

# Chapter 2

## Water/Wastewater Infrastructure Security: Threats and Vulnerabilities

Laurie J. Van Leuven

### 2.1 Introduction

The nation's critical infrastructure is made up of thousands of networks, pipelines, roads, conduits, and facilities; some are connected and some are isolated structures. Most of these critical systems are reliant on the full functionality of one or more other critical systems to ensure ultimate delivery of essential services to the public. Protecting these services requires a multilayered security program tailored for each system. Protective measures in the form of policies, procedures, and security investments can help reduce risks to critical infrastructure. The first step in developing a comprehensive security program is to recognize threats and each asset's vulnerabilities. This chapter will describe why drinking water and wastewater systems need to be protected, what threats to consider, and identify the vulnerabilities that increase risks and leave assets susceptible to an attack or large-scale system failure.

Utilities provide essential services to people 24 h a day, 7 days a week, and their services are essential to keeping communities healthy and economically viable. People rely on the constant delivery of drinking water and the collection, conveyance, and treatment of wastewater. The public uses water for the most basic human needs. Vital networks and businesses, industries, hospitals, other utilities, agriculture, and manufacturing industries are dependent on water systems. Water systems are also essential to recovery efforts following any natural disaster and for maintaining the standard of living for our everyday lives.

The systems responsible for delivering such fundamental commodities in the United States have long been identified as critical infrastructure. Drinking water and wastewater systems are both grouped into the Water Sector, one of 18 critical infrastructure sectors recognized by homeland security experts and officials as vital systems and networks that need to be protected (HSC, 2007). The Department of Homeland Security (DHS) designates the Environmental Protection Agency (EPA)

---

L.J. Van Leuven (✉)

Seattle Public Utilities/U.S. Department of Homeland Security (DHS), FEMA, Washington, DC, USA

e-mail: laurie.vanleuven@gmail.com; Laurie.VanLeuven@fema.gov

as the lead agency overseeing the Water Sector, which includes both drinking water and wastewater utilities. The Water Sector's goal is to recognize and reduce risks to infrastructure and support practices that build and maintain system resiliency (USDHS, 2010).

As of 2006, there were approximately 160,000 public drinking water utilities and more than 16,000 wastewater utilities in the United States. A high percentage of the population receives potable water and sanitary sewer service from these utilities, approximately 85 and 75%, respectively (USDHS and USEPA, 2007). The disparate ownership of the nation's water infrastructure, consisting of private, municipal, and special purpose districts, spreads across thousands of jurisdictions from coast to coast. The level of preparedness to which these independent systems could prevent or recover from a catastrophic incident varies greatly.

The wide range of dependencies on water systems increases the consequence of system outages through cascading impacts such as the effects on public health, the ability of first responders to provide emergency services, economic losses, and damage to the confidence of the American people (USDHS, 2007b). The assets necessary to keep water systems functioning are so vital that destruction or incapacity of these systems could debilitate national security, economic security, and public health or safety (USDHS, 2007a).

This chapter will examine why water infrastructure is so critical, identify the hazards that could threaten and disable an entire system, and illustrate the vulnerabilities and the potential consequences of an intentional attack on a water system. Other issues to be discussed are the drivers for security improvements and physical security countermeasures available to prevent security incidents and to protect against, prepare for, and respond to large-scale water system failures.

## 2.2 Why Secure Water Infrastructure?

Water systems are vulnerable to a variety of natural and human-caused threats. In the past decade, growing concerns about critical infrastructure becoming potential targets by terrorist attacks in the United States have contributed to a new dimension of security threats to utilities.

Utilities make up a considerable portion of the nation's critical infrastructure. Three sectors identified by DHS as critical infrastructure can be distinguished as utilities: water, telecommunications, and energy (USDHS, 2006). These utility sectors are all highly reliant on one another for their operations and in some instances they are co-located at the same geographic location (i.e., hydroelectric dams, pipes secured to bridges, and telecommunications antennas on water tanks and stand-pipes). In addition, an outage in any one of these sectors could have a significant impact on the other 17 critical infrastructures.

People may question the need to secure pump stations, water storage facilities, treatment plants, or pipelines. The simple answer is that the negative consequences of an intentional attack are too great to ignore. A significant attack on a water

system could result in widespread illness or casualties. A denial of service scenario could affect critical services such as firefighting and health care and could disrupt other dependent sectors such as energy, transportation, and food and agriculture. Most people recognize how devastating these consequences could be. However, they might question the likelihood of an attack, postulating that “the system has never been attacked before, why would it be attacked now?” The problem with this perspective is that the threats and risks to water systems are on the rise, due to an evolving threat environment.

The severe consequences of an attack on critical infrastructure and the significant interdependencies among so many sectors are enough to provide a motive to terrorists. An intentional attack on a water system would certainly spread fear and anxiety throughout society. One intentional successful attack anywhere in the country could lead to panic. People could easily become afraid to drink the water flowing out of their taps. Citizens living in other areas of the country would begin asking, “How safe is my drinking water?”

In addition to motive, the opportunity exists, since there are so many potential targets. There are literally thousands of water or wastewater assets that could be exploited by a determined terrorist. It is simply impossible to secure everything. There are also known interests by terrorist organizations to experiment with weapons of mass destruction. History has proven that attempts have been made by terrorists to contaminate drinking water systems using biological or chemical agents, mostly in other parts of the world.

Utility vulnerabilities have existed since they were built and disruptions to services are not uncommon. Water and wastewater utilities have always had to deal with the impacts of extreme weather conditions and pipeline or equipment failures that cause service interruptions. Water systems are frequently tested by natural disasters. Earthquakes, severe weather conditions, aging infrastructure, and the interdependencies among other systems are traditional threats utilities face everyday (Seger, 2003).

Since utility outages are not uncommon, most organizations have a mechanism to deal with smaller scale problems effectively. Utility operators are good at response and routine repairs. They hold a great amount of knowledge about the systems they own and operate. During a planned or manageable system outage, operators can isolate the problem and repair it quickly. System operators can usually reestablish services and return to normal operations within 12 h.

Given the quick recovery time of most service interruptions, customers have become accustomed to immediate restoration of vital water systems. However, water systems can unintentionally contribute to a less resilient community, if their customers are overreliant on immediate recovery. Water systems need to manage customer expectations by reaching out and educating the community to be self-sufficient for at least 72 h. The public will be far more resilient and less panicked if they have an adequate supply of emergency drinking water available for each member of their family during the immediate aftermath of an emergency situation.

The real challenges are preventing more significant system failures. The following list captures the most severe types of water system failures (NDWAC, 2005):

- Loss of pressurized water for a significant part of the system.
- Long-term loss of water supply, treatment, or distribution.
- Catastrophic release or theft of on-site chemicals affecting public health.
- Adverse impacts to public health or confidence resulting from a contamination threat or incident.
- Long-term loss of wastewater treatment or collection capacity.
- Use of the collection system as a means of attack on other key resources or targets.

## **2.3 Threats to Water Systems**

Utilities are adept at maintaining and repairing damage to aging infrastructure related to normal day-to-day operations. However, acquiring the expertise and funding to build the capability to effectively respond to a catastrophic natural disaster or terrorist attack (or to prevent one) that could wipe out an entire water system is a significant challenge. Recognizing threats to the water sector is a critical first step.

There are many types of threats that could harm all or parts of a drinking water or wastewater system. Even though periodic weather emergencies are to be expected, critical infrastructure providers must protect against more sinister threats that include intentional acts and build resiliency to recover from large-scale disasters that could lead to massive system damages. The growing list of threats to water systems is evolving as evident by two homeland security incidents of national significance.

### ***2.3.1 Evolving Threat Environment***

The United States has experienced a significant change in the threat environment for utilities during the past decade. Two defining incidents that have changed how our country's leaders think about threats and resiliency are the terrorist attacks of September 11, 2001, and Hurricane Katrina. These catastrophic events resulted in greater awareness of the vulnerabilities of critical infrastructure to intentional acts of terrorism as well as natural disasters. These incidents sparked new security and emergency management regulations through several legislative acts and executive directives.

#### **2.3.1.1 September 11 Terrorist Attacks**

The terrorist attacks on the World Trade Center and the Pentagon illustrate that there are people in the world with an expressed interest in harming Americans. They do not limit their targets to military personnel or facilities. Terrorist attacks can happen within our borders, at any time, and without warning. Terrorist actions are beyond criminal. According to terrorism expert Bruce Hoffman, acts of terrorism involve violence or the threat of violence and are specifically designed to spread fear and

anxiety through the whole of society and have far-reaching psychological effects (Hoffman, 2006).

Since terrorists are often outnumbered by the military forces of their target country, they most commonly use a strategy of unconventional tactics aimed at nonmilitary, noncombatant targets. This is one of the primary reasons why critical infrastructure and key resources are particularly at risk to a terrorist attack. Critical infrastructure sectors are rich targets, with many vulnerable assets across the country and not enough resources to protect and secure them all.

### **2.3.1.2 Hurricane Katrina**

Local communities throughout the United States and the world are susceptible to natural disasters that create negative impacts on residents, businesses, and visitors. Disasters can also hamper local government agencies' ability to provide essential functions for the welfare of the community. The most frequent and widespread incidents creating hardships for people related to safety of life and economic losses are due to extreme weather events.

In the aftermath of Hurricanes Katrina and Rita in 2005, residents of Louisiana and Mississippi and other areas around the Gulf Coast became painfully aware of how critical water systems are. Many essential functions were severely disrupted. There were massive problems with response and recovery coordination in the region. The lack of resiliency of these infrastructures magnified the hardships that people were experiencing. There was limited continuity of operations or government. Systems were shut down. It was difficult for emergency workers to determine where to begin. Damage assessments were slow, and the prioritization efforts suffered from lack of preplanning. Long-term recovery efforts and return to normal operations took years.

The storms devastated many infrastructure systems. In Louisiana, Mississippi, and Alabama, widespread power outages affected 2.5 million customers. Telecommunication systems collapsed and dangerous hazardous waste chemical facilities were flooded. Katrina destroyed or compromised 170 drinking water facilities and dozens of wastewater treatment facilities (SMGI, 2006). The stark realization of how unprepared the United States was to respond to the disastrous flooding from Hurricane Katrina took centerstage in the media during the aftermath. Government agencies were reactive to the criticism and promptly focused the majority of new homeland security and emergency management initiatives on preparedness and response plans, such as developing Continuity of Operations Plans. These efforts to improve preparedness are vital; however, we need to recognize the full spectrum of threats, not just the ones that have played out most recently.

### **2.3.2 Threat Assessments**

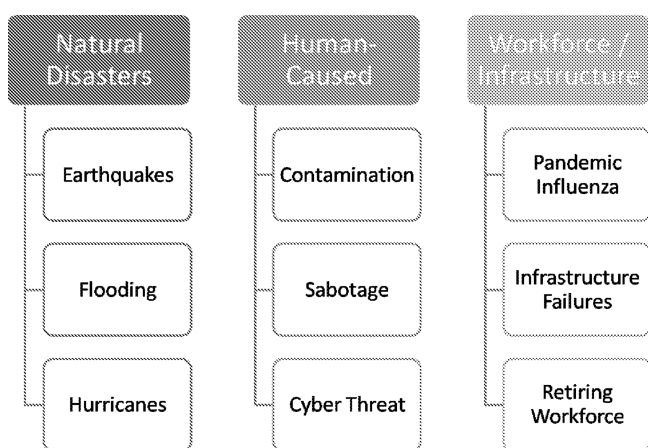
Water and wastewater utilities should conduct a Hazard Identification Vulnerability Analysis (HIVA) to determine which hazards they are most prone to (given their

climate and geographic location) and additional threats that could affect the system's operations. To effectively conduct a HIVA, water system operators should first begin by researching all available pre-existing HIVA results for their jurisdiction. For example, relevant HIVAs may be readily available from three different sources:

1. Local City Offices of Emergency Management
2. Local County Offices of Emergency Management
3. State Emergency Management Divisions

Next, water system planners should take inventory of the actual incidents that have caused or led to serious service interruptions during the past 20 years and the frequency of the incidents. This will help identify any particularly troublesome areas of the system that are vulnerable to the most common hazards. The next step involves researching specific threat information germane to your organization's geographic location. This is best achieved by reaching out to law enforcement agencies in your jurisdiction or your state's intelligence/fusion center. A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources (USDOJ, 2006). It is also important to engage with other stakeholders from within the utility's own organization and partnering agencies, who might be able to add valuable insights and perspectives.

The most common water system threats can be grouped into three different categories: (1) natural disasters; (2) human-caused incidents; and (3) workforce/infrastructure threats. Once you have identified the most likely threats, you can begin to assess the probability and the impact of an occurrence. Figure 2.1 shows the categories of all hazard threats.



**Fig. 2.1** Categories of all hazards and threats

### **2.3.3 Natural Disasters**

Depending on the region, certain threats are more likely. For example, along the Gulf Coast hurricanes may be the most frequent threat to a water or wastewater system. Communities along the West Coast are more prone to earthquakes and California suffers from frequent wildfire conditions resulting from hot, dry weather and high wind conditions. In the Midwest, there have been many problems with historical flooding when rivers rise and jump the banks, threatening homes, businesses, transportation systems, and other critical infrastructure. Other natural disasters that could impact water systems include tornadoes, severe windstorms, snow and ice storms, extended periods of freezing temperatures, lightning strikes, and droughts. Each jurisdiction has a unique set of probable hazards that could wreak havoc on water systems.

It is critical for a utility to have response plans developed for the most probable hazards that could impact their systems. Once plans have been developed, organizations need to train their employees and conduct exercises to ensure that everybody understands what their responsibilities are and what the priorities will be upon such a scenario. The importance of Continuity of Operations Planning (COOP) gained exposure after Hurricane Katrina. The value and benefits of continuity of operations planning is that it will help an organization prioritize tasks and repairs to systems by determining what things can fall off the plate when resources are overwhelmed.

#### **2.3.3.1 Human-Caused Incidents**

To fully understand the spectrum of threats facing water utilities, system operators must recognize the types of adversaries, malevolent persons, or groups that may try to prevent utilities from performing one or more of its essential functions. Information gathered about threats is critical to understanding how a potential adversary could carry out an attack on utility assets. This knowledge about potential threats helps utilities form the foundation of a targeted security program to protect critical assets. A water system's comprehensive threat profile is an important factor in risk calculations and methodologies.

There are three broad classes of intentional threats that water utilities should evaluate. They include physical threats, chemical contamination threats, and cyber threats. Each water utility must define the threats that will be used in their risk equation to calculate current and future risks and then propose security upgrades required to reduce those risks.

Information necessary to define threats includes but is not limited to the following:

- Incident reports, suspicious circumstance reports, criminal reports, intelligence reports and any historical data associated with a water utility. Sources for gathering this information include local, state, and federal law enforcement agencies and local/state offices of emergency management, fusion centers, and various other counterterrorism and federal agencies (i.e., FBI).

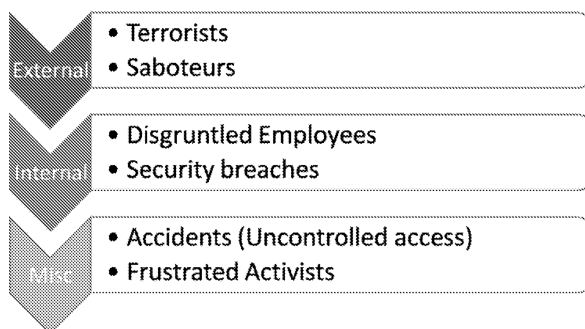
- Employee data on union disputes, employee conflicts/violence, expressed threats, etc.
- Internet, industry associations, WaterISAC (information sharing, analytic center), professional publications, etc.

Not all human-caused incidents are intentional or caused by outsiders, which is why we will explore external threats deeper by the type of individual or group who might perpetrate an incident. Since an intentional plot to contaminate the potable drinking water for an entire community or to wipe out a water system's ability to meet the service level needs of citizens would be a catastrophic incident, we will first focus on external threats and the possibility of an insider/outsider collusion attack. Figure 2.2 illustrates possible threat sources.

### 2.3.3.2 External Threats

External threats to a utility include everything from low-level vandals to very high-level terrorist threats. While there has not yet been a catastrophic attack on a drinking water system, there have been attempts demonstrating that the potential, means, motive, and opportunity exists. History has proven that terrorists have considered and carried out attacks on drinking water systems in the United States and other countries.

Critical infrastructure is an attractive target for terrorists due to the potential consequences and ripple effects of a successful attack. Drinking water systems have long been recognized as being vulnerable to an intentional chemical or biological contamination attack even though the probability of such an attack is uncertain (CRS, 2005). The tactic of poisoning an urban drinking water system supports an objective to commit indiscriminate harm on all parts of society. Such an attack could affect entire communities, especially vulnerable populations (i.e., infants, elderly, and immune compromised), businesses, industries, and health-care facilities. The distribution portion of a water system is especially at risk due to the ease of exploiting its vulnerabilities and the potentially large number of deaths and illness that



**Fig. 2.2** Possible threat sources



could result. The number of casualties from this type of attack, if successful, could surpass the death toll of 9/11.

The DHS has issued advisories to water utilities indicating that al-Qaeda has shown interest in using cyanide, *Botulinum toxin* (Botox), *Salmonella typhi* (the causative agent of typhoid fever), and *Bacillus anthracis* (the causative agent of Anthrax) to attack US water systems (USDHS, 2003). Terrorist organizations such as al-Qaeda are not the only external sources with motives to use chemical or biological weapons to attack a water system. The following list describes others who pose a threat:

- Vandals with no specific agenda, but possessing an interest in chemical and biological weapons and a propensity for violence.
- Anarchists seeking attention and independence.
- Ecoterrorists protesting the use of dams to manage water supply or other perceived environmental impacts related to chemicals or discharges into waterways.

There is empirical evidence that chemical and biological weapons have already been used or considered in plots to contaminate drinking water systems. The chronology of intentional water contamination events with chemical or biological hazards dates back thousands of years. While the actors, motives, tactics, and outcomes of chemical or biological attacks vary, the following is a partial list (Tucker, 2000; Kroll, 2010) of historical incidents that confirm the interest in such attacks:

- R.I.S.E., a neo-Nazi terrorist group, plotted to poison urban water supplies to incapacitate populations and gain attention for their cause. They were arrested and at the time had possession of several biological agents that had been produced in a college laboratory (1972).
- In North Carolina a water reservoir was intentionally contaminated resulting in denial of water to customers. Water had to be trucked in for residents (1977).
- New York City received anonymous threats of plutonium poisoning to the city's water supply. Subsequent testing for plutonium revealed 200 times the normal concentration levels, but not enough to warrant public health concerns (1985).
- Al-Qaeda members were arrested in Rome, in the process of attacking a water distribution system with cyanide near the US Embassy. They had detailed plans and equipment, but were thwarted at the last minute. While the compound turned out to be a benign cyanide derivative, it could have been a pre-event effort to trace the compound and the flow in the water system (2002).
- Two al-Qaeda members in possession of documents about how to poison US water supplies were arrested in Denver (2002).

Saboteurs can come in many forms. A saboteur may not be a terrorist but rather somebody who wants to cause the agency itself harm. They may be an adjacent property owner who is frustrated, but not attempting to make any political statement and not seeking to harm people. They may not be aware of the impact their actions could cause, but they are still a threat. Saboteurs target equipment and assets not

people. There are other threats to utilities that can be accidental such as a facility without adequate access control or an employee who does not secure a gate. If anybody can just walk in from the street, unintentional damage may occur. The capabilities and types of attacks that could be carried out by an external threat range from low-level all the way up to very high-level threats.

#### Low-Level Threat

A threat in this category could include one or two outsiders with no authorized access or inside information with the intent to cause physical damage to the water utility facility or theft of property or equipment.

#### Medium-Level Threat

A medium-level threat could include a small group of one to three outsiders who possess a limited amount of knowledge about the water system's assets, processes, and security systems. This level of threat may involve equipment or tools that are portable and easy to obtain.

#### High-Level Threats

A high-level threat could include an organized, highly motivated group of up to five outsiders with intent on sabotage or some type of major disruption to the system. They may be equipped with sophisticated tools, explosives, or weapons. The perpetrators of this type of attack would have extensive knowledge about water system assets, processes, and the security system. They also may have sophisticated cyber capabilities with a moderate level of resources. It is quite possible a planned attack. This category would include a combination of physical and cyber attacks on the water system assets for the purpose of a denial of water attack.

#### Very High-Level Threat

This group of adversaries possess all of the capabilities listed under the high-level threats, along with access and intent to use weapons of mass destruction, including chemical, biological, radiological, nuclear, or explosive substances. Tactics might include larger than backpack quantities of explosives such as truck bombs and chemical and biological substances with the intent to cause a significant number of deaths and unleash psychological terror on society.

### **2.3.3.3 Internal Threats**

Other threats to a water infrastructure are those that are tied to internal threats. This includes a disgruntled employee who may or may not be currently employed at the organization. There have been attacks on water systems as a direct result of a disgruntled employee. In Pittsburgh, a disgruntled employee deliberately contaminated

water mains by injecting weed killer into fire hydrants (Tucker, 2000). Other deliberate actions by insiders include a scenario where pipelines from drinking water distribution system were cross-connected with a wastewater collection pipeline.

Insiders, who include employees, former employees, contractors, and vendors, pose a particularly dangerous threat to utilities. They have specific knowledge of how the systems function. They know where the systems' weaknesses are. They already have access or may know how to circumvent existing security systems. They are trusted partners and can cover up their actions with minimal scrutiny. The capabilities and risks to utilities from insiders can also be categorized from the low-level threat to a high-level threat.

### Low-Level Threat

One individual with access to hand or simple power tools, whose intent is to physically damage the water utility or to profit from theft of materials for monetary gain.

### Medium-Level Threat

A single motivated insider (employee or contractor) working unaccompanied with authorized access and who possesses extensive knowledge of the utility's systems, processes, procedures, security systems, and emergency response protocols. They also may have knowledge about cyber systems including SCADA systems. This insider has access to hand and power tools and the ability to access on-site chemicals. The intent of this insider is to prevent the delivery of water by damaging or manipulating components of the water system or to introduce substances of concern into the water supply to damage the utility's reputation.

### High-Level Threat

A single, disgruntled individual, with motive and intent on harming the utility and/or personnel. This insider has all of the same capabilities as the medium-level threat, in addition to more extensive knowledge about the system, facilities, staffing rotations, and schedules. This individual may have recently undergone disciplinary actions or may have been terminated from employment and might hold other utility personnel or management responsible for their undesirable employment status. This high level of threat adversary may use handguns, explosives, or other violent acts to intimidate or harm people.

#### **2.3.3.4 Cyber Threats**

Cyber threats to water systems include the intent of individuals or groups to electronically corrupt or seize control of data or information essential to system operations. Adversaries attempting an attack via cyber mechanisms may seek out

information that contains highly sensitive knowledge about a system's vulnerabilities. This includes supervisory control and data acquisition (SCADA) networks, which contain computers and applications that perform remote control functions within the system.

SCADA systems have contributed greatly to water system efficiencies, by allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations. However, they present a significant security risk (USDOE, 2010). Similar to the vulnerabilities we see due to aging water infrastructure that was not designed with security in mind, SCADA systems were designed primarily to maximize functionality, not security. This leads to some SCADA networks that could be vulnerable to disruption of service, process redirection, or manipulation of operational system components that could result in asset failures and public safety concerns. All water system owners/operators should be cognizant of SCADA vulnerabilities and take actions to secure their SCADA networks (USDOE, 2010).

Additional cyber vulnerabilities are related to the need to secure sensitive information stored on data servers and in paper files. Examples of sensitive utility information includes vulnerability assessments, site security plans, response and recovery plans, water system and asset plans and specifications, descriptions of chemical processes and storage capacity, detailed maps and drawings, customer records, and financial data, all stored in electronic formats on information technology data servers.

The threat of a cyber attack carried out by a hacker can range greatly in sophistication. It can include low-level access via the Internet only or an individual or group with access to the information technology structure within an organization. A hacker may have direct access via modem or PC and may have use of sophisticated hacker tools for the purpose of compromising the system. They also may have access to administrator functions and may coordinate cyber attack with a physical attack. Perpetrators may use sophisticated network gear or other hacker tools. Results of a cyber attack may include denial of service, disruption of business functions, or the ultimate destruction of data and systems.

While the motivations of any of these groups may be unknown, effective security is critical to protect the assets and systems regardless of who might act out the threat or what their tactics might be. To get a better handle on which level of external threat to focus on, an organization should go through a process of determining their design basis threat.

### ***2.3.4 Design Basis Threat***

Given the wide variety of potential threats and the various capabilities of the actors involved with carrying out each threat, water systems need to carefully examine their entire threat spectrum. Once all of the potential threats have been collected, utilities need to evaluate and make a determination of what level of threats they are prepared to protect against. This predetermined level of adversary to which the utility must

be protected from is called the Design Basis Threat (DBT). Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence (ASIS, 2010).

The factors to consider include the adversary's ability to gain access to an asset, the history of any previous attempts on the asset, the type of damage the asset has sustained in the past, the motivation of the adversary, the tactics used, and whether or not the individual or group still exists in the geographic area. Other factors to include are the capabilities, history or intention, or specific targeting. For example, if neighboring utilities have been hit by vandals and criminals who have targeted water tanks, the likelihood that other nearby water tanks will be targeted is also high.

Determining the probability or likelihood of high-level threats is inherently difficult. There is currently a lack of industry-wide information on the probability of threats to water utilities. The most concrete data to pull from are historical events; however, that approach does not fully account for an evolving threat environment. Just because there is no history of a particular type of attack it does not mean an organization should dismiss the possibility of such an attack. We know the risk is greater than zero and therefore utilities must make an assumption of the likelihood of an attack. Water utilities in larger, urban areas will have a higher likelihood of a terrorist attack than rural community water systems. Utilities should attempt to find a ratio or probability factor that can satisfy a reasonable person's test. There are many different risk assessment methodologies available on how to calculate risk, so each utility should find a risk assessment system that meets their needs and will enable them to update their risk profile on an annual basis.

### ***2.3.5 Continuity Threats to Workforce and Infrastructure***

It is important to recognize other types of threats to a water system's ability to deliver essential functions. Any type of circumstance that could lead to a significant reduction in workforce or a significant increase in needed resources, should be considered in an organization's threat spectrum. This could be an aging workforce that may result in a spike in retiring employees with substantial system knowledge; aging infrastructure that could lead to a large-scale infrastructure failure; or a public health emergency in which many critical field or office employees are not able to report to work due to illness or dependent care needs.

#### **2.3.5.1 The Dual Threat: Aging Infrastructure and Aging Workforce**

Water system employees and infrastructure are both showing signs of the aging process. The risk of losing institutional knowledge about utility systems can dramatically affect the proficiency of maintenance activities of existing infrastructure. The average field employee age in utility industries ranges from 45 to 54. With more than 25 years of experience under their belts, these employees hold a considerable amount of expertise and familiarity with the assets they helped develop, install, and maintain through the years. As baby boomers draw nearer to retirement, a large

percentage of lead technicians and crew chiefs will take their individual knowledge base with them (Radice, 2010). With the extreme budget constraints that most utilities are facing, replacing these lost positions is not a guarantee. Many utilities are simply required to do more with less and may sacrifice expertise for quick fix contractors who will not aid in creating a sustainable in-house knowledge base for the next generation.

### **2.3.5.2 Aging Infrastructure**

At the same time as water system employees are aging and preparing to retire, the assets and infrastructure they have cared for through the years are also aging. In every community around the country there are examples of spectacular infrastructure failures that have led to large-scale service interruptions, significant property damage, and human injury as a result of the failure. Much of the nation's critical infrastructure still in service has exceeded its planned operating life and requires major renovations or replacement. The wear and tear of above- and belowground system components is evident as assets are exceeding their life cycle expectancy, many times without plans to replace them prior to failure. Large transmission water lines that are old may provide no warning at all that they are reaching a failure point. While smaller infrastructure breaks can be managed effectively, large-scale infrastructure failures can send a utility into crisis mode.

### **2.3.5.3 Interdependent Infrastructure Failures**

Other types of critical infrastructure are also aging and susceptible to failures that can have an impact on our water system operations. For example, in an urban location, a wide transportation system outage could greatly impact an organization's workforce. A good example of this is the I-35 Bridge failure in Minneapolis that occurred in 2007 (USA Today, 2007). Just after 6 p.m. on the evening of August 1, 2007, the 40-year-old bridge collapsed into the river and its banks without warning, killing 13 and injuring 121 others. At the time, there were approximately 120 vehicles, carrying 160 people, on the bridge. Transportation infrastructure, especially bridges, can have a significant impact on the mobility of water system employees. A bridge collapse could also wipe out water infrastructure such as transmission pipelines if they are attached to the structure.

### **2.3.5.4 Workforce Illness**

Another threat is that of a public health crisis or a pandemic influenza. In 2009, Mexico, the United States, and many other countries around the world became enthralled in the growing possibility of a worldwide pandemic. The swine flu (H1N1) sent shockwaves through public health and emergency management communities as they scrambled to dust off their pandemic influenza (or bird flu) emergency plans. While the name of the virus may change, planning for a pandemic

outbreak that could take away 40% or more of an organization's employees is critically important.

But, the largest threat to water systems may be that of complacency in which the low probability of occurrence outweighs the desire to reduce the risk in advance. The enhancement of security and the abilities of water systems to respond to all types of hazards are key to maintaining reliable supply and delivery of essential functions. Once the owners and operators of a water system better understand the threats they face, they need to become aware of their vulnerabilities.

## 2.4 Water System Vulnerabilities

Water systems are complex with many intricate connection points and interactive networks. Water system vulnerabilities can be general or specific. An example of a general vulnerability is that most water or wastewater infrastructure in service today was built many years ago. Aging infrastructure has inherent vulnerabilities because the materials used during the initial manufacturing or construction may not be as resilient as current day materials. The wear and tear on system components through the years also contributes to weakened structures. Another generalized vulnerability of water systems is heavy reliance on other critical sectors that are also subject to significant system failures such as electricity and telecommunications. Since older water infrastructure was not built with security as an objective, assets and facilities often were built with an excessive amount of access points (doors, hatches, vaults, etc.), contributing to increased vulnerabilities. Examples of specific infrastructure vulnerabilities might include a treatment facility with inadequate perimeter controls; a pump station with faulty locking mechanisms on a roll-up door; or an elevated water tank co-located with telecommunication towers and antennas that will require frequent access by contractors.

Vulnerabilities can be described as elements that are susceptible to accidents, failures, or attacks that are difficult to defend. Vulnerability assessments are an important step to take prior to identifying and implementing security counter-measures. The components of a water system that should be considered in a comprehensive vulnerability assessment include the following:

- Distribution systems including pipes and constructed conveyances
- Physical barriers
- Water collection, pretreatment, and treatment facilities
- Use, storage, and handling of various chemicals
- Storage and distribution facilities
- Electronic, computer, or other automated or cyber systems

Out of the above-listed system components, distribution systems, chemical treatment facilities, and cyber systems are generally considered the most vulnerable type of assets. The next section will explore vulnerabilities by

grouping the system components into three categories: above-ground structures, below-ground structures, and cyber systems.

2.4.1 Above-Ground Structures

Above-ground structures are water system components that are clearly visible, either by passersby or from aerial views. The popularity of satellite photographs and software available for free on the Internet (via GoogleEarth and other geospatial mapping tools) have made it easier for Joe and Jane Public to know exactly where above-ground critical infrastructure assets are located, even if the assets are situated in remote locations. As information sources become more advanced and accessible, water system operators will no longer be able to rationalize lack of security based on the obscurity of an asset’s location.

Above-ground water structures include dams, intake structures, wells, water and wastewater treatment plants, pumping stations, reservoirs, tanks and other water storage facilities, exposed conveyance or transmission pipes, open channels, tunnels or support facilities, command and control facilities, and administrative offices. All of these structures are vulnerable to threats, although some have higher level of consequences and risk.

Buildings or complexes that store chemicals such as chlorine, fluorosilicic acid, sodium hypochlorite, oxidizers, propane, diesel, and fluoride can multiply the risks for workers and neighboring communities. Gaseous chlorine is a particularly hazardous chemical of concern that increases risks to communities from the time it leaves the manufacturing facility during transit, to the storage of it on-site, until it is fully utilized in processes at the water facility.

Table 2.1 provides some guidance on how to evaluate the vulnerabilities of above-ground structures. In general, this exercise should provide information about how easily a villain could gain entry to a critical facility.

Table 2.1 Evaluation of above-ground structures

Feature	Quantity/capacity	Quality/construction	Security measures
Perimeter controls	Exterior fences, interior fences, gates, bollards, and vehicle barriers	Height, material, anti-climb, set backs, clear zones, and lighting	Access control, motion detection, and CCTV
Doors, hatches, and vaults	Number of access points	Hollow, steel, reinforced, etc.	Locked hatches, ladder locks, and intrusion detection
Locks and keys	Double entry systems, physical or electronic locks and keys, and padlocks	Automated locking, and tamper-resistant hinges	Door strikes and alarm contacts



### ***2.4.2 Below-Ground Structures***

Drinking water and wastewater owner/operators are incorporating an increasing number of underground water infrastructures into their systems. This includes efforts to bury water storage reservoirs that used to be above ground, construction of underground water and wastewater pump stations and overflow storage containment, and various vaults that provide access to electrical panels, equipment, and large transmission and conveyance pipelines. The mere fact that the structures are below ground provides a good barrier to certain types of threats. Below-ground structures are inconspicuous since they are not readily visible to a passerby. Some buried drinking water reservoirs have been turned into parks or open spaces for the enjoyment of neighboring communities. This can be a good activity generator to deter criminal behavior during daylight hours; however, entry points need appropriate security to deter and prevent unauthorized access. Below-ground infrastructure may have more protection against low-/mid-level threats than above-ground structures; however, they may be at an increased risk of other threats such as earthquakes and flooding.

Drinking water distribution systems are incredibly vulnerable due to the thousands of cross-connections and entry points into the system and difficulty detecting an intrusion. A motivated terrorist could facilitate a simple backflow contamination event with pumps and a number of chemical or biological agents. The introduction point into the distribution system could be from a fire hydrant, a residential home or apartment, or a commercial building. An example of how effective this tactic could be is the fact that accidental backflow occurrences have resulted in many incidents of waterborne illness and even death. According to the EPA, backflow events caused 57 disease outbreaks and 9,734 cases of waterborne disease from 1981 to 1998 (USEPA, 2001). If the system is vulnerable to accidents, it is just as vulnerable to a deliberate attack.

An intentional dissemination of a chemical or biological agent or contaminant through a backflow event is a significant concern to the drinking water industry. The detection of such an incident would most likely occur after people become ill and hospitals begin observing a trend. Currently, there are several studies and evaluations of new technology to enable early water contamination warning systems via online water quality monitoring stations throughout a distribution system. The downsides to these systems are that they are very costly to implement, administer, and maintain, and there is a natural resistance to trusting a positive reading (for fear of overreacting to a false-positive reading). All that being said, improvements in this detection area as the science and technology progresses are promising.

### ***2.4.3 SCADA and Cyber Systems***

SCADA system vulnerabilities are diverse depending on how each system has developed and deployed the technology. Some systems may have multiple subsystems that are networked together. These systems allow personnel to activate and

deactivate pumps and valves from a remote computer system or they can be designed to accommodate local intelligent valve control.

While best practices models tout the importance of physically separated systems on standalone networks, SCADA systems are occasionally linked (even unknowingly) to general utility business computer networks. Utilities that link SCADA networks to its technicians, engineers, or operational decision-makers for convenience sake create vulnerabilities. When any bridge between the two networks occurs, the entire SCADA system becomes only as secure as the weakest point of the business network. Even when the networks are truly separated, many SCADA systems are only protected by simple passwords.

Cyber security vulnerabilities are also related to an organization's posture on public information policies. Revealing too much information about critical utility systems, processes, treatment facilities, and other assets in public forums creates unnecessary vulnerabilities. Utility web sites, as well as those of utility consultants and contractors, frequently provide a goldmine of information that could be used to gain access to additional information or to plot an attack against a water system. For example, some utility web sites might list employee names and e-mail addresses, thus providing a window of opportunity to solicit or seize sensitive data and information, while a consultant web site might boast photographs, drawings, and detailed descriptions of large capital projects involving critical infrastructure.

#### ***2.4.4 Vulnerability Assessments***

Vulnerability or risk assessments are intended to provide a roadmap for lowering risks. Vulnerability assessments are the best way for an organization to take inventory of their system's critical components and determine what security risks owners/operators should focus on first.

One way to assess vulnerabilities is by pairing up individual assets or system components with a particular threat. This matching up of assets/threat pairs provides an opportunity to evaluate how successful an intentional act to disrupt the system could be. The various types of threats that might be matched up with one individual asset (a pump station) are illustrated below and summarized in Table 2.2.

There are many different formats and categories that can be used when developing a vulnerability assessment. The technical components of a comprehensive vulnerability assessment include the following:

- Characterization of the facility or system
- Inventory of significant assets and areas
- Threat assessment (including DBT and asset/threat pairs)
- Consequence assessment
- SCADA assessment
- Organizational security policies and procedures
- Local, state, and federal interactions

Table 2.2 Potential asset/threat combinations

Asset	Threat	Tactics	Likelihood of success
Pump station	External, sabotage	Explosives, mechanical tampering, arson	<i>Medium</i> – Depending on access control and detection capabilities
Pump station	External, cyber	Control of SCADA system, manipulation of valves and equipment	<i>High</i> – Could gain control and proceed undetected
Pump station	External, vandal, or criminal	Graffiti, property damage, theft of equipment or wire	<i>Medium</i> – Depending on fences and access control
Pump station	Internal, disgruntled employee	Mechanical tampering or electronic panels	<i>High</i> – Employees have access, knowledge, and opportunities

- Physical security components
- Risk analysis
- Risk reduction options and recommendations

Vulnerability assessments should be updated after every significant security incident and annually with new information about system facilities, assets, processes, and updated threat analyses. Once the owner/operator of a water utility has completed or updated their vulnerability assessment, they need to make determinations about which recommendations to implement and how to fund the security improvements. It is almost certain that the list of recommendations from a system-wide vulnerability assessment will far outweigh the funding available to address all of the security risks. Resource allocation decisions about how to proceed are not made lightly. Chapter 22 will address the drivers for security improvements, types of physical security measures, and the need for a multilayered security program approach.

References

(ASIS) American Society of Industrial Security. (2010). International, Protection of Assets Manual. <http://www.asisonline.org/library/glossary/d.pdf>

(CRS) Congressional Research Service. (2005). Report for Congress, Terrorism and Security Measures Facing the Water Infrastructure Sector, Jan 2005, p. 4.

Hoffman, B. (2006). *Inside Terrorism*. Columbia University Press, New York, NY, p. 40.

(HSC) Homeland Security Council. (2007). *National Strategy for Homeland Security*. The White House, Washington, DC, Oct 2007, pp. 1–25.

Kroll, D. (2010). *Securing Our Water Supply: Protecting a Vulnerable Resource*, PennWell Publishers, Tulsa, OK, pp. 19–27.

(NDWAC) National Drinking Water Advisory Council. (2005). Water Security Group Findings, May 18, 2005, p. vii.

Radice, S. (2010). The Dual Threat: Aging Infrastructure and Aging Workforce Call for Integrated Asset and Workforce Management, Electric Energy Online, [http://www.electricenergyonline.com/?page=show\\_article%26;mag=47%26;article=351](http://www.electricenergyonline.com/?page=show_article%26;mag=47%26;article=351)

- Seger, K.A. (2003). *Utility Security: The New Paradigm*, PennWell Publishers, Tulsa, OK, Penwell Corporation, p. 35.
- (SMGI) Security Management Group International. (2006). Overview – Hurricane Katrina Crisis, Aug 15, 2006. <http://www.smgicorp.com/resources/documents/SMGI-KatrinaCS.pdf>.
- Tucker, J.B. (2000). “Lessons from Case Studies”. *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. Edited by J.B. Tucker, Cambridge, MA, MIT Press, pp. 250–251.
- USA Today. (2007) On Deadline Blog. Latest on Deadly Minneapolis Bridge Collapse. Retrieved Feb 20, 2008, from message posted to <http://blogs.usatoday.com/ondeadline/2007/08/latest-on-deadl.html>
- (USDHS) U.S. Department of Homeland Security. (2003). Advisory: Potential Al Qaeda Threats to US Water Supply, June 23, 2003.
- (USDHS) U.S. Department of Homeland Security. (2006). *National Infrastructure Protection Plan*. Department of Homeland Security, Washington, DC, p. 3.
- (USDHS) Department of Homeland Security. (2007a). Homeland Security Threat Assessment: Executive Summary, Aug 2007, p. 8.
- (USDHS) U.S. Department of Homeland Security. (2007b). National Strategy for Homeland Security, Oct 2007, p. 28.
- (USDHS) U.S. Department of Homeland Security. (2010). National Infrastructure Protection Plan Water Sector Snapshot, [http://www.google.com/url?sa=t&source=web&ct=res&cd=4&ved=0CCkQFjAD&url=http%3A%2F%2Fwww.dhs.gov%2Fxlbrary%2Fassets%2Fsnipp\\_snapshot\\_water.pdf&rct=j&q=epa+water+sector+security&ei=tkP7S9OtO4KwMomUqb0B&usg=AFQjCNF-6XMn3r4GtVTX3FwqnVyhBAEzcQ](http://www.google.com/url?sa=t&source=web&ct=res&cd=4&ved=0CCkQFjAD&url=http%3A%2F%2Fwww.dhs.gov%2Fxlbrary%2Fassets%2Fsnipp_snapshot_water.pdf&rct=j&q=epa+water+sector+security&ei=tkP7S9OtO4KwMomUqb0B&usg=AFQjCNF-6XMn3r4GtVTX3FwqnVyhBAEzcQ)
- (USDHS & USEPA) U.S. Department of Homeland Security and the U.S. Environmental Protection Agency. (2007). Water Sector Specific Plan as Input to the National Infrastructure Protection Plan. (Office of Ground Water and Drinking Water, EPA 817-R-07- OOlA) May 2007, p. 3.
- (USDOE) U.S. Department of Energy. (2010). 21 Steps to Improve Cyber Security of Data Networks, <http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf> 3
- (USDOJ) U.S. Department of Justice. (2006). Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, Aug 2006. [http://it.ojp.gov/documents/fusion\\_center\\_guidelines.pdf](http://it.ojp.gov/documents/fusion_center_guidelines.pdf)
- (USEPA) US Environmental Protection Agency. (2001) Potential Contamination Due to Cross-Connections and Backflow and the Associated Health Risks: An Issues Paper, Sept 27, 2001. [http://www.epa.gov/cgi-bin/epalink?logname=allsearch&referrer=potential contamination due to cross-connections an issue paper|1|All&target=http://www.epa.gov/safewater/disinfection/tcr/pdfs/issuepaper\\_tcr\\_crossconnection-backflow.pdf](http://www.epa.gov/cgi-bin/epalink?logname=allsearch&referrer=potential%20contamination%20due%20to%20cross-connections%20an%20issue%20paper%5B1%5D&target=http://www.epa.gov/safewater/disinfection/tcr/pdfs/issuepaper_tcr_crossconnection-backflow.pdf)

Handbook of Water and Wastewater Systems  
Protection

Clark, R.; Hakim, S.; Ostfeld, A. (Eds.)

2011, XVI, 528 p., Hardcover

ISBN: 978-1-4614-0188-9