VANGUARD™ | SENTINEL™

USE CASE

Power Grid Vulnerability: Addressing Physical and Cyber Threats to Critical Infrastructure

CLIENT:

Power Utilities and Other Critical Infrastructure

SOLUTIONS:

SENTINEL™ = A seamless sphere of protection for perimeters, facilities, and environmental conditions.

VANGUARD™ = Cyber defense securing SCADA, critical network and communication networks.

INSIGHT™ = Alarm Management that maximizes security investments.

KEY BENEFITS

- **All-in-One Protection:** Unified coverage across perimeters, facilities, electrical pathways, and network fiber—physical, cyber, and operational security in a single solution.
- **Real-Time Alerts & Response:** Detect threats instantly, from intruders to network disruptions, and act before damage occurs.
- **Multi-Asset Awareness:** Monitor fiber rights-of-way to protect not just networks, but adjacent buried utilities like gas, water, and communications lines.

THE CASE FOR INTEGRATED PHYSICAL AND CYBER SECURITY

Modern threats demand modern defenses. Critical infrastructure facilities—once thought secure behind fences and cameras—are increasingly targeted through coordinated physical and cyberattacks. These incidents expose how vulnerable even well-protected systems can be when physical security is overlooked or disconnected from network monitoring.

Deployed for over a decade by the DoD, DHS, and leading defense contractors, our solutions remain the most cost-effective and field-proven means of protecting the backbone of critical infrastructure. Powered by advanced fiber optic sensing, these systems deliver real-time intrusion detection and seamlessly integrate with existing infrastructure to trigger automated responses. As part of a layered security strategy, when a potential threat opens a manhole to cut off communications or approaches the perimeter, security teams receive instant alerts—gaining valuable time to prevent damage, theft, or service disruption.

The following real-world examples illustrate the scale and impact of such threats—and the urgent need for integrated, proactive defense solutions.

THE METCALF ATTACK

In 2013, a coordinated assault on the Metcalf, CA substation disabled multiple transformers, caused over $15 million in damage, and forced prolonged downtime. The attackers accessed underground manholes, cut fiber-optic communications cables, and after a 30-minute wait, opened fire on the transformers. Police were alerted only when automated systems detected overheating. The Metcalf attack remains a stark reminder that critical infrastructure can be compromised not only through cyberspace, but also through the physical networks that sustain it.

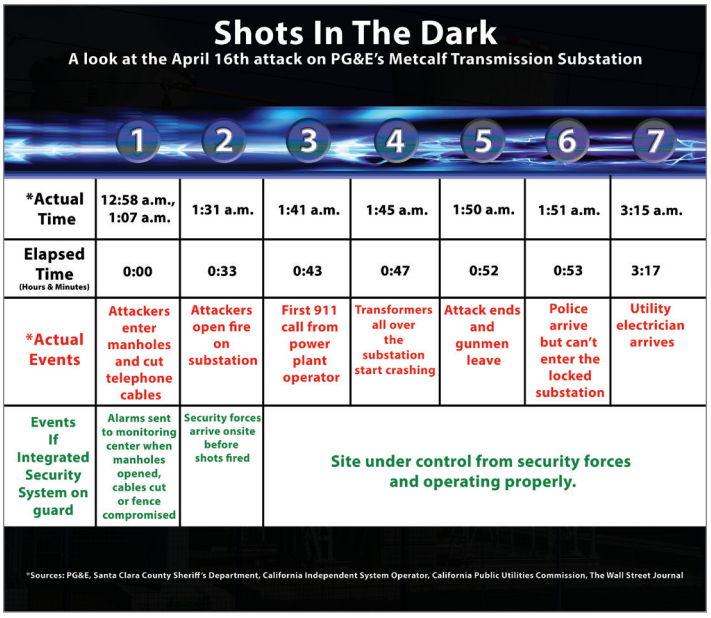
MOORE COUNTY, NORTH CAROLINA

On December 3, 2022, gunfire crippled two substations in Moore County, NC, leaving 40,000 residents and businesses without power for 5 days. One death was attributed to the outage, and full restoration took days. A state of emergency and curfew underscored the far-reaching consequences of a single incident.

DETECT EARLY. GAIN TIME. GAIN OPTIONS

The Metcalf and Moore County attacks are often cited as defining examples of the vulnerabilities facing our nation's critical infrastructure—but they are far from isolated events. In the years since, the number of physical security incidents targeting substations and transmission assets has steadily increased, prompting renewed attention from both regulators and industry. The Department of Energy and the North American Electric Reliability Corporation (NERC) have each identified physical threats—such as vandalism, theft, and coordinated attacks—as growing risks to grid reliability in their most recent assessments.

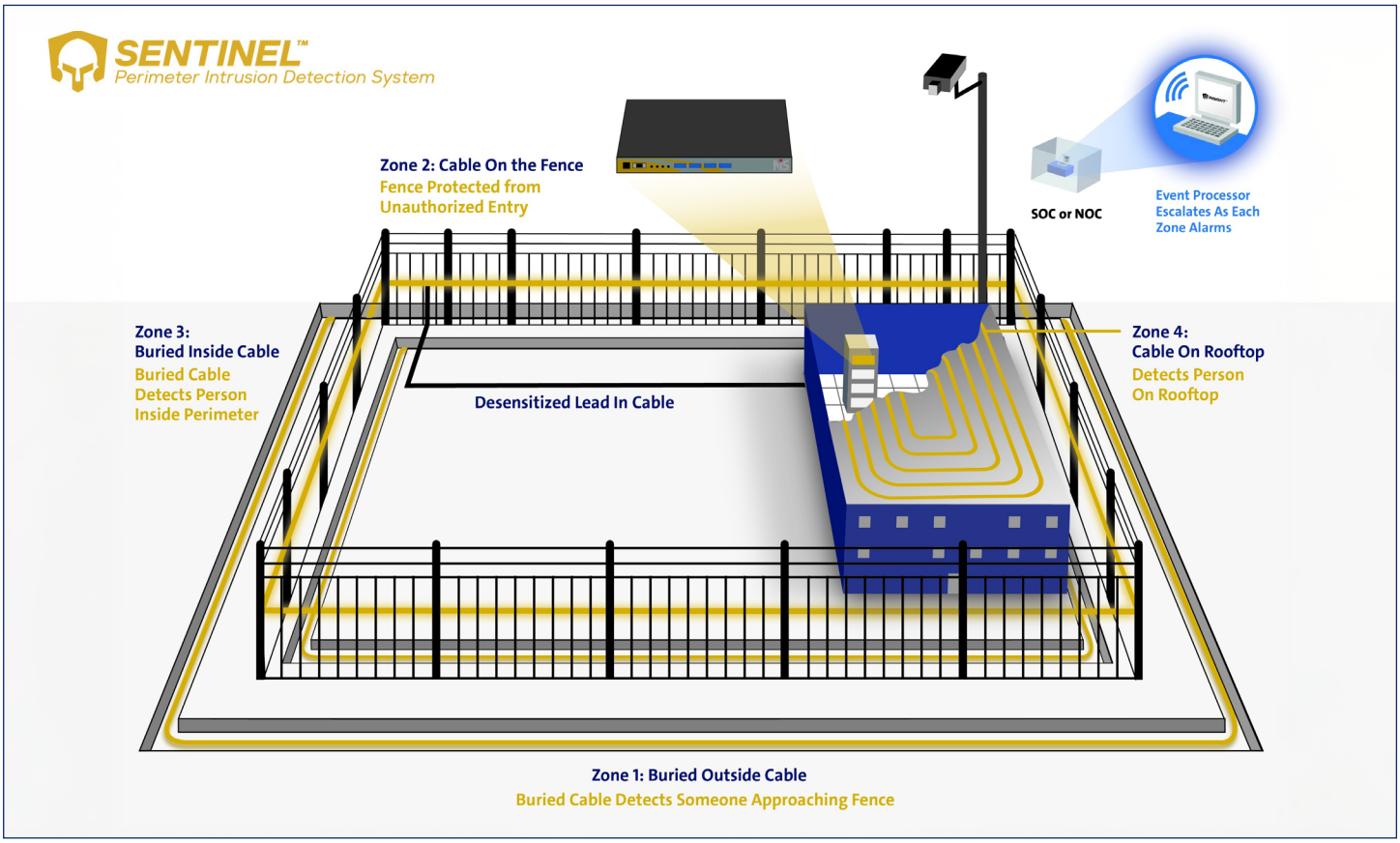
If a fully integrated physical and cyber security system had been in place at Metcalf or in Moore County, the outcomes could have been very different. Real-time sensing could have identified both the approach to the substation and intrusions into the manhole, interfacing with existing security infrastructure to generate alerts, cue surveillance cameras, activate perimeter lighting, and initiate alarms —all before damage occurred. Such layered detection and response capabilities are precisely what Network Integrity Systems' solutions are designed to deliver—providing early warning, situational awareness, and actionable intelligence to prevent disruptions before they start.

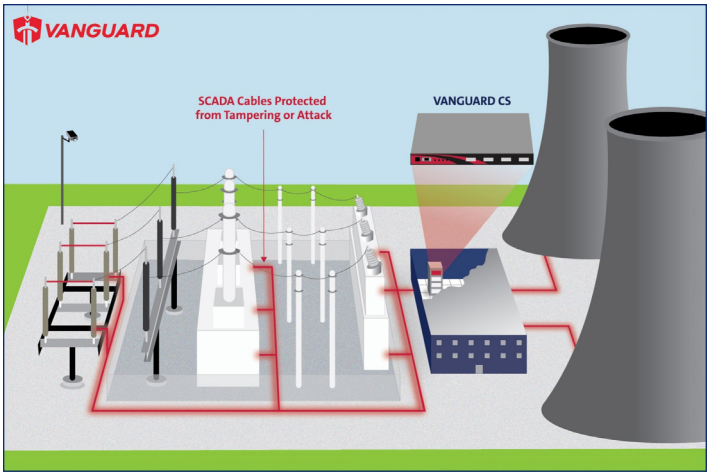


SENTINEL™: A UNIFIED SPHERE OF PERIMETER, ACCESS, AND THERMAL PROTECTION

At the core of the SENTINEL™ platform is its ability to create a seamless, 360-degree sphere of protection—covering everything from facility perimeters and access points to internal thermal conditions and underground power distribution lines. Threats are detected as they approach, attempt to breach, or move within restricted zones, providing real-time awareness across every layer of defense. Using advanced fiber optic sensing, SENTINEL can be deployed underground, along fence lines, across rooftops, alongside power cables, and within secured areas to deliver true three-dimensional coverage.

- **SENTINEL™ Perimeter Security solutions** are engineered for ultra-low false alarms, enabling security teams to respond faster and more accurately to verified threats. With proactive service and regular maintenance included under contract, NIS ensures long-term reliability and a low total cost of ownership across the system's lifecycle.
- **SENTINEL AXS™** open/close manhole and cabinet sensors protects the often-overlooked access points adversaries target—manholes, handholes, and cabinets where critical infrastructure is most exposed. By detecting unauthorized openings the instant they occur, SENTINEL AXS enables rapid intervention before disruption or damage can take place. Its no-power-at-point design makes it ideal for remote or hard-to-reach access points that traditional systems cannot effectively monitor.
- Extending protection beyond intrusion detection, **SENTINEL TS™ Distributed Temperature Sensing System** adds real-time thermal monitoring for power busways and other essential electrical pathways. This early-warning capability helps operators prevent overheating, equipment failure, and fire hazards—protecting uptime, assets, and lives.





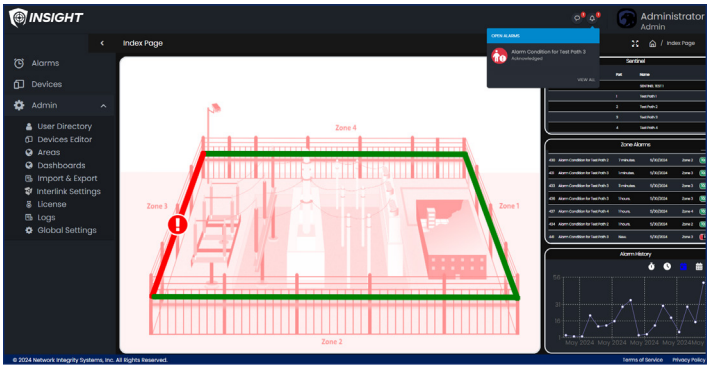
VANGUARD™: CYBER PROTECTION FOR AN UNBROKEN LINE OF DEFENSE

While SENTINEL™ safeguards the facility and its electrical pathways, VANGUARD™ protects the network infrastructure itself—creating an unbroken line of defense across the fiber routes that link power stations and carry vital SCADA and communications data. Whether the threat arises from accidental excavation, fiber tapping, environmental stress, or deliberate disruption (as seen in the Metcalf attack), VANGUARD detects and alerts to risks before they escalate into service outages or catastrophic failures.

As an additional advantage, VANGUARD's continuous monitoring of fiber cables installed in rights-of-way also extends protection to other buried utilities—such as gas, water, and communication lines—that share those same corridors. This multi-asset awareness helps operators prevent secondary damage, reduce risk, and maximize the value of a single sensing system. Together, SENTINEL and VANGUARD deliver complementary, layered protection—uniting physical, electrical, and network security into one integrated defense for critical infrastructure.

INSIGHT™: UNIFIED ALARM MANAGEMENT FOR GRIDWIDE PROTECTION

To streamline monitoring and incident response, SENTINEL and VANGUARD integrate with our INSIGHT™ Alarm Management software, a comprehensive platform that consolidates device management, alarm visualization, and analytics into a single intelligent interface. INSIGHT enables seamless integration with existing and future systems, including access control, video surveillance, and LIDAR, supporting a modular security strategy.



WHY NOW

Relying solely on unmonitored fences, walls, or legacy security measures is no longer sufficient. With SENTINEL and VANGUARD, utilities gain a comprehensive, layered defense that anticipates modern threats, detects them in real time, and enables rapid response before damage is done.

MADE IN THE USA, FOR THE USA

Network Integrity Systems designs, engineers, and supports the SENTINEL, VANGUARD and INSIGHT platforms in-house—including firmware and software—while providing full consultation, installation, and support for select OEM components. This U.S.-based, end-to-end approach delivers accountability, security, and unmatched responsiveness.

With a **single point of accountability** throughout the solution's lifecycle, NIS ensures consistency and reliability from project execution to ongoing support—giving customers a seamless defense that safeguards people, assets, and critical infrastructure for the reliable, uninterrupted operation of the utilities that power our world.

www.networkintegritysystems.com