Designing Security into the Connected Industrial Enterprise

contents
To connect securely or not to connect, that is the question............S2
Benefits of Connectedness..............S3
Interconnectedness: How to Address the Risks..................S5
The Connected Enterprise Vision from Rockwell Automation ..........S6
Research Shows Manufacturers Emphasize Data Security...............S7
For many manufacturers, integrating plant floor data with enterprise systems poses sufficient challenges, let alone bringing Internet connectivity to their production operations. It’s no secret that one of the biggest reasons manufacturers are hesitant to connect plant floor systems to the corporate network and extend Internet connectivity to production data is security.

However, providing corporate planners, sales staff, extended supply chain and customers access to certain plant floor data promises significant business value. For this reason, seamless and secure connectivity between isolated production systems and processes throughout the entire value chain has long been a goal of manufacturing and production enterprises.

By bridging the gap between plant-level systems and office-information systems, manufacturers that adopt the vision of a connected enterprise are able to improve planning, sharpen visibility into work in process, and better manage risk. Through improved utilization of operational data, industrial companies are able to achieve greater productivity, fuller utilization of assets, and better decision-making.

These are among the benefits deriving from the broad vision of enterprise information—connecting the plant floor with enterprise systems in a secure fashion utilizing new technologies such as mobile devices, the cloud and virtualization to manage such big data. Clearly, the convergence of technologies including the Internet and Ethernet, along with interoperability standards such as XML, is having an impact on the enterprise, allowing the reliable and secure meshing of systems in the plant with the office. For example, real time monitoring of devices on the plant floor enables

To connect securely or not to connect, that is the question.
Designing Security into the Connected Industrial Enterprise

companies to make better decisions on energy consumption material management, or quality control. Industrial firms are seeking to reap the benefits that make these technologies worthwhile investments.

But along with the gains afforded by this level of connectivity come certain risks. One is the potential for loss of intellectual property. For this reason, many companies are reluctant to put their plant information on the corporate intranet. There also is the possibility of industrial sabotage. And there is the chance of an inadvertent breach of data due to employee carelessness.

Nor is it realistic for manufacturers to take a “head in the sand” attitude going forward. Every day the momentum driving the connectivity of things increases. The world is moving inexorably toward an ever expanding, interwoven electronic fabric that has been labeled the “Internet of Things.”

Also referred to as the “Programmable World” in the June 2013 issue of Wired, this view of a fast-approaching future envisions sensor-equipped objects surrounding us at home, on the road, at the mall, in the office, and in the plant, constantly providing updates, feeding information to us and others for faster, smarter decision-making. Rather than being directly connected to the Internet, most of these devices instead will communicate through simple wireless protocols. Some have called it the “Sensor Revolution.” Unfortunately, with each additional connection of a device, a system, a plant, or a company comes a loose but expanding array of cyber risks posing a threat to the functioning of each part and its larger network.

In industrial organizations, the network’s data flow often is essential to the functioning of critical processes, machinery, or systems on which the company depends. Thus, Cybersecurity—rather than being an option—becomes a necessity, a critical piece of every system in the organization.

Given these realities, what benefits of the connected enterprise are being realized today? How far along are manufacturers toward achieving this vision, and how are they dealing with the Cybersecurity risks? How can manufacturers adopt this vision while ensuring that plant floor data is secure? Finally, how can industrial automation vendors guide industrial organizations to realize this vision of connectedness and security?

Benefits of Connectedness

Integrating plant floor data with the enterprise and beyond offers new capabilities to various parts of the organization that previously were either not possible or too time and cost intensive. Internally, the ability of a sales representative to check the status of a customer’s order and give an exact completion and shipping time can be invaluable to the customer relationship. Externally, enabling a vendor to have electronic access to a manufacturer’s just-in-time requirements facilitates the smooth flow of parts required in a lean manufacturing environment.

For many industrial companies, the ability to have enterprise-wide visibility into production data can pay off in numerous ways, including energy savings, better inventory management, and improved throughput. Often these goals are realized through visibility into operations, collaborating with suppliers, and reducing IT costs through utilization of cloud-based services. Finally, the ability for customer-facing staff to leverage mobile devices, the Web, and the cloud to access plant floor information has become less the exception and more the rule for today’s industrial enterprise.
The cloud offers particular benefits for industrial enterprises that depend on remote monitoring of devices. An example of this is Hilcorp Energy Co., which operates an oil drilling rig off Alaska’s Kenai Peninsula. The company is using the Virtual Support Engineer service from Rockwell Automation. Leveraging Microsoft’s Windows Azure cloud platform, the service allows Rockwell Automation engineers to remotely monitor secure information provided by the Hilcorp network of medium-voltage drives to predict potential failure of these units in the field.

Following an upgrade to electrical pumps, the company wanted to ensure that when a piece of equipment incurred a problem, they would be able to quickly identify and fix it to get back on line. In a recent field incident, when a well tripped offline, a Rockwell Automation specialist thousands of miles away identified the problem immediately, enabling the company to fix it in under 15 minutes, versus what normally would take six hours. After seeing the value of the connected enterprise, the company shifted from a pilot project to a broader application of this technology.

Another company leveraging the connected enterprise is M.G. Bryan, a manufacturer of heavy equipment and machinery for the oil and gas industry. The company tapped cloud computing for remote asset management of high-tech fracturing equipment. Designed and integrated by Rockwell Automation, the new control and information system uses the Microsoft Windows Azure cloud to provide real time information and automated alerts.

The company wanted the capability of remotely monitoring its fracking trucks, which often run in remote areas where there are no IT servers or Internet connectivity. Using a gateway into the cloud via cellular or satellite connections, M.G. Bryan was able to analyze its in-field service information to provide remote service and preventative maintenance.

The solution also opened the door to a new business model that reduces project risk and cost of production, while improving time-to-value for these fracturing vehicles. M.G. Bryan can now monitor vehicle use by the minute, hour and day, and has changed its leasing agreement from the industry-standard monthly agreements to a pay-by-use model. The company’s customers no longer need to rent equipment by the month, paying the same price for those vehicles that pump 24/7 as they do for backup trucks that never see any action. Vehicle rentals have spiked as a result.

With this cloud-based solution, the company has a highly scalable, cost-efficient method to store and remotely access real time information to help extend equipment lifecycles and provide improved value to customers.

Leading manufacturers have found that by integrating their manufacturing execution system (MES) with the company’s ERP system, business people can tap into the production information they need to make better decisions. For example, Rockwell Automation MES solutions integrate smoothly with ERP systems as well as with automation devices on the plant floor and include pre-built libraries and information workflows speeding time to value. Rockwell Software MES suites adhere to both S95 standards for integrating with the enterprise system and S88 for connecting with plant automation systems.

In fact, broader visibility into plant floor operations is a key goal of today’s MES. In addition to tying the classic execution systems with the information systems to provide business people with the information they need to make better decisions, manufacturing intelligence software allows companies to transform and contextualize data accessed via common web clients from the plant floor systems.

One of world’s largest aluminium smelters—The Emirates Aluminium Company Ltd. (EMAL)—used Ethernet-to-the-Factory to improve manufacturing efficiency. Achieving their goals demanded a control network for smelting
operations, as well as the ability to share control data with manufacturing execution systems (MESs) and the company’s enterprise resource planning (ERP) system. Although each production area needed its own discrete network to isolate it from problems in any other area, overall efficiencies could only be maximized by sharing information. The challenge was how to converge these disparate networks without compromising resilience and security.

EMAL knew that the traditional approach to manufacturing plant networking would not deliver the truly integrated, but discrete, model that the company needed. In meeting these needs, the company looked to take advantage of the strategic alliance between Cisco and Rockwell Automation. Taking an architectural approach is enabling EMAL to significantly improve plant efficiency.

Information that previously was not available, either because it was isolated or because it relied on manual collection, can now pass between the plant and the office, enabling schedules to be adapted and potential barriers removed. The new generation of systems being developed to improve plant efficiency means that it is important that those plants have a robust, flexible, scalable, and secure network architectures in place to make best use of them.

This enterprise-level reporting of operational information—about process compliance, error rates, production-line anomalies, material consumed, and work-in-process—provides value to decision makers, whether they are in sales, production scheduling, or quality control. Indeed, this is a prime example of how a greater level of connectedness allows companies to get more value out of their existing MES or manufacturing intelligence solutions through broader enterprise-wide reporting of the data. In today’s world, information-savvy industrial companies realize they need this kind of manufacturing intelligence not only to run their operation, but to remain competitive.

Interconnectedness: How to Address the Risks

Industrial control systems pose special issues for companies seeking to leverage the benefits of connectivity while limiting possible risks. Many industrial control systems already include logical and mechanical provisions designed to enhance their safety and reliability. Often these systems are comprised of a mix of old and new components that change slowly over time, so that a common scenario on the plant floor is a mix of old equipment and new systems. For complex control systems, the shift to greater connectivity and data accessibility unavoidably results in greater exposure to a new set of cyber risks.

In today’s technological environment, as companies become more connected both internally and externally, the possibility of security problems increases, requiring an industrial security strategy that is deeply entrenched within both the plant and the broader enterprise. Process automation systems that once were built upon isolated, proprietary networks today are becoming part of larger corporate networks and enterprise systems.

These interconnected systems work best when they are based on open architectures using the standard internet protocol (TCP/IP) to facilitate interoperability with various other systems and applications. Although this

About CISCO

Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. For ongoing news, please go to www.thenetwork.cisco.com.
openness and increased flexibility offers significant advantages to today’s enterprise, it also opens the door to threats directed against the company.

To guard against such attacks, security cannot be implemented as an after-thought or bolt-on, but rather should be designed into the devices, the control systems, and the networks that make up the automation environment. Nor is there any going back to a closed system that denies management’s need for real time production information. Instead, companies need to take a holistic view of industrial security—addressing people, process and technology-related risks—to maintain operational integrity and protect the company’s most important operational assets.

Industrial security by necessity requires a “defense-in-depth” strategy addressing both internal and external security threats. A defense-in-depth security architecture is based on the premise that any one point of protection or single firewall may, and most likely will, be penetrated by the persistent attacker over time. The solution is to adopt multiple layers of defense—physical, electronic, and procedural.

Thus, multiple layers of network security can protect networked assets, data and end points in the same way that multiple layers of physical security can protect high-value physical assets. Under this scheme of defense:

- Security is designed into the infrastructure and becomes a set of layers within the overall network security;
- Attackers must first penetrate or circumvent each layer of security without detection; and
- Any point of vulnerability or flaw in one security layer can be backstopped by different variables or capabilities provided by other layers.

The Connected Enterprise Vision from Rockwell Automation

Rockwell Automation has laid out a security roadmap to enable manufacturers to create and implement a security policy that reaches all the way down to the level of the individual device, whether it’s a sensor on the plant floor or a smartphone in a sales representative’s hand. This vision contrasts with the more common approach of securing the plant and enterprise systems separately.

The explosion of data at the plant level—in production drives, servos, and PACs—warrants a high level of security to ensure that product and process information remains adequately protected. Although the PAC was the central point of information on the plant floor in the past, today’s automation environment in manufacturing includes a variety of more powerful devices. Through the Rockwell Automation vision of the connected enterprise, much of this plant floor data can be accessed via smartphones and other devices, allowing the information contained in the machine zone to be shared by others in the enterprise.

A key difference in this approach is the inclusion of security down to the device level. By contrast, in much of the industrial world, it is commonly accepted to have security at the PAC level or at a machine level as a zone, but no security at the device level. Thus, while manufacturers are in the position of wanting access to the information contained in a device, they typically remain unconcerned or unaware of the possibility of an intruder hacking that device to obtain process secrets or to do unexpected damage to equipment or personnel.

Rockwell Automation has teamed with Cisco and other industry leaders to enable manufacturers to build a security environment that addresses the needs of the industrial system and links the enterprise all the way to end devices on the plant floor. Their goal is to help manufacturing companies become more responsive to changing market and operational conditions without sacrificing security.

Industrial firms can reap the benefits of the connected enterprise in a secure fashion by specifying that all devices utilize the common networking technologies of Ethernet and Internet Protocol (TCP/IP), the most important networking technologies in use globally today. EtherNet/IP is the world’s leading open industrial Ethernet network designed to connect across systems and subsystems and from the end customer’s IT infrastructure to the instrumentation level. EtherNet/IP uses the same Ethernet and TCP/IP protocol suite that is used for email, the Internet, and other commercial applications, providing the performance, resiliency, and security of traditional fieldbus solutions.

To make this solution a reality, plant managers and operational staff at manufacturing firms must become more fully educated and aware of the need for an enterprise-wide security environment. Only by securely connecting plant floor automation systems with the enterprise are companies able to make production data available in a secure fashion to the business, suppliers, and customers via the cloud and other technologies.
Research Shows Manufacturers Emphasize Data Security

In an effort to assess the level of connectivity of current plant automation systems as well as manufacturers’ level of concern over Cybersecurity, Rockwell Automation teamed with IndustryWeek Magazine to survey a sample of the manufacturing community on these issues.

The group surveyed were generally representative of a broad cross-section of the U.S. manufacturing community, with about a third (32%) of the companies having sales of $1 billion or more, and the largest group (44%) with sales of $100 million or less. They represented all kinds of industrial firms, with the largest groups represented being industrial machinery (15%), and automotive and aerospace (both 11%).

In the September 2013 survey of 265 executives, managers, and other employees at manufacturing companies, three out of four respondents indicated that their companies placed a high importance on data security. However, this same group of manufacturers exhibited a general lack of awareness of both the benefits of the connected enterprise, and the Cybersecurity risks associated with it.

Regarding the benefits of plant floor connectivity with the enterprise and the Internet, manufacturers responding indicated a mixed level of awareness. When asked how valuable Internet-enabled equipment is for various aspects of the manufacturing process, nearly half (47%) indicated that they saw little or no value to be derived from Internet connectivity to the plant floor for improving demand-based order response rates. In a similar fashion, nearly two out of five (39.4%) said they could see little or no benefit from connecting the plant floor with the Internet as a means to improve their supply chain efficiency.

Most manufacturers reported having minimal or no connectivity between the plant floor systems and the company’s network or enterprise systems, let alone any Internet capability. For instance, just 14% indicated that their plant or production operations data collected on the plant floor was fully integrated into their enterprise information system. Another 12% reported that their production systems weren’t connected at all with the larger enterprise. (See figure 1)

As far as Internet connectivity goes, about one-third (30%) said their plant floor systems had none. Another third (31%) reported that one fifth or less of their automation systems were Internet-enabled. Similarly, when asked what percentage of their plant floor machinery was connected to the company network, either through Ethernet cables or wifi, almost two-thirds (65%) said less than 40% of their automation systems were tied into the company network. (See figure 2)

Regarding barriers to enabling machinery on the plant floor to have Internet connectivity, companies cited three reasons almost equally: cost (42%), security (40%), and lack of need (40%). In other words, industrial companies need first to be made aware of the benefits to be derived from such an investment, as well as how to overcome the potential security hurdles such connectivity would entail. (See figure 3)

Perhaps equally telling from an awareness standpoint, very few manufacturers (6%) reported having experienced an incident of plant floor data being compromised due to an intentional or unintentional breach in security. Of course, it’s possible that some companies were unaware that such a breach may have occurred, and some may not have wanted to admit they’d experienced a serious lapse in security procedures. (See figure 4)
The more data you can collect, the more costs you can recover.

Good information is good. More and better information is, well, better. Collect the right data at the right time from disparate sources. Then deliver it in the right form to the right people at the same time. Organizing and synchronizing information at high speed saves real money. What could be better?

Learn more and see strategy in action
discover.rockwellautomation.com/mi