SLOAN
SECURITY GROUP

Scan to view on the web

WHITEPAPER

Substation Physical Security: Best Practices Every Plan Should Have

WWW.SLOANSG.COM

Substation Physical Security: Best Practices Every Plan Should Have

Physical security best practices to help protect electrical infrastructure from breaches, intrusions, blasts, and gunfire attacks.

Introduction

Terrorist attacks and criminals continue to target power utilities, dams, and electrical substations all over the world. Power substations are critical infrastructures that need to be protected with the latest physical security technology and best practices to prevent devastating power outages.

Physical protection for power generation sites must be carefully planned to reduce the threat of physical or ballistic attacks that can impact millions instantly.

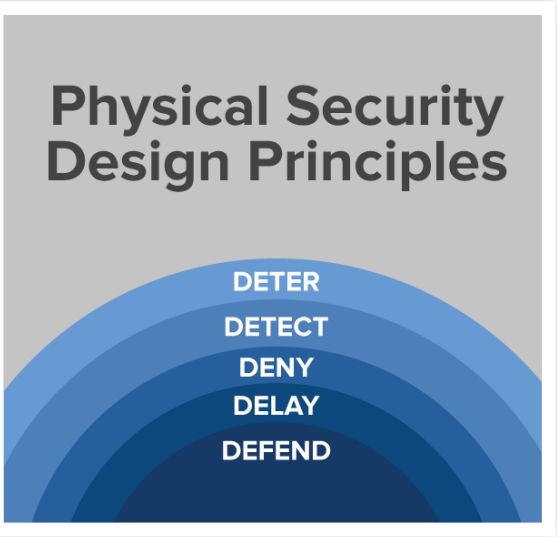
NERC and Critical Infrastructure Protection (CIP)

Following the 1965 Northeast Blackout, the United States Department of Energy established the North American Electrical Reliability Council (NERC) in 1968 to promote power transmission system reliability in North America. In 2006, the North America Electric Reliability Corporation (NERC) replaced it, which sets enforceable standards for reliability and critical infrastructure protection for the power transmission system. NERC manages the Critical Infrastructure Protection (CIP) program, which oversees critical infrastructure preparedness and response.

The Reliability Standard (CIP-014-2) guidelines are focused on protection for substations and their primary control centers. The goal of establishing these standards is to keep power operable in the event of an attack. Proper physical security design and integration are essential to secure power utilities and substations. Consider implementing some of these physical security best practices.

Physical Security Design Best Practices

To ensure effective physical security design, it is important to follow the 5 Ds principle: deter, detect, deny, delay, and defend. This principle works on the “onion skin” theory, where multiple layers of security are added to work together and reduce attempts of attacks, prevent site access, provide response time to breaches, and deny and defend if necessary. It is always wise to consult with experts in security design like Sloan Security Group. suggestions to address security challenges.



Sloan’s expertise covers a wide range of high-tech and low-tech solutions that have been gleaned from over 25 years of securing sites around the world. The design, construction, and maintenance of Military sites, U.S. Embassies, Oil/Gas facilities, Hydro-Electric dams, and Fortune 500 Corporate HQs have provided the Sloan team with a wealth of experience in the wide range of solutions available as well as knowledge in what different solutions cost and how difficult they are to implement.

Intrusion Detection and Monitoring

The deterrence layer of physical security includes visible barriers such as anti-climb and anti-cut fencing, high-security gates, surveillance cameras, signage, and more. The detection layer is responsible for the alarm function of these perimeter solutions and can be improved with non-visible monitoring solutions such as drone detection, thermal sensors, license plate readers, ground-based radar, and other detection systems.

Detection solutions are critical for responding to breaches or suspicious activity in and around the site. These detection devices need to be carefully designed to capture all threat possibilities. They need to extend from outside the perimeter walls to inside the fence where the transformers, turbines, and generators live. IP Video software and intrusion detection devices should deliver real-time surveillance feeds, recordings, and emergency alert systems to an off-site security team.

Perimeter Walls and Anti-Climb Fences

To meet CIP-014-2 NERC security standards, it's essential to use crash-rated fencing, walls, gates, and barriers at perimeter and vehicle access points. Ballistic-rated walls and fencing with anti-climb and anti-cut features, high-security gates, and crash-rated barriers can help prevent breaches and violent attacks.

Choosing the right barrier products requires considering the site design and environment and working with a security integrator can ensure the best outcome. The barriers should work together to achieve the 5 Ds principle of security: deter, detect, deny, delay, and defend.

Vehicle Access and Pedestrian Gates

To ensure power substations remain secure, aTo ensure power substations remain secure, authorized staff and vehicles must be the only ones to have access to buildings and surrounding areas. Restricting access through a role-based authentication system and limiting entry points can help monitor and manage access.

It's also crucial to have an access plan and procedure that all must adhere to. Security managers and their teams should prepare for worst-case scenarios, with heavy-duty crash-rated vehicle gates.

Personnel Training and Response

To ensure proper incident management, it is essential to have detailed documentation and a physical security checklist for power substations Conducting threat response drills and security audits can keep personnel prepared for potential incidents, as stress levels and adrenaline are likely to rise during such situations.

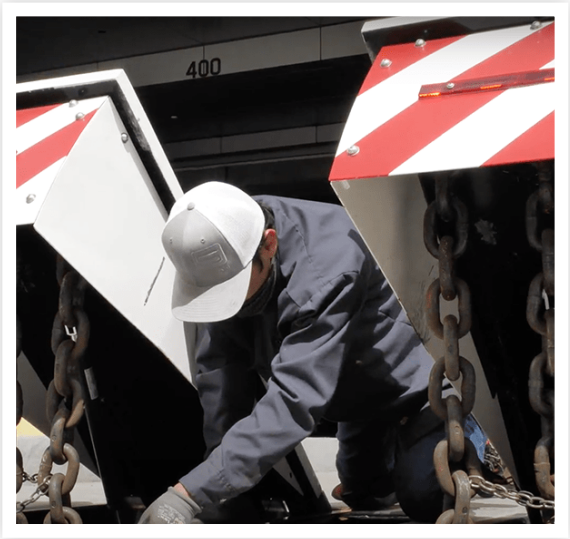
Proper equipment training is also crucial for personnel operating and managing barriers, performing test cycles, and coordinating repairs. Partnering with a company like Sloan Security Group to train personnel on barriers, gates, and security components can reduce human error and equipment malfunction.

Ballistic Threat Analysis

Threat analysis is critical to perform prior to the design phase of any substation security. In addition to intrusion, blast, and crash attacks, gunfire attacks have been trending upward. Ballistic attacks need to be accounted for and the use of sight-line analysis technology can reduce this vulnerability. The technology utilizes 3D modeling and simulations to determine where the design needs to include obstructions to defend against shooting a key part of the transformers that would cause a power outage. .

Perform Preventative Maintenance

Preventative maintenance can enhance the dependability and lifespan of security equipment like pop-up barriers, bollards, and automatic gates, improving overall performance and operational efficiency.



Outsourcing maintenance to a technical security services company like Sloan Security Group can be beneficial, as it ensures prompt support and maintenance without disrupting the internal team's workflow. 24/7 emergency repair support provided by companies like Sloan Security Group can limit unnecessary downtime

Conclusion

Attacks on substations are on the rise and having a robust and comprehensive physical security plan is critical.

As substation threats continue to grow, having a trusted partner to assist in your planning like Sloan Security Group is the best way to be prepared for the future. Being proactive and implementing some of these best practices will help substations have a more successful physical security outcome.

If you have questions about Substation Physical Security or need design assistance, please contact us.

SLOAN
SECURITY GROUP

Contact

Sloan Security Group, Inc.
6828 W. Melrose St.
Boise, ID 83709
+1-888-382-8379

WWW.SLOANSG.COM