IEEE
Std 279-1971
(Revision of
IEEE Std 279-1968)

IEEE Standard:
Criteria for Protection Systems for Nuclear Power Generating Stations

IEEE
Std 279-1971
(Revision of
IEEE Std 279-1968)

IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations

Sponsored by the

Joint Committee on Nuclear Power Standards

of the

IEEE Group on Nuclear Science

and the

IEEE Power Engineering Society

Approved Nov. 3, 1970

Joint Committee on Nuclear Power Standards of the IEEE Group on Nuclear Science and the IEEE Power Engineering Society

J. C. Russ, *Chairman*

T. J. Martin, *Vice Chairman* J. T. Boettger, *Secretary*

J. F. Bates	E. R. Gasser	A. J. Simmons
R. G. Benham	L. M. Johnson	J. H. Smith
K. J. Brockwell	A. Kaplan	A. J. Spurgin
D. F. Brosnan	G. S. Keeley	D. H. Steele
O. K. Brown	W. R. Klein	W. L. Stiede
F. W. Chandler	V. A. Moore	D. F. Sullivan
E. F. Chelotti	W. S. Morgan	S. Tjepkema
R. J. Cooney	M. I. Olken	C. S. Walker
D. G. Fitzgerald	E. S. Patterson	E. C. Wenzinger
J. P. Fitzgerald	D. G. Pitcher	J. V. Werme
J. M. Gallagher	R. A. Saya	C. J. Wylie

Approved June 3, 1971

IEEE Standards Committee

B. B. Barrow, *Chairman*

J. Forster, *Vice Chairman* S. I. Sherr, *Secretary*

S. J. Angello	J. A. Goetz	R. H. Rose, II
E. C. Barnes	A. D. Hasley	S. V. Soanes
F. K. Becker	G. E. Hertig	L. Van Rooij
W. H. Cook	A. R. Hileman	R. V. Wachter
W. H. Devenish	H. Lance	B. O. Weinschel
C. J. Essel	D. T. Michael	C. E. White
R. F. Estoppey	J. B. Owens	W. T. Wintringham

The IEEE will maintain this document current with the state of technology. Comments are invited on this document as well as suggestions for additional material that should be included. These should be addressed to:

Secretary
IEEE Standards Committee
The Institute of Electrical and
Electronics Engineers, Inc.
345 East 47 Street
New York, New York 10017

Foreword

(This Foreword is not a part of the IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations.)

The functional performance and reliability of nuclear power generating station protection systems is a matter of concern for manufacturers, for users, and for those who are responsible for licensing and regulating nuclear power generating stations. With the increased volume of nuclear power generating stations planned or being designed, attention has focused on criteria and standards as mechanisms for promoting safe design practice and for evaluating the performance and reliability of proposed systems. These criteria are an industry consensus of an acceptable approach to assessing the adequacy of protection system functional performance and reliability in meeting design requirements.

As interpretation of the term "protection system" seems to be evolving, this document should also include criteria for actuator systems. Work to expand the scope of the document to this end is underway and will be reflected in a future revision. At that time, the system presently described herein can more appropriately be called a "protection signal system," which by definition includes both instrument and logic channels. The protection system will then consist of the protective signal system and the actuator system. The user should recognize that neither the present nor the expanded scope includes all of the structures and equipment required for complete plant protection.

The Institute of Electrical and Electronics Engineers (IEEE) undertook the development of these criteria through the Standards Committee of the Nuclear Science Group in 1964 at the request of ASA Sectional Committee N6, Reactor Safety Standards. In 1966, the working group responsible for generating these criteria was made a subcommittee of the Reactors and Reactor Controls Committee of the IEEE Nuclear Science Group. Unanimous subcommittee approval for the proposed criteria was obtained in June 1966, and in the Nuclear Science Group Standards Committee in September 1966. In addition, the proposed criteria were reviewed by other interested persons, both within and outside the IEEE. In 1968, final approval of the proposed criteria was given by the IEEE Standards Committee and they were published on a trial-use basis as IEEE No. 279, Proposed IEEE Criteria for Nuclear Power Plant Protection Systems, effective August 30, 1968.

At the time of this publication a full national consensus in the U.S.A., necessary for the adoption of the criteria by the American National Standards Institute, did not exist. This was basically because of a feeling in some quarters that paragraph 4.7 should be more stringent in its requirements for separation of control and protection functions. In order to resolve this question and to respond to comments on and suggestions for additional material that should be included in the criteria, Subcommittee 6, Reactor Protection Systems, was formed under the Nuclear Science Group Standards Committee. In January, 1970, the IEEE established JCNPS (the Joint Committee on Nuclear Power Standards) as an instrument of the Power and Nuclear Science Groups, to plan, organize, expedite, and coordinate all IEEE Nuclear Power Standards work under one approval procedure. The activities of SC-6 were included under this Joint Committee. In 1970, SC-6, with approval from the JCNPS membership, proposed several changes in the original document. Members of the subcommittee participating in the generation of the revised criteria at the time of final JCNPS approval were:

J. M. Gallagher, Jr., *Chairman*

J. T. Boettger	G. S. Keeley	J. R. Ward
E. F. Chelotti	A. J. Spurgin	J. V. Werme
J. H. Caveglia	L. Stanley	E. C. Wenzinger
E. R. Gasser	W. L. Stiede	C. S. Walker
	G. H. Strong	

Following the approval of IEEE Std 279-1971 by the Joint Committee on Nuclear Power Standards of the IEEE Group on Nuclear Science and the IEEE Power Engineering Society, the standard was reviewed and approved by American National Standards Committee N42 on Radiation Instrumentation. On approval by the IEEE Standards Committee, the Institute of Electrical and Electronics Engineers, as Secretariat for N42, has submitted this standard to ANSI for approval as an American National Standard. At the time it ballotted on IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations, American National Standards Committee N42 had the following personnel:

Louis Costrell, *Chairman* David C. Cook, *Secretary*

Organization Represented	*Name of Representative*
American Chemical Society	Louis P. Remsberg, Jr
American Conference of Governmental Industrial Hygienists	Jesse Lieberman
American Industrial Hygiene Association	W. H. Ray
American Nuclear Society	W. C. Lipinski
	Thomas Mulcahey (*Alt*)
American Society of Mechanical Engineers	R. C. Austin
American Society of Safety Engineers	*Representation Vacant*
American Society for Testing and Materials	John L. Kuranz
	Jack Bystrom (*Alt*)
Atomic Industrial Forum	*Representation Vacant*
Electric Light and Power Group	G. S. Keeley
	G. A. Olson (*Alt*)
Health Physics Society	J. B. Horner Kuper
	Robert L. Butenhoff (*Alt*)
Institute of Electrical and Electronics Engineers	Louis Costrell
	Lester Kornblith, Jr
	J. J. Loving
	J. Forster (*Alt*)
Instrument Society of America	M. T. Slind
	J. E. Kaveckis (*Alt*)
Manufacturing Chemists Association	Mont G. Mason
National Electrical Manufacturers Association	Theodore Hamburger
Oak Ridge National Laboratory	Frank W. Manning
Scientific Apparatus Makers Association	Robert Breen
Underwriters' Laboratories	Leonard Horn
U. S. Atomic Energy Commission, Division of Biology and Medicine	Hodge R. Wasson
U. S. Atomic Energy Commission, Division of Reactor Development and Technology	Paul L. Havenstein
	W. E. Womac (*Alt*)
U. S. Department of the Army, Materiel Command	Abraham E. Cohen
U. S. Department of the Army, Office of Civil Defense Mobilization	Carl R. Siebentritt, Jr
	T. G. Provenzano (*Alt*)
U. S. Department of Commerce, National Bureau of Standards	Louis Costrell
U. S. Department of Health, Education, and Welfare, Public Health Service	Henry J. L. Rechen, Jr
	Roger Schneider (*Alt*)
U. S. Naval Research Laboratory	D. C. Cook
Members-at-Large	O. W. Bilharz
	S. H. Hanauer
	John M. Gallagher, Jr
	Voss A. Moore
	R. F. Shea

Contents

IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations

1. Scope

These criteria establish minimum requirements for the safety-related functional performance and reliability of protection systems for stationary land-based nuclear reactors producing steam for electric power generation. Fulfillment of these requirements does not necessarily fully establish the adequacy of protective system functional performance and reliability. On the other hand, omission of any of these requirements will, in most instances, be an indication of system inadequacy. For purposes of these criteria, the nuclear power generating station protection system encompasses all electric and mechanical devices and circuitry (from sensors to actuation device input terminals) involved in generating those signals associated with the protective function. These signals include those that actuate reactor trip and that, in the event of a serious reactor accident, actuate engineered safeguards such as containment isolation, core spray, safety injection, pressure reduction, and air cleaning.

2. Definitions

The definitions in this section establish the meanings of words in the context of their use in these criteria.

channel. An arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single action signals are combined.

components. Items from which the system is assembled (for example, resistors, capacitors, wires, connectors, transistors, tubes, switches, springs, etc).

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

protective action. A protective action can be at the channel level or the system level

(1) A protective action at the channel level is the initiation of a signal by a single channel when the variable sensed exceeds a limit

(2) A protective action at the system level is initiation of the operation of a sufficient number of actuators to effect a protective function.

protective function. A protective function is the sensing of one or more variables associated with a particular generating station condition, signal processing, and the initiation and completion of the protective action at values of the variables established in the design bases.

system. Where not otherwise qualified, the word "system" refers to the nuclear power generating station protection system, as defined in the scope section of these criteria.

type tests. Tests made on one or more units to verify adequacy of design.

3. Design Basis

A specific protection system design basis shall be provided for each nuclear power generating station. The information thus provided shall be available, as needed, for making judgments on system functional adequacy.

The design basis shall document as a minimum, the following:

(1) the generating station conditions which require protective action;

(2) the generating station variables (for example, neutron flux, coolant flow, pressure, etc) that are required to be monitored in order to provide protective actions;

2352

(3) the minimum number and location of the sensors required to monitor adequately, for protective function purposes, those variables listed in Section 3(2) that have a spatial dependence;

(4) prudent operational limits for each variable listed in Section 3(2) in each applicable reactor operation mode;

(5) the margin, with appropriate interpretive information, between each operational limit and the level considered to mark the onset of unsafe conditions;

(6) the levels that, when reached, will require protective action;

(7) the range of transient and steady-state conditions of both the energy supply and the environment (for example, voltage, frequency, temperature, humidity, pressure, vibration, etc) during normal, abnormal, and accident circumstances throughout which the system must perform;

(8) the malfunctions, accidents, or other unusual events (for example, fire, explosion, missiles, lightning, flood, earthquake, wind, etc) which could physically damage protection system components or could cause environmental changes leading to functional degradation of system performance, and for which provisions must be incorporated to retain necessary protective action;

(9) minimum performance requirements including the following:

(a) system response times;

(b) system accuracies;

(c) ranges (normal, abnormal, and accident conditions) of the magnitudes and rates of change of sensed variables to be accommodated until proper conclusion of the protective action is assured.

NOTE: The development of the specific information to be used in fulfillment of the above requirements is not within the scope of these criteria.[1]

4. Requirements

4.1 General Functional Requirement. The nuclear power generating station protection system shall, with precision and reliability, automatically initiate appropriate protective action whenever a condition monitored by the system reaches a preset level. This requirement applies for the full range of conditions and performance enumerated in Sections 3(7), 3(8), and 3(9).

4.2 Single Failure Criterion. Any single failure within the protection system shall not prevent proper protective action at the system level when required.

NOTE: "Single failure" includes such events as the shorting or open-circuiting of interconnecting signal or power cables. It also includes single credible malfunctions or events that cause a number of consequential component, module, or channel failures. For example, the overheating of an amplifier module is a "single failure" even though several transistor failures result. Mechanical damage to a mode switch would be a "single failure" although several channels might become involved.

4.3 Quality of Components and Modules. Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Quality levels shall be achieved through the specification of requirements known to promote high quality, such as requirements for design, for the derating of components, for manufacturing, quality control, inspection, calibration, and test.

4.4 Equipment Qualification. Type test data or reasonable engineering extrapolation based on test data shall be available to verify that protection system equipment shall meet, on a continuing basis, the performance requirements determined to be necessary for achieving the system requirements.

NOTE: Attention is directed particularly to the requirements of Sections 3(7) and 3(9).

4.5 Channel Integrity. All protection system channels shall be designed to maintain necessary functional capability under extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents.

4.6 Channel Independence. Channels that provide signals for the same protective function shall be independent and physically separated to accomplish decoupling of the effects of unsafe environmental factors, electric transients, and physical accident consequences documented in the design basis, and to reduce

[1] The development of standard criteria and requirements relating to the determination of such design basis information as unsafe conditions requiring protective functions, variables to be monitored, operational limits, margins, set points, etc., are under consideration in American Nuclear Society Standards Subcommittee 4.

2333

the likelihood of interactions between channels during maintenance operations or in the event of channel malfunction.

4.7 Control and Protection System Interaction.[2]

4.7.1 *Classification of Equipment.* Any equipment that is used for both protective and control functions shall be classified as part of the protection system and shall meet all the requirements of this document.

4.7.2 *Isolation Devices.* The transmission of signals from protection system equipment for control system use shall be through isolation devices which shall be classified as part of the protection system and shall meet all the requirements of this document. No credible failure at the output of an isolation device shall prevent the associated protection system channel from meeting the minimum performance requirements specified in the design bases.

Examples of credible failures include short circuits, open circuits, grounds, and the application of the maximum credible ac or dc potential. A failure in an isolation device is evaluated in the same manner as a failure of other equipment in the protection system.

4.7.3 *Single Random Failure.* Where a single random failure can cause a control system action that results in a generating station condition requiring protective action and can also prevent proper action of a protection system channel designed to protect against the condition, the remaining redundant protection channels shall be capable of providing the protective action even when degraded by a second random failure.

Provisions shall be included so that this requirement can still be met if a channel is bypassed or removed from service for test or maintenance purposes. Acceptable provisions include reducing the required coincidence, defeating the control signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

4.7.4 *Multiple Failures Resulting from a Credible Single Event.* Where a credible single event can cause a control system action that results in a condition requiring protective action and can concurrently prevent the protective action from those protection system channels designated to provide principal protection against the condition, one of the following must be met.

4.7.4.1 Alternate channels, not subject to failure resulting from the same single event, shall be provided to limit the consequences of this event to a value specified by the design bases. In the selection of alternate channels, consideration should be given to (1) channels that sense a set of variables different from the principal channels, (2) channels that use equipment different from that of the principal channels to sense the same variable, and (3) channels that sense a set of variables different from those of the principal protection channels using equipment different from that of the principal protection channels. Both the principal and alternate protection channels shall meet all the requirements of this document.

4.7.4.2 Equipment, not subject to failure caused by the same credible single event, shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment shall meet all the requirements of this document.

4.8 Derivation of System Inputs. To the extent feasible and practical, protection system inputs shall be derived from signals that are direct measures of the desired variables.

4.9 Capability for Sensor Checks. Means shall be provided for checking, with a high degree of confidence, the operational availability of each system input sensor during reactor operation.

This may be accomplished in various ways, for example:

(1) by perturbing the monitored variable; or

(2) within the constraints of paragraph 4.11, by introducing and varying, as appropriate, a substitute input to the sensor of the same nature as the measured variable; or

(3) by cross checking between channels that bear a known relationship to each other and that have read-outs available.

4.10 Capability for Test and Calibration. Capability shall be provided for testing and calibrating channels and the devices used to de-

[2] Work is under way to develop the requirements for actuator systems which will be included in a future revision of this document. This revision will contain requirements as they relate to control and protection system interaction at the actuator level.

rive the final system output signal from the various channel signals. For those parts of the system where the required interval between testing will be less than the normal time interval between generating station shutdowns, there shall be capability for testing during power operation.

4.11 Channel Bypass or Removal from Operation. The system shall be designed to permit any one channel to be maintained, and when required, tested or calibrated during power operation without initiating a protective action at the systems level. During such operation the active parts of the system shall of themselves continue to meet the single failure criterion.

Exception: "One-out-of-two" systems are permitted to violate the single failure criterion during channel bypass provided that acceptable reliability of operation can be otherwise demonstrated. For example, the bypass time interval required for a test, calibration, or maintenance operation could be shown to be so short that the probability of failure of the active channel would be commensurate with the probability of failure of the "one-out-of-two" system during its normal interval between tests.

4.12 Operating Bypasses. Where operating requirements necessitate automatic or manual bypass of a protective function, the design shall be such that the bypass will be removed automatically whenever permissive conditions are not met. Devices used to achieve automatic removal of the bypass of a protective function are part of the protection system and shall be designed in accordance with these criteria.

4.13 Indication of Bypasses. If the protective action of some part of the system has been bypassed or deliberately rendered inoperative for any purpose, this fact shall be continuously indicated in the control room.

4.14 Access to Means for Bypassing. The design shall permit the administrative control of the means for manually bypassing channels or protective functions.

4.15 Multiple Set Points. Where it is necessary to change to a more restrictive set point to provide adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of assuring that the more restrictive set point is used. The devices used to prevent improper use of less restrictive set points shall be considered a part of the protection system and shall be designed in accordance with the other provisions of these criteria regarding performance and reliability.

4.16 Completion of Protective Action Once It Is Initiated. The protection system shall be so designed that, once initiated, a protective action at the system level shall go to completion. Return to operation shall require subsequent deliberate operator action.

4.17 Manual Initiation. The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc). No single failure, as defined by the note following Section 4.2, within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means. Manual initiation should depend upon the operation of a minimum of equipment.

4.18 Access to Set Point Adjustments, Calibration, and Test Points. The design shall permit the administrative control of access to all set point adjustments, module calibration adjustments, and test points.

4.19 Identification of Protective Actions. Protective actions shall be indicated and identified down to the channel level.

4.20 Information Read-Out. The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety. The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator.

4.21 System Repair. The system shall be designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.

4.22 Identification. In order to provide assurance that the requirements given in this document can be applied during the design, construction, maintenance, and operation of the plant, the protection system equipment (for example, interconnecting wiring, components, modules, etc), shall be identified[3] distinctively as being in the protection system. This identification shall distinguish between redundant portions of the protection system. In the installed equipments, components, or modules mounted in assemblies that are clearly identified as being in the protection system do not themselves require identification.

[3] Work is in progress to establish a criterion for identification of protection system equipment or drawings and other documentation and the extent to which such identification should be required.

IEEE Standards of Particular Interest to Nuclear Engineers and Scientists

IEEE Std	Title
159	Methods of Testing Gas-Filled Radiation Counter Tubes (1952)
278	Guide for Classifying Electrical Insulating Materials Exposed to Neutron and Gamma Radiation (1967) (ANSI N4.1)
279	Criteria for Protection Systems for Nuclear Power Generating Stations (1971)
300	Test Procedure for Semiconductor Radiation Devices (1969) (ANSI N42.1)
301	Test Procedure for Amplifiers and Preamplifiers for Semiconductor Radiation Detectors (1969) (ANSI N42.2)
308	Criteria for Class IE Electric Systems for Nuclear Power Generating Stations (1970)
309	Test Procedure for Geiger-Muller Counters (1970) (ANSI N42.3)
317	Electrical Penetration Assemblies in Containment Structures for Nuclear Generating Stations (1971)
323	General Guide for Qualifying Class I Electric Equipment for Nuclear Power Generating Stations (1971)
325	Test Procedure for Germanium Gamma-Ray Detectors (1971)

For a free catalog of IEEE Standards write the

Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, N. Y. 10017, U.S.A.