Wireless Reliability in HARSH ENVIRONMENTS

Sponsor Overview

About Moxa: Your Trusted Partner in Automation

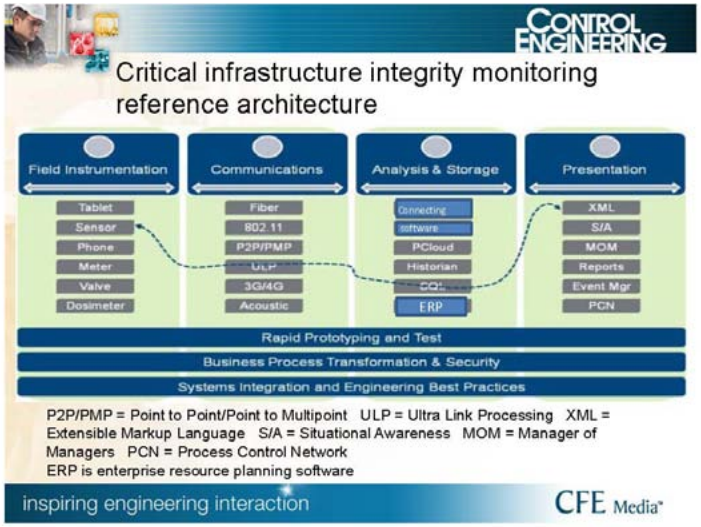
Moxa is a leading manufacturer of industrial networking, computing, and automation solutions. With over 25 years of industry experience, Moxa has connected more than 30 million devices worldwide and has a distribution and service network that reaches customers in more than 70 countries. Moxa offers a full spectrum of innovative, high-quality solutions that have been deployed in a wide variety of industries, including factory automation, smart rail, smart grid, intelligent transportation, oil and gas, marine, and mining. Moxa's expertise gives industry partners the tools they need to harness the power of automation network convergence and make their operations smarter, safer, and more efficient. 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.

Video brought to you by our Sponsor MOXA Reliable Networks ▲ Sincere Service

Industrial Wireless Monitoring And Sensing

Applying industrial wireless applications to monitoring and sensing can serve as a risk management policy. Strong communications address many challenges facility operators face during process transformations.

Douglas Bowers 05/14/2013



Industrial wireless can be easier to implement when referencing a reference architecture, which can serve as a critical infrastructure integrity monitoring (CIIM) model. Courtesy: SAIC

Wireless technology is a constantly evolving area, especially for industrial users, which often makes wireless infrastructure deployments in industrial environments difficult. Before taking on such a project, facility operators need to be aware of the challenges from rapid prototyping of wireless sensors in an industrial environment and the best practices for radio frequency (RF) design in complex or harsh RF environments, such as manufacturing, industrial, or power generation facilities.

The business drivers for this type of project can most often be associated with the transition from conditioned-based monitoring to performance-based monitoring. The conditioned-based monitoring approach typically means lack of on-line data to support diagnostics, and poor data alignment (such as with data residing in separate databases). In addition, the data points are usually collected manually, and the lack of continuous data does not allow for complex analytics or modeling.

Implementing wireless sensor sets create benefits across multiple areas. For instance, scarce engineering resources can focus on data analysis rather than data collection from disparate sources and can concentrate on few degrading trends rather than every trend. Maintenance workers can reduce or entirely eliminate selected data collection rounds through placement of wireless monitoring sensors. The need for deep technical capabilities on-site and concerns about inconsistent diagnostic results due to experience levels of individual employees can be greatly reduced.

By leveraging wireless technologies, operators can acquire critical component monitoring data in significantly higher volumes, reduce staff impact of making collection rounds, and focus those resources on data analysis and prognostics of issues. By implementing a wireless infrastructure and using it for the rapid deployment of new sensor types, operators can create significant advances in critical component monitoring.

Industrial Wireless Monitoring And Sensing (continued)

Clear wireless infrastructure design

A haphazard approach to wireless infrastructure project strategy can create huge cost and end user satisfaction issues. Even with good performance parameters, failure can occur if they are for the wrong application. To design the project for success, start with a solid system integration approach and define the business case and a clear concept of operations (ConOps). At the very least, list and prioritize applications.

The approach, business case, and ConOps should drive technical specification and help manage end-user and client expectations. With this in hand, the throughput needs can be defined. These will affect technical decisions, such as access point density, backhaul infrastructure, switching, power requirements, cable/fiber runs, and facility penetrations, among others.

Next, focus on the RF design process. Major steps in the RF design process should include passive and active surveys. Start with a passive survey for RF data collection, spectrum analysis, building composition analysis, and the outdoor features/topology noted. The deliverable after the passive survey should be the preliminary design. Once complete, all of the data can be imported into the RF modeling software to generate the preliminary model and design.

Once the preliminary design is finalized, the active survey can start at the facility. The active survey should validate the exercise for the preliminary access point placements. Measure the actual signal performance and confirm the final design approach. Once approved, it is critical to work with the plant information technology staff and engineer of record to formulate the build package and for iterative reviews of design during the installation process as issues arise. After commissioning, designers should return to the facility for testing and tweaking of the operational system for optimal performance. This last step is often overlooked but is critical for successful implementation.

Critical infrastructure problem

Critical infrastructures have their own unique monitoring needs that are not being met, but a strategically planned wireless infrastructure deployment approach may help alleviate some challenges. Critical infrastructure systems are increasingly a complex blend of old and new systems with varying tolerances and management requirements. Aging infrastructure is expensive to instrument, monitor, and maintain. Often, this causes accidents. New infrastructure has its own set of issues and can generate an unmanageable "firehose" of uncorrelated data.

To complicate things further, today's compliance requirements are reactionary and constantly evolving, and the market is flooded with fragmented point solutions. Right now, the industry lacks a clear "systems approach." Accidents, shutdowns, and cyber attacks can occur with a failure to monitor and act, so a well-developed wireless deployment plan is even more important on a critical infrastructure project.

Industrial Wireless Monitoring And Sensing (continued)

Pervasive wireless network

Facility operators often face aging, legacy equipment that may be "un-instrumented," and data acquisition on performance and maintenance may be natively impossible. Being able to retrofit ad hoc instrumentation and communicate to gather data and metrics can allow for better operational monitoring and maintenance planning and reduce downtime. One solution is to develop ad-hoc (off- the-shelf) modules for sensor types (humid, temperature, vibration, pressure) to allow rapid deployment of wireless-based sensors to gather relevant data. This allows ad-hoc, short-term, or emergency surveillance of problem devices. Plus, it allows a modular approach to wireless sensor measurement in an aging facility environment without large-scale digital equipment upgrades.

Beyond the delivery of voice over Internet protocol (VoIP) and mobile worker/data applications, the availability of a pervasive wireless network within the facility allows deployment of low-cost sensors and meters for tactical or short-term operational needs. A "bug-like" approach for the deployment of multi-sensor devices that is specific to the operation's needs should be used.

For example, if a faulty motor or pump is suspected, a camera, vibration sensor, and hall-effect monitor can be attached to the housing. In today's market, the sensor takes three minutes to assemble the modules in the "plant shop" and one minute to provision on the network.

Cohesive reference architecture

One of the best ways to avoid wireless technology obsolescence, ensure a long system lifecycle, and maximize system utility is to select and deploy wireless infrastructure in the context of a cohesive reference architecture. A reference architecture's chief function is to provide a baseline roadmap related to interfaces and capabilities of related technology systems and business processes for legacy and planning perspectives. Investing the energy and effort in development of a well-thought-out reference architecture provides several key benefits. These include ensuring equipment compatibility, adherence to and compliance with evolving standards across the enterprise, realization of long-term return on investment goals, and optimal planning of capital expenditure spending.

In an industrial setting the major components comprising a reference architecture typically include field instrumentation, communications, storage/analytics, and presentation/visualization. There are dozens, if not hundreds, of field devices that can be connected using one or more wireless technologies. Capturing field devices in the reference architecture provides an easy method for managing the multiple interfaces that need to occur between field and communications devices. Similarly, management of the interfaces between communications networks to the analytics/storage and presentation/visualization layers is also important to capture in a reference architecture. This ensures that higher layer factors including communications protocols, application programming interfaces, interface libraries, and other critical communica-

Industrial Wireless Monitoring And Sensing (continued)

tions functions are well understood and accounted for during the wireless technology selection process.

Embracing wireless

Although not without challenges, wireless solutions can act as a common enabling technology. They can:

- Provide ubiquitous communications capabilities
- Offer cross-operational value and utility
- Deliver common IP access using standards with robust cyber security
- Reduce lead time and costs associated with wired cabling.

On many projects, doing nothing is not an option, so the wireless solution acts more as a risk management policy. Plus, a strong communications foundation can address many challenges facility operators face during process transformation.

- Douglas Bowers is a senior project manager at SAIC. He has more than 15 years of experience in system integration for communication and network systems, identifying requirements, writing specifications, design, testing, and delivery, including rapid prototyping and development of sensor systems for industrial environments. Edited by Mark T. Hoske, content manager, CFE Media, Control Engineering and Plant Engineering, mhoske@cfemedia.com.

ONLINE

www.saic.com/EEandI

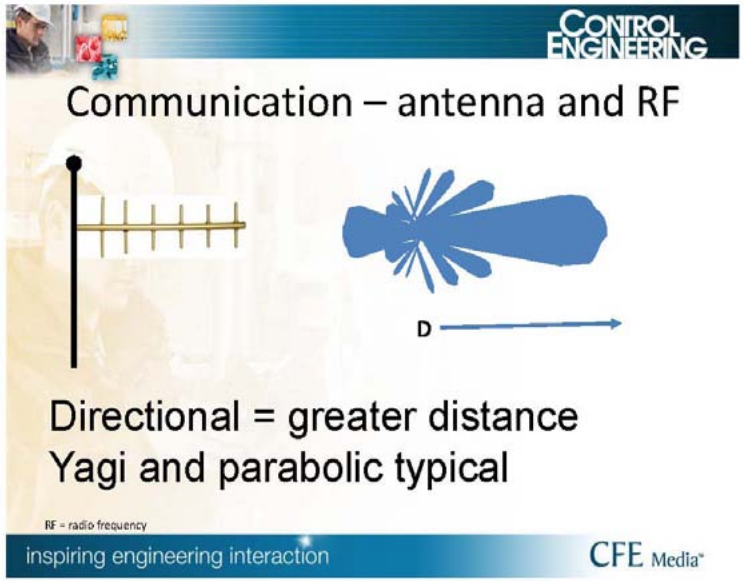
Bowers presented in a *Control Engineering* industrial wireless webcast. Learn more at www.controleng.com/webcast.

www.controleng.com/wireless links to related coverage.

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

Wireless technology tips and answers from feedback and questions submitted during a Control Engineering wireless webcast.

Stephen Muenstermann 04/17/2013



A Yagi is the typical directional antenna. However, a parabolic antenna offers a tighter focus and less RF splash on the back side of the signal.
Courtesy: Control Engineering Industrial Wireless Webcast, RoviSys Building Technologies

What are important performance metrics of wireless networks?

Top 5 performance metrics for wireless networks are radio signal strength indication, packet delivery, signal-to-noise ratio, receivers' sensitivity, and line of sight. More information on each follows.

Wireless network metrics:

- ***RSSI*** – Radio Signal Strength Indication – How strong is the receive signal

- ***Packet Delivery*** – This indicates that that your message was sent and received. Typically greater than 50% is solid as the data is spread out across a spectrum.

- ***SNR*** – Signal to Noise Ratio – which is the power ratio between the signal (meaningful information) and the background noise (unwanted signal)

- ***Receivers' sensitivity*** – a negative number -83dBm or greater is common. The more negative, the better sensitivity. Every time your receiver sensitivity drops by a factor of -3, it makes its ability to hear the incoming signal two times greater.

- ***LOS (line of site)*** – what this means is the distance the two radio frequency (RF) transceivers can visibly see each other without obstruction. This is more important when trying to shoot through walls, trees, canyons of steel, etc.

- ***Diversity*** – In many of these technologies they have what they call multipathing. That is where the same signal bounces off a metal wall and comes in slightly later. Most systems have great diversity.

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

• ***Determinism*** – Is the signal/network deterministic? This assures that you only get the data you want from each location.

• ***Encryption and authentication*** – These are security measures. The first refers to the RF in the cloud, the second refers to how it becomes recognized into the network.

Get testimonials from clients using the technologies you are evaluating.

After you become more familiar with RF you will find that it will be easy to pick and choose. About 70% of the problems I have seen in the field have been related to mounting practices of the radios or antennas. Fortunately, this can be easily fixed by moving either item around.

What is an IT wireless network?

The real important part is the network side of it. That is what we are forming connections with wireless. We can create multiple layers with multiple stacks, while exchanging copious amounts of information. Information technology (IT) is used as we are exchanging, storing, manipulating, retrieving, and transmitting data.

One transmitter?

Would multiple signals go through a single transmitter?

All sensor networks have unique points. Most of the "standard" sensor networks are designed to send multiple signals through a single transmitter. This mesh style network is to prevent a single point of failure and to be self-healing. So the short answer is: yes!

Did anything ever come of OCARI wireless?

OCARI (Optimization of Communication for Ad hoc Reliable Industrial network) has not yet been used in the United States, so I am only familiar with it by what I have studied since the standard started in 2010.

By its design it looks fairly solid. It's late to the party on standards and probably hasn't grabbed acceptance yet. It was developed mostly by the French, so it may take a while for it to grab broader acceptance simply do to the momentum of the other standards and that they are not in the heart of heavy industrial applications. Only time will tell.

What about designing RF links for facilities overseas, what advice do you have?

Many of the challenges overseas are the limitations of what is accepted by the country in which you are working. The 2.4 GHz band has been the most widely accepted because of the microwave oven. A typical microwave oven leaks about 1 W or more of RF energy. As a result, most countries have opened that frequency spectrum to allow people the ability to cook food (and popcorn) quickly.

In doing so it opened up a vast number of technologies in that spectrum from cordless phones, Wi-Fi, to WirelessHART, ZigBee, ISA100.11a, and others.

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

So my advice is stick with 2.4 GHz but be cautious of your power output and check the local limits. The last network I did in Finland only allowed for 280 mW radio output and 350 mW of ERP (effective radiated power). In the USA we can generate as much as 1 W from the radio and 4 W of ERP. (The ERP is related to what the antenna adds to the radio output power.)

Testing for wireless network health

You mentioned many wireless technologies. Since we are dealing with heterogeneous sensor networks deployment, have you thought of how to address remote testing of the performance and health of these sensors and sensor networks?

This is where the standards protect you most. The IEEE is pretty hard on what they will accept. And most manufacturers do not want to create radio networks that will fail. So these technologies are built with what the call anti-collision technology. So if they sense someone climbing into their specific spot in the frequency, they will divert the other direction. They keep a list of multiple nodes in their memory so they can jump to another node if the signals become too interruptive.

In understanding how a radio works, look at a cell phone. We have millions of people talking here in Chicago simultaneously with little or no interruption. So what the radios do is locate the cell that has the cleanest signal-to-noise ratio and links with that cell. It avoids the other cells even though the signal strength may be better.

From a heterogeneous standpoint: That is why you want to manage those networks, antennas, RF propagation, radio placement, and power output.

The radio receiver would be the most likely to fail if blasted with RF over numerous years. But, then again, the cost of a radio replacement is very cheap.

Wireless application questions

What radio technology was used for the wireless vibration applications mentioned? Are transceivers being used versus strictly transmitters from end devices?

With vibration testing, I have used both 900 MHz and 2.4 GHz technologies. ISA and HART standards use 2.4 GHz.

On the transceiver question, all the radios in a network are transceivers. They operate in a poll response fashion in their configuration, and when they do not, they give the proper response. So they are asked a question (receiver) and then sent their message (transmitter). Devices that act as nodes receive and transmit.

What is FEL?

FEL stands for front end loading.

When engineering a project (past proof of concept), FEL determines project details before starting the project itself. FEL balances risk over the cost of the project. If the cost is too high, you cannot implement unless the risks are resolved. Wireless can help mitigate risk.

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

Can wireless technology be applied to ESD procedure?

I am assuming that you are talking about static discharge from items located in the atmosphere. Or maybe asking if wireless devices shed static outputs? Hopefully one of these will answer your question:

• Most of these units are intrinsically safe, which means they are incapable of holding enough energy to produce a spark.

• The RF output is so significantly low that I have used more than 700 of these in a data center in Atlanta with absolutely no issues, and they have been there 10 years to date.

• I have installed 70 of these transmitters in a contained area in a nuclear facility. In testing, prior to installation, we found that they succumb to potential radiation failure after approximately 4 years. So the client put them on a 2-year replacement cycle.

• I have installed them in a refinery in California because the traditional wired sensors used were failing due to ambient static discharge and lightening issues.

Emergency shutdown

The ESD I meant stands for emergency shutdown. Normally we do this function with wired technology (no software routines).

I agree. I do not expect this technology to ever be accepted for ESD in my lifetime. That is too critical for wireless.

[Editor's note: Separately, *Control Engineering* machine safety blog has raised questions about wireless safety-related applications. See "Machine safety: Can hand-held devices play a role?" and "Machine safety and wireless devices."]

What technologies are used in various markets?

Many wireless and sensor technologies serve different purposes.

Wi-Fi most certainly has the largest exposure. On the sensor technology there are tens to hundreds of thousands in each category. Is there one dominant wireless standard? The answer is: not yet.

Related *Control Engineering* articles:

Industrial wireless market booming, but still underutilized

Research: Wireless use in industry

How about antennas with different frequencies?

What if antennas are handling different frequencies and modulations?

Antennas are cut or built to specific frequencies. They do not care about modulations.

Take your HDTV public signal: the same aerial antenna that you used with your old analog TV would work just fine. (The reason rabbit ears do not work as well is because the signal being transmitted is being transmit-

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

ted horizontally and is extremely crisp. Rabbit ears are really designed for vertically RF transmitted signals.)

What are the main problems or challenges of wireless for industrial controls?

The two biggest challenges for applying wireless to industrial controls today are:

• Speed of response. If it is battery powered, you can only operate as fast as 1 second updates. This is not good for fast control like flow, but is usually okay for most level applications.

• Acceptance.

I have had many engineers use this technology for control. I have set up numerous SCADA [supervisory control and data acquisition] applications that are totally wireless dependent.

Free of cables? What about batteries? Reliability?

Are wireless field instrumentation devices completely free of cable? What about battery replacement and battery faults? Which is the normal life of the battery for a sensor for a fast process? What about interference over time in an ever-changing plant environment?

Radios typically use very little power. So here is where sensor technology comes into play.

Most sensors that are wireless independent will send out a warning sign prior to failure. But the speed and life of the battery is usually the field sensor issue and not the radio. The ISA100.11a and WirelessHART protocols have specifications that define the speed capabilities. Currently the fastest is 1 second for both. However, most manufacturer specs cannot achieve battery life greater than 3-5 years at that point. The longer you extend the sample rate, the longer your battery life will last. Many claim as long as 10 years for both.

My job is not to convince anyone of the technology but only to inform. As an engineer you need to evaluate the risks and make your own decisions on what is best for your facility. Being skeptical of a technology is a good thing as it will help you clearly evaluate what would be the next best move for your plant.

But I would like to mention something that may offer a window into the future and what a facility will look like in 10 years. Wireless technologies are very new to the industrial world. Wi-Fi (802.11) has only been released since 1997. In less than 10 years, it has become a common platform in almost every business sector, hotel, restaurant, etc. The technology has grown from its first release of IEEE 802.11a, which was solid and secure, to what we have today, which is IEEE 802.11, more than twice as fast, and many are convinced it is more reliable and secure than their Ethernet (CAT 5 Hardwire) network.

Moore's law tells us that technology doubles every two years. So it is known that this technology will only improve with time. Technicians and engineers going through industrial engineering schools are already

Wireless Technology Tips From Control Engineering Wireless Webcast (continued)

learning wireless technology. What you will see in the future is that your networks will be managed internally by extremely competent staff members. The need for a survey will not be necessary as the staff members will have their networks mapped out with a very specific strategy. The radio sets will only grow more robust in the future with forward and reverse capabilities for migration, and will take every element that you are concerned about into consideration.

Wireless will never take over every aspect of control or monitoring in a facility. It will probably never be used for any level of safety system or critical control. RF noise levels can easily be controlled in a facility and equally coexist with any changes from telecommunications systems at a neighboring plant today if properly installed initially without further changes. That is why I suggest that if you make your first move into this technology, it is always best to seek the wisdom of a group that can properly map out and plan your strategy.

Compare it to pneumatics over 4-20 mA wired technology. In the late 1980s, there were still many plants that had not adopted this technology, except in a few small areas due to skepticism, at an extremely high cost to their facilities. They continued to manage and maintain complex pneumatic systems riddled with moisture, leaks, and numerous other issues. But even those that did convert still use pneumatics throughout their facility in places that 4-20 mA or smart technology will never replace control valves.

A curiosity for learning new technology is a very good thing. This way, if and when you do decide to move forward, you will have all the proper information you need to build the right wireless strategy that offers significant cost savings to your plant while allowing no risk to currently well-managed wired application.

Many thanks

- Stephen Muenstermann is RoviSys Building Technologies DC market manager. Edited by Mark T. Hoske, content manager, CFE Media, *Control Engineering*, mhoske@cfemedia.com.

See also, related PDF from Muenstermann's part of the webcast, "Wireless technology tips from Control Engineering wireless webcast" in the webcast archive.

Also see www.controleng.com/wireless for additional information about industrial wireless.

Research: Wireless Use In Industry

What wireless technologies are being used for industrial applications? IEEE 802.11, Bluetooth, and wireless are widely used. More information is being gathered.

Tom Moore 03/20/2013

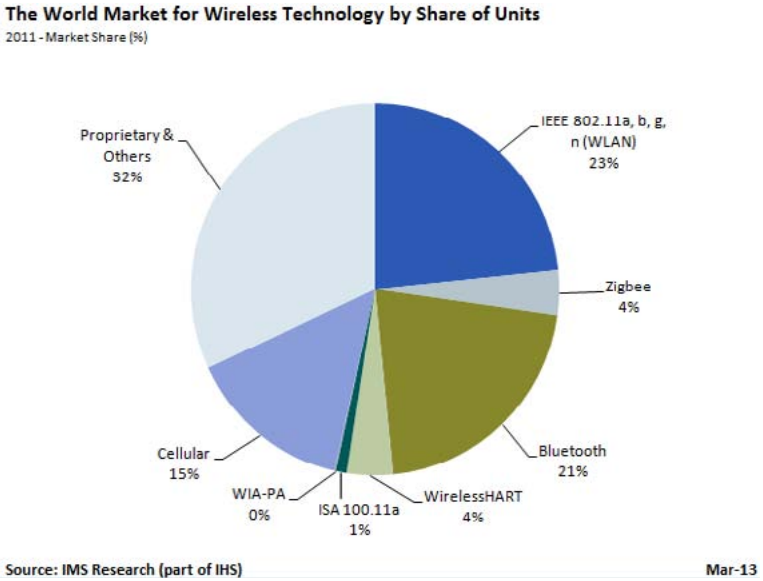


Figure shows wireless networks used for industrial applications. For 2013, information is being gathered on individual protocols.
Courtesy: IMS Research (Part of IHS Inc.)

Wireless in industrial applications has been around for a number of years. Its use has mainly been in areas where a traditional networking solution of industrial Ethernet or fieldbus has not been feasible, either through problems with distance, cost, or lack of existing infrastructure. Wireless technology has had to overcome a number of barriers in the past: A perceived lack of reliability, its suitability for control, and its ability to transmit in a busy environment have all hindered its adoption. However, as the technology has matured, user acceptance has grown.

Wireless communications used in factory and process automation are currently driven by three main technologies. In 2011, IHS estimated that almost one quarter of all new wireless connections made were made by wireless LAN. This can be in the form of 802.11a, b, g, and n. Modes a, b, and g are more popular, but n mode is beginning to make headway as it moves from the consumer market into the industrial space. Common use of multiple antennae means it has built-in redundancy should a single antenna be damaged or fail.

Bluetooth is also widely used within industry and is estimated to account for over one-fifth of total new wireless connections in 2011. Classic Bluetooth is relatively low bandwidth, but the newer Bluetooth high-speed variant is designed to improve this. Bluetooth can be suitable for battery-powered solutions, although Bluetooth Low Energy has been designed specifically with this in mind.

Cellular technology has been in used in wireless communication for some time now and is estimated to make up 15% of new connections. It is very suitable for long-distance transmission due to the existing cellular infrastructure in remote locations. This makes it very suitable for SCADA systems.

Research: Wireless Use In Industry (continued)

Many proprietary and "other" solutions exist in the wireless space. These include unlicensed bands such as the sub-GHz range as well as long haul communications. These are popular in the process industry and, like most wireless solutions, do not require any existing network infrastructure. The lower cost of installation can make them an appealing prospect to those looking to install wireless. WirelessHART and ISA100.11a have, until recently, been working toward a single standard. This, however, has not been successful and is unlikely to occur in the near future. The lack of convergence means these two technologies will continue to vie for new connections in the industrial space.

- Tom Moore, B.Sc, is analyst for industrial automation, IMS Research (Part of IHS Inc.). Edited by Mark T. Hoske, content manager, CFE Media, *Control Engineering* and *Plant Engineering*, mhoske@cfemedia.com.

ONLINE

IMS Research (IHS) July 2013 wireless networking report link

www.imsresearch.com

www.ihs.com

Wireless Networks: Adding Cellular Technology To The Industrial Toolbox

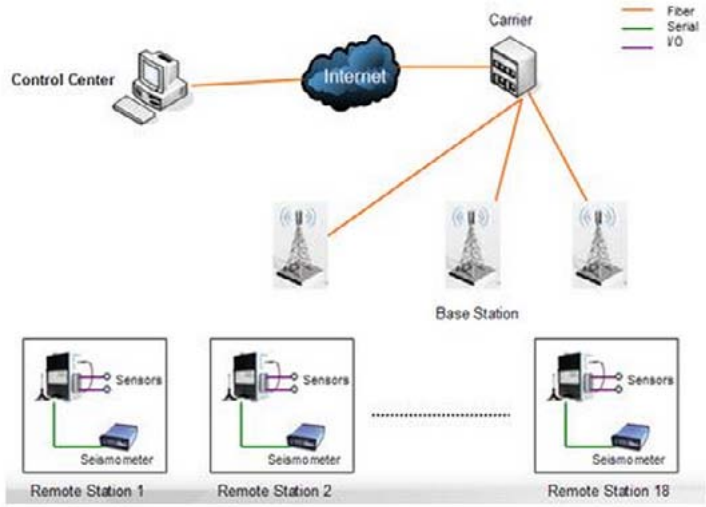
Can cellular networks provide a practical alternative for industrial use? While it may not be your primary wireless technology, Moxa explains that in certain applications, cellular is practical and economical.

Peter Welander

Cellular technology is one of the options available as companies look for ways to increase efficiency when working with remote sites and applications. However, many people are still unfamiliar with the technology, where to apply it, and what challenges users of it can face. This tutorial can provide an introduction and answer those questions.

Cellular technology covers two prevailing standards, GSM (global system for mobile communications) and CDMA (code division multiple access). GSM is used by such carriers in the US such as AT&T and T-Mobile, and is the predominant standard globally. CDMA is favored by carriers such as Sprint and Verizon, and is found mostly in the U.S. There are several generations within those standards that dictate the speed of the data rate you can expect. Those seeking higher bandwidth should stick with 3G networks, referred to as HSDPA/HSUPA for GSM networks, and EV-DO in CDMA networks.

One of the main challenges that users struggle with is where to use cellular vs. Wi-Fi or even traditional wired networks. There are a few key points to look for in terms of finding where to deploy cellular technologies:



Cellular technology is another wireless networking tool

- Is it difficult or expensive to pull wired networks (copper or fiber) to the location that needs network connectivity? Often times it can cost thousands of dollars to pull cable to a remote site for data that is only going to be sent on a periodic basis.

- Is there only a small amount of data that needs to be transmitted? In cellular, every byte sent has a cost associated with it. Because of this, a heavy bandwidth consumer like real-time video streaming, is not recommended over cellular due to the extremely high cost of sending so much data. On the other hand, if you have a PLC that needs to send its data every once in a while, or needs to be programmed remotely, this is a great fit for cellular.

Wireless Networks: Adding Cellular Technology To The Industrial Toolbox (continued)

• Is the device in a location where the network is locked down? Many system integrators who provide devices to end users need some way of getting to those devices remotely. However, many IT departments will not allow outside users into their network. In this circumstance, cellular is an ideal solution as it allows outside network access to a device that cannot provide that access through a company's own local network.

There are challenges to deploying a cellular solution that you should consider at the outset. One of the main ones is knowing exactly how to get information to or from the end device. Under most circumstances, cellular providers will generally give a SIM card a private IP address. This private IP address is firewalled behind a provider's network, thus not allowing access to that SIM card from outside the cellular network. Consequently, most users are also firewalled and are also assigned a private IP address from their IT department. Thus the challenge is to get the two sides talking to each other. There are a few ways to address this. One is to use a tunneling service which is provided by some carriers. Another option is to use a private IP software solution. This software is usually provided by the hardware manufacturer and allows both sides to connect to a server on a public address. This server will then open ports on both sides to create a virtual tunnel for the connections.

A second point is to watch the amount of data transferred through the system. Many times, it's difficult to estimate the total amount of data that will be transferred per month as there are multiple types of data being transferred. These include not only data sent by the end device, but also data transferred upon connection, establishing communications, data from keep alive packets, and others. These can all increase the amount of data that is transferred every month and consequently increase service costs.

Even with these challenges, cellular connections are a very viable and attractive alternative to traditional networking methods. With careful planning, cellular can be very cost effective, and in many instances, can save money by providing access to a device or location that may otherwise require a costly site visit. It is becoming more and more reliable, and the highly competitive nature of the business is driving faster network speeds.

Some of the more common cellular applications center on meter reading or accessing remote automation. There are huge numbers of machines or devices serving process manufacturing units that have some sort of PLC or control device running them. If that machine goes down or there is an error or unexplained behavior from that PLC, often times the machine builder has to go to the customer site and physically plug into the PLC in order to troubleshoot. This is not only time consuming, especially if the machine is located out of state or even out of the country, but also costly. To mitigate this, many machine builders are choosing to install cellular IP modems in their machines that are connected to either a spare Ethernet or serial port on their PLC or controller. When an issue arises, all they need to do is open up the software that is used to monitor or program that PLC, and use the cellular modem to log in remotely. Often the solution is simple fix

Wireless Networks: Adding Cellular Technology To The Industrial Toolbox (continued)

that a technician can implement from afar. An illustration of this can be seen below.

Other times, cellular applications can be more imaginative. An environmental monitoring application is one example of this. In regions of the world where earthquakes are common, there is a great need to monitor and track seismic activity. Since sensors for earthquakes are often in remote locations, it's often too expensive for governments to install network wires, and a standalone solution is desired. Traditionally, these include single board computers connected to I/O devices and seismic sensors. With cellular I/O, extraneous components can be eliminated and the sensor can be directly connected into the IO device, which in turn has a cellular modem already integrated into it. Combining all the legacy devices into one saves money, and increases the reliability of the system since there are fewer potential points of failure. Using an integrated cellular modem also eliminates the need for a seismic technician to personally visit each of the sensors to take a reading, thereby increasing efficiency for that employee. An overview of this system can be seem in the below illustration.

Cellular technology can be daunting for those who are not familiar with its concepts. However, once understood, cellular becomes a practical and cutting edge technology that is a better fit for many applications than traditional networking.

–Ariana Drivdahl is industrial wireless product marketing manager for Moxa Americas.

-Edited by Peter Welander, process industries editor, PWelander@cfemedia.com
Control Engineering Process & Advanced Control Monthly eNewsletter

WiFi Technology For Industrial Environments

Advice on how to set up a wireless infrastructure supporting industrial environments, signal integrity and protocol selection.

Peter Fröhlich 02/22/2012

Industrial environmental conditions are more demanding than in an office environment, with extreme temperatures, dirt, dust, moisture, shock, and vibrations. Industrial grade chipset have improved (passive) cooling and sturdy design to ensure reliability and longevity under these adverse conditions.

High- power electrical consumers, such as engines, welding robots or drives with their frequency converters, cause additional challenges. These can cause overvoltage, glitches, spikes, and noise on power supply lines due to magnetic induction, potential shifts, or high-frequency (HF) coupling. Industrial-grade networking gear uses internal dc-dc coupling with filtering and stabilization that compensates these effects.

Also, the radio can be heavily affected by stray HF noise, various other radios in the environment, and generally highly increased electromagnetic pollution compared to office environments. A special danger in outdoor applications has proven to be a constant threat to office-type access points: lightning strikes in the vicinity, with their extreme currents, cause high voltage spikes in outdoor WiFi antennas, which can easily destroy the radio. New-generation radios designed for industrial use employ overvoltage protection and narrow filters that keep other radio frequencies away and therefore increase reach, reliability, and throughput.

For any new installation only IEEE 802.11n should be chosen as the wireless standard. This standard increases data throughput compared to IEEE 802.11 b or g, although this is often not the prime concern. It also uses spatial information, which means that waves reflected from walls or steel structures are used just as direct waves are for retrieving the data.

Therefore, IEEE 802.11n offers much better stability of the data streams especially in industrial environments where a lot of large structures and metal objects are common.

Whitepaper: Critical Components Of Industrial-grade Wireless Devices

Jeffrey Ke - Product Manager
Mark Wu - Technical Writer

Executive Summary

For hard-to-wire locations and constantly-changing work landscapes with moving equipment and heavy machinery, such as applications commonly found at mining sites, wireless connectivity is the ideal solution for providing highly flexible and efficient network communication. However, most industrial applications require a stable and reliable wireless network that can only be achieved with industrial-grade wireless devices.

Industrial operators using commercial-grade wireless devices for mission-critical wireless applications may be getting satisfactory wireless network service, but frequent maintenance and system downtime can add up to a high total cost of ownership. In this paper, we reveal many harmful effects commonly found in industrial environments that can quickly disable a commercial-grade wireless device, and discuss the types of protection an industrial-grade wireless device should provide to ensure continuous wireless network communication.

Overview

Wireless failures at home or in the office will be an inconvenience until a replacement device is installed. Wireless network failures in industrial applications, however, can jeopardize the safety of onsite personnel, damage expensive machinery/equipment, and possibly translate into thousands of dollars per minute in production losses. In addition to network redundancy, industrial operators must also assess the application environment for elements that can impact network performance, compromise device reliability, and lead to unplanned system downtime.

Many industrial wireless applications, such as those for mining, railway, and oil & gas, are deployed in harsh environments and require the use of industrial-grade devices. While some environmental factors are obvious, such as extreme temperatures and moisture, there are other elements that are not so apparent but can also quickly disable an unprotected device. Below is a list of environmental conditions and effects commonly found in industrial wireless applications that can cause a device to malfunction or fail entirely.

- Power interference
- Magnetic field/emissions
- Flammable gases
- Extreme temperatures
- Humidity and moisture
- Airborne particles and contaminants
- Shock and vibration

Whitepaper: Critical Components Of Industrial-grade Wireless Devices (continued)

Industrial-Grade Protection for Wireless Devices

Electromagnetic Susceptibility (EMS)

According to the International Electrotechnical Commission (IEC)[1], EMS is defined as, "The inability of a device, circuit, or system to perform without degradation in the presence of an electromagnetic disturbance." Below are common types of electromagnetic disturbances that can interfere with device operation.

• **Electrostatic Discharge (ESD)**
ESD is the sudden transfer of static electricity between two objects with different electrical potentials. For example, factory workers wearing rubber boots and gloves can easily accumulate high levels of static electricity. Physical contact with wireless devices can discharge several kilovolts (kV) of static electricity and permanently damage internal circuitry.

• **Surge/Burst/Electrical Fast Transients (EFT)**
Switching disturbances, short circuits, and especially lightning strikes, can inject high-level voltage spikes to cause serious damage to wireless devices. Surge protection devices (SPDs), such as transient voltage surge suppressors (TVSS), metal oxide varistors (MOV), and gas discharge tubes (GDT), are necessary to provide industrial-grade protection against electrical transients.

Switching disturbances
Industrial high-powered equipment/machinery can require large amounts of energy to switch on and turn off components such as motors and hydraulic systems. This switching can abruptly generate high quantities of power flow, disrupting the steady voltage flow in the electrical system, which can be severe enough to instantly damage, or gradually degrade, device system circuitry.

Whitepaper: Critical Components Of Industrial-grade Wireless Devices (continued)

Short circuits

Accidental contact or unintended paths of two points in a circuit with different line potentials can cause a short circuit. In addition to yielding high levels of electrical surge and disturbance that can potentially damage device circuitry, short circuits can also generate intense heat, damage/burn wire insulations, and even cause fires/explosions.

Lightning strikes

Protection against direct lightning strikes requires the installation of a lightning rod (lightning conductor) to direct the massive amount of electricity quickly to the ground terminal. However, when lightning strikes, or is directed to, ground, surrounding wireless equipment can also be affected by the sudden rise in voltage because wireless equipment is also grounded.

• Electrical Field Emissions (Radiated)

Not to be confused with conducted electromagnetic emissions, electrical field emissions can affect almost every device. Electromagnetic radiation can be emitted by one device to generate RF currents in surrounding devices, causing electromagnetic disturbances and even possibly damaging a device. RF shielding, such as metallic device housings, can effectively repel electrical field emissions. Antenna isolation, as described in the next section (Galvanic Isolation Protection), can also eliminate the damaging effects caused by electromagnetic radiation.

Galvanic Isolation Protection

Transformers are generally used for changing voltages, but when used for circuit isolation, isolation transformers can transfer power between two physically-separated circuits to provide protection against electrical shocks, and prevent excessive electrical currents from entering the system when ground loops have different electrical potentials. Antennas on wireless devices can also be galvanically isolated to provide total isolation of internal device circuitry and further protection from electromagnetic disturbances.

Ingress Protection (IP)

Ingress protection is highly desirable for outdoor applications, where precipitation and/or debris can quickly penetrate the device housing, causing system performance deterioration and even permanent damage to the printed circuit board (PCB). Ingress protection

IP # #

Protection against solid objects	Protection against liquids
0: no protection	0: no protection
1: ≥ 50 mm in diameter	1: dripping vertically
2: ≥ 12.5 mm in diameter	2: dripping (when tilted up to 15°)
3: ≥ 2.5 mm in diameter	3: spraying
4: ≥ 1.0 mm in diameter	4: splashing
5: dust resistant	5: jetting
6: air tight protection	6: powerful jetting
	7: temporary immersion
	8: continuous immersion

Whitepaper: Critical Components Of Industrial-grade Wireless Devices (continued)

ratings (labeled as IP##) are used to indicate precise information about the level of protection a device offers against solid particles and liquids. For example, a wireless access point with an IP68 rating is completely air tight and can be submersed under water for long periods of time. See below for more detailed information about ingress protection.

Shock/Vibration Protection

Wireless connectivity is generally deployed for industrial applications where network flexibility is required, especially for moving vehicles, heavy machinery, and job sites that are constantly relocating, which can expose wireless devices to shock and vibration. Long-term exposure to shock and vibration can eventually result in electrical shorts, broken solder joints, loose PCB components, PCB delamination, and cracked device housings.

Shock and vibration can also disable a wireless device by shaking loose wires for power, data, and redundancy. Power, data, and redundant connections should be securely fastened to the device with terminal block, M12, or QMA connectors to prevent unintentional disconnections.

Extreme Temperature Protection

Extreme outdoor temperatures can reach below freezing at night, and rise to an excess of 50°C (122°F) during the day. Temperatures inside roadside cabinets can even reach extreme temperatures of over 60°C (140°F). Thermal stress/cycling will cause PCBs to expand and contract, which can also cause broken solder joints and PCB delamination.

Commercial-grade wireless devices may seem adequate for applications in air-conditioned environments, but are at risk of overheating when air-conditioning systems fail. Wireless network reliability should not be compromised by the failure of the air-conditioning system. For mission-critical wireless applications, operators should consider the possibility of deploying a fully-industrial wireless network.

Industrial Wireless Networks Need Industrial-Grade Devices

Conventional wireless networks, such as those found at the library or local coffee shop, typically provide only a best-effort level of service, and does not guarantee the user a level of service for packet delivery, transmission

Whitepaper: Critical Components Of Industrial-grade Wireless Devices (continued)

speed, or redundancy. Industrial wireless networks with mission-critical applications will have low latency-tolerance and must operate uninterrupted with high reliability, which can only be ensured with the deployment of industrial-grade wireless devices.

What many operators may not realize, and where many industrial wireless devices can fail, is that the use of commercial-grade wireless devices can present unforeseen vulnerabilities. Deploying a fully-industrial wireless network will require a greater initial investment, but the benefits of improved network uptime, enhanced network performance, and reduced maintenance costs will all contribute to a lower total cost of ownership.

For more information on how industrial-grade wireless devices can benefit your mission-critical wireless application, please visit: www.moxa.com/iw