Security Guidelines for the Electricity Sector: Physical Security — Substations

NERC	*Guideline*
Guideline Title: Physical Security — Substations	**Version: 1.0**
Revision Date: October 15, 2004	**Effective Date: October 15, 2004**

Purpose:

Each entity should implement physical security measures at their critical substations to safeguard personnel and prevent unauthorized access to critical assets, control systems, equipment, and information that may be resident in the substation. Each entity should implement substation security solutions in a way that is consistent with the criticality of the substation and sufficient to provide appropriate situational awareness of activity at these substations so that the entity can initiate an appropriate and timely response.

The NERC document "An Approach to Action for the Electricity Sector" version 1.0 dated June 2001, lists the following as examples of critical infrastructure assets that, if disrupted or threatened, would adversely impact regional, national, or the North American electrical grid reliability:

- important regional transmission hubs,
- interregional tie lines,
- substations that feed interregional ties,
- interregional communications facilities, and
- security [control] centers.

While some of the above facilities are attended around-the-clock to support operations, most are normally unattended. Unattended critical facilities such as substations require appropriate levels of physical security. Many of the security solutions that are readily applicable to attended facilities cannot be readily applied at the unattended substation.

Applicability:

This guideline applies to critical electric substations. While many substations contain critical assets, some substations are more critical than others to the support of the electricity infrastructure and the overall operation of the bulk power system.

Each entity, using a risk assessment methodology, should define and identify those substations, whether attended or not, it believes to be critical, keeping in mind that the ability to mitigate the loss of a substation through redundancies or operations may make that facility less critical than others.

A critical facility may be defined as any facility or combination of facilities, if severely damaged or destroyed, that would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Guideline Statement:

This guideline recommends that "most effective practices" be applied at an appropriate level for electric substations consistent with the level of criticality of the substation as determined by the asset owner. This guideline should be used in conjunction with the Physical Security Guideline and the Vulnerability and Risk Assessment Guideline as well as any other guidelines that apply, which assists entities in identifying critical facilities.

Background:

Attended facilities like control centers, communication facilities, and corporate offices, present a different physical security challenge because they tend to be more complex, centralized, and have multiple physical perimeters. While the more centralized nature of attended facilities allows more economy of scale, this advantage is balanced against the risks associated with common points of failure and cascade effects associated with a single event. Attended facilities also tend to house a great deal more critical cyber assets than the unattended facility. NERC cyber security standards specifically addresses many of the physical security needs of attended facilities in the following sections:

- Physical Security Perimeter[s]
- Physical Access Controls
- Personnel
- Monitoring Physical Access
- Systems Management
- Physical Incident Response Actions

In addition, critical attended facilities typically require many more support assets such as UPS, chilled water, redundant external power supply, environmental controls, and communication infrastructure that the typical unattended facility would not require. Since these support assets are fundamental to the reliable operation of the critical facility, they are themselves critical assets and require appropriate physical protection.

Unattended facilities like substations are common elements in the electric industry. Substations contain many of the fundamental critical assets necessary for the transmission and distribution of electric power to customers. Transformers, breakers, busses, switches, capacitor banks, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Intelligent Electronic Devices (IEDs), and communication systems can reside within the confines of the substation. The compromise of any one of these elements can impact the integrity of the electric grid, depending on the amount and type of load being served by this substation at the time of the incident.

Approved by NERC Board of Trustees: October 15, 2004

While the substation is in many ways the "neuron" of the electrical network allowing effective monitoring and control of electric energy in that particular area of the network, they are attended for very short periods of time. Unlike control centers and most power plants that are staffed around the clock, there is typically no staffing, limited or no roving security patrols, and roofed structures are typically designed to protect electronic equipment and switch gear. Typically, substations out number power plants 30:1 and can be located in a downtown setting or in the most remote of rural areas. While most critical substations will logically be located in or near major load centers, interregional ties located in remote substations may be just as critical for interconnection purposes.

Substations are located in urban, suburban, rural, and industrial/commercial sites and the effectiveness of security methods differs greatly from site to site. Because of the diversity in substation size, location, and criticality, each substation should be assessed and classified. In general, more rigorous security measures should be applied to the more critical substations. While all substations are a critical element in the transmission and distribution of electric energy, not all substations are equally critical to North American electric grid reliability.

This guideline is intended to provide suggestions when considering the physical security at critical substations with a focus on practical methods using existing technology and proven processes. All of the security methods discussed here can be applied to existing substations, whether they are critical or not.

Definitions:

Entity — The facility or critical asset owner, operator, etc.

Critical Asset — Those facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety.

Intruder — Any unauthorized individual or any individual performing unauthorized activity within the substation.

Physical Security Perimeter — A type of gate, door, wall, or fence system that is intended to restrict and control the physical access or egress of personnel.

Security Assets — Fences, gates, alarm systems, guards, and other security elements that can individually or as a system be applied to critical electrical assets to maintain reliability or reduce risk.

Substation Secure Area — The area contained within the first or outer substation physical security perimeter.

Guideline Detail:

Physical security typically comprises five distinct elements, or systems:

- Delay/Deterrence
- Detection
- Assessment
- Communication
- Response

Together, these elements provide a consistent "systems approach" to protecting critical assets. While the application of these five elements will differ between substations, they all apply to some degree.

Each entity should prioritize its critical substations and associated critical assets. This prioritization should consider risks based on factors such as prior history of incidents, threat warnings from law enforcement agencies, loss of load consequences, response time, recovery time, and overall operating requirements. Each entity also should consider an inspection and assessment program to review existing security systems at substations and to make recommendations for appropriate changes. (See guideline for conducting vulnerability assessments.)

General Guidelines:

The details included below can generally be implemented with currently available technology. Many of these solutions are also discussed in the Physical Security Guideline:

1. fencing, gates, and other barriers to restrict access to the facility for both safety and security purposes;
2. limiting access to authorized persons through measures such as unique keying systems, "smart locks," access card systems, or the use of security personnel;
3. access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e., photo ids, visitors passes, contractor ids) to be displayed while in the substation;
4. alarm systems to monitor entry into substation grounds;
5. perimeter alarm systems to monitor forced intrusion into and surveillance of the substation;
6. alarms, CCTV, and other security systems reporting to an attended central security station that can then be evaluated and entity personnel or law enforcement authorities dispatched to investigate a potential problem;
7. guards (special events or targeted substations);
8. vehicle barriers;
9. adequate lighting;
10. signage;
11. a comprehensive security awareness program.

Physical security systems should be augmented in accordance with the "Threat Alert System and Physical Response Guidelines for the Electricity Sector" based on changes in threat levels, scenarios, and categories. In designing a physical security system, the objective of the intruder should be considered. The four major objectives in describing an intruder's behavior are:

- Damaging, operating, or tampering with substation equipment and controls,
- Stealing or damaging substation equipment, materials, or information,
- Posing a threat to the safety of entity personnel or customers,
- Creating adverse publicity.

Specific Guidelines:

1. Each entity should have a security policy or procedures in place to manage and control access into and out of critical substations. These policies should clearly state what practices are prohibited, which ones are allowed, and what is expected of all personnel with access to the substation. The substation security policies should clearly define roles, responsibilities, and procedures for access and should be part of an overall critical infrastructure protection policy.
2. The physical security perimeters at each substation should be clearly identified. All physical access points through each perimeter should be identified and documented. Most substations typically have at least two physical security perimeters such as the fence and the control house building. All access points through the substation fences and substation control houses should be identified.
3. Physical access controls should be implemented at each identified perimeter access point. All access into and out of critical substations should be recorded and maintained for a period of time consistent with NERC standards. At minimum, these records should indicate the name of person(s) entering the substation, their business purpose, their entity affiliation, time in, and time out.
4. Access into and out of critical substations should be monitored with authorization procedures. Substation access may be authorized by the system or security operator if not performed by electronic means such as a card reader where authorization is predetermined. Even if card readers are in place, it is recommended that personnel entering the substation contact the system or security operator so that the station can be tagged as "attended" in the event of an incident.
5. Records that identify all entity, contractor, vendor and service personnel that have unescorted access privileges to substations should be identified and documented. While most entity personnel will have unescorted access to all substations, contractors and vendors should only have unescorted access to substations they have contractual business in.
6. All contractors and vendors with critical substation access privileges should be required to pass a background screening before being issued an entity-provided contractor ID badge. Only those contractors with entity-issued ID badges should be granted unescorted substation access. Even in these circumstances, an entity employee

with unescorted access to the substation should confirm and monitor the contractor's activity while in the substation appropriately.

7. A substation incident response program should be established that at a minimum would provide a rapid assessment of events in the substation in order to differentiate normal electromechanical failures from malicious acts. If malicious activity is evident, the priority should be to notify law enforcement and return the substation to normal functionality while preserving forensic evidence where possible.
8. Entities should avoid dual use of critical substation grounds for non-critical functions where possible. That is, eliminate or restrict the use of the substation secure area for non-critical activities such as equipment storage, non-critical asset storage, contractor staging, and personal vehicle parking. If dual use is unavoidable, the entity should consider the establishment of another physical security perimeter that excludes the non-critical activities from the substation secure area, or the entire area should conform to this security guideline.

Security Asset Matrix Example:

As stated earlier, each entity should perform a risk assessment on all substations and prioritize each substation based on their own criteria for threat, vulnerability, and consequences. The security asset matrix example below is intended to illustrate how various substation security solutions might be applied. Because this security asset matrix example is intended to be an illustration only, three categories of substations are used for simplicity. In fact, most entities may find additional categories and security assets more useful. For the purposes of this security asset matrix example, Category 1 is a most critical substation, Category 2 is a moderately critical substation, and Category 3 is a least critical substation.

Security Asset Matrix:

	Category		
Security Assets	**1**	**2**	**3**
Card Key	▲		
Special Locks	▲	▲	▲
Security Guard (roving)	▲		
Fence	▲	▲	▲
CCTV	▲		
Door & Gate Open (SCADA)	▲	▲	
Alarm System	▲		
Motion Detectors	▲	▲	

While the security asset matrix example above appears static, the specific security solutions applied to each category of substation should be adjusted as needed to respond to relevant specific threat information.

Substation Security Assets:

Card Keys — A means of electronic access where the access rights of the cardholder are predefined in a computer database. Access rights may differ from one physical perimeter to another.

Special Locks — These may include locks with non-reproducible keys, magnetic locks that must be opened remotely, and possibly some sort of interlock system that restricts access through one perimeter while another is open.

Security Guard (roving) — Either staff or contract security personnel may randomly patrol multiple facilities. This asset is typically used for special events, periods of high threat levels, areas experiencing high intrusion levels, or substations that serve as a staging area for construction.

Fence — This is the minimal security asset and usually defines the first physical security perimeter encountered at the substation. There are several levels of fencing ranging from solid material, to standard chain link fencing (most common), to cable reinforced chain link fence.

CCTV — CCTV can be very effective in substation settings. Examples of pre-processed video surveillance that "cans" or captures images of activity in the substation preceding a substation security alarm can provide the system operator or security operator a "quick review" of the substation without requiring an operator to monitor traditional CCTV screens in real time.

Door & Gate Open (SCADA) — These alarms are typically based on some sort of "contact status" that indicates a door or gate has been opened. These alarms are particularly useful when used in conjunction with some sort of "attended station" status. Note: While these alarms, if received via SCADA, at most will represent only a handful of additional status points for the most critical substation, appropriate attention to RTU scan loading should be considered.

Alarm System — These systems typically incorporate several security solutions into a surveillance and alarming package. These package solutions are usually specific to a high-risk substation, do not interface with any other system, and are set up to provide enhanced forensic evidence at that site.

Motion Detectors — These devices use various means to detect motion in a specific area. While the IEEE's Standard 1402–2000 lists motion detectors as very effective in almost all sites, these systems can generate false alerts due to the open substation environment.

Exceptions:

None

Certified Products/Tools:

None

Related Documents:

Security Guidelines for the Electricity Sector: Guideline Overview

- Physical Security
- Vulnerability and Threat Assessment
- Threat Response
- Emergency Plans
- Continuity of Business Processes
- Communications
- Cyber Security
- Employment Background Screening
- Protecting Potentially Sensitive Information

IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE STD 1402-2000, January 2000.

Threat Alert System and Physical Response Guidelines for the Electricity Sector: Definitions of Physical Threat Alert Levels; A Model for Developing Organization Specific Physical Threat Alert Level Response Plans, Version 2.0, October 8, 2002.

Internet links:

- *Security Guidelines for the Electric Sector* http://www.esisac.com/library-guidelines.htm
- *Urgent Action Cyber Security Standard*, NERC, August 13, 2003, http://www.esisac.com/library-guidelines.htm
- *An Approach to Action for the Electricity Sector, Version 1,* NERC, June 2001, http://www.esisac.com/library-other.htm
- Threat Alert Levels and Physical Response Guidelines, NERC, October 2002, http://www.esisac.com/library-guidelines.htm

Revision History:

Date	Version Number	Reason/Comments
5/17/2004	0.01	Split out this draft into a separate guideline from the Physical Security Guideline and made several grammatical and content changes.
6/7/2004	0.02	Various wording changes. Added page numbers, alarm system description, and removed several Internet links.
7/1/2004	0.03	Minor wording changes. Omission of "projectile barriers" from page 5. Swap categories 1 & 3 on page 7. Change "CCTV" description on page 7.
7/20/2004	0.04	Various grammatical changes. Replace "must" with "should" where appropriate. Separated matrix example better. Introduced reference to Threat Alert System and Physical Response Guidelines for the Electricity Sector. Defined Intruder. Eliminated surveillance in Item 5 Under General Guidelines. Replaced "three years" with "consistent with NERC Standards".
8/16/2004	0.05	Various wording and grammatical changes. Altered definitions of critical facility and critical asset to more closely match the definition in the NERC Overview Guideline. Changed all references to company to entity. Returned security elements to original order. Added "Where appropriate" to specific guidelines.
8/19/2004	0.06	Removed "bulk" from applicability. Removed construction from Specific Guideline 8.
9/16/2004	0.07	Various wording changes. Changed definition of "Critical Asset" to that approved by CIPC. Added adjective "critical" as appropriate for clarification. Removed "Where appropriate" from Specific Guidelines. Returned "bulk" to Applicability.
10/15/04	1.0	Approved by NERC Board of Trustees.