CERIAS Tech Report 2012-15
Mapping Water Sector Cyber-Security Vulnerabilities
by James H. Graham, Jeffrey L. Hieb and J. Chris Foreman
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Mapping Water Sector Cyber-Security Vulnerabilities

James H. Graham, Jeffrey L. Hieb and J. Chris Foreman
Intelligent Systems Research Laboratory
University of Louisville
Louisville, Kentucky 40292

Abstract

This paper identifies, characterizes, maps, and prioritizes cyber-vulnerabilities in the industrial control systems which are used throughout the Water Sector (includes both drinking water and wastewater treatment facilties). This report discusses both technical vulnerabilities and business/operational challenges, with concentration on the technical issues. The priority order is based upon the research team's review of the "Road Map to Secure Control Systems in the Water Sector," DHS Control Systems Security Program documents, a CSET-CS2SAT evaluation, and from comments by the project advisory board and individual discussion with water sector personnel.

The major technical cyber-security vulnerabilities for water sector industrial control systems, in priority order, are: poorly secured legacy systems, lack of trained cyber-security specialists for water sector control systems, delayed application of operating system and application software patches, lack of cyber-security situational awareness, unsecured communication between components, and poorly secured remote access. The business and operational challenges include, but are not limited to, the following: lack of a business case for cyber-security, lack of risk management integration, and existence of a two cultures problem between IT and control systems personnel. Related and relevant on-going research for cyber-security vulnerabilities is included, along with identified needed additional research for each vulnerability area.

Key Words: Cyber-security, Water Sector, Vulnerabilities, Assessment

1 Introduction

Recent events in the United States and around the world have highlighted the threat to critical infrastructure components, such as the electric grid, oil and gas pipelines, rail transportation systems and water and wastewater treatment facilities through electronic intrusion over network connections. The Intelligent Systems Research Laboratory at the University of Louisville has recently completed a project for the Department of Homeland Security consisting of identifying, analyzing and prioritizing the major vulnerabilities of industrial control systems in the Water Sector through unauthorized, remote computer-based intrusions (commonly designated as cyber-attacks) on these control systems which are intended to disable, damage and otherwise impact the water systems that these control systems regulate and control.

The second section of this paper presents some background information on industrial control systems, while section three gives an overview of a DHS created tool for evaluating cyber vulnerabilities in these systems. Section four of this paper presents the major identified technical vulnerabilities for Water Sector industrial control systems and also the major business and operational vulnerabilities. Section five divides the technical vulnerabilities into three prioritized groups and indicates ongoing research relevant to these vulnerabilities. Finally, section six provides recommendations for future research for addressing the identified vulnerabilities.

2 Background

Industrial control systems regulate much of the critical infrastructure of every developed nation. They are used to control electrical power distribution, oil and gas pipelines, chemical process plants, rail transportation systems and water and wastewater treatment facilities. A typical industrial control system consists of a control center, one or more field devices, a communications infrastructure, and field equipment. At the control center, a master terminal unit (MTU) processes information received from field sites and sends control directives back out to field sites. Human operators or control algorithms initiate control signals that are delivered from the control network. These control signals or field operations are carried out by field devices which are connected to field equipment, sensors and actuators, through analog and digital input and output hardware. Common types of field devices are remote telemetry units (RTU),

intelligent electronic devices (IED) and programmable logic controllers (PLC). Field devices and the Master are connected by a communications network. The communications network could be leased lines, PSTNs, cellular networks, IP based landlines, radio, microwave, satellite, or industrial Ethernet. In general the communication protocols used by field devices and master control units are referred to as SCADA protocols, where SCADA is an acronym for supervisory control and data acquisition. Because these systems are now implemented with commercial off-the-shelf hardware and software, and are increasingly connected to the Internet, they have become vulnerable to many the same cyber attacks that plague other computer installations.

3 CS2SAT/CSET

The Control System Cyber Security Self-Assessment Tool (CS2SAT) is a cyber-security assessment tool for ICS owner and operators. CS2SAT was initially developed at Idaho National Labs (INL) by Jeff Tebbe and Ed Gorski [2]. CS2SAT was originally released in 2007, and updated to version 2.0.0 in August of 2008. In 2009 CS2SAT was combined with the Cyber Security Vulnerability Assessment (CSVA) tool to form the Cyber Security Evaluation Tool or CSET [3]. The CSET tool is available from DHS along with on-site training. The remainder of this section refers to CSET, but the discussion is limited to the features of the updated version of CS2SAT that is part of CSET.

CSET is a desktop software application. To use CSET a user describes a control system by creating a diagram of the control systems network components. The user then answers a long series of questions driven by selected ICS cyber-security standards and traditional IT security standards applied to the control system components in the diagram. Using the answers to the questions, CSET generates a report based on a comparison of the answers with selected standards and best practices relevant to that component. Currently the questions and guidance provided by CSET are not sector specific although it is anticipated that the next major release of the CSET tool will allow designation of a specific application sector.

There are five main components to CSET:

1. **Standards selection**
   To begin the assessment the user must select from a list of standards that will be used for the assessment. Standards include: NERC CIP 002 through 009, NIST SP800-5 rev.0,1,2, ISO/IEC 15408, DoDI 8500.2 and SANS Top 20.
2. **Site assurance Level (SAL)**
   To proceed, the user next needs to establish a security assurance level (SAL), which indicates the severity of impact that a "cyber-attack" on the facility might possibly incur.
3. **Components diagram**
   As part of every self-assessment, users must define a control systems diagram for the installation.
4. **Components questions**
   CSET generates a series of questions about the security configuration and capabilities of each element of the component diagram. The questions range from encryption and authentication to logging and security monitoring.
5. **Assessment report**
   When all the questions are answered, CSET will generate an assessment report. The assessment report includes a compliance bar graph, a set of pie chart and a gap analysis for each component in the control system diagram. A typical evaluation summary is shown in Table 2.1.

Table 2.1.CSET Evaluation component compliance summary.

Component	Percent of Questions meeting target SAL	Percent of Questions 1 SAL below target SAL	Percent of Questions 2 SAL below target.
Modem	100%	0%	0%
HMI	74%	14%	12%
Router	65%	10%	25%
Database Server	61.9%	23.8%	14.3%
Firewall	40.7%	25.9%	33.3%
Switch	38.1%	19%	42.9%
Serial Radio	33.3%	8.3%	58.3%
Terminal Server	29.4%	35.3%	35.3%
RTU	27.8%	27.8%	44.4%
PLC	27.8%	22.2%	50%

For the PLC and RTU components, the largest gaps in compliance are related to the notification of security personnel to potential attacks (detected by the PLC/RTU) and the lack of roles defined for the PLC/RTU (both are 35% compliant). Event monitoring (recording events and associating them with a user, comparing monitored events against a rule set, and protecting the integrity of audit records) is the second major gap area for PLCs and RTUs. The last significant

gap area relates to the ability of the PLC to return to a normal operating mode after failure or manual restart.

The updated version of CS2SAT, now a part of CSET, is a useful assessment tool for ICS security. The need for a team to answer questions may present a problem, especially for smaller utilities as they may lack the human resources, or may even have contracted ICS support. While the output of CSET is valuable, it does not generate a set of actions specific enough to clearly define steps that need to be taken, though it does provide an adequate initial prioritization of deficiencies. Another challenge with the use of CSET is that users may, lacking full understanding of the question, answer questions incorrectly, which could lead to a skewed report.

4 Mapping of ICS Vulnerabilities for the Water Sector

This section addresses the issue of mapping and prioritizing the major cyber-security vulnerabilities in the industrial control systems used in the water sector. Cyber-security challenges identified by this project fall into two major categories: technical challenges and business/operational challenges, discussed in detail in sections 4.1 and 4.2 respectively.

4.1 Major Technical Cyber-Security Vulnerabilities

1. **Poorly Secured Legacy systems**.
    - ***Longer replacement periods***: Legacy systems typically have a 20-30 year life cycle. Because of this, it can take a long time for state of the art technologies to penetrate the sector. This life cycle has started to shorten in terms of HMI, Historian, and others components that are typically PC based, however, the PLC, RTU, and I/O components are still designed around this longer life cycle.
    - ***Costly and difficult to replace***: Very old legacy control systems are costly and difficult to replace, particularly for the water sector. New control systems rarely add functionality to the controlled process so a sufficient return on investment is usually not possible. New systems are typically very different in hardware and software so operation and maintenance are greatly impacted with the need for retraining. Lastly, during the controls upgrade, the process is down for an extended time period, which is difficult for water sector companies to endure.
    - ***No security built in***: Many legacy systems were designed before cyber-security concerns became relevant. They were designed to be standalone systems in which threats from outside parties were nearly impossible due to physical security of the system itself.
    - ***Reduced processing power***: Legacy systems, by definition, are constructed with older technology. This results in reduced processing power, memory, and other storage resources, often to the degree that advanced algorithms for cyber-security are not possible or practical to implement.

- ***Difficult to integrate new security technologies in to legacy systems:*** Legacy systems are often incompatible with emerging ICS cyber-security technology in general because they lack processing power or use proprietary hardware or software.
- ***Relevant research***:
    - The AGA 12 serial link encryption standard can help protect legacy field equipment such as RTUs by adding cryptographic protection to field communications.
    - The University of Louisville's ISRL continues to investigate securing legacy field devices as part of its security hardened RTU. Reduced kernels have been one area of investigation.
    - Legacy systems also present challenges for IT in general, and other institutions, such as CMU and Purdue, are investigating the more general problem of interfacing legacy systems with state of the art systems.

2. **Lack of trained cyber security specialists**: In the water sector, on-site control engineers are typically trained in the control hardware and software from the aspect of controlling the process itself. Engineers have begun to use IT infrastructure technologies over the past decade such as Ethernet, switches, etc, however there is a gap in training with regard to implementing effective security using existing features of these components, not to mention the latest cyber-security enhancements.
    - ***Combination of ICS and IT security***: A combination of control system and IT security expertise are rare. Most Water Sector personnel would have expertise in one or the other but not both.
    - ***ICS cyber-security training for new systems different from ICS cyber-security training for legacy systems***.
    - ***Installing and configuring security can be time consuming***.
    - ***No precise definition of a Secure Water Sector ICS***.
    - ***Relevant research***:
        - The ISRL at the University of Louisville has previously examined the issue of SCADA security training for control systems and this plus additional work will be covered in more detail in the report for task 5 of this project.
        - The University of South Australiahas examined developing a SCADA systems security program for an engineering program.
        - Sandia National Laboratory and Idaho National Laboratory offer ICS cyber-security training.

3. **Delayed application of Operating System and application software patches**
    - ***Patches are not applied at all***, or not for a substantial time after their initial release, leaving the system vulnerable to well-known and possibly public domain attacks.
    - ***Delay in applying patches***: New patches are released on nearly a daily schedule. Control engineers do not have the time to apply these patches on such a schedule. Often, the application of patches can disrupt the controlled process so they are only scheduled once in a while. This leaves the control system vulnerable while waiting for patches to be applied.
    - ***Incompatibility of patches***: Software utilized in control systems are custom implementations and are often not verified against patches as they are released. Patches can break control systems and the process is typically down or compromised until recovery can be completed.

- ***Cannot test patches***: Patches are usually not able to be tested against a control system configuration since these configurations are custom for each site. Each site in the water sector cannot afford to perform this and often do not have the training required.
- ***Security patches are difficult to install in the control system***
- ***Relevant research***:
    - Patch management has been studied at Purdue University, Carnegie Mellon University and other research institutions. However much of this research is aimed at the traditional IT environment.
    - Some guidance on Patch Management is provided by DHS CSSP, but there is no technical simple solution at this point.
    - No specific technical solutions for industrial controlare currently being researched, to our knowledge.

4. **Lack of cyber-security situational awareness**. Water ICS systems have limited logging capabilities, the focus of which has been of control and operation and not on cyber-security. ICS components' logging and event generation capabilities are focused on trouble shooting the system or determining if an operator failed to do his/her job. The limited logging that is available is not aggregated, and on-going audit comparisons are rare. This introducesa vulnerability by giving an attacker a significant amount of time to observer and attack network ICS components without being detected.
    - ***Water Sector ICS components lack security related event generation:***In some cases event generation capabilities may not be configured, in other cases devices, especially field devices such as PLCs and RTUs, do not have this capability or it is very limited. Examples of cyber-security related events include: authentication failure, forced register manipulation, firmware changes, and malformed protocol messages.
    - ***Centralization of generated events***: For ICS components able to generate events and or logs, systems do not exist to make accessing and analyzing these events quick and easy. Nor do systems exist which assure the logs remain unchanged.
    - ***Lack of event correlation***: Individual cyber-security related events are by themselves usually meaningless. It is the grouping of several events that can lead to a confident diagnosis of a cyber-security related event, for example: multiple failed login attempts, followed by a firmware upgrade.
    - ***Not integrated with ICS control view***: Water Sector personnel regularly monitor the system's ICS. Their view of the system does not include ICS cyber-security.
    - ***Relevant research***:
        - LOGIIC system developed by a public and private partnership including Sandia National Labs collects events from many parts of an ICS, collects them in one place and provides automated event correlation to reduce the number of viewable events by several orders of magnitude.
        - Portaledge and Quickdraw are research projects lead by Digital Bond that are investigating passive collection of ICS network traffic and security event aggregation.
        - The ISRL at the University of Louisville is investigating field intrusion detection systems which give more information about process anomalies.

5. **Communication security**
    - ***Unsecure Protocols***: Many protocols used in the water sector for control were designed for simple and reliable communications, with no consideration for security. Security adds a layer of complexity and unreliability that may not be feasible for process control.

- ***Unsecured Links***: Many links are confined to the site and thus, physical security prevails. In the water sector, however, field sites are linked by many different means such as radio, ISND, POTS, etc based on cost and availability. Securing these links is a challenge due to lack of training and hardware in current/legacy control systems.
- ***Lack of isolation/separation***: Control networks are poorly isolated from enterprise networks.
- ***Relevant research***:
  - The AGA-12 SCADA serial encryption standard protects serial links to field equipment.
  - The ISRL at the University of Louisville continues with design and development of secure SCADA communications by adding authentication and message integrity capability to existing SCADA protocols. Two approaches have been tested – authentication octets and challenge-response.
  - The University of Tulsa designed and evaluated a secure Modbus protocol.
  - The DNP3 Technical Group is continuing with an addition to the DNP3 protocol called Secure Authentication, which uses a challenge –response approach.

6. **Remote access**
   - ***Employee access***: Engineers need remote access to control systems for quick troubleshooting and for ease of configuration when sites are geographically spread out as is typical of the water sector. The points of access are usually POTS modem and occasionally Internet. These points of access are often not secured sufficiently.
   - ***Vendor access***: In the last several years, vendors have wanted remote access to components they supply to the water sector for control from similar points of access as employees utilize. This also benefits the water sector by reducing costs of vendor maintenance since travel and hours are reduced. However, security becomes a greater concern when vendors gain access to the control system.
   - ***Relevant research***:
     - Some of the efforts at the University of Louisville's ISRL security hardened RTU research applies to remote access to field devices.

4.2 *Major Business and Operational Vulnerabilities*

Business and operational challenges to Water Sector ICS operators and asset owners are a significant impediment to achieving cyber-security for the Water Sector ICS. On the business side, a lack of buy-in from upper managers due to an inadequate understanding of the threat can prevent a utility from using available resources to improve its ICS cyber-security posture. A lack of understanding across the operation can also prevent the appropriate resolution of conflicts between IT security governance and ICS operation and maintenance. This project focuses primarily on the technical vulnerabilities, so this information is provided for completeness and recognition of its practical importance in real world ICS systems in the Water Sector. Major business/operational challenges include, but are not limited to those listed below.

1. **Business Case:** There is not a well-defined or understood business case for ICS security
   - Limited recognition of ICS security threat by upper level business managers

- Limited resources are available to invest in mitigation solutions
- Lack of financial resources
- Cost of new systems
- Competing priorities for operational and maintenance activities limit resources
- Limited recognition of ICS security threat by upper management
- Difficult to estimate damages for an ICS Cyber-security attack.
- No well-defined Water Sector ICS security requirements
- Security is optional so justifying cost is difficult.

2. **Risk Management Integration:** ICS Cyber-Security is not integrated into the business risk management
   - Limited understanding of ICS risk factors
   - The rapid pace of change in threat actors and vulnerabilities

3. **Two Cultures Problem:** IT Security personnel have very different goals and skills from Control personnel
   - Limited collaboration between IT department and Control engineers.
   - Lack of ICS security training resources, especially sector specific
   - Lack of separation of duty constraints.
   - IT and Control fall below very different branches of the corporate organization

4. **OtherBusiness and operational vulnerabilities**: include the following
   - The Water Sector is a small share of the market for ICS components.
   - Different Water Sector actors may have different, even conflicting, points of view about ICS
   - Managing change in mission critical systems
   - Overloading the control engineer.
5. **Related Research**
   - The I3P group has several research projects related to risk, risk mapping, and risk pricing, as well as a business rational for cyber-security
   - The CSSP of DHS CSSP has several business guidance documents that address specific vulnerabilities mentioned above.
   - University of Illinois is developing model driven approaches for ranking vulnerabilities, an approach that could provide guidance for managers.

5 *Prioritization of Water Sector ICS Cyber Security Vulnerabilities*

While all of the items listed in Sections 4.1 and 4.2 have been identified as significant threats to the cyber-security of water sector control systems, the priority rankings of this section attempt to incorporate our collective assessment of the magnitude of potential damage if a vulnerability is successfully exploited and the perceived degree to which the vulnerability is present across the water sector. Table 4.1 shows the assessments of the research team for these two factors, as well as the difficulty of exploiting the vulnerability. This analysis resulted in separation of the vulnerabilities into three classes or levels as discussed below.

(1) The highest vulnerability priority level was assigned to poorly secured legacy systems. Legacy systems are clearly recognized in the "Road Map to Secure Control Systems in the Water Sector" and by our advisory board as permeating the water sector. Many of these systems were designed and installed well before cyber-security became a threat and they will not soon be replaced or upgraded. These systems, in an unsecured state, pose hazards ranging from inconvenience to customers to damaged equipment and a long shut down and restart period. Thus the exposure level and potential damage level are both rated as very high for this vulnerability.

(2) The second highest vulnerability priority level was assigned jointly to lack of trained cyber-security specialists and delayed patch application. In our discussion with our advisory board and with other water sector personnel, it became very apparent that the limited number of technical personnel in most water systems makes it unlikely that operators and engineers have sufficient training to prepare for and respond to cyber security threats. Patches are often delayed because of concerns that systems will not operate properly when patched. This problem is exacerbated by incompatibilities between operating systems components and applications software packages, and again by the lack of properly trained personnel. The exposure level is rated high and the potential damage level is rated high for these vulnerabilities.

(3) The third highest vulnerability priority level was assigned jointly to lack of cyber security situational awareness, communications security and remote access. All of these areas are rated as medium in exposure level and medium or high in the potential damage level. All of these are still significant vulnerabilities, but somewhat less critical in impact level and exposure level than for the previously discussed vulnerabilities.

Table 4.1.Prioritization of vulnerabilities.

Vulnerabilities	Prevalence	Impact severity	Exploit Difficulty
Legacy Systems	***Very High***	***Very High***	***Low***
Lack of Trained Cyber-Security Specialist	***High***	***High***	***N/A***
Delayed Patches	***High***	***High***	***Medium***

Lack of cyber-security Situational Awareness	***High***	***Medium***	***Medium***
Communication Security	***Medium***	***High***	***Medium***
Remote Access	***Medium***	***High***	***High***

6 Conclusions and recommended research activity.

Based upon the mapping and priority assessments provided in this paper, this section provides the recommendations of the research team for needed additional research to address vulnerabilities in the industrial control systems in the Water Sector.

(1) **Legacy Systems** – Research is needed to identify, design, and test technical approaches to enhance legacy system cyber-security which can be implemented with low to medium cost for these systems. These security enhancements must be simple to add and not require undue patching or updates to existing components.

(2) **Lack of Trained Cyber-Security Specialist** – Research is needed to identify gaps in training and education in ICS cyber-security for Water Sector personnel. We note that this is being done as part of this project and results will be reported as part of the Task 5 Deliverable.

(3) **Delayed application of Patches** – Research is needed to simplify the patch management process and to allow water sector personnel to verify that operation of the control system will not be compromised by application of operating systems and application software patches.

(4) **Lack of cyber-security situational awareness** – Further research, testing and evaluation are needed in the collection, centralization and analysis of ICS events. Intrusion detection and event correlation systems need to be designed and tested that are easy for Water Sector personnel to install and configure, and which provide meaningful and actionable information that does not burden Water Sector ICS personnel with additional administrative overhead. Also more research should be performed in the combination of field device intrusion and network intrusion detection systems.

(5) **Communication Security**–This area has been well investigated in other sectors, including traditional IT applications. However, approaches for enhancing communication security need to be specialized for Water Sector applications and tested and evaluated.

(6) **Remote Access** – Access control has been extensively studied in traditional IT applications. Research is needed to specialize this research to Water Sector ICS systems.

(7) **Business and Operation Vulnerabilities** – Research is needed to integrate Cyber-Security Risk into the business planning process model for the Water Sector.

As discussed in sections 4.1 and 4.3, it was the opinion of both the research team and the advisory board that poorly secured legacy systems currently pose the most significant threat to the cyber-security of Water Sector industrial control systems. To address this vulnerabitity our research group is presently prototyping a security preprocessor which will be an add-on (bolt-on)

appliance that can be added to existing control systems with minimal hardware/software changes to the control system architecture. It will utilize and expand technologies previously developed at the University of Louisville for NIHS for hardening remote terminal units and other field devices against cyber-attacks. It will employ a role-based access system, challenge response SCADA communication security, and other security features. The security preprocessor will be based on a specialized microkernel security architecture, which compartmentalizes network components, security components, and field device components in separate partitions. This device will be created in prototype form and tested in our laboratories during the coming year.

Acknowledgement

This work was sponsored by a grant from the Dept. of Homeland Security administered through the National Institute for Hometown Security. The opinions expressed in this paper are solely those of the authors.

References

[1] Graham, James H., Hieb, Jeffrey L., and Foreman Christopher J., "ICS Cyber Security Landscape Assessment," Secure ICS Project Deliverable 3 rev. 1, Louisville, Kentucky, 2010.

[2] The Blueprint to Security. *Idaho National Laboratory.* [Online] http://www.inl.gov/featurestories/2007-03-09.shtml

[3] Control System Security Program, Cyber Security Evaluation Tool, [online] http://www.us-cert.gov/control_systems/satool.html

[4] "Project 12 Report: Improving Protection of Privately Owned Critical Network Infrastructure ThroughPublic-Private Partnerships," [online] http://info.publicintelligence.net/NetworkInfrastructurePublicPrivate.pdf

[5] Water Sector Coordinating Council Cyber Security Working Group, "Roadmap to Secure WaterSector," [online] http://www.nawc.org/policy-issues/utility-security-resources/Final%20Water%20Security%20Roadmap%2003-19-08.pdf