genasys

The Critical Infrastructure Response Gap

Protecting Power and Data Infrastructure: From Perimeter Threats to Real-Time Response

genasys.com

Executive Summary

Power utilities and data centers operate across large, distributed environments with limited on-site personnel. While most facilities can detect intrusions, they often lack the ability to stop them in real time. This creates a critical security gap.

Physical attacks are increasing and targeted. Substations, remote assets, and high-value infrastructure are frequently hit because intruders know response will be delayed. Detection systems work, but during the first critical 10 to 30 minutes it takes responders to arrive, intruders act without resistance.

By the time help arrives, the data center or power facility has been compromised, and the damage is often already underway or complete:

- Equipment is damaged or stolen, leading to emergency repair and replacement costs, higher insurance exposure, and increased risk of repeat targeting
- Operations are disrupted or taken offline, risking SLA breaches, financial penalties, extended outages, and loss of customer trust
- Regulatory and compliance exposure increases, leading to heightened scrutiny, audits, fines, and mandatory corrective actions

Security systems that only observe and notify are not sufficient. Facilities must be able to act the moment an incident begins.

This requires a shift from passive monitoring to active deterrence, where systems don't just detect threats, but engage them in a forceful way. Long-range, targeted communication capabilities enable operators and security personnel to issue clear warnings, establish control, and stop intrusions without deploying personnel and equipment.

At the same time, highly critical data and power facilities cannot rely on a single system for effective protection. They require coordinated communication across teams, systems, and locations, ensuring the right people receive the right information instantly and can act without delay.

In this eBook, you'll see these capabilities in action through real-world critical infrastructure case studies and learn how to:

- Deter intrusions before they escalate
- Communicate clearly across large, noisy environments
- Coordinate response across teams and systems in real time
- Reduce downtime, risk, and operational disruption

The Security Gap in Critical Infrastructure

Power utilities and data centers operate across large, distributed footprints that are difficult to secure in real time, often with limited or no personnel on-site.

Utilities manage hundreds or thousands of substations, many in remote or lightly populated areas. Data centers, while more centralized, still span large campuses with multiple access points and perimeter zones. In both cases, continuous on-site coverage is not practical, leaving large areas physically unmonitored.

Increasing Physical Threats

Physical security incidents are documented and rising:

- Attacks on data centers and substations, including vandalism and ballistic damage, have increased in recent years (2022–2025) as reported by federal and industry organizations
- Copper theft and equipment tampering remain frequent, especially at remote sites
- Data centers and energy facilities face intrusion attempts and protest activity
- Break-ins, sabotage, and attempts to disable substations also happen to support secondary crimes

These incidents consistently target locations where immediate intervention is unlikely.

Detection Without Immediate Action

Most data centers and power facilities already have strong monitoring in place that includes:

- State-of-the-art surveillance cameras
- Intrusion detection sensors
- Automated alerts

When an incident occurs, the process is consistent:

- Alert is triggered
- Sent to personnel
- Reviewed and verified
- Response is initiated

However, there is a gap between detection and action. During this window, nothing within the existing security systems forces the threat to stop. In these critical minutes the damage is already being done.

Response Time Defines the Outcome

Incidents unfold quickly:

Intrusions occur in seconds > Damage happens in minutes > Theft is often complete before responders arrive

At the same time, response is not immediate:

- Law enforcement typically arrives in 10–30 minutes depending on how remote the location is
- Internal teams, if they exist, must mobilize and travel in minutes

Most security systems detect threats, but they do not act on them. By the time a response reaches the data or power center site, the outcome is often already determined.

The Core Problem: Delayed Responses

The Consequences of Delayed Response

Picture this: Late at night, a small, coordinated group of three to four individuals pull up outside a remote data center facility, leaving a driver in the vehicle while the others move quickly to the perimeter. They know exactly where to go. Using bolt cutters and portable saws, they breach a low-visibility section of fencing and head straight for high-value equipment, cutting and stripping copper grounding wires within minutes.

Sensors and cameras detect the activity almost immediately, triggering alerts to internal personnel. Someone wakes up, checks the feed, and tries to determine if it's a real threat. Law enforcement is called and dispatched.

On-site, however, nothing forces the intruders to stop. A general alarm sounds but is ignored as they continue working, load the materials, and leave the way they came.

By the time responders arrive 15–20 minutes later, the site is empty, but critical components have already been damaged or removed, and end users have already been impacted.

Without a way to directly confront intruders, facilities and operations are at risk. Depending on the incident, delayed response exposes you to:

- Equipment theft and infrastructure damage
- Extended outages and service disruption
- SLA breaches and financial penalties
- Emergency repair and replacement costs
- Regulatory scrutiny and compliance risk
- Worker and contractor safety exposure
- Increased insurance costs and claims
- Repeat targeting of vulnerable sites
- Loss of customer and stakeholder trust
- Internal accountability and operational pressure

LRAD: Immediate, On-Site Intervention

The Long Range Acoustic Device ® (LRAD) introduces a capability most security systems lack: direct engagement at the point of intrusion.

LRAD projects tightly focused audio beams up to 5 km (16,404 ft), cutting through noise, physical barriers, and chaos. With powerful voice broadcasts and deterrent tones, it enables targeted communication, real-time engagement, and effective deterrence at a distance.

From Passive Security to Active Deterrence

Most physical security systems are designed around a passive model. They are built to observe activity, document events, and notify personnel when something occurs.

An active model shifts the objective from observation to influence.

- **Deter** — Discourage intrusion before it escalates
- **Intervene** — Engage immediately when an incident begins
- **Control** — Shape outcomes at the point of activity

This changes the role of the security system from monitoring events to directly impacting them as the crime unfolds.

With LRAD, operators can forcefully communicate with perpetrators to:

- Issue real-time verbal warnings or deterrent tones before an incident begins or escalates
- Establish intent at a safe distance keeping personnel out of range
- Direct individuals to comply or leave immediately

LRAD systems are remotely operated, allowing teams to:

- Engage threats immediately without deploying personnel
- Employ a macro or expanded field of operations over an entire facility and surrounding area
- Expand real-time coverage of the entire facility without increasing personnel or physical presence
- Maintain safe standoff distance without escalating a potentially lethal response from the perpetrators
- Monitor and protect multiple locations from a central command center

By combining precision targeting, long-range intelligibility, and remote operation, LRAD shifts security from passive monitoring to immediate, on-site intervention.

The Benefits of Active Security Systems

When intrusion is met with immediate deterrence, the outcome changes:

- Incidents are stopped before damage or loss occurs
- Critical equipment remains online and operational
- Downtime and service disruptions to end-users are avoided
- SLA breaches and financial penalties are prevented
- Emergency repair and replacement costs are avoided or minimized
- More area is secured without the added cost of additional security staff or equipment
- Regulatory and compliance exposure is minimized
- Worker and contractor safety is preserved
- Sites are less likely to be targeted again
- Customer and stakeholder confidence is maintained

Why Trust LRAD

On October 12, 2000, a small boat packed with explosives struck the US Navy vessel, the USS Cole in Yemen, killing 17 sailors and injuring more than 40. At the time, the crew had no way to project clear, authoritative warnings at distance. That communication gap cost lives.

In response, Genasys developed the world's first LRAD, giving militaries and governments a tool to deliver unmistakable voice commands across thousands of meters. It set a new global benchmark for clarity in crisis, opening a new market for critical communication systems. Its proven effectiveness in defense and border security operations has since led to widespread adoption across critical infrastructure, where immediate, on-site intervention is just as essential.


MAA
MAA
CMWD

Genasys Protect: Coordinated Communication and Response

While acoustic systems provide immediate, on-site intervention, Genasys Protect connects detection, communication, and coordination into a single workflow.

Genasys Protect integrates with existing sensors and monitoring systems to trigger instant, automated multi-channel alerts when an incident is detected. These alerts can be tailored and delivered simultaneously to internal teams, security personnel, responders, and, when appropriate, the public. Operators can manage incidents from a shared, real-time map-based view, improving coordination across teams without switching between systems.

This allows data centers and power facilities to:

- Automatically escalate incidents the moment they are detected
- Notify the right people with the right information immediately
- Coordinate internal teams and external responders faster

Genasys Acoustics (Wide-Area Communication)

Genasys Acoustics systems broadcast clear, intelligible voice alerts 60° to 360°, over local and large areas. Built-in solar charging, battery backups, and satellite connectivity keep systems online even when power grids, networks, or other critical infrastructure are down.

Unlike conventional speakers or sirens our systems boast an STI of .95. This means what you broadcast is clearly heard and understood.

While LRAD enables targeted, directional engagement, Acoustics provides site-wide coverage, ensuring that once a message is sent, it reaches everyone who needs to hear it.

Case Studies

Entergy Nuclear Power Facility

Energy | Nuclear Security | Perimeter Protection

Operating under strict Nuclear Regulatory Commission requirements, Entergy's Arkansas Nuclear One facility needed to protect over 1,000 personnel and surrounding communities while maintaining secure separation between the public and the site. Legacy communication systems limited their ability to deliver immediate, large-area warnings and act as a deterrent during security breaches.

Entergy deployed LRAD systems across blast-resistant enclosures around the facility perimeter, enabling clear, long-range voice commands and deterrent tones. Security teams can now warn and deter intruders from a distance, maintain controlled perimeters, and communicate instantly across the site, improving response time and strengthening overall facility security.

Hoover Dam

Dams | Physical Security | Intrusion Deterrence

Protecting restricted areas at Hoover Dam required constant monitoring and the ability to deter intruders without relying on resource-intensive patrols. Existing tools lacked range, clarity, and 24/7 coverage.

LRAD systems with integrated cameras and searchlights were deployed to provide continuous surveillance and long-range communication. Security teams can identify, track, and issue clear verbal warnings or deterrent tones to intruders up to 3,000 meters away, reducing manpower needs while strengthening perimeter security.

Texas Power Plant

Energy | Industrial Safety | Facility-Wide Alerting

A large Texas power plant serving approximately 800,000 homes needed a reliable way to communicate with over 180 workers in a high-noise industrial environment. Traditional sirens and PA systems lacked clarity and range, creating risk during emergencies where instructions must be understood immediately.

The plant deployed Genasys Acoustics systems integrated with Genasys Protect to broadcast clear voice instructions and alerts across the facility. Workers can now hear and understand messages above ambient noise, enabling faster response, safer evacuations, and improved coordination during incidents.

Multinational Energy Company

Oil & Gas | Enterprise Operations | Multi-Site Security

A global energy company with over 73,000 employees across distributed sites struggled with fragmented communication systems that slowed response times and limited coordination during emergencies. The lack of a unified platform created risk across both remote and urban operations.

By implementing Genasys Protect and integrating it with existing enterprise systems, the company established centralized control over multi-channel communications. Security and operations teams can now send geo-targeted alerts instantly, coordinate responses across sites, and significantly reduce response times while improving workforce safety and business continuity.

Case Studies

Puerto Rico Dam Early Warning System

Critical Infrastructure | Dams | Public Safety

After hurricanes Irma and Maria caused severe flooding and the Guajataca Dam breach threatened nearby communities, Puerto Rico recognized the growing danger posed by its aging dam infrastructure, many structures more than 70 years old.

Puerto Rico addressed this risk by integrating sensors that monitor reservoir levels, spillway flows, weather conditions, and seismic activity with Genasys Protect across 37 dams threatening hundreds of thousands of downstream residents. Emergency managers now monitor conditions from seven EOCs and issue instant automated alerts through multiple channels, including Genasys Acoustics, when thresholds indicate danger, giving communities critical time to take protective action.

Port Houston

Maritime Safety | Trade Protection | Critical Infrastructure

Port Houston manages **52 miles of the Houston Ship Channel and more than 200 public and private terminals**, supporting one of the largest cargo ports in the United States. Recurring threats from hurricanes and severe weather threatened the thousands of workers, visitors, and ships moving across facilities miles apart.

Port Houston unified alerting with Genasys Protect integrated with the port's ERP contact management system. The platform now delivers multi-channel alerts through SMS, email, and 13 Genasys Acoustics devices, enabling managers to quickly communicate instructions and deploy resources when incidents occur anywhere along this critical supply chain corridor.

Tengiz Oil Field

Oil & Gas | Large Facilities

Oil from Kazakhstan's Tengiz Field is produced under extremely high pressure and contains large concentrations of sulfur and other hazardous gases, creating serious safety risks for workers and site visitors.

To protect personnel across **one of the world's largest oil fields**, operators deployed more than **100 Genasys Acoustics devices** integrated with gas detection sensors. When hazardous gas levels are detected, the systems automatically trigger emergency sirens and broadcast clear voice safety instructions across the site, giving workers immediate warnings and time to move to safety.

Conclusion - Strengthening Critical Infrastructure with Intelligent Acoustic Communication

Demand for energy and data continues to rise, increasing the scale, load, and strategic importance of power infrastructure and data centers. These facilities face persistent risks, including intrusion, sabotage, and operational disruptions that can interrupt power delivery, degrade network availability, and impact the communities and organizations that rely on them. In these environments, effective security systems are essential to maintaining continuity, protecting assets, and enabling a coordinated response during critical events.

Traditional methods, including sirens, radios, and fragmented notification systems, often fall short in high-risk or time-sensitive scenarios. They lack clarity, range, or the ability to deliver actionable instructions when it matters most. For facilities that power communities and protect critical digital infrastructure, this gap creates unnecessary risk.

This is where advanced acoustic technologies redefine what is possible when it comes to keeping data centers and power facilities safe and operational.

LRAD and **Genasys Acoustics** solutions provide clear, intelligible voice communication over long distances, even in acoustically challenging environments. Whether managing a security breach, coordinating emergency response, or guiding personnel during evacuation procedures, these systems ensure that critical instructions are heard, understood, and acted upon immediately.

When combined with modern platforms that enable zone-based targeting, real-time situational awareness, and a common operating picture, LRAD and Acoustics solutions enhance decision-making, reduce response times, and improve overall outcomes.