Mapping Dams Sector Cyber-Security Vulnerabilities

by J. Chris Foreman, James H. Graham, and Jeffrey L. Hieb
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Mapping Dams Sector Cyber-Security Vulnerabilities

J. Chris Foreman, James H. Graham, and Jeffrey L. Hieb
Intelligent Systems Research Laboratory
University of Louisville, Louisville, Kentucky 40292
[jcfore01, jhgrah01, jlhieb01@louisville.edu]

Abstract

Vulnerabilities in the cyber-security of industrial control systems as used in the Dams Sector are identified, analyzed, and prioritized. These vulnerabilities span both organization and technical aspects operational control in the Dams Sector. The research team has completed projects in both the Water and Dams Sectors for the Department of Homeland Security as recent attacks in these and other critical infrastructure have become more prevalent. The analysis is based on expert knowledge by the research team, interviews with field personnel, tours of field locations, and an associated project advisory board.

1 Introduction

Several events in recent years have indicated a present and growing threat to the cyber-security of computer-based Industrial Control Systems (ICS) [1]. Of particular concern are ICS utilized in the operation of critical infrastructure such as the electric power grid, oil and gas pipelines, rail transportation systems, water and wastewater treatment facilities, and dams. The Intelligent Systems Research Laboratory (ISRL) at the University of Louisville has completed projects for the Department of Homeland Security (DHS) in the Water and Dams Sectors consisting of identifying, analyzing, and prioritizing the major vulnerabilities of ICS with respect to unauthorized, computer-based intrusions (commonly designated as cyber-attacks). These cyber-attacks are intended to disable, damage, and otherwise impact the infrastructure under their control, which results in a significant impact to society in general.

The Dams Sector is one of 18 critical infrastructure sectors established under the authority of Homeland Security Presidential Directive 7. There are over 82,000 dams in the United States; approximately 65% are privately owned and more than 85% are regulated by State Dam Safety Offices [2].

Section 2 of this paper discusses the operational environment of ICS with respect to the Dams Sector, as they are unique in comparison to Information Technology (IT) systems. Section 3 identifies the major organizational and technical vulnerabilities uncovered. Section 4 analyzes and prioritizes these vulnerabilities. Section 5 compares cyber-security in the Dams Sector with that of the Water Sector. Finally, Section 6 provides recommendations for mitigation technologies and future research to address the identified vulnerabilities.

2 ICS in the Dams Sector

Dams are designed to regulate reservoir elevations by controlling the flow of water through the dam's spill/flood gates. Dams may also regulate waterway traffic between upstream and downstream elevations through locks. In some cases, hydro generating stations are also present at a dam's facility and these are typically cooperative in water management, although usually controlled separately [3]. The layout of these is illustrated in Figure 1.

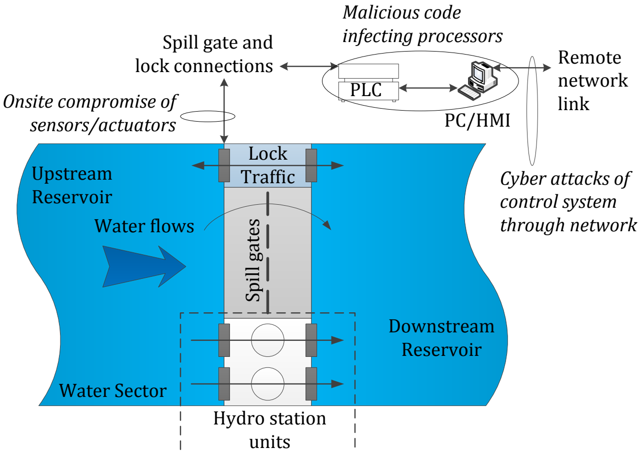

Figure 1. Overview of ICS and attack points in the Dams Sector [3].

2.1 Manual Control

The types of control systems used in dam operation typically fall into two categories. The first is a completely custom configuration based on hydraulics, or possibly pneumatics, and often manually (hand) operated. These are the mechanical systems left over from the dam's original construction [3]. While manual control would seem to be impervious to cyber-attack, there are some organizational vulnerabilities discussed in Section 3. Also, these systems are rapidly becoming replaced with automated control to reduce maintenance requirements and simplify operation.

2.2 Automated Control

The second category are modernized ICS, including Supervisory Control and Data Acquisition (SCADA). These systems are predominately based on control by Programmable Logic Controllers (PLC) with computer-based Human Machine Interfaces (HMI). Many of these systems are several years old, in the legacy generation, yet they still allow linking control of the dam to the outside world for monitoring and/or control, onsite or remotely [3]. Though there have been some advances in cyber-security in recent generations of ICS, these are very sparsely deployed. In nearly all cases, ICS continue to rely on legacy protocols, e.g., Modbus, which do not incorporate cyber-security measures to prevent common network attacks such as message modification, message spoofing, and replay.

3 Identification of Vulnerabilities in the Dams Sector

The cyber-security vulnerabilities from both an organizational as well as technical perspective are identified and categorized. Organizational vulnerabilities refer to vulnerabilities in security and operational policies and procedures, including business, personnel, and management factors that affect cyber-security. Technical vulnerabilities refer to ICS hardware and software components, network implementations and protocols, and other physical factors.

3.1 Organizational Vulnerabilities [4]

1. Business case: Although there seems to be a respect for cyber-security for ICS in the Dams Sector, there is not a well defined, or understood business case for funding ICS cyber-security projects. Some factors that may contribute to this include:
   - No well-defined Dams Sector ICS security requirements.
   - Competing priorities for operational and maintenance activities limit resources.
   - Lack of financial resources to cover the costs of new systems.
   - Difficult to estimate damages for an ICS Cyber-security attack.
   - Limited recognition of ICS security threat by upper management.
2. Risk management integration: ICS cyber-security is not effectively integrated into the organizational risk management process.
   - Most well-established risk management systems do not include a focus on the recent adoptions of ICS.
   - Limited understanding of ICS risk factors.
   - The rapid rate of change in threat actors and vulnerabilities.
3. Two cultures problem: IT Security personnel have very different goals and skills from ICS personnel.
   - IT and ICS fall under very different branches of the organization.
   - Limited collaboration between IT department and ICS engineers.
   - Lack of ICS cyber-security training resources, especially resources that are sector specific.
   - Lack of separation of duties in the configuration, operation, and management of ICS.
4. Other organizational and operational vulnerabilities:
   - The Dams Sector is a small share of the market for ICS components, which itself is a small share when compared with Commercial Off The Shelf (COTS) IT systems.
   - Different Dams Sector actors may have different, even conflicting, points of view about ICS and cyber-security strategies and priorities.
   - Managing change in mission critical systems.
   - Overloading the ICS engineer with too many responsibilities.
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 DHS Control Systems Security Program (CSSP) has several business guidance documents that address specific vulnerabilities mentioned previously [5].
   - University of Illinois is developing model driven approaches for ranking vulnerabilities, an approach that could provide guidance for managers.

3.2 Technical Vulnerabilities [4]

1. Legacy ICS: These systems represent early ICS that may have been implemented at dams before modern cyber-security measures were adopted.
   - 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: Control systems are costly and difficult to replace, particularly for the Dams 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.
   - No cyber-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 the physical isolation of the system.
   - Reduced processing power: Legacy systems, by definition, are constructed with older technology. This results in reduced processing power, memory, and other resources, often to the degree that ad-

vanced algorithms for cyber-security are not possible or practical to implement.

- Difficulty to integrate new cyber-security technologies: Legacy systems are often incompatible with emerging ICS cyber-security technology in general because they lack processing resources and/or use proprietary hardware and software.
- Relevant research: Much research has been done in the area of ICS cyber-security. There has been very little, if any, research in ICS cyber-security for the Dams Sector in particular [3].
    - 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 Carnegie Mellon University (CMU) and Purdue University, 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 Dams Sector, on-site ICS engineers are typically trained in the control hardware and software from the aspect of controlling the process itself. IT Engineers are rarely utilized in this position due to their lack of training in the specifics of dam operation and equipment. ICS engineers are most often Civil, Mechanical, or Electrical Engineers. These 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 cyber-security using existing features of these components, not to mention the latest cyber-security enhancements.
    - Combination of ICS and IT security: A combination of ICS and IT security expertise are rare. Most Dams Sector personnel would have expertise in ICS only, with IT security expertise being a rarity.
    - ICS cyber-security training for new systems is different from ICS cyber-security training for legacy systems.
    - Installing and configuring security can be time consuming.
    - No precise definition of a secure Dams Sector ICS.
    - Relevant research:
        - The ISRL at the University of Louisville has previously examined the issue of SCADA security training for control systems.
        - The University of South Australia has 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, leaving the system vulnerable to well known and possibly public domain attacks.
    - Delay in applying patches: New patches for COTS operating systems are released on nearly a daily schedule. ICS 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 ICS vulnerable while waiting for patches to be applied.
    - Incompatibility of patches: Software utilized in ICS are custom implementations and are often not verified against patches as they are released. Patches can break ICS and the process is typically down or compromised until recovery can be completed.
    - Cannot test patches: Patches are usually not tested against control system configurations since these configurations are custom for each site. Each site in the Dams Sector cannot afford to perform this and often do not have the training required.
    - Relevant research:
        - Patch management has been studied at Purdue University, CMU and other research institutions. However much of this research is aimed at the traditional IT environment.
        - DHS CSSP provides some guidance on patch management, but there is no technical simple solution at this point.
        - No specific technical solutions for industrial control are currently being researched, to our knowledge.
4. Lack of cyber-security situational awareness: Legacy ICS systems have limited logging capabilities and mechanical systems have none. 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 auditing is rare. This introduces vulnerability by giving an attacker a significant amount of time to observe and attack ICS network components without being detected.
    - Dams 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: Dams Sector personnel regularly monitor traffic through a dam and the physical perimeter of the dam. The ICS will be monitored via HMI, if present, however, this view of the process usually does not include cyber-security events.
- 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 led by Digital Bond that investigate 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 control protocols used in the Dams Sector were designed for simple and reliable communications, with no consideration for security. Security adds a layer of complexity and unreliability that may be difficult to integrate into existing systems.
   - Unsecured links: Many communications and network links are confined to the specific site and thus, physical security prevails. In the Dams Sector, however, multiple dams and their central control, if utilized, may be linked by many different means such as radio, ISDN, POTS, etc. based on cost and availability. Securing these links is a challenge due to lack of training and hardware in current/legacy ICS.
   - Lack of isolation/separation: ICS networks may be poorly isolated from enterprise networks, such as the organization's WAN, if these resources are shared.
   - Relevant research:
     - ▪ 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: Remote access in the Dams Sector is not as prevalent as in other sectors, such as power and water. Dams are almost always capable of backup operation in the event of ICS failure. Still, there may be occasions when remote access would be beneficial and cyber-security quickly becomes an important consideration in these circumstances.
   - Employee access: Engineers may need remote access to control systems for quick troubleshooting and for ease of configuration when sites are geographically spread out. 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 the ICS components they supply for troubleshooting, product maintenance, and product update purposes. This also benefits the Dams Sector by reducing the costs of travel and engineering hours charged. However, security becomes a much greater concern when vendors gain access to the ICS.
   - Relevant research:
     - ▪ Some of the efforts at the University of Louisville's ISRL security hardened RTU research applies to remote access to field devices.
7. Mechanical control systems, e.g., hydraulic systems: Though not directly a cyber-security vulnerability, many dams operate in a purely mechanical mode. The spill gates and other dam controls are operated by manually actuated valves and/or hydraulic pumps via local control only and thus, no cyber-systems are employed in these cases. Reservoir level readings may also be obtained by manual measurement.
   - Telephone spoofing/phishing: There are vulnerabilities associated with such manually operated systems as they rely heavily on operator judgment, which may be influenced by telephone phishing attacks if an attacker gives false information or directives.
   - Lack of authentication: There are also concerns for physical security as once physical access is obtained to such controls, there are no cyber-security safeguards in place to require operator authentication, for example login/logout methods.

4 Prioritization of Vulnerabilities in the Dams Sector

The vulnerabilities in Section 3 are prioritized based upon our review of the "Dams Sector Road Map to Secure Control Systems" [1], information from DHS CSSP documents [5], participation in the 2013 Dams Sector Information Sharing Drill exercise hosted by the DHS Homeland Security Information Network (HSIN) [6], a site visit to a dam that has recently installed a modern ICS, and from comments by the project advisory board. The priority rankings, summarized in Table 1, incorporate this collective assessment of the magnitude of potential damage if vulnerabilities are successfully exploited, the degree to which vulnerabilities are present across the Dams Sector, and the difficulty of exploiting the vulnerability. The vulnerabilities were separated into the following three levels.

1. The highest priority level was jointly assigned to poorly secured legacy systems and to a lack of trained cyber-security specialists. It was determined that these two vulnerabilities both contributed to unsecured ICS deployed in the Dams Sector. These two vulnerabilities are realized through ICS that are either incapable of secure operation, or improperly installed for secure operation to be effective. ICS, in an unsecured state, pose hazards ranging from inconvenience in operation to potentially damaged equipment, further extending denial of service. In some cases, failure could result in flooding of the managed reservoir with expected consequences. Thus the exposure level and potential damage level are both rated as very high for this vulnerability.
   - Legacy systems are clearly recognized in the "Dams Sector Road Map to Secure Control Systems." [1]. In many cases, these installations are unlikely to be upgraded in the near future.
   - A lack of ICS cyber-security training has also been recognized. Although several cyber-security standards exist for the IT Sector, and some exist for other sectors, such as the Power Sector's NERC CIPS [7], there are no standards for the Dams Sector in particular, leaving most organizations to either omit or attempt to apply another sector's standards in absentia.
2. The second highest vulnerability priority level was determined to be delayed patch application. Delayed patch application can result in the compromise of an ICS that had previously been properly secured, thus negating the effectiveness of any cyber-security measures in place. 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. These vulnerabilities contribute to an environment that is not conducive to ICS cyber-security and/or result in an environment that is more open to attack than necessary for dam operations. All of these areas are rated as high or low in exposure level and medium or high in the potential damage level. While all of these are still significant vulnerabilities, they are somewhat less critical in both impact level and exposure level than for the previously discussed vulnerabilities. In most of these cases, policy changes can mitigate much of these vulnerabilities. The following points are also noteworthy for mitigating these vulnerabilities.
   - Situational awareness has come into focus in recent years so this vulnerability is diminishing. Many dams are now employing closed circuit monitoring via video cameras.
   - The Dams Sector makes extensive use of manual, telephone communications for coordination with reservoir traffic as well as other dams. It would be very difficult for a cyber-attacker to breach this security since most parties know each other well and thus, self authenticate.
   - Remote access seems to be a reduced concern in the Dams Sector, although a few dams may excessively utilize this access. Since dams are usually manned continuously, there is usually someone on site to override a cyber-attacker's malicious activity. The dams process is slow acting compared with other sectors and affords sufficient time to react when manual overrides are available and an operator is on site.

Table 1. Vulnerability Prioritization in the Dams Sector.

Vulnerabilities	Prevalence	Impact severity	Exploit Difficulty
Legacy systems, isolated ICS network	Very High	Very High	High
Legacy systems, integrated with WAN	Medium	Very High	Medium
Lack of training and standards in cyber-security	Very High	Very High	Medium
Delayed patches, isolated ICS network	High	High	High
Delayed patches, integrated with WAN	Medium	High	Low
Lack of cyber-security situational awareness	High	Medium	Medium
Lack of communication security	High	Medium	High
Remote access	Low	High	Medium

5 Comparison with the Water Sector

In a related project, a vulnerability mapping and prioritization analysis was created for ICS used in the Water Sector [8]. There are many similarities between these sectors such as the use of similar ICS, the lack of cyber-security training and/or skilled employees in charge of ICS and cyber-security, and the exposure to similar threat actors and attack surfaces. However, dissimilarities were also uncovered due to differences in the controlled process and in both operational and organizational strategies. Though some dams may be coordinated with other dams or adjacent hydropower generation, most dams are operated as a single location with an isolated ICS network. This is in contrast to the Water Sector, which relies heavily on a geographically dispersed ICS network to control both water treatment and remote lift pump stations. The dams also incorporate a process that operates on a longer time scale, thus allowing time to respond to failures and attacks. Reservoir levels take a long time to change and both spill gates and locks usually incorporate manual controls as a backup. In fact, dams are almost always manned 24/7 while remote sites in the Water Sector are unmanned most of the time. The Water Sector also tends to be more privatized versus dams, which tend to be more government operated, e.g., by the Army Corps of Engineers [4].

6 Discussion and Future Recommendations

This paper has presented a look at common cybersecurity vulnerabilities in the industrial control systems (ICS) utilized in dams and locks, both in the United States and worldwide. Secure next generation control systems should, at a minimum, should have the following characteristics: real-time situational awareness, self-protection capabilities, message integrity mechanism, firmware integrity mechanism, secure restart capability, and self-healing features. Many of these characteristics are under development at our laboratory, and other laboratories worldwide, because of the life-critical nature of the physical systems that these industrial control systems monitor and regulate. Based on recent conference presentations and private conversations with researchers, it appears that many of these technologies should be ready for commercial application within the next few years.

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] Department of Homeland Security (DHS) Office of Infrastructure Protection and the National Cyber Security Division, "Dams Sector Road Map to Secure Control Systems," http://www.damsafety.org/media/Documents/Security/DamsSectorRoadmaptoSecureControlSystems2010.pdf, WWW, 2010.

[2] United States Army Corp of Engineers, National Dams Inventory, http://geo.usace.army.mil/pgis/f?p=397:12, WWW, June 2012.

[3] Chris Foreman, Jeff Hieb, and James Graham, "Landscape Assessment Dams Sector ICS," Cyber-Security for Industrial Control Systems Used in the Dams Sector: Project Deliverable 3, Intelligent Systems Research Laboratory, University of Louisville, Louisville, Kentucky, 2012.

[4] Chris Foreman, Jeff Hieb, and James Graham, "Mapping Dams Sector Cyber-Security Vulnerabilities," Cyber-Security for Industrial Control Systems Used in the Dam Sector: Project Deliverable 4, Intelligent Systems Research Laboratory, University of Louisville, Louisville, Kentucky, 2012.

[5] DHS The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), CSSP documents, https://ics-cert.us-cert.gov/, WWW, 2013.

[6] DHS Homeland Security Information Network (HSIN), "2013 Dams Sector Information Sharing Drill," participation as observer, February 2013.

[7] North American Electric Reliability Corporation (NERC), "Critical Infrastructure Protection (CIP) Standards," http://www.nerc.com/page.php?cid=6|69, 2013.

[8] Graham, James H., Hieb, Jeffrey L., and Foreman, J. Chris, "Mapping Water Sector Cyber-Security Vulnerabilities," Cyber-Security for Process Control Systems Used in Critical Infrastructure, Project Deliverable 4, Louisville, Kentucky, February 2011.