

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

Sponsor

**Nuclear Power Engineering Committee
of the
IEEE Power Engineering Society**

Approved 1 July 1998

IEEE-SA Standards Board

Abstract: Minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems are established. The criteria are to be applied to those systems required to protect the public health and safety by functioning to mitigate the consequences of design basis events. The intent is to promote safe practices for design and evaluation of safety system performance and reliability. Although the standard is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, post-accident monitoring display instrumentation, preventative interlock features, or any other systems, structures, or equipment related to safety.

Keywords: actuated equipment, associated circuits, Class 1E, design, failure maintenance bypass, operating bypass, safety function, sense and command features, sensor

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1998 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1998. Printed in the United States of America.

ISBN 0-7381-0326-8

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

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. 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.

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.

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 all 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 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.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

(This introduction is not a part of IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.)

This standard establishes minimum functional design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems. These criteria are established to provide a means for promoting safe practices for design and evaluation of safety system performance and reliability. However, adhering to these criteria will not necessarily fully establish the adequacy of any safety system's functional performance and reliability; nonetheless, omission of any of these criteria will, in most instances, be an indication of safety system inadequacy.

Application

The criteria established by this standard apply to those systems defined as safety systems and do not necessarily apply to all of the systems, structures, and equipment required for complete plant safety. Although the scope is limited to safety systems, many of the principles may have applicability to equipment provided for safe shutdown, accident monitoring display instrumentation, preventive interlock features, or any other systems, structures, or equipment related to safety, or all of the above.

To determine those systems subject to these criteria, an analysis of the overall plant response to postulated design basis events shall be performed. Good engineering judgment should be exercised in this analysis to assure that adequate margins exist in the design to protect the health and safety of the public without imposing unduly restrictive criteria on the design.

Interdisciplinary approach

The safety system criteria herein are established using a systems approach to the design of the power, instrumentation, and control portion of the safety system, as opposed to a specific engineering discipline approach (that is, electrical, mechanical, or civil). It is recognized that the safety functions cannot be accomplished without mechanical, as well as electrical equipment and circuitry. It shall also be recognized that some safety functions may be implemented using digital computers and computer programs. Therefore, the design by other disciplines should consider these criteria. In order for the safety system to meet the requirements of this standard and the supportive standards, the aggregate design of the safety system (without regard to discipline) may be constrained. For example, the consideration of common cause failure is an item that requires an interdisciplinary review and design solution. Such constraints are themselves implicit interface requirements imposed upon the individual constituent parts to enable the entire safety system to meet these requirements. The areas where this standard interfaces with other standards are shown in Figure 1.

While this standard takes a systems approach to the design of the power, instrumentation, and control portion of the safety system, it does not attempt to establish new or different criteria for mechanical equipment or components. Such an attempt by a user is a misapplication of this standard. Nor does this standard attempt to establish the system-level requirements that may be required by mechanical or civil equipment; for example, in-service inspection of piping is intentionally excluded. This standard provides criteria for the safety system without conflicting with existing standards. This standard is not intended to duplicate or conflict with component design requirements such as the ASME Boiler and Pressure Vessel Code. Rather, this standard is to complement and interface with such documents. This standard and others (for example, ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983) establish systems criteria while other codes and standards establish detailed design requirements necessary to ensure the functional adequacy of the individual constituent parts of the safety system.

Evolution

This standard was evolved from IEEE Std 603-1980, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. It represents the sixth Subcommittee 6 (SC-6) publication of a systems criteria document. The series began with IEEE Std 279-1968, a trial-use standard for protection systems, followed by IEEE Std 279-1971, a standard for protection systems; IEEE Std 603-1977, a trial-use standard for safety systems; IEEE Std 603-1980 and IEEE Std 603-1991, a standard for safety systems.

Relationship to other standards

This standard establishes functional and design criteria that are general in nature. It requires supportive standards containing both general and detailed criteria to comprise a minimal set of requirements for the safety system.

Other IEEE standards prepared in support of the criteria of this standard are referenced throughout this standard. The American National Standards, in particular ANSI/ANS 51.1-1983 and ANSI/ANS 52.1-1983, also contain functional and design criteria for safety systems.

International standard IEC 60231A (1969-01) [B7]¹ also contains functional and design criteria for safety systems.

The definition of the term “safety system” in Section 2 references 10 CFR Part 100. This definition is the same as used by other groups, such as, the ANS and ISA. This is per agreements made with the other organizations.

Purpose of revision

The purpose of this revision is to clarify the application of this standard to computer-based safety systems and to advanced nuclear power generating station designs. This revision provides guidance for the treatment of electromagnetic interference (EMI) and radio-frequency interference (RFI), clarifies definitions (e.g., “Class 1E”), and updates references.

IEEE Std 7-4.3.2-1993 provides additional guidance on applying the safety system criterion specified by this standard for the use of computers as components in safety systems.

Future work

In the future, consideration will be given to incorporating the requirements of IEEE Std 494-1974 [B9] into this standard.

The subcommittee recognizes that the term “Class 1E” is sometimes misapplied. A note was added in the 1991 revision of this standard to clarify the use of the term. The subcommittee will continue to review the definition of “Class 1E” to ensure clarity.

The subcommittee also recognizes the terms division, channel, and train have interchangeable definitions in different industry standards. The terms division and channel were clarified in this standard. The subcommittee will review other industry standards to ensure clarity.

Further clarification of the criteria used to determine reliability goals, as discussed in Clause 4 item i) and 5.5 of this standard, will also be considered.

¹The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex C.

Consideration will be given to providing additional guidance or reference(s) to address electromagnetic interference.

The requirements for accident monitoring instrumentation, contained in ANS 4.5-1989 and IEEE Std 497-1981, are currently undergoing revision. References to IEEE Std 497-1981 are made in Clause 4 item e), and 5.8 of this standard. The criteria in ANS 4.5-1989 and in IEEE Std 497-1981 are being combined and updated in a new revision to ANS 4.5-1989. The revised ANS 4.5 standard will contain criteria that addresses the use of computerized displays and developments in human factor designs. The user is advised that updated criteria may provide useful guidance. The approved ANS 4.5 will be incorporated into the next revision of this standard.

Participants

This document was prepared by the Safety-Related Systems Working Group Subcommittee 6.3 of the IEEE Nuclear Power Engineering Committee. At the time this standard was prepared, the working group had the following membership:

David J. Zaprazny, Chair

Ron E. Battle
Wes W. Bowers

Clifford K. Doult
Edward F. Dowling
Pat M. Duggan

Britton P. Grim
Rick Kendall

The following persons were on the balloting committee:

Satish K. Aggarwal
Vincent P. Bacanskas
Farouk D. Baxter
Wes W. Bowers
Daniel F. Brosnan
Nissen M. Burstein
S. P. Carfagno
Robert C. Carruth
Raymond J. Christensen
Robert L. Copyak
J. J. Disosway
Gary L. Doman
Edward F. Dowling

Rich E. Dulski
Surinder Dureja
Jay Forster
J. R. Fragola
John M. Gallagher
Wil C. Gangloff
Luis C. Gonzalez
Lawrence P. Gradin
John Greene
Britton P. Grim
Robert E. Hall
Joe T. Hazeltine
Gregory K. Henry
Sonny Kasturi

James T. Keiper
Alex Marion
John R. Matras
R. B. Miller
Burt Nemroff
Neil P. Smith
Peter B. Stevens
Peter Szabados
James E. Thomas
Raymond Weronick
G. O. Wilkinson
David J. Zaprazny
Mark S. Zar

The final conditions for approval of this standard were met on 1 July 1998. This standard was conditionally approved by the IEEE-SA Standards Board on 25 June 1998, with the following membership:

Richard J. Holleman, *Chair*

Donald N. Heirman, *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Clyde R. Camp
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Thomas F. Garrity
Ruben D. Garzon

James H. Gurney
Jim D. Isaak
Lowell G. Johnson
Robert Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Jim Logothetis
Donald C. Loughry

L. Bruce McClung
Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Catherine K.N. Berger
IEEE Standards Project Editor

Contents

1.	Scope.....	1
1.1	Illustration.....	1
1.2	Application.....	2
2.	References.....	4
3.	Definitions.....	5
4.	Safety system design basis.....	8
5.	Safety system criteria.....	9
5.1	Single-failure criterion.....	9
5.2	Completion of protective action.....	9
5.3	Quality.....	9
5.4	Equipment qualification.....	10
5.5	System integrity	10
5.6	Independence	10
5.7	Capability for testing and calibration.....	11
5.8	Information displays	11
5.9	Control of access.....	12
5.10	Repair	12
5.11	Identification	12
5.12	Auxiliary features.....	12
5.13	Multi-unit stations.....	13
5.14	Human factors considerations.....	13
5.15	Reliability.....	13
5.16	Common cause failure criteria.....	13
6.	Sense and command features—functional and design requirements.....	13
6.1	Automatic control	13
6.2	Manual control	14
6.3	Interaction between the sense and command features and other systems	14
6.4	Derivation of system inputs	15
6.5	Capability for testing and calibration.....	16
6.6	Operating bypasses	16
6.7	Maintenance bypass	16
6.8	Setpoints.....	16
7.	Execute features (functional and design requirements).....	17
7.1	Automatic control	17
7.2	Manual control	17
7.3	Completion of protective action.....	17
7.4	Operating bypass.....	17
7.5	Maintenance bypass	17

8. Power source requirements	18
8.1 Electrical power sources	18
8.2 Non-electrical power sources.....	18
8.3 Maintenance bypass	18
Annex A (informative) Illustration of some basic concepts for developing the scope of a safety system.....	19
Annex B (informative) Electromagnetic compatibility.....	27
Annex C (informative) Bibliography	31

IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations

1. Scope

The criteria contained in this standard establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations. To satisfy the criteria in this standard, interface requirements may be imposed on the other portions of the safety system as shown in Figure 1. Safety system functional and design criteria are also contained in other standards.¹

1.1 Illustration

Figure 2 illustrates the scope of this standard in the form of a 3×3 matrix. The labeling across the top of the matrix illustrates that the safety systems can be subdivided into the three general elements of sense and command features, execute features, and power sources. These general elements represent a grouping of devices that provides similar performance characteristics for many discrete safety functions. The labeling on the left side of the matrix illustrates that the safety systems can also be subdivided into the three operational elements of reactor trip system and engineering safety features, auxiliary supporting features, and other auxiliary features. When viewing an entire row of the matrix, it can be seen that an operational element may form a system.

Illustrating the scope of this standard in matrix form shows that each operational element contains one or more general elements. This matrix should not be interpreted to mean that every operational element shall contain all of the general elements or that a particular general element is limited to application in only one operational element.

Figure 3 illustrates typical equipment examples for each portion of the matrix diagram. As shown, some components can be fitted into more than one category depending on the component's use.

Figure 4 illustrates where criteria for each portion of the matrix can be found in this standard.

¹See Clause 2 and Annex C for applicable standards.

1.2 Application

The safety system criteria established herein are to be applied to those systems required to protect the public health and safety by functioning to prevent or mitigate the consequences of design basis events. However, this standard does not apply to all of the systems, structures, and equipment required for complete plant safety, for example, fire protection systems.

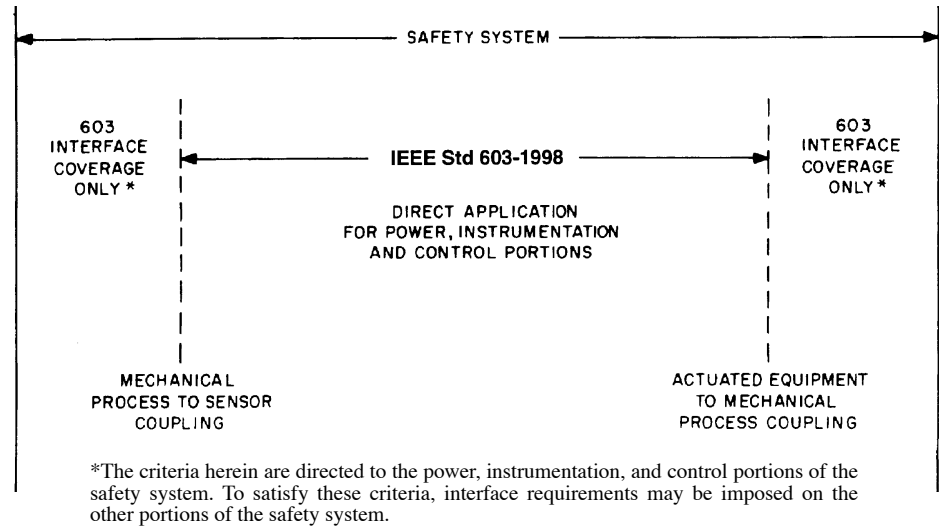


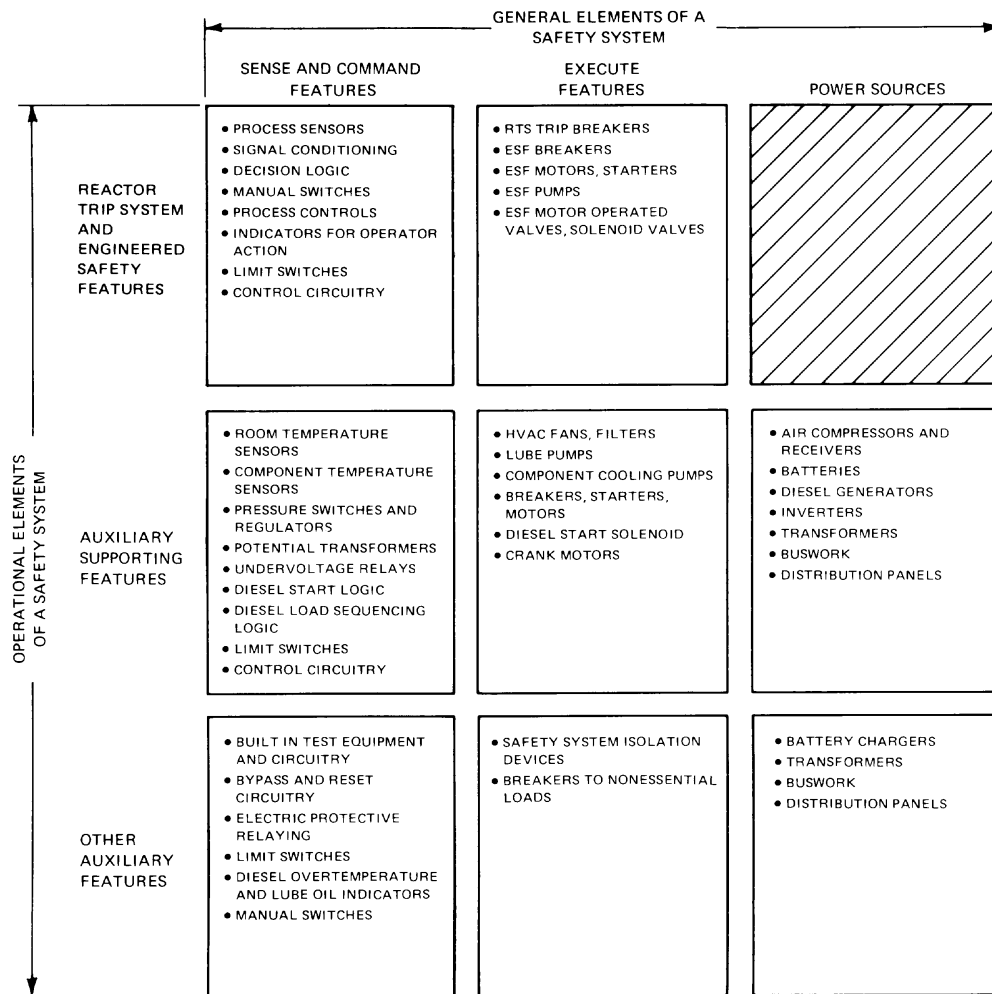
Figure 1—Nonelectrical interface scope diagram

GENERAL ELEMENTS OF A SAFETY SYSTEM			
OPERATIONAL ELEMENTS OF A SAFETY SYSTEM	SENSE AND COMMAND FEATURES	EXECUTE FEATURES	POWER SOURCES
	REACTOR TRIP SYSTEM AND ENGINEERED SAFETY FEATURES		See Note 2
	AUXILIARY SUPPORTING FEATURES		
	OTHER AUXILIARY FEATURES		

- NOTES
- 1—The protection system of IEEE Std 279-1971 [B8]² and of this standard is the sense and command features for the reactor trip system and the engineered safety features.
- 2—Power sources, by definition, are considered auxiliary supporting features or other auxiliary features and, therefore, are not shown as part of the reactor trip system and engineered safety features.
- 3—When viewing an entire single row of the matrix, it can be seen that an operational element may form a system; for example, a service water system. However, when viewing an entire column, general elements represent a grouping of devices that provide similar performance characteristics (e.g., sensors) for many discrete safety functions.
- 4—Each operational element contains one or more general elements. Every operational element does not necessarily contain all of the general elements.
- 5—A device that serves as a general element is not necessarily limited to application in only one operational element.

Figure 2—3 × 3 matrix representation of safety system

²The numbers in brackets preceded by the letter B correspond to those of the bibliography in Annex C.



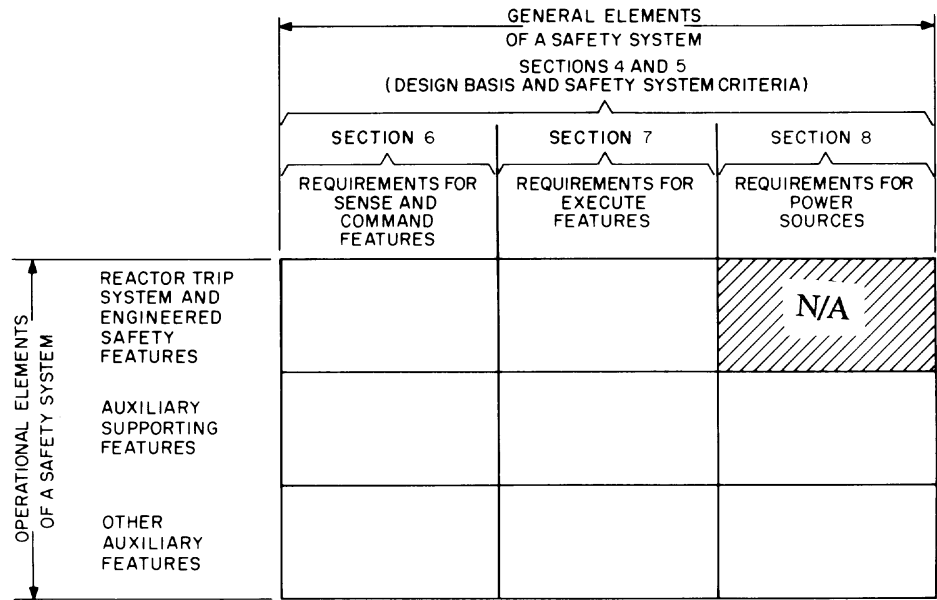
NOTES

1—The items listed are only representative examples as to inclusion or location in the matrix.

2—See Figure 2 for additional notes.

3—Computer hardware, firmware, and programs are representative examples as to inclusion or location in the matrix.

Figure 3—Examples of equipment fitted to safety system scope diagram



NOTE—See Figure 2 for notes.

Figure 4—Scope diagram for IEEE Std 603-1998

2. References

This standard shall be used in conjunction with the following publications. When the following standards are superseded by an approved revision, the revision shall apply.

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.

ANSI/ISA S67.04-1994, Setpoints for Nuclear Safety-Related Instrumentation.⁴

ASME NQA-1-1994, Quality Assurance Program Requirements for Nuclear Facilities.⁵

IEEE Std 7-4.3.2-1993, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.⁶

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

³ANSI/ANS publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

⁴ANSI/ISA publications are available from 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709, USA or from the American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

⁵ASME publications are available from the American Society of Mechanical Engineers, 22 Law Drive, Fairfield, NJ 07007, USA.

⁶IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.