IoT Transforming The Industrial Sector

Jeff Reinke, Editorial Director

The Internet of Things has already been a positive disruption for U.S. manufacturing, and a number of indicators show that we're just getting started.

The use of data, big data if you prefer, can take on many forms. My preferred application is its ability to paint a clearer picture of what is important and provide clarity from what can be a haphazard collection of ledger lines, surveys, reports and projections.

When it comes to breaking down the multi-faceted components, resources and benefits the Internet of Things encompasses, its portrait offers an intriguing display of opportunity, investment and concern. IoT's surge into the everyday lives of nearly every person represents significant social and cultural change, with its impact being felt in numerous areas. Today, we're going to stay focused on how the IoT will specifically impact manufacturing.

For manufacturers, the IoT refers to an infrastructure or network that's been constructed so a variety of unique devices, machines, software platforms, etc. can be connected – either physically or remotely to access and share all of the data being generated. This advanced connectivity translates to an abundance of operational, supply chain and purchasing information that can be used to analyze a multitude of factors both historically and in real-time.

Globalization Brings IoT Closer to Home

Improved market conditions, along with goals that include shortening time-to-market and expanding asset utilization, have led manufacturers to invest more heavily in infrastructure and operational systems that allow for competing in an increasingly global marketplace. Much of this investment is tied to new equipment, software and data accessibility.

As these new pieces of the operational puzzle have been added, they essentially represent new data points and connections within the manufacturer's information network. Guido Jouret, vice president and general manager for Cisco's Internet of Things, offers this perspective.

"Separate networks or even work cells are being challenged by a convergence of connectivity. Bringing all the different assets together used to be more complicated, but today we don't have to worry about physical connections. It's about software on servers that can be housed anywhere and connected by an Ethernet network. We've moved from physical to global, virtual connections. The challenge used to be figuring out where to house the network and how to establish connection points. Now, manufacturers need to figure out where they want to manage their assets from and where the servers storing all that data should be located."

Data supplied by Rockwell Automation and Cisco Systems demonstrates the impact that IoT activity currently has, and will continue to have. From a global perspective, IoT represents a $14 trillion opportunity, with manufacturers potentially gaining the largest amount – 27 percent. Over half of U.S. manufacturers will be on the cloud in less than two years.

One of the driving forces that also makes IoT more feasible is the growth in mobile device use on the plant floor. It's estimated that 63 percent of all businesses are currently implementing policies around BYOD (bring your own device) and 50 billion smart devices (not all specific to manufacturing) will be in use by 2020. They've seen a faster adoption rate than electricity or telephones.

Jouret feels the trend of more and more manufacturing enterprises encouraging BYOD practices represents equal parts opportunity and concern. "BYOD brings us back to convergence," he states. "These devices not only allow for connecting to apps for plant operations, but personal ones as well. For example, basic programs for e-mail can tax the bandwidth used for operational purposes. This had led to the implementation of distributed computing that allows separate routers to differentiate between personnel and production needs."

These types of solutions place less strain on the network, but obviously call for additional investment. More devices on the plant floor also creates new challenges that are being written and defined by the IoT movement.

According to Rockwell Automation, over $60 billion was spent on global security in 2011. This is projected to grow by more than 20 percent by 2020. So accompanying all of this device use is the obvious need to keep them, the network they're accessing, and the data being reviewed secure.

According to Jouret, the only secure device is one that's turned off, so the challenge is combining enterprise security with ease of access. In the past, providing or denying this access was defined by the device and the software it used. The network could understand both and therefore infer whether or not to approve access.

"The logic was put in place so the software could automatically connect, eliminating another step for plant floor personnel," he states. "Over time this morphed into automatic or default settings on too many devices. The challenge we now face deals with figuring out how much can be automated without losing control.

"I like comparing it to cruise control in a car. You have to trust the mechanical systems of the vehicle when the cruise control is activated, but there is always a switch that can be flipped to resume manual control. Similarly, there needs to be options for network security. While the network needs to function smoothly and provide easy access, measures must be put in place to ensure employees can't unknowingly make things worse or less secure."

Traditional approaches have focused on keeping hackers and other outside sources

from breeching network security. Jouret offers a different take on how manufacturers can ensure they will not be left exposed by all the new connections which define the IoT.

“You can have security and connectivity if we change the way we do things. Instead of thinking that we need to erect a high wall to keep people out, the bigger threat is on the inside. Software updates on robots or equipment is usually done by connecting to the manufacturer’s server or via a USB brought in by a tech. These are all potential security issues.

“It was recently reported that 50 percent of utilities in the U.S. have found Stuxnet running on their networks. It got there through infected USBs used by techs when updating firmware. So security must be designed with walls within walls, protecting cells or connections from each other. Plants also need to ensure the right people are accessing the plant. Cisco has mandates in place that require the correct badge be shown before someone can connect to a network.”

The growth in connections and security measures runs the risk of impacting reliability, which is obviously crucial in the manufacturing world. “If it’s done right, you can have convergence and reliability,” he states. “If the communication amongst devices is somewhat limited, i.e. a robot only needs to talk to the local controller, then you’re meeting all the goals of not over-tasking the facility bandwidth, eliminating unnecessary security risks and maintaining a high level of operability.”