sufficient specificity to be clearly applied by the user. When the characteristics of the protection or protective action system were considered to be such that a requirement could not be generalized in Section 4 without losing this objective, separate Section 5 or Section 6 requirements, or both, were established containing the desired degree of specificity.

(3) The safety system scope, initially conceived as being limited to the reactor trip system and engineered safety features, has been expanded to include auxiliary supporting features.

(4) To assist in the application of IEEE Trial-Use Std 603-1977, the foreword has been expanded and Appendix A contains an illustrative example.

(5) A close alignment of IEEE Trial-Use Std 603-1977 criteria with related criteria has been established by:

(a) Expanded and revised definitions, developed to encourage consistent terminology throughout IEEE, the American Nuclear Society, and other technical society standards

(b) Specific references to supplemental standards listed in Appendixes B and C.

(6) Section 3 has been reorganized so that the design basis considerations unique to automatically initiated protective actions are grouped in 3.4; those unique to manually initiated protection actions are grouped in 3.5; and those common to both automatically and manually initiated protective actions follow.

Relationship to Class 1E

The term “Class 1E” has been intentionally avoided in the title, scope, and requirements of this standard for the following reasons:

(1) The safety system is limited in scope to those systems required to minimize the probability and magnitude of release of radioactive material to the environment. The scope of Class 1E may encompass more than just the safety system. However, it should be clear from the definition of Class

1E that the electric portions of the safety systems are definitely Class 1E.

(2) The systems approach taken by this standard is interdisciplinary. Use of Class 1E would limit its application to “electric” power, instrumentation, and control portions. These criteria apply to safety systems pneumatically, hydraulically, or electrically powered, instrumented, or controlled, or all of the preceding.

(3) Use of Class 1E in combinations with the term safety system could incorrectly imply that non-Class 1E electric safety systems also exist.

Hence through its avoidance of Class 1E, it is the intent of Subcommittee 6 to broaden the interdisciplinary application of this standard and yet restrict its application to features required to mitigate the consequences of design basis events.

Relationship to IEEE Std 308-1974

The relationship between this trial-use standard and IEEE Std 308-1974, Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, deserves a special explanation. The major role of the Class 1E Power System is to provide electric power to the reactor trip system, engineered safety features, and auxiliary supporting features and therefore the Class 1E Power System itself is an auxiliary supporting feature.

In its role as an auxiliary supporting feature, the Class 1E Power System is covered by both IEEE Std 308-1974 and IEEE Trial-Use Std 603-1977. (Auxiliary supporting feature coverage is indicated on the lower half of Fig 1 of this standard.) The Class 1E Power System is unique in that it extends throughout the plant having far more complex interfaces than other auxiliary supporting features. Most other auxiliary supporting features are limited to one area or a single process in the plant and are basically mechanical systems. Characteristic of the complex interfaces of the Class 1E Power System is the fact that it is an auxiliary supporting feature for other auxiliary supporting features; other auxiliary supporting features are auxiliary supporting features for it; and it may provide support for nonsafety system equipment, as well as providing the means for the execution of the safety system protective actions.

In its role in the protective action system, some Class 1E Power System equipment, switchgear, circuit breakers, power cabling, and loads (primarily motors) are not only part of the Class 1E Power System but are integral parts of the engineered safety features as well. This can be seen in the upper right-hand portion of Fig 1 of this standard.

Consequently, the Class 1E Power System is subject to the requirements of IEEE Std 308-1974 and of IEEE Trial-Use Std 603-1977, and neither can be subjugated by the other.

Relationship to Other Standards

This standard establishes functional and design criteria that are general in nature. It requires supportive standards containing both general and detailed criteria to comprise a minimal set of requirements for the safety system. The American National Standards Institute standards (in part) Refs [C1], [C4], [C8], [C9], and [C10] in Appendix C also contain functional and design criteria for safety systems.

Other IEEE standards prepared in support of the IEEE Std 279-1971 criteria are referenced throughout this standard to aid the user in applying the criteria.

Future Tasks

Subcommittee 6 recognizes the need for standards which are applicable to other overall specific safety related systems, structures, and equipment. Hence Subcommittee 6 acknowledges the need to undertake the additional work described below:

- (1) Development of criteria for post-accident monitoring display instrumentation Ref [B11].
- (2) Development of criteria for preventive interlocks (Project P659).
- (3) Continued consideration of design requirements in IEEE Trial-Use Std 603-1977 pertinent to:
 - (a) Diversity and redundancy
 - (b) Reliability goals
 - (c) Interlocks

- (d) Interface requirements
 - (e) Shared systems
 - (f) Design basis events.
- (4) Pursuit of joint societal sponsorship of this standard.

Acknowledgements

Members of NPEC's Subcommittee 6 participating in the generation of these revised criteria at the time of final NPEC approval were:

G. M. McHugh, Jr, *Chairman*
H. K. Stolt, *Vice Chairman*
R. S. Darke, *Secretary*

T. M. Bates, Jr.
J. T. Beard
W. W. Bowers
G. W. Brastad
R. C. Carruth
C. J. Crane
B. Curtis

R. P. Daigle
P. M. Duggan
N. C. Farr
A. Laird
T. Matsumoto
J. I. Martone
F. E. McLane
D. C. Nau

E. S. Patterson
C. E. Rossi
W. F. Schmauss
L. Stanley
J. E. Thomas
D. Tondi
C. S. Walker

Liaison was provided by:

R. Brockman — liaison from SC-4
A. R. Kasper — liaison from ANS 50
L. K. Holland — liaison from ANS 4
E. A. Kollitides — liaison from SC-4
A. Nathan — liaison from SC-4

The subcommittee wishes to emphasize its acknowledgement to the following members:

L. Stanley — for this three years of service as Subcommittee Chairman
R. P. Daigle — for his two years of service as Working Group Chairman.

The subcommittee also wishes to acknowledge the contributions of the following former members;

R. H. Dalry
S. J. Ditto

A. J. Spurgin

R. L. McIntyre
R. D. Pollard

Members of the Nuclear Power Engineering Committee (NPEC) participating in the approval of these revised criteria were:

T. J. Martin, *Chairman*
A. J. Simmons, *Vice Chairman*
R. E. Allen, *Standards Coordinator*
L. M. Johnson, *Secretary*

J. F. Bates
J. T. Bauer
F. D. Baxter
J. T. Beard
R. G. Benham
J. T. Boettger
D. F. Brosnan
F. W. Chandler
C. M. Chiappetta

N. C. Farr
J. M. Gallagher
J. B. Gardner
R. I. Hayford
T. A. Ippolito
I. M. Jacobs
R. F. Karlicek
A. Laird
J. I. Martone
T. J. McGrath

G. M. McHugh, Jr
W. C. McKay
W. P. Nowicki
W. E. O'Neal
E. S. Patterson
J. R. Penland
D. G. Pitcher
H. V. Redgate
B. M. Rice
J. C. Russ

W. F. Sailer
J. H. Smith
A. J. Spurgin
L. Stanley
W. Steigelmann
H. K. Stolt
D. F. Sullivan
P. Szabados
H. A. Thomas