

# Securing Critical Control Systems in the Water Industry

## *Where Do I Begin?*

<sup>1</sup>Don Dickinson, Phoenix Contact USA, P.O. Box 4100, Harrisburg, Pennsylvania, USA, 17111  
(\*correspondence: ddickinson@phoenixcon.com)

**FORMAT:** 6-12 page paper plus 30-minute PowerPoint presentation

### **KEYWORDS**

Cyber Attack, Stuxnet, Flame, Duqu, Industrial Control System, Critical Infrastructure, Cyber Events, SCADA, Malware, Security Plan, Industrial Automation and Control Systems, Cyber Security Management System, Risk Mitigation, AWWA G430, ISA99, AWWA J100 RAMCAP, CSET

### **ABSTRACT**

Public health and safety are dependent on the availability and reliability of water systems. Cyber attacks on information technology (IT) networks are well known, but attacks on the control systems used to monitor and control plant processes are increasing in frequency and in their potential threat to public safety. The highly sophisticated Stuxnet worm discovered in 2010 was the first publicly known malware to specifically target industrial control systems used in critical infrastructure. Stuxnet is proof that potential threats to critical infrastructure can no longer be ignored.

IT professionals are responsible for ensuring the availability and security of enterprise networks. However, protecting an IT network from a cyber attack can be very different from protecting an industrial control system. As a result, plant engineering and operations will need to take an active role in developing a security plan to protect critical control systems that will minimize the potentially adverse impact of a cyber event on public health and safety. For many the greatest challenge in developing a security plan is knowing where to begin.

This paper will review existing and emerging threats to critical infrastructure and the potential impact of cyber events on water systems. An overview will be provided of industry standards, guidelines and recommendations, and other available resources to aid in the development of a utility security plan essential for protecting critical assets.

### **Introduction**

Computer networks are attacked millions of times a day. Reports of cyber attacks on IT networks are a common occurrence yet many attacks go unreported for a variety of reasons, including avoidance of negative publicity. Successful cyber attacks go undetected or are detected only after the damage has been done. Malicious attacks leading to data breaches can result in significant costs to both individuals and organizations. In its 2010 Annual Study: U.S. Cost of a Data Breach <sup>1</sup> the Ponemon Institute found that malicious or criminal attacks are the most expensive causes of IT data breaches. Additionally, nearly all respondents (97 percent) considered cyber attacks as the most severe threat to their ability to carry out their organization's mission.

Cyber threats can range from unsophisticated attacks by individuals to concerted, state-sponsored attacks that can pose serious economic threats to large populations.

***US report blasts China, Russia for cybercrime*** (Associated Press, November 3, 2011)

*U.S. intelligence officials have accused China and Russia of systematically stealing American high-tech data for their own national economic gain. It was the most forceful and detailed airing of U.S. allegations after years of private complaints. U.S. officials and cyber security experts said... cyber attacks are on the rise and represent a “persistent threat to U.S. economic security.”<sup>2</sup>*

Attacks on critical infrastructure, including water systems, occur regularly as well and can have a profound impact on the public’s security, safety and economic wellbeing. In the past, cyber threats to control systems were of limited concern given the proprietary nature of legacy systems and the relatively isolated environments in which they operated. Much has changed in the past two decades. The use of open communication standards such as Ethernet has greatly increased interconnectivity between control systems and IT networks. There are many benefits realized through increased information flow between control networks, business systems and public networks. However, increased connectivity also has allowed well-known and commonly exploited vulnerabilities in the IT world to migrate into process control networks, increasing the likelihood and severity of attacks on critical control and SCADA systems. Although the threat of cyber attack on industrial control systems (ICS) has increased, the types of attacks and mitigation strategies to counter these attacks also are well known. As asset owners and operators have begun to recognize the risk of cyber threats, there has been a dramatic change in the threat scenario.

During the last two years the threat of a cyber attack on critical infrastructure has taken on greater importance with the discovery of a highly sophisticated malware (malicious software) known as Stuxnet.

### **Stuxnet – Cyber Weapon of Mass Destruction<sup>3</sup>**

In the summer of 2010 reports of problems with nuclear centrifuges at the Natanz facility in Iran led to the discovery of Stuxnet. Security experts determined that the control system used to monitor and control the centrifuges had been infected with malware causing the centrifuges to self-destruct. The malware dubbed Stuxnet is unique because it is the first known malware that specifically targets industrial control components. More important, unlike other malware, the intent of Stuxnet was not to steal sensitive data but to do physical damage to a real-time control system. Ralph Langner, a German control system security consultant and his team were involved in deciphering the structure and purpose of Stuxnet. Mr. Langner describes Stuxnet as “...rocket science. Like nothing we’ve ever seen before.”<sup>3</sup> Given the apparent purpose of Stuxnet, Mr. Langner called it a “cyber weapon of mass destruction.”<sup>3</sup> Because of its complexity Stuxnet was believed to be a state-sponsored effort. Although no nation has officially taken credit for Stuxnet, it has been reported recently that Stuxnet was the work of the United States and Israel.<sup>4</sup> According to reports in the New York Times Stuxnet was the result of a program started under the Bush administration and accelerated by President Obama during the early part of his administration. The cyber attacks had been underway for some time; however, a coding error in one variant of the malware allowed Stuxnet to escape the Natanz facility in the summer of 2010 and spread throughout the world via the internet. Since that time two other cyberweapons related to Stuxnet have been identified – Duqu and Flame. Although different in nature and in their intended purpose, Duqu and Flame were written on the same platform as Stuxnet and are believed to have been developed as part of the same campaign.<sup>5</sup>

Some utilities might consider the threat of a state-sponsored attack unimportant due to the low probability of its occurrence. The real threat of cyberweapons such as Stuxnet is that “Pandora’s box” has been opened and now copycat attackers could use readily available malicious code as a blueprint to attack critical infrastructure in target-rich countries such as the U.S.

In an interview with Steve Kroft on a CBS 60 Minutes segment entitled “Stuxnet,”<sup>6</sup> Ret. Gen. Mike Hayden, former head of the National Security Agency and CIA director under George W. Bush said, “We have entered into a new phase of conflict in which we use a cyber weapon to create physical destruction, and in this case, physical destruction in someone else’s critical infrastructure.” In that same interview Defense Secretary Leon Panetta said, “There’s a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack.” Stuxnet is proof that the threat of cyber attacks on critical infrastructure can no longer be ignored.

### **Protecting Critical Infrastructure**

The Department of Homeland Security (DHS) is responsible for protecting and ensuring the continuity of critical infrastructure and key resources (CIKR) of the United States. Homeland Security Presidential Directive 7 (HSPD-7) established U.S. policy for enhancing protection of CIKR. This directive established a framework to identify, prioritize, and protect the nation’s CIKR from terrorist attacks. It identified 18 CIKR sectors, including the water sector. This sector includes both drinking water and wastewater utilities, which are vulnerable to a variety of attacks including cyber attacks.

A key component in protecting critical infrastructure is protecting the control and SCADA systems used to monitor and control plant processes. At the direction of DHS, the U.S. Computer Emergency Readiness Team (US-CERT) established the Control Systems Security Program (CSSP). This program aims to reduce industrial control system risks within and across all CIKR sectors by coordinating efforts among federal, state and local governments, as well as ICS owners, operators and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

### **Threats to Water Systems**

An attack on a critical control system used in a water process can significantly alter the system’s performance and negatively impact public health and safety. In their report, *Roadmap to Secure Control Systems in the Water Sector*,<sup>5</sup> the Water Sector Coordinating Council (WSCC) highlights some of the ways a cyber event could impact water system operations. The Council identified potentially adverse effects a cyber event could have on water systems as shown in Figure 1.<sup>7</sup>

To ensure the availability and reliability of water systems, control systems and SCADA networks must be protected against cyber attacks. It is important to understand the threats and associated risks to control systems in order to establish a plan for protecting critical assets.

### **Cyber Threats for Industrial Control Systems**

Establishing a plan to protect ICS from cyber attack begins with understanding the source of potential attacks. The US-CERT Control System Security Program (CSSP) referenced previously defines a cyber threat to an ICS as “a person or persons who attempt unauthorized access to a control system device and/or network using a data communications pathway. This access can be directed from within an

organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders.”<sup>8</sup>

**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 in public health. Cyber events could do the following:

- Interfere with the operation of water treatment equipment, which can cause chemical over- or under-dosing
- Make unauthorized changes to programmed instruction in local processors to take control of water distribution or wastewater collection systems, resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways
- Modify the control systems software, producing unpredictable results
- Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions
- Change alarm thresholds or disable them
- Prevent access to account information
- Although many facilities have manual backup procedures in place, failures of multiple systems may overtax staff resources—even if each failure is manageable in itself
- Be used as ransomware

**Figure 1:** How

Can Cyber Events Affect Water Systems?<sup>7</sup>

A critical point is that a cyber threat can come not just from outside the organization, but from inside as well, even by a trusted user. This point is reinforced by the fact that Stuxnet is believed to have been introduced into the Iranian nuclear plant on a USB memory stick. A security strategy of maintaining an “air gap” between critical control networks and the outside world does not fully address the threat of cyber attacks. A comprehensive plan to reduce the threat of cyber attack on control systems and networks must consider all possible threats.

### **Why Control Networks Need Security**

Cyber attack is only one of many threats to ICS. Preventing or minimizing the possibility of any action, intended or otherwise, that impacts the availability and reliability of a critical control system should be a priority. A variety of cyber events can impact system performance, including:

- Technical defects: Hardware problems resulting in broadcast storms that overload the network and limit access to control functions and data
- Human errors: Improper operation of system, introduction and dissemination of malware or phishing, resulting in reduced system reliability or loss of sensitive data
- Malware (malicious software): Harmful software that negatively impacts system operation or loss of data
- Intended, targeted attacks from inside and outside: Sabotage, espionage, white-collar crime or cyber terrorism resulting in loss of control, or denial-of-service of critical systems, loss of sensitive data, extortion or theft-of-service

These same threats also apply to IT networks; however, the associated risks have far different implications for control networks used in critical infrastructure. When a critical system is disabled or its reliability diminished, the results can lead to:

- Loss of control over critical functions negatively impacting public health and safety and the environment
- Loss of compliance with regulatory directives resulting in fines or litigation
- Damage to public image or loss of public confidence
- Denial-of-service resulting in economic losses

### **Developing a Security Plan for Control Systems – *Where do I begin?***

When developing a security plan to protect critical control and SCADA systems, it is important to remember that cyber security is not an absolute. It is not a “safe” versus “unsafe” matter. Security is a matter of degree. Additionally, because of limits to resources such as funding and personnel, it is neither practical nor feasible to mitigate all threats. There will always be risks associated with any plan. Asset owners and operators must determine acceptable levels of risk and establish an appropriate plan to mitigate known vulnerabilities. Further, because control systems and networks change over time, utilities must reassess risks and vulnerabilities on a recurring basis and security plans revised as needed.

### **Standards, Guidelines and Recommendations**

Although there are no specific directives in the water sector for securing ICS, there are numerous standards, guidelines and recommendations that are useful in developing a security plan for protecting critical control systems as part of an overarching security plan.

The ANSI/AWWA G430-09 standard: Security Practices for Operation and Management <sup>9</sup> provides a framework for establishing a security plan. Its purpose is to define the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence. The standard defines a security plan as a comprehensive plan developed by the utility, which includes its security goals, objectives, strategies, policies and procedures. The security plan should coordinate closely with the utility’s Emergency Preparedness Plan and Business Continuity Plan. A key point of the standard is the establishment of an **explicit commitment to security**.

Section 4.1.1 Explicit and visible commitment of senior leadership to security: The utility shall establish an explicit, visible, easily communicated, enterprise-wide commitment to security. <sup>9</sup>

Given the rapid change of cyber threats to ICS, an effective, sustainable security plan to protect critical systems requires a commitment to security supported by policies, procedures and personnel.

The G430-09 standard addresses various aspects of security such as intrusion detection and contamination detection. The standard also addresses protection of critical, security-sensitive and information systems that are essential to the efficient and continuous operation of a utility. The G430-09 standard recommends the *Roadmap to Secure Control Systems in the Water Sector* <sup>7</sup> as an aid in evaluating ICS or SCADA vulnerabilities and for strategies in securing critical control systems.

## Roadmap to Secure Control Systems in the Water Sector

The *Roadmap to Secure Control Systems in the Water Sector* (Roadmap) was developed by the Water Sector Coordinating Council (WSCC) Cyber Security Working Group (CSWG) with support from the Department of Homeland Security National Cyber Security Division and American Water Works Association (AWWA). The Roadmap considers many variables for mitigating vulnerabilities and reducing risks to control systems in the water sector.

The purpose of the Roadmap is to:

- Define a consensus-based framework that articulates strategies to manage and reduce risks to ICS
- Produce a broad-based plan for improving security preparedness, resilience, and response/recovery of ICS
- Guide efforts of industry, academia and government to plan, develop and implement ICS security solutions
- Promote extensive collaboration among key stakeholders to accelerate ICS security in the water sector

The key provision of the Roadmap is to define a strategy for securing ICS in the water sector. The Roadmap outlines the vision, challenges, goals, milestones and end state of this strategy. As noted in the Roadmap, by implementing this strategy “industry leaders believe that within ten years (by 2018) ICS throughout the water sector will be able to operate with no loss of critical function in vital applications during and after a cyber event.

**Vision for Securing Industrial Control  
Systems in the Water Sector**

---

**In 10 years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event.**

**Figure 2: Roadmap - Vision for Securing ICS in the Water Sector**<sup>7</sup>

This vision confronts the formidable technical, business, operational, and societal challenges that lie ahead in strengthening the resilience of critical systems against increasingly sophisticated cyber attacks.”<sup>7</sup>

The G430-09 standard provides a framework for developing an overarching security plan for a utility while the Roadmap highlights general strategies for securing critical control systems. They are not meant to be a recipe for securing ICS. Asset owners and operators require a more prescriptive standard for developing a comprehensive security plan for industrial automation and control systems.

### **ISA99 Security for Industrial Automation and Control Systems**

The Industrial Automation and Control Systems committee (ISA99) of the International Society of Automation (ISA) produces standards, recommended practices, technical reports and related information defining procedures for implementing electronically secure manufacturing and control systems, and security practices for assessing electronic security performance. The ISA99 committee is

developing a multipart standard focused on cyber security for industrial automation and control systems (IACS). The components of the ISA99 series are listed in Table 1.

<b>ANSI/ISA-99.01.01-2007</b>	Terminology, Concepts and Models
<b>ANSI/ISA-TR99.01.02-2007</b>	Security Technologies for Industrial Automation and Control Systems
<b>ANSI/ISA-99.02.01-2009</b>	Establishing an Industrial Automation and Control System Security Program
<b>ISA-99.02.02</b>	Operating an Industrial Automation and Control System Security Program ( <i>in development</i> )
<b>ISA-99.03.xx</b>	Technical Security Requirements for Industrial Automation and Control Systems ( <i>in development</i> )

**Table 1: The ISA99 Series: Security for Industrial Automation and Control Systems**<sup>10</sup>

Three parts of the series have been publicly released as American National Standards Institute (ANSI) documents. The other two are currently under development. The ISA99 series also serves as a foundation for the IEC 62443 series of the same title being developed by the International Electrotechnical Commission (IEC).<sup>10</sup>

The ISA99 series provides guidance for those designing, implementing or managing control systems as well as users, system integrators, security practitioners and, control systems manufacturers and vendors. The purpose of the standards is to improve the confidentiality, integrity and availability of components or systems used for manufacturing or control and, provide criteria for procuring and implementing secure control systems.<sup>11</sup>

#### **ANSI/ISA-99.01.01-2007 Terminology, Concepts and Models**

This standard describes the basic concepts and models relating to cyber security and serves as the basis for the other parts of the ISA99 series. It focuses primarily on industrial automation and controls and SCADA (supervisory control and data acquisition) systems used in critical infrastructure industries such as water and wastewater. In addition to defining key concepts and terminology the standard provides a series of models that can be used in the design of a security program. These control and SCADA system models are used to identify security needs at a level of detail necessary to address security issues with a common understanding of the framework and vocabulary.<sup>12</sup>

#### **ANSI/ISA-99.02.01-2009 Establishing an Industrial Automation and Control System Security Program**

This standard describes the elements contained in a cyber security management system (CSMS) for use in the IACS environment and provides guidance on how to develop those elements. These elements are primarily related to policy, procedures, practice and personnel and are grouped into three main categories:

- Risk analysis
- Addressing risk with the CSMS
- Monitoring and improving the CSMS

As noted in the standard, *It is not the intent of the standard to specify a particular sequential process for identifying and addressing risk that incorporates these elements. Thus, an organization will create such*

*a process in accordance with its culture, organization, and the current status of its cyber security activities.*<sup>10</sup> However, to assist organizations with application of the standard an example of a process for identifying and addressing risk is provided as well as a step-by-step guide that an organization can reference as they can begin to establish a cyber security management system.

The first main category of a CSMS is Risk analysis that includes risk identification, classification and assessment. There is a number of risk assessment methodologies available on the market that identify and prioritize risks related to IACS assets. A free Cyber Security Evaluation Tool (CSET) available from DHS is discussed later in this paper.

The second main category is addressing risk with a CSMS. This category contains the bulk of the CSMS requirements and is divided into three element groups:

- Security policy, organization and awareness
- Selected security countermeasures
- Implementation

The third main category is Monitoring and improving the CSMS. Elements in this category ensure that the CSMS is being used and its effectiveness reviewed on a regular basis.

### **Assessing Risk**

Developing an actionable plan for protecting critical systems begins with understanding vulnerabilities and associated mitigation strategies. There are a variety of assessment tools available to aid in this process.

Risk is defined as a function of the likelihood of an event, vulnerability to the event, and the consequence of the event. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 required water utilities serving more than 3,300 people to perform security vulnerability assessments.<sup>13</sup> Various methodologies were developed or adopted by industry groups to conduct these vulnerability assessments for utilities. These methodologies assess the general security posture of a utility and are instrumental in helping asset owners and operators make informed decisions on resource allocation to mitigate risk in the most efficient manner possible.

Risk assessment tools are available to aid in the evaluation of IACS as well. A useful tool from DHS is the Cyber Security Evaluation Tool (CSET) that assists organizations in protecting their key cyber assets. CSET is a stand-alone, desktop software tool that guides users through a step-by-step process to assess their control system and IT network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cyber security posture of the organization's enterprise and industrial control cyber systems. CSET is available from the DHS National Cyber Security Division as a download or DVD.

Cyber risk assessment tools such as CSET are useful in securing critical control systems and thus help to protect critical infrastructure. However, asset owners may want a more holistic security methodology, one that mitigates risk for "all hazards", both naturally occurring and intended attacks. The Risk Analysis and Management for Critical Asset Protection (RAMCAP®)<sup>13</sup> standard meets that need. RAMCAP is a process for analyzing and managing the risks to critical infrastructure associated with intended attacks, such as a cyber attack, and naturally occurring hazards such as hurricanes and tornadoes. As part of a

RAMCAP analysis, risks from specific reference threat scenarios can be quantified to assess options for reducing these elements of risk. This process allows for evaluation of the benefit (changes in threat likelihood, vulnerability, and/or consequences) versus the cost of a specific countermeasures or mitigation option. As a result, decisions on resource allocation can be made based on the benefit-to-cost ratio ensuring the most efficient use of resources to protect critical assets.

One of the RAMCAP reference hazards is Sabotage, either by physical attack or a cyber attack. In both scenarios the attack can be quantified as an attack by an insider or by someone outside the organization. By including cyber attacks as a reference hazard, RAMCAP ensures that all hazards are considered when developing a security plan.

## Summary

The Department of Homeland Security identified the water sector as one of the critical infrastructures and key resources essential to the nation's security, public health and safety, economic vitality, and way of life. Protecting critical infrastructure from the threat of cyber attack has become more challenging due to the increased connectivity between critical control systems and enterprise networks. Cyber attacks on control and SCADA systems are increasing in frequency and severity. Stuxnet is proof that threats to critical assets cannot be ignored. Industry standards, guidelines and recommendations are useful aids for developing strategies for protecting industrial automation and control systems. Risk analysis and management methodologies for the water industry are essential tools for establishing security plans for critical asset protection and resource allocation. The development of comprehensive security plans will help to ensure the availability and reliability of water systems in the future.

## List of Acronyms

AWWA.....	American Water Works Association
CIKR .....	Critical Infrastructure and Key Resources
CSET.....	Cyber Security Evaluation Tool
CSMS .....	Cyber Security Management System
CSSP.....	Control System Security Program
CSWG .....	Cyber Security Working Group
DHS.....	Department of Homeland Security
HSPD-7 .....	Homeland Security Presidential Directive - 7
IACS .....	Industrial Automation and Control Systems
ICS .....	Industrial Control System
IT .....	Information Technology
RAMCAP® .....	Risk Analysis and Management for Critical Asset Protection
SCADA .....	Supervisory Control and Data Acquisition
US-CERT.....	U.S. Computer Emergency Readiness Team
WSCC.....	Water Sector Coordinating Council

## References

- <sup>1</sup> Ponemon Institute. "2010 Annual Study: U.S Cost of a Data Breach." March 2011.
- <sup>2</sup> Baldor, Lolita C., The Associated Press. "US report blasts China, Russia for cybercrime." November 3, 2011.
- <sup>3</sup> "Ralph Langer: Cracking Stuxnet, a 21<sup>st</sup> century cyber weapon." TED2011 TALKS. Web. <[http://www.ted.com/talks/ralph\\_langner\\_cracking\\_stuxnet\\_a\\_21st\\_century\\_cyberweapon.html](http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html)>
- <sup>4</sup> Sanger, David E., The New York Times. "Obama Order Sped Up Wave of Cyberattacks Against Iran." June 1, 2012. [http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?\\_r=1&pagewanted=all](http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all)
- <sup>5</sup> Perlroth, Nicole, The New York Times. "Researchers Find Clues in Malware." May 30, 2012. [http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html?\\_r=1](http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html?_r=1)
- <sup>6</sup> Steve Kroft. "Stuxnet" CBS News 60 Minutes. Aired March 4, 2012 <[http://www.cbsnews.com/8301-18560\\_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/?tag=contentMain;contentBody](http://www.cbsnews.com/8301-18560_162-57390124/stuxnet-computer-worm-opens-new-era-of-warfare/?tag=contentMain;contentBody)>
- <sup>7</sup> Water Sector Coordinating Council Cyber Security Working Group. "Roadmap to Secure Control Systems in the Water Sector." March 2008. Web. <<http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf>>
- <sup>8</sup> US Computer Emergency Readiness Team. Cyber Threats Source Descriptions. Web. <[http://www.us-cert.gov/control\\_systems/csthreats.html](http://www.us-cert.gov/control_systems/csthreats.html)>
- <sup>9</sup> ANSI/AWWA G430-09 (First Edition) Standard: Security Practices for Operation and Management (Effective date: May 1, 2009)
- <sup>10</sup> ANSI/ISA-99.02.01-2009: Security for Industrial Automation and Control Systems, Part -2: Establishing an Industrial Automation and Control System Security Program (approved January 13, 2009)
- <sup>11</sup> ISA99, Industrial Automation and Control Systems Security. <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>
- <sup>12</sup> ANSI/ISA-99.00.01-2007: Security for Industrial Automation and Control Systems, Part -1: Terminology, Concepts, and Models (approved October 29, 2007)
- <sup>13</sup> ANSI/ASME-ITI/AWWA J100-10 (First Edition) Standard: Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems (Effective date: July 1, 2010)

## Resources for Additional Information on Protecting Control Systems:

### Department of Homeland Security: Protecting Critical Infrastructure

[http://www.dhs.gov/files/programs/gc\\_1189168948944.shtm](http://www.dhs.gov/files/programs/gc_1189168948944.shtm)

Homeland Security Presidential Directive 7 (HSPD-7) established U.S. policy for enhancing protection of Critical Infrastructure and Key Resources (CIKR) by establishing a framework to identify, prioritize, and protect the nation's CIKR from terrorist attacks. The directive identified 17 CIKR sectors and designated a federal Sector-Specific Agency (SSA) to lead CIKR protection efforts in each. The Environmental Protection Agency (EPA) is the Federal lead for the Water Sector's critical infrastructure protection activities. All EPA activities related to water security are carried out in consultation with DHS and the EPA's Water Sector partners. The Water Sector includes both drinking water and wastewater utilities that are vulnerable to a variety of attacks including cyber attacks. Successful attacks would impact public health and economic vitality.

### U.S. Computer Emergency Readiness Team (US-CERT)

<http://www.us-cert.gov/>

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at the Department of Homeland Security (DHS). It is a public-private partnership. The NCSD was established by DHS to serve as the federal government's cornerstone for cyber security coordination and preparedness, including implementation of the National Strategy to Secure Cyberspace. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. US-CERT interacts with federal agencies, industry, the research community, state and local governments, and others to disseminate reasoned and actionable cyber security information to the public.

### Control Systems Security Program (CSSP)

[www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)

The goal of the DHS National Cyber Security Division's Control Systems Security Program (CSSP) is to reduce industrial control system risks with and across all critical infrastructure and key resource sectors by coordinating efforts among federal, state, local and tribal governments, as well as industrial control systems owners, operators and vendors. The CSSP coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation activities.

### US-CERT Cyber Security Evaluation Tool (CSET)

[http://www.us-cert.gov/control\\_systems/satool.html](http://www.us-cert.gov/control_systems/satool.html)

The Cyber Security Evaluation Tool (CSET) is a DHS product that assists organizations in protecting their key cyber assets. CSET is a desktop software tool that guides users through a step-by-step process to assess their control system and IT network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cyber security posture of the organization's enterprise and industrial control cyber systems. CSET is available from the DHS National Cyber Security Division, on DVD.

### **About the Author**

**Don Dickinson** has more than 27 years of sales, marketing and product application experience in Industrial Controls and Automation, involving a wide range of products and technologies in various industry segments. Don is the Senior Business Development Manager – Water Sector for Phoenix Contact USA and is the current chair of the NC AWWA-WEA Automation Committee. He can be reached at [ddickinson@phoenixcon.com](mailto:ddickinson@phoenixcon.com).

### **About Phoenix Contact**

Phoenix Contact is a leading developer of industrial electrical and electronic technology. The company's diverse product range includes components and system solutions for industrial and device connection, automation, electronic interface and surge protection. Phoenix Contact GmbH & Co. KG, Blomberg, Germany, operates 46 international subsidiaries, including Phoenix Contact USA in Middletown, Pa. Phoenix Contact's formal Integrated Management System is registered to ISO quality, environmental and safety standards (ISO 9001:2008, 14001:2004 and 18001:2007).