IEEE STANDARDS ASSOCIATION

IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations

IEEE Power and Energy Society

Sponsored by the
Nuclear Power Engineering Committee

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

IEEE Std 692™-2013
(Revision of
IEEE Std 692-2010)

IEEE Std 692™-2013
(Revision of
IEEE Std 692-2010)

IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations

Sponsor

Nuclear Power Engineering Committee
of the
IEEE Power and Energy Society

Approved 23 August 2013

IEEE-SA Standards Board

Abstract: Criteria for the design of an integrated security system for nuclear power generating stations are provided in this standard. 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, CAS, central alarm station, cyber security, duress alarms, IEEE 692™, integrated security system, intrusion detection, line supervision, perimeter intrusion alarm, portal security lighting, remote video surveillance, SAS, secondary alarm station, security lighting, security systems, threat assessment, uninterruptible power supply system, UPS, voice communications

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

PDF: ISBN 978-0-7381-8605-4 STD98363
Print: ISBN 978-0-7381-8606-1 STDPD98363

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 Security Systems Working Group had the following membership:

David A. Horvath, *Chair*
Thomas M. Worrell, *Vice Chair*
Marie-H. Cuvelier, *Secretary*

Randall H. Flowers
Brian B. Linde
T. David Mills
Paul A. Phelps
James E. Vaughn
Raymond W. Yeager

In addition, the working group would like to acknowledge the valuable contributions of Sara E. Seamans and Michael E. Waterman to this revision.

Working Group 3.2 would like to acknowledge and commemorate the instrumental and dedicated efforts of our colleague Einar "Bill" Pearson to our working group. We regret his unfortunate passing in 2011 shortly after this revision was initiated.

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

James K. Liming, *Chair*

Yvonne Williams, *Vice Chair*

Tom Crawford, *Secretary*

Gopal Aravapalli
George A. Ballassi
John Beatty
Thomas Carrier
Suresh Channarasppa
Hamidreza R. Heidarisafa
Sharon Honecker
David A. Horvath
Steven Hutchins
Peter J. Kang
Jacob Kulangara
Robert Lane
Singh G. Matharu
Kirklyn Melson
Joseph Napper
Jim Parello
Vish Patesh
Ted Riccio
Glen E. Schinzel
Zdenko Simic
Rebecca Steinman
John A. Stevens
Yvonne Williams

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

William Ackerman
Satish Aggarwal
Stan Arnot
George Ballassi
Royce Beacom
Robert Beavers
H. Stephen Berger
Wesley Bowers
Daniel Brosnan
Nissen Burstein
Robert Carruth
Suresh Channarasappa
Keith Chow
Alireza Daneshpooy
John Disosway
Gary Engmann
Wells Fargo
Stephen Fleger
James Gleason
Randall Groves
Daryl Harmon
Hamidreza Heidarisafa
Werner Hoelzl
David A. Horvath
Greg Hostetter
Peter Hung
Randy Jamison
Paul Johnson
James Jones
Piotr Karocki
Chad Kiger
Joseph L. Koepfinger
Robert Konnik
William Lumpkins
John MacDonald
Faramarz Maghsoodlou
Kimberly Mosley
Michael S. Newman
James Parello

Einar Pearson
Ted Riccio
Bartien Sayogo
Glen Schinzel
Sara Seamans
Gil Shultz
David Singleton
James Smith
Robert Stark
Rebecca Steinman
S. Thamilarasan
James Thompson
John Vergis
Thomas Worrell

When the IEEE-SA Standards Board approved this standard on 23 August 2013, 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*

Catherine Berger
IEEE Standards Senior Program Manager, Document Development

Malia Zaman
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of IEEE Std 692-2013, IEEE Standard for 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.

The International Atomic Energy Agency (IAEA) defines nuclear security as "the means and ways of preventing, detecting, and responding to sabotage, theft, and unauthorized access to or illegal transfer of nuclear material and other radioactive substances, as well as their associated facilities."[a] "For reactor facilities, the malicious act may target either systems whose failure would cause core damage, leading to radiological consequences, or areas where nuclear fuel (fresh or spent) or radioactive material is kept or stored." The requirements for the development of security systems criteria for nuclear power generating stations are emphasized by international organizations' publications such as the Nuclear Security Series from the IAEA. In particular:

a) IAEA Nuclear Security Series No. 13 *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities* (INFCIRC/225/Revision 5) [B9][b] provides "guidance to States and their competent authority on how to develop or enhance, implement and maintain a physical protection regime for nuclear material and nuclear facilities […] in order to reduce the risk of malicious acts involving that material or those facilities."

b) IAEA Nuclear Security Series No.4 *Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage* [B7] is a technical guidance elaborating "methods for evaluating—and, if necessary, for proposing corrective actions aimed at reducing (mainly through upgrades)—the risk related to any malicious act that, directed against a nuclear power plant, could endanger the health and safety of plant personnel, the public and the environment through exposure to radiation or the release of radioactive substances. These guidelines describe a methodology for assessing the capacity of a selected subset of a nuclear plant's safety related SSCs to withstand sabotage-induced events". Sabotage is defined by the IAEA as "any deliberate act directed against a nuclear facility or nuclear material in use, storage, or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances."[c]

I&C components, electrical, and electronic systems play an important role in the operation of computer and communication networks, intrusion detection, access control systems, and, more generally, in the physical protection of a nuclear facility. The requirements for the design, testing, or maintenance of security systems specific to cyber-security, intrusion detection systems, or access control systems at nuclear facilities have been not only emphasized in IAEA publications but also mandated by regulatory documents including the Code of Federal Regulations (CFR). Among them are the following publications:

c) IAEA Nuclear Security Series No. 17, *Computer Security at Nuclear Facilities* [B8]. This Technical Guidance presents approaches, structures and implementation procedures in order to establish a computer security program specific to nuclear facilities. Evaluation methods for

[a] IAEA Office of Nuclear Security, "IAEA: working to build a global response to a global threat," booklets 12-0921, March 2012, Vienna. http://www.iaea.org/Publications/Booklets/NuclearSecurity/ns0312.pdf.

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

[c] IAEA Office of Nuclear Security, Engineering safety aspects of the protection of nuclear power plants against sabotage: technical guidance. — Vienna, International Atomic Energy Agency, 2007, p. 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 4) STI/PUB/1271 ISBN 92–0–109906–1.

existing programs and risk reduction measures to new cyber-induced vulnerabilities are also detailed in this publication.

d) 10 CFR Part 73.54, *Protection of Digital Computer and Communication Systems and Networks* [B5]. This requires that a cyber-security plan be established to provide protection to digital computer and to communication systems and networks against cyber-attacks.

e) 10 CFR Part 73.55, *Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors against Radiological Sabotage* [B6]. This requires that a physical protection program be established and maintained to provide "high assurance that activities involving special nuclear material (plutonium, uranium-233, and uranium highly enriched in uranium-233 or in uranium-235) are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety." In particular, "the physical protection program must protect against the design basis threat of radiological sabotage" as defined in paragraph 73.1.

f) NUREG-1959, *Intrusion Detection Systems and Subsystems* [B19]. "Intrusion detection and assessment systems are an integral part of any physical protection system. Detection and assessment provide a basis for the initiation of an effective security response." This report provides "information relative to designing, installing, testing, maintaining, and monitoring intrusion detection systems (IDSs) and subsystems used for the protection of facilities licensed by the U.S. Nuclear Regulatory Commission." It contains information on the "application, use, function, installation, maintenance, and testing parameters for internal and external IDSs and subsystems, including information on communication media, assessment procedures, and monitoring. This information is intended to assist licensees in designing, installing, employing, and maintaining IDSs at their facilities."

g) NUREG-1964, *Access Control System* [B20]. "The overall objective of access control is to help ensure that only authorized and properly searched personnel, vehicles, and materials are granted access to, and exit from, areas that require protection." This report provides "technical details applicable to access control methods and technologies commonly used to protect facilities licensed by the U.S. Nuclear Regulatory Commission."

This standard is intended to establish both guidance and minimum requirements for acceptable security system design for nuclear power generating stations worldwide. 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 the following 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. A major revision was completed in 2010. Soon afterward there were changes in the industry that necessitated additional updates to the standard.

This new revision incorporates the following improvements and updates:

- Rearranged the wording and format (e.g., dash list vs. bullet list) in the overall document for improved compliance with the IEEE Standards Style Manual
- Updated the Introduction
- Updated four definitions and added three (*controlled access area, line supervision, single act*) to reflect current security term usage, and deleted three (*legitimate access, remote access, remote control*), which are no longer used in the standard.
- Redrew Figure 1, Figure 2, Figure 3, and Figure 4 for improved clarification
- Revised Clause 4 for consistency with definitions
- Added references for guidance in Clause 4 on design, and cyber security issues
- In Clause 5, allowed the use of fiber optics for perimeter intrusion to credit technology improvement and added a consideration for unattended openings.
- Eliminated prescriptive requirements for lighting in Clause 6, which are now considered unnecessary when considering improved technology for video surveillance now available and being used.
- Added subclauses in Clause 14 providing functional details on various power supply devices
- Reviewed and updated the bibliography to confirm relevance of old standards or to refer to the latest versions of the standards

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. Certain aspects of this standard may also apply to other nuclear facilities (such as fuel cycle, high level nuclear waste, and nuclear weapons) at the discretion of the facility owner or operator. 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 sabotage, 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 reduce 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

Contents

IEEE Standard for 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 electrical, instrumentation, and control 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.