Water Infrastructure Resilience

epa.gov/emergency-response-research/water-infrastructure-resilience

August 13, 2019

Detection

EPA conducts contaminant detection research to support water utilities. Most drinking water utilities use commercially available water quality sensors to monitor for changes in water quality indicators. Indicators include pH, levels of free or total chlorine, total organic carbon, and others. Some contaminants, known as agents, are of concern because they can be adapted for use as weapons. EPA has tested commonly used sensors to learn if they can detect water contaminated with chemical, biological, or radiological agents, in addition to detecting routine water quality variations. Current research focuses on novel detection technologies that are new to the market, and technologies that could detect of contamination in source water, such as reservoirs.

Physical/cyber Protection and Resilience

Water systems are considered one of the nation's critical infrastructures. It is assumed that no physical or software protection can prevent all attacks. So this critical infrastructure requires increased protection and the ability of utilities to detect, respond to, and recover from physical and cyberattacks. Water system operators can lose their ability to control the flow and quality of the water or lose the ability to track the true status of the water system. Thus, water system managers need to improve their ability to know:

- when their treatment systems, pumps, valves, tanks, etc. are being compromised,
- how to quickly stop an attack,
- how to recover so that safe and full service can be returned to the community

Cybersecurity

EPA is leading a steering committee of water industry experts to develop the capability to evaluate and test cybersecurity equipment for the protection of water system infrastructure. Experts come from other federal agencies and private companies representing water system operators, hydrant manufacturers, intrusion detection and water quality sensor manufacturers, and data management service providers. Research to improve the cyber security of water utilities will be carried out at the EPA Water Security Test Bed (WSTB) located at the Department of Energy Idaho National Laboratory near Idaho Falls, Idaho.

The researchers will investigate the ability of hackers to take over the control and operation of pumps, valves, and hydrants, or to provide incorrect operational and water quality information to the water system operators, thus compromising pipe integrity water quality

and fire protection. The full-scale WSTB hydraulic network and control system will be made more complex to better simulate a water system with multiple communication systems (cellular, WIFI, WAN), cloud services, SCADA (supervisory control and data acquisition) and "internet-of-things the interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.", multiple commercial network software, anomaly detection equipment, artificial intelligence, and machine learning programs. This will enable red team/blue team (attacker vs. defender) exercises and the development of an operator training curriculum. The lessons learned will provide information so water systems can become more resilient to the ever present and increasing risk of cyber attacks.

Physical Protection and Resilience

The Bioterrorism Act of 2002 requires that drinking water utilities serving more than 3,300 people conduct vulnerability assessments and develop emergency response plans. EPA and its partners helped utilities meet these requirements by developing tools and a system of methods (links at the bottom of this page). One such tool is,

The Blast Vulnerability Assessment (BVA) tool - a desktop computer application developed by EPA, can provide estimates of damage that could occur from an attack on a water utility using explosives. This tool is available from the Water Information Sharing and Analysis Center (WaterISAC), a secure website with a controlled subscription list.

The consequence estimation component of the *Threat Ensemble Vulnerability Assessment (TEVA) Sensor Placement Optimization (TEVA-SPOT) tool* allows water utilities to estimate health consequences, risks, and vulnerabilities from contamination. Through the use of this tool, utilities can harden their system against contaminant attacks, better handle security incidents, and day-to-day operations.

The*Water Network Tool for Resilience (WNTR)* is a Python package designed to simulate and analyze the resilience of water distribution networks. WNTR has an application programming interface (API) that is flexible and allows for changes to the network structure and operations, along with simulation of disruptive incidents and recovery actions.

EPA has collaborated with the American Water Works Association (AWWA) to develop contingency plans in the event of a large-scale disaster. *Planning for an Emergency Drinking Water Supply*has recommendations on planning for alternative drinking water sources and water and wastewater treatment.

Related Links

- EPA's Water Security Testbed
- EPA’s Water Security Test Bed (WSTB) video
- WaterISAC