IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

IEEE Power & Energy Society

Sponsored by the
Nuclear Power Engineering Committee

692™

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

12 February 2010

IEEE Std 692™-2010
(Revision of
IEEE Std 692-1997)

IEEE Std 692™-2010
(Revision of
IEEE Std 692-1997)

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power & Energy Society

Approved 2 February 2010
IEEE-SA Standards Board

Abstract: Criteria are provided for the design of an integrated security system for nuclear power generating stations. Requirements are included for the overall system, interfaces, subsystems, and individual electrical and electronic equipment. This standard addresses equipment for security-related detection, surveillance, access control, communication, data acquisition, and threat assessment.
Keywords: access control, central alarm station (CAS), cyber security, duress alarms, integrated security system, intrusion detection, line supervision, perimeter intrusion alarm, portal security lighting, remote video surveillance, secondary alarm station (SAS), security lighting, security systems, threat assessment, uninterruptible power supply (UPS) system, voice communications

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

PDF: ISBN 978-0-7381-6201-0 **STD96036**
Print: ISBN 978-0-7381-6202-7 **STDPD96036**

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 or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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 his or her 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.

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. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the 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, explanation, or interpretation of the IEEE.

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. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

Introduction

This introduction is not part of IEEE Std 692-2010, IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations.

The physical protection and security of nuclear power generating stations concerns utilities, manufacturers, the general public, and those who are responsible for licensing and regulating nuclear power generating stations and other nuclear facilities. This standard is intended to establish both guidance and minimum requirements for acceptable security system design for nuclear power generating stations. This standard focuses on the design, operation, and maintenance of various security-related electrical and electronic equipment, including integration to achieve an acceptable security system. As described in this standard, to be effective, the electrical and electronic aspects of such an integrated security system need to include 11 essential elements:

- Perimeter intrusion alarms
- Security lighting
- Video surveillance
- Access control
- Interior intrusion detection
- Data acquisition, processing, and display
- Voice communications
- Line supervision
- Duress alarms
- Power supplies
- Maintenance and testing

The integrated security system and each of these 11 elements are addressed in separate clauses of this standard.

The development of these criteria was initially undertaken in January 1978. The standard was originally issued in 1986 and then updated in 1997 and later reaffirmed in early 2005. In September 2005, Working Group 3.2 (Nuclear Security) of Nuclear Power Engineering Committee's Subcommittee 3 (Operations, Maintenance, Aging, Testing, and Reliability) was directed to undertake another update of the standard.

This new revision incorporates the following improvements and updates:

- Update of the Introduction
- Development of high-level design basis requirements for the integrated security system and each of its 11 elements
- Re-format and revision of each clause to achieve improved consistency, clarity, usability, and level of detail
- Update of definitions to reflect current security term usage
- Update of terminology throughout the standard to reflect current industry usage
- Update of each of the four figures to reflect current industry approaches
- Deletion of several overly prescriptive requirements in favor of performance-based approaches

— Deletion of references to obsolete technology and replacement with current state-of-the-art usage

— Update and validation of guidance and requirements in Clause 4, Clause 5, Clause 6, and Clause 7 on threat assessment

— Update of Clause 6 to address IESNA comments on the 1997 version, to reflect current approaches, and to provide guidance on maintaining minimum illumination levels throughout the life of the plant

— Addition of guidance in Clause 4 and Clause 10 on addressing cyber security issues

— Addition of new requirement to consider duress alarms in badging areas that are located outside the Protected Area

— Update of bibliography

This revision is intended primarily to assist development of security systems at new nuclear power generating stations but may also be helpful for design modification efforts at older plants and at other nuclear facilities. The working group attempted to stay abreast of and consistent with the rapidly changing security requirements evolving after the September 11, 2001 terrorist event in the U.S., but at the same time avoided the level of detail that could compromise any safeguard aspects of such changes.

Note that this standard is not intended to cover all security-related topics. An understanding of the goals and objectives of the security system with an appreciation for the financial, operational, testing, and maintenance functionality of the site will enhance the compatibility of the various plant systems, features, and operator actions required to mitigate events such as radiological, fire, loss of site power, and security events. The plant layout shall be compatible with the need to control access and maintain separation of areas due to pipe break accident, missiles, fire, radiation exposure, and flooding considerations. Physical protection measures should be incorporated into the design prior to the start of construction to enhance physical protection and non-obtrusive security system installation and to minimize cost.

Consequently, such features as listed below should be incorporated in the initial design:

— Embedment of card readers/conduit

— Hardened walls, floors, and ceilings

— Bullet-resistant features

— Minimized utility ports

— Utility port barriers

— Security door hardware

This standard is not intended to cover the following security-related topics:

— Development of threat and response criteria

— Security force composition, deployment, or weaponry

— Classification of vital equipment or vital areas

— Contingency plans

— Security requirements during the plant construction stage

— Personnel screening

— Physical, civil, and structural aspects of security boundaries

— Controls on safeguards information

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

Updating of IEEE documents

Users of IEEE standards 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. 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 Standards Association Web site at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA Web site at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at this URL: http://standards.ieee.org/reading/ieee/interp/index.html.

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 with respect to the existence or validity of any patent rights in connection therewith. 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 standard was submitted to the IEEE-SA Standards Board for approval, the Security Systems Working Group had the following membership:

David A. Horvath, *Chair*

Thomas M. Worrell, *Vice Chair*

Sara E. Seamans, *Secretary*

William D. Drake
Randall H. Flowers
Brian B. Linde
Einar W. Pearson
Paul A. Phelps
Raymond W. Yeager
Deanna J. Zhang

In addition, the working group would like to acknowledge the valuable contributions of David Axt, Frank Carpency, Cliff DuBord, and R.V. Rao to this revision.

At the time this standard was balloted, Subcommittee 3 on Operations, Maintenance, Aging, Testing, and Reliability had the following membership:

George A. Ballassi, *Chair*

Glen E. Schinzel, *Vice Chair*

Ted Riccio, *Secretary*

Tom Crawford
Alireza Daneshpooy
Larry Gradin
Rachel B. Gunnett
Hamidreza R. Heidarisafa
David A. Horvath
Peter J. Kang
Jacob Kulangara
James K. Liming
Jim Parello
Mansoor H. Sanwarwalla
Owen Scott
Craig Sellers
John Stevens
Yvonne Williams
Kiang Zee

At the time this standard was balloted, the Nuclear Power Engineering Committee had the following membership:

Scott J. Malcolm, *Chair*

John D. MacDonald, *Vice Chair*

Satish K. Aggarwal, *Secretary*

Ijaz Ahmad
George Attarian
George Ballassi
Farouk D. Baxter
Mark Bowman
Daniel F. Brosnan
Nissen M. Burstein
Robert C. Carruth
John P. Carter
John Disosway
Stephen Fleger
Robert J. Fletcher
Robert B. Fuld
James Gleason
Dale T. Goodney
William L. Hadovski
David A. Horvath
Paul R. Johnson
Thomas Koshy
Harvey C. Leake
Alexander Marion
Michael H. Miller
James Parello
Mansoor H. Sanwarwalla
Glen E. Schinzel
James E. Stoner Jr.
James E. Thomas
Paul L. Yanosy Sr.
David J. Zaprazny

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

William J. Ackerman
Satish K. Aggarwal
Stan Arnot
George Ballassi
Royce Beacom
Robert Beavers
H. Stephen Berger
Wesley Bowers
Daniel Brosnan
Nissen M. Burstein
Robert C. Carruth
Suresh Channarasappa
Keith Chow
Alireza Daneshpooy
John Disosway
Gary Engmann
Wells Fargo
Stephen Fleger
James Gleason
Randall Groves
Daryl Harmon
Hamidreza R. Heidarisafa
Werner Hoelzl
David A. Horvath
Greg Hostetter
Peter Hung
Randy Jamison
Paul Johnson
James Jones
Piotr Karocki
Chad Kiger
J. Koepfinger
Robert Konnik
William Lumpkins
John MacDonald
Faramarz Maghsoodlou
Kimberly Mosley
Michael S. Newman
James Parello
Einar W. Pearson
Ted Riccio
Bartien Sayogo
Glen E. Schinzel
Sara Seamans
Gil Shultz
David Singleton
James E. Smith
Robert Stark
Rebecca Steinman
S. Thamilarasan
James Thompson
John Vergis
Thomas Worrell

When the IEEE-SA Standards Board approved this standard on 2 February 2010, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

John Barr
Karen Bartleson
Victor Berman
Ted Burse
Richard DeBlasio
Andy Drozd
Mark Epstein
Alexander Gelman
Jim Hughes
Richard H. Hulett
Young Kyun Kim
Joseph L. Koepfinger*
John Kulick
David J. Law
Ted Olsen
Glenn Parsons
Ronald C. Petersen
Narayanan Ramachandran
Jon Walter Rosdahl
Sam Sciacca

*Member Emeritus

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

Howard L. Wolfman, *TAB Representative*
Michael Janezic, *NIST Representative*
Satish K. Aggarwal, *NRC Representative*

Lorraine Patsco
IEEE Standards Program Manager, Document Development

Matthew J. Ceglia
IEEE Standards Program Manager, Technical Program Development

Contents

IEEE Standard Criteria for Security Systems for Nuclear Power Generating Stations

1. Overview

1.1 Scope

The standard provides criteria for the design, testing, and maintenance of security system equipment for nuclear power generating stations. Such equipment includes permanently or temporarily installed systems, subsystems, and components used by the security force for physical protection of the station against security threats. It includes equipment for security-related detection, assessment, surveillance, access control, communication, and data acquisition.

1.2 Purpose

This standard establishes criteria for the design of an integrated security system for nuclear power generating stations. These criteria assist in the selection and application of equipment to detect, monitor, display, and record security conditions and events.

2. Normative references

There are no publications normatively referenced in this standard.