White Paper **WP152006EN**

Redesigning automation network security

Presented at
Power and Energy Automation Conference (PEAC),
Spokane, WA,
March 2014

Jacques Benoit

Eaton's Cooper Power Systems

Abstract

The NERC CIP standards have often been challenged on the grounds that they have brought utilities to foster a culture of compliance, instead of developing a culture of security. Correcting this situation was thus one of the goals of the Standard Drafting Team as they set forth on the development of Version 5 of the standards. The changes that have been brought to the applicability requirements and the extension of the scope to a larger number of utilities have been widely discussed. However, little has been said on the evolution of the technical aspects of the standards, more specifically as it concerns network architecture.

This paper discusses some of the technical aspects of the NERC CIP Version 5 Cyber Security Standards, the new technologies to which it opens the door, and how the automation network can evolve to become secure by design, reflecting the convergence of Operations Technology (OT) and Information Technology (IT).

Introduction

Version 5 of the NERC CIP Cyber Security Standards, recently approved by FERC, constitutes the most recent step in improving the security of the critical infrastructure. The previous versions of the standard have often been criticized by security practitioners for fostering a culture of compliance instead of true security. With this new version, the Standard Drafting Team has addressed many of the issues of the previous versions and has defined a security framework that is in much better alignment with existing security approaches such as the NIST Risk Management Framework, as well as current industry best practices.

For the security practitioner, the standards bring clarity by including for each requirement the rationale and guidance on its implementation. For instance, the standards now recognize existing technical limitations and accept alternative technical approaches, such as malware protection through white-listing, which would have been subject to interpretation or Technical Feasibility Exceptions (TFEs) in previous versions.

In another far-reaching change, the standards have moved the focus from the asset level to the system level. The architecture of the automation network can now be viewed as being composed of "trust zones" connected through well-defined Electronic Access Points. This architecture is a key security concept and best practice, also part of the ISA/IEC-62443 (ISA-99) standards for secure Industrial Automation and Control Systems.

For the author, these changes are an illustration of the convergence of Operations Technology (OT) and Information Technology (IT); an example being the use of Intrusion Detection Systems in automation networks, which is now a requirement at higher impact levels.

The following sections discuss the technical aspects of the new standards and provide the background necessary to understand them.

Redefining cyber assets

Previous versions of the CIP Cyber Security Standards focused on Critical Assets (CA) and Critical Cyber Assets (CCA). Utilities had to determine their CAs through a risk-based assessment process. Facilities such as transmission substations and control centers had to be considered and evaluated during the process. CCAs were defined as being any electronic system, associated with a CA, and accessible through dialup or a routable protocol.

With Version 5, the focus now shifts to the system level and introduces a number of new concepts, the most important of which is the impact level rating.

Definitions

Critical Cyber Assets are no longer part of the standards. Instead, the following terms have been introduced or redefined with the Version 5 CIP Cyber Security Standards:

- **Cyber Assets** are programmable electronic devices including the hardware, software, and data in those devices
- **BES Cyber Assets** are Cyber Assets that can impact the reliable operation of the Bulk Electric System within 15 minutes if rendered unavailable, degraded, or misused. Each BES Cyber Asset is included in one or more BES Cyber Systems
- **BES Cyber Systems** consist of one or more BES Cyber Assets logically grouped to perform one or more reliability tasks

Powering Business Worldwide

These changes are important as they bring the scope of applicability of many requirements to the system level instead of the individual device level.

In addition to the BES Cyber Assets and systems, there are other types of systems that play an important role and must be protected. While utilities had to take these into account in their risk assessment process, they were not formally identified in the standards and were not directly the subject of security requirements.

- **Electronic Access Control or Monitoring Systems (EACMS)** such as Electronic Access Points, Intermediate Devices, authentication servers (e.g., RADIUS servers, Active Directory servers, Certificate Authorities), security event monitoring systems, and intrusion detection systems
- **Physical Access Control Systems (PACS)** such as authentication servers, card systems, and badge control systems
- **Protected Cyber Assets (PCA)** such as file servers, FTP servers, time servers, LAN switches, networked printers, digital fault recorders, and emission monitoring systems, to the extent they are within the Electronic Security Perimeter (ESP)

As can be seen from these new definitions, the authors of the standards have recognized the increasing use of IT systems in automation networks and the need to protect these systems.

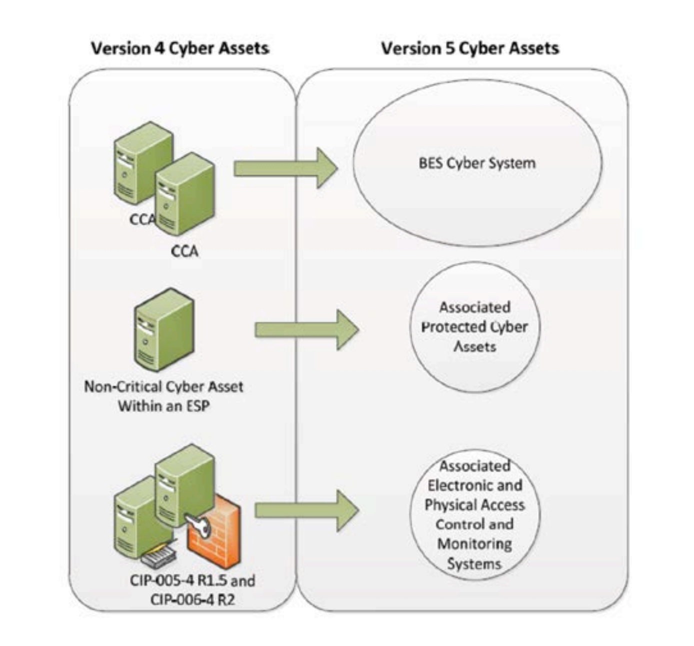
Version 4 Cyber Assets
Version 5 Cyber Assets
CCA
CCA
BES Cyber System
Non-Critical Cyber Asset Within an ESP
Associated Protected Cyber Assets
CIP-005-4 R1.5 and CIP-006-4 R2
Associated Electronic and Physical Access Control and Monitoring Systems

Figure 1. CIP Version 5 BES Cyber System Categorization Excerpted from "CIP-002-5.1 — Cyber Security — BES Cyber System Categorization"

Impact rating

An important change to the CIP Cyber Security Standards is the introduction of impact ratings. Previously, an asset was considered to be either critical or not critical. Now, the question to be asked is *"Will the loss of a BES Cyber Asset or BES Cyber System adversely impact within 15 minutes one or more BES Reliability Operating Services?"* The level of impact being determined by the type of facility or service affected. While a discussion of impact level rating criteria is beyond the scope of this paper, the concept is important as it will determine the design of the network infrastructure. For the sake of simplicity, let us assume that large control centers and transmission substations have a high impact rating. Smaller control centers and substations will typically have a medium impact rating. All assets that were not previously in scope of the CIP standards will now have a low impact rating.

Electronic perimeters and access points

In previous versions of the standards, the Electronic Security Perimeter (ESP) was more a compliance boundary than a true network security concept. The requirements did not directly map to the capabilities of standard network routers, switches, and data concentrators. As we will see, the standard has evolved and many of the security requirements have been assigned to the Electronic Access Points (EAP) rather than the logical perimeter.

The electronic security perimeter

The concept of ESP is still important as it defines the boundaries of the system. The ESP is thus defined as *"The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."* The ESP acts as the primary defense mechanism for all BES Cyber Assets and provides a layer of protection for devices that do implement cyber security functions. The definition of the ESP now reads *"All applicable BES Cyber Assets that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP)".*

Network segmentation

Not all devices connected to the network share the same impact level. For instance, in control centers and large substations, there will also be Protected Cyber Assets (PCAs), such as printers and file servers, connected to the network. Because the whole system can be compromised by any asset connected to the network, the standards state that all BES Cyber Systems connected to a network now need to comply with the requirements of the one with the highest impact level.

This concept, called "high water marking", opens the door to network segmentation, which consists of breaking down the network in different segments with different impact ratings in order to apply the level of security appropriate to each system in a facility.

The concept of network segmentation is a best practice for control systems and is also a key element of the ISA/IEC 62443 (ISA99) standards as we will discuss later.

The electronic access point

The ESP is required even for standalone networks as it defines the boundaries of the system. If there is routable connectivity across the ESP into any Cyber Asset, then an Electronic Access Point (EAP) must control traffic into and out of the ESP. This requirement also applies to data exchanged between network segments of different impact rating.

Previous versions of the standards had already defined security requirements for the ESP such as restricting traffic to what is necessary for operation of the system. With Version 5, many of these are now assigned to the EAP. In addition, the EAP needs to control both inbound and outbound network traffic. This new requirement recognizes the fact that unauthorized outbound traffic is often the first symptom of a compromised system. Malware typically sets up, or tries to set up, an outbound connection to a control and command host on the Internet. Obviously, communications with the external world, the utility network, and the other segments of the automation system should be carefully managed through rules and access control lists.

Intrusion detection systems

Another IT best practice that has found its way into the CIP standards is the requirement to implement methods for detecting ingoing or outgoing malicious communications through the EAP.

IT systems generally implement a defense in depth approach with multiple defensive layers. In addition to firewalls, one common practice is the use of Intrusion Detection System (IDS) and Intrusion Protection Systems (IPS). These systems perform deep packet inspection with the goal of detecting malicious traffic (IDS), or even blocking such traffic (IPS). The challenge with IPS is that legitimate traffic could be flagged and blocked as malicious, preventing critical data from reaching a control center, or a control operation from being performed. Fortunately, automation systems generate much more predictable traffic than IT systems, simplifying up to a certain point the configuration of IDS and IPS.

Serial devices and data diodes

The previous definition of Critical Cyber Assets was based on the use of a routable protocol. Cyber Assets that used serial communications were not considered CCAs and thus did not need to comply with NERC CIP. However, as we have seen in the previous sections, Cyber Systems are now defined as *"programmable electronic devices,"* without any mention of connectivity. A Cyber System that can impact the reliability of the Bulk Electric System is considered a BES Cyber System and needs to be protected. While this will bring serial devices into scope, they will still be exempted from many EAP requirements as there is no applicable firewall or perimeter capability for directly connected, non-routable, serial connections.

"Data Diodes," or unidirectional communication devices, are a technology that has been the subject of much discussion in the context of NERC CIP. These devices provide the capability to send data outside of the Electronic Perimeter to maintenance applications or data historians. By removing the capability for the receiving system to reply or send back any data within the perimeter, they claim to "break" the external routable connection. NERC had issued a Compliance Application Notice (CAN-0024) on this subject, which unfortunately did not provide very clear guidance. This notice applied to CIP Version 3 and is no longer applicable, leaving us with no clear guidance on this topic.

Interactive remote access

Traffic through the EAP can be characterized as being either SCADA data used for monitoring and control, or interactive remote maintenance access. The requirements that we have discussed so far apply implicitly to machine-to-machine communications using network or data exchange protocols. Interactive remote access poses a much greater risk as it opens a communications path between a human and a BES Cyber System. NERC had already recognized this risk and issued a document entitled "Guidance for Secure Interactive Remote Access." Many of these guidelines have now been incorporated into the standards as Electronic Security Perimeter requirements.

One of the guidelines that has become a requirement is the use of an intermediate device, or proxy, so that the Cyber Asset initiating remote access does not have direct network access to a BES Cyber System or a Protected Cyber Asset within the ESP.

In addition, communications must now be encrypted to protect the confidentiality and integrity of each Interactive Remote Access session. Finally, the requirement for "strong authentication," which was kind of vague, has been replaced by a requirement for multi-factor authentication.

ANSI/ISA–99.00.01–2007 security for industrial automation and control systems

The NERC CIP standards are not the only efforts being made to protect the critical infrastructure. The International Society of Automation (ISA) is another group working on developing security and safety standards for industrial automation. As we mentioned previously, by defining the concept of network zones, the CIP Version 5 standards are coming in alignment with the work being done by ISA and other groups to secure automation systems.

The *"ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems"* standard defines a network security model based on zones and conduits. This standard is now known as *"ANSI/ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models"* and is the basis of the *"IEC 62443 Network and system security for industrial-process measurement and control"* family of standards that are currently under development.

The ISA99 standard provides valuable guidance that is applicable to the implementation of a secure architecture for an electric utility automation system. A basic premise is that it is not necessary to apply the same level of security to all components in the system. The standard thus proposes the concept of network security zones to handle the different trust levels that exist between areas or systems to protect.

In the simplest case, a security zone can be defined physically by grouping assets sharing a physical location. Alternatively, a zone can be logical or virtual, grouping assets according to their function instead of their location. As an example, within an organization all the desktop computers on a given floor can be grouped in the same zone. Alternatively, computers can be grouped by function, such as accounting or engineering. This example is often used when discussing VLAN networking technology. In an automation system, sensors and actuators would be in a different zone than an HMI or file server.

In order to determine zones, the network architect needs to determine the communications requirements of the various assets composing the system. Communication between zones is ensured by a special type of zone called a "conduit."

The following diagram illustrates the concepts of zones and conduits for an automation network.

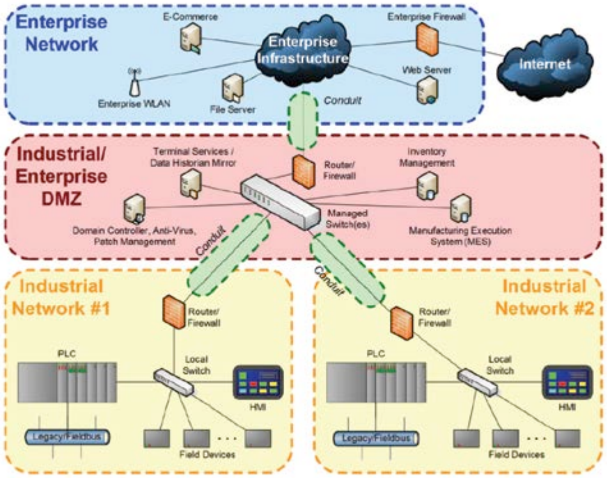

Figure 2. Zone and Conduit Example Excerpted from "ANSI/ISA 62443-1-1 (99.01.01) Draft"

The zone and conduit model provides a conceptual framework for creating a secure network architecture. As with the CIP ESP, a zone has a border that creates a boundary to identify trusted and untrusted systems. Conduits are constructs that identify communications flow. As with zones, conduits can be trusted or untrusted. Conduits that do not cross zone boundaries are typically trusted. A trusted conduit can cross zone boundaries, but it must then use end-to-end secure communications. Untrusted conduits are those that connect zones of different trust levels. It is then the responsibility of the conduit to ensure communications security. This concept is similar to the CIP EAP.

Implementing the segmented network

Defining zones and trust levels

While it is beyond the scope of this paper to perform detailed network design and propose a secure architecture, it is valuable to analyze how the utility automation system maps to the zone and conduit system.

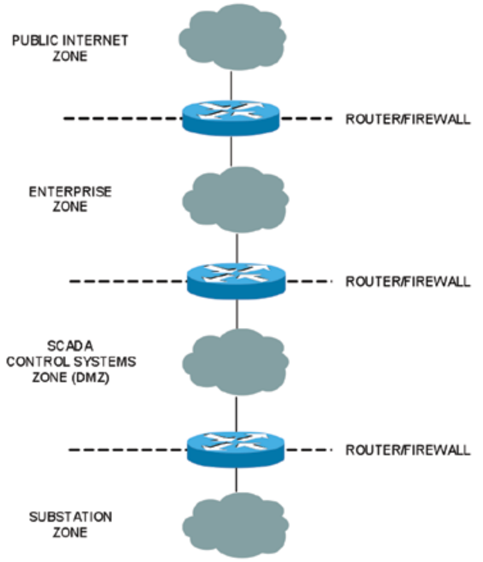

Figure 3. Utility Automation System Zones and Trust Levels Example

At a very high level, an electric utility automation system can be broken down in the following zones:

- The Public Internet zone is the least trusted and corresponds to external users, or vendors, that would require remote maintenance access through the public Internet
- The Enterprise zone corresponds to the utility business network. All devices within this zone comply with corporate IT policies and meet baseline security requirements. Corporate IT will generally subdivide the enterprise network into additional zones according to geography, or functions such as accounting and engineering. From the CIP perspective, this zone would not contain BES Cyber Systems. However, some of the enterprise-level users will require access to BES Cyber Systems in the next, more secure, level
- The SCADA and Control Systems zone contains the trusted systems that communicate with the critical substation devices. This zone is often referred to as the Demilitarized Zone (DMZ), as it acts as a "buffer" zone between trusted and untrusted zones. From the CIP perspective, this zone contains BES Cyber Systems as well as *Electronic Access Control or Monitoring Systems (EACMS), Protected Cyber Assets (PCA) and maybe Physical Access Control Systems (PACS).* This zone would also contain servers acting as intermediate devices to provide access to the BES Cyber Systems in the next level
- The Substation zone is the most trusted and contains BES Cyber Systems and BES Cyber Assets such as RTUs, data concentrators, and protection relays. Depending on the size of the substation, this zone may also be further broken down into different trust levels

As automation systems evolve, the model we have just described is rapidly becoming even more complex. Data processing capability is being added to the substation in order to reduce the dependency on the network connection to the enterprise. The substation may now include authentication servers, event processing systems, data loggers, automated password management, configuration management software, database servers, and historians. Breaking up complex substation networks into additional zones then becomes a basic requirement to provide security and ease of maintenance.

LANs

Up to now we have been discussing zones and conduits without delving on implementation details. Segmenting a network is a basic IT operation based on the use of IP subnets, switches, and routers. All devices sharing the same trust level are assigned to the same IP subnet and connected to the same network switch, or cascaded switches. A router is then used as a conduit between the different zones.

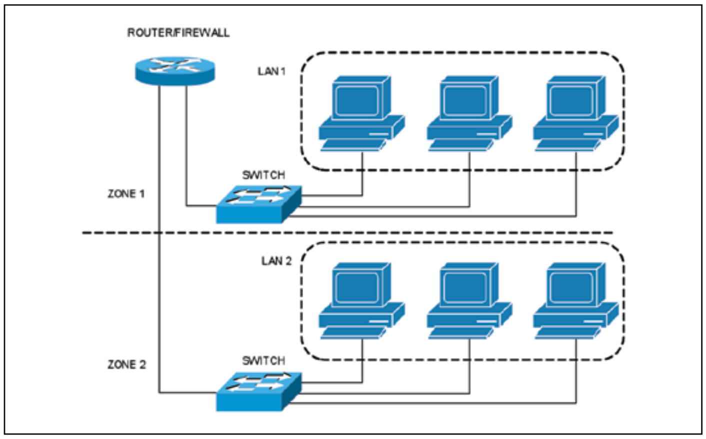

Figure 4. Network Segmentation Using LAN Segments

Besides managing the exchange of data between the different network segments, routers also provide access control and firewall capabilities, performing many of the functions of the EAP for each network segment or zone. An additional benefit resulting from this architecture is that it also provides improved performance by restricting the propagation of broadcast messages.

VLANs

LANs and subnets provide segmentation functionality at Level 3 of the TCP/IP stack. Virtual LANs (VLAN) are a technology that provides segmentation capability at layer 2 of the protocol stack. This is the layer where switches operate. Each networked device can be assigned to a VLAN. Switches that support VLANs are designed not to exchange data between devices that have different VLAN tags. In this manner, devices at different trust levels can be connected to the same switch, but still be isolated.

In the IT world, VLANs are often used when computers with different functional requirements are connected to the same physical network, i.e., engineering workstations would not be able to access financial data.

A router or a layer 3 switch with routing capability is required to exchange data between VLANs. Because devices are connected to the same switch and isolation is only ensured by network settings, VLANs are not considered as secure as separate LAN segments based on separate switches. However, they can be combined with LAN subnets to provide increased security and network performance.

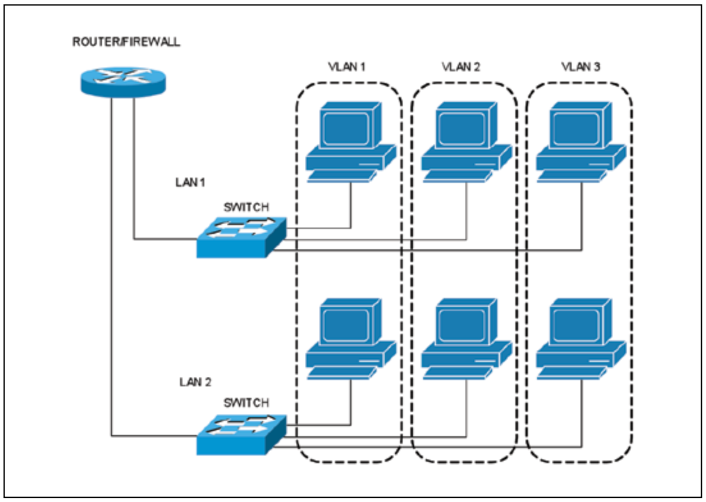

Figure 5. Network Segmentation Using VLANs

Data concentrators and security appliances

In the previous sections we have seen how standard IT switches and routers are used to implement a segmented network. Vendors of automation products have also developed OT specific solutions that provide network segmentation. A typical solution is to support multiple network adaptors and provide application-specific management rules. Each network adaptor is then assigned to a specific subnet, or to a VLAN. For instance, data concentrator products often have two network adaptors, where one is connected to the WAN and the other to the substation LAN. Such devices typically do not perform packet routing, instead they act as proxies or intermediate devices and ensure that data can only be forwarded to preconfigured devices.

Because they are designed to meet specific functional requirements, data concentrators and security appliances designed for electrical substations will generally be easier to set up and provide additional benefits when compared to general-purpose networking devices.

An example of this is the DOE funded Lemnos project, which defined standard IPsec VPN profiles for automation systems. These profiles can be used to create secure conduits between two zones. While this capability is achievable using standard routers, Lemnos-compliant devices should be easier to set up and can include additional application-specific functionality.

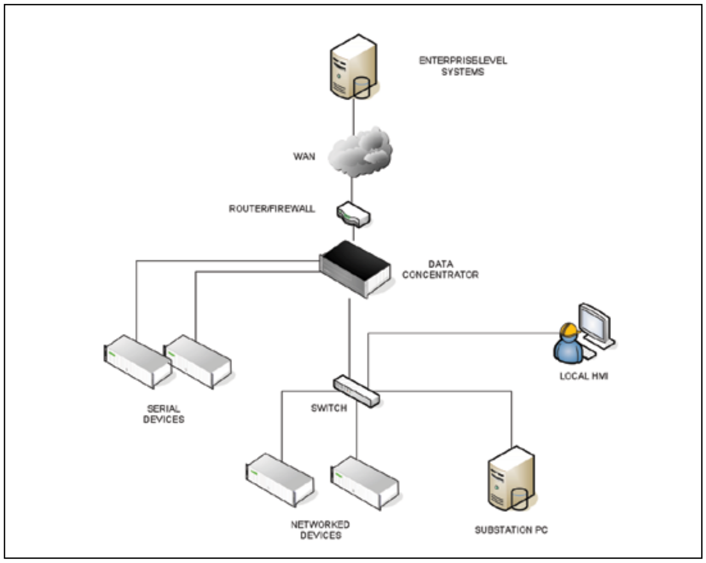

Figure 6. Network Segmentation Using a Data Concentrator

Conclusion

The NERC CIP Cyber Security standards have often been criticized for not being grounded in security best practices. This paper presented some of the technical changes in Version 5 of the standards and discussed how the standards now recognize standard IT technology and are in better alignment with industrial automation security best practices. Additional guidance on secure network architecture can be found in the ISA99, now IEC 62443-1-1 standard.

Implementing secure automation systems still remains a challenging task that requires extensive technical skills, especially from a networking perspective. While many of the applicable technologies are in common use to secure IT networks, there is still a limited number of practitioners that can bridge the gap between IT and OT. This gap may be closing as vendors of automation products introduce IT security features in their products.

References

1. "Evolving NERC CIP," Jacques Benoit, presented at Power Energy Automation Conference, Spokane, WA, March 2013.
2. NERC Critical Infrastructure Protection Standards, retrieved from: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
3. Guidance for Secure Interactive Remote Access, NERC, retrieved from: http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/2011%20Alerts/FINAL-Guidance_for_Secure_Interactive_Remote_Access.pdf.
4. ISA-62443-1-1 (99.01.01)-2007 Security for Industrial Automation and Control Systems Terminology, Part 1: Terminology, Concepts and Models.
5. Water and wastewater SCADA cybersecurity, Norman Anderson, P.E., and Bill Phillips, P.E., ISA InTech, October/November 2013, retrieved from: http://www.isa.org/InTechTemplate.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=94401.

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122
United States
Eaton.com

Printed in USA
Publication No. WP152006EN / Z16059
January 2015

Powering Business Worldwide