ODVA

TECHNOLOGY OVERVIEW SERIES

CIP Safety:
Wireless Functional Safety

AT A GLANCE

This white paper addresses how to apply functional safety communication, like the CIP Safety distinctive network service on the EtherNet/IP network, over wireless/cableless communication networks on moving and remote equipment. The advantages for wireless networks are discussed, followed by principles for functional safety. Industrial communication networks, particularly EtherNet/IP, are reviewed in both wired and wireless contexts. The diagnostic capabilities of CIP Safety are introduced, followed by the procedures for deploying a successful wireless network using CIP Safety.

Introduction

The last 15 years have seen unprecedented growth in industrial connectivity. This has been driven by increasing demand for system performance while being supplied by consumer and IT communication technologies that brought costs down. At home and in the office, we have built up an expectation of how well wireless should perform. And that has led wireless communications to become the first-choice connection method at home and for many communications at the office. Wireless solutions are becoming more common in industrial environments and for good reason. These are some of the many places that wireless industrial communications are enabling more effective production:

- Modular and flexible plant design
- Remote process instrumentation
- Data collection on legacy equipment
- Automated guided vehicles (AGV)
- Automated mobile robotics (AMR)
- Independent cart technology (ICT)
- Automated storage and retrieval systems (ASRS)
- Predictive analytics for moving machinery
- Reducing cabling for hygienic design

With each new advance in technology, wireless communications achieve better performance, so there are likely to be even more cases that can be enabled. There are some organization cultural and technical barriers that must be addressed at companies adopting wireless communications within operational environments, such as achieving employee safety.

What About Safety?

Safety is particularly important for mobile equipment, moving machinery, reconfigurable plants and anywhere where humans are in immediate proximity to dangerous items in the industrial control system. These applications present unique challenges for industrial communications, such as how to communicate industrial information wirelessly and how to keep employees safe while interacting with mobile machinery. Wireless communications have been making steady improvements and many applications can be accomplished today with functional safety as part of the design.

How can safety work over wireless? First, it makes sense to consider functional safety requirements generally, and how those work over industrial communications. There are many standards related to functional safety in different contexts. The common themes for industrial control systems are:

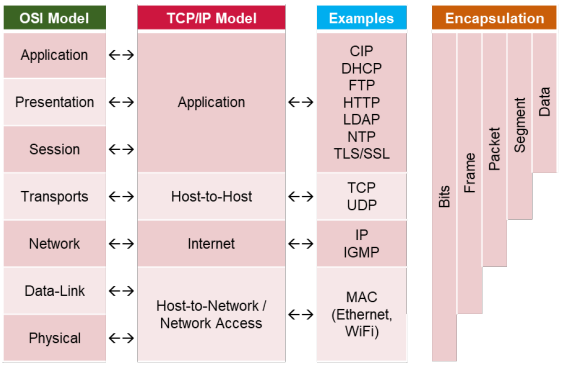
- Reduce the risk of a component failure or system failure
- Quantify the risk of failure after reductions are in place
- Detect when failures occur
- Ensure that failures always lead to a safe state

This is done by using good design practices, applying oversized components, performing statistical analysis of failure modes and running diagnostics regularly among other techniques. Modern standards for safety system design, such as IEC 61508 and IEC 62061 specify how to apply those techniques to electronics in the system, while IEC

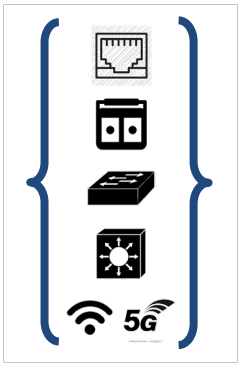
13849 adds in electromechanical systems. How do those good principles apply to something like networked communications, especially wirelessly?

Foundations of EtherNet/IP

We will begin with examining how standard industrial communications work. It is helpful to review the OSI model and the TCP/IP model for communications to understand how different parts of the communication system work together for the EtherNet/IP™ industrial communication network.



1. Data that must be communicated between two devices is generated in the higher, or application layer, using the Common Industrial Protocol, or CIP™ protocol. This is the same layer that familiar functions like HTTP and SMTP exist in.
2. In the transport layer, the CIP information is encapsulated. In the case of EtherNet/IP, that is a TCP or UDP header.
3. In the network layer, logical addressing information is added. In the case of EtherNet/IP, that is the Internet Protocol (IP) information; the packet is now ready for network access.
4. In the datalink layer and the physical layer, the packets are converted to the transmission media, sometimes with additional measures to avoid packet collisions. Combined these may be called network access layers.



This hierarchical organization is important because the critical user data for CIP is completed in the first step, independent of the transport, network, datalink or physical layers. With that independence different networks are possible, as well as different transmission media.

That means you can use one protocol, EtherNet/IP, for communications over copper, fiber and wireless, through Layer 2 switches and Layer 3 routers. Next, we will examine how those communications work over wired links.

Wired EtherNet/IP

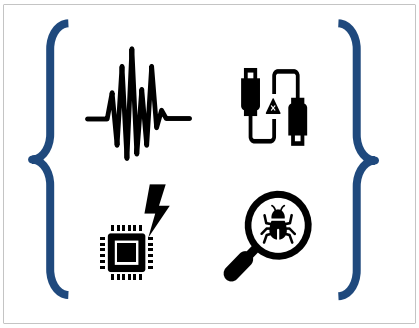
When using different network access layer implementations of EtherNet/IP, there are key differences to consider. Different transmission speeds, packet per second limitations and collision detection/prevention mechanisms may be in place. Further, the quality of the physical media is important to consider. These differences can be demonstrated to a small degree with fixed media like copper wiring:

Datalink and/or physical layer variant	Max throughput speed	Typical latency	Collision detection and prevention	Quality of physical media
10BASE-T1S (SPE)	10 Mbit/s	170 us ± 15 us	Point-to-point half/full-duplex, or half-duplex multi-drop (CSMA/CD)	15 m, 2 wire, Powered, 18 AWG twisted-pair
10BASE-T1L (APL)	10 Mbit/s	185 us ± 15 us [1000 m]	Point-to-point only, full-duplex	1000 m, 2 wire, Powered, 24 AWG twisted-pair
100BASE-TX (Fast)	100 Mbit/s	85 us ± 15 us	Full-duplex	100 m, 4 wire, Cat 5
1000BASE-T (Gig)	1000 Mbit/s	60 us ± 10 us	Full-duplex	100 m, 8 wire, Cat 5e

One advantage of fixed systems is that their reliability is highly predictable. While there are different speeds shown, the achievable net data rate can be impacted by a limited number of factors. The primary impact for reductions in throughput is based on lost, dropped or damaged packets. This can be measured by packet loss and the bit error rate (BER). With Ethernet communications, the higher levels of the OSI model are designed to detect errors in the lower levels. The errors referenced here are primarily physical layer errors.

FIBER-OPTIC MEDIA

EtherNet/IP can also be deployed over fiber-optic network links, which can significantly increase the data throughput and the distance between nodes. Fiber can increase the speed or the distance between nodes by an order of magnitude or more, but if both are increased the gains are more modest; there is a tradeoff associated with distance and throughput with fiber.



Packet loss can occur when cables are broken, collisions occur, or switch firmware mishandles the packet. These are all rare events when full-duplex communications are used, however the lack of full-duplex communications can increase the packet collisions; this is mitigated by the CSMA/CD protocol. This protocol allows each transmitter to listen to the shared media before starting to transmit. When a collision is detected, the two (or more) guilty transmitters stop transmitting and wait a random time interval before trying again.

Individual bit issues when using physical media usually arise from interference on the transmission media. For copper, that can be electromagnetic interference. The different grades of cables, shielding, twisting, and distance are all part of strict requirements around the physical media to reduce the risk of electromagnetic interference. Sometimes, electromagnetic interference cannot be avoided, or long distances must be employed; fiber-optic transmission presents an effective, but costlier solution. The most common bit errors in fiber come from dirty connectors, crushed media, and imperfections in the fiber.

Wireless EtherNet/IP

For wireless (or cableless) communications, the two dominant methods use radio frequency or optical means. Most of this paper will be focused on radio frequency, since radio frequency products for the industrial space are more available than optical products. When considering using wireless communications, the same metrics can be applied as wired communications.

Wireless medium	Max throughput speed	Typical latency	Type	Distance
Zigbee (802.15.4)	0.25 Mbit/s	40-350 ms	Mesh	10-20 m
Bluetooth (802.15.1)	1-2 Mbit/s	40-100 ms	Point-to-point	2-5 m
Wi-Fi 3 (802.11g)	3-54 Mbit/s	1-4 ms	WLAN	35-100 m
Wi-Fi 4 (802.11n)	72-600 Mbit/s	1-4 ms	WLAN	35-100 m
Wi-Fi 5 (802.11ac)	433-6,933 Mbit/s	1-4 ms	WLAN	35-50 m
Wi-Fi 6 (802.11ax)	600-9,608 Mbit/s	1 ms	WLAN	35-50 m
5G	100-20,000 Mbit/s	1 ms	Large Area	Wide Area

Note that the latency is many orders of magnitude more than wired transmission. Based on the statistics above, there are fundamental differences between the different technologies available, which will dictate how they can be applied. The specifications shown can be misleading for industrial applications that may not be able to use the full capabilities. Even when multiple technologies are available, there should be some aspects of the application that can help you decide which to use – see later sections on choosing wireless technologies.

The factors driving the differences between transmission methods are separate from that of wired media, but the same metrics can be examined. For example, the bit error rate can be used to characterize wireless communications. For radio frequency transmissions between two devices there are many different factors contributing to the bit error rate, including:

- Distance
- Obstacles
- Interference

The radio waves from the transmitting devices lose strength exponentially as they propagate away from the transmitter. Even when two devices are physically close to each other, if their transmitting equipment and receiving equipment are focused for a narrow transmission field but not aligned to each other, the communications could be transmitted without being received. Similarly, obstacles can block the signal or weaken it. Finally, the geometry of a structure, the material composition and even the paint finishes can generate interference with the signal.

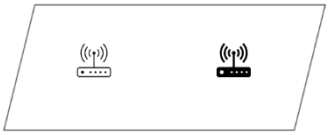
The interferences mentioned mean that wireless networks are reconfiguring much more frequently than typical wired networks. As signal strength changes, wireless devices will hop to another transmitter, which can create packet timeouts. In an office Wi-Fi environment, walking between your desk and a conference room with your laptop will likely trigger the transition to a new access point, however that transition does not change your productivity for the day. It happens fast enough not to interrupt your work. Industrial communications that transition could take long enough to disrupt the process if the devices and network are not configured properly. The amount of motion will impact how often reconfiguration happens, so you should consider these four different movement profiles:

1. Fully fixed point-to-point
2. Movement around a fixed point
3. Movement on a fixed pattern
4. Irregular movement

In any of these cases, proper antenna design and a site survey must be considered for reliable wireless performance, as well as the impact of what roaming between base stations will do to the performance of the system.

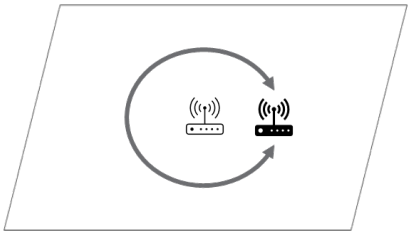
Fully Fixed Point-to-Point

Fully fixed point-to-point transmission is very useful when there is no easy way to get communications between the two stations, such as through the walls of a fully sealed vessel or where adding cable ducts could cause challenges for personnel and forklifts. There is a single point-to-point connection between the wireless stations.



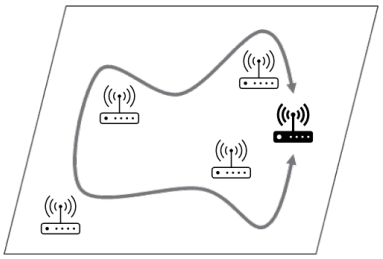
Movement Around a Fixed Point

Transmission for movement around a fixed point could be best characterized as monitoring rotating equipment. A single point-to-point connection is likely to be used, however the geometry and obstacles between those points may be changing. These applications do not usually need long-range transmission, but the constant movement may influence antenna design so that it can cover the path of the moving parts. Wireless communications offer a lower-maintenance solution compared to the traditional answer, sliprings.

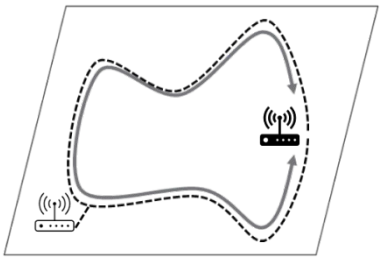


Movement on a Fixed Pattern

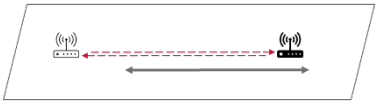
Movement on a fixed pattern can take a few forms. The simplest form could be an automated storage and retrieval system (AS/RS) or gantry crane – out and back on a straight line. A more complex pattern could be an automated guided vehicle (AGV) following an embedded path in the floor, a roller coaster following the fixed rails of the ride or a monorail transport system in an automotive factory. Each example has different considerations:



- Any of these may be a long enough distance that multiple radio base stations would be required for a system like Wi-Fi to work across its entire range.
- Another option to consider if the path is a single continuous loop is radiating cables, also known as leaky feeders or leaky coax. These coaxial cables with engineered modifications to the outer shield create a tunnel of signal to follow curvilinear paths without creating excess radio noise outside of the path.

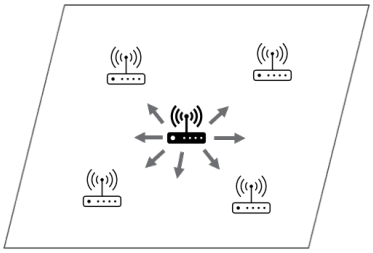


- Straight systems can sometimes use infrared or laser-based optical communications, although that requires maintaining line-of-sight between the transmitter and receiver.



Irregular Movement

More intelligence in devices is contributing to an increase in irregular movement, such as autonomous mobile robots (AMR). Another example of irregular movement would be humans with a wireless communication device that is part of the automation system, such as a wireless teach pendant or emergency stop device. Keep in mind that a tablet computer used for dashboards is likely not going to cause the process to stop if communications are lost, so it should be considered more like an IT asset than an OT asset. For this case and the other cases in this section, it is likely that multiple base stations will be required to cover the space adequately.



More Transmitting Devices Will Mean More Planning

Each of the examples shown so far considered a single wireless bridge. Realistically, your application is likely to have many wireless bridges, each following the planned motion. For a wired network, that is of little concern – full-duplex communication means that each link is an independent network connection. With wireless, the air between stations represents a commonly shared media. Not only do wireless networks often have more constrained operating parameters than wired networks, they also behave differently as the network becomes congested. How does that happen? On each frequency, only one device within the transmission range can be transmitting at a time. If two devices begin talking simultaneously, both will stop, wait a random amount of time, then attempt to transmit again. Even though wireless transmitters spread their communications across many frequencies to reduce interferences, too many transmitters on too small of a frequency range will produce more collisions and reduce the overall effective throughput of the network. In these conditions, transmitting longer bursts of data is slightly more efficient from a pure measurement of throughput like bits per second (hence features like packet aggregation in 802.11n), however those benefits for raw throughput come at the cost of latency. For industrial applications latency is usually more important than throughput.

This problem plagued early wireless technologies, but modern wireless technologies like 5G and Wi-Fi 6 (802.11ax) have been specifically tailored to higher device densities by increasing the available transmission frequencies and improving the efficiency of frequencies with scheduling.

Applying CIP Safety to Wireless Applications

Both wired and wireless communication networks have complexity, from the device to the switch, router, through all the network media, and to another device. It would be a massive undertaking to try to make an entire communication network meet the principles of functional safety, and any change to any part of the network could require revalidation. While this idea is a theoretical possibility, functional safety over communication networks instead follow a concept called the “black channel principle”, which is laid out in IEC 61508.

The black channel principle stipulates that two safety devices must have enough intelligence in themselves, and enough diagnostics in their communications, that the entire communication network has zero impact on the ability of the device to detect communication errors. Even though Ethernet communication networks have considerable error detection built into them, none of that may be used to satisfy any part of the safety function.

CIP Safety™ devices create a logical connection to each other, independent of the network technologies being used. In the devices, common errors are mitigated with various techniques, as described in IEC 61784-3-2. Time stamps are used with time expectation to detect if packets are lost, delayed, repeated or transmitted out of order. Unique device identifiers are used to authenticate the communication between two safety devices. Additional diagnostics and checks are included to validate that the messages are not corrupted in transit and all these features are separate from standard communication methods.

CIP Safety IEC 61784-3-2:2016 Page 29	Time Stamp	Time Expectation	Connection Authentication	Data Integrity Assurance	Redundancy with Cross Checking	Diff. Data Integrity Assurance Systems
Corruption				✓	✓	
Unintended repetition	✓			✓		
Incorrect sequence	✓			✓		
Loss		✓		✓		
Unacceptable delay		✓				
Insertion	✓		✓	✓		
Masquerade	✓		✓	✓	✓	✓
Addressing			✓	✓		

When these mitigations are put together as CIP Safety, a single connection between two devices, wired or wireless, can be used for communications certified up to SIL 3 per IEC 61508 and up to Category 4/PLe per ISO 13849-1.

Security for Wireless Applications

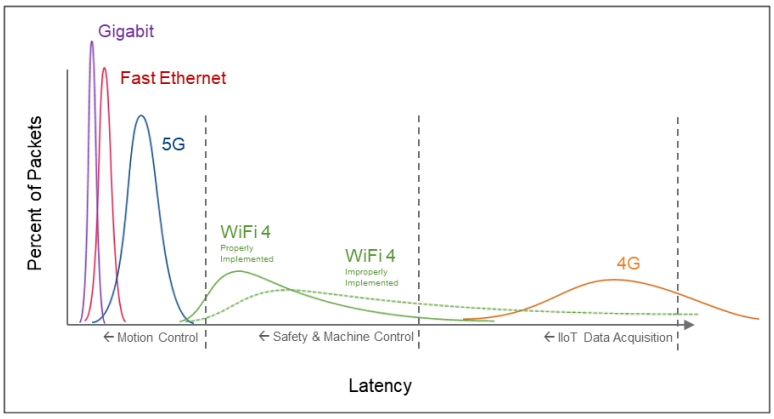
It is especially important to acknowledge security if you are considering a wireless installation, since it has a different attack surface than wired networks. Traditional physical media networks have defined access points, such as cables and switches, which must be protected from access. It is relatively easy to add physical security to a traditionally wired network; if you prevent someone from plugging into the network by locking doors, you can maintain access control.

Wireless adds another dimension since anyone nearby has potential access. Luckily, the possibility for eavesdropping has been addressed for every wireless system through encryption. Any wireless system – whether deployed for home use, office use or operations use – should activate the security features available. This will typically authenticate transmitting devices, encrypt traffic between nodes and provide mechanisms to lock the configuration. Wireless networks may be more susceptible to denial-of-service (DoS) attacks because the media is the air rather than a cable in a protected facility.

Additionally, there are decisions you can make throughout the design process that can reduce the risk of stray signals being sent outside of your intended area, such as a radiating cable and smart placement of the antennae.
Additional methods should be considered for protecting all industrial traffic from end device-to-end device, such as CIP Security™. That adds protection over wired links that may not have integrity or confidentiality today.

Plan and Build Your Wireless EtherNet/IP Installation

There are best practices to follow as you are planning, designing and implementing your wireless system. The graphic shown to the right demonstrates how different technologies can be applied for different use cases. While not comprehensive of technologies or applications, this can be a guideline for where to start. This also shows how the distribution of packets can be dramatically changed by the specific features implemented, as shown with the Wi-Fi example.



Which Technology Will Work Best?

For motion control and very high-speed reaction times, wired networking is recommended between the controller and the device. It is possible to do some coordination of servo axes on different sides of a wireless bridge, if both of their respective controllers are local to the drives and if there is suitably small network latency and clock jitter for the time synchronization. Wireless technology available today, such as Wi-Fi (see sidebar), can be used for this with careful tuning of the system. However, Wi-Fi 6 and private 5G systems should improve the reliability of this type of deployment. Public cellular systems like 4G LTE are unlikely to succeed due to long round-trip times, and private 4G LTE implementations never took hold in the market. Bluetooth and ZigBee systems are unlikely to succeed in these applications.

For time-critical safety and I/O applications, there are slightly more options. While the individual devices will use the safety protocol to detect failures in communications and bring the system to a safe state, it is still important to use a reliable network to get the appropriate uptime without nuisance trips. Wired networks and Wi-Fi systems have been proven for these applications when properly used. The latest revision of Bluetooth has increased its applicability to industrial control applications, including safety protocols.

Wi-Fi: What are the different versions?

There are many different versions of Wi-Fi that have been developed. Here are the most common designations you'll find:

Early Wi-Fi (802.11a/b/g)
Clocking in at up to 54 Mbit/s, these standards are suitable for many industrial applications.

Current Wi-Fi (802.11n/ac)
Called Wi-Fi 4 and Wi-Fi 5, each of these revisions focused on improving throughput; the bulk capacity increases benefited consumer use cases, such as file transfer and web traffic. There is not typically a benefit to using these for industrial control traffic but they can still be useful for other plant data; in rare cases, some of these features can work against industrial control reliability.

Wi-Fi 6 (802.11ax)
New additions are targeted at improving industrial applications and the Internet of Things (IoT). This includes connecting to more devices per area, lower latency, better time determinism and higher overall speed.

While 5G and Wi-Fi 6 are still emerging at the time of this writing, preliminary testing shows that safety protocols work well over those new technologies. Be sure to compare your requirements against the capabilities of the technology you are investigating.

For other data monitoring applications, if you can tolerate higher latency, the full range of wireless technologies are available including cellular and mesh networks.

Determine Your Needs – Traffic Rate, Latency, Power Consumption, Distance

You must understand what your needs for wireless will be before you start choosing technology. There are a few different characterizations that should be applied, but the first to consider will be the wireless traffic requirements. You should try to predict what will be going across the wireless bridge: what kinds of packets (big or small), how many packets per second will be transmitted and your application information, such as control loop times and safety reaction time limits that will need to be accounted for. Vendor tools can help you to illustrate what those requirements will look like for your application.

With the basic information about what needs to be transmitted, review what kind of motion path is being considered, how many devices are transmitting wirelessly and how far the transmissions need to go. This is a good time to also consider the environmental factors that are involved, such as heat, humidity, shock and vibration.

Power consumption may influence the technology you choose. Certain wireless technologies are optimized for lower power consumption so that they can be effectively used with batteries – others are not. Is there sufficient power where your wireless bridge will be located? Many applications that use wireless power have access to significant power, either through electrified rails or wireless inductive power transfer; both options can be coupled with rechargeable batteries. Some applications, particularly for periodic data collection, may employ single-use batteries designed for many years of operation. Your process for choosing a wireless communication technology must include power consumption analysis if batteries are the primary power source.

The following table helps to explain the potential impact that traffic rate, latency, power consumption, and distance may have on a wired versus wireless decision:

Traffic	Latency	Power Consumption	Distance	Recommended	Wired or Wireless
High	Low	High	Short		Likely Wired
Medium	Medium	Medium	Medium	→	Application Dependent
Low	High	Low	Long		Likely Wireless

All factors mentioned can influence your decision for what kind of technology to use, along with which specific product characteristics are required for your antennae.

Perform a Site Survey

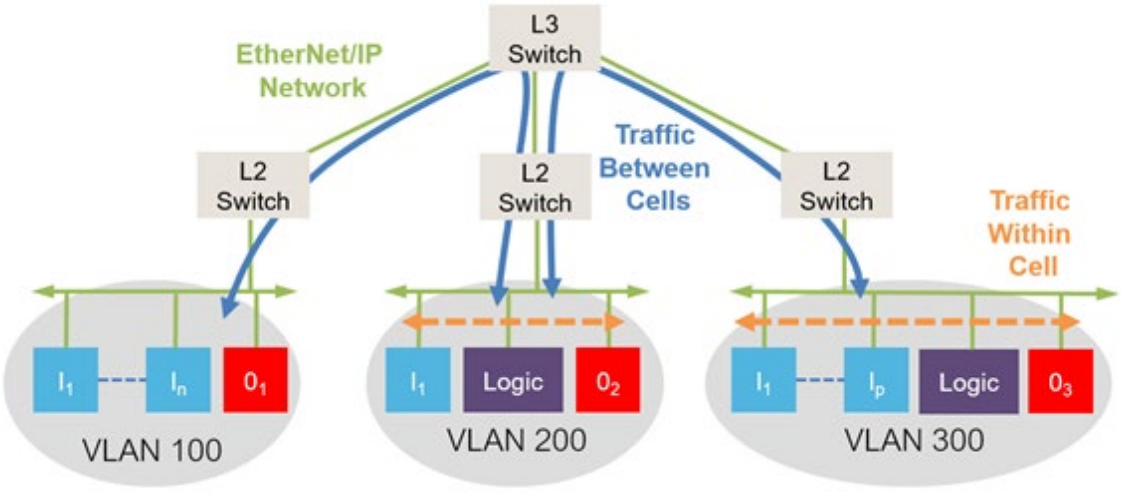
Each facility can be different and bring unique challenges to implementing a wireless system. How a facility was constructed and arranged will change where devices must be placed because different surface finishes and geometries reflect and dampen radio waves. During the site survey, wireless equipment should be placed around the site to measure signal strength based on the placement and number of the wireless devices. It is important to perform site surveys. Your partner for wireless equipment will often have services to assist with the site survey.

Commissioning and Tuning

Your wireless partner should help commission and tune the system so you reach the desired level of uptime. Since missed or delayed packets can lead to the safety function being activated, you want to make sure that packets are making it across the wireless bridge as expected. In addition to tuning the control system, there are likely settings in the wireless devices that can be optimized to confirm that the frequent, small CIP Safety packets are prioritized over other traffic that may be on the wireless link. These settings may have small differences between vendors.

Implementing the following will help optimize and prioritize CIP Safety packets over an EtherNet/IP network:

1. A fully switched network. This will eliminate collisions and improve the deterministic behavior of the data network.
2. Quality of Service (QoS) traffic prioritization. QoS prioritization allows time critical traffic to have preferential handling over supervisory traffic.
3. Logical segmentation of the network. VLANs improve security and contain broadcast messaging.
4. IGMP snooping. This will control multicast messages that can slow the performance of the network hosts. It also exponentially reduces the amount of traffic on the network, reducing the chance for congestion and consequent packet loss.



Please see ODVA Pub 35 Network Infrastructure for EtherNet/IP and PUB 110 CIP Safety: Safety Networking for Today and Beyond for more details.

Successful Use Cases

New designs are possible utilizing wireless communications and you should be assessing if your traditional constraints are still applicable. Plan for a multi-party collaboration between the wireless device vendor, the equipment builder and the end user. Wireless deployments continue to come down in cost while increasing capabilities. CIP Safety has been deployed already to hundreds of installations and the list continues to grow.

Author: Oliver C. Haya