CONTROL

November 2014

# ESSENTIALS OF THE CONNECTED ENTERPRISE

## About the *Control Essentials* Series

The mission of the *Essentials* series is to provide industrial automation professionals with an up-to-date, top-level understanding of a range of key 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 edition useful. Check in at ControlGlobal.com/Essentials for other installments in the series.

—*The* Control *Editorial Team*

Rockwell Automation

This Control Essentials guide is made possible by Rockwell Automation. See page 8 for more information on how the Rockwell Automation technology portfolio as well as the company's assessment, implementation and lifecycle management tools and services can help manufacturers, machine builders and other industrial companies realize the promise of The Connected Enterprise.

# THE CASE FOR THE CONNECTED ENTERPRISE

The global population recently rounded 7 billion on its way to 8 billion by 2030. And an estimated 70 million of those souls will enter the burgeoning middle class each year, placing an ever greater demand on supplies of energy, water, food, and other manufactured goods. To meet these demands, manufacturers and other industrial operations must become ever more productive even as they wring inefficiencies out of their processes and supply chains. Today's production systems already throw off data at an unprecedented rate. But the sheer volume of data—coming as it does from isolated, disparate sources—is as likely to overwhelm as it is to inform. Fortunately, advances in communications and computing technology as exemplified by the rise of the Internet of Things, Big Data & Analytics, and the Cloud promise to enhance the creation of what Rockwell Automation refers to as The Connected Enterprise.

Better information sharing can simultaneously drive better decision making, expose process inefficiencies, and facilitate compliance and best-practices collaboration. Indeed, organizations that embrace what's possible with today's rapidly advancing computing and communications technology stand to uncover new competitive advantage, even as those who do not face escalating competitive risk.

The idea of an industrial enterprise that is integrated from top to bottom and out across its distributed value chains has been with us for decades. Even as the first microprocessor-based controllers and software applications began to seep into every corner of the industrial operation, the inkling began to take hold that smartly integrating the information otherwise stranded in these isolated devices and systems could lead to dramatic performance improvements. But building these

custom, point-to-point linkages was both expensive and labor-intensive. Further, they proved relatively brittle and inflexible. As a result, only the highest priority integration projects were undertaken, and integrated systems remain more the exception than the rule across industry. For example, in a recent survey by LNS Research, manufacturers still cite disparate systems and data sources second only to lack of collaboration across departmental functions as top operational challenges.

Today, technology is finally poised to catch up with the longstanding promise of integration to expedite The Connected Enterprise. Ever smarter, more capable digital devices are converging with increasingly pervasive networks and unprecedented, on-demand computing power. In the broader technology arena, these umbrella forces are variously classified as the Internet of Things, Big Data & Analytics, Cloud Computing and Virtualization. But for most industrial organizations, the idea of terabytes of proprietary data instantly flowing to anyone anywhere is not necessarily a comforting thought. Enter Rockwell Automation and its vision for The Connected Enterprise.

In the balance of this Essentials report, we'll explore in greater detail several important dimensions of a Connected Enterprise: a robust network infrastructure based on standard Internet/Ethernet protocols; an inventory of "working data capital" that acknowledges the contextual information needs of people and systems; and network security in the form of ongoing threat management practice, policy and culture across all levels of the organization and across its supply chain.

# A COMMON NETWORK INFRASTRUCTURE

One characteristic of The Connected Enterprise is a converged control and communication architecture based on standard Ethernet and Internet Protocol (IP) technology. This does not mean that the entire site is plugged into one common network. Rather, a common architecture based on these standards makes it far more straightforward for organizations to securely integrate and manage advantageous information flows across the entire extended enterprise.

Many devices being used in industrial automation already are IP-enabled, and the IP connectivity of many more devices from the non-industrial world stand to be leveraged by adopting an Ethernet-based infrastructure. These technologies, such as tablets, video cameras and RFID readers, provide many opportunities for greater productivity, innovation and collaboration.

To take advantage of these devices, operations must allow these machines, equipment and non-industrial devices to communicate with each other via a standard, IP-centric infrastructure. The Ethernet Industrial Protocol (EtherNet/IP™) was created to support this interoperability and to ensure seamless enterprise-wide connectivity within a single infrastructure. In contrast, proprietary, or purpose-built network technologies often require gateways or other specialized translation devices, restricting and complicating network architecture. Plus, they introduce custom coding and legacy support issues.

Because EtherNet/IP™ complies with IEEE 802.3 and TCP/UDP/IP standards and conventions, it also leverages

readily available, off-the-shelf infrastructure components. This helps operations and IT professionals collaborate on deploying and maintaining a secure, reliable and robust network infrastructure within the enterprise and throughout the industrial environment. Using standard Internet and Ethernet protocols like EtherNet/IP™ helps tie operation data together with the rest of the enterprise. It also provides a future-proof communication backbone for pervasive growth in Internet-enabled devices.

As EtherNet/IP™ continues to become more universally deployed in both discrete and process automation environments, Connected Enterprises are beginning to realize the business value of the right information delivered to the right decision-maker at the right time. Indeed, new visibility into production data and supply-chain information offers the next wave in competitive differentiation.

# WORKING DATA CAPITAL

Clearly, the era of Big Data has arrived, and industrial operations lead the way in terms of sheer volume. Simply capturing that data to storage is perhaps a good start, but without context it remains meaningless.

Industrial organizations on their way to becoming Connected Enterprises should address their data strategically. Capturing more data isn't necessarily better. Instead, they should target the data that's most relevant, starting with their most critical assets. They should ask searching questions such as "What could the right data tell us if we had it?" Indeed, the true value of Big Data lies not in the data itself, but in what analytics applied to the right data reveal. In this way, raw information can be transformed into "working data capital," and put to work on behalf of The Connected Enterprise.

Once identified and/or derived, this working data capital needs to get to the systems and/or decision-makers who can put it to best use. Three particularly relevant technologies that are enabling more efficient analysis, communication and visualization of working data capital to be scalable to The Connected Enterprise are virtualization, cloud computing and mobility.

In short, virtualization and cloud computing entail the relocation of software applications from local servers to an on-premise or off-site datacenter. This can reduce local IT footprint together with associated maintenance and energy costs. From an operational standpoint,


such hosting strategies are ready-made for supervisory applications such as remote asset management, performance and energy monitoring, and supply chain collaboration. Virtualization, in which application software is effectively abstracted from its operating system and hardware specifics, is a companion technology to cloud computing on the uptake in industrial environments. While today's cloud datacenters are built from the ground up on virtualization technology, locally hosted software and systems also can benefit from the lower hardware, energy and maintenance costs of virtualized solutions.

On the mobility front, more than 60 percent of businesses already allow employees to bring devices to work, according to the Manufacturing Enterprise Communications Research Services. In fact, five terabytes of data were viewed on mobile devices in the last year. And while accessing industrial data on any tablet or smartphone is a key benefit of mobility, the ability of information and workers to be "mobile" and access applications on the go is just as beneficial.

# SECURITY THROUGHOUT

While the proliferation of Internet-enabled devices and the deployment of standard Ethernet across The Connected Enterprise promise tremendous benefit, this convergence also brings security concerns to the fore. Networks, as well as assets, intellectual property and site availability all need to be secured from potential threats—both accidental and intentional. What's needed is an active security culture that permeates every person, policy and procedure in The Connected Enterprise. Security can't be tacked on; it must be woven into the network infrastructure, new and legacy control systems, machinery & equipment, industrial devices and enterprise-level systems.

The breadth of threats that exist today combined with a constant stream of new threats requires that security in The Connected Enterprise be robust and capable of stopping threats on multiple fronts. As a result, a "defense-in-depth" security approach that addresses both internal and external security threats is required.

Defense-in-depth security encompasses physical, network, computer, application and device security. A defense-in-depth strategy is recommended in the IEC 62443 standard series (formerly ISA 99), the National Institute of Standards and Technology (NIST) Special Publication 800-82 and the U.S. Department of Homeland Security's external report INL/EXT-06-11478.

For its part, Rockwell Automation continues to address industrial security systemically throughout its Integrated Control and Information portfolio, adopting specific design-for-security development practices into its product and system development processes. Further, it continues to expand the physical, cyber and intellectual property protection mechanisms in its control products, and has cultivated relationships with network infrastructure vendors like Cisco® to enhance its active threat monitoring capabilities and to provide industry with guidelines, recommendations and practical advice for reducing operational risk.

Fortunately, the same technologies that characterize The Connected Enterprise also provide the means to actively protect it—from corporate servers all the way down to controllers and other connected devices on the remotest edge of the enterprise network.

# MADE POSSIBLE BY

# Rockwell Automation

This *Control Essentials* guide was made possible by Rockwell Automation, which believes that new networking, control and information technologies, securely applied, can bring about a revolution in industrial productivity, asset utilization, collaborative decision-making and global competitiveness.

Learn more about the Rockwell Automation vision for The Connected Enterprise.