United States
Environmental Protection
Agency

Enhanced Security Monitoring Primer

For Water Quality Surveillance and Response Systems

Office of Water (MC 140) EPA 817-B-15-002B May 2015

Introduction

A Water Quality Surveillance and Response System (SRS) provides a systematic framework for enhancing distribution system monitoring activities to detect emerging water quality issues and respond before they become problems. An SRS consists of six components grouped into two operational phases, surveillance and response. The surveillance components are designed to provide timely detection of water quality incidents in drinking water distribution systems and include: Online Water Quality Monitoring, Enhanced Security Monitoring, Customer Complaint Surveillance and Public Health Surveillance. The response components include Consequence Management and Sampling & Analysis, which support timely response actions that minimize the consequences of a contamination incident. The *Water Quality Surveillance and Response System Primer* provides a complete overview (USEPA, 2015).

This document provides an overview of Enhanced Security Monitoring (ESM), a surveillance component of an SRS. It presents basic information about the goals and objectives of ESM in the context of an SRS. This primer covers the following four topics:

- **Topic 1**: What is ESM?
- **Topic 2**: What are the major design elements of ESM?
- **Topic 3**: What are common design goals and performance objectives for ESM?
- **Topic 4**: What are cost-effective approaches for ESM?

Topic 1: What is ESM?

ESM utilizes physical security equipment at key distribution system facilities to detect unauthorized entries that could lead to a contamination incident. ESM equipment can also be effective for detecting vandalism and theft. Furthermore, video monitoring systems used for ESM can provide operational benefits by allowing utility staff to view process equipment and conditions at remote facilities without a site visit.

Figure 1 is a schematic representation of ESM. Intrusion detection is provided by equipment strategically located at a utility facility. Alerts generated are transmitted by a reliable communication system, and personnel are notified of the alerts through emails, mobile devices or display at a central control facility. ESM investigations are guided by documented procedures and coordinated with external agencies such as local law enforcement.

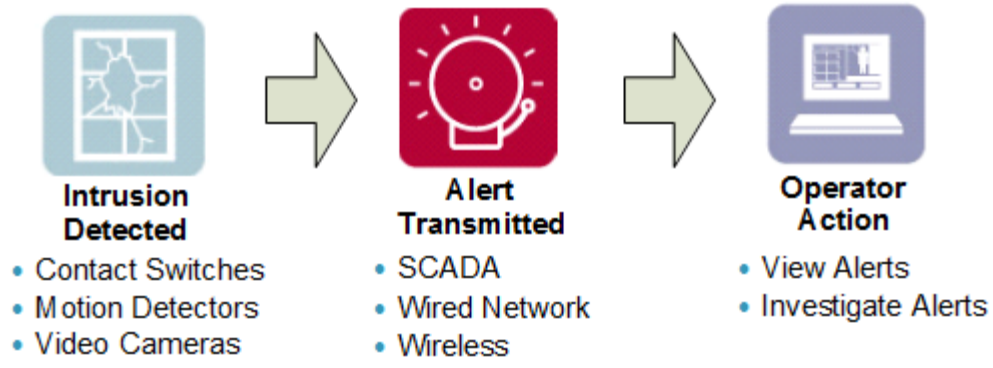

Figure 1. Schematic Representation of ESM

Topic 2: What are the major design elements of ESM?

The major design elements for ESM are shown in **Figure 2** and described under the remainder of this topic.

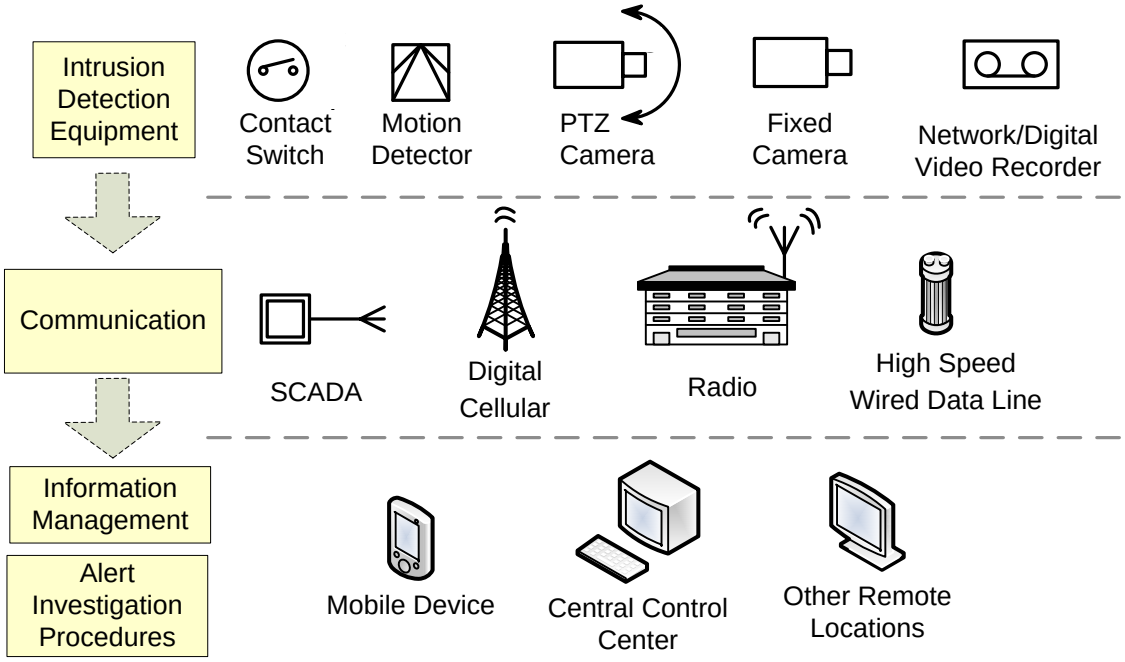

Figure 2. ESM Design Elements

Intrusion Detection Equipment

The Intrusion Detection Equipment design element focuses on selecting facilities for security enhancements and proposing equipment for each selected facility. The facility and equipment selection process can use a risk-based methodology such as the Vulnerability Self-Assessment Tool, which is compliant with the J100 industry standard. This process assesses the threat of, vulnerability to and consequence of attacks at each facility under consideration and evaluates the overall reduction in risk provided by ESM enhancements. This analysis provides a quantitative basis for selecting facilities and equipment for ESM.

The deployment of intrusion detection equipment is at the core of the ESM component. The ability of ESM equipment to detect intrusions depends on the placement, number and types of intrusion detection sensors and video cameras. Physical security equipment is continuously improving as sensing technology advances, with equipment becoming less expensive, more reliable and more configurable. These advances provide for broader coverage with fewer invalid alerts and have allowed utilities with limited resources to implement real-time security monitoring at remote utility facilities.

DID YOU KNOW?

The EPA's Vulnerability Self-Assessment Tool (VSAT) is a J100 standard compliant risk assessment software tool for water, wastewater and combined utilities of all sizes.

The tool assists drinking water and wastewater facility owners and operators in performing security threat and natural hazard risk assessments, as well as updating utility Emergency Response Plans. (EPA, 2013).

ESM equipment can be divided into two general categories: Intrusion Detection and Video Surveillance. Examples of each category are illustrated in **Table 1**.

Table 1. ESM Equipment

Equipment Types		Description
Intrusion Detection	Door and hatch sensors	Contact switches such as magnetic proximity and mechanical limit types Used at site access points (for example, on doors, windows or hatches)
	Motion sensors	Used for site or interior area coverage (for example, along a row of windows)
	Fence-mounted sensors	Used for disturbance sensing (for example, taut wires and magnetic field sensors)
	Buried-line sensors	Used for perimeter security (for example, near fencing)
Video Surveillance	Internet protocol cameras	Converts images into digital data
	Infrared cameras	Used for outdoor or low light conditions
	Event-based network or digital video recorders	Transmits video clips on demand and stores video data
	Video analytics	Algorithms embedded in video software to detect static (loitering or unattended items) or dynamic (walking or running) situations captured by monitoring cameras

Communications

The Communications design element consists of systems that transmit ESM alert information from facility intrusion detection equipment to a central control facility. The communications infrastructure must be capable of supporting the required data speed (bandwidth) such that ESM alert information can be transmitted to the central control facility in a timely manner. Data speed requirements will vary greatly depending on whether the system includes video data and how the video monitoring system is configured to transmit data.

Information Management

Once the data is delivered to the central control facility, it should be displayed on a user interface that allows utility staff to quickly recognize and respond to the alert. Furthermore, ESM alert information must be stored and accessible for post-incident analysis. Information technology architecture configurable by system administrators is a standard approach.

DID YOU KNOW?

A useful resource for ESM is the *Guidelines for the Physical Security of Water Utilities / Guidelines for the Physical Security of Wastewater/Stormwater Utilities* (ASCE/AWWA, 2011), a collaborative publication from the American National Standards Institute, American Society of Civil Engineers (ASCE), American Water Works Association (AWWA), and Water Environment Federation. This document is available for purchase from ASCE.

For both the Communications and Information Management design elements, leveraging existing network and communications infrastructure can reduce the cost of equipment and installation. When designing these elements of the system, consideration should also be given to in-house capabilities and compatibility with existing equipment.

Alert Investigation Procedures

ESM alerts need to be promptly investigated by utility personnel to determine whether or not the potential intrusion might be related to drinking water contamination. The following are basic example steps that may be performed during ESM alert investigations.

1. An ESM investigation begins after utility staff receives an intrusion alert.
2. Utility personnel use a checklist to guide them through a predetermined investigation procedure to determine whether the intrusion could disrupt utility operations or present a risk of contamination. The checklist may guide actions such as:
    a. Assessing known activity at the facility, such as maintenance by utility personnel or contractors
    b. Assessing video, if available, to verify the intrusion incident
    c. Notifying and dispatching investigators to physically inspect the facility where the alert originated
3. If definitive video evidence is not available, an investigation is conducted to verify or rule out the intrusion and determine whether there was access to the finished water supply.
4. If the investigation determines that the alert was not caused by unauthorized activity, the investigation is closed and logged.
5. If the investigation verifies an intrusion with access to the finished water, the investigation continues according to procedures in the drinking water utility's Consequence Management Plan.

DID YOU KNOW?

Invalid alerts associated with procedural errors are common and often caused by employees who forget to call in when accessing a monitored facility or forget to completely close all monitored doors when leaving the facility. Equipment and environmentally-caused invalid alerts are less common.

Topic 3: What are common design goals and performance objectives for ESM?

The design goals and performance objectives established for ESM by the utility provide the basis for the design of an effective component.

ESM Design Goals

Design goals are the specific benefits that utilities expect to achieve by implementing ESM. A fundamental design goal of an SRS is the ability to detect and respond to possible distribution system contamination incidents. In addition to this fundamental SRS design goal, other ESM-specific design goals such as detecting theft, vandalism and sabotage incidents can be realized. Examples of common ESM design goals are listed in **Table 2**.

Table 2. Examples of Common ESM Design Goals

Design Goal	Description
Identify intrusion incidents that could lead to water contamination	ESM can provide early warning of contamination incidents that could harm public health or utility infrastructure, which can trigger response actions to minimize consequences. In some cases, ESM may even preempt water contamination if the perpetrator is caught in the act.
Deter, detect and respond to theft, vandalism and sabotage	ESM systems can detect all types of intrusion incidents including those where contamination is not the intent of the intruder. Such criminal activity may not have a significant impact on public health, but can place utility staff at-risk and impact a utility's operating budget and day-to-day maintenance activities.
Remote monitoring of process equipment	If ESM includes video monitoring, operational benefits can be realized if the ESM cameras can also be used to monitor process equipment at unstaffed facilities. For example, pumps can be observed for malfunctions and intake structures can be monitored for the build-up of debris. Video monitoring can reduce the amount of travel time and on-site inspections required, thus reducing utility labor costs.
Increased collaboration within the utility and with local law enforcement	Collaboration with law enforcement during water utility drills and exercises can lead to improved coordination during response to real-world emergencies. Also, an ESM camera with a field of view of a public area can support law enforcement investigations unrelated to a water incident.
Improved response decision making	Developing ESM procedures can streamline and standardize a utility's decision-making process when investigating an intrusion incident. Thus, procedural improvements can enhance a utility's overall preparedness and responsiveness to physical security alerts.

ESM Performance Objectives

Performance objectives are measurable indicators of how well the SRS meets the design goals established by the utility. Throughout design, implementation and operation of the SRS or its components, the utility can use performance objectives to evaluate the added value of each capability, procedure or partnership. While specific performance objectives should be developed by each utility in the context of its unique design goals, general performance objectives for an SRS are defined in the *Water Quality Surveillance and Response System Primer* (USEPA, 2015) and are further described in the context of ESM as follows.

- **Incident coverage**: Detect and respond to a broad spectrum of water quality incidents. One of the primary focuses of ESM is deploying intrusion detection sensors and video monitoring equipment to reduce the risk of contamination at select sites. The intent of such equipment is to monitor all areas that provide access to finished water, and detect all intrusions that could lead to a contamination incident. ESM design goals may also include detection of vandalism and theft, which could require monitoring of areas that do not provide access to finished water.
- **Spatial coverage**: Achieve spatial coverage of the entire distribution system. ESM is limited in its ability to detect contamination incidents throughout the distribution system because only specific utility facilities are monitored for intrusions. However, utility facilities are chosen for ESM equipment based on their overall risk of contamination and the amount of risk reduction that would result from such enhancements. Thus the sites selected for enhancements can have the potential to impact a large portion of the distribution system and general population.
- **Timeliness of detection**: Detect water quality incidents in sufficient time for an effective response. Utility staff must be immediately alerted of intrusions and investigate alerts in a timely manner. To meet this objective, alerts from remote facilities must be transmitted to the central control facility without delay. ESM also includes procedures for initiating and conducting an investigation in a timely manner. With a rapid response, it may be possible for the ESM component to prevent a contamination incident from occurring.

- **Operational reliability**: Minimize downtime for equipment, personnel and other support functions necessary for the component to meet the other performance objectives. One of the criteria for selecting intrusion detection equipment and information management systems should be reliability. In many cases, selecting a more reliable device that is more expensive can save money over its lifecycle when compared to a less expensive device requiring more maintenance.
- **Alert occurrence**: Reliably indicate unauthorized intrusions with a minimum number of invalid alerts. When implementing ESM enhancements, proper commissioning is recommended to ensure that each intrusion sensor is sensitive enough to detect intrusions with at least a 95 percent confidence level, but not overly sensitive and prone to an unacceptable number of invalid alerts.
- **Sustainability**: Realize benefits that justify the costs and level of effort required to implement and operate ESM. Benefits are realized through attainment of the design goals for ESM. The AWWA's J100 Risk Analysis and Management for Critical Asset Protection Standard can be consulted for quantifying non-quantifiable benefits of security enhancements (ANSI/ASME-ITI/AWWA, 2010). Costs should be considered over the lifecycle of the component, including implementation costs, operation and maintenance costs, and renewal and replacement costs.

DID YOU KNOW?

Utilities may be able to make modest changes or additions to existing physical security capabilities to implement their ESM component.

Topic 4: What are cost-effective approaches for ESM?

Utilities can take the following simple steps to develop the foundation for ESM:

- Rank major utility facilities with respect to the risk of contamination.
- At the facilities determined to have the greatest risk, add simple, inexpensive intrusion sensors, such as contact alarms on doors and hatches. Use existing communications to transmit ESM alerts if possible.
- Establish procedures for the joint utility and law enforcement investigation of ESM alerts that might be indicative of contaminated drinking water.

Next Steps

Visit the Water Quality Surveillance and Response Website at http://water.epa.gov/infrastructure/watersecurity/lawsregs/initiative.cfm for more information about SRS practices. The Website contains guidance and tools that will help a utility to enhance surveillance and response capabilities, as well as case studies that share utility experiences with SRS implementation and operation.

References

ANSI, ASME-ITI and AWWA. (2010). *Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems. AWWA J100-10*. Denver, CO.

ASCE and AWWA. (2011). *Guidelines for the Physical Security of Water Utilities (56-10) and Guidelines for the Physical Security of Wastewater/Stormwater Utilities (57-10)*. Denver, CO.

USEPA. (2013). *Vulnerability Self Assessment Tool (VSAT)*. Retrieved from http://yosemite.epa.gov/ow/SReg.nsf/description/VSAT.

USEPA. (2015). *Water Quality Surveillance and Response System Primer*, 817-B-15-002.