

AIRAYA WirelessGRID™

**Proven, Predictable and Scalable Wireless Video Distribution
For the Physical Security Market**



Table of Contents

- The Physical Security Market..... 2
- Wireless Video Opportunities within the Physical Security Market..... 2
- Attributes of a Modern Video Security Network 3
 - Throughput and Scalability 3
 - Network Performance 4
 - Security 4
 - Configuration and Management..... 4
 - Investment Protection 4
- Selecting the Right Wireless Infrastructure 5
 - Overview 5
 - Comparison of WirelessGRID, Mesh, Wi-Fi and EVDO Wireless Technologies 6
 - Comparison - Continued..... 7
 - AIRAYA WirelessGRID™ – Designed for Modern Video Security Networks 7
- Conclusions 8

Proven, Predictable and Scalable Wireless Video Distribution for the Physical Security Market

The Physical Security Market

A transformation is underway in the physical security market. The demands of asset protection, the command and control capabilities of information technology (IT) networks, and the processes of crisis management are merging to redefine how organizations effectively communicate and respond to threats. In order to assess an organization's physical security situation, it is important to leverage advancements in technology and identify a proven infrastructure solution that is efficient, reliable, and that scales with the organization's growth.

Advancements in video technology, control and management, and storage protect an organization from today's increasingly sophisticated threats. Video technologies have undergone this same convergence of the physical security and IT layers. While the majority of installed video systems are based on legacy analog technology, network video cameras have taken the lead since their first introduction over ten years ago. A network camera captures and transmits live images directly over an IP network, enabling authorized users to locally or remotely view, store, and manage video over standard IP-based network infrastructure. With the push to digital networks, investments in legacy analog systems are not lost. Digital video encoders digitize the analog signal, compress, and send the video to the network. Once the video is on the network, it is identical to a video stream coming from a network camera.

Recording and storage technologies have undergone a similar change. Instead of rooms full of archived tape, modern physical security network operators control digital video recorders connected to data storage arrays. These enhancements enable high-speed search, retrieval, and event correlation across multiple sources.

The key elements for assembling a modern physical security network combine reliable IP network infrastructure, network cameras, digital video record and capture software, analytics software, and storage while protecting the investment in the legacy analog video system.

Wireless Video Opportunities within the Physical Security Market

The U.S. Department of Homeland Security has identified hundreds of thousands of assets critical to the nation's economy needing to be secured (see sidebar, "Critical Infrastructure and Assets"). The global opportunity is even greater. Facilities and personnel that need protection include public safety, homeland security, and enterprises.

Public safety entities provide security for the community and regional services. Transportation systems need to protect bus and taxi passengers as well as personnel and equipment. As more and more railroads, highways and public transit are identified as potential targets for those wishing to do us harm,

Critical Infrastructure and Assets

Critical Infrastructure and Assets	
Agriculture and Food	87,000 food-processing plants
Water	1,800 federal reservoirs
	1,600 municipal waste water facilities
Public Health	5,800 registered hospitals
Emergency Services	87,000 U.S. localities
Defense Industrial Base	250,000 firms in 215 distinct industries
Telecommunications	2 billion miles of cable
Energy	
Electricity	2,800 power plants
Oil and Natural Gas	300,000 producing sites
Transportation	
Aviation	5,000 public airports
Passenger Rail	120,000 miles of major highways and railroads
Highways, Trucking	590,000 highway and Busing bridges
Pipelines	2 million miles of pipelines
Maritime	300 inland/coastal ports
Mass Transit	500 major urban public transit operators
Banking and Finance	26,600 FDIC insured institutions
Chemical Industry and Hazardous Materials	66,000 chemical plants
Postal and Shipping	137 million delivery sites
Key Assets	
National Monuments	5,800 historic buildings and Icons
Nuclear Power Plants	104 commercial nuclear power plants
Dams	80,000 dams
Government Facilities	3,000 government owned/operated facilities
Commercial Assets	460 skyscrapers
Source: US Department of Homeland Security. *Approximate figures.	



it becomes increasingly important to ensure the safety of all transport users and the infrastructure they rely on. Transportation managers require remote visibility to identify causes of roadway delays and send the appropriate response. Police agencies need video evidence collection. Educational campuses desire visibility into campus areas where staff cannot continuously monitor. Hospital staff can provide medical care to their patients in a safe and secure environment. Correctional facilities must ensure the safety of their personnel in real-time.

Homeland security protects a country by controlling points of entry and securing access to government facilities. Airports, seaports, utilities and national borders require constant monitoring and intelligent analytics.

Cutting-edge applications such as license plate and facial recognition require automated data collection and real-time processing with analytics. Local and central government organizations demand perimeter security for administrative buildings, legislative headquarters, and federal offices.

Enterprise security addresses the asset protection of industrial facilities, office buildings, and retail centers. Industrial facilities and office buildings require flexible, innovative, intelligent, and permanent security for critical installations. Office buildings need security from a centrally located monitoring system. Retail managers, shopping centers, and entertainment venues want assurance that their facilities and parking lots are well protected.

The complete list of assets and applications is extensive. The use of wireless infrastructure in the Video Market is increasingly selected as best practice for many of the following reasons:

- 1) Installation schedules demand the quickest infrastructure build out
- 2) The option to extend fiber or cable is not an option or inappropriate
- 3) The installation requires Portability
- 4) The cost to install cabling is prohibitive
- 5) Redundant links are required for full system fault tolerance
- 6) Project scale requires most cost effective use of technology.

It is clear that both wired and wireless networks will play an important role in protecting assets in a timely, cost-effective, and reliable manner. It is also clear that the extended operating capabilities that wireless infrastructure brings to the Physical Video Security Market ensures that the use of wireless infrastructure will play an increasingly important role in deploying today's modern physical security networks.

Attributes of a Modern Video Security Network

Organizations have a variety of requirements that define the type of infrastructure best suited for their needs. These requirements include: throughput and scalability, network performance, predictability, reliability, security, configuration and management, and investment protection.

Throughput and Scalability – Modern Video Security Networks must have low latency, high data-rate capacity for current megapixel, PTZ and fixed cameras as well as aggregate system capacity to handle the demands of large-scale camera networks. Large data pipes are used to handle the bandwidth-intensive video streams and can be aggregated to provide redundancy and additional capacity where needed. The ability to handle multiple cameras over one wireless link, as well as multiple cameras through a Base Station are



important attributes of a high quality wireless network. In addition the wireless network should have minimal signal latency, which results in better reliability and higher video quality.

Network Performance – By design, Modern Video Security Networks should be predictable and reliable. This means these networks should be architected by professionals to ensure video streams, control data, and alarms are sent over a proven and reliable network with predictable results.



1) Unicast and multicast video streams should be supported. Unicast is communication between a single sender and a single receiver over the network. A new connection is established for each new camera. In contrast, multicast decreases bandwidth usage by simultaneously delivering a single video stream to multiple network recipients. In reality, Multicast video sent from cameras actually increases network traffic and latency on networks of more than 3 cameras. For this reason, Multicast filters are a requirement when using wireless transport of video traffic. Without them, video reliability is jeopardized.

2) Packet error rates should be negligible. Lost packets equal lost pixels and video frames that cannot be recovered.

3) Infrastructure growth should be expected and planned for during the design phase or as requirements change. A highly reliable, flexible and predictable architecture ensures that plans for additional cameras, storage, and management application changes result in a network infrastructure that scales with the organization.

Security - The infrastructure maintains secure connections to thwart data payload theft. Private networks are designed for public safety applications. They separate physical security systems from public networks such as WI-FI access to ensure video is available to authorized personnel only.

Configuration and Management - System operators must be able to manage multiple streams from multiple locations. Managers will route video to monitors for real-time security and to storage for retrieval and surveillance monitoring at their discretion. Applications will utilize industry standard configuration and management tools for interfacing with the network.

Investment Protection – IP-based networks incorporate the benefits of digital technology, while maintaining the previous investment in analog devices. Infrastructure components can be deployed and redeployed as network requirements change and this must happen quickly, but without excessive cost.

When building a new wired network proves too costly, time-consuming or prohibitive, a wireless network should be considered as a proven and reliable alternative. A private standards-based transport of wireless video streams provides flexible location selection and coverage without the costs of trenching or hanging cables.

When expanding a current video network to new locations, wireless networks play a very important role. When designed properly, they are generally easier to install, quicker to deploy, cost less, and extend to hard to reach areas with very good results.

However, all wireless systems are not created equal.





Selecting the Right Wireless Infrastructure

Overview

Knowing the requirements for an organization's video distribution system, different options for deployment of a wireless video distribution infrastructure can be examined. Four choices available, but not ideal for the modern physical security market include: legacy analog wireless, Wi-Fi radios, EV-DO cellular broadband and mesh networks.

Legacy Analog Wireless systems use a point-to-point wireless connection for each camera link. Locating multiple point-to-point systems at a single location is challenging because radios occupy the same frequency space and interfere with each other when co-located. Analog wireless systems do not share the benefits of the Modern Video Security Networks that operate over standards-based IP networks. IP-based Video Networks support point-to-multipoint topology (ie: A base station with multiple wireless video cameras). This IP-based architecture permits a larger pipe to be shared across multiple video cameras with minimal radio interference from surrounding systems.

Utilizing **Wi-Fi radios** or a municipal Wi-Fi network can be an attractive proposition for reducing the cost of network infrastructure, but it comes at the expense of network security, reliability, predictability and performance. In addition, multiple Wi-Fi security risks have been exposed for keeping data private. Municipal networks are typically "open" for the community to access and do not utilize security or data encryption. Network performance is impacted by sharing the available data throughput capacity with other agencies or the general public. These vulnerabilities rule out the use of Wi-Fi for secure, mission critical applications.

EVDO cellular broadband is gaining popularity as a wide-area broadband technology for business, consumer and government access to IP networks and has a place in mobile video. Having said that, it is clear that the data rates achieved on today's EVDO networks fall far below the minimum requirements for real-time video surveillance applications where sustainable data rates above 2 Mbps per camera stream are required and the minimum acceptable latency is measured in milliseconds. While the service has proven itself valuable for easy access to remote IP data, early adoption of this shared open architecture has also shown that the service is not available in many areas and throughput varies greatly throughout coverage areas. In addition, reoccurring monthly usage charges make this technology expensive to use on a continual basis.

Wireless **mesh networks** promise to effectively link cameras together by allowing data to travel over multiple paths. The benefits of a mesh network fall short, however, when building a physical security network. The theory is you put enough mesh nodes up and you create a fully redundant system that is always available. In reality, the funds required to deploy a mesh network are estimated at \$100,000 per square mile, and even if you could afford it, you'd have just increased system latency and reduced the predictability of your video network by adding multiple paths to and from your video sources. When you look at the numbers, you'll quickly conclude that if each "hop" adds latency, then the more mesh hops video frames go through, the less the odds are you will receive video frames in a predictable and timely fashion. Every mesh node that is crossed between the camera source and the network management system increases latency, keeping time-sensitive video from reaching its intended destination within acceptable parameters. Also, low data rates of 1 to 6 Mbps are typical as mesh networks are scaled, coupled with high packet error rates that make video frames unusable, highlight the fact that mesh networks are not well suited for video transmission. Mesh manufacturers recognize these shortcomings and recommend installation of additional 'intermediate' mesh nodes intended to reduce the number of wireless hops, which further increases infrastructure cost and system latency. **Ultimately, companies recommend disabling Layer 3 mesh all together, removing any potential benefit that could arise from this architecture.**

Comparison of WirelessGRID, Mesh, Wi-Fi and EVDO Wireless Technologies

Comparison of Wireless Video Technologies					
Technical Highlights	WirelessGRID	Mesh	Wi-Fi	EVDO	Summary and Comments
Proven Wireless Video Solution	Yes	No	No	No	<p>WirelessGRID equipment is deployed and running reliably in wireless video networks with more than 100 wireless video cameras</p> <p>Mesh equipment manufacturers typically require that video installations run without Mesh enabled or minimally configured.</p> <p>Wi-Fi equipment is deployed in small scale installations for non-critical applications.</p> <p>EVDO systems have been tested and are being deployed for low resolution, wide-area in-car mobile video.</p>
Predictable Performance	Yes	No	No	No	<p>The WirelessGRID Layer-2 architecture allows design of a reliable, predictable Wireless Video Camera System supporting analog cameras + encoders and network video cameras.</p> <p>Mesh Networks, while providing multiple paths through a network, are NOT predictable. Due to the many routing paths available on a fully deployed (and very expensive) mesh network, video packets can and do arrive at different times, which increases latency and decreases video quality.</p> <p>Wi-Fi networks are typically shared public access networks and predictability is not attainable. Available bandwidth depends on uncontrollable factors such as other users, deployed infrastructure, and coverage area.</p> <p>EVDO systems share bandwidth between all system users, both private and public. Bandwidth is limited in all cases.</p>
Reliable High-Speed Video Transmission	Yes	No	No	No	<p>WirelessGRID Layer-2 protocol provides a very low latency, high availability transport for Video. Tuning parameters for Multicast and Lost Video Frames ensure stable and reliable wireless network operation.</p>
Secure Multi-Layer Transmission	Yes	Yes	No	No	<p>WirelessGRID SecureRF™ Security Architecture</p> <ol style="list-style-type: none"> 1. Unique RF Mask (4.9 GHz band) 2. Proprietary Bridge Protocol 3. Mutual Bridge Authentication 4. 128-bit AES Encryption 5. Integrated VLAN Support <p>Note Some Mesh manufacturers use an open architecture protocol with a mesh "driver" that reduces their security by making them susceptible to hacking attacks common in standard 802.11abg products.</p>
Cost-Effective and Affordable	Yes	No	Yes	No	<p>WirelessGRID Network Bridges are only deployed where Video Cameras require a reliable network connection.</p> <p>Mesh Networks require extensive Access Point deployments to allow multiple paths through network. (Typical Cost: \$100k-\$200k per square mile).</p> <p>2.4 GHz Wi-Fi hotspots have been installed at many sites. New Wi-Fi networks have many low cost hardware options available.</p> <p>EVDO networks require contracts per user per month and infrastructure is still being rolled out in many areas.</p>
Private or Public (Open) Network Architecture	Private	Private	Open	Open	<p>Private networks use proprietary protocols to ensure systems are considered more secure against attacks typically used by hackers operating wireless sniffing programs and spoofing tools. They are designed for access by authorized system personnel only.</p> <p>Note Some Mesh manufacturers use an open architecture protocol with a mesh "driver" that reduces their security by making them susceptible to hacking attacks common in standard 802.11abg products.</p> <p>Open networks are not secure and should not be used for video networks. They are designed for easy access by anyone in public spaces and operate with very limited security using known protocols such as 802.11b, 802.11g, and 802.11a. Many hacking tools are available to monitor and obtain data from these systems.</p>
Version for Mobile/Fixed Convergence	Yes	Yes	Yes	Yes	<p>All four technologies provide some level of mobile capability. EVDO, in particular, is designed as a mobile technology. EVDO could potentially be used for fixed video, but does not support the high data requirements of most video applications.</p>

Comparison - Continued

Comparison of Wireless Video Technologies					
Technical Highlights	WirelessGRID	Mesh	Wi-Fi	EVDO	Summary and Comments
Usable TCP/IP Bandwidth per Base Station or Access Point	Up to 100 Mbps (Measurable Net TCP/IP Throughput)	Up to 32 Mbps	Up to 32 Mbps	Up to 800k	Each WirelessGRID SuperBASE contains 4 WirelessGRID Radios and is capable of 100 Mbps Net Throughput and supports up to 496 Wireless Clients. Multiple Base Stations can be collocated at one tower to add additional WirelessGRID network capacity as video system requirements grow. Each of the other technologies uses a shared architecture yielding much lower shared and available aggregate throughput.
Optimized for Video Multicast Traffic	Yes	No	No	No	All WirelessGRID Radios support Multicast filtering, which significantly reduces radio traffic and latency. Systems of three or more network cameras benefit greatly from this unique WirelessGRID feature.
Tunable Video Frame Retry Parameters	Yes	No	No	No	All WirelessGRID Radios have tuning settings for video frame retransmission, which significantly reduces radio network traffic, improves network performance and reduces latency. With current IP Network designs, lost video frames and loss of connection to remote video cameras requires a large number of retries on all Wireless networks.
Video/Enclosure Remote Power Subsystem	Yes	No	No	No	WirelessGRID Radios may be ordered with an optional 5 Volt, 12 Volt, or 48 Volt Power Subsystem supporting camera and enclosure power requirements up to 70 Watts. Reliable Camera Power Subsystems are not available from any other Mesh, Wi-Fi, or EVDO manufacturer.
5, 10, 20, 40 MHz-wide channels	Yes	Some	Some	No	Maximum number of channel widths allows precise network design. Spectrum is optimized at each location and avoids interference from known interferers. Some Mesh vendors support this functionality. Wi-Fi and EVDO systems share channels with public and private users at same time.
Embedded 128-bit AES Encryption	Yes	Some	No	No	WirelessGRID radios use hardware-based 128-bit AES encryption. WirelessGRID Radios run at full-speed with AES encryption enabled. Mesh and Wi-Fi systems typically use RADIUS server-based authentication and encryption solutions, which add latency and decreases throughput, or disable these functions for open network access with no security. EVDO systems have weak encryption unless additional cryptographic systems are added to system.
Certified for Public Safety, ISM Bands in Single or Four Radio Designs	Yes	Some	No	No	WirelessGRID Radios have been certified in every significant regulatory domain worldwide. Each WirelessGRID Radio has a modular certification and is usable in licensed public safety bands between 4.90-4.99 GHz, 5.25-5.35 GHz ISM band, the 5.47-5.72 GHz ETSI band, and the 5.72-5.85 GHz ISM band.

AIRAYA WirelessGRID™ – Designed for Modern Video Security Networks

Proven in private government, public safety, and enterprise networks around the world, AIRAYA's WirelessGRID™ networks are used by many agencies and enterprises to help monitor and respond to potential and real threats. AIRAYA WirelessGRID™ radios are secure, scalable, reliable, and predictable in wireless video distribution systems.

Each WirelessGRID™ radio is capable of operating at TCP/IP speeds up to 42 Mbps. SuperBASE base stations combine either three (3) or four (4) WirelessGRID radios in a single 10x8x6 outdoor IP67 rated enclosure providing more than 100 Mbps of aggregate multipoint capacity where and when you need it for wireless video security networks. The WirelessGRID system grows with your organization, scaling from tens to hundreds or thousands of simultaneous camera feeds. By adhering to networking industry standards for modern video security networks, new video capabilities, additional cameras, and extra storage capacity are easily added.

All WirelessGRID™ radios have tunable parameters for frequency range, channel size, transmit power, and user definable packet handling filters for multicast video, and packet retransmission. These parameters, coupled with our exclusive layer 2 bridging protocol provide an enhanced video operating environment with higher network performance and predictability.

Our SecureRF™ architecture provides multiple layers of security including unique radio masks for public safety bands, an exclusive bridging protocol, mutual radio authentication and AES data encryption to protect sensitive video content from unauthorized viewing.

Configuration and management of WirelessGRID™ radios can be done using the integrated Web and Telnet utilities. Monitoring can be done using Web, Telnet, or SNMP.

WirelessGRID™ networks continue to be deployed with leading analog camera/encoder combinations from leading security camera companies such as Pelco and Bosch. With the integration of these legacy analog cameras into digital IP networks, additional technologies can be added to further enhance the capabilities of these systems. Examples include IP-based access control systems, native IP cameras, and megapixel fixed cameras with high-resolution digital zoom capability.

Conclusions

Clearly, there are big changes happening in the physical security market. Modern video security networks and recent events around the world are putting new demands on both the folks that design, install and manage these networks, as well as the manufacturers that develop technologies used in these networks.

The AIRAYA WirelessGRID™ architecture has become a proven, predictable and scalable platform for designing and deploying reliable modern video security networks. Our experience in this category allows us to offer expert review and advice in wireless video network planning design, and architecture.

If you would like to discuss a project with someone on our staff, you can call or email AIRAYA using the contact information provided below. Your questions will be answered by an industry expert every time.

To learn more about how your organization can benefit from the many advantages of AIRAYA's WirelessGRID™ modern video security network architecture, Please visit AIRAYA on the web at <http://www.airaya.com>



About AIRAYA

AIRAYA was formed in November, 2001 by a team of wireless industry veterans with more than twenty years of combined experience in the field. The company's mission is to provide proven, reliable, fast and affordable wireless bridges for the broadband wireless marketplace. Our portfolio includes a complete line of high-performance indoor and outdoor wireless bridges, cameras, and TDM voice products and accessories for connecting IP network equipment at distances up to 30 miles.

AIRAYA

Information: info@airaya.com
Support: support@airaya.com

Corporate Headquarters
18449 Technology Drive
Morgan Hill, CA 95037 USA
Toll-free: 866.224.7292
International: 408.776.2846
Fax: 408.776.3339