IEEE Std 379-2000
(Revision of IEEE Std 379-1994)

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

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.

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 ìAS IS.î

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.

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 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:

  ìThe 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.î

  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:

  ìWhere 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.î

Copyright © 2001 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

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.

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

Copyright © 2001 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

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

David J. Zaprazny, *Chair*

R. E. Battle	C. K. Doutt	Britton P. Grim
Wesley W. Bowers	P. M. Duggan	Rick Kendall
R. Copyak		M. H. Miller

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

Satish K. Aggarwal	Wilmer C. Gangloff	John R. Matras
Vincent P. Bacanskas	Luis C. Gonzalez	Richard B. Miller
Farouk D. Baxter	John Kenneth Greene	Burt Nemroff
Wesley W. Bowers	Britton P. Grim	Neil P. Smith
Daniel F. Brosnan	Robert E. Hall	Peter B. Stevens
Robert C. Carruth	Gregory K. Henry	John B. Waclo
Raymond J. Christensen	David A. Horvath	Raymond Weronick
John J. Disosway	Sonny Kasturi	G. O. Wilkinson
C. K. Doutt	James T. Keiper	Paul L. Yanosy
Richard E. Dulski	Peter M. Kelly	David J. Zaprazny
Jay Forster	Rick Kendall	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	James H. Gurney	James W. Moore
Mark D. Bowman	Richard J. Holleman	Robert F. Munzner
Gary R. Engmann	Lowell G. Johnson	Ronald C. Petersen
Harold E. Epstein	Robert J. Kennelly	Gerald H. Peterson
H. Landis Floyd	Joseph L. Koepfinger*	John B. Posey
Jay Forster*	Peter H. Lips	Gary S. Robinson
Howard M. Frazier	L. Bruce McClung	Akio Tojo
Ruben D. Garzon	Daleep C. Mohla	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

Copyright © 2001 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

2. References 2

3. Definitions 2

4. Statement of the single-failure criterion 4

5. Requirements 4

5.1 Independence and redundancy 5
5.2 Nondetectable failure 5
5.3 Cascaded failures 5
5.4 Design basis events 5
5.5 Common-cause failures 5
5.6 Shared systems 6

6. Design analysis for single failure 6

6.1 Procedure 6
6.2 Systems portions analysis 7
6.3 Other considerations 8

Annex A (informative) Bibliography 9

Copyright © 2001 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 Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems

1. Overview

1.1 Scope

This standard covers the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating station safety systems.

1.2 Purpose

The purpose of this standard is to interpret and provide guidance in the application of the single-failure criterion, discuss failures, and present an acceptable method of single-failure analysis. It is not the function of this standard to identify where the single-failure criterion is to be applied or to force compliance on any system; however, in those cases where the single-failure criterion has been invoked, this standard establishes the requirements for its application.

This standard shall be used to establish conformance with the requirements of IEEE Std. 603-1998[1] and the single-failure criterion as stated in that standard.

NOTEó The single-failure criterion is also applied to designated safety functions in other standards, e.g., IEEE Std 308-1992, ANSI/ANS 51.1-1983, and ANSI/ANS 52.1-1983. Application of the single-failure criterion to the aggregate of all plant structures, systems, and components is specified in 3.2.1 of ANSI/ANS 51.1-1983, ANSI/ANS 52.1-1983, and IAEA Safety Series No. 50-P-1 (1990) [B3][2].

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

[2]The numbers in brackets correspond to the bibliography items listed in Annex A.

Copyright © 2001 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:

ANSI/ANS 51.1-1983 (Reaff 1988), Nuclear Safety Criteria for the Design of Stationary Pressurized Water Reactor Plants.[3]

ANSI/ANS 52.1-1983 (Reaff 1988), Nuclear Safety Criteria for the Design of Stationary Boiling Water Reactor Plants.

IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.[4]

IEEE Std 308-1991, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations.

IEEE Std 352-1987 (Reaff 1993), IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.

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

IEEE Std 577-1976 (Reaff 1992), 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 741-1997, IEEE Standard Criteria for the Protection of Class IE Power Systems and Equipment in Nuclear Power Generating Stations.

3. Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards Terms* [B4] should be referenced for terms not defined in this clause.

3.1 actuated equipment: The assembly of prime movers and driven equipment used to accomplish a protective action.

NOTEó Examples of prime movers are turbines, motors, and solenoids. Examples of driven equipment are control rods, pumps, and valves.

3.2 actuation device: A component or assembly of components that directly controls the motive power (electricity, compressed air, hydraulic fluid, etc.) for actuated equipment.

NOTEó Examples of actuation devices are circuit breakers, relays, and pilot valves.

3.3 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]ANS publications are available from the American Nuclear Society (ANS), 555 N. Kensington, LaGrange Park, IL 60525 (http://www.ans.org/).

[4]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (http://standards.ieee.org/).

Copyright © 2001 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

3.4 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 protective action signals are combined.

3.5 common-cause failure: Multiple failures attributable to a common cause.

3.6 design basis events: Postulated events used in the design to establish the acceptable performance requirements for the structures, systems, and components.

3.7 detectable failures: Failures that can be identified through periodic testing or that can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures.

NOTEóIdentifiable, but nondetectable failures are failures identified by analysis that cannot be detected through periodic testing or revealed by alarm or anomalous indication.

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

NOTEó In some instances, protective actions may be performed by execute features that respond directly to the process conditions (e.g., check valves and self-actuating relief valves).

3.9 failure: The termination of the ability of an item to perform its required function.

3.10 periodic test: Test performed at scheduled intervals to detect failures and verify operability.

3.11 protection system: The part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features.

3.12 protective action: The initiation of a signal within the sense and command features, or the operation of equipment within the execute features, for the purpose of accomplishing a safety function.

3.13 redundant equipment or system: A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.

NOTEó Duplication of essential functions can be accomplished by the use of identical equipment, equipment diversity, or functional diversity.

3.14 safety function: One of the processes or conditions (e.g., emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) that is essential in maintaining plant parameters within acceptable limits established for a design basis event.

NOTEóA safety function is achieved by the completion of all required protective actions by the reactor trip system or the engineered safety features, or both, concurrent with the completion of all required protective actions by the auxiliary supporting features.

3.15 safety group: A given minimal set of interconnected components, modules, and equipment that can accomplish a safety function.

Copyright © 2001 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

3.16 safety system: A system that is relied upon to remain functional during and following design basis events to ensure one of the following:

a) The integrity of the reactor coolant pressure boundary

b) The capability to shut down the reactor and maintain it in a safe shutdown condition

c) The capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the guidelines given in CFR Publication 10CFR100 (1994) [B2].

NOTES

1ó The electrical portion of the safety system that performs a safety function is classified as Class 1E.

2ó This definition of *safety system* agrees with the definition of *safety-related systems* used by the American Nuclear Society (ANS) and CFR Publication 10CFR50.49 (1994) [B1].

3.17 sense and command features: 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.

3.18 shared systems: Structures, systems, and components that can perform functions for more than one unit in multiunit stations.

NOTEóThis definition includes the following:

a) Systems that are simultaneously shared by both units.

b) Time sequential sharing or systems that would be shared by two units at different times, according to the sequence of events.

c) Systems that would only be used by one unit, at any given time, but that could be disconnected from that unit and placed in the other unit on demand.

3.19 system logic: That equipment that monitors the output of two or more channels and supplies output signals in accordance with a prescribed combination rule (e.g., two of three, two of four).

4. Statement of the single-failure criterion

The safety systems shall perform all required safety functions for a design basis event in the presence of the following:

a) Any single detectable failure within the safety systems concurrent with all identifiable, but nondetectable failures.

b) All failures caused by the single failure.

c) All failures and spurious system actions that cause, or are caused by, the design basis event requiring the safety function.

The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function.

5. Requirements

In applying the single-failure criterion to the design of safety systems, certain conditions are implicit. These conditions are described in 5.1ñ5.6.

Copyright © 2001 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

5.1 Independence and redundancy

The principle of independence is basic to the effective utilization of the single-failure criterion. The design of a safety system shall be such that no single failure of a component will interfere with the proper operation of an independent redundant component or system.

5.2 Nondetectable failure

The detectability of failures is implicit in the application of the single-failure criterion. Detectability is a function of the system design and the specified tests. A failure that cannot be detected through periodic testing, or revealed by alarm or anomalous indication, is nondetectable. An objective in an analysis of safety systems is to identify nondetectable failures. When nondetectable failures are identified, one of the following courses of action shall be taken:

- *Preferred course:* The system or the test scheme shall be redesigned to make the failure detectable.
- *Alternative course:* When analyzing the effect of each single failure, all identified nondetectable failures shall be assumed to have occurred.

5.3 Cascaded failures

Whenever the design is such that additional failures could be expected from the occurrence of a single failure from any source (e.g., mechanical, electrical, and environmental), these cascaded failures, collectively, shall be considered to be a single failure.

5.4 Design basis events

A design basis event that results in the need for safety functions may cause failure of system components, modules, or channels. In order to provide protection from these failures, the equipment should be designed, qualified, and installed so as to be immune to such anticipated challenges. When analysis indicates that failures in a safety system result from design basis events, these failures shall be considered a consequence of the event.

5.5 Common-cause failures

Certain common-cause failures shall be treated as single failures when conducting the single-failure analysis. Such failures can be in dissimilar components and can have dissimilar failure modes. Failures resulting from cascaded failure (see 5.3) and design basis events (see 5.4) have already been discussed, and are those that shall be included in the analysis.

Common-cause failures not subject to single-failure analysis include those that can result from external environmental effects (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference), design deficiencies, manufacturing errors, maintenance errors, and operator errors. Design qualification and quality assurance programs are intended to afford protection from external environmental effects, design deficiencies, and manufacturing errors. Personnel training; proper control room design; and operating, maintenance, and surveillance procedures are intended to afford protection from maintenance and operator errors.

Additionally, provisions should be made to address common-cause failures. Examples of techniques are detailed defense-in-depth studies, failure mode and effects analysis, and analyses of abnormal conditions or events. Design techniques, such as diversity and defense-in-depth, can be used to address common-cause failures.

Copyright © 2001 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

Guidance on using diversity to address common-cause failures in digital computers is provided in IEEE Std 7-4.3.2-1993.

5.6 Shared systems

The single-failure criterion is applied to units with shared systems as follows:

a) The safety systems of all units shall be capable of performing their required safety functions with a single failure assumed within the shared systems or within the auxiliary supporting features or other systems with which the shared systems interface.[5]

b) The safety systems of each unit shall be capable of performing their required safety functions, with a single failure initiated concurrently in each unit within the systems that are not shared.

Provisions shall be included in the design to ensure that single failures within one unit will not adversely affect (propagate to) the other unit, thereby preventing the shared systems from performing the required safety functions.

The failures in criteria (a) and (b) need not be considered simultaneously in the performance of the single-failure analysis, i.e., the single-failure analysis is conducted for the plant to demonstrate that criterion (a) is met. The single-failure analysis is repeated to demonstrate that criterion (b) is met.

6. Design analysis for single failure

A systematic analysis of the design shall be performed to determine whether any violations of the single-failure criterion exist. This clause provides guidance for performing a single-failure analysis. Although the method suggested is not the only way of analyzing a system, it does illustrate an acceptable approach. Other procedures for the performance of the single-failure analysis are described in IEEE Std 352-1987.

6.1 Procedure

For each design basis event, the following steps shall apply:

1) The safety function for which the analysis is to be performed (e.g., reduce power, isolate containment, and cool the core) shall be determined.

2) The protective actions at the system level (e.g., rapid insertion of control rods, closing of containment isolation valves, safety injection, and core spray) that are available to accomplish the safety function shall be determined.

3) The safety groups that will sufficiently satisfy the required safety function shall be determined. For example, either two core spray systems, or one core spray and two low-pressure coolant injection subsystems would be adequate to cool the core.

4) The independence of the safety groups that were established in step (3) shall be verified. This independence shall be verified by observing that there are at least two safety groups that have no shared equipment or points of vulnerability (e.g., relays; switchgear; busses; power sources; less than acceptable separation, location, and arrangement). Once independence is established, redundant capability exists to perform the safety function. It follows then that, for the purpose of satisfying the single-failure criterion, it is not necessary to consider further the potential for failures within the redundant parts.

[5]For example, the same safety system in each unit of a two-unit station shares the same emergency power supply. The shared supply, however, is not rated to supply both systems at the same time. The safety system in each unit is designed with an interlock to prevent certain loads in both units from operating at the same time. The interlock prevents a single failure in one unit from impacting performance of the safety functions in the other unit.

Copyright © 2001 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

NOTEó In some cases, it is not always possible to readily establish independence (e.g., in a two-of-three configured system where redundant channels or divisions are brought together). In other cases, independence is more readily established (e.g., in a one-of-two configured system where channels and divisions are not brought together). For further guidance, see 6.2.1 and 6.2.2.

5) For systems or parts of systems where independence cannot be established, a systematic investigation of potential failures shall be conducted to assure that the single-failure criterion is not violated. Examples of failures include short circuits[6], open circuits, grounds, low ac or dc voltage, and those that would be caused or are the consequences of the application of the maximum credible ac or dc potential.

Electrical, mechanical, and system logic failures shall be considered.

A given component can have different failure modes. Separate analysis shall be conducted for each mode.

The location and arrangement of safety equipment shall be analyzed to determine the effects of common-cause failures.

6.2 Systems portions analysis

When performing the single-failure analysis, certain portions of the safety systems require considerations that may be unique. Potential areas of concern in applying the single-failure criterion to these portions are described in 6.2.1ñ6.2.6.

6.2.1 Interconnections between redundant channels

Interconnections between redundant channels (through devices such as data loggers and test circuitry) are areas where independence could be lost. These interconnections shall be analyzed to assure that no single failure can cause the loss of a safety function. The means for isolating the redundant channels shall be analyzed for single failures that will lead to loss of a safety function.

6.2.2 System logic

The system logic is of particular importance in the single-failure analysis since it is here that redundant channels and redundant actuator circuits may be brought together. The analysis shall verify that no single failure in the system logic will cause failure in the channels or actuation circuits, that would then cause loss of the safety function.

6.2.3 Actuation devices

Those actuators designed to fail in a preferred mode upon loss of power shall be analyzed to assure that no single failure can cause a loss of safety function. For example, failures that will cause power to be maintained incorrectly on the actuator system terminals or cause mechanical binding preventing movement to the preferred position shall be analyzed.

Those actuators designed to apply power when protective action is required shall be analyzed to assure that no single open circuit, short circuit, or loss of power can cause loss of a safety function.

The complete actuator system, which can encompass pneumatic, mechanical, electrical, and hydraulic parts, shall be analyzed for failures that might affect the ability of the system to meet the single-failure criterion. Particular attention shall be directed to assuring that failures in mechanical portions of actuators do not cause

[6]Examples of short circuits, as defined in IEEE 100 [B4], includes connections between two points of the same or different potentials, and a connection of a conductor to ground through an impedance.

Copyright © 2001 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

electrical failures in redundant equipment, and that electrical failures do not cause mechanical failures in redundant equipment.

6.2.4 Electrical power supplies

Power supplies have the potential for causing the loss of safety functions in several ways. For example, a power-supply malfunction resulting in a high voltage could cause failures (such as transistor failures) in redundant channels. A low voltage could cause a loss of redundant channels. Changes in frequency or wave shape could cause set point shifts in redundant channels. The single-failure analysis shall include the entire power supply system, including devices that may shed nonessential loads. For further guidance in this area, see IEEE Std 308-1991.

6.2.5 Auxiliary supporting features

Any auxiliary supporting features that are required for proper operation of any safety system to which the single-failure criterion is applied shall be included in the single-failure analysis as part of its support system. For example, when a portion of a system is dependent on the maintenance of a controlled environment, failure of the environmental system becomes a potential violation of the single-failure criterion, unless it can be shown that failure of the system will not result in loss of the safety function when required.

If the auxiliary supporting features were not designed to meet the single-failure criterion, the ability to complete the required safety function regardless of the loss of the auxiliary supporting feature shall be assured.

6.2.6 Sensing lines

Lines connecting sensors to the process systems (including, for example, reference chambers, equalizing valves, and isolation valves) shall be included in the single-failure analysis.

6.3 Other considerations

6.3.1 Other systems coupled to safety systems

All non-safety systems (e.g., non-safety test circuitry) or other safety systems (e.g., alternate channels) coupled in some manner to safety systems to which the single-failure criterion is applied shall be examined to establish whether any failure within these systems can degrade the safety systems to which they are coupled. If they can degrade any portion of the safety systems to the point of failure, those failures shall be assumed to exist as an initial condition to the single-failure analysis of the safety system. For further guidance in this area, see IEEE Std 384-1992.

6.3.2 Performance of a probabilistic assessment

A probabilistic assessment shall not be used in lieu of the single-failure analysis. However, reliability analysis, probability assessment, operating experience, engineering judgment, or a combination thereof, may be used to establish a basis for excluding a particular failure from the single-failure analysis. For further guidance in performing reliability analyses and probabilistic assessments, see IEEE Std 352-1987 and IEEE Std 577-1976.

6.3.3 Potential for system actuation due to single failure

The potential for system actuation due to single failure shall be examined to determine whether such actuation will constitute an event with unacceptable safety consequences. For any such actuation thus identified as being unacceptable, the single-failure criterion shall be met (i.e., the safety systems must not initiate the actuation as a result of any single detectable failure in addition to all nondetectable failures in the systems).

Copyright © 2001 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)

Bibliography

The following documents provide additional information that may be useful in the application of this standard.

[B1] CFR Publication 10CFR50.49 (1994), Energyó Domestic Licensing of Production and Utilization Facilitiesó Environmental Qualification of Electric Equipment Important to Safety for Nuclear Power Plants.[7]

[B2] CFR Publication 10CFR100 (1994), Energyó R eactor Site Criteria.

[B3] IAEA Safety Series No. 50-P-1 (1990), Application of the Single Failure Criterion.[8]

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

[7]Code of Federal Regulations (CFR) publications are available from the Superintendent of Documents, U.S. Government Printing Office, P.O. Box 37082, Washington, DC 20013-7082, USA.

[8]International Atomic Energy Agency (IAEA) publications are available from IAEA, P.O. Box 100, Wagramer Strasse 5, A-1400 Vienna, Austria (www.iaea.org/).

Copyright © 2001 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