

IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society

Reaffirmed 27 March 2008
Approved 21 September 2000

IEEE-SA Standards Board

Abstract: Application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating safety systems is covered in this standard.

Keywords: actuator, cascaded failure, common-cause failure, design basis event, detectable failure, effects analysis, safety system, single-failure criterion, system actuation, system logic

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

Copyright © 2001 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 9 March 2001. Printed in the United States of America.

Print: ISBN 0-7381-2603-9 SH94874
PDF: ISBN 0-7381-2604-7 SS94874

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.

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.

IEEE is the sole entity that may authorize the use of certification marks, trademarks, or other designations to indicate compliance with the materials set forth herein.

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; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not part of IEEE Std 379-2000, IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.)

The requirement for nuclear power generating station safety systems to meet a single-failure criterion is found in many documents, including IEEE Standards, American Nuclear Society (ANS) standards, and federal regulations. It is the intention of this document to

- Conform specifically with the requirements of IEEE Std 603-1998
- Interpret the single-failure criterion as stated in IEEE Std 603-1998
- Provide guidance in the application of the single-failure criterion as stated in IEEE Std 603-1998

It is recognized that the single-failure criterion is applicable to the aggregate of electrical and mechanical systems. However, the criterion statement, as found in this document, has been developed for electrical systems. Where the interface with mechanical systems is unavoidable (e.g., sensing lines), the mechanical portions are considered to be part of the electrical system with which they interface. It should be noted that the systems include the actuation and protection systems, as well as the sense, command, and execute features of the power system (in accordance with IEEE Std 741-1997).

The purpose of this revision to the standard is to

- Update the references cited in the text
- Provide clarification of single-failure criterion as applied to shared systems of multiunit stations
- Address any comments obtained from the user community since the issuance of IEEE Std 379-1994

This revision also addresses regulatory positions and issues as identified in Regulatory Guide 1.53 (issued June 1973). A discussion of each of the regulatory positions and issues follows:

- Regulatory Guide 1.53 states that 5.2 of IEEE Std 379-1972 should be supplemented as follows:

“The detectability of a single failure is predicated on the assumption that the test results in the presence of a failure are different from the results that would be obtained if no failure is present. Thus, inconclusive testing procedures such as continuity checks of relay circuit coils in lieu of relay operations should not be considered as adequate bases to classify as detectable all potential failures which could negate the functional capability of the tested device.”

Subclause 5.2 of IEEE Std 379-1972 states that when undetectable failures are identified, a preferred course of action is to redesign the protection system or the test scheme to eliminate potential undetectable failures. Since the issuance of IEEE Std 379-1972, testing criteria for safety systems to verify that they are able to perform their safety function was identified and defined in IEEE Std 338-1987 and Regulatory Guide 1.118. Therefore, the proposed supplement to IEEE Std 379-1972 has been addressed by IEEE Std 338-1987 and Regulatory Guide 1.118.

- Regulatory Guide 1.53 states that 6.2 of IEEE Std 379-1972 should be supplemented as follows:

“Where a single mode switch supplies signal to redundant channels, it should be considered that the single-failure criterion will not be satisfied if either (a) individual switch sections supply signals to redundant channels, or (b) redundant circuits controlled by the switch are separated by less than six inches without suitable barriers.”

Subclause 6.2 of IEEE Std 379-1972 states that interconnections between channels are areas where channel independence could be lost. The supplement statement addresses independence criteria. These requirements are now in the scope of IEEE Std 384-1992. Therefore, this proposed supplemental statement is addressed by IEEE Std 384-1992.

- Regulatory Guide 1.53 states that 6.3 and 6.4 of IEEE Std 379-1972 should be interpreted as not permitting separate failure mode analyses for the protection system logic and the actuator system. The collective protection system logic-actuator system should be analyzed for single-failure modes which, though not negating the functional capability of either portion, act to disable the complete protective function.

The concern, as stated in the Regulatory Guide 1.53, is to ensure that the performance of single-failure analyses for the protection system logic and the actuator system are collective. The subsequent revisions and restructuring of IEEE Std 379-1972 address this concern. Clause 4 of IEEE Std 379-1972 requires the safety systems be able to perform all safety functions with a single failure occurring within the safety systems. Subclause 6.2.2 of IEEE Std 379-1972 requires the analysis to verify that no single failure would cause failure in the channels or actuator circuits, that would then cause loss of the safety function. Subclause 6.2.3 of IEEE Std 379-1972 also requires the analysis to assure that no single failure could cause loss of the safety function, the analysis to address the complete actuator system, and the analysis to assure any failures (electrical or mechanical) do not cause failures in redundant equipment.

Several areas addressed by, but not completely developed within, this standard are as follows:

- *Relationships with other guides and standards.* Other guides and standards should be incorporated in any good design to produce an acceptable and reliable system. The relationship of the single-failure criterion to these other guides and standards, documentation requirements, reliability and probability studies, testing, and operation is not within the scope of this standard.
- *Shared systems.* This standard in the present revision, describes the manner in which the single-failure criterion should be applied to shared systems. The intent is to neither endorse for forbid the use of shared systems, but rather to provide minimum requirements to assure that shared systems are analyzed as rigorously for the effects of component failures as they would be if sharing were not used.
- *Single operator error.* Operator actions should be considered, but are beyond the scope of this standard.
- *Common-cause failures.* Common-cause failures not subject to single-failure analysis include those that can result from external environmental effects, design deficiencies, manufacturing errors, maintenance errors, and operator errors. Common-cause failures are of concern in assessing plant safety.

Common-cause failure should be addressed using reliability and probability tools, and should consider the consequences of the loss of safety function. IEEE Std 7-4.3.2-1993 addresses common-cause failures for digital computers. IAEA 50-P-1 (1990) [B3]¹ also addresses common-cause failures.

¹The numbers in brackets correspond to the bibliography items listed in Annex A.

Participants

The Working Group SC 6.3 that prepared this standard had the following membership:

David J. Zaprazny, *Chair*

R. E. Battle
Wesley W. Bowers
R. Copyak

C. K. Doult
P. M. Duggan

Britton P. Grim
Rick Kendall
M. H. Miller

The following members of the balloting committee voted on this standard:

Satish K. Aggarwal
Vincent P. Bacanskas
Farouk D. Baxter
Wesley W. Bowers
Daniel F. Brosnan
Robert C. Carruth
Raymond J. Christensen
John J. Disosway
C. K. Doult
Richard E. Dulski
Jay Forster

Wilmer C. Gangloff
Luis C. Gonzalez
John Kenneth Greene
Britton P. Grim
Robert E. Hall
Gregory K. Henry
David A. Horvath
Sonny Kasturi
James T. Keiper
Peter M. Kelly
Rick Kendall

John R. Matras
Richard B. Miller
Burt Nemroff
Neil P. Smith
Peter B. Stevens
John B. Waclo
Raymond Weronick
G. O. Wilkinson
Paul L. Yanosy
David J. Zaprazny
Mark S. Zar

When the IEEE-SA Standards Board approved this standard on 21 September 2000, it had the following membership:

Donald N. Heirman, *Chair*

James T. Carlo, *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Mark D. Bowman
Gary R. Engmann
Harold E. Epstein
H. Landis Floyd
Jay Forster*
Howard M. Frazier
Ruben D. Garzon

James H. Gurney
Richard J. Holleman
Lowell G. Johnson
Robert J. Kennelly
Joseph L. Koepfinger*
Peter H. Lips
L. Bruce McClung
Daleep C. Mohla

James W. Moore
Robert F. Munzner
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Akio Tojo
Donald W. Zipse

*Member Emeritus

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

Alan Cookson, *NIST Representative*

Donald R. Volzka, *TAB Representative*

Yvette Ho Sang

IEEE Standards Project Editor