Remote Condition Monitoring Technology

Benefits and Challenges

Joe Van Dyke, P.E.
Vice President, Operations

Abstract

The increased availability of wireless technology for industrial asset condition monitoring merits some discussion of the various benefits and challenges of the different types of devices and technologies available.

New manufacturing technologies, such as Machine to Machine (M2M) interfaces, rely heavily on remote wireless monitoring to erase the safety and reliability concerns of yesteryear. Gone are the days of maintenance pros climbing ladders or placing their hands in turbines to collect machinery information; instead, all of that information is sent to a central repository and analyzed by trained analysts 24/7 so maintenance personnel fix only the equipment that needs attention at that moment. Previously, it could take days to manually collect and analyze data but now that process can be successfully and conveniently automated.

This paper describes how manufacturers can best integrate remote wireless monitoring into their plant operations to improve the safety conditions for employees, increase productivity and reduce downtime.

We will be discussing the importance of manufacturing facilities adapting to these innovative and evolving technologies within the predictive maintenance industry. With new concepts of going beyond the traditional machine monitoring practices becoming more of a wide spread thought across executives, the idea of implementation is beginning to weigh heavily on priority lists. It is critical for facilities to begin implementing remote wireless technologies to ensure complete awareness over critical machinery health data.

Remote Sensing Devices (wireless condition monitoring)

Benefits

Wireless machinery monitoring saves money. Compare automated wired monitoring solutions to similar wireless solutions, and in almost all cases wireless saves money. This is because there is a much lower installation cost. Depending on the sensor, there may be no sensor cable wires to install. Wireless systems may cost more to maintain than wired systems, however, over a reasonable period of time, that effect is small in comparison to amount of time and expense required to install a wired solution because the installation cost isn't just wiring and hardware and labor to install, but time spent on necessary change documents, paperwork, and modifications. One recent example demonstrated that just the cost of wiring an online system to 60 sensors in an industrial environment required welding, electrical work, and specialized cabling with a cost of over $250k, roughly 3 times the cost of the actual hardware and software.

Compared to the cost of a walk-around program with the same level of surveillance, using an automated dedicated system, remote monitoring saves money. This is because the automated system can gather readings on many machines on a near continuous basis. In order to accomplish gathering large volumes of machine data, with a walk-around program, it would require a number of technicians each with an expensive meter working around the clock. For manageable numbers of machine surveys of machine condition monitoring data walk-around programs are clearly the most economical option when considering monthly or quarterly routes.

Often, but not always, existing Wi-Fi infrastructure that serves other plant purposes such as VOIP or mobile computing is available to accommodate the wireless monitoring hardware. Permanent wireless or M2M monitoring systems improve safety by eliminating the need for personnel to be in close proximity to dangerous environments or equipment. It allows for collecting data in sensitive, dangerous, or hazardous areas without risking harm to your personnel, processes, tools or the assets you are monitoring. Even when the equipment or the environment is considered safe, safety ratings should be expected to improve because automated data acquisition eliminates the need for personnel to be physically entering machinery spaces, carrying instrumentation up and down stairs and ladders, and all but eliminating the potential of contacting energized equipment.

Wireless monitoring systems provide information on machinery condition on a periodic, but more frequent basis. This allows for closer monitoring of machinery without a need for data collection personnel to be present. Test frequencies vary depending on the type of test conducted, but near real-time test frequencies are possible when testing high speed equipment or gathering overall vibration or scalar data like temperatures and pressures. This can provide continuous updates to plant personnel away from the machine and outside the control room or even outside the walls of the plant if desired.
Wireless monitoring systems inherit all the advantages of permanently installed systems at a lower cost. These include the ability to more readily observe dynamic changes in machine fault

conditions arising from changes in load, speed, and operating conditions. This can be very useful for several reasons.

Often machinery will exhibit signs or indications of a problem only when operating under certain load conditions and if these load conditions occur outside the times when data is normally collected by personnel in a walk-around monitoring program, or if they occur when it is unsafe to gather data, you can miss the telltale signs of a problem. Combine this continuous system presence with integration into SCADA systems and you can design a wireless monitoring program that wakes up fairly often but only collects data when the right loading and operations conditions exist. This helps to detect problems, save batteries life and avoid collecting data when the machine is idling, unloaded or off.

So we've identified some of the benefits of permanent wireless monitoring systems for industrial plants and assets. These benefits are considerable, but these systems also pose some challenges and the next section spells out some of these hurdles.

Challenges

Wireless condition monitoring devices fall into a few general categories. There are small compact self-contained units that have a radio, a battery and sensing element with its circuitry all combined into one enclosure. Then there are larger enclosures that house the battery and the circuitry with one or more sensors connected by cable. Also there are these same types of units that can or must be line powered but communicate wirelessly. And even line powered multichannel measurement devices that can support a lot of computations and sensors, but communicate over great distances via radio communications links. For these discussions, we are mostly considering battery operated devices.

General Challenge #1:

Battery operation: Given the nature of wireless devices, being designed to operate remotely and autonomously, they are often battery powered. Yes, it is possible to set up a power harvester and approach independence from batteries. Energy harvesting technology converts or scavenges mechanical energy from a nearby vibration source which is normally a rotating or reciprocating motor or engine of some sort, but that comes with its own issues.

Typically battery life is approximately 2 years for sensors. These may wake up on a frequent basis and collect data for overall alarming on several sensors or provide narrow band data less frequently. On the high side battery life has been quoted as exceeding 5 years on some products. A real life example demonstrated 24+ month battery life on units that covered 4 standard ICP accelerometers and 4 temperature sensors testing twice a day transmitting 4096 sample waveforms on the accelerometers. That same type of unit, collecting more rapidly on 10 minute intervals with only 2 channels activated lasted less than one month.

With the battery operation come other challenges.

Intermittent operation: Most devices are designed to sleep for a period of time, then wake up and conduct some set of predefined tests, transmit the resultant readings, and then go back to sleep. This can be a challenge because if and when a machinery event occurs like a sudden bearing lubrication system loss, and the supervisory system has the ability to detect it and interface with the wireless monitoring system, the wireless system may not be set to wake up any time soon and will miss the event or capture it well after the time has passed to gain any advantage by early detection.

In some cases, the devices can ping the home controller (sometimes called a gateway) at a fairly rapid interval like once a minute to check for possible activation commands and to get test instructions. This arrangement can minimize the chance of missing an important event, and can provide some fairly responsive behavior in devices. It does however reduce battery life, as the shorter the heartbeat interval is, the faster it will consume available battery life.

Limited test capabilities: Another result of living with battery operation is the fact that, as a rule the tests conducted are limited intentionally by design in order to limit power consumption.

These constraints can impede diagnostic capability by the supervisory system or by the analysts who are scrutinizing the data. Examples of this include when a lower number of waveform samples is chosen to keep collection and transmission time down. This results in lower frequency resolution in the spectrum and makes analysis harder and less specific and/or less accurate. Another example is omitting some preferred tests, like secondary sampling rates for better low frequency analysis, long time waveforms for digitally post processed envelope analysis, or omitting waveforms and spectra entirely and only collecting.

RMS (overall) data: One astute response from manufacturers and developers of wireless devices is to push as much smarts upstream into the sensor as possible. This means doing the measurement, and data processing locally at the measurement position, comparing bands to thresholds and computing other parameters based on frequency and waveform analysis, then transmitting only the data when alarms are exceeded and not the entire waveform, only the exceeding values. This saves battery life and reduces the amount of data that must be managed.

Battery changes: When batteries die or get depleted to low remaining useful life, it is necessary for personnel to swap out the batteries. This can be a time consuming process and costs are certainly not negligible. To address this by replacing batteries as a preventative maintenance action or when they hit some low threshold voltage, results in at least some wasted remaining battery life. Addressing the problem in a reactive manner results in lost monitoring capability because the device will cease operation and miss at least one set of readings before it gets new batteries installed. This approach may also cause other problems if the devices require reconfiguration after the battery expires.

Battery life reporting: Reliable estimation of remaining battery life is a challenge. The nonlinear nature of battery usage and life depletion means that you may not so easily be able to identify exactly when the battery will be done and unable to accomplish another reading. Often for wireless devices, when the battery gets weak, with some measurable capacity left, it will conduct the needed measurements but be unreliable in communicating them back to the server or gateway. This erodes reliability of the device itself.

General Challenge #2:

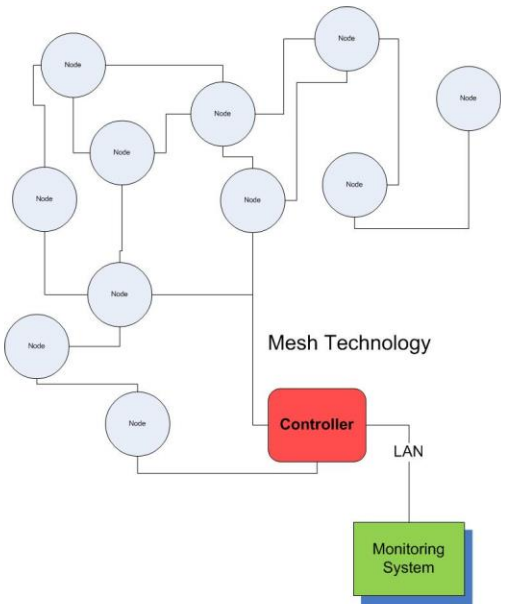
Interference: Industrial wireless condition sensor technologies fall into two general technical categories: Mesh technology or a direct node to access points (APs) arrangement like regular Wi-Fi 802.11. In either case, they typically use ISM band frequencies such as 2.4GHz typical.

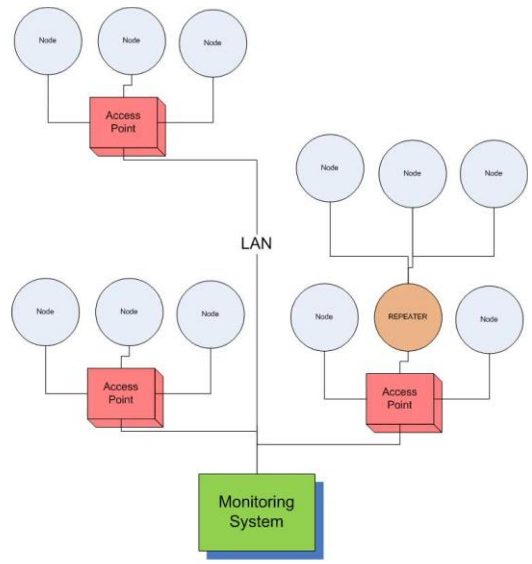
Mesh devices form their own self-healing network and can theoretically survive the temporary introduction of an electromagnetic interference source or sink that interrupts a communications path between elements of the mesh. This model is indeed robust, but not failure-proof, since a node that has only one connection can get disconnected, and interference can affect more than one pathway.

Node-to-AP based arrangements rely on a robust array of receivers and/or repeaters for reliability. While the set of APs can be designed to provide redundancy, many wireless devices will lock onto a preferred wireless access point and even when it is weakened or unreliable, will continue to use it rather than switch to a temporarily stronger more constant access point signal. This can introduce reliability issues.

Sources of interference or wireless signal problems can be as simple as an object or structure placed between a transmitter and a receiver, or a strong magnetic field like having a transmitter or receiver too close to an energized motor or other wireless device. Sometimes having the devices themselves too close to each other can cause problems. To remedy this, there are Wi-Fi surveyor companies and tools that are available on the market. Use of these services or tools can help identify persistent issues, but don't always capture intermittent interference, which can be the most common type of interference.

When sensors, surveyed assets, or access points are subject to intermittent strong EMF, a wireless system that transmits only small amounts of data will be more robust. A system that must transmit long sets of readings will have more trouble because the longer time required is more likely to span an interference event.





Access Point / Repeater technology

General Challenge #3:

Recognize and refuse data that is compromised: The first two challenges, battery life and wireless signal interference combine to create another general challenge: to design a supervisory/surveillance system that can manage when networks or readings or devices are affected by such issues and can react by reporting the device condition as compromised. The system needs to recognize bad readings and discard them, and also respond to missing readings with some alerts that can propose remedial solutions.

Remote/Distance Support:

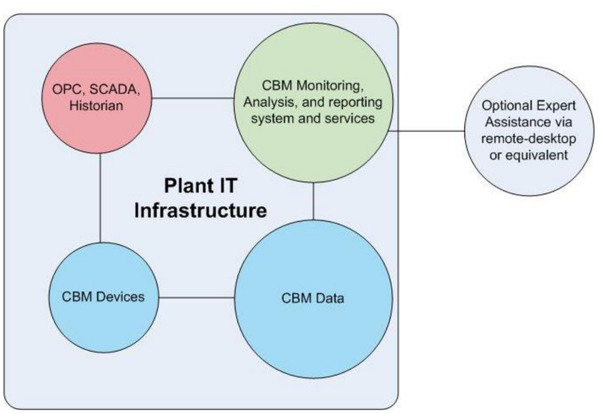
Whether you are using wireless technology for remote connectivity to sensors on your machines/assets within the confines of the plant, or wired automated data collection technologies, or walk-around devices, or some combination of all the above, systems are available to allow remote monitoring of that data by your own plant or corporate personnel, or contractors. This monitoring can generally be set up such that only an internet connection is required and can allow for anything from webpage viewing of dashboard-type summaries of machinery condition, to in-depth analysis and reporting, to resetting the systems, to actual programming of the devices in place and refining diagnostic criteria.

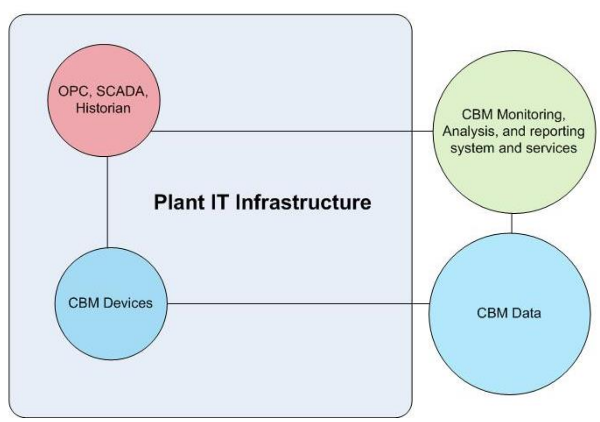
Remote/distance support models cover the spectrum and differ widely but can be divided roughly into the following three definitions:

1) Data and systems stay in the plant and with remote access allowed via secure VPN. This is more common for plants with restrictive corporate data policies.

2) Data stored/hosted offsite with access to the hosted data for analysis via web apps or websites or dashboards etc. This is becoming a very common model, with the availability of highly secure hosted data and data services. In this scenario, systems for acquisition of data communicate their information offsite for secure storage and management and analysis. The plant personnel access the data via applications running on workstations or corporate servers or as web applications.

3) Mixed, with remote access to components in place at the plant, and hosted cloud components with some data on site and some off site. This is generally the most flexible solution, offering the best plant systems integration options while still allowing for good distance support.

<table>
<tr><th>Everything onsite and
optional services outsourced</th><th>Data analysis systems hosted offsite</th></tr>
<tr><td>


</td><td>


</td></tr>
</table>

Benefits

These distributed data and distance support models provides benefits in a number of categories:

1) Allows sharing of information with corporate counterparts for the purposes of consultation, troubleshooting, collaboration, and reporting of KPI's and other performance-related issues.

2) Provides for the ability to have multiple resources in multiple locations looking at machinery performance and troubleshooting data.

3) Provides for the ability to compute and observe parameters other than what would normally be monitored in a traditional condition monitoring program.

4) The ability to assess machine performance in terms of efficiency, throughput, etc., and relate that data to machine condition.

Challenges

1) Satisfying IT security policies can be difficult.

2) Systems that are installed must fit into the plant IT infrastructure even when minimal connectivity is maintained. An example is a standalone XP industrial PC riding on industrial LAN for distance support. This computer may have been acceptable when installed, but then is deemed unsuitable because its operating system cannot be upgraded to accommodate current and changing LAN security policies.

3) Ensuring data security is of paramount importance whether the system resides in plant or off site. This paper is not on the subject of data security measures, but it is recognized to be a very critical challenge for distance support systems that push data out to the cloud or allow access in from remote users. The system firewalls must be constructed and managed to restrict all unnecessary access and suitable data encryption methods must be employed.

4) Use of data centers/cloud system must consider data ownership and data protection. Data is generally considered the property of the asset owner, but explicit provision of matter should be ensured using contract terms so the data is protected, not copied, and returned if and when the contract is canceled.

5) Continuity of services must be considered. Vulnerabilities to IT operations need to be identified to minimize impact on the system. An example is where a critical link to the OPC system for test operating conditions is severed because the IT department unknowingly changes

a password on a server that is being accessed by the remote CBM system. This can cause cessation in monitoring.

Another example is where the CBM system is feeding results into the OPC system but it stops due to a permissions issue leading to problem report that devices have failed starting a wild goose chase.

Connectivity within the Plant

Because they are normally integrated into the existing IT infrastructure, permanent automated condition monitoring systems can also be more readily connected into the plant's SCADA or OPC or Process historian systems for the purpose of detecting machinery operating state, capturing relevant process and performance data such as load and speed, and storing, trending and displaying results for plant operations and maintenance. Systems that run on resident standard plant servers or VMs and rely on the plant network rather than standalone autonomous systems are much easier to integrate with plant systems.

This integration improves overall accuracy of the system by ensuring that test operating conditions are met and adhered to during testing of the equipment. Test operating conditions are critical to assessing machinery conditions for several reasons.

A simple example involves the loaded or unloaded state of a compressor. When loaded, the system components are under stress, changing the forces on the bearings, gears, shafts and couplings. When unloaded, the stress is reduced or removed and changes aspects of the vibration patterns in such a way that it can actually indicate a fault such as bearing wear if such patterns were exhibited while the machine was loaded.

Conclusion

When considering the many configuration options surrounding remote monitoring via wireless sensing devices and remote monitoring of plant performance and condition information via hosted services or remote access, a number of benefits and challenges have been presented and discussed. This is by no means an exhaustive and complete listing. Benefits can be very significant resulting in advanced notice on machinery problems that can have devastating financial and safety ramifications and challenges are being addressed through new products and innovations very rapidly.

Author

Joe Van Dyke, P.E., Vice President, Operations & Business Development, Azima DLI

Joe manages commercial and government engineering activities for AzimaDLI and is a member of the company's senior management team. Joe is the original designer and developer of the automated diagnostic system software that is contained in the ExpertALERT™ predictive maintenance systems. Joe is a recipient of the US Department of the Navy's Reliability, Maintainability and Quality Assurance Award in recognition of the contribution to the overall fleet readiness made possible through the development and deployment of Azima DLI's ExpertALERT software. Joe holds a master's of science degree in mechanical engineering from the University of Washington and is a licensed mechanical engineer for the State of Washington. He is the author of several papers on the subject of automated diagnostic techniques for machinery.

