

SECURING THE FUTURE

A DEEP DIVE INTO PHYSICAL SUBSTATION SECURITY



TABLE OF CONTENTS

3	INTRODUCTION	17	CONTEMPORARY SOLUTIONS FOR EFFECTIVE SAFEGUARDING
4	UNDERSTANDING THE THREAT LANDSCAPE	19	A CASE STUDY: SECURITY PLAN VALIDATION
8	KEY SECURITY CHALLENGES	21	STRATEGIC RECOMMENDATIONS FOR ENHANCING SECURITY
11	RISK ASSESSMENT PRIORITIZATION	23	A CASE STUDY: OPTIMIZED TRANSFORMER PROTECTION
13	NERC CIP REGULATIONS	24	BALANCING SECURITY COSTS WITH BUDGETARY CONSTRAINTS
15	REGULATORY COMPLIANCE VS. PROACTIVE SECURITY	27	CONCLUSION
16	INDUSTRY TRENDS AND COMPREHENSIVE STRATEGIES	28	REFERENCES

MITIGATING RISKS TO SUBSTATIONS: A TACTICAL APPROACH TO DEFENSE

The power grid is indispensable to nearly every aspect of daily life—from powering homes and businesses to ensuring the smooth operation of essential services.

Substations are vital components within this grid, responsible for transforming, controlling, protecting and distributing electricity efficiently and reliably across vast geographic areas. The significance of these facilities makes them attractive targets for malicious physical attacks, which have been steadily increasing in frequency for at least the past decade.

Disruptions in electricity supply can halt critical infrastructure operations that are crucial during emergencies, such as hospitals, water treatment plants and communications networks. Additionally, physical attacks can result in significant costs for utilities.

In an escalating threat landscape, there is an urgent need for more robust strategies to mitigate these risks.

This document provides a comprehensive overview of the challenges currently facing substation security professionals. Its primary focus is on physical security—such as vulnerability assessments, protective strategies, and incident response—it does not detail the distinct CIP regulatory standards that specifically address the increased risk posed by cyber threats.

Although the emphasis is on vulnerabilities at substations, the principles and recommendations outlined here are broadly applicable across all sixteen critical infrastructure sectors identified by the Cybersecurity and Infrastructure Security Agency (CISA). These sectors include chemical, commercial facilities, communications, critical manufacturing, emergency services, water and wastewater systems, nuclear reactors, materials and waste management, transportation systems and energy.

The physical and virtual assets, systems and networks within these sectors are considered essential to the United States. Their disruption or destruction could have severe consequences for national security, economic stability, public health and safety.¹

By exploring the costs associated with enhancing security measures alongside practical strategies for implementation, this document seeks to balance security effectiveness with feasibility.

01

UNDERSTANDING THE THREAT LANDSCAPE

Human-caused physical breach events—defined as physical attacks, vandalism, theft and suspicious activity—accounted for less than a quarter of all electric disturbance events reported to the United States

Department of Energy (DOE) in 2021. By 2023, that number had risen to account for more than half of the year's reports.²

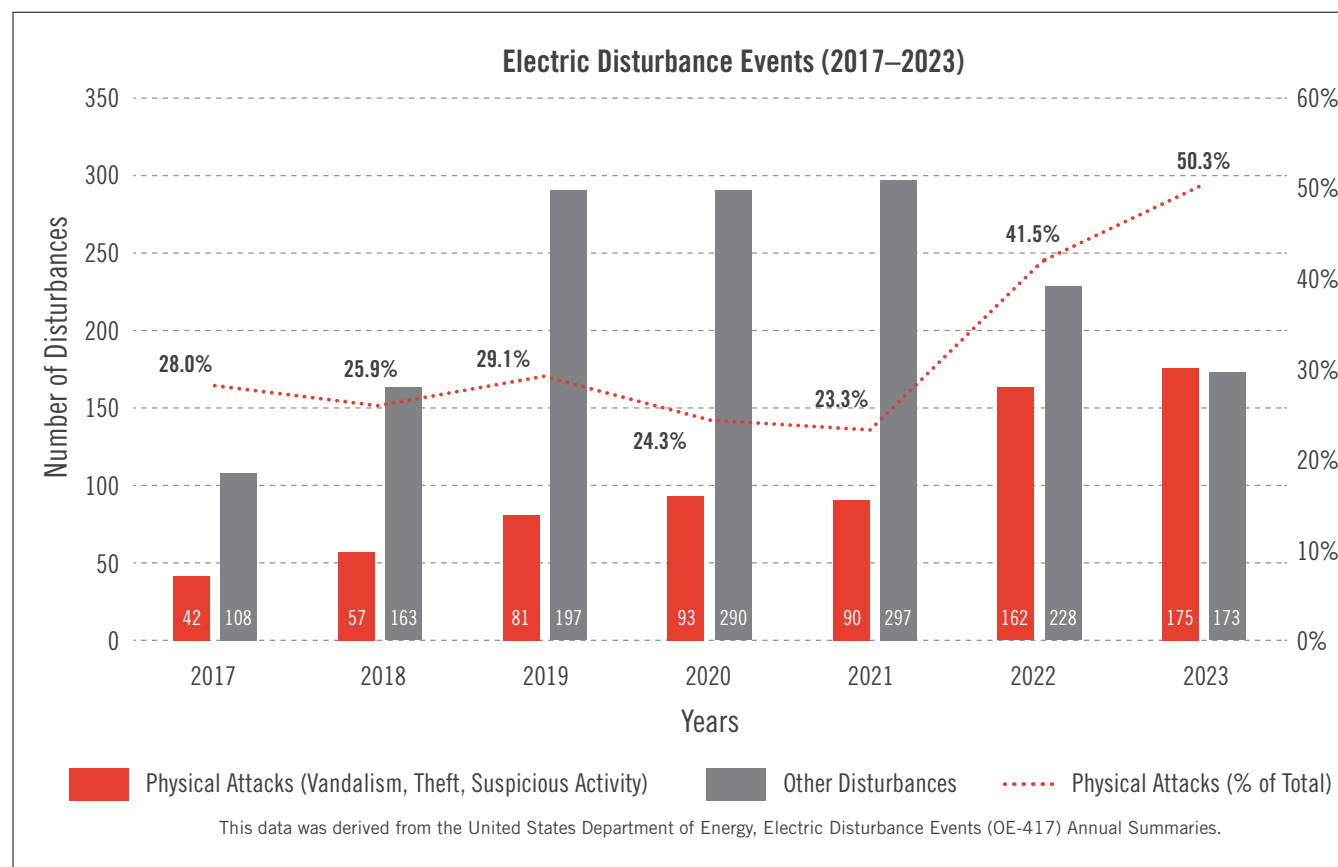


Figure 2: Electric Disturbance Events (2017–2023)²

A detailed analysis of the DOE data reveals a troubling trend: the reported number of human-caused physical disturbances has increased significantly, from 42 incidents in 2017 to 175 incidents in 2023.² This underscores an alarming upward trajectory that is expected to continue into the coming years.

Additionally, between 2017 and 2023, only four states did not report human-related physical incidents to the DOE. California, Texas and Washington state have seen the most incidents within this timeframe, as shown in Figure 2.

WHY IT MATTERS

Utilities have been seeing higher operational costs due to the expenses associated with repairing and replacing vandalized or stolen equipment as well as the cost of investing in enhanced security measures. Widespread power outages can also come with longer restoration times, which can damage utility reputations and result in economic losses for businesses reliant on stable power supplies.

Damaged electrical equipment also poses a greater risk of injuries or fatalities among utility workers and first responders responding to attack-related incidents.

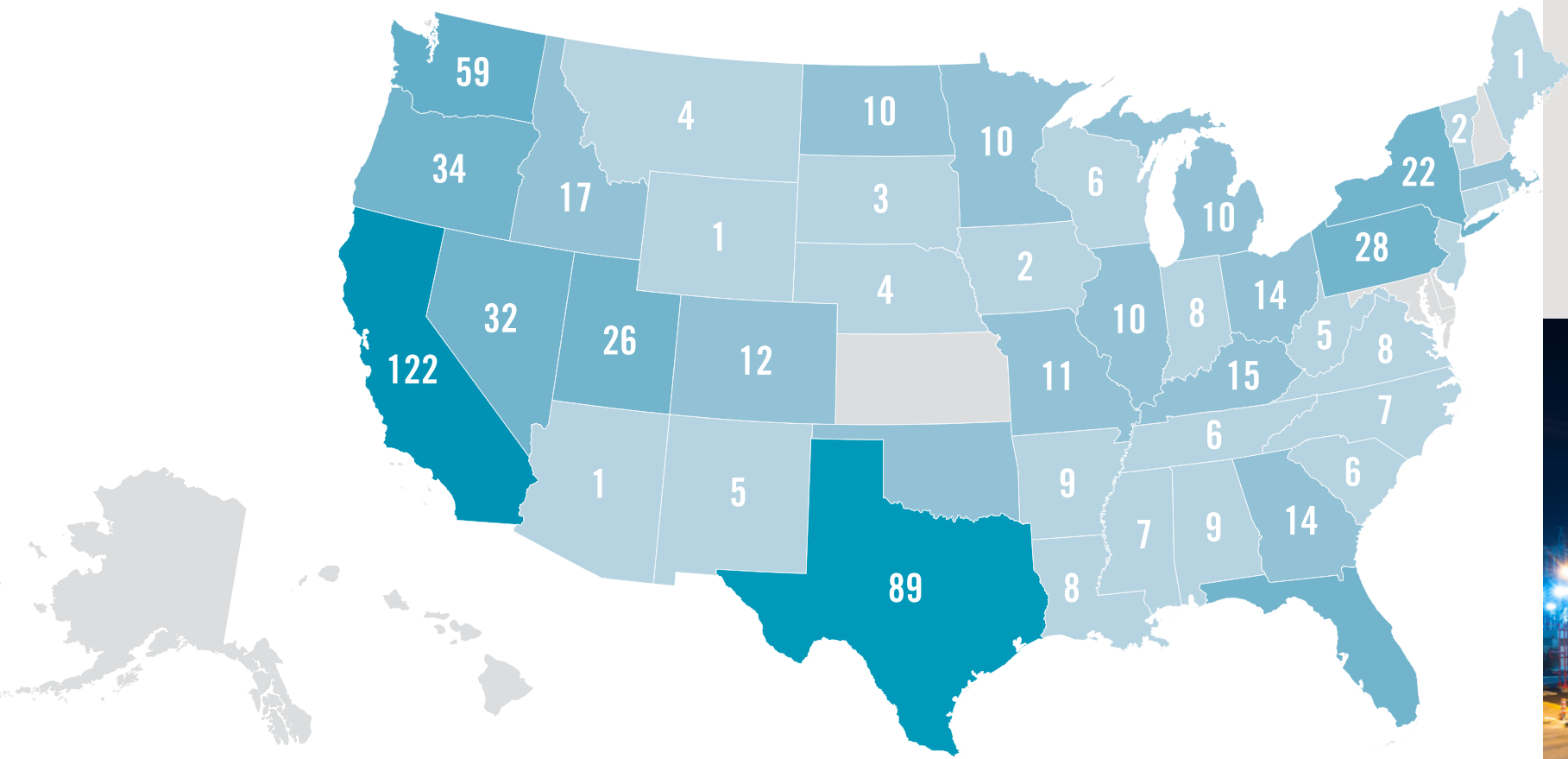


Figure 2: Human-related physical incidents (2017–2023) by state.²



METHODS OF PHYSICAL ATTACK

A variety of physical attack methods have been reported throughout the years, each posing unique challenges for substation security. The following are examples that have been observed in the power delivery industry, as identified by the Cybersecurity and Infrastructure Security Agency and DOE.³

- Vandalism, theft and sabotage
- Ballistic attack
- Explosive devices
- Vehicle ramming attacks
- Unmanned aircraft systems

Many security professionals are keeping an eye on drone, unmanned aerial vehicle and flying improvised explosive device threats overseas, anticipating that such threats will soon become more prominent in the United States.

MOTIVATIONS BEHIND PHYSICAL ATTACKS

Understanding why physical attacks happen is crucial for developing effective security strategies.

» **Terrorism or Extremism**
Terrorism—both foreign and domestic—may be the greatest threat the United States power grid currently faces. With access to constantly evolving technologies, techniques and information, terrorist organizations are becoming alarmingly more organized, sophisticated and violent.





- » **Criminal Activities**
Many physical breaches are motivated by criminal activities such as opportunistic vandalism and copper theft. The valuable materials present in substations make them attractive targets for thieves seeking quick profits. Additionally, general criminality can lead to break-ins or thefts of tools and other equipment.
- » **Copycat Attacks**
Prominent incidents like the Metcalf Substation attack in California have inspired copycat attacks. These events can create a ripple effect where similar methods are replicated by individuals looking to cause damage without the original intent.
- » **Misinformation and Disinformation Campaigns**
Misinformation and disinformation campaigns spread false information that may incite individuals or groups to take destructive actions based on misguided beliefs.

NOTABLE HIGH-PROFILE INCIDENTS

Over the years, several high-profile incidents have highlighted the vulnerability of critical infrastructure to physical attacks. These events not only caused significant damage but also raised awareness about the need for more robust security measures.

- » **California Sniper Attack (2013)**
One of the most influential physical incidents occurred in California in 2013 when snipers targeted the Metcalf Substation. This coordinated attack resulted in \$15 million in damages and brought national attention to the issue of physical security at substations. The attackers fired over 100 rounds, disabling 17 transformers and causing widespread concern about the potential for similar attacks.
- » **North Carolina Gunfire Attack (2022)**
In 2022, gunfire disabled two substations in North

TABLE 1: A BRIEF BREAKDOWN OF COMMON EXTREMIST IDEOLOGIES

 POLITICAL	 NATIONALIST/SEPARATISTS	 RELIGIOUS	 SPECIAL INTEREST
Those who subscribe to an extremist political framework and resort to violence in an attempt to influence a government or political situation.	Devoted to the interests or culture of a group or a nation. Typically share a common ethnic background and wish to establish or regain a homeland.	View modernization efforts as corrupting influences on their society or traditional religious culture.	Groups who subscribe to other extremist ideologies or doctrines that resort to violence to achieve a goal or spread a message for a specific cause.

Carolina, leaving 45,000 customers without power for several days. This incident underscored the devastating impact that such attacks can have on communities, particularly when they result in prolonged outages affecting thousands of households and businesses.

- » **Washington State Coordinated Vandalism (2023)**
During the holiday season of 2023, coordinated vandalism at four substations in Washington state disrupted power for thousands of residents. This attack demonstrated how even amateur coordinated efforts can cause significant disruptions.
- » **Tennessee Telecommunications Bombing (2020)**
Critical assets in other industries are becoming prone to physical attacks as well. On Christmas Day in 2020, a bombing in Nashville, Tennessee resulted in a communications blackout that extended from Georgia to Kentucky. The explosion impacted communications to and from emergency services and law enforcement, revealing vulnerabilities within telecommunications infrastructure. This incident emphasized the

interconnected nature of critical infrastructure sectors and their reliance on secure communication channels.

WHAT MAKES SUBSTATIONS AN ATTRACTIVE TARGET?

Substations are essential for transforming voltage levels and ensuring the reliable distribution of electricity. However, this makes them attractive targets for malicious attacks. The reason behind this attraction may vary based on the following factors:

- » **Geographic Dispersion or Remoteness**
Substations in remote locations are difficult for first responders to get to quickly. This gives attackers more time to carry out their activities without immediate detection or interference.
- » **Criticality**
Substations play a crucial role in maintaining grid stability and reliability, and a strategic disruption can cause widespread power outages that affect homes, businesses, emergency services and critical

infrastructure. The high impact of such disruptions makes substations prime targets for those looking to cause significant harm.

- » **Relative Vulnerability**
Compared to other parts of the power grid, like generation facilities, substations often have relatively less physical security. Traditional security measures like chain-link fences, while sufficient many years ago, are no longer the most effective mitigation strategy for modern, evolving threats.
- » **Under-Protection**
Implementing comprehensive security measures across all substations can be expensive. The large physical footprint of many substations means protecting every access point and potential vulnerability can be challenging and resource intensive. Utilities must often choose between effectiveness and cost, leading to potential gaps or a complete absence of security coverage. Unprotected substations are an easy target.



A good operational security program will deny intelligence to threat actors. Be aware of the techniques they might use to collect information and avoid rigid operational routines. The less they know about our grid's vulnerabilities, the better.

—CHRIS OTT, E.E., PHYSICAL SUBSTATION SECURITY SPECIALIST

02

KEY SECURITY CHALLENGES

Current substation security efforts are susceptible to a variety of challenges, especially with how rapidly threats are evolving. Some of these challenges are explored below.

THE LIMITATIONS OF CURRENT ASSESSMENT METHODOLOGIES

When it comes to mitigating ballistic threats, the following traditional site analysis methods have been widely used to inform security decisions. However, each method presents significant challenges that can hinder effective threat assessment and mitigation.

Field Inspector Site Analysis

Traditional site analysis has typically required a field inspector to travel to the location to conduct a physical site walk, which entails having an individual walk around and test the areas that they think are most vulnerable.

One challenge of this approach is that it is **subjective**, relying on the expertise and attentiveness of the inspector. It has the potential to introduce human error and negligence, which may leave some vulnerabilities unidentified and unaddressed.

Another challenge is **safety**. Not everyone who needs to contribute to mitigations will have the necessary training to safely visit a site. In high-voltage environments especially, there are a lot of hazards present that may complicate an

individual's ability to thoroughly inspect the area and leave some critical assets unassessed.

Coordination is also tricky in this method. The obstacles associated with gathering multiple individuals in one physical location can hold up a project for days, or even weeks.

Finally, **access restrictions** can be a big problem. If an area of concern is not owned by the station owners or operators, gaining access to view and assess the area can be difficult. In addition to land use and ownership challenges, some areas may have limited access because of the potential dangers they contain. This may result in an incomplete evaluation of the study area and may conceal critical vulnerabilities.

Static Analysis with Public Data

A lot of traditional site assessment strategies will use publicly available data as a starting point for their analyses. From there, they will often create static shop drawings that will be iterated upon by engineering, design and drafting teams until a suitable mitigation strategy is identified.

One challenge of this method is **accuracy**. The accuracy of publicly available data from sources such as online maps can vary dramatically from location to location. There is no guarantee that the mapping data will be of high enough quality to conduct a thorough and precise assessment.

Relevancy is another challenge, since some publicly available data is old enough that it no longer provides an accurate depiction of the current location. Substation layouts can be altered, buildings can be erected nearby and vegetation shields can die off. Trying to consolidate outdated data with current information can be time consuming and labor intensive, delaying the analysis and decision-making processes.

Adaptability is also an issue. The static engineering drawings produced by this method have limited use cases beyond the initial assessments. They can be difficult to update, meaning that they have limited value to evolving and future project needs. Additionally, while they are often used to communicate design decisions with constituents and stakeholders, they can be difficult for presentation audiences to understand and interpret.

VISA Methodology

The Vulnerability of Integrated Security Analysis (VISA) methodology, which is endorsed by E-ISAC as the primary or recommended methodology for power utilities, leverages subject matter experts from various disciplines to logically develop and evaluate scenarios. It can be based on documented values, professional judgment or a combination of both. The process

involves gathering professionals into the same room to engage in multiple multi-hour collaboration sessions, but while it is an extremely useful collaboration guideline, it does have a few limitations.

One of which is the **expertise** of the individuals involved. The quality of the analysis conducted through this methodology is limited by the capabilities of the subject matter experts who attend. Failing to include the right individuals can lead to unrepresented perspectives and potential gaps in mitigation strategies.

Another challenge is **visualization**. During collaboration sessions, the subject matter experts typically work from static photos, graphics and drawings. This can make it difficult to quickly communicate ideas and answer questions. Static resources may also lack information about specific scenarios that may come into question, such as the view of a particular angle of a substation.

Like with field inspections, **coordination** is also an issue for this method. It can be difficult to coordinate all participants in the same room for multiple sessions. Experts may be based in different locations and may be in demand for other projects in faraway places.

No Analysis

In lieu of lengthy analyses and review processes, some utilities have chosen the simplest option: no analysis. Instead of pinpointing vulnerabilities many have elected to erect large concrete walls around the entire perimeter of their facilities in hopes of quickly complying with regulatory requirements.



This method tends to result in **overbuilding**. In most situations, building a wall around the entire perimeter of a substation is significantly more mitigation than is needed. This means that some facilities are spending time, money and effort on security solutions that are not protecting anything.

Because of this, many utilities are also **overspending**. While this approach may save some time, it certainly does not save money. Construction and material costs are expensive and will likely be significantly higher than the costs that would have been associated with strategic security analyses and the subsequent security upgrades.

Finally, this method can cause locations to be **under protected**. While a perimeter wall will likely mitigate the majority of vulnerabilities, it can still leave portions of a facility unprotected. Neighboring hills or buildings, for example, could provide line-of-sight to critical assets above those walls.

These problems may not be present in all instances where perimeter walls are the chosen mitigation strategy, but without analysis, it is impossible to know if the strategy is living up to its perceived value. This can make it difficult to justify the cost of building around everything to shareholders.

In addition to these limitations, traditional methods also often overlook critical parameters such as social, political and economic contributions to substation vulnerability. There may also be little evidence used to support decisions to include or exclude certain threats.

A REACTIVE VS. PROACTIVE SECURITY APPROACH

A major limitation of current security practices is their post-incident focus. Security measures are frequently implemented only after an attack or breach has occurred, leading to a cycle of reacting to threats rather than anticipating and mitigating them beforehand. This approach leaves critical assets vulnerable during the interim between identifying new threats and deploying appropriate countermeasures.

LIMITED DATA-BASED RISK PREDICTION

Traditional assessments often depend on historical incident data or subjective expert opinions without leveraging advanced predictive modeling techniques.

Data-based risk prediction involves integrating diverse datasets into sophisticated algorithms that utilities can use to better anticipate potential threats, identify patterns and prioritize resources towards the areas that are most at risk.

A lack of robust predictive capabilities leaves utilities ill-prepared against the evolving threat landscape. Without the foresight of advanced analytics, they remain one step behind adversaries who are constantly adapting their tactics.

COST CONSTRAINTS

Finally, the cost of upgrades can be prohibitive for smaller utilities, and many cannot justify conducting on-site assessments that occupy internal resources.

TABLE 2: THE LIMITATIONS OF LEGACY SECURITY ANALYSIS METHODS.

Methodology	Limitations
Field Inspector Site Analysis	Subjectivity
	Safety
	Coordination
	Access Restrictions
Static Analysis with Public Data	Accuracy
	Relevancy
	Adaptability
VISA Methodology	Expertise, if available (resource dependent)
	Visualization
	Coordination
	Evidence for audit
No Analysis	Overbuilding
	Overspending
	Under Protecting
	Compliance issues

RISK ASSESSMENT PRIORITIZATION

BALANCING COST AND RISK

Substation owners and operators face the challenge of securing thousands of substations while managing limited budgets, meaning prioritizing investments based on risk assessments is crucial. However, not all substations present the same risk profile.

The National Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards recommend

evaluating the criticality of substations based on a set of criteria and ranking them with the most critical substations gaining the highest priority for security upgrades. These criteria include things like what kind of customers and populations it serves and whether it is part of an interdependent system that could result in cascading failure if targeted.

However, this risk assessment can be applied even further.



Those responsible for infrastructure outside of [NERC] CIP-014's jurisdiction would do well to adopt these security requirements for their out-of-scope systems, too. . . The value of this standard goes beyond keeping [the most] critical [stations] secure.⁴

—CHRIS OTT, SENIOR PHYSICAL SECURITY EXPERT

EVOLVING THREATS

Modern attackers employ diverse tactics that include not only conventional methods, but also advanced and emerging technologies. Drones, for example, can be used for surveillance or to deliver destructive payloads, complicating defense efforts. Additionally, cyber-physical incidents—where digital attacks are combined with physical actions—pose significant challenges by targeting both infrastructure and control systems simultaneously.

Risks

A decade ago, shortly after the start of widespread attacks on substations, a federal analysis conducted by FERC and reported by the Wall Street Journal indicated that the U.S. could suffer widespread blackouts if saboteurs knocked out just nine specific substations.⁵

Consequences/Impact--How event risk levels affect the bulk power system (BPS)	
C5 Severe	Impacts may have widespread effects to the BPS across North America.
C4 Major	Impacts may have widespread effects to the Regional Center (RC) area.
C3 Moderate	Impacts may have widespread effects to portions of the RC area.
C2 Minor	Impacts may have effects on the local entity.
C1 Negligible	Impacts may have small or non-existent effects to the BPS.

Reliability Risk Matrix					
Consequence/Impact (C)	Likelihood (L)				
	L1 Very Unlikely	L2 Unlikely	L3 Possible	L4 Likely	L5 Almost Certain
C5 Severe	High	High	High	Extreme	Extreme
C4 Major	Medium	Medium	High	High	Extreme
C3 Moderate	Medium	Medium	Medium	High	High
C2 Minor	Low	Low	Medium	Medium	Medium
C1 Negligible	Low	Low	Low	Low	Low

Figure 3: A risk matrix to determine the criticality of various scenarios.⁶

Likelihood—What is the reasonable probability that consequences will occur?	
L5 Almost Certain	Mandatory Controls—No NERC reliability standards in place for mitigation. Emerging Trends—Increasing trends have been identified. Event History—Documented events or widely publicized exploits have been recorded.
L4 Likely	Mandatory Controls—No NERC reliability standards in place for mitigation. Emerging Trends—Some trends have been identified. Event History—Documented events or generally publicized exploits have been recorded.
L3 Possible	Mandatory Controls—NERC reliability standards in place for limited mitigation. Emerging Trends—Some trends have been identified. Event History—No documented events, or moderately publicized exploits have been recorded.
L2 Unlikely	Mandatory Controls—NERC reliability standards in place for mitigation. Emerging Trends—Some trends have been identified. Event History—No documented events or minimally publicized exploits have been recorded.
L1 Very Unlikely	Mandatory Controls—No NERC reliability standards in place for mitigation. Emerging Trends—No known trends have been identified. Event History—No documented events or publicized exploits have been recorded.

NERC CIP REGULATIONS

The NERC CIP-014 standard⁷ is designed to protect critical transmission stations, substation and primary control centers from physical attacks that if rendered inoperable could result in instability, uncontrolled separation or cascading failures within the grid. Its primary focus is identifying facilities deemed critical to the bulk electric system and incentivizing measures to mitigate security risks at these facilities.

HOW TO KNOW IF A TRANSMISSION FACILITY IS CRITICAL⁷

1. **Voltage inclusion criterion:** Substations operating at 500 kV or higher automatically qualify as critical due to their role in grid stability
2. **Weighting factor inclusion criterion:** Substations operating between 200 kV and 499 kV that are connected to three or more other substations and have an aggregate weighted value exceeding 3000 are considered critical
3. **Interconnection reliability operation limits (IROL):** Facilities identified by reliability coordinators, planning coordinators or transmission planners as critical to IROL derivation are included due to their importance in maintaining grid stability
4. **Nuclear plant interface requirements:** Facilities essential for meeting nuclear plant interface requirements are also included in CIP-014 applicability criteria

KEY REQUIREMENTS (R1-R6) OF NERC CIP-014

The following information is a summarization of the requirements outlined in the NERC CIP-014 standard.⁷ For additional details and information about exemptions, please consult the standard directly.

Requirement R1—Risk Assessment

This requirement mandates that substation owners and operators perform an initial risk assessment and subsequent risk assessments on their critical transmission facilities.

Subsequent risk assessments are required every 30 or 60 calendar months, depending on whether the transmission owner has identified one or more critical transmission facilities in previous risk assessments.

Requirement R2—Verification

This requirement requires owners and operators to have an unaffiliated third party verify the risk assessment performed under requirement R1. The unaffiliated verifying entity must be either:

- a. A registered planning coordinator, transmission planner or reliability coordinator; or
- b. An entity that has transmission planning or analysis experience

Requirement R3—Notification

Transmission owners must notify transmission operators about identified critical facilities under their operational control.

Requirement R4—Threat Evaluation

Transmission owners must evaluate potential physical security threats and vulnerabilities for identified critical substations or control centers.

Requirement R5—Physical Security Plan Development

Transmission owners must develop a documented plan within 120 days after completing requirement R2.

Requirement R6—Third Party Review and Periodic Review

Transmission owners must review their physical security plans at least once every 30 months to ensure they remain effective against evolving threats.

THE IMPACT OF NERC CIP-014

NERC CIP-014 ensures that limited industry resources are focused on protecting the most critical facilities within the bulk power system. It prioritizes high risk substations that could cause widespread outages if compromised; provides a structured framework for assessing risk, implementing security measures and coordinating with law enforcement; and, by requiring periodic reviews, it ensures that utilities review and adapt their plans to address evolving threats.



REGULATORY COMPLIANCE VS. PROACTIVE SECURITY

While the NERC CIP-014 standard outlines requirements for identifying critical assets and implementing physical security measures, and while compliance is essential, it should be viewed as a baseline for security practices rather than a comprehensive solution.

GOING BEYOND COMPLIANCE

Proactive utilities are investing in measures that exceed regulatory requirements, including:

- » Advanced technologies that identify line-of-sight threats
- » AI powered surveillance tools
- » Regular training exercises with law enforcement

The often-cited 5Ds of security—deter, detect, deny, delay and defend—have been given a new treatment under NERC CIP-014. Security plans are now being designed collectively to deter, detect, delay, assess, communicate and respond to threats.

QUICK TIPS FOR PROACTIVE APPROACHES

1. Having a security specialist involved in site selection can result in cost savings for security systems later in the design process.
2. Site security analyses can be useful for many other disciplines, provide evidence for audits and help build a comprehensive security plan.
3. Waiting to bring security experts into the design process can add financial, operational spacing restraint and limitations on protection challenges.

INDUSTRY TRENDS & COMPREHENSIVE STRATEGIES

COMMON PHYSICAL MEASURES AND MITIGATION TACTICS

Perimeter Protection

- › Implementing gunshot detection systems can provide instant alerts during incidents, enabling rapid response. Pairing these systems with other systems like security cameras can help reduce false alarms or false positive results.
- › Anti-climbing fencing and reinforced vehicle gates deter unauthorized access and vehicle-based attacks.
- › Vegetation management is crucial; clearing dense foliage improves visibility while strategic planting can act as a natural barrier.

Critical Asset Protection

- › Erecting walls or billboards around critical assets offers additional layers of defense against ballistic threats.
- › Exploring innovative mitigations tailored to each site's unique characteristics enhances overall security.

Worst-Case Incident Procedures and Drills

- › Regularly conducting drills simulating worst-case scenarios ensures preparedness among staff, strengthens response protocols and minimizes potential downtime during actual events.
- › Establishing strong relationships with local law enforcement agencies bolsters situational awareness through information sharing about emerging threats or suspicious activities near substations. Collaborative planning enables coordinated responses during incidents.

Rapid Recovery Plans

- › Maintaining an inventory of spare equipment reduces lead times for repairs or replacements after an attack, facilitating swift recovery efforts without prolonged outages.
- › Developing detailed recovery plans prioritizes restoring power quickly following disruptions by identifying critical paths for repair work based on impact assessments conducted beforehand.

COST FACTOR CONSIDERATIONS

Within limited budgets, substations must weigh the risks posed by potential attacks against the costs associated with recommended mitigations. While larger operators might adopt a “build around everything” strategy involving extensive perimeter defenses like concrete barriers encircling entire facilities—this approach has its drawbacks too:

- » It may lead to overbuilding where resources could be better allocated elsewhere within the grid network instead of protecting non-critical areas unnecessarily.
- » High initial investments in construction materials along with ongoing maintenance expenses can strain financial resources over time without necessarily providing proportional benefits relative to other targeted interventions focused on specifically high-risk zones.

To address these challenges effectively, utilities should pursue balanced approaches integrating data-driven risk assessments alongside cost-effective solutions designed to maximize protection returns.

CONTEMPORARY SOLUTIONS FOR EFFECTIVE SAFEGUARDING

Recognizing the need for comprehensive, data-backed security assessments, a team of physical security experts and visualization specialists at POWER Engineers, member of WSP, set out to create a tool that could quickly and accurately identify vulnerabilities and test mitigations in an interactive virtual environment.

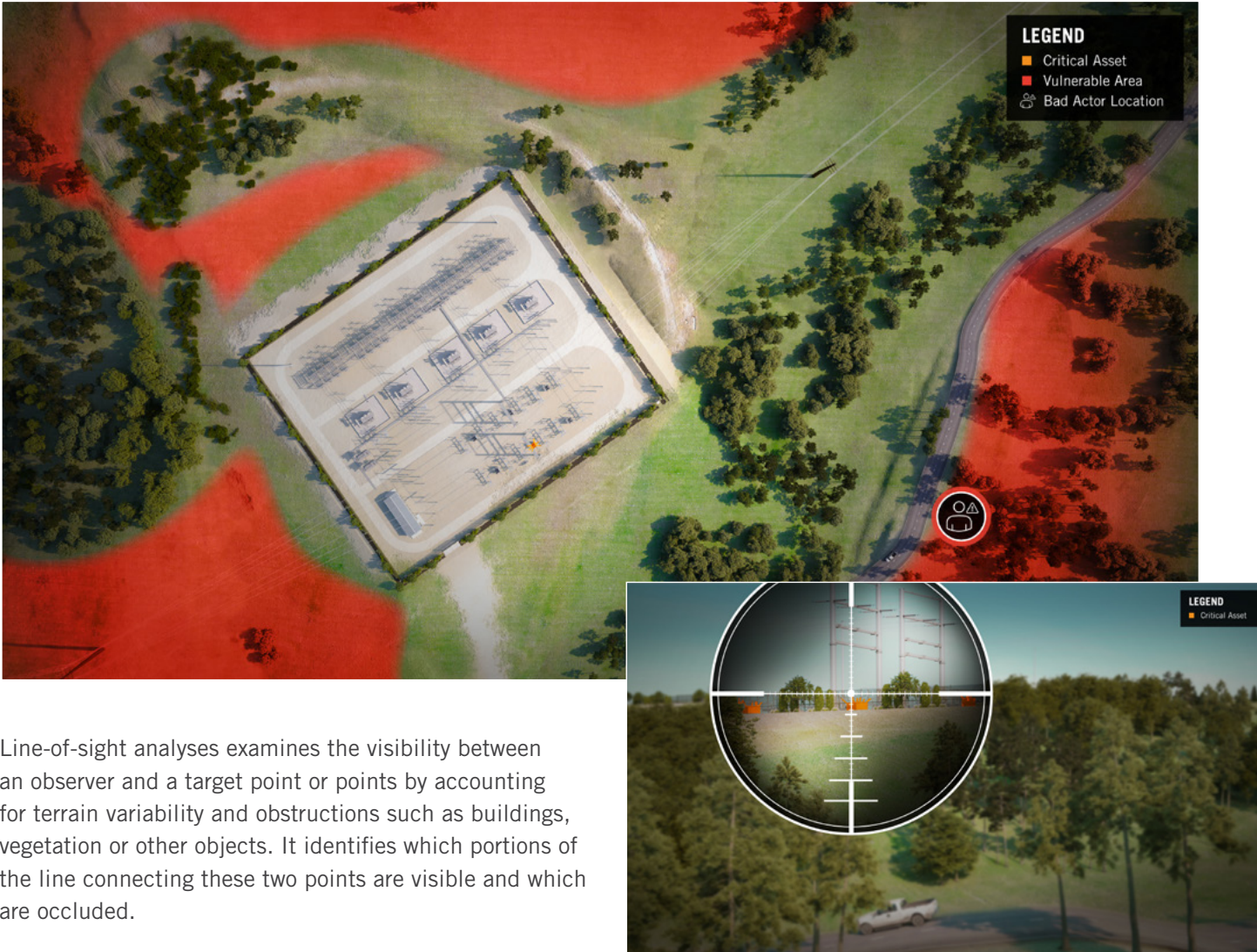
CLARITY THROUGH DATA: SMARTER LINE-OF-SIGHT ASSESSMENTS

- » Acquire **high-fidelity, quality data** that drives informed decision making.
- » Receive **accurate digital recreations of substations** and their surrounding environments that ensure a thorough visualization of vulnerabilities.
- » Experience **real-time assumption testing** in an interactive virtual environment.
- » Gain direct access to an **industry-leading team** of experts.
- » Obtain **comprehensive threat mitigation reports** and secure transfer of a 3D model.
- » Unlock **enhanced collaboration** and decision-making protocols to effectively safeguard your energy assets.
- » Invest in an innovative solution and **minimize the subjective evaluation and human error** inherent in traditional assessment methods.
- » Secure compliance assurance or **third-party validation**.
- » Develop **cost- and time-efficient solutions**.
- » Reveal **optimal placement** of security cameras and other equipment.



Figure 4: Chris Ott demonstrates the value Meerkat™ provides.

WHAT IS A LINE-OF-SIGHT ANALYSIS?



Line-of-sight analyses examines the visibility between an observer and a target point or points by accounting for terrain variability and obstructions such as buildings, vegetation or other objects. It identifies which portions of the line connecting these two points are visible and which are occluded.

Line-of-sight analyses are highly effective for security applications. They enable security planners and managers to evaluate visibility between strategic positions, identify obstructions and optimize surveillance and defense strategies.

Figure 5: Maps exposure points and direct sightlines to transformers (inset: threat actor's perspective)

APPLICATIONS OF LINE-OF-SIGHT ANALYSES

Urban Planning⁸

- » Assess visual impacts of new infrastructure on landmarks or scenic views
- » Optimize building placements to preserve visibility corridors

Telecommunications⁹

- » Determine optimal locations for cell towers or antennas to ensure signal coverage
- » Identify obstructions that may block radio signals

Transportation¹⁰

- » Evaluate sight distances for road safety
- » Analyze driver visibility on highways using single-line or radial methods

Astronomy and Navigation¹¹

- » Use line-of-sight for deep-space navigation by tracking celestial bodies

Security and Defense^{12, 13}

- » Secure event venues by analyzing visibility from various vantage points
- » Augment security plans for critical infrastructure or components

These analyses typically require high-quality digital elevation models (DEMs) or digital terrain models (DTMs) to meet data accuracy requirements. The results can also vary with changes to factors like observer height, terrain resolution and zoom level.

A CASE STUDY: SECURITY PLAN VALIDATION

Due to the sensitive nature of security projects, the following case study has been sanitized of any identifying information.

Background: *A client with a 3,523 linear foot fence line was planning to construct an all-new 15 ft tall concrete masonry unit (CMU) wall around the perimeter of their substation to protect their critical assets from a line-of-sight attack. This facility's existing security perimeter was made of a chain-link legacy fence. It was old, outdated and due for replacement. However, they wanted to validate this decision before moving forward. For this, they partnered with physical security specialists at POWER Engineers, Member of WSP, who performed a threat assessment using their Meerkat™ tool.*

Security Plan Validation: *The first step of testing the validity of the security plan was modeling the proposed 15 ft tall perimeter wall in Meerkat™, which had already been set up to display the facility and surrounding terrain with high accuracy. Using that model, the team performed a comprehensive, data-backed threat assessment and found that there would still be significant risks present even after the wall was constructed. The client's estimations group predicted that the wall construction alone would cost between \$12 million and \$15 million, and the price for the proposed ballistic rated gate to accompany it had yet to be calculated, meaning additional costs were still looming.*



Our goal is to make sure that any amount spent on security is the right amount.

—CHRIS OTT, SENIOR PHYSICAL SECURITY EXPERT

Working Backward: Recognizing that the original plan was unlikely to mitigate risks as effectively as hoped, the client decided to explore alternative solutions. The Meerkat™ team worked side-by-side with the client's electrical engineers, civil engineers, transmission planners and other key personnel to test the effectiveness of other mitigation strategies. The security designs were rethought in a series of brief, one-hour daily workshops over several days, dramatically shortening the timeline compared to conventional methods.

The first step was identifying the most critical assets within the facility. The client's experts were able to point out the pieces of equipment that if rendered inoperable would cause significant instability in their system and portion of the grid. These assets then became the “targets” for mitigation measures.

With each critical asset in mind, the team began modeling different mitigation ideas in Meerkat™. The tool's interactive nature meant that they could move ballistic protections closer, or make them larger, in just a few simple clicks, seeing in real time how effectively different tactics protected vulnerable components. The key was finding the right balance between cost and value.

The Results: The team found that instead of a 15 ft wall around the entire 3,523 linear foot perimeter of the station, they could implement two separate 166 ft long, 25 ft tall walls in strategic locations around critical assets and get much more comprehensive protection for a fraction of the price. The cost to implement this solution was estimated to be approximately \$3.4 million. It would increase their security stance, lower their risk profile and prevent them from spending \$15 million on inadequate protections.

TABLE 3: A QUICK COMPARISON OF MITIGATION APPROACHES

Approach	Description	Estimated Cost	Effectiveness
Full physical hardening	15 ft CMU perimeter wall	\$12 million–\$15 million	Effective for some equipment, but significant risks are still present and unaddressed
Alternative mitigation	12 ft expanded metal fence	\$1.06 million	Somewhat effective, but vulnerabilities are still present
Integrated, targeted solution	Ballistic protections close to assets with bespoke heights for added protections	\$3.4 million	Highly effective. Identified critical assets are fully protected from line-of-sight risks



STRATEGIC RECOMMENDATIONS FOR ENHANCING SECURITY

To effectively safeguard substations against evolving threats, utilities should implement strategic recommendations that leverage advanced technologies and expert insights. Here are a few key strategies to consider:

TECHNOLOGY INTEGRATION

Integrating cutting-edge technology is essential for determining the optimal placement of physical barriers. Advanced tools like Meerkat™ use real-time data and line-of-sight analyses to identify vulnerabilities and guide the strategic positioning of defenses such as walls, fences and surveillance systems.

RISK-BASED PRIORITIZATION

Detailed risk assessments allow utilities to prioritize resources based on the identification of high-risk components or assets. By focusing on the areas most susceptible to attacks, utilities can allocate their security budgets more efficiently and enhance protection where it's needed most.

DRONE DETECTION

With the rise in drone usage, incorporating drone detection systems into substation security plans is crucial. These systems can identify unauthorized aerial vehicles approaching facilities, enabling timely responses to potential threats.

USE OF LINE-OF-SIGHT TECHNOLOGIES

Line-of-sight technologies like Meerkat™ provide comprehensive visibility into substation vulnerabilities. This approach enables utilities to assess sightlines accurately and implement targeted mitigation measures that address specific risks posed by surrounding landscapes or structures.

RAPID RECOVERY PLANS¹⁴

Developing rapid recovery plans ensures swift restoration of services following disruptions. Use strategies for reducing lead times associated with procuring replacement parts, thereby minimizing outage durations.

» **Equipment Sharing Programs**—These initiatives allow participating utilities to access a shared pool of spare assets, reducing downtime during emergency events and non-routine failures. Programs such as the Spare Transformer Equipment Program (STEP) and SPAREConnect facilitate efficient communication among members, ensuring quick access to necessary equipment within specific voltage classes.

- » **Grid Assurance**—Grid Assurance offers strategically located and secure storage sites where spare long-lead-time assets are housed. In the event of an emergency, these resources can be rapidly deployed to affected areas, providing critical support for recovery efforts. This program addresses national security needs by enhancing grid resilience through readily available backup components.
- » **RESTORE Program**—The Regional Equipment Sharing for Transmission Outage Restoration (RESTORE) program complements existing sharing initiatives by offering additional or alternative sources for critical components. As a voluntary agreement between members, RESTORE ensures that utilities can recover swiftly from major damage to transmission infrastructure through collaborative resource sharing.
- » **Proactive Damage Prevention**—While equipment-sharing programs focus on post-incident recovery, tools and services like Meerkat™ enable proactive prevention strategies that reduce reliance on emergency replacements due to physical attacks.

BUILDING REDUNDANCY INTO PHYSICAL SECURITY

Incorporating redundancy into physical security measures enhances resilience against potential breaches or failures. By deploying multiple layers of defense—such as overlapping surveillance coverage or dual access control points—utilities can maintain robust protection even if one element is compromised.

CONSULT WITH A TEAM OF EXPERTS

Engaging a team of experts across various disciplines ensures comprehensive evaluations and well-informed decisions regarding all aspects of substation security. Collaborating with professionals in fields such as engineering, cybersecurity and risk management provides diverse perspectives that strengthen overall security strategies.

FACTORS TO CONSIDER WHILE PLANNING SECURITY ENHANCEMENTS

- » Operations security
- » Personnel security
- » Physical security
- » Awareness education and training
- » Planning crisis management
- » Performing crisis management



A CASE STUDY: OPTIMIZED TRANSFORMER PROTECTION

Background: A client in the power delivery sector faced a new security standard requirement during the design phase of a greenfield substation project. This standard mandated the installation of ballistic walls around power transformers to safeguard against potential threats. To address this challenge effectively, they needed a solution that not only provided protection, but also allowed for operational efficiency and accessibility of the equipment.

Recognizing the importance of precision in meeting these standards without compromising substation functionality, the client chose Meerkat™ to help develop a comprehensive solution.

3D Modeling and Mitigation Testing: The Meerkat™ team used detailed topography data of the substation pad and proposed substation layout to create an accurate 3D model. This digital representation served as a foundation for testing various mitigation strategies, including strategic placement of ballistic walls around power transformers. This model helped to strategically determine which wall heights were necessary to obstruct line-of-sight from up to one mile outside the perimeter fence (a study area radius chosen for analysis by the client). The team also determined the maximum height above grade that the bottom of the wall could be using the same method.

Real-Time Adjustments and Optimization: Collaborating with the substation design team through several web meetings, the Meerkat™ team fine-tuned wall specifications in real-time—adjusting height, distance from transformers and opening sizes—to maximize access while ensuring security. Special consideration was given to accommodating oil handling

equipment typically transported on trailers, which would need to have access to the transformers for routine maintenance.

Digital analysis confirmed that line-of-sight would be effectively blocked while openings for access and emergency egress around each transformer's ballistic wall setup would be ideal—an exercise that demonstrated how technology could enhance both safety measures and operational flexibility.

Client Engagement and Feedback: Throughout this iterative process, the client was actively involved in reviewing demonstrations and visual representations showcasing optimized layouts that were designed without compromising critical equipment visibility or accessibility needs.

Following thorough evaluations by both line-of-sight specialists and substation designers, the client expressed satisfaction with the initial drafts.

Final Report Issuance: After successfully addressing all identified concerns, finalized documentation was issued across multiple sites, paving the way towards completion.

The Results: Two access points were designed for each transformer ballistic wall to maximize access and emergency egress. The walls were strategically overlapped or extended to allow for that access while still blocking all avenues of line-of-sight to critical assets.

This case study exemplifies how leveraging cutting-edge methods can transform traditional approaches into agile responses capable of meeting stringent standards efficiently—all while maintaining operational excellence across complex projects.

BALANCING SECURITY COSTS WITH BUDGETARY CONSTRAINTS

Security upgrade projects can easily become expensive, but there are ways to save money without reducing effectiveness. Some of these methods include:

- » Integrating safety into substation builds
- » Building only what's needed
- » Eliminating assumptions through data-driven solutions
- » Drawing on the skills and expertise of professionals
- » Evaluating each location on its own merits (not one-size-fits-all)

FUNDING PHYSICAL SECURITY UPGRADES

The most frequently used funding mechanisms for substation assessment and upgrades include, but are not limited to:

Federal Grants and Programs

Substations and other critical infrastructure service providers can apply for federal grants, such as those offered by the U.S. Department of Energy, the Department of Homeland Security or the Federal Emergency Management Agency. These include preparedness or hazard mitigation assistance grants which may support physical security enhancements, technology upgrades, emergency preparedness and modernization efforts.

Public-Private Partnerships to Achieve Goals

Policy shifts in Washington D.C. encourage critical infrastructure owners and organizations to take a fresh look at how to best confront the modern needs and challenges of their facilities with renewed focus on public-private partnerships.¹⁵ For example, the Cybersecurity and Infrastructure Security Agency encourages public-private partnerships and the collaborative exchange of ideas, expertise and technological innovation.

Internal Budget Allocation

Utilities and operators can use a hybridized model for assessment and validation services, as well as security mitigations. This approach strategically combines traditional methods with advanced digital tools, enabling more comprehensive evaluations and targeted interventions.

A critical aspect of implementing a hybridized model is balancing capital expenditures (CAPEX) with operational expenditures (OPEX). Utilities must carefully weigh the costs and benefits associated with conducting thorough analyses against those related to executing necessary security upgrades. Investing in detailed assessments using data-driven solutions can initially increase upfront CAPEX but often leads to

long-term OPEX savings by reducing the likelihood of costly incidents and optimizing maintenance efforts.

On the other hand, focusing solely on extensive physical security upgrades might seem prudent but could result in overspending without adequately addressing specific risks. By strategically splitting resources between analysis and mitigation measures

based on risk prioritization, utilities ensure that every dollar spent contributes maximally towards enhancing substation resilience within budgetary constraints.

The table below outlines some of the pros and cons that assessments and upgrades have on CAPEX and OPEX.¹⁵

TABLE 4: PROS AND CONS OF ASSESSMENT METHODS ON CAPEX & OPEX				
	Capital Expenditure		Operational Expenditure	
	Pros	Cons	Pros	Cons
Security Assessments or Validation Services	<ul style="list-style-type: none">» Improve security hardening» Reduce long-term replacement costs» Forecast and spread the investment across a rate case assessment» Amortize the investment and roll it into the return on investment (ROI)	<ul style="list-style-type: none">» Relatively low cost of assessments» Generally long approval times» Technology/solutions can change by the time the funds are made available	<ul style="list-style-type: none">» Addresses security as immediately relevant to operational needs» Ensure continued operations and regulatory compliance» Gain an immediate competitive edge by investing in vital areas» Easier budget planning» Best practice for recurring services for regulatory compliance	<ul style="list-style-type: none">» Immediate income statement impact, but also yields tax benefits in the year incurred» May need to cut other operational budget items to accommodate» Operational budget increases are harder for some clients
Security Hardening or Mitigation Builds	<ul style="list-style-type: none">» Investments (fences, walls, cameras, ballistic barriers, etc.) can be capitalized and then depreciated over their useful life, providing tax deductions» Can be budgeted for in a financial cycle, achieving financial predictability and economies of scale» Avoids large upfront investments	<ul style="list-style-type: none">» Assets may become obsolete due to evolving threats or technology requiring replacement	<ul style="list-style-type: none">» Yields immediate tax benefits by reducing taxable income	<ul style="list-style-type: none">» May affect profitability if proposed measures are unbudgeted

Utility Revenue and Bonds

Utilities may fund upgrades through a variety of mechanisms¹⁶ that distribute costs over time and among ratepayers. These include, but are not limited to:

- › Rate Adjustments: By incrementally increasing rates, utilities can generate additional revenue dedicated specifically to security enhancements. While this method requires careful consideration of consumer impact, it provides a steady stream of funding that supports ongoing investments in infrastructure protection without requiring large upfront expenditures.
- › Issuing Municipal Bonds: Municipal bonds are debt securities used by local governments or public entities like utilities to finance capital projects. By issuing bonds earmarked for substation security improvements, utilities can secure substantial funding upfront while spreading repayment obligations over an extended period. This approach not only enables timely implementation but also allows ratepayers to contribute toward debt servicing through future revenues rather than immediate rate hikes.
- › Utilizing Capital Reserves: Drawing on existing capital reserves, if available, minimizes reliance on external borrowing or drastic rate increases while ensuring critical projects receive prompt attention when needed most.

BEST PRACTICES

Ensuring robust security for substations requires more than one-time investments; it demands a comprehensive approach that encompasses the entire lifecycle of security systems. From initial setup to ongoing maintenance, regular assessments and timely upgrades, utilities must prioritize funding across each phase to safeguard critical infrastructure effectively.

Initial Investments in Security Infrastructure

Begin by allocating resources toward high-quality security installations tailored to the specific needs of each substation. This includes advanced perimeter defenses, surveillance technologies and access control systems designed to mitigate identified risks. Investing in reliable infrastructure from the outset minimizes vulnerabilities and sets a strong foundation for future enhancements.

Ongoing Maintenance

Regular maintenance is crucial to ensuring security systems operate optimally over time. Establish a routine schedule for inspecting equipment, testing alarms and verifying system functionality. Allocate funds specifically for maintenance activities to prevent deterioration or malfunctions that could compromise protection efforts.

Regulated Security Assessments

Conducting regulated security assessments every three years—or as required—provides valuable insights into evolving threats and changing site conditions. These evaluations enable utilities to adapt strategies based on new intelligence while maintaining compliance with industry standards. Funding these assessments ensures continuous improvement driven by data-backed recommendations.

Timely Upgrades

Stay ahead of potential threats by planning periodic upgrades aligned with technological advancements. As emerging tools become available, integrate them into existing frameworks to enhance both detection capabilities and responsiveness. Prioritize budget allocations enabling swift integration and cutting-edge solutions addressing current and future challenges alike.





CONCLUSION

As we look toward the future of power delivery in an increasingly complex threat environment, embracing tools like Meerkat™ will be essential for utilities committed to protecting their infrastructure while supporting reliable energy supply. By remaining at the forefront of technological innovation and continuous improvement, we can ensure that our critical assets remain secure against ever-evolving challenges—ultimately safeguarding public safety and national security.

REFERENCES

1. Critical Infrastructure Sectors. (n.d.). Cybersecurity & Infrastructure Security Agency. Retrieved from www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.
2. Electric Disturbance Events (OE-417). (2024). United States Department of Energy. Retrieved from https://www.oe.netl.doe.gov/OE417_annual_summary.aspx (discontinued website).
3. Sector Spotlight: Electricity Substation Physical Security. (2023). Cybersecurity & Infrastructure Security Agency (CISA) and the United States Department of Energy (DOE). Retrieved from www.cisa.gov/sites/default/files/2023-02/Sector%20Spotlight%20Electricity%20Substation%20Physical%20Security_508.pdf.
4. Happel, M. (2024, February). Unlock CIP-014 for Comprehensive Security. T&D World Magazine. 20–23.
5. Smith, R. (2014, March). U.S. Risks National Blackout From Small-Scale Attack. The Wall Street Journal. Retrieved from www.wsj.com/articles/SB10001424052702304020104579433670284061220.
6. MRO Reliability Risk Matrix. (2021). Midwest Reliability Organization. Retrieved from www.mro.net/document/mro-reliability-risk-matrix-2021/?download.
7. North American Electric Reliability Corporation (2025). Critical Infrastructure Protection (Standard No. CIP-014-3). Retrieved from www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-3.pdf.
8. Conduct Line of Sight Analysis. (n.d.). ArcGIS 3D Workflows. Retrieved from <https://doc.arcgis.com/en/3d/workflows/analysis/conduct-line-of-sight-analysis.htm>.
9. Line-of-Sight Analysis. (n.d.). PennState College of Earth and Mineral Sciences: Department of Geography. Retrieved from <https://www.e-education.psu.edu/geog480/node/485>.
10. Line of Sight. (n.d.). Bentley OpenSite CONNECT Edition. Retrieved from <https://docs.bentley.com/LiveContent/web/OpenSite%20Designer%20CONNECT%20Edition-v10/en/GUID-5C0E6C16-16A9-44C9-8017-EDB155EB4A24.html>.
11. Casini, S. et al. (2023, October). On Line-of-Sight Navigation for Deep-Space Applications: A Performance Analysis. ScienceDirect. Retrieved from www.sciencedirect.com/science/article/pii/S0273117722011097.
12. Li, M. (n.d.). Perform Visibility Analysis to Increase Security. Esri. Retrieved from <https://learn.arcgis.com/en/projects/perform-visibility-analysis-to-increase-security/index.html>.
13. Smarter Protection: Risk Mitigation with Meerkat™. (2025). POWER Engineers, Member of WSP. Retrieved from <https://meerkat.powereng.com/how-it-works>.
14. Edison Electric Institute (2023, August). Spare Equipment and Grid Resilience. Retrieved from <https://www.eei.org/-/media/Project/EEI/Documents/Issues-and-Policy/Reliability-and-Emergency-Response/Spare-Equipment-and-Grid-Resilience-Programs.pdf>
15. Cain, D. (2024, April). Strategic Patenting: Public-Private Partnerships Fostering Technological Innovation. LinkedIn. Retrieved from www.linkedin.com/pulse/strategic-patenting-public-private-partnerships-fostering-david-cain-i8v1c/?trackingId=2%2FQU4Ic7TSKINnha7K847g%3D%3D.
16. Gordon, S. (2024, March). CapEx vs OpEx: Overview and Differences. Datarails. Retrieved from www.datarails.com/capex-vs-opex/.
17. Funding Mechanisms Guide for Public Safety Communications. (2021, June). Cybersecurity and Infrastructure Security Agency. 5-27. Retrieved from www.cisa.gov/sites/default/files/2024-08/24_0828_s-n_funding_mechanisms_guide_public_safety_comms_2021_final_508.pdf.

