

IEEE Guide for Physical Security of Electric Power Substations

IEEE Power and Energy Society

Developed by the
Substations Committee

IEEE Std 1402™-2021
(Revision of IEEE Std 1402-2000)



IEEE Guide for Physical Security of Electric Power Substations

Developed by the

Substations Committee
of the
IEEE Power and Energy Society

Approved 23 September 2021

IEEE SA Standards Board

This is a Redline document produced by Accuris.

Redlines are designed to save time and improve productivity by using the latest software technology to find and highlight document changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document. This Redline is produced solely by Accuris. The publisher has not prepared this Redline and is not responsible for its accuracy.

Contact:

<https://store accuristech.com/pages/contact.html>

Redline Processing Notes:

1. ~~Red Text~~ - Red strikethrough text denotes deletions.
2. Blue Text - Blue underlined text denotes modifications and additions.

Abstract: Guidance for the physical security of electric power substations is provided in this guide. It addresses a number of threats, including unauthorized access to substation facilities, theft of material, and vandalism. It describes some options for positive access control, monitoring of facilities, and delay/deter features that could be employed to mitigate these threats. This guide also discusses options for different levels of physical security risk for electric power substations. The guide does not establish recommendations based on voltage levels, size, or any depiction of criticality of the substation. The user will make these decisions based on threat assessment and criticality assignment by the substation owner. Large scale overt attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc., are beyond the scope of this guide.

Keywords: access, access control, alarms, fences, IEEE 1402™, intrusion, lighting, monitoring, perimeter fence, perimeter wall, physical security, power substation, security lighting, security plan, substation lighting, substation physical security, substation security, substation threat assessment, theft, threat mitigation, vandalism

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

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 9 November 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

National Electrical Safety Code and NESC are registered trademarks and service marks in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-7992-9 STD24963
Print: ISBN 978-1-5044-7993-6 STDPD24963

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>.

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.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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: THE NEED TO PROCURE 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 is 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, nor 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile and Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

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 constitute 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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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 10 years. When a document is more than 10 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 [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

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 <https://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.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE guide was completed, the E7 Working Group had the following membership:

Arthur Graves, *Chair*
Mark Smedvig, *Secretary*

Greg Ardrey	Keith Graham	Jeremy McNutt
Matthew Bauer	Alan Gaetz	Charles Steven McCarley
Gary Beane	Roderick Giron	Shashikant Patel
Geoffery Biela	Charles Haahr	Craig Preuss
Mike Brown	Paul Kruger	Thomas Proios
Christopher Carson	Charlie (Chun) Li	Alonso Rodriguez
W. Bruce Dietzman	Reginaldo Maniego	Jesse Shank
Brian Farmer	Olivialin Miller	Logan Trombley

The following members of the individual Standards Association balloting group voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman	Piotr Karocki	Michael Richardson
Ali AlAwazi	John Kay	Timothy Robirds
Jay Anderson	Gael Kennedy	Charles Rogers
Thomas Barnes	Yuri Khersonsky	Richard Rohr
Paul Barnhart	Boris Kogan	Bartien Sayogo
George Becker	Jim Kulchisky	Christopher Searles
Steven Bezner	Mikhail Lagoda	Robert Seitz
Thomas Blair	Chung-Yiu Lam	Devki Sharma
Derek Brown	Bruce Mackie	Suresh Shrimavle
Demetrio Bucaneg Jr	Arturo Maldonado	Hyeong Sim
William Byrd	Reginaldo Maniego	Douglas Smith
Thomas Callsen	William McBride	Jerry Smith
Paul Cardinal	Thomas McCarthy	Gary Smullin
Suresh Channarasappa	John McDonald	Joseph Sowell
Michael Chirico	Susan McNelly	Ryan Stargel
Robert Christman	Jeremy McNutt	Andrew Steffen
Stephen Conrad	Donnie Moreau	Gary Stodter
Robert Dempsey	Charles Morse	Paul Sullivan
W. Bruce Dietzman	William Munn	David Tepen
Michael Dood	Ryan Musgrove	Matthew Vacha
Brian Farmer	Dennis Neitzel	James Van De Ligt
Kenneth Fodero	Arthur Neubauer	Roger Verdolin
James Formea	Nick S. A. Nikjoo	John Vergis
Waymon Goch	Joe Nims	Jane Verner
Edwin Goodwin	Michael Novev	Diane Watkins
Arthur Graves	Gearold O.H. Eidhin	Karl Weber
Randall Groves	Michael O'Brien	Donald Wengerter
Jeffrey Helzer	Lorraine Padden	Kenneth White
Werner Hoelzl	Bansi Patel	Aaron Wilson
Gary Hoffman	Pathik Patel	Terry Woodyard
Yi Hu	Craig Preuss	Roland Youngberg
Anthony Johnson	Moises Ramos	Jian Yu
Gerald Johnson		Sandeep Zope

When the IEEE SA Standards Board approved this guide on 15 September 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Doug Edwards
Ramy Ahmed Fathy
J. Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law

Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley

Mehmet Ulema
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1402-2021, IEEE Guide for Physical Security of Electric Power Substations.

This guide was revised by members of Working Group E7/Physical Security of Electric Power Substations and is under sponsorship of the Substations Environmental Subcommittee of the IEEE Power and Energy Society Substations Committee. This revision accounts for the segregation of physical and cyber security.

Contents

1. Overview.....	11
1.1 Scope.....	11
1.2 Purpose.....	11
1.3 Word usage.....	11
2. Normative references	12
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions.....	12
3.2 Acronyms and abbreviations	12
4. Threat assessment.....	13
4.1 Overview.....	13
4.2 Social, political, and economic background of threats.....	13
4.3 Characteristics of the perpetrator.....	13
4.4 Tools and methods used to carry out threats.....	14
4.5 Characteristics of an intrusion	14
5. Design considerations for threat mitigation.....	16
5.1 Overview.....	16
5.2 Principal threat mitigation measures	17
5.3 Supplemental threat mitigation measures	19
6. Analysis process.....	24
6.1 Overview.....	24
6.2 General components of a substation physical security design analysis.....	24
6.3 Design criteria considerations for physical security	25
7. Physical security plan.....	32
7.1 Overview.....	32
7.2 Identify personnel.....	33
7.3 Define the objectives and requirements	33
7.4 Identify the substation vulnerabilities.....	33
7.5 Prioritize improvements	33
7.6 Incident response plan	33
7.7 Plan review	34
Annex A (informative) Example substation physical security vulnerability assessment checklist	35
Annex B (informative) Bibliography	38

IEEE Guide for ~~Electric Power Substation~~ Physical and ~~Electronic~~ Security of Electric Power Substations

1. Overview

1.1 Scope

This document provides guidance for the physical security of electric power substations. It addresses a number of threats, including unauthorized access to substation facilities, theft of material, and vandalism. It describes some options for positive access control, monitoring of facilities, and delay/deter features that could be employed to mitigate these threats. This guide also discusses options for different levels of physical security risk for electric power substations. The guide does not establish recommendations based on voltage levels, size, or any depiction of criticality of the substation. The user will make these decisions based on threat assessment and criticality assignment by the substation owner.

Large scale overt attacks against the substation for the purpose of destroying its capability to operate, such as explosives, projectiles, vehicles, etc. are beyond the scope of this guide.

~~This guide identifies and discusses security issues related to human intervention during the construction, operation (except for natural disasters), and maintenance of electric power supply substations. It also documents methods and designs to mitigate intrusions.~~

1.2 Purpose

The purpose of this document is to provide considerations and examples of sound engineering practices for substation physical protection that could be applied to mitigate the risks associated with the fact that substations are typically unmanned, and thus susceptible to unauthorized access, theft, and vandalism.

~~Access to electric supply substations by unauthorized personnel is an increasing problem for the electric industry. These intrusions may result in loss, damage, and misoperation of equipment and facilities and may create potential safety and environmental liabilities.~~

~~This guide presents various methods and techniques presently being used to mitigate human intrusions, as identified in an industry survey.~~

~~In 1994, an IEEE Substation Security Guide Survey questionnaire was sent to utilities internationally; the responses from this survey are presented in Clause 7 of this guide.~~

~~Refer to IEEE Std 1264-1993¹ for methods being used to counteract nonhuman intrusions.~~

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{1,2}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

¹The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

²The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

⁴~~Information on references can be found in Clause 2.~~

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.

There are no normative references in this guide.

~~This guide shall be used in conjunction with the following publications:~~

~~Accredited Standards Committee C2-1997, National Electrical Safety Code[®] (NESC[®]);²~~

~~IEEE 100-1996, The IEEE Standard Dictionary of Electrical and Electronics Terms, Sixth Edition.³~~

~~IEEE Std 1127-1996, IEEE Guide for the Design, Construction, and Operation of Electric Power Substations for Community Acceptance and Environmental Compatibility.~~

~~IEEE Std 1264-1993, IEEE Guide for Animal Deterrents for Electric Power Supply Substations.~~

3. Definitions, acronyms, and abbreviations

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.³

²~~The NESC is 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~~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/>).~~

³IEEE Standards Dictionary Online is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

substation: An assemblage of equipment for purposes other than generation or utilization, through which electric energy in bulk is passed for the purpose of switching or modifying its characteristics.

utility: An electric power generation, transmission, or distribution organization; utility also includes any owner of an electric substation.

3.2 Acronyms and abbreviations

API application-programming interface

CCT color coordinated temperature

CRI color rendering index

FOIDS fiber-optic intrusion detection systems

GIL gas-insulated lines

GIS gas-insulated switchgear

HID high-intensity discharge

IP internet protocol

IR infrared

LED light-emitting diodes

PIDS perimeter intrusion detection systems

PIR passive infrared

~~Definitions of terms pertinent to the subject matter are listed here. Definitions as given herein apply specifically to the application of this guide. For additional definitions, see IEEE 100-1996.~~

~~**3.1 construction stage**: The time related to the installation or modification of fixtures or structures, including services, foundations, steel, conductors, buildings, and grounding.~~

~~3.2 intrusion: Unauthorized human access to the substation property through physical presence or external influence.~~

~~3.3 operational stage: The time following commissioning of the facility.~~

~~3.4 undeveloped stage: The time prior to the installation of permanent structures, site preparation, preliminary surveying, surface stripping, fence erection, road building, equipment and material staging, furnishing construction power, etc.~~

4. Threat assessment

4.1 Overview

Threats to substations can arise in many different forms. Threats can come from both outside and inside an organization that designs, builds, operates, and maintains a substation; they also be driven by location, be intentional (planned) or opportunistic, be disruptive to operations, or simply be vandalism or theft. Effective substation security starts with first acknowledging and evaluating the potential threats to a substation. This clause assesses some common threats to substations; other threats are possible and should be assessed to determine whether mitigations are needed to minimize those threats. For more on threat assessment and security plan development see Clause 7 of this guide.

Threats to assets and operations due to natural forces, poor asset management, human error, etc., are beyond the scope of this guide.

4.2 Social, political, and economic background of threats

Threats to substations are typically associated with some form of motivation that drives individuals to attempt to compromise a substation or its operations. Subclauses 4.2.1 through 4.2.4 discuss several typical factors that can lead to threats.

4. Intrusions

4.1 Types of intrusions

Intrusions can be classified into the following categories:

- a) *Pedestrian*: A person walking onto the substation property or into the substation proper, either accidentally or for the purpose of vandalism, robbery, theft, dumping, or other illicit activities.
- b) *Vehicular*: A vehicle driven into a substation, either through an open gate or through the perimeter fence or wall. This intrusion may be for the same purposes listed in item a), or may be the result of an accident.
- c) *Projectile*: Foreign objects thrown or propelled into the substation area that may damage substation equipment or the control room (e.g., rocks, kites, bottles, missiles, explosives, and bullets).
- d) *Electronic*: Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, programmable logic controllers, and communication interfaces.

4.2 Parameters and events that influence intrusions

4.2.1 Economic

According to a 2010 US Department of Energy report [B15], the major factor directly influencing copper theft from utilities is the price of copper.⁴ As the price of copper increases, copper thefts rise. Some of the other factors influencing the rates of copper theft include drug use, proximity to scrap dealers, population density, unemployment, and poverty.

⁴The numbers in brackets correspond to those of the bibliography in Annex B.

~~In some areas, theft of copper, aluminum, or other components from a substation may be prevalent.~~

4.2.2 Substation location

The location of a substation can contribute to increased risk for threat, particularly vandalism and theft (primarily of copper and aluminum) due to being located in higher crime areas or due to the remoteness of the substation. Utilities may choose to review the history and level of illegal activity of the area in which a substation is located and plan accordingly, especially during construction activities when tools and materials are used or stored on site.

4.2.3 Political or labor unrest

Political unrest can be very unpredictable in its occurrence and focus. Substations can be either the target of or collateral damage from acts of sabotage, vandalism, riots, civil disobedience, and protests. Similarly, labor unrest within substation's owners and operators by workers or contractors may provide the impetus for possible retribution by damaging assets or disrupting normal operations at substations.

4.2.4 Disgruntled employees

Current and former employees and contractors can be a particular threat because of their insider knowledge of the electrical system and operating procedures. This is of particular concern as such employees or contractors could take action while they still have access to a substation.

4.3 Characteristics of the perpetrator

Understanding the human aspects of threats supports better security designs. The following are some factors to consider:

- Means of access: Perpetrators can attempt to gain access by scaling walls or fences, crossing moats, breaking down physical barriers, etc.

- Intentional, not accidental: Most threats that would significantly impact the assets or operations of a substation are deliberate in nature. Vandalism may be more spontaneous (e.g., crime of opportunity), but nonetheless also deliberate.
- Not authorized: Threats and actions may be caused by non-employees, contractors, or non-authorized employees and thus are individuals who are not authorized to be within the substation. These individuals would need to breach physical security to gain access or generate damage from outside the physical perimeter security.
- Disgruntled former/current employee: Current and former employees and contractors can be a particular threat because of their insider knowledge of the electrical system and operating procedures.

4.4 Tools and methods used to carry out threats

There are various means that can be used to attempt to carry out a threat. These can include more traditional tools as well as cyber methods. For more on cybersecurity, see IEEE Std C37.240™ [B11].

Some tools and methods used to carry out threats are as follows:

- Vehicular: Many types of vehicles can be used to attempt to breach perimeter security. Frequently, trucks (pickups, flatbeds, and other large delivery trucks) can be used to knock down, pull down, or otherwise open gates or sections of walls and fencing. Other vehicles can include construction equipment (e.g., backhoes) and defense (army) vehicles.
- Bolt cutters: Bolt cutters have been one of the more traditional means of gaining access through a chain link fence or gate. Bolt cutters can also be used to cut wire and cable for theft or interruption of operations.
- Portable power equipment: The prevalence and availability of portable power tools such as saws, grinders, etc., has led to them often being the tools of choice for many of the low-level threats, such as the theft of copper and aluminum. These tools allow obtaining access at more secluded sections of the perimeter, rather than through the front gate.

- Ropes: Though not commonly used, ropes could be used to pull down fences or structures/bus work within the substation.
- Hacking: An increasing threat to substation operation, and potentially, localized power system operation due to interconnected communication networks that may be present at substation by breaking into and manipulating (hacking) computer-based systems. In addition to concerns about grid operations (cyber security), hacking can also be used to control or override physical security systems (access systems, gates, cameras, etc.). Hacking can occur either at the physical site or remotely via the internet or other communications system.
- External ballistic attack: Someone outside the substation, shooting at electrical equipment or
components inside the substation with firearms.
- Unmanned aerial vehicles: Many types of unmanned aerial vehicles (drones) can be used to attempt to breach perimeter security means. These vehicles can be used in themselves to cause damage or used to transport explosives.

4.5 Characteristics of an intrusion

A threat can take many forms or occur at various times. The following are some of the more common characteristics of threats:

- Time of day: Intrusions can occur at any time of day, depending on the nature of the event. However, most tend to occur in the late evening or nighttime when darkness affords more concealment, lessening the probability of detection.
- Duration of the event: Most events are relatively short in nature. Gunshots or explosives can occur within a few minutes. Intruders can be in and out in an hour or less. Quick response rates are imperative.

- Visible vs secretive: As with almost all illegal activity, intrusions most likely occur either at night or when no one else is around. Acts of sabotage are generally not publicized ahead of time (though certain individuals or groups may claim responsibility afterward).
- Noisy versus quiet: Since most individuals prefer not to draw attention to themselves or be seen, they tend to be as quiet as possible.

4.5.1 Objectives of substation intrusion

The physical security components of a substation are intended to deter acts that affect the operation of the substation or compromise the integrity of the assets by damage or theft. Subclauses 4.5.1.1 through 4.5.1.4 discuss some typical objectives of the intruder.

4.5.1.1 Compromising operating systems or enterprise data through unauthorized physical access

Modern microprocessor-based relays are an integral part of system operations and communications systems. Individuals intending to disrupt system operations could seek to gain access to these devices and the operations communication systems. Interfering with these systems can have significant impact on system operations causing grid instability or local to wide-area blackouts. Unauthorized physical access to cyber assets provides a way to compromise the system. See IEEE Std C37.240 [B11] for more information on cyber security.

In addition, enterprise records may be at risk. Enterprise business systems are typically separated from the operations and SCADA systems that are found in substations. Nonetheless, access into the business system may compromise asset records, financial records, or customer data. Intrusion may include stealing, changing, deleting, or otherwise interfering with data and programs in the computer systems. This can compromise customer trust and put the substation owner and operator at higher risk of investigation and fines from any regulatory body providing oversight. Enterprise business systems are just as critical to business operations as the grid operations systems.

4.5.1.2 Theft of material

An increasingly common objective of substation break-ins is for theft. Materials (particularly copper ground cable and cable on reels stored at the site), or tools and equipment that can be readily used, sold, or 'scrapped' for cash are often the target of substation break-ins. Any substation asset that is thought to have monetary value, including landscaping or architectural enhancements, may be stolen for financial gain.

4.5.1.3 Vandalism and loitering

Some activities are not undertaken to incapacitate facilities but may be intended to send a message or for personal reasons. Some examples are as follows:

- Vandalism: May be done to cause economic loss to the owner, i.e., intentional destruction of property to inflict financial harm, or to take out frustration, not necessarily directed at the owner/operator.
- Sabotage: For personal satisfaction, retribution, or to draw public attention to a cause.
- Personal comfort: e.g., seeking shelter or a warm place to sleep.
- Commercial or personal convenience: May include illegal dumping or a shortcut to the other side of the property.
- Thrill seekers and suicide: Those who like the thrill of taking a risk (e.g., target practice with guns, creating a fault within the substation, or other activities seen as challenges). Less likely, but possible, is an individual intending to commit suicide.
- Sightseeing: Typically, no malice is intended, but simply a desire to satisfy one's curiosity.

4.5.1.4 Unauthorized use of substation facilities

An example of unauthorized use of substation facilities is business convenience. Though not common, an individual (employee, contractor, or unrelated person) may attempt to access a substation to utilize some of the facilities (phone, internet, tools, restroom, etc.), even though they are not authorized to do so.

5. Design considerations for threat mitigation

5.1 Overview

Each utility planning to establish a physical security program may choose to perform a risk assessment and implement an appropriate mitigation program at each substation recognized as being important to the resiliency strategy of the utility's and the region's electric supply system. Typical criteria for implementing substation physical security programs are based on probability and impact assessments of threats and vulnerabilities to the following:

- Individual substations
- Neighboring substations or generation stations
- Electric transmission system
- Customers served
- Equipment present inside the substation
- Criticality of load
- Ability to restore equipment and the electric transmission system to normal operation following an event
- Response time for law enforcement personnel for criminal threats

- Response time for substation personnel as it relates to operational recovery and the mitigation of electrical hazards

For many years, utilities have centered their substation physical security programs on theft prevention. Recently, utilities have had to also consider sabotage, where a criminal element is organizing to target substations by damaging electrical substation equipment (or electrical components). Such an event could render the transmission system inoperable and possibly cause large scale power outages and/or public panic.

As utilities consider various threats and perform a risk assessment for each of their substations, the cost-to-benefit ratio of threat mitigation measures can be difficult to establish but should be considered because it is an important part of the decision-making process. It is likely that each utility would assess threats differently and employ threat mitigation measures that may be unique and tailored to their own substation physical security program and the collective strategy for each substation.

Utilities may choose to consider any or all of the examples of threats to electric substations found in Clause 4.

5.2 Principal threat mitigation measures

In general, there are many security solutions that can address any one threat or vulnerability to electrical equipment, electrical components, and the operational capabilities of an electric substation. These threats are usually identified during threat assessments and evaluations. For a facility at risk, principal solutions can be viewed as an approach to deter, detect, or delay the impact of certain types of events.

5.2.1 Perimeter security fences

Fences of various materials serve as the principal barrier that limits access to electric substations, where basic requirements are documented in current versions of various codes, such as the National Electric Safety Code® (NESC)® [B1]. Galvanized steel chain-link fences continue to serve as the most basic perimeter security fence for electric substations. In general, fences at electric substations have been 1.8 m to 2.1 m (6 ft to 7 ft) tall and they often utilize top guard, such as strands of barbed wire. A common barrier/surface used has been 5 cm (2 in), chain-linked fabric. Traditionally, these fences provide a basic security barrier and a line of demarcation that identifies the enclosed electric substation. By incorporating universal safety signs and building to physically comply with the requirements noted in codes, these fences serve to identify the borders of a facility that is generally considered hazardous to unauthorized personnel.

The benefits for standardizing on the use of steel chain-link fence are low cost, resource availability, and ease of installation/modification/repair. In addition, the industry's best practices for grounding chain-link fences at electric substations are well known and documented throughout industry references.

As owners of substations experience unauthorized forced entry events, other perimeter fence options have been employed to stop or mitigate activity at affected facilities. Owners of substations have realized that the materials traditionally used for perimeter fences [5 cm (2 in), chain-link mesh] may not be considered a proper security barrier for perimeters that require heightened physical security. The material used for the primary barrier would likely be commensurate with the evaluated threats and security risk assessment for that substation. Chain-link fence is easily cut, easily climbed, and provides very little screening for assets in the interior of the enclosed area.