About the Industry Essentials Series
The mission of the Industry Essentials series is to provide industrial professionals with an up-to-date, top-level understanding of a range of key industrial automation topics. Our intent is to present essential engineering concepts in a practical, non-commercial fashion, together with a review of the latest technology and marketplace drivers — all in a form factor well suited for onscreen consumption. We hope you find this first edition on Network and Security Services useful. Check back for other installments in the months to come.
—The Plant Services Editorial Team

This Plant Services Essentials guide is made possible by Rockwell Automation. See page 9 for more information on Rockwell Automation’s full range of network and IT security solutions.
Sensitive data, critical control instruction, and proprietary business information travel over networks of all types — from internal industrial networks to the Internet — each with its own level of encryption. How secure is it? This installment in the popular Essentials series will help you to understand the impact of the skilled worker shortage on manufacturing network security, how to put the proper infrastructure in place, which factors to consider when implementing virtualization in a manufacturing environment, which needs to satisfy for secure remote access, and where the Industrial Internet of Things affects an organization’s network security.

As our world becomes more connected, fewer and fewer people are on-site, yet they still need to access data securely. Remote access to production assets, data, and applications needs to be secure. The ability to bring together skills and resources for collaboration, independent of physical location, is a big benefit to manufacturers. Enabling secure remote access to plant-based applications and data offers the ability to share information and collaborate internally and externally. Building the right infrastructure with the right design principles ensures security, so the wrong people can’t traverse the entire network.

In addition to off-site workers, many maintenance, reliability, and control engineers will retire in the next few years. They understand the systems and machines in their facilities, but replacing them and their experience will be difficult. A robust remote support strategy will allow access to expertise anywhere in the world. Being able to connect equipment and monitor it and gain access to expert analysis, regardless of location, can be advantageous, but network security is top of mind. The skilled worker shortage is a demographic challenge in replacing those workers with people who understand IT and OT.

Putting the right infrastructure in place allows organizations to more proactively monitor their networks. Multiple networking technologies and types exist and each plant has legacy control networks and islands of automation. The first step in evaluating your infrastructure is assessing what you have. Most facilities don’t fully understand their current state because it was never documented. Following an assessment, networks can be repaired, updated or replaced to strengthen the infrastructure. A well-designed plant-wide network will give the scalability, flexibility, and efficiency to increase productivity and decrease downtime.
INDUSTRIAL IT PAIN POINTS

Three major pain points are associated with industrial IT departments. They are inefficiency, vulnerability, and inflexibility.

**Inefficiency:** Industrial IT infrastructure has evolved over the decades with multiple proprietary protocols, islands of automation, and limited capital funding. The resulting lack of standards, knowledge and documentation contributes to a higher mean time to repair (MTTR). The challenge of solving a communication issue within this complex operating environment is time-consuming during project commissioning and more costly when the maintenance team is facing an unplanned downtime event.

Further compounding this challenge is the quest for more actionable information. As the manufacturing economy grows, so do concerns about the availability of enough people with the right skill sets to support the growth. Today’s leaner staffs are already stretched from monitoring and responding to changing conditions. The result is that industrial data, which is growing exponentially with the proliferation of new data-generating smart sensors and devices, can be difficult to access without an efficient industrial infrastructure.

With only 10% of industrial operations already fully integrated with their enterprises, there’s a huge productivity gain to be realized and a competitive urgency to capture it.

**Vulnerability:** Security within the industrial environment has been an afterthought for companies. The control system is no longer an isolated operation, and industrial organizations are recognizing that a seamless flow of information created by connecting industrial control systems to the enterprise is a path to significant operational improvements. But with these benefits come new challenges. Cyber risks from both internal and external sources expand with each new connection, creating threats capable of disrupting control system operation, safety, productivity, and the ability to protect assets, machinery, and information. These
threats have the potential to strike at the heart of a company’s reputation and its long-term viability.

Companies can mitigate security risks, improve uptime and availability, and protect people, corporate assets, and information if their company-wide security program is based on sustained investments in technical and non-technical controls and governance programs.

Unless companies make ongoing investments in secure industrial infrastructure that help address people-, process-, and technology-related risks, they may be exposed to unnecessary risks as they capitalize on the technology opportunities.

**Inflexibility:** Over the next decade, the global population will exceed 7.6 billion and more than 70 million people annually will cross into the middle class. This expanded middle class will add $8 trillion in consumer spending, which means more demand for products and resources from manufacturing and industrial companies.

Price pressures will force companies to address the inflexibility of their infrastructure to stay competitive. Isolation inhibits competitiveness. Non-integrated environments will not be able to keep up with the demands for capturing and transforming real-time and historical data from intelligent devices and multi-disciplined control into actionable information. To remain competitive, nothing can be isolated anymore, and a flexible architecture is fundamental to converting islands of automation to integrated, responsive operations; moving from simply automating labor to leveraging information; changing pockets of expertise to global collaboration; and mitigating risk by transitioning systems from open to open-and-secure. A flexible, scalable industrialized IT infrastructure is needed to manage the data; and a governance and security framework is needed to trust the data.
**DISRUPTIVE CHANGES**

**The Connected Enterprise**

The connected enterprise brings major advances in information technology — the Internet of Things, the proliferation of smarter endpoints that are both valuable and vulnerable, cloud computing, Big Data and analytics, virtualization, and mobility — to life in manufacturing and industrial settings. A connected enterprise consists of industrial operations that are integrated, optimized, and secure at the machine and equipment levels, throughout the organization, and across the supply chain, enabling connection and collaboration among global and remote operations, assets, and users.

Bringing IT goals and industrial manufacturing goals together is fundamental to the connected enterprise. This is achieved by delivering a control system network infrastructure based on standard, unmodified Ethernet IP — the same protocol that is used for the Internet — combined with best practices, modern automation technologies, information software, and professional services that help customers reduce risk and improve performance.

Integrated control, network, and information solutions break down barriers securely, providing access to data that has traditionally been trapped in operations’ historians and contextualizing data to provide the right data to the right people, creating actionable information related to KPIs and improved business value, including production throughput, process quality, asset health, and energy efficiency.
Industrial Internet of Things

The Internet of Things (IoT) has been estimated by Cisco CEO John Chambers to create $19 trillion of potential business — $14 trillion in the private sector at stake and 27% of that value will be in manufacturing. The IoT describes a network of physical things — from consumer products to industrial machines and equipment — connected to one another through the Internet.

The connected enterprise could exist and has existed without the Internet of Things, but when it takes advantage of the IoT its value is exponential. For instance, a connected enterprise can leverage the Internet of Things to more easily tap and interconnect intelligent devices on open networks and allow data from those devices to be cost-effectively shared by a much broader set of users throughout the manufacturing/industrial supply chain using technologies such as cloud, mobility, and visualization.

Cloud and Virtualization

Cloud and virtualization allow improved productivity and business intelligence, whether deployed on-premise or off-premise, self-hosted or hosted by a third party. Within the industrial enterprise, for example, an off-premise cloud-computing platform allows an industrial equipment builder to offer its customers product enhancements, such as remote monitoring and data analytics. An industrial operation’s remote or field-based equipment’s control and information system can leverage an off-premise cloud-computing platform to help provide secure remote access to real-time information, automated maintenance alerts, and service and parts delivery requests. Enabling companies to move industrial applications off-premise and host them at remote data centers shifts capital expenditure outlays for industrial IT infrastructure to more flexible and scalable operation expenditure outlays.
**Mobility**

Mobility addresses the industry desire for context-based information available on whatever device — smartphone, tablet — the user chooses, as well as smart devices with mobile sensors that can transmit location-based data. Employees with access to business, production, and supply-chain information can deliver greater productivity and value throughout the day. The growing adoption of mobile devices such as tablets, wireless laptops, and smartphones in the consumer world has been a catalyst for change in the industrial sector. Mobility means more than smartphones, tablets, and wireless laptops. It also includes smart devices with mobile sensors that can transmit location-based data when the device is in motion. When near a “receptor,” data from these smart devices with mobile sensors is captured, retransmitted to a data processor, and collected in a historian for analysis.

**Big Data**

Big Data and analytics are becoming increasingly important to support collaboration, decision making, and better ways to serve customers in the connected enterprise. In fact, due to advanced automation, manufacturing, and industrial operations generate more big data than any other sector. For example, a typical oil rig generates more than 1 terabyte of data in a single day. Today, this data is used mostly for control and operator interface; however, this real-time data is very rich in important information such as asset health, performance, and energy efficiency. By analyzing production data, hidden inefficiencies can be discovered, and changes implemented to improve productivity and product quality, and overall customer service.
MOVING FORWARD

The next steps to network and security harmony involve the IT infrastructure. There are many smart devices or assets in a typical plant or industrial facility, but historically data has been trapped in those assets due to disparate automation technologies, machines, and equipment from many different machine builders or equipment builders, legacy and proprietary communications systems, and an inability for devices and controllers to add context around data and turn it into useful information.

A plant-wide approach will establish a secure environment that both protects the industrial control system and links endpoint devices in manufacturing and industrial operations within the enterprise and supply-and-demand chain. The plant-wide approach enables solutions and technologies including virtualization, mobility, cloud, and analytics by bringing scalable common network and security environments on a single, unified network infrastructure.

Infrastructure: Assess how far from industry-leading your existing infrastructure is or design a plant-wide converged Ethernet architecture to enable the connected enterprise. Improve your industrial security by applying defense-in-depth principles without impacting operations productivity based on proven architectures that scale and provide flexibility.

Enable secure remote access to leverage off-site expertise. The ability to bring together skills and resources for collaboration, independent of physical location, is a big benefit to manufacturers. Enabling secure remote access to plant-based applications and data offers the ability to share information and collaborate internally and externally.

Virtualization as a Service: Virtualization has become widely adopted as a standard in the information technology industry and is now becoming a growing trend in the manufacturing and production industries. By adopting virtualization today, you can discover benefits such as:

- reduced server footprint
- extended application longevity
- improved infrastructure reliability with management and recovery features.
This Plant Services Essentials guide on Network and Security Services was made possible by Rockwell Automation. The Industrial Data Center from Rockwell Automation can help your business realize cost savings through a pre-engineered, scalable infrastructure offering. All the hardware you need to run multiple operating systems and multiple applications off of virtualized servers are included in the cost.

Rockwell Automation also offers virtualization as a service via the Industrial Data Center with remote monitoring and administration. This VaaS-managed service allows industrial customers to achieve a secure, scalable flexible platform on premise. As a pre-engineered solution, the Industrial Data Center is designed to ease the transition to a virtualized environment, saving you time and money. The Industrial Data Center combines equipment from industry leaders that are pre-configured specifically for the manufacturing and production industries. All equipment is shipped pre-assembled and a Rockwell Automation professional will come to your site and commission the system.

Click here to learn more about Rockwell Automation’s Network Services.