IEEE Guide for Electric Power Substation Physical and Electronic Security

Sponsor

Substations Committee
of the
IEEE Power Engineering Society

Approved 30 January 2000

IEEE-SA Standards Board

Abstract: Security issues related to human intrusion upon electric power supply substations are identified and discussed. Various methods and techniques presently being used to mitigate human intrusions are also presented in this guide.
Keywords: construction, intrusion, operation, safety

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

Copyright © 2000 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 04 April 2000. Printed in the United States of America.

Print: ISBN 0-7381-1960-1 SH94822
PDF: ISBN 0-7381-1961-X SS94822

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.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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.

--`,,`-`-`,,`,,`,`,,`---

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS Not for Resale

Introduction

(This introduction is not part of IEEE Std 1402-2000, IEEE Guide for Electric Power Substation Physical and Electronic Security.)

This guide was revised by members of Working Group G3/Substation Security and is under the sponsorship of the Substations Environmental Subcommittee of the IEEE Power Engineering Society Substations Committee.

Participants

The members of the Working Group who participated in the creation of this guide were as follows:

Michael J. Bio, *Chair*
William M. Malone, *Vice Chair*

Michael J. Bogdan
James C. Burke
Richard G. Cottrell
John W. Dean
W. Bruce Dietzman
David L. Harris
Richard A. Jones
David S. Lehman
John Oglevie
Patrick M. Rooney
Alan C. Rotz
Anne-Marie Sahazizian
C. M. Stine
Charles Stoll
Raymond L. Stoudt
Robert F. Weeden

The following members of the balloting committee voted on this standard:

Hanna E. Abdallah
William J. Ackerman
Stuart Akers
Stan J. Arnot
Michael H. Baker
George J. Bartok
Michael J. Bio
Kenneth L. Black
Charles Blattner
Wayne R. Block
Michael J. Bogdan
Stuart H. Bouchey
Steven D. Brown
James C. Burke
Frank Y. Chu
John R. Clayton
Richard G. Cottrell
Richard Crowdis
Frank A. Denbrock
W. Bruce Dietzman
Richard B. Dube
Gary R. Engmann
Markus E. Etter
William R. Fajber
Dennis R. Falkenheim
David Lane Garrett
Barry M. Gore
Floyd W. Greenway
Robert E. Howell
Donald E. Hutchinson
Danny L. Johnson
James Jung
Richard P. Keil
Hermann Koch
Alan E. Kollar
Terry L. Krummrey
Donald N. Laird
William M. Malone
Rusko Matulic
John D. McDonald
John E. Merando Jr.
Jovan M. Nahman
Philip R. Nannery
Robert S. Nowell
James S. Oswald
Michael W. Pate
Shashi G. Patel
Trevor Pfaff
Percy E. Pool
Paulo F. Ribeiro
Alan C. Rotz
Anne-Marie Sahazizian
Hazairin Samaulah
Samuel C. Sciacca
David Shafer
Gary Simms
Mark S. Simon
Bodo Sojka
Robert P. Stewart
Brian Story
Raymond L. Stoudt
Duane R. Torgerson
Georg Wild
Mark S. Zar

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

When the IEEE-SA Standards Board approved this standard on 30 January 2000, it had the following membership:

Richard J. Holleman, *Chair*
Donald N. Heirman, *Vice Chair*
Judith Gorman, *Secretary*

Satish K. Aggarwal	James H. Gurney	Louis-François Pau
Dennis Bodson	Lowell G. Johnson	Ronald C. Petersen
Mark D. Bowman	Robert J. Kennelly	Gerald H. Peterson
James T. Carlo	E. G. "Al" Kiener	John B. Posey
Gary R. Engmann	Joseph L. Koepfinger*	Gary S. Robinson
Harold E. Epstein	L. Bruce McClung	Akio Tojo
Jay Forster*	Daleep C. Mohla	Hans E. Weinrich
Ruben D. Garzon	Robert F. Munzner	Donald W. Zipse

*Member Emeritus

Also included is the following nonvoting IEEE-SA Standards Board liaison:

Robert E. Hebner

Andrew D. Ickowicz
IEEE Standards Project Editor

--`,,`-`-`,,`,,`,`,,`---

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

1. Overview 1

1.1 Scope 1
1.2 Purpose 1

2. References 1

3. Definitions 2

4. Intrusions 2

4.1 Types of intrusions 2
4.2 Parameters and events that influence intrusions 3
4.3 Problems caused by intrusions 3

5. Criteria for substation security 5

6. Security methods 6

6.1 Barriers 6
6.2 Electronic 7
6.3 Other methods 8

7. Effectiveness of security methods 12

8. Substation security plan 15

8.1 Objective of the security plan 15
8.2 Responsibility for security 16
8.3 Basic security requirements 16
8.4 Additional security measures 16
8.5 Sample security assessment 16

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

IEEE Guide for Electric Power Substation Physical and Electronic Security

1. Overview

1.1 Scope

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

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 1264-1993[1] for methods being used to counteract nonhuman intrusions.

2. References

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

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

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

[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/).

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

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

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. 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.

[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/).

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

4.2 Parameters and events that influence intrusions

4.2.1 Economic

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

4.2.2 Location

Higher levels of crime, vandalism, and graffiti may be common behaviors in certain neighborhoods. School properties or other public areas adjacent to or near a substation or substations located in remote areas may also present additional opportunities for intrusions.

4.2.3 Aesthetics

Walls, plantings, or screening treatments may make substations an attractive and secluded meeting spot for various recreational or illicit activities.

4.2.4 Labor conflicts

Strikes, slowdowns, personnel reductions, or other labor conflicts by utility or contract workers can be a significant factor influencing intrusions as the substation can be an attractive target.

4.2.5 Use of adjacent property

Uses of adjacent property may lead to intrusions onto substation property. Commercial activities, building, storage, equipment and material locations, and building structures can facilitate intrusions onto substation property.

4.2.6 Curiosity and ignorance

Many items in a substation may attract curious individuals who are unaware of the hazards that exist within the substation fence.

4.2.7 Civil/political unrest

Terrorism, war, riots, civil disobedience, and public events provide increased opportunity for intrusions.

4.2.8 Joint-use facilities

Establishment of a substation on or adjacent to a facility that is shared, owned, or used by others could provide additional opportunity for intrusions as the potential for legitimate access by unqualified personnel increases.

4.2.9 Natural and/or catastrophic disasters

The effects of natural and/or catastrophic disasters may render security systems ineffective.

4.3 Problems caused by intrusions

Human intrusions onto substation sites can create many problems and can occur during any of the following three stages of substation development:

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

a) The undeveloped stage
b) The construction stage
c) The operational stage

These problems, which can be unique to only one stage or can be common to one or more of the three stages, are discussed in 4.3.1, 4.3.2, and 4.3.3.

4.3.1 Undeveloped stage

This guide assumes that at the time a substation property is obtained, it is free of any hazardous materials.

The problems associated with an undeveloped substation property can generally be classified as attractive nuisances, dumping, vandalism, illicit activities, and sabotage.

Attractive nuisances are any items that, by their mere presence, may draw people's attention for use or play without recognizing their dangerous qualities. These may include, but are not limited to, old wells, septic systems, caves, trees, rock formations, and ponds. These items may attract people onto the property, where they may be injured or killed. Civil lawsuits could result from these occurrences.

An unsecured substation property is an attractive place for the dumping of trash or hazardous materials. This dumping can cause public complaints or legal citations. The removal of these materials may be quite expensive.

Vandalism on the property can create problems similar to those caused by dumping.

A vacant property may also provide a place for various unwanted or illicit activities to occur. These activities may also cause public complaints and possible civil actions.

Finally, sabotage can be caused by disgruntled or striking employees, other personnel (e.g., construction crews, contracted services, customer utility manpower), or groups opposed to the development of a substation at the site.

4.3.2 Construction stage

Each problem associated with an undeveloped property and described above can occur during the construction stage of a substation and should be considered. In fact, the presence of construction materials and equipment can create additional attractive nuisances. New hazards such as excavations, uncompleted structures, and construction equipment now are on site that could cause injury to unauthorized personnel.

Additional problems that can occur during the construction stage are theft and increased vandalism. Construction materials that contain copper and aluminum are very attractive since they can easily be sold for scrap. The use of copper-clad or galvanized steel wire or stranded wire may be a theft deterrent due to its negligible scrap value compared to solid copper wire or strand. During the construction stage, these items are often packaged for convenient removal and may be stored in unsecured areas. Construction equipment, such as pickup trucks and excavation equipment, is motorized and can be easily removed from the site. The removal or vandalism of materials and equipment will increase the cost of the project. In addition, many of the items required for the construction of a substation have long delivery times and are not easily replaced. The loss of these items may also drastically delay the completion of the project and increase cost.

4.3.3 Operational stage

Although the substation is normally energized during the operational stage, nearly all of the potential problems described above, as well as the removal of gauges and copper ground materials, meter damage, and the opening of transformer valves, can occur. The fact that a substation is energized does not deter these problems.

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

An additional concern during the operational stage arises from the fact that the substation is normally energized and often unattended. At this stage, intrusions can affect the integrity of the electric power supply and the reliability of the transmission and distribution grid, if the intrusion results in power interruptions. Examples include projectiles, poles, or kites that come in contact with energized parts, and electronic interference with relaying and control circuits. Intruders have been known to open valves, push buttons, and operate circuit breakers, reclosers, and switches.

Another area of concern comes from employees and other authorized personnel with legitimate access to a substation. Their actions can defeat the security aspects of the station design in order to facilitate their functions, such as removal of a vehicle gate center-stay to allow easier snow removal. This action may allow a locked gate to move beyond its design limits and permit unauthorized access.

Sabotage becomes more of a concern in the operational stage. Sabotage can be done by those who normally have legitimate access to the substation, such as construction crews, contracted services, customer or utility manpower, or by those with no legitimate access, such as criminals, activists, and extremists.

Safety concerns increase significantly because of the potential for accidental human contact with energized equipment or removal of grounding material that could cause hazardous conditions for personnel. Some examples include persons under the influence of alcohol or drugs, teenagers on a dare, and unsuspecting children. All have been known to come in contact with energized conductors or equipment.

Substations located on slopes can be subject to erosion and wash out, which can create openings under the fence and compromise security.

In addition, electronic intrusion becomes a concern. Electronic interference, whether accidental or intentional, can disrupt communications, protective relaying, control, supervisory control and data acquisition (SCADA), and other instrumentation. Security systems can also be defeated or jeopardized.

Substations may contain microprocessor-based relays and programmable logic controllers (PLCs), as well as other intelligent electric devices (IEDs). In addition, many utilities are including local area network (LAN) systems within the substation environment. These LAN systems will allow IEDs and relays to share information as well as transmit important system data directly to the control center of various utilities. However, the introduction of computer systems with on-line access to substation information is significant in that substation relay protection, control, and data collection systems may be exposed to the same vulnerabilities as all other computer systems. As the use of computer equipment within the substation environment increases, the need for security systems to prevent electronic intrusions may become even more important.

Electronic computer intrusion in its broadest definition can cover all acts that change, delete, or otherwise interfere with the data and programs stored in computer files. This includes deliberate acts to steal, alter, or destroy information.

5. Criteria for substation security

A mitigation program should be put in place either during the initial design or after experiencing substation intrusions. Typical criteria for implementing substation security programs are based on an assessment of probability, frequency, duration and cost of occurrences, safety hazards, severity of damage, equipment type, number and type of customers served, substation location, design type, criticality of load, and quality of service at existing substations. Also, weather conditions in the area of the substation should be considered, since they can impact response time to an intrusion.

The point at which cost of occurrences and safety hazards justify implementing deterrent programs is often difficult to establish. However, the security survey results indicate that the most common parameters for

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

implementing corrective actions are physical injuries, criticality of load, and extent of damage. These issues should also be considered in new designs.

6. Security methods

Security requirements should be identified in the early design stages of the substation project. Generally, it may be more economical to anticipate and incorporate security measures into the initial design rather than retrofit substations at a later date.

This clause identifies the use of barriers, electronics, and other methods of providing substation security.

6.1 Barriers

6.1.1 Fences

Fences of various materials provide primary security to limit access to substation property; refer to the National Electrical Safety Code® (NESC®) (Accredited Standards Committee C2-1997) for fence requirements. In addition, adding top and bottom rails on fence sections, closed track roller systems to sliding gates, and methods such as welding to prevent hinge pins and bolts from being easily removed, may improve the overall integrity of the fencing system. Also, the extension of materials above and below grade, such as concrete curbing, has been used to reduce the possibility of erosion and dig-ins under the fence.

Double-fencing (enclaving), increased fence height, and smaller-dimension mesh fabric that impedes climbing may also be considered to avoid access over the fence. Areas that experience large snow accumulations should consider use of higher fences.

The material utilized for the fence should be commensurate with the evaluated security risk of the area. A standard chain-link fence is easily cut and most purposeful intruders use this method to gain access. Chain-link fences are therefore of little value against this type of intruder.

6.1.2 Walls

Solid masonry or metal walls may provide an additional degree of security. Solid walls are generally more difficult to breach and also prevent direct line-of-sight access to equipment inside the substation. Solid walls may prevent external vandalism, such as gunshot damage, depending on the height of the wall, surrounding terrain, and elevation of equipment inside the substation.

6.1.3 Entrance/equipment locks

All entrances to substations should be locked. All equipment located outdoors within the substation fence should have a provision for locking cabinets and operating handles where unauthorized access could cause a problem. Padlocks should be of a type that can utilize a nonreproducible key. Similar locking devices should be used on gates and doors to any buildings within the substation fence. Maintenance of equipment alignment is important to ensure proper installation of locks. In places where it is difficult to keep equipment in alignment, the use of a chain and lock is a practical method to secure the gate. However, avoid the substitution of chains where possible, since they may compromise the security of a locking system.

6.1.4 Other barriers

Access to energized equipment and bus may be of concern if the perimeter security measures are breached. Polycarbonate or other barriers on ladders and structure legs should be considered in order to prevent

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

inadvertent access. Refer to the NESC and Occupational Safety and Health Administration (OSHA) requirements.

Driveway barriers (gates, guard rails, ditches, etc.) at the property line for long driveways can help limit vehicular access to the substation property.

6.2 Electronic

A variety of commercially available systems can be employed to provide varying levels of security in the substation. Caution should be used when employing sensing devices that are subject to erroneous activation due to movements caused by animals, wind, seismic events, or vibrations. All wiring for electronic security systems should be installed in a manner that will ensure operational integrity and resistance to tampering.

6.2.1 Photoelectric/motion sensing

Perimeter systems using photoelectric or laser sensing may be utilized to provide perimeter security. Overall area security may be provided by motion-sensing devices; however, great attention should be shown in the placement of these devices since animal intrusion alarms may become a nuisance and sensors may be deemed ineffective.

6.2.2 Video surveillance systems

Video systems can be deployed to monitor the perimeter of the substation, the entire substation area, or the building interiors. Systems of this type require 24 h monitoring, which can be a costly alternative.Video systems are available that utilize microwave and infrared to activate a slow-scan video camera. This can be alarmed and monitored remotely and automatically videotaped.

6.2.3 Building systems

One of the more common methods utilized is an intrusion alarm on control buildings. These systems include, at a minimum, magnetic contacts on all the doors, and have the provisions to communicate through the existing telephone network or SCADA systems. A local siren and strobe light may be located on the outside of the building to indicate the alarm condition. The system should be capable of being activated or deactivated using an alphanumeric keypad, keyswitch, or a card reader system located inside the building. All siren boxes and telephone connections should have contacts to initiate an alarm if they are tampered with.

6.2.4 Computer security systems

Computer security systems can be subdivided into three major components: identification, authentication, and auditing. Identification is simply a login name or user identification (user id) to determine who wants access to the information. Authentication is the process of verifying that the person logging in is who they say they are. Finally, the audit is an attempt to verify that only authorized personnel are accessing the data through the use of separate reporting and logging systems. Some typical security methods are discussed in 6.2.4.1 through 6.2.4.5.

6.2.4.1 Passwords

Probably the most widely used and most common form of protection is the user ID and password. All security systems, regardless of their sophistication, begin with a user ID and password protection system. However, working alone, they are also the easiest to break. Keep in mind the following points:

a) Do not use personal information, such as birthdays, names, etc.
b) Do not use common words or names.

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

c) Use at least four characters and preferably more.
d) Memorize them.
e) Mix symbols, numbers, and both upper and lower case letters.
f) Change the password periodically.
g) Limit the number of attempts to enter a password.

6.2.4.2 Dial-back verification

This technique provides one of the best methods of protecting a system from external access. The system is based on the intended user first calling the equipment via modem, which initiates a dial-back response by the equipment using a predetermined telephone number. Although this technique provides increased protection from external intrusion, it provides little protection from electronic intrusion by those within the organization.

6.2.4.3 Selective access

This technique allows access for information purposes to a large group while restricting authorization for modification of files to a smaller group through the use of an additional password.

6.2.4.4 Virus scans

A computer virus is another form of electronic intrusion. With the increased use of desktop and laptop equipment to access substation equipment, it is possible that an infected computer could spread a virus to the substation equipment. The introduction of computer viruses can be limited by the following:

a) Employing virus scanning software.
b) Scanning all floppy discs prior to use on any computer system.
c) Destroying all discs suspected of infection.

6.2.4.5 Encrypting and encoding

Where it is suspected that intruders may be able to defeat the identification and authentication security measures and gain unauthorized access to the computer, further protection may be warranted. The program or its critical data can be encoded or encrypted to block access, even after access to the computer has been gained. This method also can be used to block access by unauthorized personnel with legitimate access to the area housing the computer, especially when the computer may be routinely left on-line.

6.3 Other methods

6.3.1 Lighting

The entire interior of the substation may be provided with dusk-to-dawn lighting to provide a minimum light level of 21.52 Lux (2 footcandles). Placement of lighting posts should be such as not to assist an intruder who may climb the posts to enter the substation. All wiring to the lighting posts should be in conduit or concealed to minimize tampering by an intruder. In addition, areas outside the substation, but within the facility property, should also be considered for lighting to deter loitering near the substation.

Zoning and other local regulations may restrict or prohibit lighting.

6.3.2 Landscaping

Any landscaping treatment around substations should be carefully designed so as not to create potential security problems.

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

6.3.3 Building

In general, most building materials provide adequate security protection. Selection of the type of building construction should be suitable for the level of security risk. Typically, features that should be included are steel doors with tamper-proof hinges and roof-mounted heating/air conditioning units. Any wall openings (i.e., wall air conditioners) should have security bars over and around the unit. A building that is part of the perimeter fence line should be at least as secure as the fence. Construction of a building to enclose the substation or exposed equipment and materials can provide an additional layer of protection against intruders. For example, using trailers or buildings to enclose material stored at construction sites may deter theft.

6.3.4 Patrols

In areas where vandalism has been a chronic problem and at critical substations, judicious use of security patrol services should be considered. A partnership should be established with local law-enforcement agencies to facilitate the need for local patrols of selected substation facilities to deter vandalism and unauthorized entry. Security procedures should be established that specifically identify who handles security alarms and what the notification procedure is within the company and local law enforcement agencies.

Furthermore, during special or unusual occasions, such as labor disputes, the Olympics, or a presidential visit, security procedures at critical substations may include identification checks by security patrols and limited access to the substation.

6.3.5 Special precautions for natural and/or catastrophic disaster

During a disaster, responding security or law-enforcement personnel may not be able to respond within an acceptable time due to transportation restrictions or higher priority emergencies. However, proper planning for disasters that might occur in a given location can help to protect a substation and preclude the need to deploy personnel during the event.

Failure to recognize the impact of the following events and to institute precautions could result in numerous false alarms:

a) *Wind*. Do not use security measures that might be activated by high winds.

b) *Seismic activity*. Do not use devices that could be triggered by earth tremors.

c) *Vehicular, rail, or aircraft intrusion*. While prudent siting methods can reduce the likelihood of such an event, substations at times must be contiguous to these modes of transportation as a matter of necessity. Alternate means of accessing the site can be helpful when the normal access is blocked by an intrusion. In addition, prudent planning for emergency response to the above should include the availability of items such as emergency lighting and temporary fencing materials.

6.3.6 Communications

A key element of theft or loss control is communication, both internal and external to the company. Notification of a loss and the monetary or safety implications increase problem awareness and vigilance.

6.3.6.1 Internal

Companies should ensure that employees are advised of their security responsibilities. Employees responsible for the resources under their care or control should take reasonable precautions against loss, theft, or damage. Operational and inspection procedures can be utilized to reduce the potential for intrusions. These procedures should include inspection of the perimeter for breaks in the security measures, including padlocks, electronic security systems and alarms, the condition of all warning signs, and the integrity of the fence. Alertness, vigilance, and reporting of incidents will contribute to improved security.

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Awareness can be improved by

a) Providing tutorial information to employees.
b) Using posters on-site.
c) Circulating information on reported incidents.
d) Using a site security checklist.
e) Encouraging suggestions for improvement.
f) Marking tools with company identification.
g) Encouraging customers and property owners to report suspicious activity around facilities.

Identification of all losses is essential to determine the security measures required on a future project. Losses can be the result of employees or non-employees identifying and exploiting an opportunity. The purpose of the internal communication is to identify the problem to all levels of management on an internal company basis. Details of an incident include date, time, location, value, loss description, impacts, and contributing factors/suspects. All are important data to identify. Suspect names or very specific data regarding a particular incident should be carefully screened to prevent adverse impacts on further legal action or prosecution. As an example of a proposed format, see Figure 1. Once a format is developed, a common database program can sort incidents and may help identify patterns.

6.3.6.2 External

Another important element in reducing theft is communication with groups outside the company, including neighbors adjacent to the substation. If a loss occurs, quickly disseminating information on a regional basis may help identify the parties involved and may potentially deter future acts. Facsimile, e-mail, or phone notification networks to possible outlets for stolen goods, such as local companies, scrap or recycle dealers, and law enforcement can provide an expeditious vehicle for loss notification. Suspicious conductor scrap sales, vehicle thefts, and regional loss problems can be better investigated through coordinated and cooperative industry and law-enforcement efforts.

In addition, once intruders are apprehended and convicted, information concerning the intrusion and individuals involved could be made public in an effort to deter future attempts.

6.3.7 Additional security measures

The following additional security measures should be considered:

a) Structures and poles should be kept a sufficient distance from the fence perimeter to minimize the potential use of the structure itself to scale the fence.

b) All sewer and storm drains that are located inside the substation perimeter, with access from the outside, should be spiked or fitted with vertical grillwork to prevent entry.

c) Manhole covers or openings should be located on the inside of the substation perimeter fence.

d) Driveway barriers (gates, guardrails, ditches, etc.) at the property line for long driveways can help limit vehicular access to the substation property.

e) Signs should be installed on the perimeter fence to warn the public that:

   1) Alarm systems are providing security for the substation.
   2) Entry is not permitted.
   3) There is a danger of shock inside.

f) Most of the security measures described in this clause can be utilized in a retrofit application at an existing substation.

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

INCIDENT ALERT

**Issued in the interest of
incident prevention
by the Security Department**

Issue Number 001

Date: June 1, 1996 Time: 12:25 p.m.

Location: ACB Company, Inc.

Value of material involved: $500 + (estimated)

Loss: Approximately 500 lb, 100 mcm, 15 kV scrap copper cable stored in backyard.

Impact: Monetary/potential hazard to employees and visitors — suspect almost ran over employee while exiting facility after being approached.

Contributing factors/suspects: Vehicle – yellow, full size, 1983 station wagon, driven by white male, 30s, 6'1", 180 lbs, blonde hair. Other similar incidents past few years. Facility has interior security system. Yard not covered presently.

Note: Copies of actual Loss Report which provides more detail may be obtained by contacting Mr. Smith at (800) 555-1234, extension 567.

Figure 1—Example form

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

7. Effectiveness of security methods

Table 1 through Table 4 contain a summary tabulation of responses to the security survey. The tabulation provides an indication of the effectiveness of security methods used by the respondents in four types of substations: urban, suburban, rural, and industrial/commercial. Regardless of the substation type, some general observations are possible. Use of lights, signs, and special locks are by far the most common security methods employed. Although generally effective according to the majority of the respondents, these methods were not found to be completely effective and can be defeated.

The remaining methods surveyed apparently are not often utilized, based on the limited number of respondents employing the specific methods. This is probably the result of increased cost, complexity, and/or inconvenience. When employed, these methods have been found to be generally more effective than lights, signs, and special locks. Those methods (alarm systems, motion detectors, and electronic protection) used least often were reported to be completely effective.

Other methods reported in the survey included portable video cameras, sirens activated by motion, silent alarms, private security companies, and laser alarms. These methods were not widely used and there was no report as to their effectiveness.

Table 1—Effectiveness of security methods—urban substations

Method	Number of respondents reporting to survey	Respondents reporting method not effective (%)	Respondents reporting method somewhat effective to effective (%)	Respondents reporting method very effective to completely effective (%)
Lights	31	7	77	16
Signs	27	7	78	15
Special locks	18	1	66	33
Solid wall	7	0	57	43
Security guard	5	0	60	40
Manned station	4	0	100	0
Optical alarms	4	0	75	25
Fence	4	0	75	25
Video camera	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	67	33
Door alarm (to SCADA)	2	0	0	50
Alarm system	2	0	0	100
Motion detectors	1	0	0	100
Electronic protection	1	0	0	100

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 2—Effectiveness of security methods—suburban substations

Method	Number of respondents reporting to survey	Respondents reporting method not effective (%)	Respondents reporting method somewhat effective to effective (%)	Respondents reporting method very effective to completely effective (%)
Lights	31	6	78	16
Signs	27	11	81	8
Special locks	19	5	69	26
Security guard	6	0	100	0
Fence	5	0	60	40
Solid wall	4	0	75	50
Manned station	4	0	100	0
Optical alarms	4	0	100	0
Video camera	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	67	33
Door alarm (to SCADA)	2	0	0	100
Alarm system	2	0	0	100
Electronic protection	2	0	0	100
Motion detectors	1	0	0	100

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 3—Effectiveness of security methods—rural substations

Method	Number of respondents reporting to survey	Respondents reporting method not effective (%)	Respondents reporting method somewhat effective to effective (%)	Respondents reporting method very effective to completely effective (%)
Lights	31	13	74	13
Signs	22	11	77	12
Special locks	17	6	65	29
Optical alarms	5	0	100	0
Fence	5	0	60	40
Passive and microwave systems	4	0	0	100
Security guard	4	25	50	25
Video camera	3	0	66	34
Manned station	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	100	0
Alarm system	2	0	0	100
Door alarm (to SCADA)	1	0	0	100
Solid wall	1	0	100	0
Motion detectors	1	0	0	100
Electronic protection	1	0	0	100

--`,,`-`-`,,`,,`,`,,`---

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Table 4—Effectiveness of security methods—industrial/commercial substations

Method	Number of respondents reporting to survey	Respondents reporting method not effective (%)	Respondents reporting method somewhat effective to effective (%)	Respondents reporting method very effective to completely effective (%)
Lights	28	4	82	14
Signs	25	8	84	8
Special locks	15	7	73	20
Security guard	5	0	40	60
Solid wall	3	0	34	66
Manned station	3	0	100	0
Fence	3	0	66	34
Video camera	2	0	100	0
Optical alarms	2	0	100	0
Special equipment (metal-clad, polymer)	2	0	50	50
Door alarm (to SCADA)	1	0	0	100
Alarm system	1	0	0	100

8. Substation security plan

The preparation of a security plan shall require answering the following:

a) Why is the plan needed?
b) Who will administer the plan?
c) What security measures are required by the individual facility?

These questions need to be addressed before a comprehensive and cost-effective security plan can be created.

8.1 Objective of the security plan

For any plan to be successful, it must have a clearly stated objective. Using historical operating data, demographics information, and industry experience, each company can determine the level and type of security required. Defining the objective will help focus attention on those security methods most appropriate to the company's needs. The objective should state the present and primary concerns, such as vandalism and theft in existing stations, or theft and injury during substation construction.

--`,,-`-`,,`,,`,`,,`---
Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

8.2 Responsibility for security

Identification of the person or persons responsible for security implementation and administration is critical to the effectiveness of the plan. Therefore, defined levels of responsibility and specific tasks are required for each level. Each company should have someone in charge of facilities security. This individual should be responsible for assuring that a security plan is developed, implemented, regularly reviewed, and updated. Regular inspection of facilities to assure that security measures are in effect should be part of the security plan, along with employee training and methods that enable employees to report irregularities or breaches of security.

8.3 Basic security requirements

All existing and new substations have a basic minimum level of security required. This includes fences with locked gates, control buildings with locked doors, a special type of grounding system if copper theft is prevalent, and minimum clearance distances between perimeter fences and energized equipment. Basic security requirements should list these measures as required in all cases, regardless of location or age of the station. In addition, some types of security breach may require special or immediate action by operations staff. For example, damage to the ground system of an energized station should be treated with care in case of the unlikely event of a dangerous touch potential. These types of security breaches should be noted in the security plan.

At construction and material storage sites, or vacant land, minimum security levels may either not exist, or may be inadequately described. Therefore, it is important to define the security measures required by type of facility or site, especially if the measures required are different from other basic measures normally required. For instance, vacant land should be inspected on a regular basis for evidence of use for illicit activities, unauthorized dumping, and existence of holes that could cause injury due to falls. Security methods at active construction sites can include moving all construction equipment inside of fenced areas at night and check-in/check-out of personnel through a security gate.

8.4 Additional security measures

Additional security measures, over and above the basic requirements, may be determined to be necessary based on the security survey results. The increased security measures required should be based on restricted access or high-risk areas. The types of security used in these instances could include motion detectors, perimeter/area detection systems, security cameras, jersey barriers, and posted guards.

8.5 Sample security assessment

A plan for evaluating the effectiveness of any mitigating measures should be initiated. Records should be kept for each substation to document the security option used, date of application, type of intrusion and problem the option is intended to mitigate, and the history of intrusion problems. This record is necessary to monitor the performance of the applied option in order to evaluate the feasibility of future applications. The form shown in Figure 2 is a sample format for security assessment and includes a summary of the items addressed in this guide.

Copyright © 2000 IEEE. All rights reserved.
Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

Security Assessment

Assessment completed by: _____

Date: _____

I. SUBSTATION LOCATION: _____

II. SUBSTATION CLASSIFICATION:

A. Type:

❑ Rural
❑ Urban
❑ Construction site
❑ New facility
❑ Existing facility
❑ Permanent facility
❑ Temporary facility
❑ Land bank

1. Construction type_____
2. Location_____
3. Distance to nearest occupied facility_____
4. Type of access road_____
5. Visibility/screening from view_____
6. Distance to regularly traveled road_____
7. Topography_____
8. Environmental consideration_____

B. Planned activity:

❑ Vacant
❑ Pre-construction
❑ Construction
❑ Operational

C. Equipment involved:

❑ None (unoccupied)
❑ Storage
❑ Construction equipment
❑ Energized facility

III. SITE RISK EVALUATION:

Local demography
Local economics
Local crime rate/reported incidents
Local building/construction aesthetics
Labor conflicts/disputes
Adjacent landowners (uninhabited)
Adjacent landowners (inhabited)
Substation value

IV. SITE MAINTENANCE:

	Yes	No
A. General observation:		
Evidence of use	❑	❑
Bottles and/or cans	❑	❑
Refuse	❑	❑
Standing water	❑	❑

Comments/explanation: _____
_____
_____

Figure 2—Security assessment

Copyright © 2000 IEEE. All rights reserved.

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale

	Yes	No
B. Walls and fences:		
Damage	❑	❑
Graffiti	❑	❑
Broken strands or holes	❑	❑
Rust to galvanizing	❑	❑
Undermining	❑	❑
Evidence of attempted entry	❑	❑
Damage to locks or hinges	❑	❑

Comments/explanation:_____

_____

	Yes	No
C. Station yard:		
Refuse	❑	❑
Disturbed grading	❑	❑
Damage to grounding conductor or hardware	❑	❑
Graffiti on walls or equipment	❑	❑
Loose valves or evidence of tampering	❑	❑
Evidence of vandalism	❑	❑
Broken or chipped porcelain	❑	❑

Comments/explanation:_____

_____

	Yes	No
D. Control building:		
Attempted entry	❑	❑
Stolen or missing maintenance equipment	❑	❑
Evidence of occupancy	❑	❑
Tampered control equipment	❑	❑

Comments/explanation:_____

_____

Comments/other:_____

_____

Recommendations: _____

_____

_____

_____

Figure 2—Security assessment (continued)

Copyright The Institute of Electrical and Electronics Engineers, Inc.
Provided by IHS under license with IEEE
No reproduction or networking permitted without license from IHS
Not for Resale
Copyright © 2000 IEEE. All rights reserved.