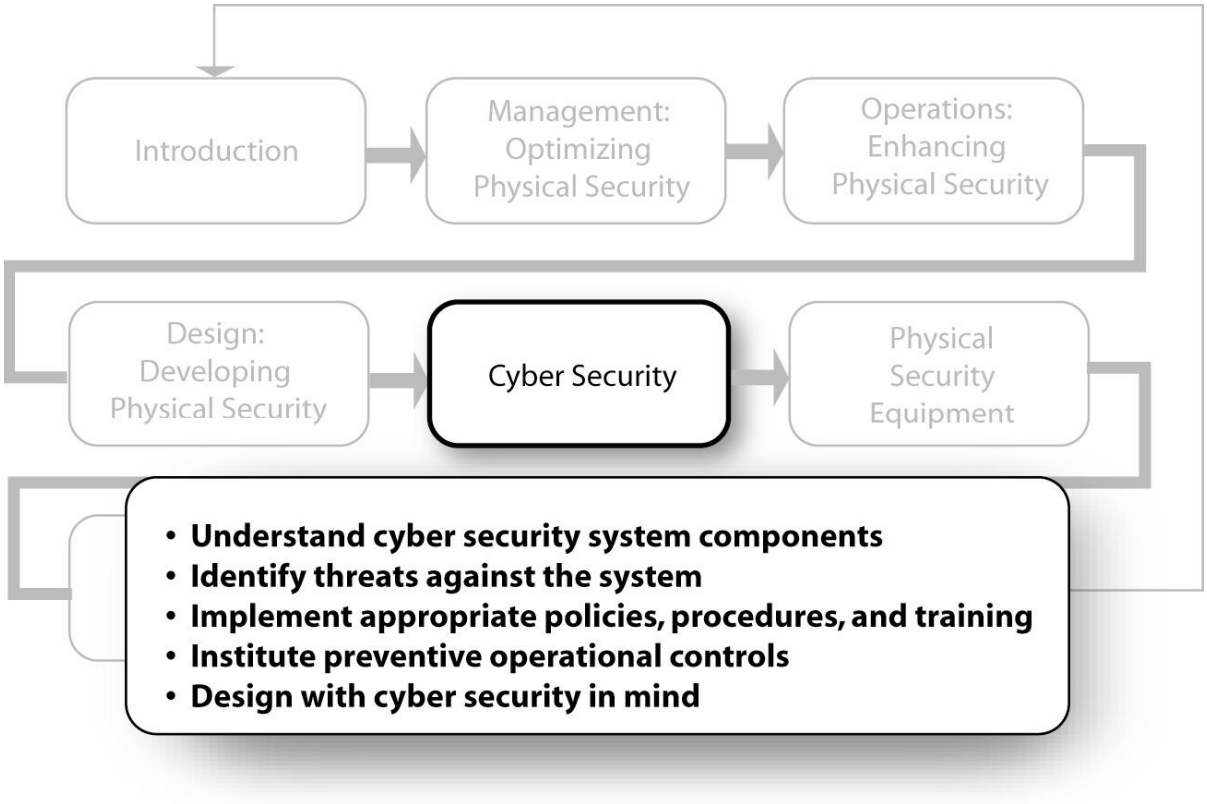
SECTION 5

Cyber Security Management, Operations, and Design Considerations



5.1 Overview

Cyber security is the protection of enterprise information systems from outside or inside attack. The reliance of a water utility on its automated systems can be substantial: the SCADA system runs the plant, the financial system maintains fiscal equilibrium, and several systems facilitate most business processes. Competitive financial pressures have decreased the staff at most facilities to the point where few, if any, utilities can run in "manual mode" for long. In short, if the information systems do not work, the enterprise will not operate.

Unfortunately, security was largely an afterthought in the developing computer industry. The Internet has gone from a trusting network of academic colleagues to daily world-wide alerts for destructive viruses. By virtue of their isolation, SCADA systems have typically been the least defended systems of all. Proactive prevention and response plans can provide utilities with substantial levels of protection from both external and internal adversaries.

This section first describes the components of a cyber system and then identifies existing threats against the system. Management, operations and maintenance, and design guidance that applies specifically to cyber security is then included. Keep in mind that, as in the rest of this document, the intent of the guidance is to provide suggestions and ideas for consideration by utilities as they each create their own customized security plan.

5.2 Utility Cyber Networks

A water utility often deploys an array of specialized information systems. This document will distinguish between those systems residing on the business network versus those on the control network.

A valuable tool for management to understand those portions of the enterprise system that are at greatest risk is the cyber security vulnerability assessment. This type of vulnerability assessment is a focused examination of the entire business and control network from a security perspective. Each component is evaluated for its degree of susceptibility to outside or inside attack. Based on analysis of the utility's DBT, specific recommendations are developed aimed at preventing the most likely types of attacks. (This information can be found in Section 5.6.1, "General Design Best Practices."

5.2.1 Business Network

The business network hosts software applications and databases that facilitate enterprise business, scientific, and engineering processes. These include:

- **Enterprise Resource Program.** A comprehensive financial program that includes modules for General Ledger, Accounts Payable, Accounts Receivable, Payroll and possibly Human Resources.
- **LIMS.** A repository of laboratory result information and process data to support regulatory compliance and treatment plant operations.
- **CMMS.** A work order system to provide preventative maintenance on assets, such as pumps, pipes, hydrants, and valves.
- **Customer Information System.** A system that facilitates customer invoicing and resolving customer complaints.
- **Internet/Intranet.** A tool that provides customers and employees with the ability to interact around-the-clock with the utility from any computer.
- **Other Systems.** E-mail, permitting, geographic information system, and fuel usage.

5.2.2 Control Network

The SCADA system consists of numerous electronic components distributed in the plant and over a large, sometimes very large, geographic area. The system's main function is to oversee and operate the pumps, valves, and instruments that control the intake, treatment, and distribution of finished water to customers. Operable elements of the SCADA system are located in a wide range of facilities, including the intake facilities, the treatment plant, pump or booster stations, tanks, reservoirs, wells,

and other remote facilities. Though SCADA systems vary widely in their composition, the following represents a typical list of components, grouped by function:

- Computers
  - SCADA servers
  - SCADA Human Machine Interface (HMI) programming workstations
  - SCADA HMI workstations and view nodes
- Networking
  - Switches (optical and Ethernet)
  - Routers
  - Hubs
  - Firewalls
  - Modems
  - Serial interfaces (connecting telephone lines to SCADA devices)
- Data Conveyance
  - Ethernet cabling
  - Optical cabling (e.g., plant loop)
  - Telephone lines (leased or owned)
  - Radio transmitters and antennas
  - Wireless transmitters and antennas
- Distributed Control Components
  - Programmable Logic Controllers (PLCs)
  - Remote Terminal Units (RTUs)

5.3 Cyber Security Threats

There is no shortage of potential intruders to the enterprise from the Internet. For the purposes of the following cyber security discussions, intruders are defined as:

- **Outsider Hackers.** The primary goal of hackers is unauthorized entry; their motivation is thrill-seeking or criminal opportunity.
- **Outsider Attackers.** The primary goal of attackers is to destroy enterprise operations; their motivation is often political.
- **Insider Attackers.** The primary goal of an inside attacker is to disrupt enterprise operations; their motivation is personal gain or vengeance.

To maintain consistency with discussions of physical security in other sections of this document, Table 5-1 correlates physical intruders and cyber intruders.

TABLE 5-1
Correlation Between Physical and Cyber Intruders

Physical Intruder	Equivalent Cyber Intruder
Vandal	Outside Hacker
Criminal	Outside Hacker
Saboteur	Outside Attacker
Terrorist	Outside Attacker
Insider	Insider Attacker

Information systems are more vulnerable than ever before. Today's information management trends point to a technology convergence resulting in a standardized system architecture. A demanding regulatory environment and the need for defensible decision-making push today's utilities to integrate previously isolated information systems onto standardized platforms. In addition, employees increasingly request 24 hour-per-day access to internal information systems. Taken together, these trends create more, not fewer, opportunities for intruders to access and affect the entire enterprise information structure.

Gaining unauthorized entrance to an organization's information infrastructure is no longer the province of a small cadre of skilled intruders. The specific vulnerabilities of widely used platforms, like Microsoft Windows™, are detailed on numerous web sites. An arsenal of hacking tools is readily available on the Internet at no cost. These "freeware" programs are easy to operate and effective at gaining entrance to organizations via the Internet, radio, telephone, or wireless devices. Novice hackers can generate destructive virus code from special applications with no knowledge of programming. This shorter learning curve benefits attackers intent on intrusion and destruction. Cheap laptops, anonymous Internet accessibility, and readily available hacking tools offer political organizations a potent tactical weapon.

As the result of the existence of these adversaries, utilities have realized the need to become more vigilant to protect their valuable infrastructure. Information system failure can have catastrophic repercussions to a utility. Compromise of the financial system can result in millions of dollars of lost revenue. Corruption or destruction of operational data can lead to fines due to late or inaccurate regulatory reporting. A sabotaged web site has the potential to shake public trust during a time of crisis. Interruption of the plant process because of SCADA malfunction can lead to a wide range of health implications for the community.

5.4 Management

Management considerations for cyber security provides the policies and procedures that tie operational practices and system designs into an integrated approach for utilities. Key areas of concern focus on SCADA system access, passwords and other IT interface points within the utility.

5.4.1 Cyber Security Policies and Procedures

The most effective course of action available to utility management is the creation of a cyber security plan (often within the context of a physical security plan). A cyber security plan provides the policies, procedures, and direction for system enhancements that minimize intrusion risk as well as insider malfeasance. It is, however, an unfortunate reality that even the most vigorous anti-intruder security may not thwart a determined attacker.

For water utility operators, the SCADA system is of particular concern. Any disruption to the accurate operation of the SCADA system could have adverse health repercussions to the community. As such, specialized assessment of the SCADA system is indicated due to its marked difference from a more traditional information technology (IT) system. It is worth noting that the trend in automation systems is to use a more "open architecture" that does not rely on proprietary vendor protocols. The result is a more publicly available standardized operating platform, which increases the odds that its vulnerabilities are more widely known.

The centerpiece of a cyber security plan is its policies. Publicized and enforced policies can reduce the opportunity for an insider to anonymously sabotage any portion of the information system. Elements of this plan should include:

- a process for granting/revoking access to information systems
- password policies
- restricted information flow between the business and control networks
- comprehensive system documentation
- outlawing of unauthorized wireless or modem connections
- a Disaster Recovery Plan
- incident response goals

A forward-looking plan also provides a method for continuous security improvements. In this rapidly evolving field, it is essential to stay current. Several organizations are in the process of formulating cyber security standards. At the time of this writing, for example, the National Institute of Standards and Technology, a federal standards agency, maintains a highly informative web site that publicizes best practice security guidelines (csrc.nist.gov).

5.4.2 Cyber Security Training

Training activities can result in a higher level of cyber security in the workplace. User acceptance is an important part of adherence to security policies. Training sessions help to review security procedures and impart to all employees the importance of individual responsibility. Basic examples of the types of training to perform include these:

- Training for the general user population so that they understand all security policies and procedures. Specific items to be discussed should include:
  - Not to share passwords with others.
  - Not to write passwords down.
  - Not to set up wireless networks or wired connections between networks without authorization.
  - To password-protect home personal computers (PCs) used to connect to the enterprise.
- Training network administrators to analyze server and network log files to pinpoint unauthorized activity.
- Training operators should be trained to log out of the HMI whenever leaving the control room to prevent unsupervised access to the SCADA system.

5.5 Operations

Cyber security addresses the need to for the continuous functioning of the information systems serving the utility. Of special concern to water utilities is the SCADA system, whose distributed components maintain the process. Given the complex and interrelated nature of the SCADA system, a detailed approach is recommended to safeguard its reliability.

5.5.1 Intrusion Defense

Cyber intruders can gain access to an enterprise network via one of four broad avenues:

1. Internet
2. Telephone system,
3. Wireless (including radio)
4. Inside attacks

The following subsections outline methods of preventing unauthorized entry from each avenue.

5.5.2 Internet Intrusion

Internet access to the enterprise is not always under the control of utility IT staff. It is common for the umbrella municipality to administer all security aspects of the Internet gateway, including firewall configuration and Intrusion Detection System (IDS) oversight. In that case, it is important that the utility IT staff participate in municipal IT matters via technical committees or similar intra-organization forums.

5.5.2.1 Outside Hacker

The outside hacker is most easily deterred at the firewall. If no entry point is penetrable, the hacker will likely move on and choose an easier target. Thus, utilities may want to:

- Coordinate with the enterprise or utility IT department to conduct penetration tests on the Internet firewall. These tests are designed to uncover "open ports" commonly used by hackers to gain entrance to the enterprise network. Once inside, a hacker is free to access any computer on the business network, including SCADA computers if the business and control networks are connected.
- Restrict general user access to critical applications. For example, segregate financial servers by locating them on a separate network segment with tightly restricted access.

5.5.2.2 Outside Attacker

Even the most daunting security at the Internet gateway may succumb to the efforts of a determined attacker. Additional steps are necessary to further secure the SCADA system if connections exist between the business and control networks. Thus, basic steps that utilities may want to consider include these:

- Identify and disconnect all connections between the business and control networks that have no security controls, such as a router or firewall. Network traffic between the two networks should be strictly controlled to allow only legitimate connections.
- Conduct server and workstation software audits to verify that the operating systems have been "hardened" with the most current upgrades and security-related patches. The Microsoft Windows™ operating system, for example, is a favorite target of hackers because of its widespread use and well-documented security flaws. Some basic activities associated with this audit might include the following:
  - Verifying that anti-virus software is updated with the latest virus patterns.
  - Verifying that all servers have latest security patches applied for applications (e.g., database programs, email, etc.) as well as the operating system.
  - Reviewing system logs for inappropriate activity.
  - Confirming that every administrator password for the operating system and HMI have been changed from the default passwords.

5.5.3 Telephone System Intrusion

The most common method of telephone system intrusion is via dial-up modem. Most SCADA systems employ a modem to facilitate operations and maintenance of the HMI by vendor or in-house SCADA technicians. Traditionally, these modem connections have little or no security; they are an attractive target for "war-dialing," a common technique used by telephone hackers that uses a software program to automatically call thousands of telephone numbers to look for any that have a modem attached.

5.5.3.1 Outside Hacker

These basic suggestions can provide increased cyber security at little or no cost to the utility.

- Configure modems to allow dial-up access from a restricted set of telephone numbers.
- Leave modems connected to the SCADA system turned off. Turn on only for use by verified personnel (vendor or SCADA technician).
- Use a timer to turn off modems after a preset period of time (e.g., one hour) if not in use.
- Coordinate with the enterprise IT department to verify security on non-SCADA modems connected to the business network.

5.5.3.2 Outside Attacker

Utilities should instruct employees not to divulge user information—especially passwords—over the telephone. Hackers have a high success rate of obtaining passwords from unwary employees by posing as an IT technician needing user account information. This technique is known as "social engineering." Employees can be made aware of any authorized need for this information and asked to report any attempt to elicit password information without the proper authorization.

5.5.4 Wireless Intrusion

The explosion of wireless networking at home and in the workplace has created an enormous security risk for network administrators. Many wireless installations in the workplace can exist without the knowledge of the IT group. These installations generally have little or no security and can be accessed by anyone within signal range.

5.5.4.1 Outside Hacker

Utilities should eliminate unauthorized wireless networking (use wireless detection software and appropriate antenna/laptop software to identify unauthorized installations). A wireless access point using the default settings is open to network attack. Many wireless products are capable of configuration to acceptable levels of transmission security.

5.5.4.2 Outside Attacker

Modify and configure authorized wireless networking to the highest encryption levels. Minimize broadcast range and consider turning off "beaconing" features.

5.5.5 Insider Intrusion

Although an inside attacker has a decided advantage by possessing access privileges to the enterprise system, a stringent security environment renders operational staff activities less anonymous. A well-designed cyber security plan seeks to minimize inadvertent or intentional damage to the SCADA system by former or current employees and contractors. At the core of any security plan is an enforceable security policy and accompanying procedures that promote operational accountability and auditability.

The water utility industry is often staffed by long-term employees. The introduction of more stringent security procedures can rankle as untrusting. The current security-minded national environment, however, supports the perception that procedural changes to protect the enterprise are inevitable.

5.5.5.1 Management and Operational Security of the SCADA System

Several security practices that promote accountability and auditability are part of this mainstream movement, including these basic operational security considerations:

- Development of security policies that are posted in all control rooms
- Requirement for individual logon credentials to access the SCADA system
- Configuration of HMI logon privileges to match responsibility level
- HMI log files that are associated with user logon credentials with actions and changes made to HMI (creating a non-refutable audit trail of operator actions)
- Requirements for appropriate password strength rules for user access (i.e., more "complex" passwords for those with higher access privileges, such as an administrator)
- Immediate removal of a user account from the HMI if the account becomes inactive due to voluntary, and especially involuntary, termination
- Configuration of an inactivity timeout logout (or proximity sensor logout) to protect the control system if no one is present in the control room or the operator has stepped away from a remote workstation
- Requirement for a password to make software programming changes to RTUs/PLCs
- Programming of set point ranges to reject potentially harmful out-of-range adjustments

Advanced operational security considerations include these:

- Install third-party software—or upgrade current HMI version—to enable change propagation capability that monitors revisions to programming by date/time and login credentials. This software can also "undeploy" programming changes and revert to a previous version.
- Install safeguards for laptops used for onsite programming of remote PLCs or RTUs against theft or unauthorized use.

5.5.5.2 Physical Security of SCADA Components

Sensitive electronic SCADA components are often completely accessible to anyone in the plant. Utilities can reduce crimes of opportunity through these basic operational security considerations:

- Backup of SCADA servers and programming workstations to tape every night. Appropriate tapes should be stored offsite to ensure disaster recovery.
- Lockable PLC cabinets.
- Protective, lockable casing for exposed outdoor RTUs.

- SCADA servers secured in locked, climate-controlled areas.
- Restriction of access to the control room (and network/server room) with an entry system that stores information about who has entered and departed.

5.6 Design

Design considerations for cyber security should be coordinated with planning for the physical security of the organization. For example, card-reader access systems can be specified in the physical security plan to regulate access to restricted areas. Card readers can also benefit cyber security by doubling as a logon device that can record who has logged in and out of a computer.

Consistent with the previous intrusion defense discussion, design considerations will fall under the main areas of unauthorized entry: Internet, telephone system, wireless, and insider.

5.6.1 General Design Best Practices

Several design elements are recommended to bolster both insider and outsider defense, as well as to minimize less malicious levels of unauthorized entry. Utilities should evaluate implementation of the following basic activities:

- Identify and characterize all connections between the business and control networks. Though business and control networks have traditionally been separate, current demands for enterprise-wide data access dictates intra-network communication. By designing a secure connection between the networks, the enterprise can reap the benefits of data extraction from the control network and transport to the business network without compromising the mission-critical SCADA system. All network traffic between the two networks should be strictly controlled. Methods of securely segmenting the business and control networks include these:
  - **Virtual Air Gap.** Allows one-way data traffic from a control network server to a business network server by means of an optical isolator.
  - **Dual-homed Server.** Directs SCADA process data into a database server via one network card on the control side; allows access to the database only from the other network card on the business network.
  - **Router.** Restricts traffic to a small number of destinations as regulated by an Access Control List (ACL). A firewall is appropriate here as well, especially if control of the Internet gateway is not under the utility IT purview.
  - **Firewall.** Of particular value in the case where utility IT has no control over the enterprise Internet gateway.
- Review the policy governing entries on the router ACL so that only appropriate Internet Protocol (IP) addresses (such as a designated printer or the email server) can be accessed across the business and control system networks.
- Implement restricted access (and policies) to the SCADA control room. Consider biometric devices for areas requiring the highest levels of security.
- Provide a climate-controlled, locked enclosure for SCADA servers and networking components.

- Install and use a lock and intruder switch on control panels.
- Configure identical SCADA servers for "fail-over" redundancy.
- Install anti-virus software and configure for daily virus pattern updates on all servers and workstations.
- Reset all operating system and HMI passwords away from default settings.
- Verify that the backup system consistently captures a "snapshot" of designated servers and workstations. Provide offsite storage of selected tape backups necessary for disaster recovery purposes.
- Routinely back up all SCADA programs for PLCs, distributed control units, RTUs, SCADA servers, and similar programmable devices to provide for rapid recovery in the event of loss of program or need to install new devices. Store programs offsite.
- Provide individual UPSs for critical SCADA devices not protected by the main UPS system.

The following advanced activities can also be considered:

- Provide a UPS for all servers, networking components, and vital workstations. Consider addition of diesel-powered generator if warranted by system criticality.
- Provide a backup method to collect the data from the remote systems in case of communications failure. If, for example, a spread-spectrum radio network is the main method of remote SCADA communication, then telephone lines could be used for dial-up access in case of radio failure.

5.6.2 Internet Intrusion Design

Enterprise Internet security for municipal utilities is often under the stewardship of a municipal IT department. Given its level of specialization, training may be required for the IT staff who maintain security at the Internet gateway. Regardless, the principles are the same whether applied at the Internet gateway or between the utility and municipal networks.

Devices such as firewalls and routers, if properly configured, can effectively insulate a utility's network from outside attack. It is recommended that the utility appoint an appropriately skilled staff member or hire a consultant to determine the current best practices in Internet intrusion design because these technologies are evolving rapidly. Important basic design elements at the time of this writing are listed below:

- Contract for periodic evaluation of firewall and IDS effectiveness by a third-party security specialist to continuously maintain and improve operational performance.
- Consider using a Virtual Private Network solution to prevent unauthorized access into the enterprise from the Internet.
- Ensure that the firewall is either "stateful packet inspection" or "proxy" served.

Advanced design elements include these:

- Implement both types of firewalls in a "layered" approach.
- Install an IDS at the Internet gateway and regularly audit IDS logs for evidence of unauthorized entry. An IDS, properly monitored, can identify when a firewall is under attack and provide valuable information about intrusion attempts. Other IDS tools can detect system configuration changes and log file anomalies.

5.6.3 Telephone Intrusion Design

The telephone system is vulnerable to unauthorized access through modems. Typically, modems are often found in three areas: attached to the SCADA server for maintenance purposes, attached to remote access servers on the business network to facilitate employee dial-in, and "informal" modems attached to workstations so that the individual employee can work from home. This last type of modem is difficult to track down and usually has no security configured. A basic design element to reduce risk from modems is to :

- Create policies designed to prevent the installation of unauthorized modems on enterprise equipment. Those modems are often used in conjunction with remote control software to facilitate working from home. The security risks to the business usually outweigh the convenience for the individual.

Advanced design elements to reduce risk from modems include:

- Use commercial telephone-scanning software that can usually identify modem connections not sanctioned by the utility.
- Equip all SCADA modems with "lock and key" hardware devices. Distribute the "keys" to SCADA technicians and trusted vendors only. This solution provides flexibility as well as a higher degree of security. Technicians needing access can call at any time and from any telephone (e.g., a SCADA technician on travel).
- When telephone lines are used to connect to RTUs from the field, consider encrypting commands to prevent interference from attackers "tapping" into leased or owned lines.

5.6.4 Wireless Intrusion Design

Many utilities rely on radio transmission to interact with remote SCADA components in the field. RTUs in the field exchange, monitor, and control information in "plain text." These unencrypted broadcasts can be intercepted and retransmitted with different—potentially harmful—information. As a basic method of risk mitigation, utilities may want to:

- Provide "hardened," lockable enclosures for all remote control system units. Many of these units are in isolated areas with few protective measures to deter vandalism.
- Provide signal supervision and tamper alarms to detect loss of signal and tamper attempts.

More advanced methods of risk mitigation for wireless components include:

- Encrypting radio traffic between RTUs (or PLCs with radio units) to master unit with scrambler/descrambler devices. As an alternative, modify radios with appropriate capabilities to spread spectrum frequency-hopping.
- Specifying wireless networking configurable to an appropriate security level.
- Turning off "beaconing" and minimize reception area through a combination of antenna type and wireless access point configuration.

5.6.5 Insider Intrusion Design

The difficulty in designing a secure enterprise against an insider attack is evident—the insider already has direct access to information systems. The key to deterrence is a strong and enforced security plan that:

- Reduces the chances of acting anonymously.
- Restricts potential damage through limited access privileges, both physical and electronic.