Application Guide

Oliver Haya - Business Development Manager, Rockwell Automation
Brian Allport- Product Manager, ProSoft Technology

June 2020

Wireless functional safety

Applying CIP Safety on moving and remote equipment with wireless communications

This application guide addresses how to apply functional safety communication protocols like CIP Safety over wireless/ cableless communication networks. The advantages for wireless networks are discussed, followed by principles for functional safety. Industrial communications, 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.

Industrial communications are evolving

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 ways 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 robots (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 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.

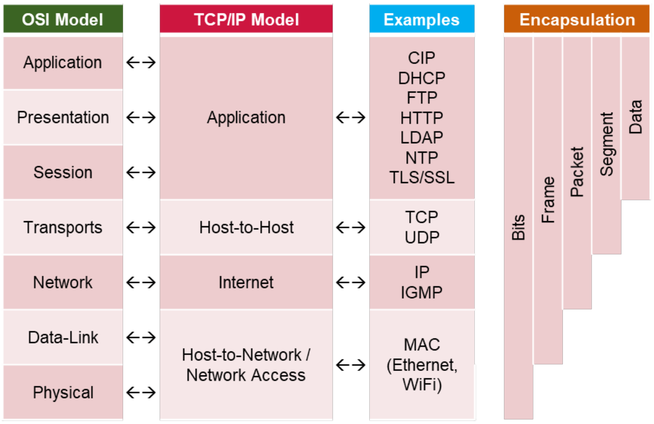
How can safety work over wireless? First, it makes sense to consider functional safety requirements generally, and how those work over industrial communications. There are many standards related to functional safety in different contexts. The common themes for industrial control systems are:

- 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 protocol.



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.

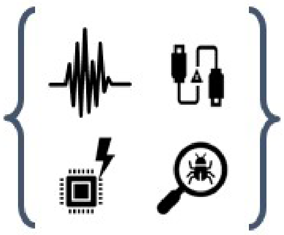
That means you can use one protocol, EtherNet/IP, for communications over copper, fiber, and wireless, and through Layer 2 switches and Layer 3 routers. Next, we will examine how those communications work over wired links.

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	85 us ± 15 us	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.



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

Wireless technologies make advanced mobile automation systems more valuable in every way. They make it possible to design more sophisticated machines, like smart conveyors and automated guided vehicles (AGVs), capable of performing tasks that would never be possible without wireless systems. But designing and deploying a robust wireless network that can keep up in an industrial environment requires forethought, careful design, and expert help. 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)	433-6933 Mbit/s	1-4 ms	WLAN	35-50 m

Radio waves from the radio 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 and other materials in the environment can block the signal or weaken it.

Ignoring the needs of the network or other aspects (like PLC programming) can also lead to communication faults. Best-case scenario: This can result in downtime and lost productivity, which in turn results in lost profits. Worst-case scenario: It's a serious safety hazard. Since wireless technologies have entered the industrial sector, machines can now move and communicate in ways that would never have been possible with hard wires. But adjusting to this new normal requires rethinking the way we approach machine communication.

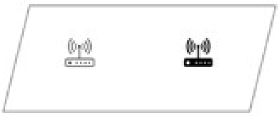
Obstructions or interferences mean that wireless networks change topology more often than wired networks. As signal strength changes, wireless devices will hop to another access point, which can create packet timeouts. In an office Wi-Fi environment, walking between your desk and a conference room with 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.

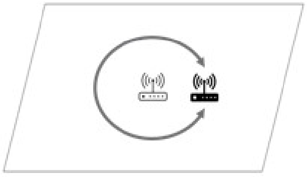
Fully fixed point-to-point

Fully fixed point-to-point transmission is very useful when there is no easy way to get communications between the two stations where adding cable ducts could cause challenges for personnel and forklifts. There is a single point-to-point connection between the wireless stations.



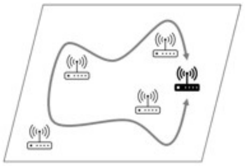
Movement around a fixed point

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, slip rings.

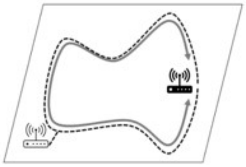


Movement on a fixed pattern

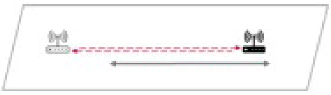
Movement on a fixed pattern can take a few forms. The simplest form could be an automated storage and retrieval system (AS/RS) or gantry crane – out and back on a straight line. A more complex pattern could be an automated guided vehicle (AGV) following an embedded path in the floor, a roller coaster 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 conductor create a tunnel of signal to follow curvilinear paths without creating excess radio noise outside of the path.

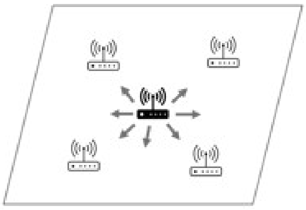


- Straight systems can sometimes use infrared or laser-based optical communications, although that requires maintaining line-of-sight between the transmitter and receiver.



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.

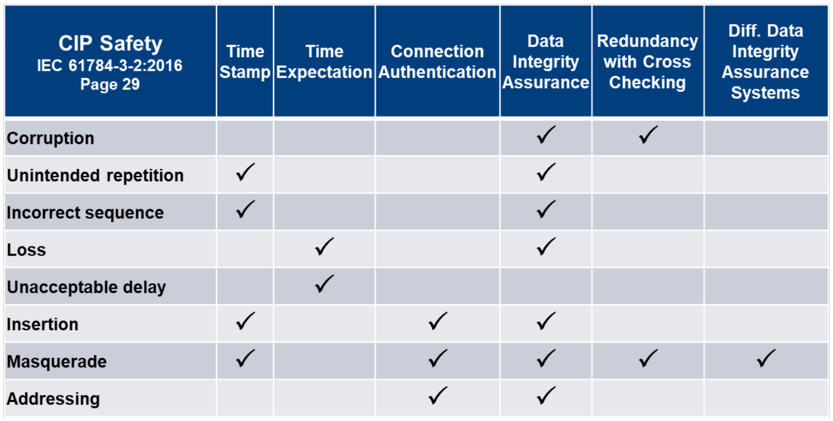


Applying CIP Safety to wireless applications

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 follows 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.

Choosing wireless products for your automation

Getting into the application, good design starts with good information. In order to build a network that can manage the tasks and traffic you need, you have to know the layout of the system you’re trying to build, the distance your network needs to cover, and the number of mobile devices the wireless system will be handling. You need to consider the amount of traffic that will be exchanged over the wireless system in order to make sure your network can handle it.

There is a lot of radio frequency noise in industrial environments, the same kind of radio frequencies wireless networks run on. There is also usually heat, dust, and other contaminants on the floor that require more hardy wireless networking equipment than the off-the-shelf equipment available at consumer electronics stores.

Both consumer and industrial networks run on specific standards, which essentially allow WiFi-equipped devices the ability to communicate with each other quickly and easily. Industrial systems have a distinct (though similar) system compared to the consumer one. The industrial version includes features and specifications designed with the particularly high stakes of the industrial environments in mind.

Network interruptions resulting in even half a second without connectivity could create serious safety hazards for the people who work around the machines in these environments. Considering the physical environment and the network’s needs isn’t limited to predicting the inside temperature and air quality. The environment also includes the people employed there and how the network can help keep them safe.

You will want a product that’s industrially hardened versus something you can get off the shelf at a store. The temperature specs, the vibration specs, and metal enclosure versus plastics all need to be considered. Industrial hardware has to be equipped for heat, dust, and dirt. You’ll also need a product that can roam quickly, to keep communication seamless. If it doesn’t roam well, you can lose the connection, the line would stop, and you would have to restart.

Remember: Nearly everything comes from the network, except the power. All operational steps, all diagnostics, all sensors have to be flawless — the smallest hiccup can shut the system down. These machines are in environments with both people and robots, moving freely. They need to be safe.

Know which setup decisions will most likely impact wireless network performance. That means looking carefully at the PLC communications, the requested packet interval (RPI), and the time out multiplier — if you set it too short, you can expect communication faults. That's why many experts advise setting it higher (typically to a value of 4 on a wireless system). Getting the RPI right is important — too fast and it'll create unnecessary traffic on the network, overloading it causing communication faults.

Knowing the number of connections to each carrier is important too. You have to know the total network load or how many packets per second will be produced, because if they overwhelm the network, you'll get communication faults and the system will stop. It's best to have a dedicated channel that's not used in any other wireless systems in the facility. That allows radios to talk without interference from other wireless networks.

Some questions to consider while engineering and deploying a wireless system:

- Do you have a line of sight?
- What are the RPI requirements of the automation system?
- CIP Safety: What is the timeout interval set to? (RPI x timeout = The safety requirement of the system)
- What is the size of the network, and how many access points are required?
- What RF channels are free, and what will the customer allow this application to access?
- What policies are in place so the customer won't introduce interference in the future as new networks are needed?

Plan and build your wireless EtherNet/IP installation

Involving experts in wireless networks for industrial environments is critical. ProSoft field application engineers help with the initial design, as well as testing and implementation after that. Having the right experts from the beginning ensures you're asking the right questions and making the right plans in the long-term.

Determine your needs – traffic rate, latency, power consumption, distance

You must understand what your needs for wireless Ethernet will be. 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. Tools like Integrated Architecture® Builder and the Safety Reaction Control Limit Calculator can help you 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.

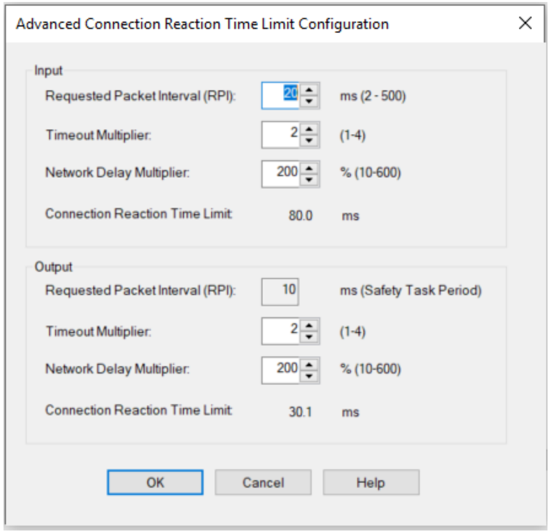
All factors mentioned can influence your decision for what kind of technology to use, along with which specific product characteristics are required for your antennae.

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 a site survey, link testing is done to determine Access Point placement. It is important to perform site surveys. ProSoft's team of field application engineers has services to assist with the site surveys.

Commissioning

ProSoft can help commission 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 the Logix Designer application, you may want to experiment with changing the Advanced Connection Reaction Time Limit Configuration during the commissioning process. This can help determine the cause of nuisance faults if they are occurring during testing. The lower these settings are, the more likely you are to see packet loss faults generated by late or lost packets. Remember that changes to these advanced settings directly impact the connection reaction time limit and the overall safety function reaction time.



Advanced Connection Reaction Time Limit Configuration

Input

Requested Packet Interval (RPI): 20 ms (2 - 500)

Timeout Multiplier: 2 (1-4)

Network Delay Multiplier: 200 % (10-600)

Connection Reaction Time Limit 80.0 ms

Output

Requested Packet Interval (RPI): 10 ms (Safety Task Period)

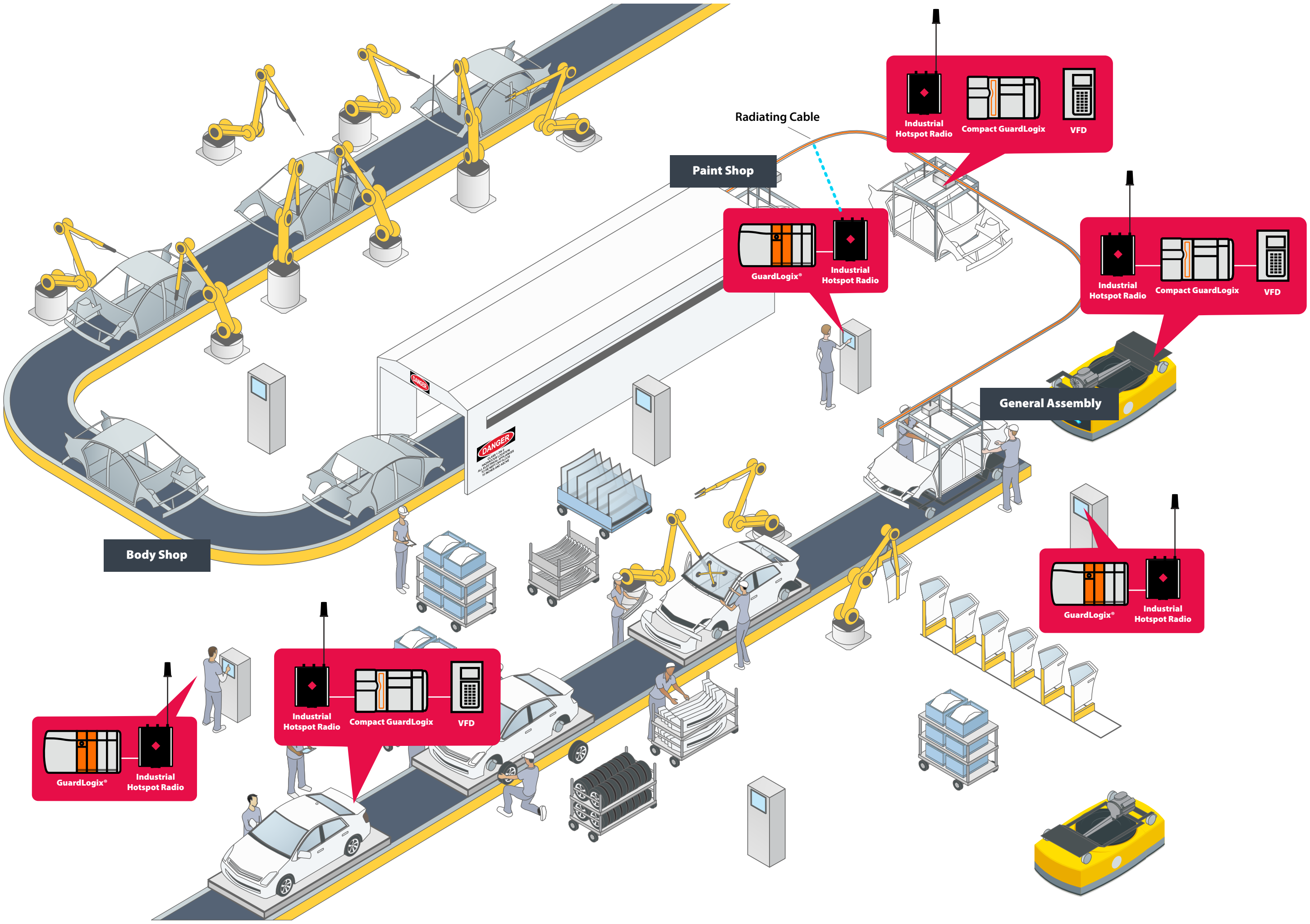
Timeout Multiplier: 2 (1-4)

Network Delay Multiplier: 200 % (10-600)

Connection Reaction Time Limit 30.1 ms

Application example

The typical CIP Safety over wireless Ethernet application would use ProSoft's **RLX2 wireless Ethernet radios.** These applications leverage 802.11n technology, which enables a standard wireless Ethernet connection in both the 2.4 GHz or 5 GHz bands, and ProSoft's industry-leading ultra-fast roaming. Roaming is when a client device, or something that you have connected to a wireless network, moves out of range of one access point and into the range of a new access point. When this happens, there is a hop-over time for the client to roam from access point to access point, and in industrial automation systems it is critical for this roam to happen as fast as possible to avoid communication loss.



CIP Safety over wireless is heavily leveraged in several applications, including factory automation in production environments like those found in automotive assembly plants. In these plants, several different types of conveyance systems, such as AGVs, are used to move vehicles and parts throughout the production cells. In these systems, the auto manufacturers prioritize the safety of their employees, and the flexibility of the system for future enhancements. This creates the requirement for Functional Safety via CIP Safety, and the wireless link to enable it.

In the typical AGV application, there are several AGVs traveling hundreds of feet. Each AGV would be outfitted with electronics including sensors for collision avoidance, location awareness, and safety, as well as drives for propulsion, I/O, and a safety controller such as a Compact GuardLogix®. This AGV system requires a wireless communication connection to the main safety controller, which may be a GuardLogix. This main controller also serves as the traffic cop for the entire AGV application and thus the system requires control, safety, and diagnostic data to be transmitted wirelessly. To establish this wireless link, an RLX2 industrial radio from ProSoft may be installed on each AGV in a Repeater mode, and installed in the network with the main control system in Master mode.

While connected to the main controller network, Master RLX2 radios are to be installed around the AGV application as specified by the site survey. These radios may be installed with directional antennas, omni-directional antennas or radiating cable depending on the results of the site survey. The Repeater radio may be installed onboard the AGV in the control cabinet, with an omnidirectional antenna installed outside of the control cabinet to ensure line of sight to the Master throughout the application.

Field Application Engineers from ProSoft help to ensure the success of the application through:

- Understanding the technical requirements
- Conducting site surveys
- Determining the best wireless frequency to use for the network
- Identifying master radio and antenna locations
- Identifying optimal radio settings

Worldwide Offices

Asia Pacific

Regional Office
Phone: +60.3.2247.1898
asiapc@prosoft-technology.com
Languages: Bahasa, Chinese, English, Japanese, Korean

Regional Tech Support
support.ap@prosoft-technology.com

North Asia (China, Hong Kong)
Phone: +86.21.5187.7337
china@prosoft-technology.com
Languages: Chinese, English

Regional Tech Support
support.ap@prosoft-technology.com

Southwest Asia
(India, Pakistan)
Phone: +91.98.1063.7873
india@prosoft-technology.com
Languages: English, Hindi, Urdu

Australasia
(Australia, N. Zealand)
Phone: +60.0.467.023.666
pacific@prosoft-technology.com
Language: English

Southeast Asia
(Singapore, Indonesia, Philippines)
Phone: +60.3.2247.1898
seasia@prosoft-technology.com
Languages: English, Bahasa, Tamil

Northeast & Southeast Asia
(Japan, Taiwan, Thailand, Vietnam, Malaysia)
Phone: +60.3.2247.1898
neasia@prosoft-technology.com
Languages: English, Chinese, Japanese

Korea
Phone: +60.3.2247.1898
korea@prosoft-technology.com
Languages: English, Korean

Europe/M. East/Africa

Regional Office
Phone: +33.(0)5.34.36.87.20
europe@prosoft-technology.com
Languages: French, English

Regional Tech Support
support.emea@prosoft-technology.com

Middle East & Africa
Phone: +971.4.214.6911
mea@prosoft-technology.com
Languages: Hindi, English

Regional Tech Support
support.emea@prosoft-technology.com

North Western Europe
(UK, IE, IS, DK, NO, SE)
Phone: +44.(0)7415.864.902
nweurope@prosoft-technology.com
Language: English

Central & E. Europe, Finland
Phone: +48.22.250.2546
centraleurope@prosoft-technology.com
Languages: Polish, English

Russia & CIS
Phone: +7.499.704.53.46
russia@prosoft-technology.com
Languages: Russian, English

Austria, Germany, Switzerland
Phone: +49.(0)1511.465.4200
germany@prosoft-technology.com
Languages: German, English

BeNeLux, France, North Africa
Phone: +33.(0)5.34.36.87.20
france@prosoft-technology.com
Languages: French, English

Mediterranean Countries
Phone: +39.342.8651.595
italy@prosoft-technology.com
Languages: Italian, English, Spanish

Latin America

Regional Office
Phone: +52.222.264.1814
latinam@prosoft-technology.com
Languages: Spanish, English

Regional Tech Support
support.la@prosoft-technology.com

Brazil
Phone: +55.11.5084.5178
brasil@prosoft-technology.com
Languages: Portuguese, English

Regional Tech Support
support.la@prosoft-technology.com

Mexico
Phone: +52.222.264.1814
mexico@prosoft-technology.com
Languages: Spanish, English

Regional Tech Support
support.la@prosoft-technology.com

Andean Countries, Central America & Caribbean
Phone: +507.6427.48.38
andean@prosoft-technology.com
Languages: Spanish, English

Southern Cone
(Argentina, Bolivia, Chile, Paraguay & Uruguay)
Phone: +52.222.264.1814
scone@prosoft-technology.com
Languages: Spanish, English

North America

Regional Office
Phone: +1.661.716.5100
info@prosoft-technology.com
Languages: English, Spanish

Regional Tech Support
support@prosoft-technology.com

Tech Support

ProSoft Technology's technical support is unparalleled in the industrial automation industry. To continue our world-class technical support, we have opened offices in most time zones in an effort to support our customers at a local level. See Regional Tech Support contact information above.

Wireless Safety

ProSoft® TECHNOLOGY
www.psft.com