WHITE PAPER

# Redundant Wireless Bridges: The Reliability of Wired Networks with the Cost Savings of Wireless

**Jeffrey Ke**
*Moxa Product Manager*

MOXA®

## Abstract

Wireless networks should be saving money and improving flexibility for industrial users and public transport operators, but reliability concerns have hindered adoption. Now, new technological innovations are making low-cost wireless as reliable as old-fashioned wired networks.


## Overview

Wireless networks can bring huge cost savings and efficiency gains compared to wired networks—especially for hard-to-wire industrial applications—thanks to their lower installation and maintenance costs, and their easier network scalability. However, operators are understandably concerned about the reliability of intangible wireless data links, compared to old-fashioned cables. To address these concerns, vendors offer a variety of wireless redundancy technologies, each claiming that they can handle the challenges of real-world wireless reliability. Although several of these technologies have something to offer, there are still critical applications and harsh operating environments where wireless reliability remains a problem, even with redundancy.

The challenges are tough and the stakes are high: What if a wireless radio link across a harbor channel is blocked by a huge oil tanker, just when communications are most needed? How about a high-speed train that is unable to send vital location and maintenance updates for tens of seconds because a brief power disturbance has rebooted a critical wireless node? But the rewards from a reliable wireless network, in cost savings and flexibility, are also high.

Industrial, control and automation networks are converging. We are heading towards a future in which all systems within an organization are connected on one single network. This makes machine to machine communication smarter, but it also makes network reliability more important than ever. A single point of failure can cause widespread network downtime and the loss of vital systems. So operators need more reliable wireless redundancy to avoid tremendous cost and time wastage. At the same time, wireless frequencies are becoming ever more crowded as a proliferation of consumer and industrial devices contends for limited bandwidth, increasing the risk of interference that can knock mission-critical wireless network links offline.

This paper illustrates the pros and cons of current wireless redundancy methods, shows why Moxa's AeroLink Protection technology ensures network reliability, and explains how this innovative technology is applied in mission-critical applications.

Released on June 15, 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

Reliable Networks ▲ Sincere Service

## Why Do Wireless Networks Fail?

There are two main causes of wireless network failure: radio interference, and hardware faults.

Other WiFi networks are, of course, a major source of radio interference. But non-WiFi communications devices also cause interference: Cordless telephones and Bluetooth/ZigBee devices are just a few of the many products which can severely impact the effectiveness of wireless networks, as they share similar radio frequency ranges. A wide variety of industrial machinery and equipment can also cause interference, such as motors, generators, and microwave-emitting devices. Even a poorly-wired electrical circuit can cause interference, through effects such as ground loops. Another hazard with similar effects to radio interference is physical obstruction of the radio signal's direct path by any large metallic object, such as a truck, train, ship, or mobile machinery. Metal objects are also particularly likely to cause multipath interference, creating unpredictable wireless "dead zones".

Hardware faults include issues like power irregularities, cable disconnection, hardware failure, software crashes, etc. Buildup of static electricity, followed by electrostatic discharge, which is commonly caused by staff and equipment activity, can damage hardware, as well as causing radio frequency interference.

Even brief radio link interruptions or transient hardware faults can severely reduce throughput, or disable an entire network, by forcing devices to frequently restart or renegotiate a data link.

## How Can Redundant Wireless Communications Help You?

So, as we have seen, in the real world, there are many factors that can disrupt wireless communications and make critical networks unreliable. These unavoidable challenges appear to make wireless a much less attractive option for backbone communication. So instead of using an easy-to-deploy, low-cost wireless communication system, integrators are forced to use time-consuming and expensive cabled networks. But for users who understand how to set up a redundant wireless network using the latest technological innovations, wireless communication can now be at least as reliable as cabled connections, if not more reliable.

Now that we can remove the unreliability factor from the wireless equation, users can finally start to enjoy these great advantages of wireless technology:

1. Lower Implementation Cost, and Faster Deployment—avoiding the time and cost of laying hundreds or thousands of meters of traditional cables. With wireless, there's no need to dig trenches or to run conduits through crowded, busy and hazardous environments.
2. Reduced Maintenance Time and Cost—with wired communication, paying for cable maintenance and repair staff is inevitable. Cables are vulnerable to accidental cutting, snapping, or disconnection. Wireless communication narrows down the maintenance scope from long lines to small points, which can significantly reduce the maintenance time and cost.
3. Securing Intellectual Assets with Encryption—with proper security, wireless communications are well encrypted in the transmission layer. In some respects, wireless can be even more secure than wired communication. Wireless encourages watertight security throughout the network, because a weak security model based on preventing physical access is not possible.

4. Maximizing System Uptime—with a redundant wireless design, there are multiple communication paths to ensure the highest system uptime, no matter whether there is a hardware failure or wireless interference.

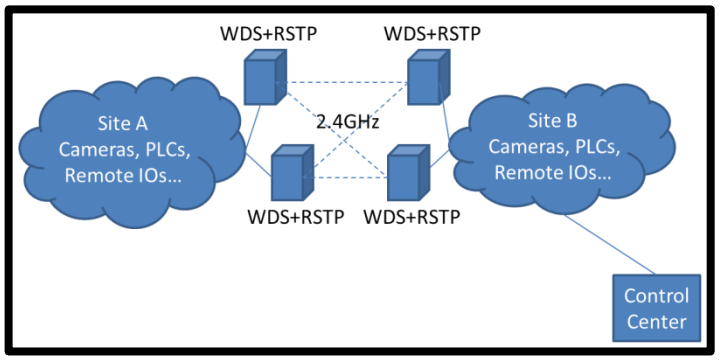
To realize all the above advantages, it is important to clearly understand the options you have for creating reliable redundant wireless communications. In the following sections, we will introduce the most common wireless redundancy methods, as well as Moxa's new AeroLink Protection technology.

## Current Wireless Redundancy Methods

There are many wireless redundancy technologies on the market today. The following paragraphs illustrate the pros and cons of three common systems.

- **WDS + RSTP**

Among the simplest common approaches to establishing a wireless bridge, or a wider wireless network, is Wireless Distribution System (WDS).



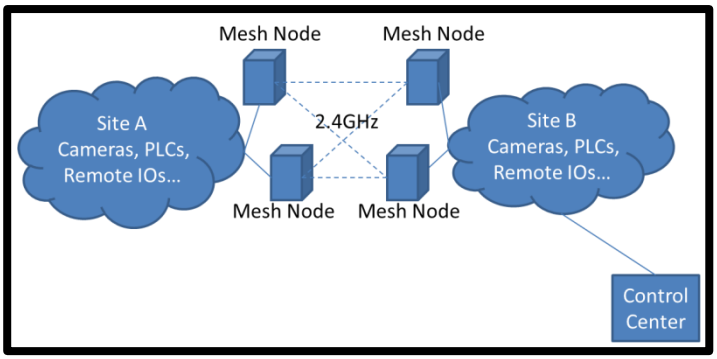

WDS allows a mesh-like wireless network to be created by manually adding each device, by its MAC address. Adding the standard Rapid Spanning Tree Protocol (RSTP) to the WDS network creates a redundant wireless mesh network, which has some ability to recover from a single point of failure that would normally bring a whole network down.

The downsides of the WDS+RSTP approach are: Poor security, because standard WDS only supports extremely weak wireless security modes. Communication across the whole WDS network can be interrupted for several seconds whenever a node goes offline or interference blocks a wireless link, because RSTP takes time to recover from interruptions. Another major issue is very inefficient bandwidth utilization, as all nodes on a WDS network share a single radio frequency channel. Furthermore, if that channel suffers continuous interference or is jammed, WDS+RSTP is not able to recover automatically, so communication is completely blocked. Finally, the user needs significant time for the initial network configuration, and for adding or removing devices later, because every WDS network node must know the MAC address of every other node—a task usually performed by manually entering them into each device's settings.

- Redundancy: Device-level redundancy only
- Recovery time: 3-6 seconds
- Advantages: Low-cost device-level redundancy
- Disadvantages: Insufficient wireless security, difficult to configure, and low throughput and vulnerability to interference due to all nodes sharing the same frequency.

- **Wireless Mesh Networking**

Wireless mesh networks are widely used. Every vendor offers their own solution, with variations in behavior and performance. This technology was designed to allow a group of wireless access points to automatically form a network, and to automatically rebuild the network structure when one of the nodes goes down. Two common wireless mesh approaches are:



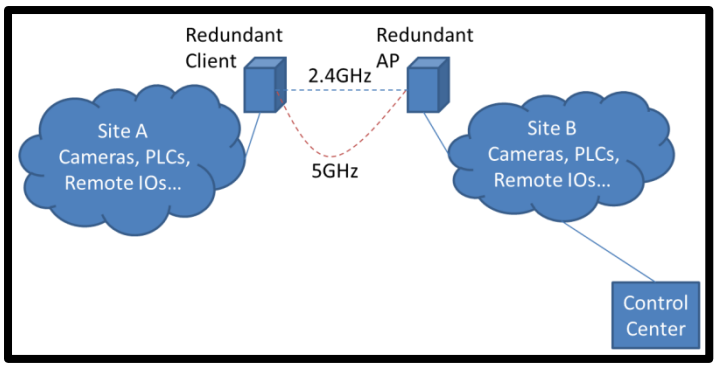

1) Proprietary mesh network: This forms a web-like, many-to-many, wireless network between wireless access points. When one node loses wireless access to the network or goes down, the others will find a route around it and transmit data via another path. This sounds good in theory—but, in practice, that re-rerouting process can be too slow for mission-critical applications or environments where there is frequent disruption of the network. This problem (the excessive network convergence time for route calculation, required to prevent loops), is usually the web-style mesh network's greatest drawback.
2) Proprietary tree-style mesh network: To avoid the web-style mesh's network convergence delays, some vendors offer a tree-style mesh network. This approach reduces the network convergence time, but the disadvantage is that it is more vulnerable to single points of failure. In the worst case, if the tree's root node goes down, the entire tree is disabled.

No matter which approach is used, one of the common problems with single-radio mesh networks is relatively poor wireless throughput because all nodes share the same frequency. This also means that a mesh network can only handle a device level failure—not a frequency level failure, such as radio frequency interference.

- Redundancy: Device-level redundancy only
- Recovery time: Vendor dependent
- Advantages: Automatic formation of network structure
- Disadvantages: Network convergence delays and poor fault tolerance, relatively low throughput because nodes share the same frequency.

- **Dual-Radio Wireless Redundancy**

Dual-band access points are the most commonly-used wireless redundancy method. They use one radio for data transmission, with the other as a backup on a different frequency. When the main link goes down, the backup link is activated. There are many different techniques for deciding when to switch



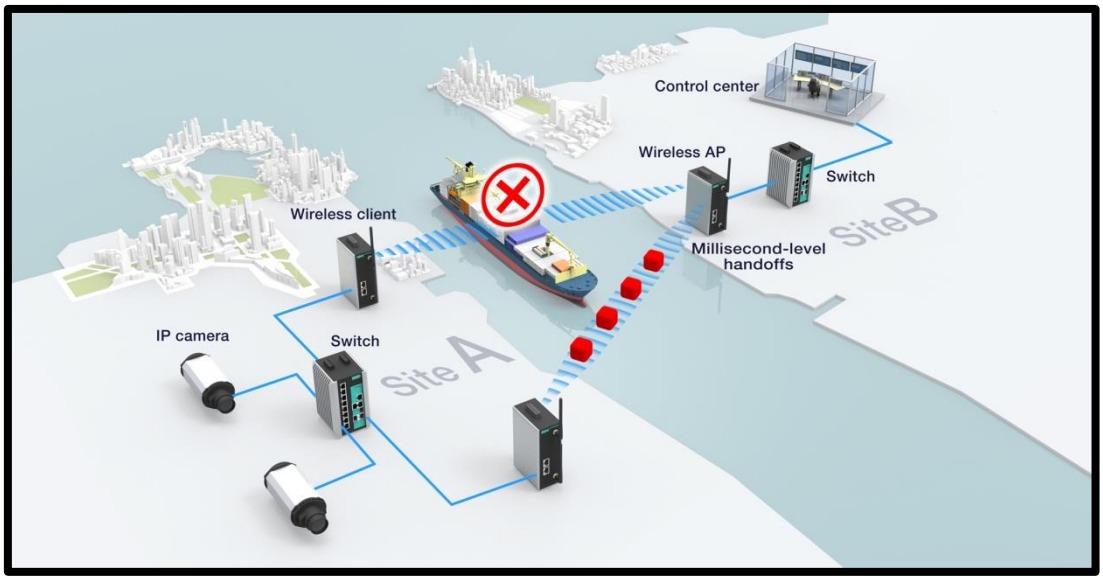
over to minimize data loss. For example, Moxa's concurrent dual-radio transmission duplicates data packets and sends both packets simultaneously via two different frequencies, to ensure that at least one packet reaches the receiver. This method almost eliminates the possibility of packet loss due to radio interference, however device failure—due to power interruption, hardware fault, or software crash—will still bring the network down.

- Redundancy: Frequency-level redundancy only
- Recovery time: 0ms
- Advantages: Easy-to-adopt redundancy with a single device.
- Disadvantages: Wireless redundancy is no help when hardware fails.

## Introduction to Wireless Redundancy with Moxa's Advanced AeroLink Protection

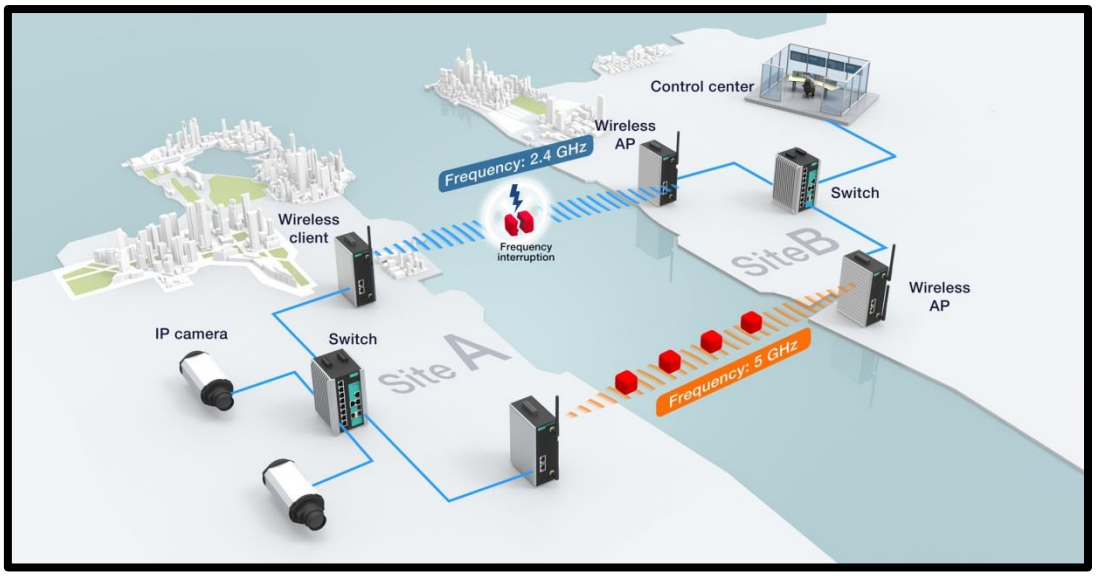
In industrial applications, such as communication between off-shore oil platforms, or train-to-ground communications, a reliable wireless bridge is essential to minimize system downtime and maximize system availability. Moxa's AeroLink Protection provides a reliable wireless bridge between two networks. As we have seen above, when you are using old-fashioned wireless bridge or WDS connections, the link is exposed to at least one of two types of risks—device failure and wireless link failure.

With AeroLink Protection, a network has two or more AeroLink Protection-enabled wireless client nodes connected to a single access point. One serves as the active node, while the others are passive, backup nodes. If the active node stops sending or receiving data for any reason, AeroLink Protection completely restores the communication link within 300ms by bringing backup nodes online. This includes the time required for network convergence and Address Resolution Protocol (ARP) update.

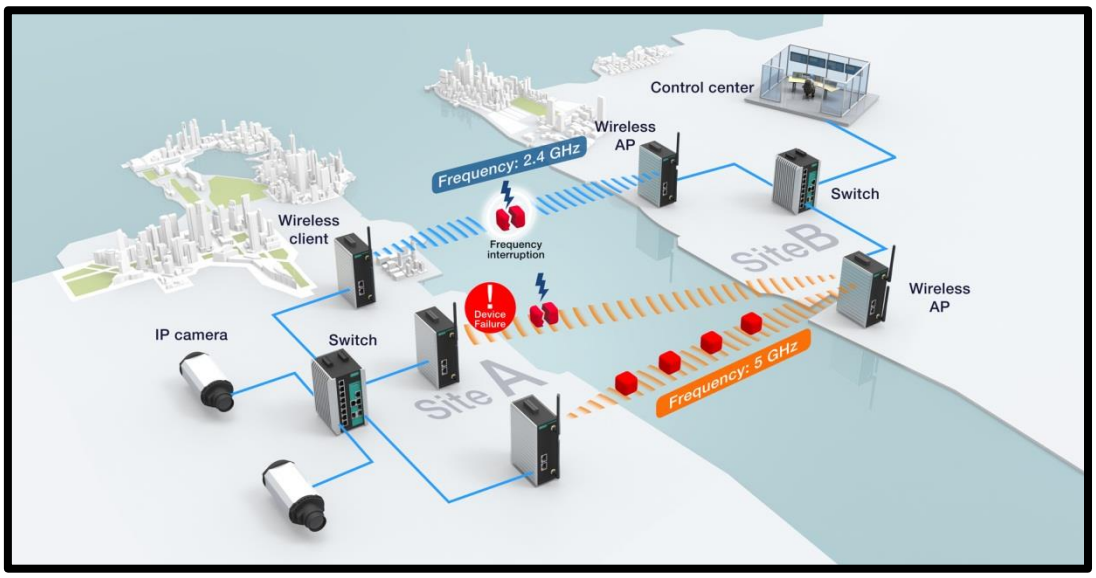



Furthermore, the passive node can be connected to a different access point on a different frequency, providing frequency-level redundancy. If there is interference on the active channel, the backup path will transmit the data via a backup device and backup frequency. The technology uses the wireless radio's standard wireless protocol to detect that the link has been

disconnected. As soon as a serious interruption is detected, Aerolink Protection takes action. The switchover to the passive node, and full network recovery, takes only 300ms.




AeroLink Protection not only guards against both device and wireless link failure, but also offers the ability to scale up your redundancy paths by adding additional hardware—providing even stronger protection for your wireless bridge network when needed. If even more robust resistance to radio frequency interference is required, three or more different backup frequencies can be used, when the 5GHz range is available.




AeroLink Protection is a client radio feature that negotiates with every other AeroLink Protection-enabled client in range to set up the active node and passive nodes. Because AeroLink Protection works at a low level, layer 2, it is effectively invisible to higher network protocol levels, so it is easy to add an AeroLink Protection bridge to an existing network: it just works. The fast recovery time and simple setup allow users to form a reliable wireless bridge that will ensure their daily operations are uninterrupted, no matter what kind of failures occur.

## How AeroLink Protection is Used in Real-World Applications

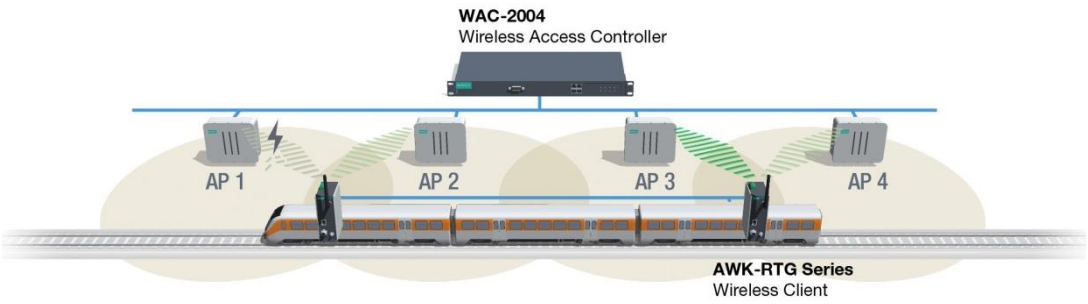
- **Heavy Industry Applications, Harbor: Scalable Network Redundancy**

Large metallic objects, including machinery, vehicles, cranes, or buildings are common on heavy industrial sites. When such equipment moves around, data transmission can be interrupted as it blocks the wireless network's communication path or causes unpredictable multipath interference.

For example, in a harbor, wireless networks that communicate across water are blocked every time a freighter passes by. These environmental challenges are inevitable, but the wireless interruption is avoidable. Moxa's AeroLink Protection is a scalable network redundancy method that ensures seamless transmission, by allowing you to deploy multiple, widely-separated backup access points. In the scenario described above, multiple wireless paths will prevent more than one path being interrupted as a freighter passes by.

- **Train-to-Ground Applications: Maintaining Constant Communication**

Train-to-ground communication usually relies on wireless networks. If wireless communication fails and can't be restored within a reasonable time, the risk is not only extra maintenance cost and time, but in the worst case: staff or passenger injury. So a reliable wireless network for train-to-ground communication is essential. In the past, to protect vital train communication systems from a single-point-of-failure, users had to double their expenditure by building a fully-redundant duplicate network (a so-called red-blue network). Even with advances in switch technologies (such as ring or chain backup mechanisms), the train-to-ground wireless link remains a bottleneck. Now, with AeroLink Protection and Moxa Turbo Roaming technologies, railway system integrators can easily create a redundant roaming system without the expense of duplicating the whole network.




- **Offshore Oil Drilling: Preventing Device Downtime and Radio Interference**

An offshore oil field is a hazardous environment where it is extremely difficult to deploy wired networks. Data transmission between drilling platforms requires a reliable wireless bridge. But even for wireless, it is a tough job: wireless devices may be subjected to punishing temperatures, moisture, corrosive materials, shocks and vibration which can easily cause device downtime. There are also many potential sources of radio frequency interference, such as high-powered communications equipment. With Moxa's AeroLink Protection, you can use two access points in master mode and two access points in slave mode to form a wireless bridge that has both a backup frequency and backup hardware, guarding against both device downtime and frequency interference.

**Technology Comparison**

| Technology | Moxa AeroLink Protection | Moxa Wireless Redundancy | WDS + RSTP | Wireless Mesh Network |
|---|---|---|---|---|
| Device-level Redundancy | ✓ | ✗ | ✓ | ✓ |
| Link-level Redundancy | ✓ | ✓ | ✗ | ✗ |
| Scalable Redundancy | ✓ | ✗ | ✓ | ✓ |
| Recovery Time (Link Break Time + Network Convergence Time) | 300ms | 0ms | 3-6 Seconds | Second-level (Vendor Dependent) |
| Total Cost of Ownership | Mid | Mid | Mid | High, some vendors require controller to facilitate convergence time |

## Enjoy Seamless Communication with AeroLink Protection

AeroLink Protection offers cast-iron redundancy by automatically handling both device failure and radio interference. Relying on industry standards for security and interoperability, it offers simple "plug and play" setup and configuration—working well with existing networks. AeroLink Protection is modular and scalable: offering anything from basic redundant wireless bridges, to increasingly robust wireless network configurations for more demanding environments.

AeroLink Protection technology is available now in the first of Moxa's new generation of A-series AeroLink Protection-enabled devices, the AWK-3131A Industrial IEEE 802.11n Wireless AP/Bridge/Client.

For more information on seamless wireless solutions for your mission-critical industrial applications, please visit http://www.moxa.com/product/AWK-3131A.htm.