



## Protecting Water Industry Control and SCADA Systems from Cyber Attacks

**A White Paper presented by:**

Don Dickinson  
Project Engineer  
Phoenix Contact  
P.O. Box 4100  
Harrisburg, PA 17111-0100  
Phone: 717-944-1300  
Fax: 717-944-1625  
Website: [www.phoenixcontact.com](http://www.phoenixcontact.com)



## Protecting Water Industry Control and SCADA Systems from Cyber Attacks

### Key concepts:

- The U.S. Department of Homeland Security has identified the water sector as one of the critical sectors essential to the nation's public health and safety, economic vitality and way of life
- Water systems are vulnerable to a variety of attacks, including cyber attacks
- Cyber attacks on information technology (IT) networks are well known, but systems for monitoring and controlling plant processes are also coming under attack
- IT professionals and control engineers both have a role to play to ensure proper operation of crucial infrastructure
- This white paper highlights security challenges for control networks, general strategies for securing networks in industrial installations and SCADA systems and identifies key resources for additional information on protecting critical infrastructure from cyber attack

### Introduction

*Botnet ring said to infect 12.7 M PCs (USA TODAY March 3, 2010) Authorities have smashed one of the world's biggest networks of virus-infected computers, a data vacuum that stole credit cards and online banking credentials from as many as 12.7 million poisoned PCs. The "botnet" (network of robot PCs) of infected computers included PCs inside more than half of the Fortune 1,000 companies and more than 40 major banks.<sup>1</sup>*

Reports of cyber attacks are a common occurrence. However, many attacks go unreported for a variety of reasons, including avoidance of negative publicity. Successful cyber attacks go undetected or are only detected after the damage has been done. Computer networks are probed and attacked millions of times a day.

In a speech in May 2009, President Obama stated, "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation. We're not as prepared as we should be, as a government or as a country."<sup>2</sup>

Attacks on critical infrastructure, including water systems, occur regularly as well. The impact of these attacks can go well beyond the loss of sensitive data. Attacks on control systems and SCADA networks can have a profound impact on the public's security, safety and economic wellbeing.

### Protecting Critical Infrastructure

*Insider Hacks Into Sewer Treatment Plant (Australia, 2001) A former employee of the software developer repeatedly hacked into the SCADA system that controlled a Queensland sewage treatment plant, releasing about 264,000 gallons of raw sewage into nearby rivers and parks.<sup>3</sup>*

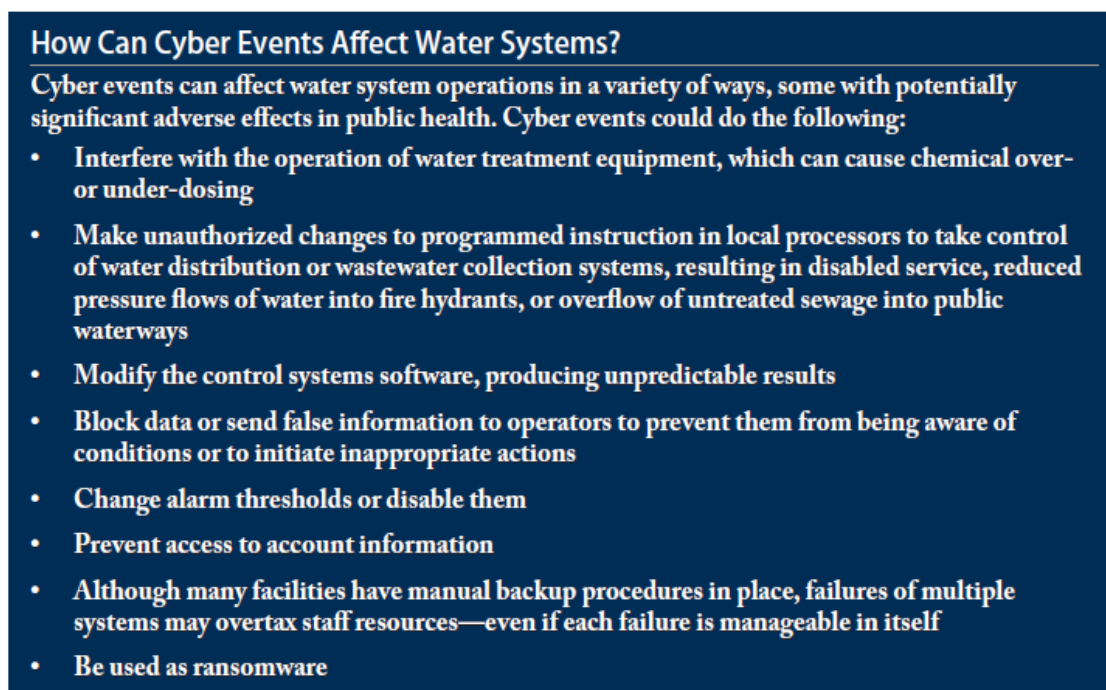
The Department of Homeland Security (DHS) is responsible for protecting and ensuring the continuity of the critical infrastructure and key resources of the United States. Homeland Security Presidential Directive 7 (HSPD-7) established U.S. policy for enhancing protection of Critical Infrastructure and Key Resources (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 in each of the sectors. 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 with and across all CIKR sectors by coordinating efforts among

federal, state and local 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.

### Threats to Water Systems

An attack on the control and/or SCADA system used in a water system 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>4</sup> the Water Sector Coordinating Council highlights some of the ways a cyber event could impact water system operations. The Council identified some possible adverse effects a cyber event could have on water systems, shown in Figure 1.<sup>4</sup>



**Figure 1:** How Can Cyber Events Affect Water Systems?<sup>4</sup>

To ensure the availability and reliability of water systems, the control systems and SCADA networks used to monitor and control plant processes 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 systems.

### Cyber Threats for Control Systems

Establishing a plan to protect control and SCADA systems from cyber attack begins with understanding the source of potential attacks. The US-CERT Control Systems Security Program (CSSP) defines a cyber threat to a control system 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>15</sup>

A critical point is that a threat can come not just from outside the organization, but from inside as well, even by a trusted user. A 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 critical control networks. Preventing or minimizing the possibility of any action, intended or otherwise, that impacts the availability and reliability of a control system, should be a priority. A variety of 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 (worms): 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. When a critical system is disabled or its reliability diminished, the results can lead to:

- Loss of production resulting in economic losses and denial-of-service
- Damage to health and environment as the result of unsafe operation or release of hazardous materials
- Loss of intellectual property such as process knowledge or sensitive data
- Loss of compliance with regulatory directives resulting in fines or litigation
- Damage to corporate image or loss of public confidence

To better understand how to protect critical systems from potential threats and their associated risks, it will be helpful to have an awareness of how control systems can be vulnerable to attack. Once specific vulnerabilities have been identified, a plan for mitigating these vulnerabilities can be established.

## Control System Vulnerabilities

Like the water sector, the energy sector is another critical infrastructure identified by HSPD-7. The energy sector (including electric power) is well aware of its vulnerabilities. The industry is leading a significant, voluntary effort to increase its planning and preparedness. Many owners and operators in the energy industry have extensive experience with infrastructure protection. More recently, the industry has focused its attention on cyber security. The Energy Policy Act of 2005, signed by President Bush, requires the implementation of mandatory electricity reliability standards in the U.S.<sup>6</sup>

The North American Electric Reliability Corporation (NERC) is a key agency tasked with ensuring the reliability of the bulk power system in North America. The NERC Control System Security Working Group (CSSWG) identified common vulnerabilities to control systems in the electric sector. Their list of the top ten vulnerabilities can serve as template for evaluating vulnerabilities for control systems used in the water sector as well.

### Top 10 (non-prioritized) Control System Vulnerabilities<sup>7</sup>

1. Inadequate policies, procedures, and culture governing control system security.
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms.
3. Remote access to the control system without appropriate access control.
4. Auditable system administration mechanisms (system updates, user metrics, etc.) are not part of control system implementation.
5. Inadequately secured wireless communication.
6. Use of a non-dedicated communications channel for command and control, such as Internet-based SCADA, and/or inappropriate use of control system network bandwidth for non-control purposes (e.g., VOIP).

7. Lack of quick and easy tools to detect and report on anomalous or inappropriate activity. Inadequate or non-existent forensic and audit methods.
8. Installation of inappropriate applications on critical control system host computers.
9. Software used in control systems is not adequately scrutinized.
10. Control systems command and control data is not authenticated.

Once specific vulnerabilities have been identified, mitigation strategies can be devised and implemented. A useful tool from DHS is the Cyber Security Evaluation Tool (CSET) 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.

When planning mitigation strategies, 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. There will always be risks associated with any plan. Organizations must determine acceptable levels of risk and establish an appropriate plan to mitigate known vulnerabilities. Further, because control systems and networks change over time, the operators must reassess vulnerabilities on a recurring basis and mitigation plans must be revised as needed.

*Cyber Incident Blamed for Nuclear Power Plant Shutdown (June 5, 2008) A nuclear power plant in Georgia was recently forced into an emergency shutdown for 48 hours after a software update was installed on a single computer.<sup>8</sup>*

Securing critical control and SCADA systems requires more than just protecting them from cyber attack. Ensuring availability and reliability of critical systems involves a thorough evaluation of all vulnerabilities that could impact system operation and taking appropriate steps to limit possible risks.

## **Securing Control Systems and Networks**

There are many facets to network security; however, there are many things that easily can be done to increase the security of control networks. First, take control of the situation. Recognize that everyone has a role to play in security – not just the IT department. Next, take simple steps, such as controlling physical access to critical components such as computers and network infrastructure components. Limiting access to these devices is a simple way to improve network security. Use other common sense measures such as managing passwords. Change default passwords and keep user lists up-to-date.

Once a connection is made to the network, there are various means of controlling access to devices on the network and how data is accessed over the network. A key strategy in defending a control network is to limit traffic, both into and out of the network. Segmenting critical networks from IT networks and other control networks provides a wider range of options for implementing security strategies.

Ethernet has become the de facto local area network (LAN) technology for industrial communications. The infrastructure components that make up an Ethernet network provide many of the functions needed to secure control networks.

An Ethernet switch typically provides the point of connection to the network via the ports on the switch. A switch provides the communications path between stations on the LAN. Managed switches provide useful security features such as port security. Ports can be enabled and disabled to control which devices can access the network. A simple but effective security precaution is disabling unused ports to prevent someone from gaining unauthorized access to the network.

Managed switches can also determine which Ethernet devices can access the network using MAC filtering. Every Ethernet device has a unique electronic serial number called a MAC (media access control) address. Based on the MAC address, a switch can permit or deny connection to the network. MAC filtering provides another security feature that helps to secure critical networks. For example, MAC filtering can be set to allow operations and

maintenance staff to connect their PCs to the network, but deny access to all others. Managed switches provide many more useful functions for both security and network management.

A router plays an important role in network security. A router controls communication between networks and provides many functions directly related to security. Routers can be used to insulate and isolate critical systems from network traffic, and to segment large networks into logical groups to improve performance. When used in conjunction with firewalls, routers can significantly increase the level of security in critical control systems.

## Firewalls

A firewall is a hardware appliance or software application that filters network traffic based on user-defined or pre-configured rules. It provides a line of demarcation in the network at its point of application, separating upstream network devices from downstream devices. For industrial networks, a hardware solution is preferred over a software firewall application for several reasons. Generally, a hardware firewall has lower latencies than a software application when processing firewall rules. Hardware does not drain the resources of the PC being used in the process and can protect multiple devices (including non-Windows-based devices). A hardware firewall will stop unwanted traffic from ever reaching a critical component.

There are different types of firewalls. A stateful firewall is well suited for use in control systems. In addition to the functions provided by a basic firewall, a stateful firewall inspects incoming and outgoing packets. Only packets matching a known connection type are allowed to pass. By rejecting all other connections, the stateful firewall provides protection from certain types of attacks. A stateful firewall performs these stateful inspections with low latency, ensuring communication for critical control is not negatively impacted.

A firewall that employs deep packet inspection provides a more thorough inspection of packets, but might not be as well suited for industrial control networks. Deep packet inspection analyzes the actual payload of data packets, but it costs more, requires more processor resources, and increases communication latency. These issues are not a concern at the IT level; however, increased latencies as part of a real-time control process could impact the performance of a control system.

## Defense-In-Depth

An important concept in securing control systems and networks is a defense-in-depth strategy. This security concept, taken from the military, establishes multiple layers of defense to protect against attacks. Multiple layers of defense require an attacker to penetrate many smaller and varied layers of defense rather than one large, single layer, which might have a flaw. Defense in depth limits the scope of attack to only the layer(s) that have been breached. Additionally, when an outer layer is breached, counter measures can be taken to prevent further intrusion.

Applying the defense-in-depth concept to a control network results in the use of several industrial routers with firewall functionality deployed at various levels in the control network. The industrial router can be used in conjunction with the IT security infrastructure to enhance the overall safety of the network. As a general strategy, the IT corporate firewall protects the enterprise from outside threats, the IT router(s) protect the corporate office network segments, and the industrial router(s) protect the control network and individual devices. A defense-in-depth strategy provides a very secure control network.

## Virtual Private Networks

By its very nature, the water industry operates as a decentralized process with geographically dispersed assets. The industry uses a variety of mediums to communicate with distant water distribution and wastewater collection systems. Traditionally, modems communicate to remote sites over phone lines and wireless telemetry.

Remote connectivity provides many benefits, such as access to process data and alarm notifications. However, the use of modems and wireless telemetry limits the type and amount of data that can be sent. The use of public communications infrastructure, such as the Internet, has brought additional benefits, but increased the need for

additional security. A virtual private network (VPN) is ideal for secure communications between multiple networks or multiple hosts. A VPN establishes a “tunnel” across the Internet that keeps data safe from “sniffing” or corruption. VPN communications are secure regardless of the path taken or the distance traveled. As a result, a greater variety of data can be sent securely and at much greater speeds. This enhances control system performance, remote support and administrative functions. Integrating VPN functionality into the industrial router can provide seamless operation of the firewall, router and VPN.

**Industrial Network Components**

Industrial-grade devices used in industrial networks have many of the same functions as the commercial-grade components employed by IT departments. A key difference is that industrial network devices are designed and packaged for installation in harsh environments, typically in control cabinets or junction boxes on the shop floor.

Another difference between industrial and commercial network devices is how those devices are configured and managed. IT tools for network management and diagnostics are highly specialized, typically text-based and require manufacturer-specific training and certification to use competently. Industrial network components typically use web-based management tools. They generally do not require special software. A standard web browser can be used to configure and diagnose network devices, simplifying support by plant personnel. Some general comparisons between industrial and commercial grade components are listed in Table 2.

<b>Industrial</b>	<b>Commercial</b>	<b>Benefit of Industrial</b>
DIN rail mount	Mounting different than control components such as 19” rack mount	Easy to install in control cabinet
24 V DC power	120 V AC, receptacle and transformer required	Can be powered by the 24V DC power supply
High temperature and humidity ratings	Low to medium temperature and humidity ratings	No auxiliary cooling required
High shock & vibration ratings	Typically no shock or vibration ratings	Can be mounted on moving equipment or next to impact loads such as presses
High noise immunity	Low noise immunity	2 to 3 times greater immunity to electrical noise, can be mounted next to power devices such as drives
Industrialized connectors	Office-grade connectors	Robust connections for reliability
Web-based management and configuration of network devices	IT-centric configuration and management tools for network devices	Ease of support and configuration of network devices by plant personnel

**Table 2:** Comparison of Industrial vs. Commercial Grade Network Components

**Conclusion**

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 has become more challenging as control systems, SCADA networks, IT networks and business systems become more interconnected, increasing the threat of cyber attack.

Securing control and SCADA systems used in the water industry begins with recognizing that critical control systems can and will be attacked. A concerted effort by all involved with control system design and operation, along with the organization’s IT professionals will ensure the availability and reliability of water systems in the future.

### **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 47 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).

### **About the Author**

Don Dickinson has twenty-six years of experience in industrial controls and automation and has been involved in a wide range of technologies and industry segments. In his role as a Project Engineer with Phoenix Contact, Don works with consulting engineers in various industries to identify solutions for process applications.

### **Resources for further information and tools for 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**

[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.

## References

- <sup>1</sup> USA TODAY. "Botnet ring said to infect 12.7 M PC's." March 3, 2010.
- <sup>2</sup>Baldor, Lolita, Associated Press. "Obama setting up better security for computers." May 29, 2009.
- <sup>3,4</sup> Water Sector Coordinating Council Cyber Security Working Group. "Roadmap to Secure Control Systems in the Water Sector." March 2009. Web. <<http://www.nawc.org/policy-issues/utility-security-resources/Final%20Water%20Security%20Roadmap%2003-19-08.pdf>>.
- <sup>5</sup> US Computer Emergency Readiness Team. Cyber Threats Source Descriptions. May 2005. Web. <[http://www.us-cert.gov/control\\_systems/csthreats.html](http://www.us-cert.gov/control_systems/csthreats.html)>.
- <sup>6</sup> Department of Homeland Security. "National Infrastructure Protection Plan: Energy Sector Snapshot." December 2008. Web. <[http://www.dhs.gov/xlibrary/assets/nipp\\_snapshot\\_energy.pdf](http://www.dhs.gov/xlibrary/assets/nipp_snapshot_energy.pdf)>.
- <sup>7</sup> North American Electric Reliability Council Control System Security Working Group. "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations." 2006.
- <sup>8</sup>Krebs, Brian. washingtonpost.com. "Cyber Incident Blamed for Nuclear Power Plant Shutdown." June 5, 2008. Web. <<http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html>>.