HOW WIRELESS MESH HELPS TACKLE

Converging Physical & Cyber Threats **Within the Industrial Security Sector**

The security executive role has never been more challenging as physical and cybersecurity threats have converged to become a two-headed monster that must be battled.

Brian Higgins, CPP, CSSP, President of Group 77 LLC

RAJANT

Table of Contents

Introduction

Security technologies have never been more challenging

With physical security systems now inextricably intertwined with the digital networks that support them, the security executive role has never been more challenging. A hacked network can provide entry into security systems, shutting down mission-critical operations that keep people and property safe. Conversely, a hacked security system can provide access into a network, leading to catastrophic data breaches. Physical and cybersecurity threats have converged to become a two-headed monster that must be battled with constant vigilance.

When it comes to delivering security KPIs, physical security technologies are only as robust as the infrastructure that supports them. The latest generation of security solutions places unprecedented demands on network performance. Industrial security strategies must be comprehensive. Strategies should include careful consideration of how reliable, redundant connectivity can extend to mobile and autonomous assets. Further, accommodating the torrents of data common to today's systems, making the data impervious to hacking and environmental interference, and still remaining affordable to install and maintain must be considered. This whitepaper will examine why wireless mesh holds the key.

The Evolving Nature of Industrial Security

Risks have never been greater or more diverse

The last decade has been pivotal for industrial security, as AI, robotics, and the IIOT have dramatically altered the technology tools available to CSO and CISOs. Smarter, integrated, and continuously connected systems empower security teams to keep much tighter tabs on the physical state of their properties and the safety of on-site workers and visitors. Collectively, they've enabled a more proactive approach to identify security threats and mitigate their associated risks.

Analytics built into cameras, access control readers, geo-fencing, and other sensor devices can flag anomalous events and issue alerts. Mobile video from body cams, drones, vehicles, and even cell phones, can be viewed, managed, and recorded as part of site-wide video surveillance platforms. Remote, automated monitoring of machine health can minimize system failures and down-time while enhancing worker safety. These are just a few of the many ways that industrial security has evolved.

Security robots are also suddenly receiving a lot of attention from the industrial security sector. Months spent on Zoom and Facetime in 2020 have made security executives more receptive to deploying robots for remote security monitoring, health monitoring, and concierge services. At the same time, corporate management recognizes how robots can reduce workplace density and the spread of disease.

The efficacy of these next-generation solutions is only as strong as the networks that support them. The bar is high for what they must deliver.

- These networks must be highly secure from cyber-hacks and breaches.
- They must offer the highest level of reliability and redundancy, speed, and bandwidth.
- They must be flexible and scalable as organizations' security needs shift and grow.
- They must support today's mobile security solutions without dropping signals or permitting dead zones.
- Out-of-pocket costs for purchase, as well as indirect and recurring operating costs, must fit within corporate budgets.

Wireless mesh delivers well against each of these metrics. But before we take a deeper dive, let's look at how the technology works.

The Basics of Wireless Mesh

A communications network of radio nodes in a mesh topology

Wireless mesh is a peer-to-peer network made up of small radio transmitters, spread out across a large area, that “talk” with each other. Networks can be any size, from under ten transmitters to several hundred. Each transmitter, also called a “node,” is programmed to communicate with others nearby, automatically identifying and transmitting to those nodes that can provide the fastest and safest connection. As network conditions change, so do its connections. Data may be rerouted in response to changing signal strength, bandwidth requirements, competing network traffic, and other factors. As a result, data transmission flows reliably across the network from node to node in an ever-shifting, dynamic path, with no single-point-of-failure.

Certain wireless mesh networks provide the added ability to position nodes on mobile assets accessing the network, a feature called machine-to-machine (M2M) connectivity. These node-bearing mobile assets, serving as fluid connection points themselves, further expand the strength and flexibility of an existing network, or they can form a new network where none existed before. For example, a team of security guards, each wearing a body cam and equipped with a radio transmitter, could leverage a wireless mesh network to transmit their video back to a centralized monitoring platform, while simultaneously becoming a part of that network itself. Rajant’s Kinetic Mesh® is currently unique in its support for M2M transmission.

Wireless mesh networks are relatively straight-forward to set up. Like any network, IT professionals handle initial system configuration, but once complete, the positioning of nodes and their assignment to assets is completely flexible and requires no networking expertise. Regardless of where they are placed or the devices they support, the nodes autonomously connect to form a highly secure, self-healing mesh. For CTOs and CIOs responsible for managing the network, wireless mesh combines ease-of-deployment with many other high-priority benefits that we’ll now examine.

Advantages for Industrial Security Applications

Reaping the rewards

Security: The private sector is highly vulnerable to cyberattacks. Retailers, hospitals, utilities, pharmaceuticals, banks, industrial manufacturers, universities, airlines—all are in the crosshairs. Today's CSOs and CISO worry that physical security risks to their facilities could happen via a cyber breach of their security technology—potentially with catastrophic consequences. The networks their systems traverse may serve as a gateway.

Runaway robots. Compromised cameras. Disabled doorways. These are the types of havoc a cyberattack to physical security systems could cause. The ability of hackers to access these systems is a function of how well the network is protected through encryption and authentication algorithms, along with administrators' adherence to best practices like password management. Wireless mesh is one of the most secure networking options available. There are no IP addresses assigned to individual devices; all transmission occurs at layer two. Furthermore, Rajant Kinetic Mesh features AES 256-bit security and FIP's 140-142 compliant military-grade encryption. HIPAA compliant, it is also suitable for a wide range of healthcare applications.

Reliability and Redundancy: While it wasn't always the case, today's security technology almost always resides on its own dedicated network, siloed from other business systems. The mission-critical nature of security requires a level of reliability and redundancy that cannot be compromised. If a company's email goes down for an hour, it may be expensive, but it won't cost lives. If a company's security systems go down for an hour, the consequences could be dire.

As explained earlier, the fundamental topology of wireless mesh ensures redundancy. Data is fluidly rerouted, as needed, to traverse the fastest, safest path between points A and B. However, not all wireless mesh systems perform equally in this regard. Traditional systems maintain a degree of hierarchical structure; many nodes connect to a smaller number of switches, creating a branching topology at the switch level. In these systems, data is rerouted via other nodes connected to the same switch if a node goes down. There is redundancy. However, if a switch goes down, so does everything beneath it—wiping out a chunk of the network. Rajant's Kinetic Wireless Mesh is a 100% peer-to-peer solution that eliminates any possible single-point-of-failure. Each and every node has its own routing capabilities, resulting in a network with virtually unlimited signal paths.

Flexible and Scalable: Security technology is evolving at an amazing speed. Solutions considered state-of-the-art when purchased may be ready for updates and expansion only a few years later. Industrial security stakeholders need to evaluate networking options not only in light of their current needs but also in terms of what the future may hold.

Wireless mesh networks not only offer unparalleled flexibility in terms of how and where they may be deployed, but are also easy to adjust and expand as needed. Nodes can be repeatedly reassigned to different devices or assets and, as long as network configurations remain constant, no additional programming is required.

New nodes can also be added with minimal effort. As they come online, they are automatically detected by their peers and seamlessly become part of the network's fabric.

In terms of scalability, Rajant's Kinetic Mesh has successfully supported networks with as many as 800 nodes with no performance degradation. Each additional node fortifies the network's connectivity because of its peer-to-peer topology, making it incrementally stronger and more resilient.

Speed and Bandwidth: Security applications are bandwidth hogs. A single 3 MP camera can require anywhere from 3 to 6 Mb/s. Try multiplying that by several hundred and pumping it across a network!

Other solutions, including autonomous vehicles, thermal imaging, and video and data analytics, are equally taxing. Wireless mesh can handle them. The network's ability to support multiple radio frequencies, increase capacity as nodes are added, and dynamically reroute signals on the fly help eliminate bottlenecks and affect more efficient load balancing.

Mobile Connectivity: Asset tracking, robots, drones, body cams, IIOT sensors on moving machinery—all of these require mobile connectivity. Traditional Wi-Fi has devices hopping from hot spot to hot spot, with the constant threat of dropped signals. Cellular transmission is often inconsistent and, for data-intensive applications, quite costly. By contrast, wireless mesh networks, particularly those with M2M support, offer seamless, consistent coverage. There are no perpetuating licensing or data-use fees. For mobile industrial security solutions, there's no better networking infrastructure.

Lightweight, compact transceivers are easily attached to fixed and movable assets. The nodes may be housed in ruggedized enclosures for use in outdoor or hazardous environments. As the assets move, their radios automatically detect and connect with nearby nodes, only disconnecting with one when another connection has been established. Because the supported assets serve as nodes themselves, their connections extend coverage into areas where it might not otherwise exist. By providing a combination of machine-to-machine and man-to-machine connectivity, wireless mesh creates an overlay that supports full mobility for any and all assets, covering areas of any size and configuration.

Cost: For private sector security stakeholders, return-on-investment is a primary concern. How much will a system cost to purchase? To operate? To maintain? How long is its lifespan? Compared to alternatives, wireless mesh offers a lower overall cost of ownership without compromising performance.

Mesh networks involve an upfront purchase of radio transceivers—enough to support immediate security needs. Once deployed, the network can accommodate unlimited data transmission with no incremental use fees. As security systems expand, additional network nodes may be purchased and added at any time. This future-proofs the investment without the need for premature spending on network capacity that isn't yet required.

Wireless mesh also reduces the overhead required for IT support. Cyber-security is hard-baked into the system, reducing the efforts required to monitor cyber-threats. Its redundancy results in much less downtime and far fewer technical support emergencies. As long as configurations are left in place, nodes can be moved to different locations or to support different assets with minimal work.

There are so many ways to leverage wireless mesh in industrial security applications that it's difficult to pick just a few examples to represent the breadth of its potential. However, here are a few hypothetical scenarios that highlight its versatility.

College and University Campuses

When 24/7 blanket protection is paramount

Let's start with cameras, since they're so ubiquitous on today's campuses. Hundreds of cameras, equipped with radio transmitters, can be mounted atop light poles and on buildings' exteriors, forming a mesh network that blankets a campus without the need for any cabled infrastructure. Surveillance coverage can then be expanded to additional locations, including temporary sites as needed. Outdoor events, construction zones, and tented dining areas during COVID-19 are just a few examples of where this would be advantageous.

Campus security wants the ability to lock down multiple buildings with the push of one button. Rather than rewire all campus buildings, which would be a time-consuming and very costly process, many schools are now layering wireless technology on top of their existing access control systems. These supplementary locking mechanisms, installed on doors and gates, can communicate via the campuses' wireless mesh network.

For many years, higher ed has gravitated toward mobile apps to push out alerts about active shooters or other emergencies, but traditional public address systems are now making a comeback. When an entire campus must be reached immediately with consistent, critical messaging, there's no faster way than to blast it out via loudspeakers. With wireless mesh, those speakers can be easily installed campus-wide without dedicated wiring, including in the most remote areas, while those making the announcements can do so from anywhere—including on the move.

And let's not forget Wi-Fi. Students are glued to their phones. Wi-Fi access points can be part of a wireless mesh network, providing high-speed, reliable coverage across the entire campus. While students may not realize it, their use of the university's Wi-Fi delivers the school's security team with invaluable tracking data about their whereabouts, which can be imported into analytics software designed to assist with security and safety-related issues.

Commercial Ports

Integrating logistics and security at global seaports

Ninety percent of world trade is carried by the international shipping industry, making ports a prime target for theft, smuggling, espionage, and terrorism.

With people, machinery and cargo constantly on-the-go throughout these sprawling sites, ports are turning to mobile technologies that can move right along with the assets they're securing. However, industrial equipment and metal cargo containers interfere with signal transmission, making it difficult to keep mobile devices connected. When wireless mesh is used, this isn't a problem. As a signal becomes blocked, another path is already available to offer constant, seamless connectivity.

For example, swarms of drones can provide overhead surveillance, connecting with tethered drones that remain in place all the time. Their M2M connectivity extends the network's reach well out to sea. Patrol boats can also connect, leveraging the network for communication with each other and back to a security command center. Should a drone spot something suspicious, a water patrol officer can be quickly sent to investigate.

Robotic dogs patrol ports, providing low-to-ground surveillance coverage and the ability to sense chemicals or radiation. Other robotic devices can provide X-ray imagery of what's inside each container.

Gigantic robotic gantries lift and move cargo off ships and onto trucks. Not only are their movements and navigation controlled through wireless connectivity, but so are the security cameras installed on them.

Site-wide asset tracking supports logistics, but is also essential for maintaining security. Knowing where assets are at all times, where and when they were moved, and who has had access to them are all key to reducing criminal activity. Technology to handle this requires the high-bandwidth, highly mobile, highly reliable, and secure transmission that's unique to wireless mesh.

.

Utilities

Bringing intelligence to the smart grid network

There’s been a whole lot of extreme weather recently, and with that comes power outages. Not only is this an inconvenience, but it’s a threat to safety and security. We need better systems to monitor the health of our infrastructure, proactively address performance issues, and more quickly bring power back online when it goes down. Wireless mesh can help.

Sensing devices, connected via an independent wireless mesh network, can notify utilities when the power goes down so that customers no longer have to call in to report an outage. They can also automatically identify rerouting options without inspection by human technicians. Drones can be quickly deployed to inspect problem sites and provide reconnaissance of the area—even in locations where down trees and powerlines make road travel treacherous.

Even when all is running as it should, our utility infrastructure requires security monitoring. Cameras placed along remote pipelines, at nuclear reactors, and near hydroelectric dams are difficult to hardwire. Electronic fencing and checkpoints to restrict access require network support. These systems must be installed in locations where no infrastructure exists. By utilizing wireless mesh, the installed technologies create their own network. And, they feature military-grade encryption, which is vitally important for utility installations. The Department of Homeland Security considers cyber-attacks on our nation’s infrastructure as one of the gravest threats we face.

Summary

Wireless mesh is a flexible, scalable, and affordable option

The advancement of physical security technology now offers industrial security teams an array of technology tools to monitor, mitigate, and manage security with efficiency and effectiveness never before possible. The integration of robotics, autonomous systems, enhanced analytics, and IIOT devices into physical security operations enhances situational awareness, the ability to identify threats proactively, and, when necessary, quickly respond to them. This new paradigm calls for a heightened focus on digital infrastructure; the underlying network is part-and-parcel with its security systems' efficacity. For the many ways industrial security is being called on to deliver, in both the realms of physical and cyber-safety, wireless mesh offers stakeholders a flexible, scalable, and affordable option that outperforms alternative networking solutions on every front.

***Mr. Brian Higgins**, CPP, CSSP, is President of Group 77, an independent security consulting company offering clients a holistic approach to security plan development and training. Previously, he served as Chief of Police and Director of Public Safety for Bergen County, New Jersey. Higgins is an adjunct faculty member at John Jay College, where he teaches courses on emergency planning, emergency management, retail and commercial security, and homeland security.*

RAJANT

*If it's **moving**, it's Rajant.*
*Industrial Wireless Networks **Unleashed.***

20+ Years OF GAME-CHANGING WIRELESS

Tel: 484.595.0233 | www.rajant.com

Discover firsthand how Rajant's private wireless network can support your security applications with mission-critical data redundancy and delivery reliability. Visit www.rajant.com or contact a representative to get started today.