IEEE STANDARDS ASSOCIATION

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

IEEE Power and Energy Society

Sponsored by the
Nuclear Power Engineering Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std **379™-2014**
(Revision of
IEEE Std 379-2000)

IEEE Std 379™-2014
(Revision of
IEEE Std 379-2000)

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

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power and Energy Society

Approved 16 May 2014

IEEE-SA Standards Board

Abstract: Requirements for the application of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power generating safety systems are provided in this standard.

Keywords: actuator, cascaded failure, common-cause failure, design basis event, detectable failure, effects analysis, IEEE 379™, nondetectable failure, 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

PDF: ISBN 978-0-7381-9124-9 STD98660
Print: ISBN 978-0-7381-9125-6 STDPD98660

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

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

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. 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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

Photocopies

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, 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 order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the Safety Systems and Single-Failure Criteria Working Group had the following membership:

Royce Beacom, *Chair*

Gary Johnson
Michael H. Miller
Frank Novak
Tom Richard
Edward Schindhelm
David Theriault
Michael Waterman
David Zaprazny

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

Satish Aggarwal
George Ballassi
Royce Beacom
William Bloethe
Daniel Brosnan
Robert Carruth
Suresh Channarasappa
Tom Crawford
David Curbo
John Disosway
Wells Fargo
Stephen Fleger
Robert Fuld
James Gleason
Dale Goodney
Randall Groves
Ajit Gwal
Daryl Harmon
Hamidreza Heidarisafa
David Herrell
Werner Hoelzl
David Horvath
Peter Hung
Randy Jamison
Ronald Jarrett
Yuri Khersonsky
Robert Konnik
G Lang
Benjamin Lanz
Michael Lauxman
Jang-Soo Lee
Bruce Lord
Greg Luri
John Macdonald
Omar Mazzoni
John Mcalhaney Jr
John Merando
Sujeet Mishra
Michael Newman
Warren Odess-Gillett
Jan Pirrong
Iulian Profir
Ted Riccio
Bartien Sayogo
Glen Schinzel
David Smith
Robert Stark
Gary Stoedter
John Vergis
Michael Waterman
Kenneth White
Yvonne Williams
Tamatha Womack
Paul Yanosy

The Nuclear Power Engineering Committee (NPEC) that recommended approval of this standard had the following membership:

George Ballassi, Chair
James Parello, *Vice Chair*
Steven Fleger, *Secretary*

Ijaz Ahmad
Dheya Al-Othmany
George Attarian
Farouk D. Baxter*
Royce D. Beacom
Mark D. Bowman
Daniel F. Brosnan
Nissen M. Burstein
Keith Bush
Robert C. Carruth
John P. Carter
Suresh Channarasappa
Dennis Dellinger
David R. Desaulniers
John Disosway
Walter F. Emerson
Stephen Fleger
Robert J. Fletcher
Robert Francis
Robert B. Fuld
David Gladey
James F. Gleason
Dale T. Goodney
Robert Hall
Kuljit Hara
Daryl Harmon
David Herrell
Dirk C. Hopp
David A. Horvath
Paul R. Johnson
Christopher J. Kerr
Bok-Ryul Kim
Thomas Koshy
James K. Liming
Bruce A. Lord
John D. MacDonald
J. Scott Malcolm
Alexander Marion*
Michael H. Miller
Edward R. Mohtashemi
Yasushi Nakagawa
Julius Persensky*
Ted Riccio
Mark F. Santschi
Glen E. Schinzel
Zdenko Simic
James E. Stoner, Jr.
Marek Tengler
James E. Thomas
Masafumi Utsumi
Michael Waterman
Edward Wenzinger
John White
Paul L. Yanosy, Sr.
Won Yong Yun
Dave J. Zaprazny
Oon-Pyo Zhu

* non-voting members

When the IEEE-SA Standards Board approved this standard on 16 May 2014, it had the following membership:

John Kulick, *Chair*
David J. Law, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi
Peter Balma
Farooq Bari
Ted Burse
Wael William Diab
Stephen Dukes
Jean-Philippe Faure
Alexander Gelman
Mark Halpin
Gary Hoffman
Paul Houzé
Jim Hughes
Michael Janezic
Joseph L. Koepfinger*
Oleg Logvinov
Ron Petersen
Gary Robinson
Jon Walter Rosdahl
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Patrick Gibbons
IEEE-SA Publishing

Malia Zaman
IEEE-SA Technical Community Programs

Introduction

This introduction is not part of IEEE Std 379™-2014, IEEE Standard for 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™-2009[a]
- Interpret the single-failure criterion as stated in IEEE Std 603-2009
- Provide guidance in the application of the single-failure criterion as stated in IEEE Std 603-2009

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™-2007, IEEE Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations.

The purpose of this revision to the standard is to

- Update the references cited in the text The standard working group has reviewed and identified that "indispensable" references are indeed in Clause 2, as the latest IEEE style manual (2014) directs. The remaining references have been included in the Bibliography (Annex A). This was included as part of the updating process for the standard.

- Verify that the terms not identified in the definitions of this standard (3.1) are identified in the IEEE-SA Standards Definition Database. The activity provides consistency with the latest direction in the IEEE Style Manual (2014).

- Update the standard as a result of changes in other standards resulting from other national and international standards development.

- Address any comments obtained from the user community since the issuance of IEEE Std 379-2000.

- The design basis events subclause (5.4) was revised to clarify design basis events and the involvement of single failures. It does not change the definition and it clarifies that the analysis, previously mentioned, "shall" be done.

- The common-cause failures (CCFs) subclause (5.5) was revised to clarify the description of CCFs. Additional clarifying information added to to clearly state that "Common-cause failures and their failure mechanisms are not normally considered in a single-failure analysis ...."

- Subclause 6.1 was revised to include some of the material on probabilistic assessment from 6.3.2. It was also revised to further describe the systematic analysis that shall be performed to identify single failures and enhance the criteria to be used for the analysis.

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

— Subclause 6.3.2 was removed. Key content is now included in 6.1.

— To try to further promote the understanding of the concept of nondetectable failures and how they are identified differently than detectable failures, Annex B, Examples of Nondetectable Failures, was added. This Annex provides five examples of nondetectable failures in a wide range of applications and technologies used.

Several areas addressed by but not completely developed within this standard continue to evolve and may or may not have applicability to ongoing revisions to this standard:

— *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 revision of the standard describes the manner in which the single-failure criterion should be applied to shared systems. The intent is to neither endorse nor 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:* The scope and purpose of this standard are focused on the application of single-failure criterion including the methods for the associated analysis and providing guidance for identification of these failure types. Common-cause failures and their mechanisms are not part of the scope and purpose of this standard. However, this revision illustrates, by the addition of a figure, the activity to screen CCFs from single failures.

In the future, separate development activities and standards on the subject of common-cause failure should propagate the level of importance of this subject, particularly as it continues to be a major concern in newer technologies. More specifically, comprehensive guidance, standards, and requirements should become more available on CCFs. One example of a standard that includes CCFs is IEEE Std 7-4.3.2™-2010, which addresses the analysis, the design techniques for prevention and the CCFs associated with systems that include computer hardware, software, firmware and interfaces. This will alleviate the inordinate amount of attention this standard receives on this subject if not just for discerning CCFs from single failure. Hopefully then, the future revision of this standard can point to documents that identify the requirements for all preventive measures of CCFs and the factors that they address. This standard then should not and will not be used to discern, analyze or identify CCFs or how to prevent CCFs from occurring.

Contents

IEEE Standard for Application of the Single-Failure Criterio n 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™[1] and the single-failure criterion as stated in that standard.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

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

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

IEEE Std 352™, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.

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

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

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

IEEE Std 741™, IEEE Standard Criteria for the Protection of Class 1E Power Systems and Equipment in Nuclear Power Generating Stations.

3. Definitions, acronyms, abbreviations, and terms

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause. [4]

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

NOTE—Examples of prime movers are turbines, motors, and solenoids. Examples of driven equipment are control rods, pumps, and valves.[5]

---

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

[2] 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/).

[3] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

[4] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

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

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

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.

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.

common-cause failure (CCF): Loss of function to multiple structures, systems, or components due to a shared root cause.

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

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.

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

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.

NOTE—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).

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

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

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

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.

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.

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

---

[5] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

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.

NOTE—A 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.

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

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

— The integrity of the reactor coolant pressure boundary

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

— The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to regulatory guidelines [B2][6]

NOTE 1—The classification of safety electrical equipment is Class 1E as defined in IEEE Std 603.

NOTE 2—This definition of *safety system* agrees with the definition of *safety-related system* used by the Code of Federal Regulations in Title 10, part 50.2 [B1].

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.

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

NOTE—This definition includes the following:

— Systems that are simultaneously shared by both units

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

— 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

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, three of four).

3.2 Word usage

In this document, the word *shall* is used to indicate a mandatory requirement. The word *should* is used to indicate a recommendation. The word *may* is used to indicate a permissible action. The word *can* is used for statements of possibility and capability.

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

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:

— Any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures

— All failures caused by the single failure

— 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

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 an alarm or anomalous indication is nondetectable. An objective in an analysis of safety systems is to identify nondetectable failures. Nondetectable failures should be identified by performing an evaluation of the safety system design that includes postulated component level failures and evaluating the effects of these failures including the ability to detect them. Some designs include redundant components to mitigate the effects of a failure, to improve system availability, or to support maintenance without impacting system availability. When evaluating the effects of a failure in such a configuration, care shall be taken to identify components whose failure will not be revealed by periodic test, alarm or anomalous indication.

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, these cascaded failures shall be included in the single-failure analysis.

5.4 Design basis events

A design basis event that results in the need for safety functions may cause consequential failures of system components, modules, or channels. In order to provide protection from these failures, the safety equipment is designed, qualified and installed to provide protection from such anticipated challenges. An analysis shall be performed to determine the consequences of safety system failures resulting from design basis events. For a system to meet the single-failure criterion, it shall be shown that the required safety function can be performed in the presence of these event-caused failures, all identifiable nondetectable failures, and any other single failure.

5.5 Common-cause failures

The requirement for a safety system to function in the presence of common-cause failures (CCFs) is beyond the scope of the application of single-failure criterion and, therefore, this standard. However, it is important to screen out the potential CCFs when performing a single-failure analysis. As part of evaluating the overall reliability of safety systems, IEEE Std 352 extends the qualitative analysis beyond that which is done for failure modes and effects analysis (FMEA), or fault tree analysis, by considering CCFs. Therefore, an extended qualitative analysis described in IEEE Std 352 should be used to identify and screen out common-cause failure mechanisms not normally considered in an analysis of independent component failures.

Common-cause failures not subject to single-failure analysis include causative factors from external environmental effects (e.g., voltage, frequency, radiation, temperature, humidity, pressure, vibration, and electromagnetic interference). Also, equipment 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. Finally, for digital safety systems, vulnerabilities to CCFs are assessed via the diversity and defense-in-depth associated with the safety system. IEEE Std 352 includes these causative factors contributing to CCFs and the possible preventative measures used to screen out these potential CCFs. The screening process is shown in Figure 1. Other failures may be identified that do not have preventative measures. These failures should be treated as single failures and should be included in the single-failure analysis

Digital safety system vulnerabilities to CCFs are assessed via the diversity and defense-in-depth associated with the safety system. Guidance on using diversity and defense-in-depth to address CCFs in digital computers is provided in IEEE Std 7-4.3.2.

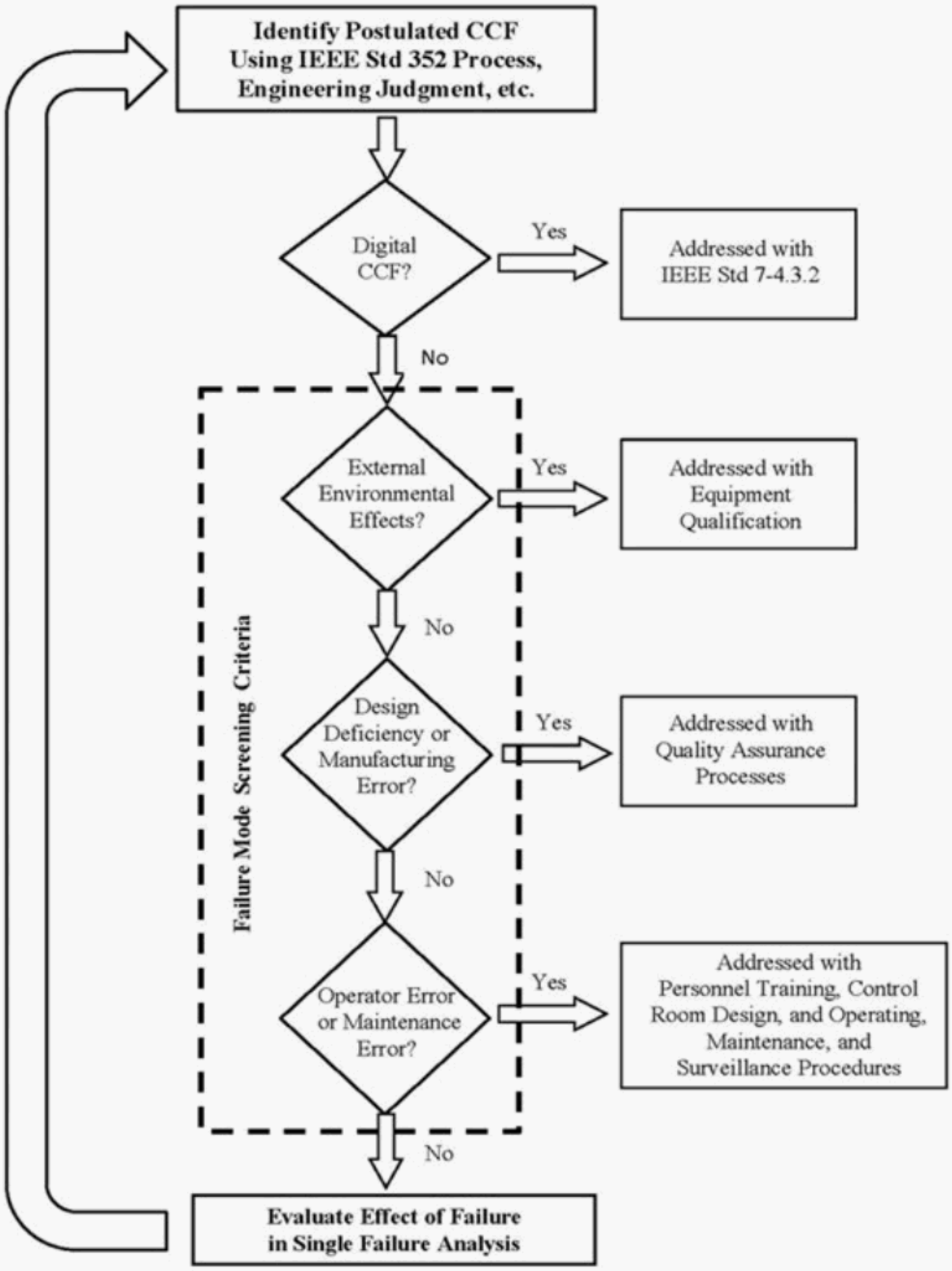

Figure 1—Flowchart for screening CCFs from single failures

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.[7]

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 help 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 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 a) is met. The single-failure analysis is repeated to demonstrate that b) is met.

6. Design analysis for single failure

6.1 General

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.

6.2 Procedure

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

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

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

c) 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 to cool the core.

d) A systematic analysis shall be performed to identify the single failures to be applied in single failure analysis to determine their effect on the protective actions. The possible effects on protective actions by data communications in digital systems is discussed in the Single-Failure

[7]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.

Criterion Section of IEEE Std 7-4.3.2. Examples of failures include short circuits[8], open circuits, grounds, low ac or dc voltage, loss of ac or dc, and those that would be caused or are the consequences of the application of the maximum credible ac or dc potential.

e) The independence of the safety groups that were established in c) shall be verified. This independence shall be verified by observing that there are sufficient 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, the single-failure analyses shall assume each of the failures identified in d) occurs within one of the redundant parts to assure that the single-failure criterion is not violated.

NOTE— 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 may be more readily established (e.g., in a one-of-two configured system where channels and divisions are not brought together). For further guidance, see 6.3.2 and 6.3.3.

f) For systems or parts of systems where independence cannot be established, the single-failure analysis shall assume each of the failures identified in d) occur within the redundant parts to assure that the single-failure criterion is not violated.

g) A reliability analysis, probability assessment, operating experience, engineering judgment, or a combination thereof, may be used to identify the scope of the single-failure analysis. A probabilistic assessment shall not be used in lieu of the single-failure analysis. For further guidance in performing reliability analyses and probabilistic assessments, see IEEE Std 352 and IEEE Std 577.

h) Electrical, mechanical, and system logic failure modes shall be considered in the single-failure analysis.

i) The maintenance bypasses, shared systems, interconnected equipment, equipment in proximity and interactions with other systems shall be considered in the single-failure analysis.

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

6.3 Analysis of portions of systems

6.3.1 Background

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 6.3.2 through 6.3.7.

[8] Examples of short circuits include connections between two points of the same or different potentials, and a connection of a conductor to ground through an impedance.

6.3.2 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.

6.3.3 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.

6.3.4 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 a safety function. For example, failures that cause power to be maintained incorrectly on the actuator system terminals (or air pressure to be unintentionally maintained to the actuator) 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, electronic, 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 electrical failures in redundant equipment, and that electrical failures do not cause mechanical failures in redundant equipment.

6.3.5 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 setpoint shifts in redundant channels. The single-failure analysis shall include the entire power supply system, including devices that shed nonessential loads. For further guidance in this area, see IEEE Std 308 and IEEE Std 741.

6.3.6 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 are 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.

6.3.7 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.

6.4 Other considerations

6.4.1 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.

6.4.2 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).

Annex A

(informative)

Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] U.S. Code of Federal Regulations, Title 10, Part 50, Section 2, Definitions.[9]

[B2] U.S. Code of Federal Regulations, Title 10, Part 100, Reactor Site Criteria.

[B3] USNRC IE Bulletin 80-20, "Failures of Westinghouse Type W-2 Spring Return to Neutral Control Switches," July 31, 1980 (Accession No. ML031210671).[10]

[B4] USNRC Information Notice 85-18, Supplement 1, "Failures of Undervoltage Output Circuit Boards in the Westinghouse-Designed Solid State Protection System," September 10, 1991 (Accession No. ML082670498)..

[B5] USNRC Licensee Event Report, 94-005-01, "Design Defect in Safeguards Bus Sequencer Test Logic Places both Units Outside the Design Basis," February 9, 1995 (Accession No. ML9502220392).

[B6] USNRC NUREG/CR-5404, Auxiliary Feedwater System Aging Study, June 1993 (Accession No. ML040360301).

[B7] USNRC NUREG/CR-5762, Comprehensive Aging Assessment of Circuit Breakers and Relays, March 1992 (Accession No. ML041280568).

[9] Codes 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.

[10] These documents are publically available in the NRC Agencywide Documents Access and Management System (ADAMS) using the ADAMS Accession number or document identifier (e.g. ML11241A096, NUREG-1620, NUREG/CR-1184, SECY-12-0028, or RIS 12-02). Public web-based access to ADAMS can be found at http://www.nrc.gov/reading-rm/adams.html

Annex B

(informative)

Examples of nondetectable failures

B.1 Background

Detectable failures are failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Failures that are undetectable cannot be identified by the means that detectable failures are identified. These nondetectable failures would be significant to the single-failure analysis. Also, nondetectable failures differ from detectable failures in that they may exist in a protection system for years. In fact, they could have been built into the system by the manufacturer. When nondetectable failures are identified, the preferred course of action is to redesign the system or component to make the failure detectable as explained in 5.2. The following are examples of several different equipment types with nondetectable failures at the time they were discovered.

B.2 Three-position switch

An example of a failure that was not periodically tested nor revealed by anomalous indication was the problem with a malfunctioning three-position spring-return-to-neutral control switch. Although the switch was in its proper neutral position when it malfunctioned, depending on how the indicating light circuit was wired, loss of continuity through the neutral position contact of the switch could remain undetected (i.e., indicating light not readily visible to the operator) until the equipment associated with the switch was called upon to operate [B3].

This was a nondetectable failure as it was not “detected through the periodic testing or revealed by alarm or anomalous indication” per 5.2. The preferred course of action, as 5.2 also states, was to “redesign the test scheme” by performing regular continuity tests. Also, in this case, the “system was redesigned” to provide a visible status indicating light.

B.3 Circuit board

Short-circuit failures of the undervoltage (UV) output circuit boards in a solid-state protection system (SSPS) would result in the loss of automatic reactor trip redundancy; the unavailability of both UV output circuits would result in the loss of the automatic trip function of the reactor protection system. Because the UV output circuits are not continuously monitored for failure and because each UV output circuit is functionally tested on a 60-day cycle, one of the two redundant UV output circuits could be inoperable for as long as 60 days before the failure would be detected. Also, the concern was that this function was not single-failure proof by one SSPS train being tested, and the other train could be shorted. In that scenario, an automatic reactor trip cannot occur [B4].

In the particular plant event, the investigation found that maintenance conducted on components that were not related to the SSPS could cause nondetectable failures of the UV output driver card. It was found that the post maintenance testing procedure had to be changed because it was incapable of identifying that the UV output driver card failed during the maintenance activities. In other words, this nondetectable failure was identified and the action was to “redesign the test scheme” (per 5.2).

B.4 Valve

In a study to assess the extent to which current utility practices are able to detect degradation or failure within a safety related system with assistance from a cooperating utility, the NRC reviewed an Auxiliary Feedwater System (AFW) system design and the operating, maintenance, and testing program. After establishing failure modes and reviewing test procedures that implement associated technical specification surveillance requirements, the NRC and utility identified a number of potential sources of nondetectable failures (or degradation) that could exist and not be detected by the existing practices or tests. These potential sources are:

— *System boundary interactions:* Potential failures that would not be detectable involve multi-component or system boundary interactions, where testing of individual components does not adequately indicate the system condition (e.g., automatic steam supply transfer sequence fails when a valve is required to close and reopen).

— *Number or duration of tests:* Most potential failure sources that are not detectable by current practices could be detected with some additional testing from the standpoint of number or duration of tests (e.g., corroded contacts fail to open or close).

— *Excessive testing:* Testing can be excessive to the point that the testing itself is a major contributor to aging and service wear-related degradation [B6].

Recommendations as a result of this study were made for improved diagnostic methods and test procedures that will verify full operability without degrading the installed equipment or system. As per 5.2, the test schemes were redesigned to make the failures detectable.

B.5 Digital system

A programmable logic controller (PLC) load sequencer for the diesel generators in one nuclear power plant unit failed to respond to a safety injection (SI) signal from the site's other unit because of a defect in the sequencer software logic. (The first unit was operating; the other unit was in an outage doing an Integrated Safeguards Test.) The defect could inhibit any or all of the four diesel generator load sequencers from responding to input signals. The problem arose in trying to design the sequencers so that if an emergency signal is received while the sequencer is being tested, the test signal would clear and the engineering safety features controlled by the sequencer would be activated. As implemented, if an SI signal is received 15 s or later into particular test scenarios, the test signal would be cleared but the inhibit signal preventing actuation would be maintained by latching logic. Thus, if an emergency signal arrived more than 15 s into a test scenario, the test signal would clear but the inhibit logic would continue to be held locked in and actuation would be prevented [B5].

The actuation prevention existed in both the manual and self-testing modes of the sequencer operation because the logic designer and independent verifier failed to recognize interactions between some logic inhibits and test logic. This made the failure nondetectable. A subsequent review concluded that not all sequencer functions were validated during all modes of automatic and manual testing in the original verification and validation process. A "system redesign" was implemented to eliminate the software logic problems during the next refueling outage, which is one of the preferred courses of actions in this standard.

B.6 Aging mechanisms

Aging has been shown to be a significant generator of failure mechanisms that are identifiable by other testing, but are not detectable by conventional inspection, surveillance, and monitoring. This has been supported by a comprehensive aging assessment of relays and circuit breakers that was completed as part of the NRC Nuclear Plant Aging Research (NPAR) Program. Relays and circuit breakers were analyzed because they are important safety-related equipment that performs critical functions in the operation and control of nuclear power plants [B7].

A recommendation of the study was that additional methods and practices be implemented for the testing of relays and breakers. Additional methods would include infrared temperature measurement and inrush current and vibration testing. This “redesign,” per 5.2, of the testing methods would increase the assurance that aging degradation can now be detected and mitigated to the extent possible.