Key Considerations for Operationalizing the Connected Industrial Enterprise

Improving Competitiveness with Information:
Insights from the Rockwell Automation Connected Enterprise Journey

LISTEN.
THINK.
SOLVE.®

Allen-Bradley · Rockwell Software

Rockwell
Automation

Globalization and other competitive pressures are accelerating the need for manufacturers and industrial operators to improve what and how information is shared across their enterprises. Better information sharing drives better decision making, exposes process inefficiencies, facilitates best-practice collaboration and uncovers new competitive opportunities.

Seamlessly and securely enabling this type of information sharing within and among sites and beyond to external partners, suppliers and customers creates a connected enterprise. Achieving a connected enterprise, however, requires a holistic understanding of manufacturing's complexities, the opportunities of emerging technologies, information, control and networking technologies, and personnel roles and related responsibilities.

To stay ahead of your competition you must carefully assess and map out a journey that captures the right data and turns it into working data capital (WDC). Based on its own experience, Rockwell Automation understands both the complexities and the rewards of this journey.

With manufacturing facilities and supporting supply chains around the globe, more than 387,000 stock keeping units (SKUs), multiple product types, including build to stock, configured to order (CTO) and engineered to order (ETO), and an average product order including 200 different part numbers, Rockwell Automation was faced with many of the same pressures to manage complexity and drive out inefficiencies as its customers. Shortening response times to customers, ensuring raw material availability, improving supply chain coordination and enabling better collaboration among engineers required a more strategic approach to sharing information among manufacturing, enterprise systems and supply chains.

Enabling information innovations are burgeoning. The Industrial Internet of Things and the proliferation of smarter end points, big data and analytics, virtualization, and mobility are the next evolutionary steps to further facilitate the decades-long pursuit of the connected enterprise for manufacturers. In doing so, you're better able to harness the most powerful element that too few manufacturers today are fully capitalizing on: your own data. This intangible commodity is the key to better understanding your operational performance at the most granular level so you can improve operations, and produce more at higher quality levels, in a more efficient manner.

Top performers achieved **24%** net margin improvement

MESA Research

The challenge for you now is: How do you move from discussing and theorizing your connected enterprise to rationalizing and operationalizing it?

Many factors need to be considered as you journey from concept to completion. And while those factors pertain to both the operational and information technology (IT) aspects of your business, this white paper is specifically tailored to the needs of you, the plant manager, and those who are involved in day-to-day plant operations.

Deployment

Launching a connected enterprise involves several people, decisions and processes. Rockwell Automation designed a related Connected Enterprise Maturity Model that is based on five key stages:

Stage 1: Assessment

Stage 2: Secure and Upgraded Network and Controls

Stage 3: Defined and Organized Working Data Capital

Stage 4: Analytics

Stage 5: Collaboration

Ideally, each stage should be assessed, designed and implemented with the others in mind. However, while it is important to note that they are not mutually exclusive and that in some ways these stages are dependent upon each other, you may initiate the process by entering the phase most appropriate for your organization and your unique needs.

This paper addresses each stage of the Connected Enterprise Maturity Model but is primarily focused on providing key considerations as you make this journey and relating valuable lessons learned from the deployment of the Rockwell Automation® Connected Enterprise.

1. Assessment

Conducting a baseline assessment is a critical first step. Be mindful of your operations' current and future states. Consider your goals regarding quality, downtime, productivity and overall equipment effectiveness (OEE), among other things. Identify key objectives, problems and metrics you're trying to impact, and consider where you're seeking greater efficiencies.

Some key questions to ask during your assessment include:

Network Infrastructure

- Are you currently using multiple, disparate networks?
- How well are both your machines or equipment and ancillary sites integrated, and how well can they communicate with each other?
- If the same problem arises at four sites, will it be solved and paid for four different ways?
- How well are your site-floor operations connected to your enterprise and business systems, and how do you know if you are improving your processes?

Production Environment

- What kind of environmental challenges does your site-floor equipment face – temperatures, humidity, vibration, noise?
- What are the connection requirements not only for the production zone but within each cell?
- What kind of education will be needed for employees as new workers enter your process?
- Can automation address workforce deficiencies?
- Where can you eliminate outdated hardware and redundant applications?
- Are you connecting all the right things to improve your operations?

Data & Reporting

- How much of your data collection and reporting is automated versus manual?
- What metrics do you want to capture that aren't being captured today or can't be captured with your existing system?
- How is your site performing against your key performance indicators (KPIs)?
- Are you seeing performance discrepancies between your site and other sites that produce the same products?
- Is your reporting standardized?
- Is data contextualized to roles so, for example, it allows operators to read actionable information quickly and clearly?
- If you find areas that aren't meeting expectations, how long does it take you to react?
- Without connections, how do you know what you don't know?

Security

- Do you have security policies and procedures in place, and are they enforced?
- What kind of network security applications are currently in place?
- Do you rely on a single security solution, or do you employ multiple layers of security?
- Who will have access to data?
- Can you audit site activities on machine, product and personnel levels, and create audit logs?
- Do you provide access to data/information based on roles, or does granting access mean granting access to everything?

It's critical that your assessment go beyond what you're doing now to also consider your future operations. A connected enterprise can enable your operations to more easily take advantage of new technologies, including:

- Wireless / Mobility
- Virtualization
- Cloud Computing
- Video
- Security
- Data Analytics
- Remote Services

The physical layout of the network is an obvious factor, but network availability is just as important.

For example, multiple network switches and network paths can help avoid single points of failure for critical processes.

Similarly, understanding real-time communications needs will help determine specific design considerations for network latency and jitter, which can affect network performance, machine performance and, therefore, operational performance.

A connected enterprise will look, act and scale differently for every manufacturer, depending on their unique needs. It may involve only a few dozen connected devices, or it may involve tens of thousands of devices.

A complete assessment will not only allow you to right-size your connected enterprise to your needs, but it also can save you costs in terms of equipment, deployment, operation and maintenance.

For example, during the Rockwell Automation baseline assessment, the company identified issues for improvement, including the need to more tightly centralize its global processes and supply chain execution. There were variations among individual manufacturing sites that included different enterprise resource planning (ERP) systems, manufacturing execution systems (MES) and custom applications that made it difficult to conduct accurate enterprise-wide benchmarking, such as measuring production efficiencies and inefficiencies across the enterprise.

A clear blueprint was developed to create consistencies among its processes, improve collaboration among its talent and optimize its supply chain.

If you're struggling to determine how to properly assess your operations or what it will take to achieve the level of connectivity that you want, seek an expert on the subject. Solution providers can use their experience from working with other manufacturers and leverage partnerships with other companies to bring in additional areas of expertise.

Establish a Cross-Functional Team

Collaboration should be a goal at the onset of the design stage, not upon the completion of deployment. The more people you involve in the beginning, the better result you will get.

The Rockwell Automation experience reiterates the importance of connecting as many people as possible to the project so a breadth of roles – operations, IT, engineering – understands and is familiar with the process. Enterprise-wide engagement is critical to establishing and understanding the type of connectivity needed, output goals and actionable information for each role.

On the design and deployment side: The site and/or MES manager(s) can take lead roles in defining the needs for your facility, putting together a scope document and specifying the requirements for deployment. The IT group conducts the majority of the system development and configuration.

At the site level: The site manager is obviously vital, from the initial project buy-in and design to deployment and ensuring the connected enterprise helps the site meet its targets. You should also recruit someone from your facility to serve as the site manager for the project. They will serve as the conduit between key site personnel – such as quality managers, control engineers and operational technology (OT) personnel – and the design and deployment team.

> ***'Operators, IT and engineering teams all need to take time to understand what they're trying to establish. Knowing what our output goals are and what information we want and need – these steps all need to be communicated in detail.'***
>
> Al Heid, plant systems project manager,
> Rockwell Automation

In the weeks leading up to deployment, these team members should be on-site together to test the system and its communications. Training for workers can include focus groups and piloting the system in a simulated environment, where workers can become comfortable with the system in the functions that they'll be using it for and familiarize themselves with new processes.

Even after deployment, collaboration is crucial to helping you get more out of your connected enterprise in the long run. In the Rockwell Automation journey, for example, the collaboration extended to the creation of an internal Challenge Team made up of multiple plants' top engineers and plant managers who regularly collaborate to share best practices, lessons learned and new developments. Processes are in constant development, and ongoing collaboration allows engineers and plant managers to foster new ideas or learn how other plants are doing things, and possibly adopt those practices themselves.

2. Secure and Upgraded Network and Controls

A connected enterprise isn't truly "connected" without a common network infrastructure that facilitates communications between your automation and control systems and your enterprise network. EtherNet/IP™ helps enable this network technology convergence through the use of standard Ethernet and Internet Protocol (IP) technology.

EtherNet/IP can facilitate the following:

- Convergence of multi-discipline applications, such as discrete, continuous process, batch, drive, safety, motion, power, time synchronization, supervisory information, asset configuration/diagnostics and energy management.
- A future-ready network design that is based on standard IT technology, increasing sustainability and reducing risk of deployment.
- Better asset utilization through a common network infrastructure that can also support lean initiatives.

- Common toolsets, such as assets for design, deployment and troubleshooting, as well as human assets and required skills and training.
- Standard and established IT security technology, best practices, policies and procedures.
- Seamless plant- and enterprise-wide information sharing due to IP's pervasiveness and the technology's routability and portability across data links, such as Ethernet and Wi-Fi.

A common network infrastructure helps businesses integrate business systems with operations systems for improved performance, regulatory compliance (including product genealogy and track and trace) and supply chain management. By using a single network technology, businesses can also connect more industrial automation and control system devices with commercial devices, which can improve asset utilization, optimization and management, and foster better collaboration. A single network technology allows expanded application support for company initiatives, such as energy management and sustainability. And it improves collaboration of industrial automation and IT groups, which previously had little interaction but now are able to collaborate and share standards, best practices, innovations, and security policies, procedures and technology.

Working with your IT team will ensure your converged network is optimized for your operations for everything from bandwidth and security to remote-access capabilities. For example, different network topologies will deliver varying levels of availability and integrity for your control and information data. And using managed infrastructure technologies, such as applying Quality of Service (QoS) to minimize any latency or jitter in your sensitive control data, can help ensure you meet your expected production goals.

Additionally, if it wasn't addressed in your assessment phase, ensure the migration of your legacy networks to your new network architecture accounts for your future needs, such as wireless, radio-frequency identification (RFID) readers, video and mobile connectivity.

> Even if you don't see a need for data-generating sensors and other "smart" devices today, consider if that will be the case **2-3 years** from now as these connected devices continue to proliferate.

An open network like EtherNet/IP also enables you to easily incorporate and take advantage of modern control technologies. Programmable Automation Controllers (PAC), for example, can communicate across the network and support increasingly information-intensive applications, such as batch processing, where additional memory is required. A PAC also can converge the drive and motion controllers into one controller, on one network, to improve performance and require fewer components and spare parts to maintain.

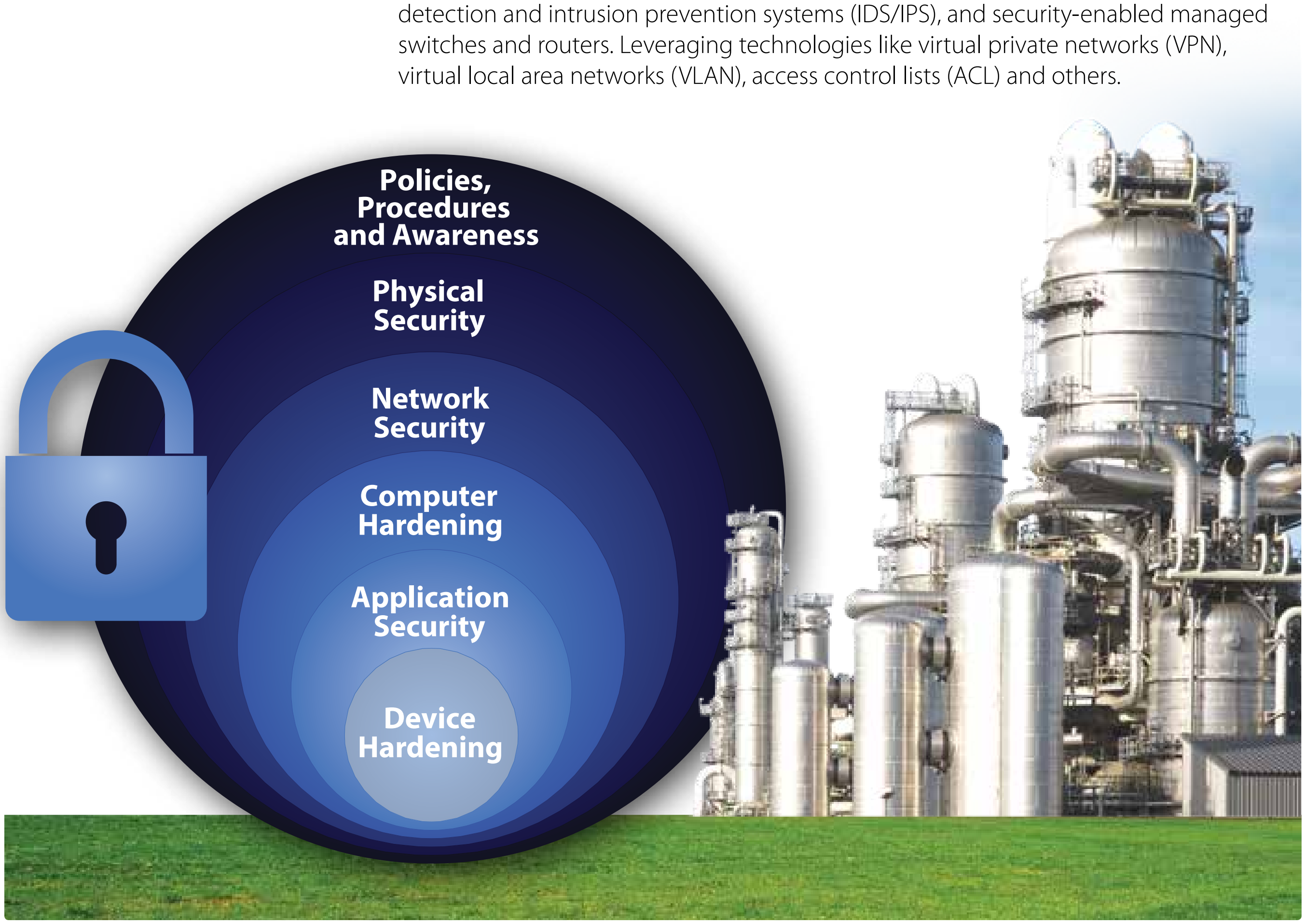
Multi-layered Security Approach: For all the benefits of connecting your site and production assets, it also introduces greater risk in the form of internal and external threats both malicious and accidental – from hackers, viruses, uneducated employees, and well-meaning contractors, among others.

Your security approach should be multi-layered – using both physical and electronic defenses – to help ensure threats can be stopped at multiple levels within the production zone using multiple safeguards. A single technology or methodology simply won't suffice against the multitude of threats that exist.

During its journey, Rockwell Automation very deliberately designed security in from the beginning as opposed to implementing it after the system was installed. It worked with its own industrial security experts and its strategic partners, including Cisco®, to apply a combination of control system design and best practices, enabling technologies, and professional services to manage all layers, including device, controller, process and enterprise. The solution allows current mitigation schemes to be deployed and upgraded across both office and plant networks.

This best practice approach includes a Defense in Depth strategy, which 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. The multi-faceted strategy includes the following key areas of security that must be addressed in your plant:

- **Policies and Procedures:** Managing the differences between manufacturing or industrial operations and IT enterprises and their associated risks to achieve production and business goals involves more than technology. It also requires policies, procedures and behavior, such as a robust password policy that requires passwords to expire and be reset, and a role-based access-control policy.
- **Physical Security:** Network-based authorization using guards, gates, RFID readers and other mechanisms to enforce the access of people (employees, suppliers or other visitors) on your physical premises. This includes role-based access to locations, such as facilities, control rooms and cabinets, and technology, such as control panels, devices and cabling. Physical security also includes non-network protective measures, such as locking electrical cabinets and blocking open ports.
- **Network Security:** Protecting your network infrastructure with firewalls, intrusion detection and intrusion prevention systems (IDS/IPS), and security-enabled managed switches and routers. Leveraging technologies like virtual private networks (VPN), virtual local area networks (VLAN), access control lists (ACL) and others.



- **Computer Hardening:** Mitigating external and internal threats to plant-floor computers, including industrial computers and human machine interfaces (HMI), using antivirus software, patch management, the disabling of auto updates, application removal, host-intrusion-detection systems and the blocking of unused ports.
- **Application Security:** Infusing security into industrial control system applications using authentication, authorization and audit software.
- **Device Hardening:** Reconfiguring the default settings of embedded devices to make access more restrictive. Using devices that conform to industry standards, and using strong passwords and use encryption where possible.

A key aspect of the network security and computer hardening components is the implementation of an Industrial Demilitarized Zone (IDMZ), as referenced in the IEC 62443 standard series and recommended by the NIST. A DMZ should be placed between your manufacturing and enterprise zones to securely manage traffic between the two. Communications can still take place between these two zones, but all traffic from either side will terminate in the DMZ.

The Defense in Depth strategy is thorough but doesn't need to be restrictive or arduous. Building it into the collaborative team that is responsible for the design, development and deployment of your connected enterprise will grow the stakeholders involved in your security strategy to help ensure employees adopt it. This team approach also will help ensure you balance your security policy against key manufacturing targets, such as lower Mean Time to Repair (MTTR) and higher OEE.

Finally, your security strategy should be a sustained journey, not an end destination. Security shouldn't be viewed simply as a "bolt-on" solution, and yet it also will never be absolute. As your connected enterprise, your operations and the threat landscape evolve, so too should your multi-layered security approach.

3. Defined and Organized Working Data Capital

A connected enterprise resolves the many problems that you might be experiencing with your operational data. Perhaps you struggle with being able to separate the "good" data from the "bad" data, or how to convert data into meaningful information. You might still be manually developing reports using Excel® spreadsheets, which can be cumbersome to produce, prone to human error and not provide information in real time. You also may not be collaborating with other sites, suppliers and customers in the form of information sharing, which can help you share best practices, give you more insight into supplier deliveries, improve your ability to respond to changing customer needs and increase your time to market.

Whatever the challenge may be, implementing manufacturing intelligence software along with your MES enables you to gather disparate data, filter it and present it as meaningful information. This includes the data not only from your production equipment but also from "smart" devices on a line and from throughout your supply chain. Turning data into action is the key.

Rockwell Automation integrated its own FactoryTalk® ProductionCentre® software to communicate between the plant floor and the corporate business systems. Rather than relying on each station on a particular line to create its own documentation, the software collects and sorts millions of data points in a more systematic, usable way. If a particular circuit board, for example, consistently fails quality checks, plant managers can now use that data to drive improvements in product design and development. The software effectively feeds information in and out of the ERP system, which has led to reduced engineering times and output efficiencies that improve manufacturing profitability.

4. Analytics

Data-based analytics can be viewed real-time in KPI dashboards, and can be monitored in concert with other real-time data as well as against historical performance data. The data also can be presented and securely disseminated across your organization using Web-based reports.

Beyond providing crucial information on your KPIs, such as quality, productivity, OEE and machine downtime, the data also can be sent to your ERP system. In an engineered-to-order production setting, for example, you can track labor costs against work orders and report the labor data back up to the enterprise to reconcile order pricing. At the plant level, such data could also be examined to give you a better understanding of direct versus indirect labor time or to provide historical data on customer changes.

Rockwell Automation has put its working data capital to work to:

- **Lower inventory** from 120 days to 82 days
- **Capture 30 percent savings** annually in capital avoidance
- **Improve supply chain delivery** from the mid-80s to 96 percent
- **Reduce lead times** by 50 percent
- **Improve customer service metrics,** including time to want from 82 percent to 98 percent and reduce parts per million quality issues by 50 percent
- **Improve productivity** an estimated 4 to 5 percent per year

Also, keep in mind that this greater availability of data can be shared down to plant floor workers, so they can make smarter decisions faster. Delivering downtime-event data to technicians on mobile devices, for example, can help them more quickly discover where the issue is, identify patterns for predictive maintenance insights, what needs to be fixed and where any necessary tools or spare parts can be located.

5. Collaboration

One of the greatest benefits of a fully connected enterprise is the ability to connect and share valuable information across people, devices and machines.

Bringing people together from across your organization, as already described, is critical to the development of your connected enterprise. But you also must consider what capabilities you will deploy to help drive collaboration, whether it's within a single site, between a site and the enterprise, or across multiple facilities and supply chains.

That could include deploying mobile applications to give workers on the site floor production access to real-time information such as OEE. Mobile devices can also provide valuable diagnostics data to maintenance personnel when a downtime event occurs, so they immediately know where a problem is happening, what the issue is and where they can get the tools they need to fix it.

Cloud computing can increase collaboration across your supply chain, which can help you improve demand planning and better manage inventories. You can use remote monitoring and diagnostics technology as part of product deliveries to connect your technicians with distant customer locations to perform real-time diagnostics.

Beyond Deployment

In a perfect world, you would be able to identify up front all of the data that you want to be mining from your operations and the information that you want to deliver in your reports. This can help prevent any retroactive changes or refinements to the system after it is deployed.

It's a goal worth striving for, but keep in mind the connected enterprise is a continuous-improvement journey. It will evolve, even for the best-prepared manufacturer. By simply getting your connected enterprise out of the gate, your operations already are taking a great leap forward – out of the industrial age and into the information age.

To discuss strategies and solutions for deploying a connected enterprise,
call a Rockwell Automation sales office or visit:
http://www.rockwellautomation.com/connectedenterprise

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication CIE-WP003A-EN-P – September 2014