

ENHANCING MISSION-CRITICAL INFRASTRUCTURE WITH WIRELESS SECURITY

The term “critical infrastructure” has been widely applied in recent years to cover everything from government facilities, power plants, and water treatment plants to highways, mass transit, and data centers, to name a few. The truth of the matter is that we depend on critical infrastructure facilities to keep things running regardless of whether they’re located in Washington, D.C. or somewhere on Main Street, USA. This poses a multitude of challenges for security personnel at public and private organizations tasked with protecting these facilities. And although different types of critical infrastructure facilities face their own distinct security challenges, they also share many commonalities at different scales across multiple facilities and geographic locations.

That’s a lot of ground to cover—literally.

One of the principal tenets of modern physical security is the need for layered solutions. There’s a long list of technologies that can be deployed to better secure critical infrastructure, but not all are appropriate for every application. The secret to success lies in the ability to combine the best possible solutions into an integrated security solution that starts at an organization’s perimeter—be it the fence line of an industrial complex in the suburbs or the front doors of a multi-tenant skyscraper in a major metro city—and moves inward to critical interior areas that require additional layers of security.

EFFECTIVE SECURITY DEMANDS EFFICIENT INFRASTRUCTURE

Protecting critical infrastructure on any scale requires robust security infrastructure (the backbone) to integrate otherwise disparate system technologies.

For the purposes of this article and area of expertise, let’s focus on two distinct security system applications: intrusion detection and duress notification.

One of the fastest trending infrastructure solutions continues to be wireless technology. First deployed for security applications some 40 years ago, wireless technology has continued to evolve from simple door and window intrusion sensors to advanced access, video surveillance, and sensor applications. Transitioning from wired to new modern wireless security infrastructure provides more economical and effective ways to extend the scale, reach, and effectiveness of security system deployments faster and with greater cost efficiency. Eliminating the need for long cable runs from independent distribution frame (IDF) closets to endpoint devices located throughout a facility saves time and money during installation and over the course of the system’s lifetime. And as the scale and complexity of a hard-wired installation increases, so do the economies of scale, yielding even greater return on investment (ROI) and lower total cost of ownership (TCO) over time.

MORE SENSORS MAKE MORE SENSE

Commercial/industrial properties increasingly rely upon a wide selection of sensors for intrusion detection, environmental control, occupancy monitoring, motion detection, traffic monitoring, smoke/CO detection, and more. In addition to performing their primary functions to detect specific types of activity, modern sensors can be integrated into many intrusion, access, or video management platforms to trigger specific sequences of events. These can include full-frame video recording, lockdowns, fire alarm activation and numerous building automation events including HVAC activation, lighting management, and even people mover system control.

The level and scale of integrating advanced wireless sensors is virtually limitless with continued growth and expansion driven by customers' needs and demands to proactively prevent and mitigate new and emerging threats. Additionally, wireless infrastructure also best supports modern wearable panic notification devices that can activate different alarm levels and provide location services to best assist first responders.

New advancements in intrusion detection system wireless technology allow any commercial enterprise to easily accommodate floor plan adjustments and changes, and scale to accommodate expansion—from the perimeter to innermost protected spaces. This holds true even when deployed at large campuses and older facilities that often present installation and operational challenges caused by thick walls, dense materials, and complex environments. Modern wireless infrastructure solutions also provide the added convenience of mobile control, allowing system admins to manage, monitor and respond to system activity from anywhere using an app on their smartphones. All these value propositions are not collectively possible utilizing dated wired infrastructure.

Why 900MHz Wireless Rules...

- | | | | |
|---|---|--|--|
| <ul style="list-style-type: none">• Frequency Hopping Spread Spectrum (FHSS) technology helps reduce susceptibility to interference and jamming attempts. | <ul style="list-style-type: none">• Deep physical penetration ensures always-on communication even with dense physical obstacles like concrete, brick, and heavy walls. | <ul style="list-style-type: none">• High resistance to other wireless interference | <ul style="list-style-type: none">• Quick, reliable installations with minimal structural impact on facilities |
|---|---|--|--|

WIRELESS SECURITY INTEGRITY

The debate over whether wireless belongs in professional security systems is over. Modern wireless systems deliver the reliability and resilience required for critical security applications. Inovonics pioneered the use of 900MHz security technology for professional security applications, which has proven to be both highly secure and exceptionally reliable across thousands of mission-critical deployments, earning the reputation as the industry standard for professionally installed commercial security systems and critical infrastructure.



Typical applications for wireless-first technology at critical infrastructure sites include a wide range of facilities. A few prime examples include:

Utility facilities and power stations: Monitor gates, perimeter access points, control rooms, equipment buildings, and restricted areas.

Water treatment plants: Protect chemical storage, pump rooms, mechanical spaces, exterior doors, and remote

equipment areas.

Transportation facilities: Secure maintenance buildings, storage yards, restricted access doors, parking areas, and operations centers.

Government or municipal buildings: Monitor public entrances, staff-only areas, records rooms, equipment rooms, and after-hours access points.

Industrial/commercial complexes: Extend security across warehouses, loading docks, service entrances, fenced areas, and multiple buildings.

Data centers: Protect valuable data and servers from being physically stolen.

LAST WORDS ON WIRELESS-FIRST

Making the transition from traditional wired to wireless-first security infrastructure allows commercial/industrial properties to extend protection to areas that are difficult, expensive, or disruptive to wire. It also allows the integration of new and emerging sensor solutions to expand the overall capabilities of existing integrated video, access, and intrusion system platforms with centralized, remote management and control with the highest levels of performance and integrity.

For more information on the efficacy of wireless-first mission-critical infrastructure, read our whitepaper, [Characteristics of RF Wireless in Commercial Applications](#).

By Andrew Griffey, Senior Product Manager, [Inovonics](#)