WHITE PAPER

How to Build Reliable, Responsive, Low-Cost Mobile WiFi Networks for the Industrial Internet of Things

Jeffrey Ke
Moxa Product Manager

MOXA®

WiFi? Why not!?

Despite its image as a consumer-level technology, WiFi is actually an ideal basis for an effective, low-cost mobile data network with wide area coverage. When used correctly, WiFi is a perfect fit for many applications that need highly mobile network access, including automated warehousing and public transportation. Compared to competing technologies, such as cellular, Bluetooth, Zigbee, and proprietary radio networks, WiFi offers numerous advantages, including:

- Lower implementation costs
- Close-to-zero operating cost
- High bandwidth
- Usable range
- Proven security
- Great future upgrade and expansion potential
- Very wide support from manufacturers

WiFi is also the best-understood wireless technology amongst engineering personnel and service staff—ensuring effective, lower-cost technical support.

However, WiFi's origins as a consumer-oriented technology mean that wireless device manufacturers need to enhance some WiFi features to better handle industrial applications. These include:

- **Reducing access point handover delays** to provide seamless roaming,
- **Hardening WiFi devices** to avoid severe damage from natural and manmade sources such as lightning, static electricity (ESD), and power surges.

This white paper discusses how to best address these critical issues, as well as other important considerations that will help users realize the unique advantages of WiFi in a network with high mobility requirements—and as a key enabling technology for the Industrial Internet of Things (IIoT).

Released on September 4, 2015

Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa delivers lasting business value by empowering industry with reliable networks and sincere service for automation systems. Information about Moxa's solutions is available at www.moxa.com. You may also contact Moxa by email at info@moxa.com.

How to contact Moxa
Tel: 1-714-528-6777
Fax: 1-714-528-6778

MOXA®
Reliable Networks ▲ Sincere Service

Overview

Fifty years ago, fully automated warehouses and robotic factories were only seen in movies. But with the progress in robotic and wireless technologies in the past five years, they have become a reality. Mobile wireless technologies also open the door to numerous other attractive applications, such as vehicular tracking for public transport and freight networks. In fact, for many years, some degree of mobile wireless data communication has been possible in those applications. The cellphone network can provide the basic network infrastructure for data coverage. But, regrettably, due to limitations of latency, bandwidth and cost, most industrial applications have been unable to fully take advantage of practical, reliable and affordable real time mobile control and communication. In fact, in addition to these issues, cellular-based data may add unnecessary expense to many applications, if they only actually require wireless coverage over some parts of a relatively small, predefined area, such as a stock yard, vehicle depot, warehouse, bus route or metro line.

Today, with continuing improvements in WiFi/802.11 technology, including higher bandwidth protocols, IP-based networking and faster roaming between access points, users are finally able to use WiFi to construct a reliable mobile wireless communication system that takes advantage of all the latest innovations to deliver substantial cost savings, easier set up and maintenance, and greater operational efficiency.

However, outdoor and industrial WiFi applications do have some special demands when it comes to protecting radios and other electronics from manmade hazards, such as electrically-noisy or unstable power sources and intense radio frequency interference; and natural dangers, including lightning, and static electricity—not to mention environmental issues such as extreme temperatures, vibration, dust, and humidity.

Electrical issues can be especially challenging and costly because they cause intermittent, hard-to-diagnose failures in random components—this may lead to repeated maintenance downtime and unnecessary replacement of affected equipment, if the root cause of the electrical disturbance remains undiscovered.

This whitepaper explains some typical applications and highlights the key factors to consider when designing a reliable mobile wireless communication network.

Mobile WiFi enables the IIoT

Although the “Internet of Things” concept has been around for some years, global deployment of IoT networks has increased rapidly during the 12 months, and the concept is spreading to industry with the Industrial Internet of Things (IIoT). The IoT centralizes data through wireless technology and uses machine learning and big data analysis to turn that data into valuable information. Bringing this concept to legacy industrial applications can reduce costs, increase productivity, and maximize uptime.

The IIoT often requires many devices to use WiFi simultaneously. The technologies and concepts in this white paper are key IIoT enablers, because they make it much easier for multiple, mobile devices to share WiFi without problems, thanks to new technologies like Turbo Roaming, and good practices like careful network design and avoidance of hidden nodes.

Business Benefits

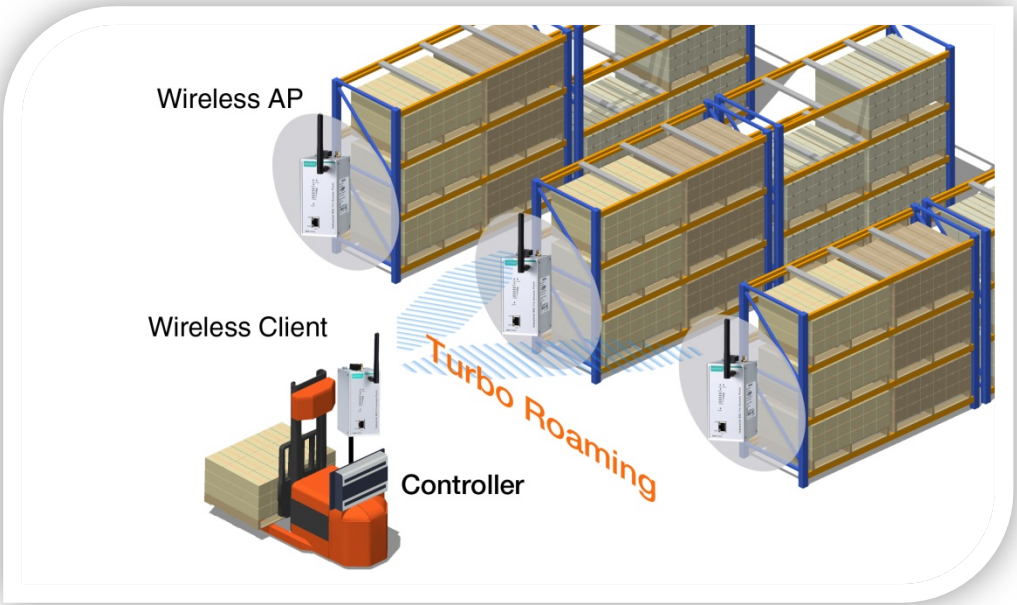
For mobile data communications, WiFi and cellular (mobile 3G/4G, etc.) are the two most commonly-used technologies. For very wide-area coverage, such as freight vehicle tracking, cellular tends to be the best choice. But for local area mobile communication, such as smart warehouses, or for fixed-route vehicles such as bus to depot/stop communication, WiFi is usually a better choice.

WiFi is, obviously, a Wireless Local Area Network technology; Unlike cellular, WiFi does not have monthly charges or data caps and there are no complications involving cellular service providers, billing, cell tower outages, and so on. Compared to Bluetooth and Zigbee, WiFi technology provides higher bandwidth and a relatively longer range—and it also has a proven history of backwards-compatible upgrades—so WiFi provides much greater headroom for future system enhancement and expansion. Unlike proprietary wireless data systems, WiFi is a standard protocol—based on the IEEE 802.11 specification—that is supported by hardware from many different vendors. So WiFi-based systems avoid the risk of vendor lock-in and ensure a longer design life than proprietary radio technologies.

As we have discussed above, WiFi is currently the most suitable technology for local area mobile communication in many cases, because it offers a unique set of advantages. We can summarize WiFi's main benefits as follows:

1. Lower operational and maintenance cost
2. Future-proof technology with higher bandwidth available for future expansion.
3. Very wide technology support from numerous vendors and hence longer system design lifetime.

Commonly-seen WiFi Mobility Applications and Their Challenges



Material Handling and Automatic Warehousing System

In a traditional warehouse, staff spend most of their time walking between shelves to store and retrieve items. As the scale of the warehouses increases, there is also an increase in the proportion of their time that staff must use moving from location to location, and an increase in costly human error due to misplaced items and other causes. Various types of AGV (Automated Guided Vehicle) and AS/RS (Automated Storage and Retrieval Systems) have been introduced, using automation to resolve these problems.

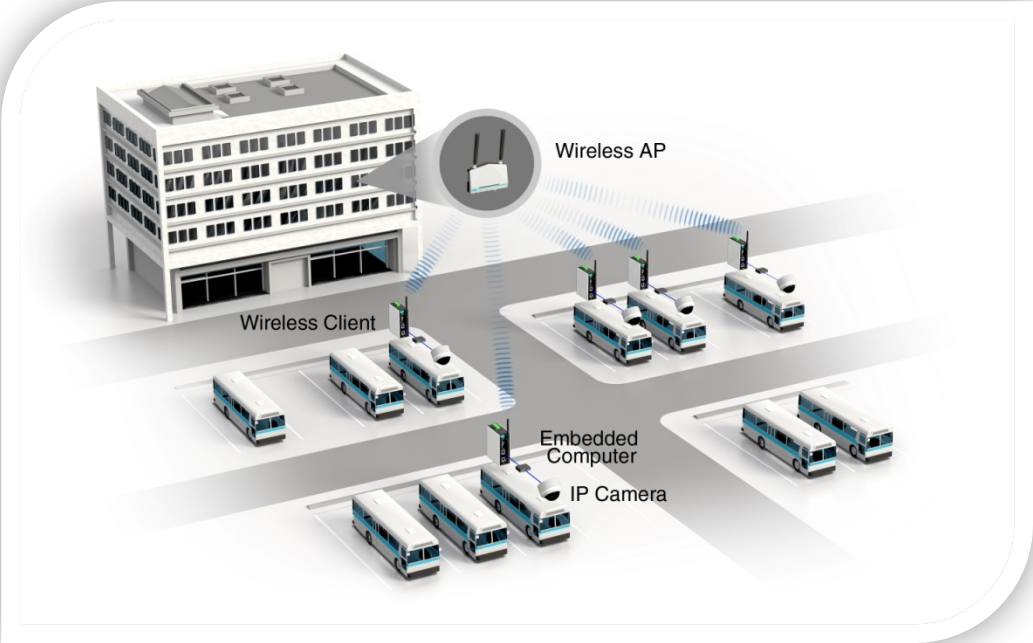
One useful example is the automated warehouse system introduced by Kiva (now known as Amazon Robotics) and Amazon in 2011. These robots move the shelves horizontally to help staff to store and retrieve products more quickly and accurately. Even though this system does not utilize vertical space as well as other AS/RS systems, it can be deployed faster and provides better scalability for medium and small warehouses. A key factor required to make AGV, AS/RS or robotic systems successful is selecting the most suitable wireless technology and implementing it correctly. In our experience, we have seen several common wireless problems in warehouse applications:

Challenge #1: Roaming reliability—WiFi has limited signal coverage, so multiple access points are necessary for full coverage throughout an entire warehouse. It is critical to ensure that the clients can roam smoothly between these access points with minimal handover time.

Challenge #2: Power supply quality—Robots and other mobile devices often have very limited space and weight-carrying capacity for a WiFi module, and the power system usually cannot be properly grounded. So system integrators must dedicate considerable effort to ensuring onboard devices cannot be affected by the inrush current (a surge of power commonly created when electrical devices switch on or start moving) that is created by the robot's motors—otherwise there is even a risk that electronics could burn out or suffer significantly reduced lifespan.

Challenge #3: Communication blockage—Unfortunately, metal is extremely effective at blocking radio signals, and large metal objects, such as vehicles and metal shelving, are common in industrial, freight and transport environments. System integrators need wireless expertise and experience to devise the most efficient positioning of APs and antennas, in order to avoid the risk of communication blind spots caused by stationary or moving metal objects.

Challenge #4: System adaptability—There are many kinds of warehouses; some require special environments such as very high or low humidity, or sub-zero storage temperatures. System integrators need to be able build a system that is adaptable to different customer needs and many different environments. So it is important to choose hardware that can handle extreme temperature ranges and has good ingress protection to keep out dust and moisture.



Bus to Depot Communication

In developed countries, computerization of bus ticketing and bus surveillance and travel records systems is common. With a computerized ticketing system, bus companies have a secure, efficient method of handling cash flow. And with computerized traffic monitoring to record vehicle position and speed, and internal and external IP video feeds, bus companies can easily determine the responsibility for accidents and make the bus service safer. To build a complete system, it is not only the bus that has to be computerized—the operations center has to be upgraded, too. Wireless communication is ideal as a bridge between moving buses and the operations center. However, compared to common office or home WiFi applications, depot wireless communication usually presents a special set of challenges for systems integrators.

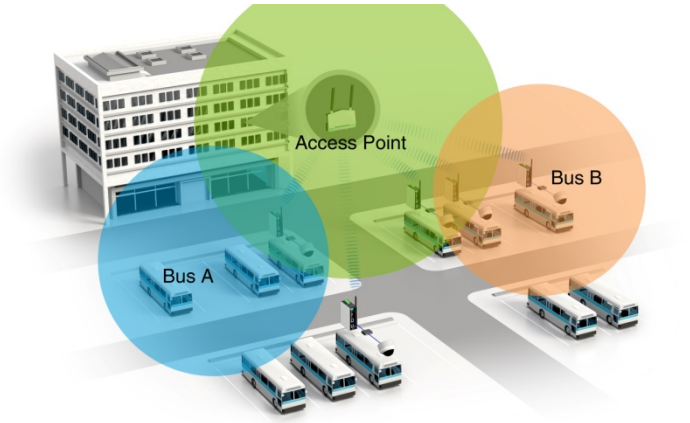
Challenge #1: Wireless network design—The most common problem we see facing systems integrators is insufficient attention to initial wireless network design. A well-designed wireless network includes channel planning to avoid channel congestion, and AP coverage planning to provide sufficient overlap between APs while minimizing the total number of APs.

Challenge #2: Installation and field protection—In order to provide good wireless coverage, some access points are usually installed outdoors. But ordinary access points are not suitable for this role, because, without proper protection, they are likely to be damaged by lightning or Electrostatic Discharge (ESD).

Challenge #3: Load balancing—Each access point's wireless bandwidth is, of course, limited. Naturally, every bus arriving at the depot will connect to the first access point it encounters—usually one close to the depot entrance. Unfortunately, without suitable technology, a common scenario is that each bus will remain connected to that same access point, even if the signal deteriorates as the bus moves further into the depot or the access point becomes overloaded with connections from new vehicles arriving at the depot. To make the best use of WiFi, systems integrators must find solutions to this problem.

Challenge #4: Hidden node problems—In our practical experience, system integrators often overlook the problem of hidden nodes, because it is difficult to guard against with traditional WiFi devices, and it may only be seen intermittently during actual operational use.

A typical hidden node scenario is shown in the picture below: Bus A and Bus B can both communicate with the same access point, but because the two buses only have low gain antennas, they are too far apart to detect each other's signals. So both buses try to communicate with the access point at the same time, and on the same frequency—and their signals interfere with each other when they reach the access point. Hence WiFi's conflict avoidance system, CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance), will fail. As a result, a high volume of packet collisions and retransmissions will overload the channel. Eventually, the access point, or even the entire wireless network, may temporarily fail under the load.



The hidden node risk can be avoided by simply enabling the RTS/CTS (request to send/clear to send) feature, but most vendors do not enable RTS/CTS by default, because it reduces the overall wireless performance.

How does the Moxa AWK-A Series Meet these Challenges?

Advanced Roaming Technology with Client-based Turbo Roaming

Old-fashioned WiFi devices commonly experience a 3 to 5 second disconnection from the network as they move between access points, causing severe disruption to real-time operations. In this scenario, a warehouse robot might simply stop until it re-establishes its network connection. Moxa's roaming technology preemptively seeks out nearby access points with strong signals and prepares to connect to them as the client moves closer to them—without a lengthy disconnection delay. But after many years cooperation with our customers, we understand seamless operation is only the most basic requirement for mobile communications. There are other requirements that are sometimes just as important for customers, for example:

- **Reliable roaming performance with multiple channels.** Due to the limited channel bandwidth, in many deployments, system integrators must use multiple frequency channels to avoid channel congestion. Moxa's Client-based Turbo Roaming is optimized to provide smooth roaming between different APs using different channels.

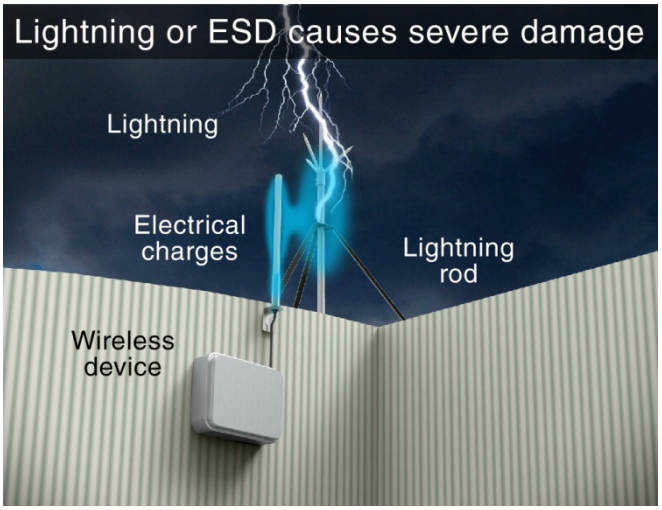
- **Adjustable roaming parameters.** System integrators usually have multiple customers with widely-varying needs, so they must provide an adaptable solution to cope with different customer requirements. As a device vendor, we also need to do the same. Moxa's Client-based Turbo Roaming allows users to adjust the roaming parameters to adapt to different venues and site environments. The roaming parameters are also commonly configured to allow location-based load balancing,

ensuring that clients are connected to the closest access point, to avoid traffic congestion.

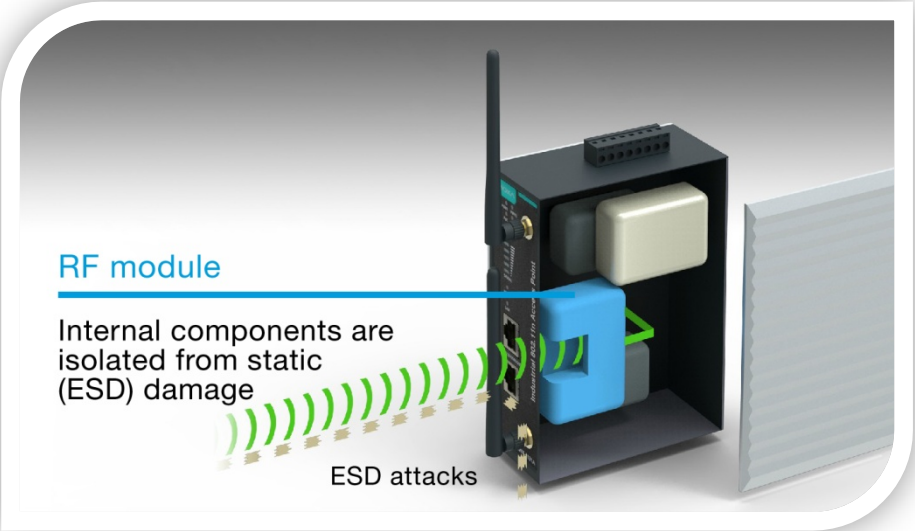
- **Reliable and seamless roaming with the strongest wireless encryption protection.** WiFi obviously signals travel through the air in the open. Without proper wireless protection, the network can easily be hacked. However the complexity of the most secure encryption protocols, such as WPA/WPA2, can sometimes affect roaming performance—particularly by causing a delay for secure key exchange when the client moves to a new access point. Moxa Client-based Turbo Roaming is optimized to ensure a delay of no more than 150ms, even with WPA/WPA2 encryption—for most applications, such a short delay has little or no effect on operations.

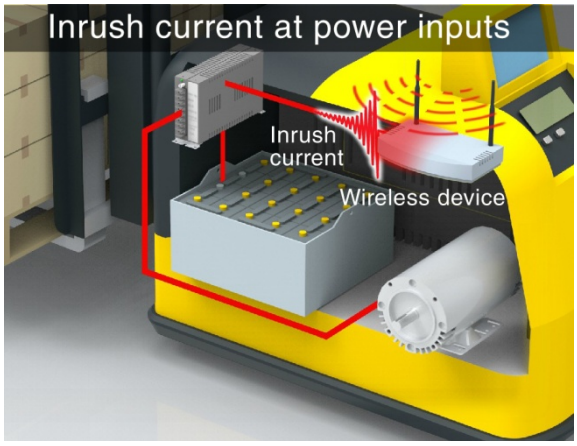
Rugged Hardware Design with Dual Isolation

Our experience tells us that it's impossible to ensure complete protection against natural and manmade electrical disturbances. All we can do is to introduce innovations to make the protection stronger. So we can at least offer a far more stable and reliable solution than an unprotected, or poorly-protected wireless device. Moxa's AWK-A series has integrated dual RF and power isolation design to ensure the best protection we can provide as an equipment vendor. Below, we discuss these two features in more detail:

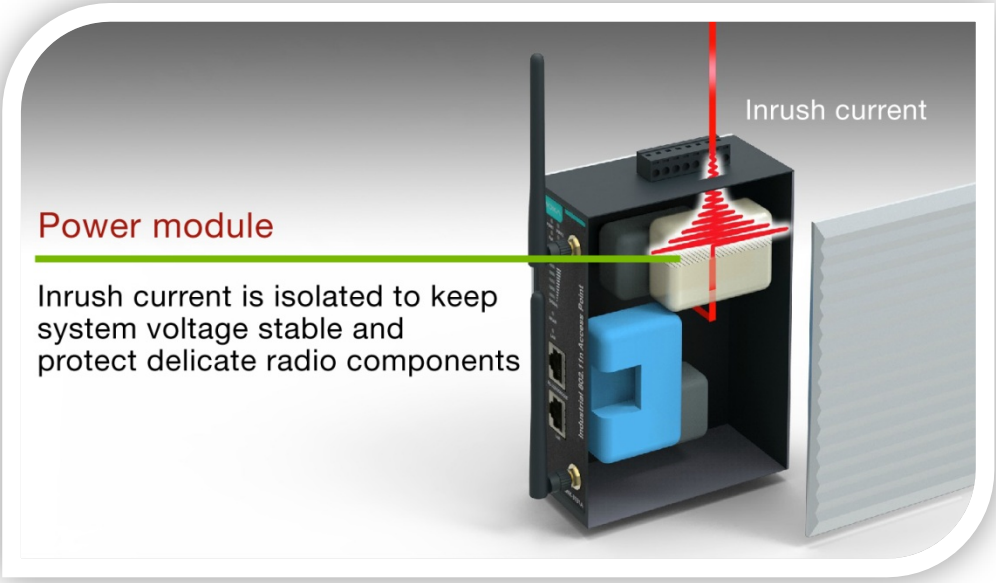


RF isolation on the antenna ports: If WiFi access points are installed outside without any lightning protection and they are struck by lightning, we just have to surrender to Mother Nature—the device is unlikely to be operational afterwards. However, sometimes even with proper protection installed, lightning-induced current or ESD could force its way through the RF cables and surge arrester, damaging the radio components inside the equipment. The Moxa AWK-A series of products have integrated RF isolators inside the device itself, enabling them to withstand a higher level of electromagnetic interference through the antenna paths than typical competing products.





Integrated power isolator for complete electrical isolation: as we mentioned in the previous section, in many mobile applications, the space available and weight allowance for integrating additional modules is limited. Often it is impossible to add an independent, well-grounded power system for the communication devices. Unfortunately, in our experience, if network devices share the same power system as the motors, the inrush current from the motors will cause system instability or sometimes, permanent hardware damage. However, with an integrated power isolator for extra protection, system integrators have one less thing to worry about and they can simplify their design accordingly, saving money and time.



DFS Channel Support

Radio data frequency bandwidth is strictly limited by regulations. Therefore, using as much of the available bandwidth as possible is the only way to maximize wireless throughput and performance. So channel planning is extremely important in the system integrator's initial design. As well as using all the normally available frequencies, Moxa AWK-A series are certified to operate on the DFS (Dynamic Frequency Selection) channels, significantly increasing the total bandwidth available. When switching to a new DFS channel, regulations do require 60 second delay to ensure the channel is clear of radar signals before transmitting, but despite this, the ability to use DFS channels greatly improves the overall bandwidth capacity of wireless networks.

Industrial-grade Production and Reliability

In order to ensure uninterrupted operation, industrial-grade equipment is usually recommended for industrial users. Features like fanless heat dissipation, sub-zero temperature operation, and metal casing for a better Electromagnetic Compatibility (EMC) rating, are usually available, making work easier for systems integrators and at the same time providing a more reliable system with a longer lifetime.

Building a Reliable Mobile WiFi System with the Moxa AWK-A Series

Moxa's AWK series devices provide all the basic building blocks of a reliable, high-performance mobile WiFi network. The AWK-1131A can be integrated into mobile clients providing all of Moxa's seamless roaming technologies, while the AWK-3131A and the AWK-4131A (available in Jan 2016) are ideal fixed access points for indoor and outdoor use respectively. All units have Moxa's Dual Isolation technology, providing electrical isolation features suitable for their designated usage, with 500V Insulation and Level 4 ESD protection.

The AWK-4131A (available in Jan 2016) offers IP68 ingress protection—particularly suited to outdoor use where direct exposure to rain, strong winds and dust or grit is a common hazard. The other units are shielded by IP30 ingress protection.

For more information on Moxa's new AWK-A series, please visit: http://www.moxa.com/Event/IW/AWK-A/overview.htm

For more information on the AWK-1131A Industrial IEEE 802.11n wireless AP/client, please visit: http://www.moxa.com/product/AWK-1131A_Series.htm

For more information on the AWK-3131A Indoor Industrial IEEE 802.11n wireless AP/bridge/client, please visit: http://www.moxa.com/product/AWK-3131A.htm