VedeniEnergy
Plugged Into The Energy Industry

NOVEMBER 2025 - I

Securing the Grid

Enhancing Physical Security of Power Infrastructure

WHITEPAPER

VedeniEnergy
Plugged Into The Energy Industry

+1 463-266-4496
www.vedeni.energy
info@vedeni.energy
Whitestown, in 46075, US.

Threat Landscape

Rising Attacks on Critical Grid Infrastructure

The United States electric grid confronts an alarming escalation in physical threats that undermine the resilience of critical infrastructure. According to the E ISAC's 2023 End of Year Report, more than 2,800 physical security incidents were shared with the E ISAC in 2023—up from roughly 1,700 incidents reported in 2022—and about 3 percent of those incidents resulted in grid impacts. This trajectory reflects not merely improved reporting but a tangible surge in malicious actions, including ballistic damage, intrusion, copper theft, equipment tampering, and vandalism. The scope of these threats spans the Southeast, Midwest, and Pacific Northwest—regions that have experienced clustering of assaults on electrical substations.

While many of the incidents recorded between 2020 and 2023 did not result in service disruption, about 3 percent of the more than 2,800 incidents in 2023 caused outages or damage to critical equipment. Utilities operating in high-demand contexts such as emergency medical care, heating or cooling systems, and water treatment depend heavily on resilient service delivery; even brief outages in such circumstances pose systemic risk.

Substations have emerged as especially vulnerable targets. Distribution and transmission substations located in remote or lightly guarded areas often suffer limited surveillance, making them attractive points of attack. Ballistic strikes targeting transformer cooling fins, switchgear, and control panels have disabled equipment, sometimes inflicted in multiple waves over successive nights. The December 3, 2022, attack on two Duke Energy substations in Moore County, North Carolina, underscores this risk. Gunfire at the facilities left approximately 45,000 customers without power for several days. State emergency declarations, nighttime curfews, school closures, community shelters, and extended utility operations in freezing conditions followed. Tragically, an elderly resident reliant on oxygen therapy died during the outage. Local authorities, along with state and federal agencies—including the North Carolina State Bureau of Investigation, Department of Energy's CESER, and FBI—initiated investigations. The case remains unsolved as of December 2024; investigators have received hundreds of leads, and law enforcement has offered a combined $100,000 reward for information leading to an arrest.

Historical events offer parallel lessons. In April 2013, armed assailants targeted Pacific Gas and Electric's Metcalf transmission substation near San Jose, California, damaging seventeen transformers worth over fifteen million dollars. Though power delivery continued via rerouting, full recovery required weeks. This incident catalyzed FERC's adoption of Reliability Standard CIP 014, mandating periodic risk assessments and security planning for substations deemed critical to bulk power system reliability.

Attack motivations vary widely. Some incidents reflect economic crimes—copper theft or equipment vandalism—while others appear ideologically driven. DHS and FBI threat assessments have documented increased online extremist chatter advocating for attacks on power infrastructure. These narratives, often rooted in conspiratorial or anarchic ideologies, emphasize

the symbolic and operational impact of causing outages. In some cases, criminal and extremist motivations overlap, complicating patterns of detection and prosecution.

Geographically, the emergence of clustered incidents—multiple substations targeted within narrow timeframes or regions—suggests serial or coordinated intent. These clusters pose heightened risks: cascading outages, cross-regional transmission instability, and simultaneous demands on utility emergency response teams. Even brief disruptions can propagate risk to healthcare systems, water utilities, traffic signals, and emergency communications networks.

Regulatory and industry responses reflect growing concern. NERC's April 2023 evaluation of CIP 014 3 responds to FERC's December 2022 directive to assess whether the standard's applicability, risk assessments, and protection criteria are adequate in light of rising attacks. Building on this evaluation, NERC's Project 2023 - 06 has developed CIP-014-4. The third draft concluded its comment period on July 21, 2025, and seeks to refine risk assessment criteria and address inconsistencies identified by FERC, with board adoption expected in October 2025. This evaluation considers whether a baseline level of physical security measures should be extended to all bulk power substations, beyond those currently regarded as critical. The E ISAC has supported threat mitigation through its Physical Security Advisory Group and released tools such as the Physical Security Resource Guide and Vulnerability of Integrated Security Analysis (VISA) workshops to support utilities in enhancing detection, delay, and response capabilities.

Community resilience and systemic readiness are emerging as central themes. Traditional perimeter protections—fences, lighting, CCTV—prove insufficient without integrated detection, analysis, and law enforcement coordination. Utilities are increasingly embracing layered approaches that align physical hardening with resilience strategies like fast deployment of mobile substations, stockpiling of spare transformers, sectionalizing networks to limit outage impact, and mutual assistance agreements across regions.

In summary, the U.S. power grid faces a severe and intensifying threat environment. Substations—particularly those in remote or minimally monitored locations—are primary targets for both opportunistic criminal activity and deliberate ideological sabotage. The rising frequency and severity of grid-impacting incidents demand proactive, layered security postures and integrated resilience planning. Utility operators, regulators, and public safety stakeholders must elevate physical deterrence, response readiness, and system recovery planning as co equal components in safeguarding critical infrastructure.

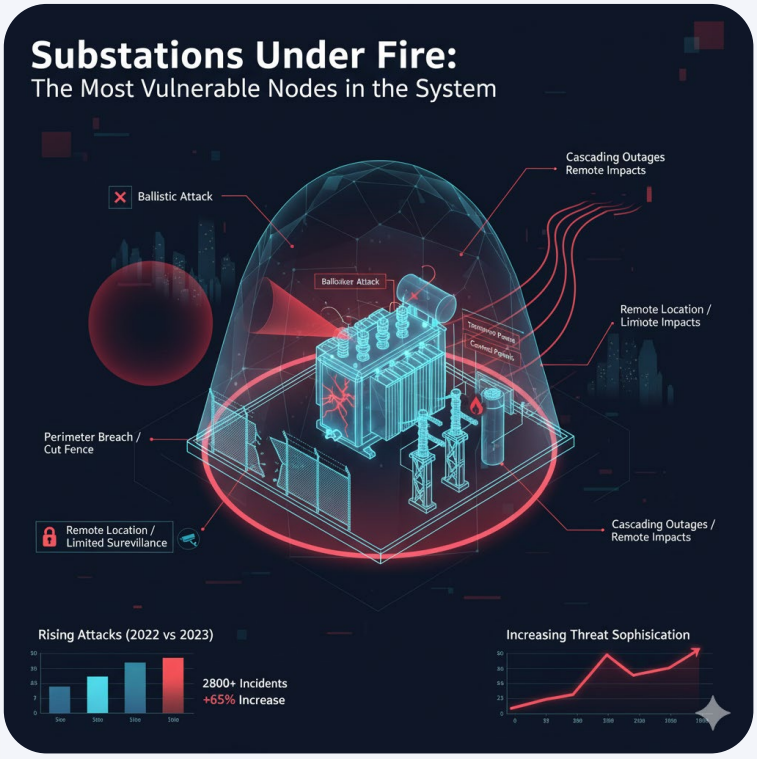
Substations Under Fire

The Most Vulnerable Nodes in the System

Within the structure of the U.S. electric power system, substations occupy a critical junction between generation and distributed service. These facilities serve as control and transformation hubs, stepping voltage up or down, switching power paths, and housing key protective equipment. Unfortunately, their strategic role is matched by their physical vulnerability. Many substations—especially those handling transmission and distribution—are located in remote, lightly supervised areas. Such locations often feature minimal security infrastructure: perimeter fences, limited lighting, chain link gates, and sometimes no on-site personnel. These conditions render substations particularly susceptible to malicious attacks, whether opportunistic, ideologically motivated, or organized.

Ballistic attacks targeting transformer cooling fins and control equipment have become increasingly common. Investigative reporting and government data from the Department of Homeland Security's CISA highlight that substations attacked in clusters during 2022—such as those near Tacoma, Washington, and in Moore County, North Carolina—suffered multi-wave intrusions. In these incidents, attackers cut fencing, fired multiple shots into power equipment, and fled after inflicting disabling damage. In Oregon's Clackamas County, perpetrators breached one substation and disabled equipment using firearms, leading to sustained outages. These incidents are not isolated; data from DOE's annual incident summaries confirm over twenty "actual physical attacks" in 2022, a sharp rise from prior years. Utilities recorded more than 2,800 physical security incidents reported to the E ISAC in 2023—up from roughly 1,700 incidents in 2022—with substations comprising a significant share of targets.

Transformers and other high-voltage components represent a particularly acute risk. High-voltage transformers cost millions of dollars each, are often custom-ordered, and can take months to replace. U.S. Congressional Research Service reports and analyses by DOE, CISA, and NASEO note that spare inventories are minimal because of their expense and uniqueness. Thus, damage inflicted at a substation—especially to transformer units—can lead to days or weeks of localized or regional power loss while replacement units are procured and installed. The financial and operational implications are significant even when service is restored relatively quickly.



FERC-authorized projections highlighted a scenario: a coordinated attack on as few as nine critical substations during peak demand could cause a coast-to-coast blackout. However, these conclusions were theoretical, and the Department of Energy's Inspector General and other analysts have questioned the underlying assumptions. The scenario nonetheless underscores that a small number of critical nodes hold disproportionate influence over system stability.

The interplay of location, infrastructure design, and systemic interdependence amplifies risk. Remote substations typically lack camera coverage, intruder detection systems, and physical delay mechanisms. Many rely solely on chain-link fences—which can be climbed or cut—and basic lighting that may not deter nighttime intrusion. Furthermore, utility segment fragmentation means that physical security measures vary widely across operators: larger investor-owned utilities may have more resources to invest in security than smaller cooperatives or municipal systems. This inconsistent posture introduces weak spots that can be studied and targeted.

Even non-ballistic threats pose a danger. Electric substations in Arkansas in 2013 experienced deliberate fire damage to control houses; other sites suffered damage from arson, tool-based sabotage, and copper theft. Although not all incidents resulted in blackouts, they exposed that substations provide relatively low-effort, high-impact potential points of failure. Hunting season has periodically driven increases in substation vandalism across rural areas, where stray bullets or intentional mischief strike insulators, transformers, or switches.

Legislative and regulatory bodies have acknowledged the vulnerability gap. FERC's 2014 order and NERC's CIP 014 standard require risk assessments and site-specific security planning for substations deemed critical. However, many substations fall outside this designation—those at lower voltage levels or not tied directly to bulk transmission—and thus lack mandated mitigation. State legislatures have responded by proposing or enacting bills requiring continuous surveillance, increased trespass penalties, or baseline security standards for all substations above certain thresholds. Still, national coverage remains uneven.

Institutional research—including CISA's 2023 Sector Spotlight report—emphasizes the importance of tailored, layered security plans. These plans combine detection, delay, and response measures: intrusion sensors, lighting, access control, alarm systems, and coordination with law enforcement. In addition, remote monitoring and periodic patrols are vital. But with tens of thousands of substations across the United States, physical hardening of every location is neither practical nor cost-effective. Rather, prioritization based on criticality, exposure, and threat intelligence is necessary.

Compounding the issue is the evolving nature of threats. Extremist actors now use online platforms to share practical advice on how to locate and attack electrical infrastructure. Domestic threat intelligence bulletins cite documents instructing individuals to target substations using rifles or low-tech sabotage methods. These emergent tools reduce the barrier to planning and execution, raising the risk that more sites may be hit in a coordinated or serial fashion. Incidents in late 2022 illustrate this dynamic: regional clusters of substation attacks appeared to be driven by common methods and possibly shared scripts.

Ultimately, substations embody a paradox: they are vital because of their role in grid functionality, yet they are often inadequately protected. Their physical exposure, combined with systemic interdependencies and limited spares, transforms even minor damage into significant outages. Bridging this gap requires a shift from ad hoc protective measures to strategic, prioritized security that matches physical investment to risk exposure and systemic consequence. Only by identifying critical nodes, hardening them appropriately, integrating detection and response systems, and coordinating across utilities and law enforcement can the U.S. grid move toward true resilience of its substation infrastructure.

From Fences to Fiber

Evolving Layers of Physical Security

Utilities across the United States are embracing a layered approach to physical security, recognizing that fences alone are no longer sufficient to deter or mitigate escalating attacks on critical infrastructure. CISA's Sector Spotlight on Electricity Substation Physical Security emphasizes a defense-in-depth strategy tailored to each facility's risk profile. The layered approach comprises visible deterrents, sensor-based detection, delay mechanisms, alarm validation, communications, response coordination, threat intelligence, and periodic audits. This holistic model aligns seamlessly with modern grid protection goals as violence and vandalism grow more targeted and sophisticated.

Deterrence forms the first tier of physical security. Substations in high-risk areas are being equipped with vehicle barriers, taller chain link fences topped with anti-climb mesh or razor wire, and high-intensity lighting to eliminate concealment at night. Signage warning of surveillance and prosecution further raises the perceived risk for would-be intruders. These visible measures signal utility awareness and elevate the effort threshold for attackers.

Detection capabilities add the next critical layer. More utilities now deploy sensors covering perimeters and equipment zones, including passive infrared, vibration sensors, acoustic gunshot detectors, and break-glass alarms. These sensors connect to supervisory control systems and often feed AI-enhanced analytics to detect anomalous motion or sound patterns indicative of intrusion. Some systems incorporate thermal imaging cameras and short-range radar to flag suspicious activity at all hours. In pilot programs, utilities in Texas and the Midwest have demonstrated that AI-driven video analytics can reduce false alarms significantly while improving response times by identifying live threats in real time.

Delay mechanisms supplement detection. Hardened enclosures around transformers and switchgear—often constructed from reinforced concrete or steel—resist ballistic assault. Access control gates with automatic locking, intrusion-resistant doors, and multi-factor authentication ensure that unauthorized movement through critical zones is slowed or prevented entirely. These physical delays provide law enforcement or utility security teams greater time to respond before catastrophic damage occurs.

Alarm validation, communications protocols, and incident response planning complete the core layers. Industry guidance encourages integration with emergency dispatch systems and establishing direct communication channels with local sheriff's offices and state fusion centers. Alarm verification—often via camera confirmation—helps reduce false dispatches, ensuring real incidents receive timely response. Incident response plans now routinely involve pre-established roles, remote dispatch authorization, and coordination agreements to deploy rapid response crews or mobile substation units within hours.

Intelligence gathering and threat analysis elevate the ecosystem from reactive to proactive. Many utilities now subscribe to E-ISAC advisories and participate in VISA workshops to analyze threat patterns across the sector. These inputs inform prioritized hardening strategies in areas with emerging patterns of extremist messaging or prior clustered attacks. For example, one utility in the Pacific Northwest undertook perimeter upgrades after E ISAC reports highlighted recurring incidents in its service region and embedded AI cameras fueled by analytics trained on local threat characteristics.

Systematic audits and continuous improvement finalize the whole defense posture. Physical security audits—mandated under CIP 014 for critical substations—are being extended voluntarily to a broader portfolio based on asset criticality. MDPI published guard rail guidance recommending risk-based audit frequency tied to threat exposure, asset value, and prior incident history. Audit results feed into iterative upgrades: digital fence sensors replaced older magnetic loops, lighting systems patched for blind spots, and detection thresholds fine-tuned based on incident data.

The convergence of these layers is particularly transformative when combined with technology innovations. AI-based analytics applied to video and acoustic streams reduce manual monitoring burdens and accelerate threat assessment. Chat GPT–style video analytics classify intrusion types—human, wildlife, or environmental—and prioritize human threats. Thermal detection during heavy foliage seasons or at remote sites improves detection accuracy. Drone detection systems leveraging radar and RF sensors can flag unauthorized aerial reconnaissance.

Protecting substation information assets is also a critical dimension. As cyber-physical integration increases, safeguarding engineering drawings, relay configurations, and substation automation systems becomes part of physical security. Recommendations from journals indexed by PubMed

highlight that adversaries may attempt to obtain design data for planning sabotage. Utilities now enforce strict access controls on drawing repositories, encrypted data in transit, and audit trails for access logs.

Institutional frameworks support the technology infusion. DHS's November 2024 Roles and Responsibilities Framework for AI in Critical Infrastructure guides the secure deployment of AI systems by infrastructure operators. It encourages transparency, testing, and data governance to prevent adversarial manipulation and unauthorized modification of analytics platforms. DHS expects utilities deploying AI in physical security to define governance models that include stakeholders such as AI vendors, system integrators, utility SOC teams, and supervisory agencies.

CISA's 2024 Year in Review and AI risk assessments underscore emerging vulnerabilities: AI systems may introduce new attack surfaces, such as adversarial input or data poisoning attacks, that impair detection capabilities. Consequently, guidance stresses securing the AI data lifecycle—from training datasets to inference—and via regular performance audits.

In practice, modern physical security for substations now comprises layered deterrence, sensing, delay, validation, communications, intelligence, and audit. AI-infused detection systems enhance situational awareness, while robust governance inhibits misuse or system failure. The result is a more responsive, adaptable posture capable of deterring, detecting, delaying, and coordinating effective response to both conventional vandalism and sophisticated extremist threats.

This evolution reflects a strategic shift: from passive fences and CCTV to integrated systems that view substation infrastructure as cyber-physical ecosystems. Operators are increasingly moving from simple physical isolation toward active, intelligence-driven defense. Nonetheless, scaling these measures across tens of thousands of facilities requires prioritization based on criticality and threat exposure. Selective deployment—backed by risk intelligence, regulatory expectation, and audit feedback—ensures cost-effective security investments. Overall, this layered model strengthens not just local deterrence but systemic resilience across the grid.

Layered Defense Strategy

U.S. utilities are shifting from simple fences to multi-layered physical security—combining deterrence, detection, delay, validation, communication, intelligence, and audits—to protect substations from increasingly targeted attacks.

AI-Driven and Risk-Based Protection Advanced AI analytics, integrated sensors, and risk-informed audits enhance threat detection, reduce false alarms, and enable proactive, intelligence-led responses—transforming substations into resilient cyber-physical ecosystems.

ACTION

Federal Action & Industry Standards

A Regulatory Snapshot

The recent rise in targeted physical attacks on electric substations has led to a recalibration of the regulatory framework governing grid security in the United States. At the center of this recalibration is the evolving role of federal agencies and industry standards bodies in both identifying vulnerabilities and codifying mitigation strategies.

A pivotal moment came in late 2022 when the Federal Energy Regulatory Commission initiated a formal evaluation of the physical security reliability standards that protect the bulk power system. This action directed the North American Electric Reliability Corporation to assess whether the current regulatory standard—CIP 014—was adequate given the increased number and severity of substation attacks. Specifically, regulators questioned whether the standard's applicability criteria excluded too many assets, whether risk assessment methodologies were consistently applied across the industry, and whether a minimum level of physical protection should be mandated universally.

In response, the North American Electric Reliability Corporation issued a report in spring 2023. The organization concluded that while the standard broadly targets the most critical substations, its effectiveness was uneven in practice. Utilities differed in how they conducted risk assessments, with many relying on subjective thresholds or limited geographic considerations. This inconsistency highlighted a gap between policy intent and operational execution. While the report did not recommend immediate expansion of the standard's scope, it triggered a new development initiative to refine its requirements, including more precise guidance for determining asset criticality and documenting technical justifications.

To further examine these findings, the Federal Energy Regulatory Commission hosted a technical conference with key stakeholders from across the utility, regulatory, and security communities. This event underscored growing consensus around the idea that risk-based assessments should inform physical security measures but also stressed the need for enhanced baseline expectations. Participants emphasized that merely meeting the letter of the standard was insufficient; utilities

must evolve toward proactive, intelligence-informed security postures capable of adapting to both regional threats and systemwide vulnerabilities.

The 2023 State of Reliability report echoed these concerns. Although the report confirmed that physical attacks had not caused cascading failures at the bulk power level, it acknowledged that response times, system redundancy, and distribution-level recovery capacity were essential in preventing wider consequences. The report also warned that as distributed energy resources continue to grow and control systems become more interconnected, the impact of physical attacks may spread more rapidly, especially in the absence of cross-sector planning.

Federal guidance in 2023 and 2024 increasingly emphasized the integration of resilience planning alongside traditional physical defenses. Agencies recommended that utilities not only improve detection and deterrence mechanisms but also invest in recovery strategies such as mobile transformers, mutual aid response networks, and sectionalization designs. These resilience measures are seen as essential complements to hard infrastructure protections.

The regulatory posture continued to evolve into 2025, with signals from both the Federal Energy Regulatory Commission and the North American Electric Reliability Corporation that revisions to physical security standards were likely. Under NERC's Project 2023 06, CIP 014 4's third draft completed a formal comment period on July 21, 2025, and is expected to be submitted for Board of Trustees approval in October 2025. In particular, compliance expectations may soon include more rigorous documentation, required participation in threat intelligence sharing networks, and stronger interagency coordination. While no single national mandate has yet emerged to govern every substation, there is a clear directional shift toward a tiered, risk-informed regulatory model.

Throughout this transformation, federal and industry leaders have shared a core belief: physical security is no longer a site-level operational concern, but a systemic reliability issue. The push toward uniform risk assessments, transparent audits, and enforceable resilience benchmarks marks a significant departure from the historically reactive nature of infrastructure protection. Instead, the emerging framework favors preemptive action, real-time coordination, and measurable outcomes.

In summary, the federal regulatory architecture for grid security is undergoing a meaningful expansion. Agencies are refining the standards that govern substation protection, pushing utilities toward integrated strategies that include both prevention and rapid recovery. The result is a regulatory environment better suited to confronting the complex, evolving threat landscape that now defines critical infrastructure in the power sector.

Resilience Beyond Defense

Rapid Recovery and Redundancy Strategies

Increasing attention has shifted toward resilience strategies that go beyond deterrence and delay, recognizing that recovery and redundancy are essential when physical infrastructure is compromised. In the wake of substation attacks, utility operators and policymakers are advancing approaches to rapidly restore service and mitigate cascading failure risks, while planning for scenarios where replacement of critical assets may take days or weeks. This resilience-centered doctrine repositions recovery as a strategic priority across all layers of grid security.

One key dimension is strategic asset redundancy, particularly involving large power transformers (LPTs), whose failure can severely disrupt regional transmission networks. The U.S. Government Accountability Office has identified chronic vulnerabilities in transformer availability, noting long lead times and low spare inventory as critical impediments to restoration in crisis scenarios. A 2017 Department of Energy report to Congress assessed options for a strategic transformer reserve and recommended a non-government solution driven by industry actions and compliance with CIP 014 2 rather than the establishment of a federally operated reserve. Subsequent legislative mandates under the Infrastructure Investment and Jobs Act required DOE to assess inventory status by mid-2022. DOE concluded that an industry-driven, voluntary coordination model—supplemented by federal support—remains the most practical path forward under existing policy frameworks. In its July 2024 Large Power Transformer Resilience Report, DOE reported that industry spare transformer sharing programs and mobile substation initiatives have expanded and recommended continued research and cost-sharing mechanisms to strengthen domestic manufacturing and supply chain resilience.

Utilities have begun scaling mutual aid agreements and transformer-sharing networks. Several regional coalitions maintain rotating stores of spare LPTs and mobile substation units—fully functional, preassembled systems that can be transported to impacted areas and energized within hours. Complementing these hardware reserves, sectionalization strategies allow grid operators to isolate damaged segments and reroute power through alternate paths, reducing outage scope. When combined with microgrid architectures and distributed energy resources (DERs), these techniques support localized continuity of service for critical loads even when transmission paths are severed.

Restoration frameworks have also evolved. The National Academies emphasize that post-event recovery should rely on pre-event system design that allows responders to assess the extent of failure and damage, dispatch resources effectively, and draw on established component inventories, supply chains, crews, and communication channels. These processes unfold in tandem across multiple operational levels—field crews, regional control centers, and centralized coordination hubs. Utilities are investing in situational awareness tools to expedite damage assessment, including drone inspections, remote thermal scanning, and GIS-based outage mapping. Rapid deployment protocols are now standard in emergency playbooks, enabling

coordinated action between grid operators, emergency management officials, law enforcement, and infrastructure owners.

Resilience planning increasingly incorporates exercises simulating ballistic assault scenarios. Grid operators and federal agencies such as DOE and CISA conduct tabletop and field drills to validate response workflows and supply chain logistics. These exercises underline the importance of pre-positioned mobile transformers, crew surge capacity, and communication interoperability in minimizing downtime. In many cases, restoration of partial service is achieved within hours to critical facilities such as hospitals, water treatment plants, and emergency shelters, even before full substation functionality is restored.

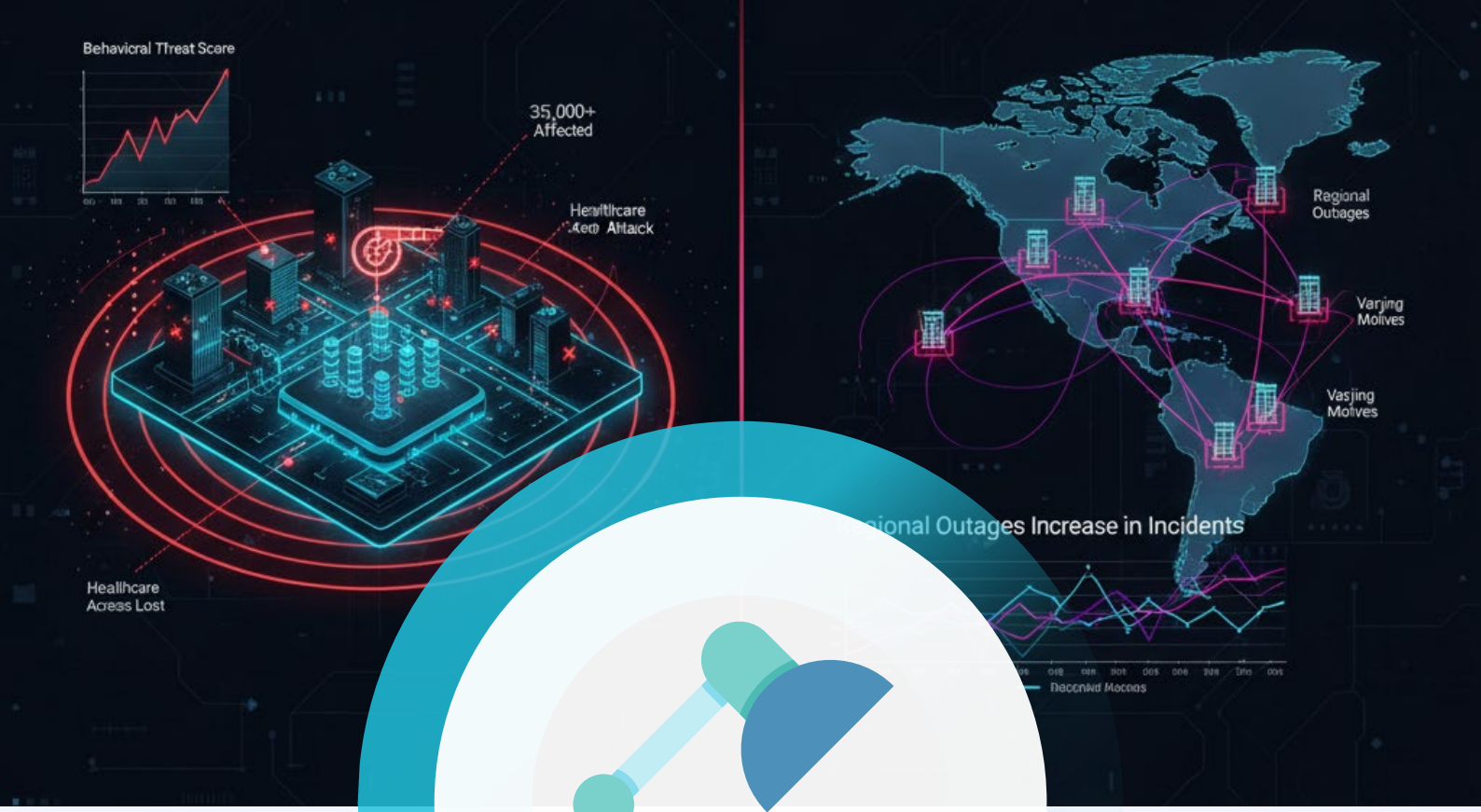
Technological enhancements also support resilience. Grid-enhancing technologies (GETs), such as dynamic line rating, phase shifting transformers, and advanced switching automation, help operators reroute loads in near real time. Meanwhile, microgrid controllers and DER assets—such as solar arrays with battery storage—offer islanding capacity to maintain power to essential services independently. Institutions across the sector increasingly recognize that these distributed resilience assets complement physical hardening and reduce dependency on centralized infrastructure recovery efforts.

Despite progress, challenges remain. The GAO and DOE reports highlight persistent gaps in transformer replacement readiness: limited domestic manufacturing capacity, unpredictable supply chains for specialized components, and cost barriers associated with maintaining reserves. Mobile substation units, while effective, often differ in rating and capability from the damaged LPT, requiring that operators manage runtime and load limitations carefully.

The deployment of DERs and microgrids presents additional integration challenges, including regulatory hurdles, interconnection complexities, and funding constraints. Smaller utilities and co-ops may face staffing or financial limitations in implementing advanced resilience technologies. Nonetheless, federal grant programs—such as DOE's Grid Resilience Innovation Partnership—offer funding pathways, and regulators are increasingly including resilience performance metrics in planning requirements.

Ideally, resilience practices are tied to broader physical security strategies. Utilities that conduct risk-based asset mapping now leverage threat intelligence to prioritize which substations should be armed with mobile units or integrated microgrid feeders. Recovery planning thus becomes a complement rather than an afterthought to deterrence and detection. When layered with physical protection measures, resilience strategies ensure that even if security is breached, functional continuity is preserved and recovery is predictable and well-practiced.

> In conclusion, resilience planning constitutes an indispensable complement to physical security. Operators are shifting from protection-only paradigms toward integrated strategies that emphasize rapid recovery and adaptability following an incident. Strategic transformer reserves, mutual aid networks, sectionalization, and DER-enabled microgrids now form the backbone of modern resilience doctrine. Through proactive restoration planning, drill-tested workflows, and strategic redundancy, the grid becomes not only harder to attack but increasingly able to bounce back when attacks succeed.



Case Studies

Real World Lessons from Grid Attacks and Responses

- **Moore County, North Carolina**
  December 2022 Substation Shootings

- **Pacific Northwest Substation Attacks**
  Late 2022 Cluster

CASE STUDY # 1

Moore County, North Carolina

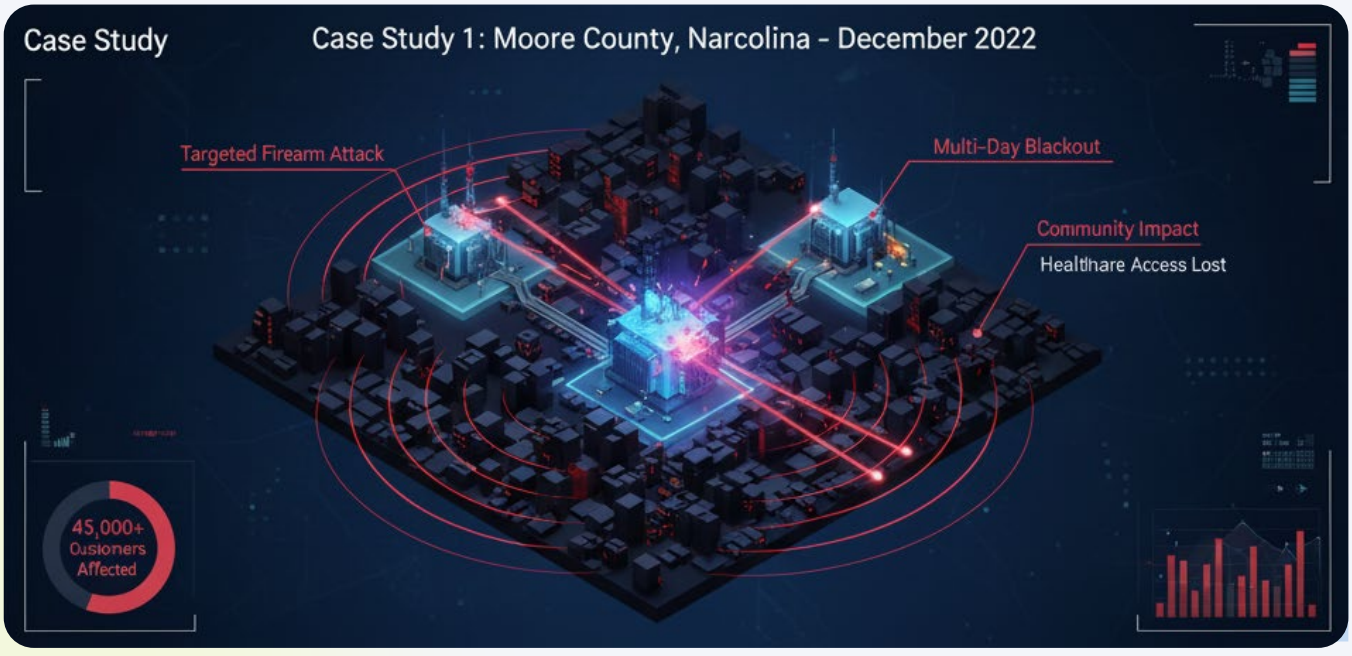
December 2022 Substation Shootings

The Moore County incident marked a pivotal moment in national awareness of grid vulnerability. A targeted firearm attack on two transmission substations caused a multi-day blackout affecting tens of thousands of residents. The disruption led to widespread community impact, including the closure of public services, emergency declarations, and loss of critical healthcare access.

While the tactical details remain under investigation, the broader significance lies in the visibility of the consequences. The incident revealed how easily unprotected infrastructure can be disrupted with minimal resources, and how that disruption can ripple through public safety, health services, and the economy. It demonstrated the limitations of traditional perimeter defenses and underscored the urgency for advanced intrusion detection, situational awareness, and recovery planning.

In regulatory terms, the attack triggered formal action. Federal agencies began reassessing whether existing physical security standards applied broadly enough, and state policymakers proposed mandatory surveillance requirements. Industry-wide, utilities accelerated investments in hardened perimeter infrastructure, deployed video analytics, and adopted more aggressive risk mapping.

This case highlighted the exposure of critical substations that may not meet the current criteria for federal oversight, prompting a reassessment of how infrastructure is categorized and protected. The consequences extended beyond the outage itself—setting in motion a systemic response from regulators, operators, and law enforcement.



CASE STUDY # 2

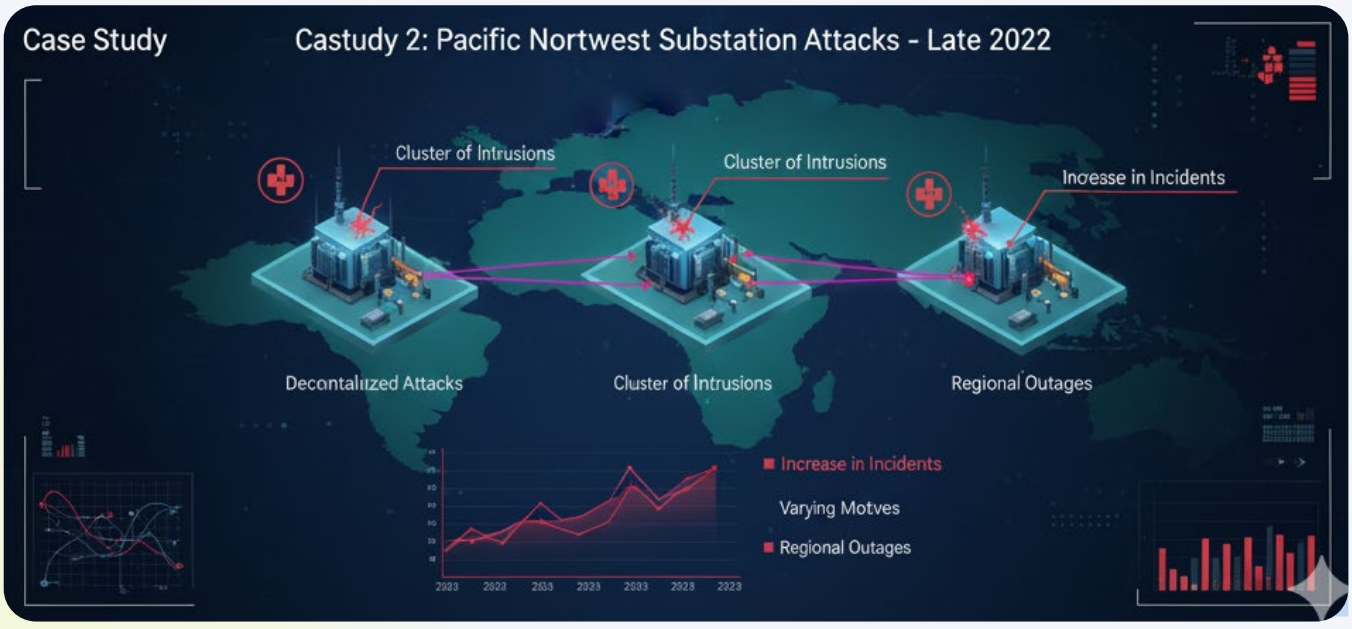
Pacific Northwest Substation Attacks Late 2022 Cluster

In late 2022, a series of substation intrusions across Oregon and Washington brought attention to the risks of repeated, decentralized attacks on regional infrastructure. Though most events caused limited outages, the pattern and frequency of incidents revealed systemic vulnerabilities. Multiple substations were accessed, equipment was damaged, and tens of thousands of customers were affected across separate but consecutive events.

These attacks were often opportunistic, and motivations varied—from criminal intent to possible ideological drivers. The lack of consistency in site protection, even within the same service region, amplified the threat. Substations targeted had minimal surveillance, low visibility, and outdated access controls. The cumulative effect exposed the fragility of assumptions around redundancy and response coordination in geographically clustered grids.

In the aftermath, utility operators reevaluated how threat intelligence was shared across service territories. Response protocols were updated to improve coordination with law enforcement, and security audits were extended to facilities previously considered lower risk. State and federal agencies issued advisories emphasizing the need for layered protection and broader asset coverage—not only for high-voltage transmission hubs but also for distribution infrastructure.

The significance of these events lies not in their scale but in their strategic implications. They demonstrated how infrastructure that falls outside of federal criticality thresholds may still pose an outsized risk when targeted in sequence. The long-term consequence was a shift toward regionally integrated security strategies, increased information-sharing, and greater regulatory scrutiny of what constitutes “critical” infrastructure in practice.



Tech-Enabled Defense

Integrating Smart Security for Smarter Grids

Utilities across the United States are adopting technology-driven approaches to harden substations against physical threats. With increasing frequency of attacks, real-time detection and automated response are becoming essential tools in maintaining grid integrity. Traditional methods—such as perimeter fencing and static camera systems—are no longer sufficient to deter or respond to sophisticated threats. Instead, utilities are leveraging artificial intelligence, machine learning, and integrated surveillance to enhance situational awareness and operational readiness.

Smart surveillance systems now use thermal imaging, acoustic sensors, and video analytics to detect and verify threats in real time. These platforms can identify unusual activity, such as trespassing or loitering near high-voltage equipment, and respond with automated deterrents like floodlights, audio warnings, and immediate alerts to operations centers. Detection systems are often embedded with edge-based processing, enabling them to operate independently of central networks. This makes them particularly useful for remote substations where bandwidth or latency constraints may exist.

An increasing number of utilities are integrating equipment monitoring with their physical security systems. Sensors attached to transformers and switchgear continuously monitor temperature, vibration, and current flow. Machine learning models trained on historical data can detect anomalies that may indicate sabotage, tampering, or mechanical failure. This convergence of asset condition monitoring and security detection supports both rapid incident response and preventive maintenance.

Unified operational dashboards aggregate intrusion alerts, camera feeds, and SCADA data, allowing security teams to correlate events and prioritize responses. These platforms enable operators to assess risk holistically, linking detection events at substations with broader grid operations and dispatch workflows. When a breach is confirmed, utilities can isolate affected segments, deploy mobile transformers, or initiate microgrid protocols to maintain local supply continuity.

Federal agencies have issued guidelines to support the secure and reliable deployment of these systems. Governance frameworks

define the responsibilities of infrastructure owners, AI developers, and service providers. Secure-by-design principles recommend end-to-end data protection for systems that use AI to detect and assess threats. Utilities are advised to implement data validation protocols, establish audit trails, and maintain oversight over third-party AI models used in critical applications.

Recent publications from infrastructure security authorities also emphasize the importance of securing the training and inference data used by AI systems. Without these safeguards, adversaries may attempt to introduce manipulated or misleading inputs that reduce detection accuracy. Guidance recommends techniques such as dataset versioning, tamper detection, and access controls to protect the reliability of AI-powered detection.

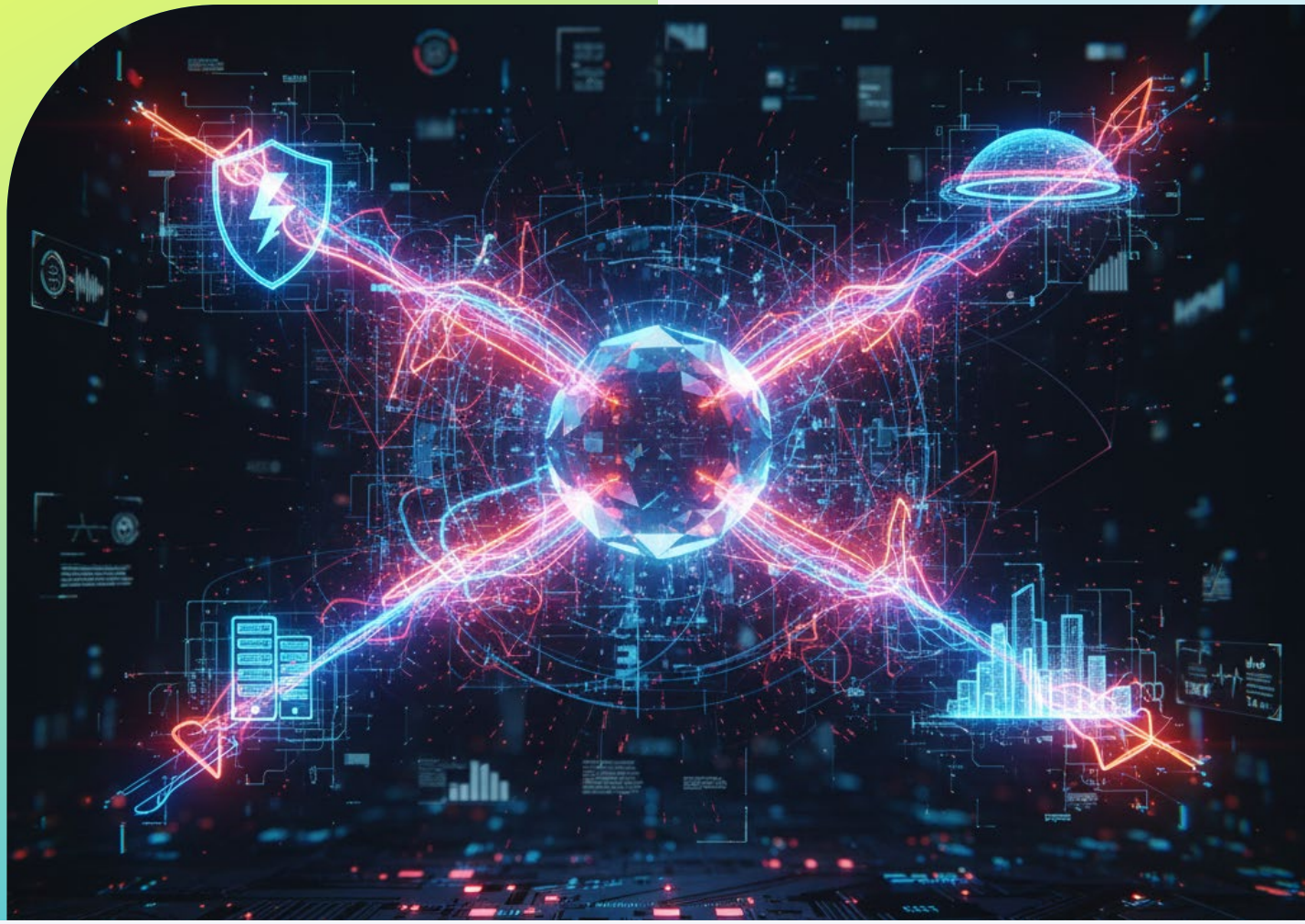
Operators are also encouraged to participate in coordinated cybersecurity and AI information-sharing initiatives. These platforms allow utilities to receive alerts about emerging threats, adversarial techniques, or misused detection systems. Shared analysis of AI deployment incidents helps refine industry standards and ensures a collective understanding of evolving physical and cyber risks to substations.

Some utilities are piloting advanced detection systems in regions with high incident rates. Evaluation criteria include detection latency, false alarm reduction, and system uptime during power outages. Testbeds are being developed in collaboration with national laboratories to simulate substation attacks and benchmark detection performance across various sensor configurations and environmental conditions.

Security operations centers (SOCs) play a central role in integrating these technologies. AI-generated alerts flow into SOC dashboards, where operators can validate incidents and coordinate field response teams. Escalation protocols are designed to activate layered defenses—ranging from law enforcement notification to grid segmentation and restoration planning.

While these smart security systems offer considerable advantages, agencies caution that they must be implemented with comprehensive governance and continuous oversight. Threat modeling, performance testing, and adversarial resilience exercises are recommended to ensure systems perform reliably under realistic attack conditions. Properly governed, AI-enabled surveillance not only protects physical infrastructure but also strengthens operational resilience.

In sum, the integration of intelligent detection, secure data governance, and operational response workflows represents a modernized approach to physical security. This adaptive model enables utilities to monitor, assess, and respond to threats at scale—reducing reliance on reactive measures and reinforcing the broader resilience of the power grid.



Public-Private Collaboration

The Human Side of Infrastructure Security

Effective physical protection of power infrastructure relies not solely on technology or regulation but critically on sustained collaboration between utilities, government agencies, law enforcement, and community stakeholders. Cross-sector coordination ensures that threat intelligence is shared rapidly, preparedness is regional, and response actions are aligned across institutional boundaries.

The framework underpinning this collaboration is rooted in partnerships facilitated by the Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Homeland Security. These partnerships engage infrastructure owners and operators through Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs), operationalizing dialogue across utilities, trade associations, local governments, and federal agencies. Such networks enable rapid dissemination of threat information, coordination during incidents, and shared planning for resilience.

At the regional level, CISA's Protective Security Advisors (PSAs) provide direct technical assistance

to electric utilities and local agencies. PSAs conduct vulnerability assessments, assist with physical hardening strategies, and connect partners with federal tools and funding opportunities. These in-person engagements support tailored security planning that reflects local asset characteristics and evolving threat conditions.

National guidance emphasizes the necessity of maintaining a baseline inventory of critical infrastructure assets and designing pre-incident collaboration among stakeholders responsible for energy, emergency services, and public health. This holistic visibility supports coordinated planning under Emergency Support Function #14 and facilitates efficient recovery sequencing across sectors.

The National Infrastructure Protection Plan (NIPP) and DC-level strategic directives outline how the public and private sectors co-manage critical infrastructure risk. These foundational documents formalize structures for shared responsibility, mutual trust, and coordinated response—establishing the joint security framework in which utilities and government partners must work.

CISA's most recent Strategic Guidance for 2024–2025 reinforces collaboration as a core mission priority. Regional CISA offices convene workshops, drills, and advisory sessions bringing together utility operators, public safety officials, and state and local governments to analyze simulated grid attack scenarios and develop joint contingency plans.

This public-private model has yielded practical outcomes: utilities across states now participate in threat-sharing networks, enabling early warning of extremist planning or emerging sabotage techniques. Some SCCs incorporate rapid response coordination, activating mutual aid between utilities when substations are threatened. Fusion centers coordinate messaging with law enforcement and utilities during escalating physical threats, ensuring organized incident resolution and resource allocation.

The human dimension of grid security thus extends beyond the perimeter fence. It involves ongoing engagement, trust-building, coordinated training exercises, and shared threat modeling. These relationships embed physical security within a broader resilience culture—one that recognizes strategic threats require more than equipment and barriers; they demand prepared, informed, and connected communities of responders.

References

01

01

Electric Information Sharing and Analysis Center (E ISAC)

2023 End of Year Report, Dec. 2023
https://www.eisac.com

02

National Conference of State Legislatures

Physical Security: Substation and Critical Infrastructure Attacks, Jan. 2023
https://www.ncsl.org

03

Federal Energy Regulatory Commission

Physical Security and Cybersecurity Interdependencies, Presentation, Jan. 2023
https://www.vedini.energy

04

Federal Bureau of Investigation

FBI offering reward for information on Moore County substation shootings, 2023
https://www.fbi.gov

05

WCNC Charlotte

Nearly 45,000 people were without power for days: Moore County substation attack remains unsolved a year later, Dec. 2024
https://www.wcnc.com

06

M. S. Donovan

Physical Security for Electric Power Infrastructure. Meerkat Publications, 2023

07

Cybersecurity and Infrastructure Security Agency

Resilient Power: Best Practices for Critical Infrastructure, 2022
https://www.cisa.gov

08

J. Johnson

Lessons from Metcalf: Ten years later, Utility Dive, Apr. 2023
https://www.utilitydive.com

09

P. W. Parfomak

Physical Security of the U.S. Power Grid: High Voltage Transformer Substations, Congressional Research Service, R45706, Mar. 2019.

10

U.S. Government Accountability Office

Electricity Grid: DOE Could Better Support Industry Efforts to Ensure Adequate Transformer Reserves, GAO 23 105813, Apr. 2023
https://www.gao.gov

References

02

11 **U.S. Department of Energy**

Large Power Transformer Resilience Report, Jul. 2024
https://www.energy.gov

12 **North American Electric Reliability Corporation**

Standards Announcement: Draft 3 of CIP 014 4 – Physical Security, May 2025
https://www.nerc.com

13 **North American Electric Reliability Corporation**

Reliability Standards Development Plan 2026–2028, Oct. 2024
https://www.nerc.com

14 **National Academies of Sciences**

Engineering, and Medicine, Enhancing the Resilience of the Nation's Electricity System. Washington, DC: The National Academies Press, 2017

15 **U.S. Department of Homeland Security**

Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure, Nov. 2024
https://www.dhs.gov Systems, April 15, 2024.
https://www.cisa.gov/news-events/alerts/2024/04/15/joint-guidance-deploying-ai-systems-securely

16 **Duke Energy News Center**

Duke Energy completes restoration to all customers in Moore County and surrounding counties, December 8, 2022
https://news.duke-energy.com/releases/duke-energy-completes-restoration-to-all-customers-in-moore-county-and-surrounding-counties

17 **FEMA**

Emergency Support Function #14 Annex: Cross Sector Business and Infrastructure, July 2020
https://www.fema.gov/sites/default/files/2020-07/fema_ESF_14_Business-Infrastructure.pdf

18 **FERC**

Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk Power System, April 14, 2023
https://www.ferc.gov/media/evaluation-physical-security-reliability-standard-and-physical-security-attacks-bulk-power

19 **FERC**

Joint Technical Conference Regarding Physical Security of the Bulk Power System, August 10, 2023
https://www.ferc.gov/news-events/events/joint-technical-conference-regarding-physical-security-bulk-power-system

20 **FERC**

Order directing study of effectiveness of physical reliability standards for the Bulk Power System, December 15, 2022
https://www.ferc.gov/news-events/news/ferc-orders-study-effectiveness-physical-reliability-standards-power-grid

References

03

21 **FERC**

Presentation: Evaluation of the Physical Security Reliability Standard and Physical Attacks to the Bulk Power System, April 20, 2023
https://www.ferc.gov/news-events/news/presentation-evaluation-physical-security-reliability-standard-and-physical

22 **FERC Order No. 802 / Complaint Docket EL20 21 000**

Reliability Standard CIP 014 2 background, June 2020
https://www.ferc.gov/sites/default/files/2020-06/EL20-21-000.pdf

23 **FERC**

Second Set of Responses of the Federal Energy Regulatory Commission... to Senator Murkowski's Questions, May 5, 2014.
http://www.energy.senate.gov/public/index.cfm/files/serve?File_id=5c3bf9d7-bb7f-4379-8f57-f58881a0b5d6

24 **MDPI**

Physical Security Auditing for Utilities: A Guide to Resilient Substation, 2024
https://www.mdpi.com/2313-576X/10/3/80

25 **National Academies of Sciences**

Engineering, and Medicine, Restoring Grid Function After a Major Disruption, in Enhancing the Resilience of the Nation's Electricity System, 2017
https://nap.nationalacademies.org/read/24836/chapter/6

26 **National Conference of State Legislatures**

Human Driven Physical Threats to Energy Infrastructure, May 2023
https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure

27 **National Rural Utilities Cooperative Finance Corporation**

Physical Security Concerns Grow Across the Utility Industry, Apr. 2023
https://www.nrucfc.coop/content/solutions/en/stories/energy-tech/physical-security-concerns-grow-across-the-utility-industry.html

28 **NERC**

2023 State of Reliability, June 23, 2023
https://www.industrialcyber.co/utilities-energy-power-water-waste/nerc-2023-state-of-reliability-finds-cyber-and-physical-security-continues-to-create-reliability-challenges/

29 **NERC**

Evaluation of the Physical Security Reliability Standard and Physical Security Attacks to the Bulk Power System, April 14, 2023
https://www.ferc.gov/media/evaluation-physical-security-reliability-standard-and-physical-security-attacks-bulk-power

30 **NCSL Summary of DOE 417 Data**

Human Driven Physical Threats to Energy Infrastructure, May 2023
https://www.ncsl.org/energy/human-driven-physical-threats-to-energy-infrastructure

References

31 **North Carolina Department of Public Safety**

State Responds to Power Outages in Moore County Following Incidents at Utility Substations, December 4, 2022
https://www.ncdps.gov/news/press-releases/2022/12/04/state-responds-power-outages-moore-county-following-incidents-utility-substations

32 **OPB/KUOW**

FBI warns of neo Nazi plots as attacks on Northwest power grid spike, January 19, 2023
https://www.opb.org/article/2023/01/19/surge-in-oregon-washington-substation-attacks-as-fbi-warns-neo-nazi-plots/

33 **OPB/KUOW**

String of electrical grid attacks in Pacific Northwest are unsolved, December 8, 2022
https://www.opb.org/article/2022/12/08/string-of-electrical-grid-attacks-in-pacific-northwest-are-unsolved/

34 **PubMed/NCBI**

Cybersecurity in Power Grids: Challenges and Opportunities, 2021
https://pmc.ncbi.nlm.nih.gov/articles/PMC8473297/

35 **Scientific Literature (Shuva Paul et al.)**

Resilience assessment and planning in power distribution systems: Past and future considerations, 2023
https://arxiv.org/abs/2308.07552

36 **TDWorld**

Security in the Sights: Utilities Face Armed Physical Security Threats, Apr. 2023
https://www.tdworld.com/safety-and-training/article/21261205/security-in-the-sights-utilities-face-armed-physical-security-threats

37 **The Guardian**

Attacks on Pacific north west power stations raise fears for US, December 9, 2022
https://www.theguardian.com/us-news/2022/dec/09/us-power-grid-pacific-northwest-attacks

38 **Think Power Solutions Blog**

Decoding NERC and FERC Compliance: What Utilities Need to Know in 2025, March 20, 2025
https://www.thinkpowersolutions.com/blogs/nerc-and-ferc-compliance-2025/

39 **Time, J. Harrell**

Is There Something More Sinister Going On? Authorities Fear Extremists Are Targeting U.S. Power Grid, January 9, 2023
https://time.com/6244977/us-power-grid-attacks-extremism/

40 **TRC Companies (Summarizing NERC)**

NERC files report on effectiveness of CIP 014 physical security standard
https://www.trccompanies.com/insights/nerc-files-report-on-effectiveness-on-cip-014-physical-security-standard

References

41

TRC Companies

What Is Grid Resilience and How Can It Be Improved? Oct. 2024
https://www.trccompanies.com/insights/enhancing-grid-resilience/

42

U.S. Department of Energy

Large Power Transformer Resilience Report, July 10, 2024
https://www.energy.gov/sites/default/files/2024-10/EXEC-2022-001242%20-%20Large%20Power%20Transformer%20Resilience%20Report%20signed%20by%20Secretary%20Granholm%20on%207-10-24.pdf

43

U.S. Department of Energy Office of Electricity Delivery & Energy Reliability

Electric Emergency Incident and Disturbance Reports (Form OE 417)
https://doe417.pnnl.gov/instructions

44

U.S. Department of Energy / E ISAC

Sector Spotlight: Electricity Substation Physical Security, Feb. 2023
https://www.cisa.gov/sites/default/files/2023-02/Sector%20Spotlight%20Electricity%20Substation%20Physical%20Security_508.pdf

45

U.S. Department of Homeland Security

Roles and Responsibilities Framework for Artificial Intelligence in Critical Infrastructure, November 14, 2024
https://www.dhs.gov/sites/default/files/2024-11/24_1114_dhs_ai-roles-and-responsibilities-framework-508.pdf

46

U.S. Government Accountability Office (GAO)

Electricity Grid: DOE Could Better Support Industry Efforts to Enhance Transformer Resilience, GAO 23 106180, Sept. 2023
https://www.gao.gov/assets/gao-23-106180.pdf

47

WFAE

Moore County attack spurs U.S. regulators to order study of electric grid security, December 15, 2022
https://www.wfae.org/energy-environment/2022-12-15/moore-county-attack-spurs-u-s-regulators-to-order-study-of-electric-grid-security

48

WUNC

A year after the Moore County power grid attacks, questions and challenges remain, December 1, 2023
https://www.wunc.org/news/2023-12-01/a-year-after-the-moore-county-power-grid-attacks-questions-and-challenges-remain

49

North Carolina Department of Public Safety

State Responds to Power Outages in Moore County Following Incidents at Utility Substations, December 4, 2022
https://www.ncdps.gov/news/press-releases/2022/12/04/state-responds-power-outages-moore-county-following-incidents-utility-substations

50

Industrial Cyber

E ISAC 2023 report highlights cybersecurity triumphs and challenges in electricity sector, February 22, 2024
https://industrialcyber.co/reports/e-isac-2023-report-highlights-cybersecurity-triumphs-and-challenges-in-electricity-sector/

References

06

51 **NERC**

Project 2023 06 CIP 014 Risk Assessment Refinement, status update, July 21, 2025
https://www.nerc.com/pa/Stand/Pages/Project_2023-06_CIP-014_Risk_Assessment_Refinement.aspx

52 **WCNC**

Still no arrests 2 years after Duke Energy substation attacks in Moore County, December 3, 2024
https://www.wcnc.com/article/news/crime/moore-county-duke-energy-substation-attacks-unsolved-two-years-later/275-338cd0cf-db3c-4122-84be-72b92c5da065

Disclaimer

About Vedeni Energy

VedeniEnergy

Vedeni Energy offers specialized services designed to help businesses navigate the complexities of the modern energy landscape. Our offerings are tailored to meet the unique needs of utilities, independent power producers, regulatory bodies, and other stakeholders, ensuring success through strategic insights, expert guidance, and innovative solutions.

Vedeni.Insights+

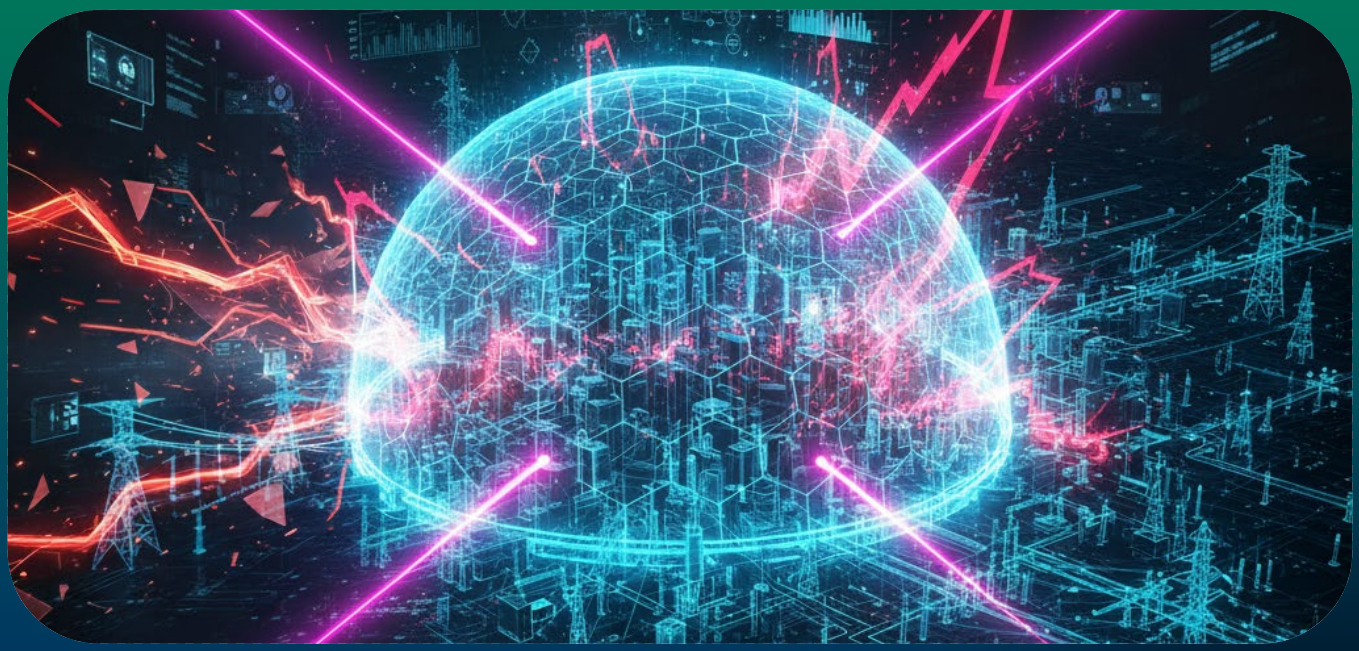
Vedeni.Insights+ is Vedeni Energy's subscription-based service, granting subscribers full access to Vedeni Energy's extensive library of whitepapers and in-depth technical analyses. These authoritative resources offer comprehensive examinations of the energy sector's critical topics, from market trends and regulatory changes to emerging technologies and strategic investment opportunities.

Vedeni.IQ+

Vedeni Energy's **Vedeni.IQ+** service provides actionable wholesale electric power market intelligence that enables clients to make informed decisions confidently. Our expert analysis and reporting distill complex energy market information into clear, concise insights, helping organizations elevate their market strategies, influence policy, and identify new opportunities.

Vedeni.Spark+

Vedeni.Spark+, a service provided by Vedeni Energy, is designed to help startups and established companies secure the capital funding necessary for growth and success. Our team of seasoned advisors works closely with clients to develop tailored funding strategies that align with their business goals and financial requirements.



TO LEARN MORE, VISIT US AT

WWW.VEDENI.ENERGY