**HiIoT / INFRASTRUCTURE**

This isn’t your father’s Internet. For manufacturers and other industrial production companies, the industrial internet of things (IIoT) promises unprecedented opportunity to manage assets and processes in real time from virtually any location and to connect disparate systems, teams, and sites. But to create the kind of hyper-responsive manufacturing environment that the IIoT enables, you need a robust network infrastructure that will support assorted smart sensors and actuators, augmented reality technologies, and more—and do so seamlessly and securely.

If you’re unsure whether your network is up to snuff to handle IIoT demands—and how to get there if it isn’t—you’re not alone. “I feel like (the IIoT) is still a mystery” to a lot of end users, says Heitor Faroni, director of solutions marketing at Alcatel-Lucent Enterprise (www.enterprise.alcatel-lucent.com), a provider of enterprise communication products and services. “They don’t know much about the technology.”

As you seek to discern what your organization needs to make the IIoT a reality, then, here are four considerations you should keep in mind.

1. **THINK “BUILT TO LAST”**

The IIoT relies on the use of smart, connected endpoints (e.g., sensors and actuators) that track and monitor real-time performance of machines and processes. If you’re looking to increase the number of these endpoints and you’ll need to add more routers, switches, and access points in tandem, make sure that the hardware in this second category is industrial-grade, too, urges Faroni. In a paper earlier this year, “Manufacturing a Digital Future – Avoiding the Roadblocks on the Way to the IIoT,” Faroni noted that this enabling hardware needs to be “hardened to operate in more extreme conditions” and able to withstand heat, electromagnetic interference, and other challenges commonly found in manufacturing environments.

“A hardened network based on rugged components is vital in ensuring a reliable and secure manufacturing network, while being able to easily expand the network to incorporate new assets and technologies as they become available,” Faroni wrote.

The importance of making sure that IT assets are sufficiently ruggedized for an industrial environment isn’t always fully appreciated—and that can spell disaster, because as Faroni notes, “(even) minimal network disruption... can have ramifications along the entire production line.” When it comes time to select IIoT-enabling assets, then, be they routers and switches or sensors and actuators—it’s a good idea to get input from all relevant stakeholders, suggests Larry O’Brien, vice president of research at ARC Advisory Group (www.arcweb.com).

“I think particularly the people at the plant level or the field level that are going to be using this technology, a lot of times they’re out of the loop,” O’Brien says. Everyday users know what kinds of conditions they and their machines face day to day, and they’ll be able to provide valuable feedback on what they need from a connectivity standpoint and the rigors that any new technology or device will have to withstand to be reliably useful.

Think of it this way. The average consumer in the market for a new smartphone may not know exactly how much data he or she needs in a month, but knowing whether/how often he or she anticipates streaming video, gaming, etc., and where the phone will be used can help guide him or her to an appropriate device and data plan.

So, “don’t leave those people out” of critical purchasing and implementation decisions, O’Brien says. “Everybody that’s going to be affected by implementing (solutions) like this, they’re all stakeholders; they all should be involved in some way.” whether they’re an operator, an engineer, a field technician, or a plant manager, he says.

Jim Mansfield, group manager for the automation process control group at Faith Technologies (www.faithtechnologies.com), echoes the sentiment. During the “discovery phase” of a network infrastructure upgrade project, in which an organization’s existing capabilities as well as its needs are assessed, pulling a multidisciplinary team together is vital, Mansfield says.

“It’s really imperative in a production environment that the key plant personnel, including the plant manager, break down the communication barrier that often exists with the IT and IS teams whether it’s corporate or at the plant level. That has been something that is very difficult, and it has to do with ownership of data and ownership of network security, or who needs the data and why and when.”

Alcatel-Lucent’s Faroni adds that IT needs to understand the priorities of an organization’s different lines of business. “What you want to avoid is what we call shadow IT, where IT is not responsive and (operations teams) see them as a roadblock and they just don’t allow in, they develop their own solutions,” he says. “It’s important they cooperate and have a well-planned evolution of their network.”

2. **CONNECT ALL THE DOTS**

The most advanced monitoring and diagnostic capabilities in the world mean nothing if the network is down or if service is spotty where you’re working. It can’t be overstated: “Connectivity needs to be reliable; it needs to have no latency,” Faroni says. For the IIoT to deliver on its promise of improved productivity and to become “a strategic part of your corporation,” he says, reliable, pervasive connectivity is essential.

What exactly does pervasive connectivity mean? It means high-performance wired and wireless connectivity anywhere in the plant, says Faroni. Connectivity should be seamless independent of the medium, he says, and it must be both secure and robust enough to support all of the applications you’re looking to run on the devices you’re looking to use.

“Some (organizations) are just concerned about what is the cheapest suite and what is the cheapest WiFi solution that they can find because they’re only looking at connectivity,” he says. “But now you need to look beyond that—what about security? What about creating a level of service necessary for the applications?”

3. **KEEP CALM AND CEDE CONTROL**

For manufacturers, moving to a managed-service cloud-based infrastructure can offload some of the heavy lifting of data storage while supporting anywhere, anytime data access and data-sharing. But companies moving to this model (and especially to a public cloud) from running their own data center need to be aware of the shift in control that it entails, says Tom Cibelli, a solutions engineer who manages the cloud solutions team at Bentley Systems (www.bentley.com).
"A lot of times they don’t anticipate the loss of direct control over their infrastructure and the direct response to that infrastructure," Cibelli says. "You can make everything an emergency when you’re running it yourself with your own staff, but it’s not quite so easy when you’re working with a managed service.”

4. CERTIFY AND VERIFY
Adding more points of connection on the shop floor, in the warehouse, or in the office means adding more points of potential security risk. Faroni notes a recent example, reported in The New York Times in January, of a hotel in Austria that found its smart electronic key system (as well as the hotel’s reservation system) hacked and taken down by ransomware. Hotel guests weren’t able to get into their rooms, and hotel management wound up paying the ransom to get back up and running.

High-tech doesn’t have to mean high-risk, but in a world of ever-evolving security threats, what do you need to know and do to ensure your network is secure? “I’d highly recommend investigating two things off the bat,” Bentley Systems’ Cibelli says. “One would be a certification path, specifically an ISO 27001 certification path.” (Per the International Organization for Standardization’s website, the ISO/IEC 27000 family of standards provides requirements for an information security management system.)

“Even if (organizations) don’t get that certification,” Cibelli says, “it will provide a good road map for the kinds of things they should be thinking about and asking about as they build out their cloud-based system or evaluate other cloud-based systems to put their data in.” Along with that step, says Cibelli, “I would strongly recommend a security and compliance-based tool that has multiple features.”

Cibelli and Faroni both note that even as security threats and threat vectors expand, most organizations aren’t adding IT personnel to assess and address these. “Every organization I’ve talked to, they’re never growing people” to deal with information security issues, Faroni says. “They’re staying the same or they’re reducing.” So in looking for tools as well as service providers to help manage security risk, make sure that solutions are scalable and that they enable your IT department to support growing security needs.

“You’ve got to have the right tools, the right procedures, and the right policies in place to allow existing headcounts or incremental increases in headcount to match the exponential increases in threat vectors and malicious agents,” Cibelli says.

From a cloud perspective, “There’s always a lot of focus on security and therefore compliance of cloud-based systems,” says Cibelli, “but I would say over the past couple of years there has been a consolidation of what that compliance and what that security should look like, what are the minimum barriers of entry, what are the kinds of questions that (a vendor will) need to answer before someone will agree to allow you to essentially host their data.”

Chief among the questions that prospective buyers should ask, according to Cibelli: What certifications or compliances do your systems hold or support? Besides ISO 27001, SOC (Service Organization Control) 2 Type 1 and Type 2 reports on nonfinancial controls relating to security, availability, privacy, and more are growing in importance, Cibelli says.

Ensuring that your organization and its security partners undergo third-party security audits to check whether security tools are operating – and of equal importance, being used – as they should is a critical step, too, he adds. At Bentley Systems, “we regularly yet our security policies and procedures via external audits to verify we’re doing what we say we’re doing,” he says.