Incorporating Cybersecurity Into Water Utility Master Planning

A Strategic, Cost-Effective Approach to Mitigate Control System Risk

By Umair T. Masud, Manager, Consulting Services Portfolio, Rockwell Automation

Cybersecurity threats are ubiquitous and far-reaching. But the stakes are highest when the threats impact critical infrastructure, including water systems. National and industry organizations provide guidance regarding how to protect these systems. Still, water utilities must determine how to incorporate actionable items within the context of their organizational structure and budgets.

Introduction

Yahoo. The Democratic National Committee. Ukraine's power grid. Significant cybersecurity breaches unwittingly kept each of these organizations in the headlines for weeks at a time in recent years. And after the headlines had faded, these companies faced a damaged reputation and an aftermath marked by fading consumer confidence and more than a few class action lawsuits.[1]

While these breaches have put consumers on alert, tactical campaigns targeting industrial applications and critical infrastructure such as Stuxnet, BlackEnergy and Havex have heightened governmental attention and resulted in additional pressure to protect vital systems.

For those safeguarding and distributing the public's water supply, these massive security breaches and threats are yet another reminder of the potential vulnerability of their systems. Due to limited budgets, uptime requirements and talent shortfalls, many utilities struggle to apply even basic security measures. The latest call to strengthen system security to meet the most advanced threats has added a new level of confusion and concern.

Historically, water utilities embraced the IT landscape later than many industries. Many are just now beginning to realize significant benefits. Most have incorporated consumer online access to account information. Others have added smart metering technologies, including advanced metering infrastructures (AMIs). Still others have built supervisory control and data acquisition (SCADA) systems that can potentially leverage cloud and mobile technology.

But while the benefits of new cyber capabilities are readily apparent, the associated risks often remain undetected and unchecked until a major breach occurs. Recognizing the catastrophic impact such a breach could have within critical infrastructure, governments and security communities around the world have stepped up research, leadership, training and guidance.

In the U.S., *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*[2], issued in 2013, was followed by the National Institute for Standards and Technology (NIST) *Cybersecurity Framework*[3] in 2014. This voluntary framework consists of referenced standards, guidelines and practices to promote the protection of critical infrastructure. Simultaneously, the American Water Works Association (AWWA) released its own *Process Control System Security Guidance for the Water Sector*[4] to provide a sector-specific approach to adopting the NIST framework.

Simply put, there is no lack of practical guidance and tools – and independent experts and suppliers eager to help. As with any security framework, program or solution, implementation can be daunting for water system professionals – especially those in public utilities with limited IT staff and resources. This white paper outlines the most dangerous cyber threats to utility control systems and why an active defense strategy is often the most practical and effective response. It also includes steps utilities can take now to prepare for the inevitable day when they are faced with a new security challenge or regulatory requirement.

Unique Water Sector Challenges: Mission, Infrastructure & Expertise

Water utilities face unique challenges when addressing cybersecurity issues. Unlike many organizations, water utilities are usually publically funded and accountable to the community at a very local level. Their mission is to provide a clean, uninterrupted water supply to their municipality – and to do so within budgets that are often politically charged.

Aging Distribution Network

It's no secret that the water infrastructure in North America is both rapidly deteriorating and in need of expansion to match population shifts. Upgrades are costly and time-intensive. In fact, the AWWA estimates that restoring and expanding existing systems will cost at least $1 trillion over the next 25 years.[5]

For municipalities of all sizes, repairing and updating water mains, reservoirs and pumping stations is an imperative – and a growing, oftentimes unpredictable, expense. Given limited budgets and resources, utilities must make tough choices. And in many cases, that means devoting the majority of available funds and personnel hours to maintaining the mechanical water distribution system.

Conversely, emerging technologies and methods are available that provide new capabilities to improve and extend the life and service level of the infrastructure. But there is often limited budget and staff available to evaluate and deploy them.

Beware the Regulatory Mindset

Regulatory compliance has been an intrinsic part of doing business for U.S. water utilities since the Safe Drinking Water Act (SDWA)[6] was enacted by the EPA in 1974. This regularly amended regulation motivates behavior and standardizes processes. But as events such as the Elk River chemical spill attest[7], meeting regulatory requirements means a utility is compliant. It does not necessarily mean the water is safe to drink.

In much the same way, adhering to cybersecurity guidelines does not confirm that a utility system is secure. In fact, a strict regulatory mindset may actually provide a false sense of security. After all, adversaries know the latest requirements, too. To truly mitigate risk, utilities must take a forward-thinking, proactive approach that extends beyond compliance.

Disparate Industrial Control & Information Systems

Of course, utilities still must attend to their industrial control systems (ICS) and IT infrastructures to meet other critical industry requirements:

- Maintain and optimize increasingly complex process control and SCADA systems – and develop ways to minimize vendor and control system sprawl.
- Establish proper risk and use evaluation for new technology to minimize negative exposure and impact to future budgets.
- Improve consumer trust – and satisfy growing demand for more transparency and access to account information.
- Meet the inevitable demands of regulatory compliance.

But with internal resources committed to maintaining system availability, many utilities are forced to postpone comprehensive upgrades. More typically, utilities evolve their systems slowly – and rely increasingly on multiple service level agreements (SLAs), system integrators and contractors for control system expertise.

Outsourcing has its advantages. However, often one unintended consequence is a "silo" approach to the ICS and IT infrastructure and disparate systems. Without appropriate oversight, this can result in a fragmented environment that, by its very nature, is more susceptible to cyber risk.

How Can Cyber Events Affect Water Systems?

Cyber events can affect water system operations in a variety of ways, some with potentially significant adverse effects on public health. For example:

- Make unauthorized changes to programmed instructions to take control of water distribution or wastewater collection systems – resulting in disabled service, reduced pressure or overflow of untreated sewage.
- Block data or send false information to operators.
- Change alarm thresholds or disable them.
- Prevent access to account information.
- Interfere with treatment equipment and potentially impact all downstream who are dependent on clean water – from private citizens to industry.

Escalating Threats – and Sophistication

Across all industries, cyber threats are escalating, both in number and sophistication.

While the private sector accounts for the majority of threats – and power generation receives most of the attention in the utility space – the water sector is equally vulnerable. Although many data breaches are the result of accidental "insider" activity, the source of the initial breach provides little consolation if it opens the door to malicious actions.

More Sophisticated. More Persistent. More Dangerous.

Perhaps of even more concern than the accelerating number of cyber threats is the nature of those threats. Today, hostile entities are applying sophisticated, orchestrated methods and multiple technologies to stay one step ahead of the IT professionals who implement safeguards to foil them.

Among the most dangerous attacks are those orchestrated by Advanced Persistent Threats (APTs). Once nearly the exclusive purvey of nation-states seeking data for political or other strategic gain, evidence suggests that APTs are now being found in critical systems on which citizens depend.

Most important to the success of an APT or any sophisticated threat actor is its ability to remain undetected for as long as possible. Therefore, a successful breach does not begin with, nor may it ever culminate in, mass destruction. Instead, it relies on a covert progression of activities which can be masked by the common noise of a typical network environment.

Sophisticated malicious actors often begin innocuously enough – with information gathering and/or "Google hacking" via public-facing websites and social media. While the initial activity appears benign, this "passive reconnaissance" phase quietly identifies possible vulnerabilities in the system.

> ***Our current efforts, geared towards "passive" cyber defense, are fixated on continuously monitoring and patching systems. Passive defense does not work and will never work against serious cyber threats.***[8]
>
> ***Steven Chabinsky***
> ***Former Deputy Assistant Director***
> ***FBI Cyber Division***

Next, the attack moves to "active reconnaissance." Now, the attacker deploys a variety of external probing and scanning activities – perhaps including "phishing" and "social media mingling" – to acquire sensitive information, such as user names and passwords. Once inside the system, the attack exploits vulnerabilities utilizing sophisticated software tools. These attack vectors take many forms and are custom-tailored to the targeted environment. In some cases, these tools may identify the presence of "zero-day" vulnerabilities. These unknown software "holes" enable further infiltration until detected and "patched." The goal of exploitation is to establish some level of command and control. Once a beachhead is established, additional reconnaissance activity focuses on locating sensitive data within the system – and then transferring it out of the network for malicious purposes. Since the exfiltration of data can resemble normal network traffic, it's very difficult to detect. At this point, the damage is done.

Impervious to Traditional Countermeasures

For years, cybersecurity programs have centered on network isolation and segmentation – and passive defense activities – designed to mitigate system vulnerability. Simply put, passive defenses are systems that do not require human intervention. These standard countermeasures are important components of any network security program and include anti-virus software, security patches, signature-based intrusion detection systems, email filters and firewalls. In recent years, water utilities have recognized the importance of installing, improving and keeping these systems up-to-date.

In addition, governments and the security community have supported this approach by instituting standards written to help ensure minimal levels of security in various business sectors.

As essential as these countermeasures are, they often leave systems susceptible – or even defenseless – against APTs and other sophisticated, targeted attacks.

Here are a few reasons why:

- Anti-virus software only protects systems from malware signatures it recognizes.
- Malicious attackers use encryption, DNS tunneling, email and other covert techniques to avoid detection by intrusion detection systems.
- Email filters struggle to stop correspondence that in every way appears legitimate.

Given today's climate, any organization that claims traditional countermeasures are enough to keep their systems secure are naïve at best. Advanced threats are real and occurring regularly across every business sector – including water and wastewater.

Moving Toward Active Cyber Defense[9]

While passive defenses still have a place in warding off low-level attacks, an agile and active defense strategy is required to stay ahead of the most advanced adversaries. At the highest level, an active defense strategy uses sophisticated forensics and intelligence sharing – across industries and governments – to identify and counter cyber threats.

Of course, not every utility faces the same level of cyber risk or requires the same type of program to achieve an appropriate level of security.

For the largest utilities, transforming their ICS Security Program into a comprehensive Security Operations Center (SOC) may be merited. For many others, an enhanced ICS Security Program that incorporates an appropriate level of external partners is sufficient.

All utilities must perform a business impact analysis or risk assessment to establish the appropriate governance and level of security for their ICS Security Program.

Where to Start:

It's a Process, Not a Project

With internal IT and ICS security expertise in finite supply – and outsourcing common – there is an understandable tendency for utilities to view any initiative related to information infrastructure, metering or process control systems as a "project." By definition, projects are limited in scope and have well-defined objectives, timelines and budgets.

For example, a water utility might initiate a project to changeover their metering system to AMI technology. It may select an outside vendor for the project, based on an open bid process. Expenditures are relatively finite and predictable – and expected outcomes can be easily communicated to the public.

Projects are focused on completing a "task." Projects begin and end – and may even co-exist at cross-purposes with other projects. But when it comes to safeguarding a utility's industrial control system, a "set-it-and-forget-it" project mentality can be dangerously limiting.

To be truly effective, cybersecurity must embrace a cohesive strategy that extends through every project in parallel with all business operations throughout a utility's lifecycle. A breach at any point can put the entire system at risk.

Simply put, cybersecurity is a critical business objective. As such, it must be approached as an ongoing process, albeit one where budget projections and public relations are challenging. And where success is measured by what doesn't happen, rather than what does.

Building the Program: Laying the Foundation

Cybersecurity touches every aspect of a typical business. For water utilities – which have a high volume of critical assets plus complicated constituency and governance – the scope of an ICS Security Program can appear particularly daunting.

However, regardless of size or complexity of the existing infrastructure, all utilities face similar challenges. And when it comes to mitigating risk, all ICS Security Programs can deploy a common, proven methodology.

That methodology must:

- Begin with an assessment of business needs and the specific operational requirements of the process control system.
- Identify critical assets and data that are essential to operation.
- Support asynchronous technology and business change – and be adaptable to the evolving landscape and move toward active defense with minimal overhaul.
- Recognize that no single product or technology will fully secure industrial networks.
- Utilize a "defense-in-depth" strategy based on multiple countermeasures that disseminate risk over an aggregate of security mitigation techniques.[10]

Stakeholders and Executive Buy-in

Identifying the right team to support and execute this methodology at the outset is critical. To be effective, this team must be endorsed at the executive level – and include expertise encompassing both the industrial control system and business level networks.

In utilities with limited ICS and IT expertise, incorporating a trusted third-party consultant is a viable option.

Ultimately, this team will be charged with formalizing and executing the policies and procedures that will guide the utility on cybersecurity issues for years to come. And will be instrumental in determining and implementing related technologies and contingency plans.

Defense-in-Depth Framework[10]

The basic tenets of this strategic framework are:

- Know the security risks faced.
- Quantify and qualify the risks.
- Use key resources to mitigate the risks.
- Define each resource's core competency and identify any overlapping areas.

Setting Strategic Priorities: Know Your Environment

An ICS Security Program based on a defense-in-depth strategy begins with a clear understanding of the environment and what needs to be protected. Once the "current state" is clearly understood, utilities can determine which critical control investments will have the most impact.

Security Assessment

Assessments are the starting point for any cybersecurity program. An assessment outlines a utility's current security posture – important baselines for system availability, integrity and confidentiality.

Through an assessment, a utility can determine what is "normal" from the standpoint of data entering and leaving the system. This is a crucial first step to identifying abnormalities and potential security events.

In addition, an assessment evaluates the robustness of a utility's security practice architecture – and its ability to protect ICS assets.

Effective security assessments also extend beyond the technology deployed. For example, Rockwell Automation® security assessments take into account not only networks and industrial control systems, but also existing policies, procedures and typical behavior. In addition, our security specialists leverage our automation expertise to provide a comprehensive review, including process control application performance within the existing infrastructure.

Specifically, an assessment should include at minimum:

- Inventory of authorized and unauthorized devices and software.
- Detailed observation and documentation of system performance.
- Identification of tolerance thresholds and risk/vulnerability indications.
- Prioritization of each vulnerability, based on impact and exploitation potential.

The final outcome of any assessment is recommended and prioritized mitigation activities. These recommended activities are often aligned with what are known as "critical security controls."

Security Controls Investment & Utility Master Planning

With the results of a security assessment and prioritized mitigation steps in hand, a utility is positioned to implement a cybersecurity program.

However, while the need for a program may be well understood within the utility, justifying funding to implement recommendations can be a significant hurdle – especially when public opinion comes into play.

The following factors pose public relations challenges – both within municipality governance and the broader community – and may forestall funding approval:

- Given finite budgets, funding a new cybersecurity investment generally means diverting funds previously allocated for other more popular purposes.
- In the public sphere, it's usually easier to justify additional costs – and potential rate hikes – for improvements to the system that immediately and directly impact water delivery or quality. The benefits of a cybersecurity program are often invisible.
- Cybersecurity is not a one-time expenditure. Security is a commitment that commands vigilance and an ongoing investment in people, process, product and technology.

Due to these factors, aligning security controls investment closely with the utility master plan is the most effective, publically palatable and fiscally responsible approach. The NIST Cybersecurity Framework released in 2014 in response to the Executive Order 13636 can assist municipalities in that effort.

What is the NIST Cyber Security Framework (CSF)?[11]

The NIST Cyber Security Framework was developed by the National Institute of Standards and Technology, in concert with other U.S agencies and industry experts to address risks in the Industrial Control environment and the critical infrastructure that are controlled by them. The framework enables any organization to apply the principles and best practices of risk management to improving the security and resilience of a municipality's industrial control infrastructure. The functions and categories that make up the framework are as follows:

1. **Identify**
    a. Asset Management
    b. Business Environment
    c. Governance
    d. Risk Assessment
    e. Risk Management Strategy
2. **Protect**
    a. Access Control
    b. Awareness and Training
    c. Data Security
    d. Information Protection Processes and Procedures
    e. Maintenance
    f. Protective Technology
3. **Detect**
    a. Anomalies and Events
    b. Security Continuous Monitoring
    c. Detection processes
4. **Respond**
    a. Response Planning
    b. Communications
    c. Analysis
    d. Mitigation
    e. Improvements
5. **Recover**
    a. Recovery Planning
    b. Improvements
    c. Communications

The Cyber Security Framework allows for each organization to align the effort of managing risk with their unique business requirements and priorities.

Additionally for water utilities, the AWWA Cybersecurity Guidelines align to the NIST Cyber Security Framework, water organizations such as the Water Sector Coordinating Council and the USEPA recognize this guidance as the sector specific implementation for NIST CSF.[12]

Ways to Align

While not an exhaustive list by any measure, here are some specific ways a utility can implement a strategic, lifecycle approach to cybersecurity investments:

- **Biggest Impact First.** It may go without saying, but follow the initial assessment prioritization – and allot funds first to those investments that are most critical.
- **Assess All Cyber Investments for Risk.** Most utilities routinely include mechanical risk assessments as an intrinsic part of the selection process for any investments related to the physical infrastructure. Extend this mindset to new investments that impact the IT infrastructure and industrial control system as well. Make it part of the purchasing decision.
- **Invest for a More Secure Future.** Do not silo cybersecurity. Take a "future-ready" mindset to all investments – SCADA systems, process control systems, power control and monitoring systems, and software – at every level of the enterprise. Work to confirm new investments incorporate cybersecurity features – even if the utility cannot immediately activate those features. Move toward a more active defense with every investment.
- **Scrutinize and Limit System Proliferation.** Narrow the scope of system suppliers and SLAs, starting with the procurement process. The fewer disparate systems within an environment, the easier it is to secure them.
- **Consider Quality Based Selection (QBS).** This pre-selection procurement system focuses on the long-term lifecycle costs of a solution, including overall sustainability – not only upfront capital costs. QBS helps set a technology direction for the future that prioritizes an integrated secure environment.[13]
- **Recognize the Value of Ongoing and Annual Assessment.** A successful cybersecurity strategy requires an ongoing audit of what exactly is occurring in the system – and an annual assessment to restate or realign priorities.

Conclusion

For years, water utilities have enjoyed the limited protection intrinsic to systems that are isolated from a connected world. The industry, too, has achieved tremendous returns on investment – thanks to the seemingly timeless products that comprise their water systems and the skilled staffs that maintain them.

Although the water systems of yesteryear may not appear very different from the day they were commissioned, the internetworking of many of these systems has changed. Typically, "islands of automation" have been replaced by hybrid systems with an intermixing of old and new products – and a variety of creative methods to exchange information. Connectivity of even the older systems to business operations and potentially to the outside world has become a norm, not an exception.

Within this environment, understanding even the current system security baseline can be a challenging task for water utilities. However, the need to address cybersecurity issues has never been greater.

By viewing cybersecurity as an ongoing process and aligning critical security controls investment with the utility master plan, utilities can better identify system vulnerabilities and undertake essential mitigation steps.

Rockwell Automation Can Help

Rockwell Automation has long recognized the importance of connecting independent automation systems in manufacturing environments.

Our vision of The Connected Enterprise,[14] with a balanced approach to industrial control system security, has guided the development of our Integrated Control and Information Technology for decades. Now, with the convergence of plant-floor Operations Technology (OT) and business-level Information Technology (IT), the vision of The Connected Enterprise is becoming a reality.

The Connected Enterprise links plant systems, in-the-field assets, utilities and enterprise IT to deliver contextualized information where it is needed. As a result, companies can make better decisions faster – and achieve a new level of operational intelligence to improve productivity and global competitiveness.

Built on a standard Ethernet infrastructure that can incorporate industry-proven protection techniques and security controls, The Connected Enterprise is enabled by our Integrated Control and Information portfolio.

Mitigating Potential Risk

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 forefront.

For its part, Rockwell Automation continues to address industrial security systemically through its Integrated Control and Information portfolio, adopting specific design-for-security development practices into its product and system development processes.

Further, Rockwell Automation continues to expand the physical, cyber and intellectual property protection mechanism in its control products. We have also cultivated relationships with network infrastructure vendors like Cisco to enhance our active threat monitoring capabilities and to provide the industry with practical advice for reducing operational risk.

Network & Security Services

Rockwell Automation Network and Security Services are designed to help customers understand and manage risk – and improve system reliability and overall equipment effectiveness.

The Network and Security Services team is comprised of multidiscipline professionals with extensive expertise:

- Process control and manufacturing applications across all industries, including industrial network architectures.
- Quantitative and qualitative analysis of security threats specific to industrial control systems.
- Diagnosis and remediation of legacy network equipment and protocols including ControlNet™, DeviceNet™, DH+™, Remote I/O and Fieldbus.
- Development of global standards specific to industrial control systems and the manufacturing industry including NIST SP 800-82; Executive Order 13636 Cybersecurity Framework; ISA/IEC 62443 (formerly ISA 99).
- Collaborative authorship of the *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide* with Cisco[15].

Learn more about Rockwell Automation *Network & Security Services* and security solutions for the *water and wastewater industry.*

Notes

[1] The lawsuits faced by these companies are well documented. Some examples: [Unattributed]: Rueters. (March 18, 2015). "Target agrees to pay $10 mln to settle lawsuit from data breach" *http://www.reuters.com/article/2015/03/19/target-settlement-idUSL2N0WL02S20150319* ; Allison, David. Atlanta Business Chronicle. (October 13, 2014). "Home Depot faces more than 20 class action suits stemming from their 2014 breach" *http://www.bizjournals.com/atlanta/news/2014/10/13/home-depot-now-facing-21-class-action-lawsuits.html?page=all*; Huddleston, Jr., Tom. Fortune. (February 6, 2015) "Anthem's big data breach is already sparking lawsuits" *http://fortune.com/2015/02/06/anthems-big-data-breach-is-already-sparking-lawsuits/*

[2] U.S. Department of Homeland Security. "Fact Sheet." (March 2013). *http://www.dhs.gov/sites/default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf*

[3] U.S. Department of Commerce. National Institute for Standards and Technology (NIST). "Cybersecurity Framework." (Retrieved April 6, 2015). *http://www.nist.gov/cyberframework/*

[4] American Water Works Association (AWWA). "Process Control System Security Guidance for the Water Sector." (2014). *http://www.awwa.org/portals/0/files/legreg/documents/awwacybersecurityguide.pdf*

[5] American Water Works Association (AWWA). "Buried No Longer: Confronting America's Water Infrastructure Challenge": p.3, para. 2. (Retrieved April 6, 2015). *http://www.awwa.org/Portals/0/files/legreg/documents/BuriedNoLonger.pdf*

[6] U.S. Environmental Protection Agency. "Safe Drinking Water Act (SDWA)." (Retrieved April 6, 2015). *http://water.epa.gov/lawsregs/rulesregs/sdwa/index.cfm*

[7] Wines, Michael. The New York Times. (December 17, 2014). "Owners of chemical firm charged in Elk River Spill in West Virginia." *http://www.nytimes.com/2014/12/18/us/owners-of-chemical-company-charged-in-elk-river-spill.html*

[8] Chabinsky, Steven. American Center for Democracy. (May 6, 2013). "Passive Cyber Defense: The Laws of Diminishing and Negative Returns." *http://econwarfare.org/passive-cyber-defense-the-laws-of-diminishing-and-negative-returns/*

[9] Lee, Robert M. Recorded Future. (February 17, 2015). "Threat Intelligence in an Active Cyber Defense, Part I." *https://www.recordedfuture.com/active-cyber-defense-part-1/*

[10] U.S. Department of Homeland Security. "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth." (2009). *https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_ Oct09.pdf.* See also: U.S. Department of Commerce. National Institute for Standards and Technology (NIST). "Guide to Industrial Control System Security." *(2011). http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.* Rockwell Automation. "Industrial Security Best Practices." (May 2012). *http://www.rockwellautomation.com/resources/downloads/rockwellautomation/pdf/products-technologies/security-technology/securat001aene.pdf*

[11] National Institute of Standards and Technology. "Framework for Improving Critical Infrastructure Cybersecurity." (2016). *https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf*

[12] American Water Works Association. "Cybersecurity Guidance & Tool." *https://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx*

[13] Water utilities are beginning to recognize the benefits of Quality Based Selection. One example: Rockwell Automation." Utilities Kingston Implements Plant-Wide Control System to Streamline Wastewater Treatment Plant." *http://literature.rockwellautomation.com/idc/groups/literature/documents/ap/water-ap014_-en-p.pdf*

[14] Rockwell Automation. "The Essentials of the Connected Enterprise." (November 2014). *http://www.rockwellautomation.com/rockwellautomation/innovation/connected-enterprise/essentials-ebook.page*

[15] Rockwell Automation. "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide." (September 9, 2011). *http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf*

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 WATER-WP002B-EN-E – March 2017
Supersedes Publication WATER-WP002A-EN-E – May 2015