SECTOR SPOTLIGHT: **Electricity Substation Physical Security**

In recent months, there has been an increase in reports of physical attacks on electric substations. Some incidents have resulted in thousands of customer outages. Attacks at several substations located in the Pacific Northwest during November 2022 resulted in customer outages and damage to substation equipment. On December 3, 2022, a physical attack on two substations in Moore County, North Carolina caused severe damage to the facilities. According to an energy provider, the ballistic attack resulted in approximately 45,000 outages. Federal authorities have also disrupted recent planned attacks before they were perpetrated.[1] Providing stakeholders and service providers with updated threat information and protective measures can improve a substation's on-site physical security—a vital strategy whether an attack is the result of domestic violent extremist (DVE) agendas or criminal actions by individuals.

The **Sector Spotlight: Electricity Substation Physical Security** increases awareness of available options that can enhance the physical security of electrical substations, establishes a means and path forward toward protected and resilient substations, and helps mitigate the inherent risks of owning and operating an electrical substation. Layered physical security is of the utmost importance to protecting an electrical substation and each substation requires a security plan tailored to its unique operating environment.

A substation is a high-voltage (HV) electric system facility used to switch generating stations, transmission systems, distribution systems, and to step voltages up or down, with some substations transforming and converting power from alternating current (AC) to direct current (DC) or DC to AC, respectively. Some substations are small with little more than a transformer and associated switches.

Step-Up Transmission Substations receive electric power from a nearby generating facility and use a large power transformer to increase the voltage for transmission to distant locations.

Step-Down Transmission Substations are located at switching points in an electrical grid. They connect different parts of a grid and are a source for subtransmission lines or distribution lines. The step-down substation can change the transmission voltage to a subtransmission voltage. The subtransmission voltage lines can then serve as a source to distribution substations.

Distribution Substations are located near end users with substation transformers changing the transmission or subtransmission voltage to lower levels for use by end users, including industrial, commercial, and residential customers.

LAYERED SECURITY STRATEGY

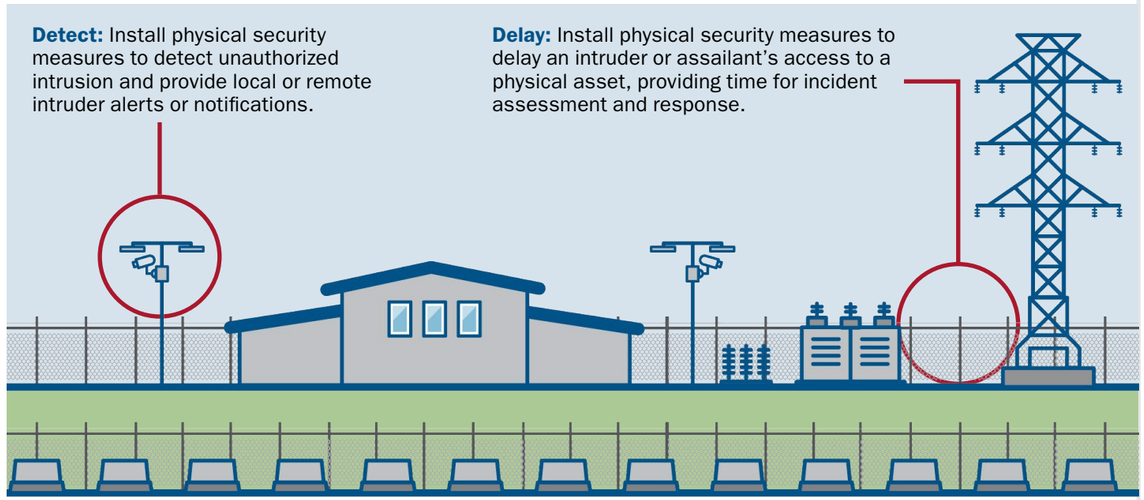
While it is impossible to prevent every attack against substations, there are mitigating steps—including physical protective security measures—to reduce or minimize the impact of an attack. Substation owners and operators should adopt a layered approach to physical security involving the following concepts:

Deter: Install visible physical security measures to dissuade potential attackers.

Assess: Develop a process to evaluate the legitimacy of an alarm and the procedural steps required to respond.

Communicate: Utilize communication systems to send and receive alarm/video signals and voice and data information. Include a documented process to communicate and report detected intrusions.

Respond: Develop measures to immediately assess, interrupt, or apprehend an intruder.



Intelligence Analysis: Design measures to collect, process, analyze, evaluate, and interpret information on potential threats.

Audit: Periodically review and inspect physical security measures to evaluate their effectiveness. This will be useful in post-incident forensics.

THREAT ENVIRONMENT

The North American electrical grid infrastructure is vulnerable to security breaches.[2] Consequences of security breaches include the possible damage or destruction of substation components resulting in service outages, as well as cross-sector impacts to other supported and supporting critical infrastructure sectors.

There are over 79,000 transmission substations in the United States;[3] attacks on these substations could result in severe outages or damage to the electrical grid. For more than 10 years, the electric utility industry and government agencies have engaged in activities to secure HV transformers from physical attack and to improve recovery in the event of a successful attack. These activities include coordination and information sharing, spare equipment programs, security standards, security exercises, and other measures.

Common attack methods and tactics, techniques, and procedures include:

Vandalism, Theft, and Sabotage: A physical attack that could potentially impact electric power system adequacy or reliability; vandalism which targets components of any security systems; damage or destruction of a facility that results from actual or suspected intentional human action.

Suspected Suspicious Behavior: Behavior such as unusual photography, surveillance, or pre-operational activities at a facility (excluding weather or natural disaster related threats) which has the potential to degrade the normal operation of the facility.

Physical Attack: A physical threat to a facility (excluding weather or natural disaster related threats) which has the potential to degrade the normal operation of the facility.

Cyberattacks: Attacks on cyber-components that could potentially impact electric power system adequacy or reliability.

Ballistic Attack: An attack involving small arms being fired at close range or those from high-caliber rifles fired from long distances against substation transformers and other critical components.

Explosive Device: An improvised explosive device (IED), vehicle-borne IED, or improvised incendiary device (IID) that could be used as a terrorist bomb attack against substation transformers and other critical components.

Vehicle Ramming Attack: The use of a vehicle as a weapon against security measures, substation transformers, and other critical components.

Unmanned Aircraft System (UAS): Unmanned Aircraft Systems can easily bypass traditional security measures to conduct surveillance and damage transmission lines and substations, and possibly be used to gain access to unsecured networks and critical operational components.

1 U.S. Federal Energy Regulatory Commission. *Docket No. RD23-2-000*, by Kimberly D. Bose. Order directing report. 2022. ferc.gov/media/e-27-rd23-2-000

2 National Academies of Sciences, Engineering, and Medicine. 2021. *The Future of Electric Power in the United States.* Washington, DC: The National Academies Press. doi.org/10.17226/25968

3 U.S. Department of Homeland Security. n.d. Homeland Infrastructure Foundation-Level Data (HIFLD) Open Data. hifld-geoplatform.opendata.arcgis.com/

SECTOR SPOTLIGHT: **Electricity Substation Physical Security**

PHYSICAL SECURITY PROTECTIVE MEASURES

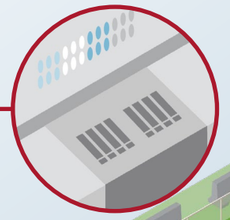
The first step in determining whether to adopt or implement any protective measures is to conduct a threat and vulnerability assessment (TVA) unique to each substation and in compliance with local and federal regulations. Protective measures should only be implemented based on a tailored threat assessment for each substation; a 'boilerplate' TVA approach—wherein the same TVA is applied to all substations—is highly discouraged and unlikely to adequately address specific threats for each unique substation.

After TVA completion for each substation, determine which substations should be prioritized. This distinction will assist with allocating limited resources to those substations whose loss or outage would have the greatest impact on the operation of facilities or assets served by the substation. Prioritizing by criticality is notably more important than prioritizing strictly by substation physical vulnerability.

Facility Controls

Control Center: If the substation is large enough to have a control center, all entrances should be electronically monitored and where possible, covered by closed-circuit television (CCTV) systems. All doors should be metal and fitted with an intrusion detection system (IDS); any windows should be covered with metal bars and shatter-resistant film.

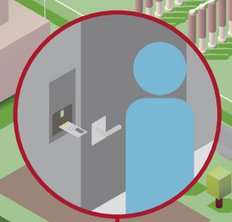
Control Cabinet: For smaller substations with no control house and fitted with a control cabinet mounted with the substation yard, all control cabinets should ideally be fitted with IDS, monitored by CCTV, and be ballistic resistant.



Monitoring and Surveillance

CCTV: Ensure CCTV covers the control house or control cabinet as well as access points to include vehicle gates and the entire perimeter of the substation. The CCTV feed should be recorded to enable better post-incident forensics.

Security Monitoring: Ensure security, operations, or maintenance personnel check substations—including small distribution substations— on a regular basis, and possibly on a varied timetable, so that attackers cannot take advantage of a predictable schedule. Regular site visits, along with a generally well-maintained substation site (both inside and outside the fenceline), are important deterrents.



Physical Access

Locks and Key Control: Establish and document key control procedures for key issuance, tracking, collection, loss, and unauthorized duplication. Use patented keys to prevent unauthorized duplication; conduct key inventories/audits in accordance with local standards.

Physical Security Control: Methods to control, monitor, and log physical access:

- Controlling physical access via card keys, special locks, or other authentication devices.
- Monitoring physical access via alarm systems or human observation of access points.
- Logging physical access via computerized logging, video recording, or manual logging.

Vehicle Access

Vehicle Gates: Ensure gates are properly functioning, well maintained, and secured with appropriate locking devices designed to resist tampering.

Vehicle Barriers: Consider use of penetration resistant physical barriers, such as concrete jersey-style barriers or other barriers to mitigate the use of vehicle as a weapon.

Personnel

Personnel Training: Provide security awareness briefings, including insider threat mitigation, to all personnel upon hiring and refresher training at regular intervals.

Outreach:

- Conduct outreach with local first responders and ensure they are aware of each substation's criticality/significance and which substations are the most important.
- Conduct outreach with residents living near substations (if applicable) and encourage them to report suspicious activity.

Drills and Exercises: Conduct periodic security drills or exercises in coordination with emergency responders.

Procedures

Communication: Develop written internal and external notification requirements and procedures for security events. Document and update contact information for local, state, and federal law enforcement agencies. Record law enforcement response times for each substation.

Maintenance and Testing: Develop written procedures to ensure security equipment is in functioning order with deficiencies addressed promptly.

Regulations: All substations must comply with federal regulations through the American National Standards Institute's *National Electrical Safety Code*, Occupational Safety and Health Administration guidelines, chemical safety and reporting standards, the National Energy Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, and follow all local regulations.

Perimeter Security

Ballistic Shielding: Consider installing shielding or obscuring the line of sight to protect critical components of the most important/critical substations.

Facility Lighting: Provide sufficient lighting for human or technological recognition of intrusion into facility perimeter or critical areas.

Perimeter Fencing: Ensure fencing completely encloses the substation; is well maintained; is updated in accordance with organizational standards; has appropriate signage indicating 'Tresspass is a violation of local laws' to discourage trespassing; and is free of vegetation to aid in facility access and sight lines.

RESOURCES

Chemical Facility Anti-Terrorism Standards: cisa.gov/chemical-facility-anti-terrorism-standards

ChemLock: cisa.gov/chemlock

CISA's Critical Infrastructure Exercises: cisa.gov/critical-infrastructure-exercises

Critical Infrastructure Vulnerability Assessments: cisa.gov/critical-infrastructure-vulnerability-assessments

CISA Infrastructure Security: cisa.gov/infrastructure-security

CISA Sector Spotlight: Cyber-Physical Considerations Electricity Sub-Sector: cisa.gov/sector-spotlight-cyber-physical-security-considerations-electricity-sub-sector

CISA Protective Security Advisors: cisa.gov/protective-security-advisors

Department of Commerce National Institute of Standards and Technology: nist.gov/

Electricity Information Sharing and Analysis Center: eisac.com/

North American Electric Reliability Corporation: nerc.com/Pages/default.aspx

US Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response (CESER): energy.gov/ceser/office-cybersecurity-energy-security-and-emergency-response

For more information or to seek additional help, contact us at **Central@cisa.gov**.