Critical Infrastructure, Sabotage, and Service Disruptions

What physical protection of energy infrastructure must achieve today

Foto: www.stockadobe.com / nilofa

Operators of critical energy infrastructure around the world are facing a fundamental transformation. New regulatory frameworks - such as international security standards, industry-specific requirements, and initiatives like the European NIS 2 Directive or comparable national legislation - are, for the first time, requiring not only protective measures across all sectors but also their systematic planning, implementation, and verifiability. For energy suppliers, grid operators, and municipal utilities, this means moving away from isolated security measures toward comprehensive, robust resilience strategies.

The threat is by no means theoretical. Physical attacks on energy infrastructure have increased significantly worldwide in recent years, demonstrating just how vulnerable even highly redundant networks can be.Bereits im September 2025 waren mehrere Hochspannungsmasten in Berlin Ziel von Brandanschlägen. Die Folgen: tagelange Stromausfälle und eine intensive öffentliche Debatte über den Zustand des physischen Schutzes kritischer Energieinfrastrukturen. Klar wurde dabei: Klassische Einzelmaßnahmen wie Zäune, Kameras oder Wachschutz greifen zu kurz, wenn sie nicht in ein übergeordnetes Sicherheitskonzept eingebettet sind.

A striking example is an arson attack on a cable bridge in Berlin's Lichterfelde district in January 2026. The incident led to a widespread power outage that affected tens of thousands of households and businesses for days - in the middle of winter. Critical facilities such as hospitals had to switch to emergency power, and public transportation was disrupted. Investigative authorities believe it was a politically motivated act of sabotage.

As early as September 2025, several high-voltage pylons had been the target of arson attacks. The consequences: day-long power outages and an intense public debate about the state of physical protection for critical energy infrastructure. It became clear that traditional individual measures such as fences, cameras, or security guards fall short if they are not embedded in an overarching security concept.

From "Best Effort" to Verifiable Resilience

Modern regulatory requirements oblige operators to systematically analyze their risk profile and develop appropriate protection and resilience measures. These include risk analyses, security concepts, reporting obligations, and comprehensive documentation. The physical protection of substations, cable routers, switches, and control rooms is explicitly included.

For energy suppliers, this represents a paradigm shift: security concepts must be risk-oriented, measurable, and auditable. They must not rely solely on empirical knowledge but must clearly demonstrate how threats are identified, assessed, and mitigated. As a result, resilience becomes an operational task - not a theoretical requirement.

The bottleneck is often at the control center

Practical experience shows that the critical point is often not at the perimeter, but in the control center. Security and operational systems have evolved over the years: access control, video surveillance, intrusion and fire detection systems, perimeter security, as well as OT and SCADA alarms often operate side by side - using different manufacturers, interfaces, and processes.

In stressful situations, this fragmentation leads to media breaks, duplicate alarms, and wasted time. Operators with many locations - some of which are unmanned - face a particular structural challenge: limited personnel resources coupled with high demands on availability and responsiveness.

What matters most, therefore, is not the individual sensor technology but the ability to quickly verify, prioritize, and systematically process events.

Operational requirements in critical Infrastructures

Physical protection of energy infrastructure involves a wide range of functional requirements. In practice, these regulatory requirements translate into a very specific set of questions:

- Who detects what - and how reliably? (e.g., someone climbing a fence vs. animal movement, a drone vs. a flock of birds)
- How quickly is verification performed? (Live video feed, site map, contextual information)
- What measures are planned? (Blockades, closures, announcements, alarm forwarding, intervention)
- Who is notified - and with what level of redundancy? (SMS/phone/email/operations control system)
- How is documentation handled? (Complete, audit-proof, evaluable for audits)

The ability to provide evidence is becoming increasingly important. In addition to legal requirements, international standards such as ISO standards, as well as cyber and resilience requirements, are increasing the pressure on operators. Processes must not only be defined but also documented in a measurable and audit-proof manner to ensure that decisions and measures can be traced at any time.

Greater efficiency and safety in the control center

Against this backdrop, many operators are turning to integrated risk management platforms that centrally consolidate existing systems. The goal is not to replace subsystems, but to correlate information, prioritize events, and provide recommendations for action in near real time.

Such solutions enable a consistent situational overview, support control center staff with structured action plans, and ensure comprehensive documentation of all events and decisions - an aspect that is becoming increasingly relevant, particularly in regulated environments.

Supplemented by AI-powered analysis methods, anomalies can also be detected, such as unusual movement patterns, recurring disruptions, or deviations from normal operations. The focus thus shifts from merely reacting to a preventive security strategy that addresses risks as they arise.

Conclusion: Resilience must work in everyday life

The expectations regarding the protection of critical energy infrastructure are clear. Security of supply is no longer a voluntary goal worldwide, but rather both a regulatory obligation and a societal expectation.

- Central platform for integrating physical security and operational systems (including video, access, fire, and perimeter systems)
- Vendor-neutral integration of existing infrastructure
- Unified situational overview for control centers at distributed, partially unmanned locations
- Structured incident handling through dynamic, predefined action plans
- Audit-proof documentation as a basis for verification and audits
- Expandable with analytics and AI functions for early detection of anomalies

Recent acts of sabotage demonstrate that physical risks are real and can have significant consequences. This calls for security concepts that integrate technology, processes, and organizational structures and function reliably in an emergency. Only those who can implement and demonstrate resilience will meet the growing demands from regulators, the public, and operations.

www.advancis.net

SECURITY INSIGHT
Fachzeitschrift für Unternehmenssicherheit, Facherrichter und Systemhäuser