Developing Integrated Water Quality Surveillance & Response System

Course No: C03-084
Credit: 3 PDH

Gilbert Gedeon, P.E.

Continuing Education and Development, Inc.

P: (877) 322-5800
info@cedengineering.com

This course was adapted from the U.S. Environmental Protection Agency, Publication No. EPA 817-B-17-001, "Designing Enhanced Security Monitoring For Water Quality Surveillance and Response Systems", which is in the public domain.

Table of Contents

List of Figures

List of Tables

Abbreviations

AWWA	American Water Works Association
CCTV	Closed-Circuit Television
CIF	Common Intermediate Format
DSL	Digital Subscriber Line
DVR	Digital Video Recorder
EPA	U.S. Environmental Protection Agency
ESM	Enhanced Security Monitoring
IP	Internet Protocol
IT	Information Technology
NVR	Network Video Recorder
O&M	Operation and Maintenance
POTS	Plain Old Telephone System
PTZ	Pan-Tilt-Zoom
RAID	Redundant Array of Inexpensive Disks
SCADA	Supervisory Control and Data Acquisition
SRS	Water Quality Surveillance and Response System
SVGA	Super Video Graphics Array
T1	T-Carrier 1

Section 1: Introduction

The U.S. Environmental Protection Agency (EPA) designed a ***Water Quality Surveillance and Response System***[1] (SRS) that employs multiple ***components*** to detect ***water quality incidents*** with potential public health and economic ***consequences***. **Figure 1-1** shows the components of an SRS grouped into two operational phases, surveillance and response. Procedures guide the systematic investigation of ***anomalies*** detected by the surveillance components in order to identify their cause. If distribution system contamination is detected, response plans guide actions intended to minimize consequences. An SRS can be implemented by drinking water utilities to improve their ability to detect and respond to undesirable water quality changes. EPA intends the design of an SRS to be flexible and adaptable based on a utility's goals and the resources available to support implementation and operation of the system.

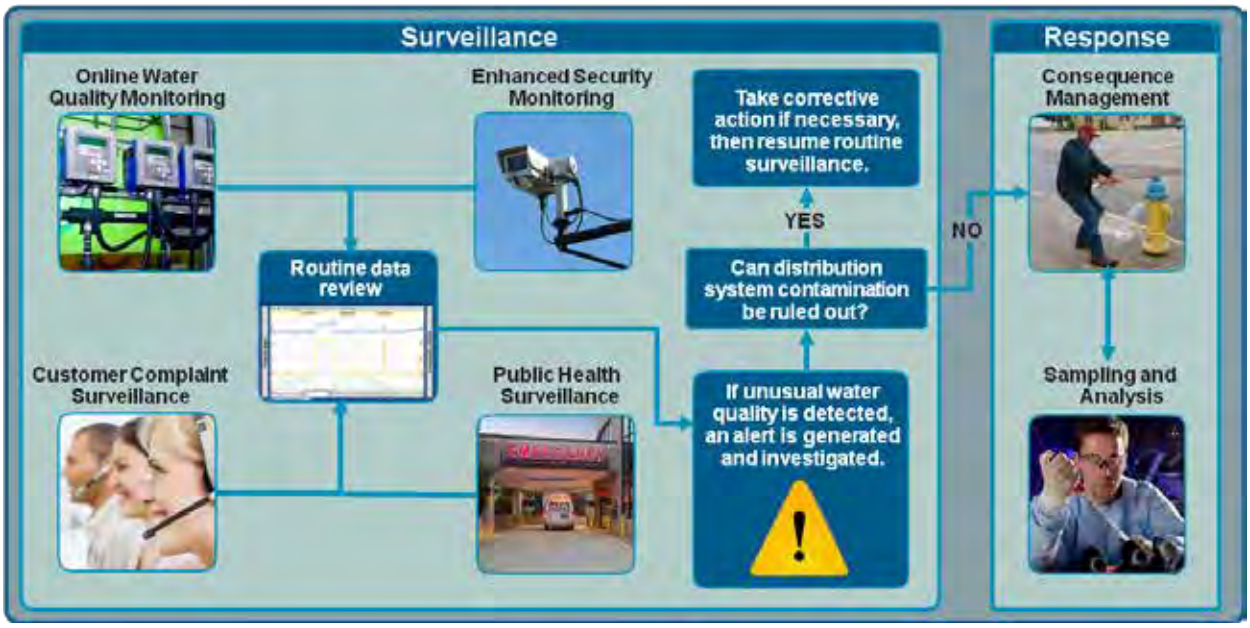


Figure 1-1. Surveillance and Response System Components

Enhanced Security Monitoring (ESM) is one of four surveillance components of an SRS. The purpose of this document is to provide guidance for designing the ESM component of an SRS. It is written for drinking water professionals responsible for coordinating with utility security personnel and local law enforcement to implement ESM.

In addition to this introductory section, the document is organized into the following major sections:

- **Section 2** provides a description of the ESM design elements that define the component. Section 2 also introduces the concepts of design goals and performance objectives and explains how they inform the design of ESM.
- **Section 3** provides guidance on selecting utility sites for ESM improvements. The section describes a qualitative method for assessing and selecting utility sites.
- **Section 4** provides guidance on selecting security equipment for ESM sites. The section describes different types of equipment and their design considerations.
- **Section 5** provides guidance on developing a communications system for transmitting data between ESM sites and a utility control center. The section provides an overview of the

[1] Words in bold italic font are terms defined in the Glossary at the end of this document.

evaluation process and criteria for technology selection and a summary of commonly available communications technologies.

- **Section 6** provides guidance on developing an information management system for displaying ESM alert information for utility security and operations personnel. The section describes design considerations and different types of hardware and software needed for an information management system.
- **Section 7** provides guidance on investigating ESM alerts. It describes attributes of an effective alert investigation procedure, explains the roles and responsibilities in an ESM alert investigation, describes tools to support the investigation, and provides guidance on investigating alerts in real-time.
- **Section 8** describes the process for developing a preliminary design for the ESM component of an SRS.
- **Resources** presents a comprehensive list of documents, tools, and other resources useful for ESM implementation. A summary and link to each resource is provided.
- **References** presents a comprehensive list of published literature cited within the document.
- **Glossary** presents definitions of terms used in this document, which are indicated by bold italic font at first use in the body of the document.

This document is written in a modular format in which the guidance provided on a specific topic is largely self-contained, allowing the reader to skip sections that may not be applicable to their approach to ESM, or that describe capabilities that have already been implemented. Furthermore, this document was written to provide a set of core guidance principles that are sufficient to design the ESM component, while pointing the reader to additional technical resources useful for a specific design task. The reader may benefit from locating and downloading technical resources of interest from the Resources section for ease of reference while reading this document.

Section 2: Overview of ESM Design

ESM utilizes ***hardening*** and ***intrusion detection equipment*** to delay and detect unauthorized entries into utility ***facilities*** or ***sites*** that could present an opportunity for contamination of ***distribution system water***. If a utility's all-hazard ***risk assessment***, using a tool such as *VSAT*, concludes that the risk of intentional contamination at utility facilities is a concern, implementation of ESM may be warranted. ESM also includes procedures and partnerships with law enforcement to respond to an unauthorized intrusion in sufficient time to prevent or mitigate the consequences of a ***contamination incident***. An overview of the ESM component of an SRS can be found in the *Enhanced Security Monitoring Primer*. ESM consists of the ***design elements*** described in **Table 2-1**.

Table 2-1. Design Elements for Enhanced Security Monitoring

Design Element	Description
Site Selection	The process used to prioritize utility facilities to receive ESM enhancements based on the risk of intentional contamination
Physical Security Equipment	Hardening and intrusion detection equipment that reduces the risk of intentional contamination by delaying and detecting unauthorized access
Communications	Wired or wireless technologies used to communicate data between remote ESM equipment and end-users
Information Management	Hardware and software that displays, manages, and stores ESM alert information
Alert Investigation Procedure	A documented procedure for the timely and systematic investigation of ESM alerts, with clearly defined roles and responsibilities for each step of the process

An effective ESM component should have capability for each of the design elements listed in Table 2-1. Sections 3 through 7 of this document define a ***target capability*** for each of these design elements, which if achieved, will result in a fully functional ESM component. However, the specific manner in which each design element is implemented can vary, and it is possible to improve ESM capabilities without fully achieving the target capability for each design element. Likewise, ESM capabilities can be implemented that exceed the target capability.

SECURITY PRACTICES REFERENCE

The AWWA G430 standard, "Security Practices for Operation and Management" describes critical security program requirements for a water utility and is a useful reference for ESM design (AWWA, 2014).

The decision regarding how to implement each of these design elements and build the ESM component is informed by ***design goals***, which are the specific benefits a utility hopes to realize through implementation of an SRS. **Table 2-2** presents examples of common design goals for ESM.

Table 2-2. Common SRS and ESM Design Goals

SRS Design Goal	ESM Design Goal
Detect water contamination incidents	Provide timely detection of intrusions at utility facilities that could lead to a possible water contamination incident.
Strengthen interagency relationships	Work collaboratively with local law enforcement to increase mutual awareness of each other's capabilities and prepare for responding to any emergency.
Enhance physical security	Verify the security of water distribution facilities and deter and detect acts of tampering, theft, and vandalism.

THEFT AND VANDALISM

An additional benefit of an ESM system is that it is an effective means of delaying, detecting, and responding to theft and vandalism incidents. For most utility sites, the risk of theft and vandalism is greater than that of intentional contamination. Furthermore, vandalism incidents can indirectly lead to contamination in cases where damage to equipment causes unintentional contamination.

Additional factors to consider when designing ESM are ***performance objectives***, which are metrics used to gauge how well the SRS or its components meet the established design goals. While specific performance objectives must be developed in the context of a utility's unique design goals, general performance objectives for an SRS are defined in the *Water Quality Surveillance and Response System Primer*. **Table 2-3** presents example performance objectives that are specific to the ESM component. The table also includes a recommended benchmark for each performance objective.

Table 2-3. Example ESM Performance Objectives

ESM Performance Objectives	Description	Recommended Benchmark
Timeliness of detection	The time between the start of an intrusion at an ESM facility and the time the intrusion is detected, which is dependent on the time required to transmit the security data via a communications system and for utility personnel to be notified of the alert via an information management system. This performance objective also considers the time necessary to investigate an ESM alert.	• Utility security personnel are notified less than five seconds after the intrusion occurs. • Preliminary conclusions from an ESM alert investigation are made within five minutes of alert notification.
Operational reliability	The percentage of time that ESM equipment (e.g., intrusion sensors, cameras, communications infrastructure, information management systems) is functioning properly. This performance objective also considers the availability of trained utility personnel to respond to intrusion alerts.	• 99.9% uptime. This amounts to eight to nine hours per year of downtime for planned outages to perform scheduled maintenance, and unplanned outages due to power failure, communications issues, equipment failure, etc.
Information reliability	The frequency of invalid alerts for intrusion detection equipment, which may be caused by environmental factors, communications outages or power irregularities. Information reliability is dependent on accuracy and sensitivity of the equipment.	• Interior intrusion sensors should have less than one invalid alert per sensor every three months. • Perimeter (i.e., outdoors) intrusion sensors should have less than one invalid alert per week per sensor.
Sustainability	The ability to maintain and operate ESM using available resources, which is dependent on the benefits derived from the component relative to the costs to maintain it.	• ESM should be fully funded for personnel training and periodic equipment replacement and maintenance per manufacturer's recommendations.

The design goals and performance objectives established by a utility provide the basis for designing an effective ESM component within project ***constraints***. The following sections present guidance on potential approaches to enhance capabilities for each of the ESM design elements described in Table 2-1. Additional background on the design elements, design goals, and performance objectives for ESM can be found in the *Enhanced Security Monitoring Primer*.

Section 3: Site Selection

The site selection process prioritizes utility facilities to receive ESM enhancements based on facility attributes that relate to the risk of intentional contamination by using a quantitative, objective approach based on Section 3 of *Framework for Comparing Alternatives Water Quality Surveillance and Response Systems*. The process consists of establishing an evaluation framework, scoring the facilities, determining the ESM improvements needed at each facility, and prioritizing the facilities by the cost of improvements divided by the facility evaluation score. The score for each facility represents its risk of intentional contamination, with a high score representing greater risk. Each step is described in detail below, including examples.

TARGET CAPABILITY

There is a prioritized list of utility facilities for ESM enhancements based on each facility's attributes that relate to the risk of intentional contamination.

3.1 Establishing the Evaluation Framework

The first step of establishing the framework is to develop a list of criteria based on facility attributes related to the risk of intentional contamination. Criteria should be non-site specific and apply to all facility types including pump stations, ***reservoirs***, and ***tanks***. Each criterion is assigned a weighting value to quantify its relative importance as follows:

- 4 = high importance
- 3 = moderately high importance
- 2 = moderately low importance
- 1 = low importance

Table 3-1 provides a list of example criteria and weighting values. The criteria in this table may be deleted, modified, consolidated, or supplemented with additional criteria. Furthermore, the weights and rationale can be modified as necessary.

Table 3-1: Example Evaluation Criteria and Weights

Evaluation Criterion	Weight	Rationale for Weight
1. Frequency of unauthorized intrusions	3	The frequency of unauthorized intrusion or tampering in the past does not correlate with intent to contaminate distribution system water, but highlights facilities that may be more prone to intrusion or tampering. The ability to detect and remotely assess intrusions at such facilities can be valuable. Thus, this example criterion was assigned a weight of 3 because of its moderately high importance.
2. Access to distribution system water	4	The more difficult it is to transport a contaminant to a facility and add it to distribution system water, the more likely it is that an intruder would be deterred from attempting to introduce a contaminant at that facility. For example, it would be difficult and deterring for an intruder to carry equipment and any significant quantity of contaminant to the top of an elevated tank that is accessible only by climbing. Thus, this example criterion was assigned a weight of 4 because of its high importance.

Evaluation Criterion	Weight	Rationale for Weight
3. Recognizability	1	The ease of recognizing a site as a water utility facility that provides access to distribution system water increases a target's attractiveness. For example, an elevated storage tank with the utility name on it is easily recognized, whereas a pump station constructed to look like a house is not so easily identified as a utility facility. However, intruders that are familiar with utility operations and processes may be able to identify any utility facility. Thus, this example criterion was assigned a weight of 1 because of its low importance.
4. Staffing	4	A staffed facility is much less likely to be intentionally contaminated than an unstaffed facility. Thus, this example criterion was assigned a weight of 4 because of its high importance.
5. Visibility	1	If a facility is visible to the public passing by or living near the facility, it is more likely that the public would witness an intrusion into the facility. While this might deter a vandal, it is unlikely that it would deter a motivated adversary intent on contaminating the drinking water supply. Thus, this example criterion was assigned a weight of 1 because of its low importance.
6. Existing security features – Detection	4	Intrusion detection equipment (e.g., door and motion sensors) is essential for detecting an intrusion incident so that response actions can be taken. Thus, this example criterion was assigned a weight of 4 because of its high importance.
7. Existing security features – Delay	2	Site hardening features such as heavy duty locks, metal doors, barred windows, ladder guards, vent enclosures, fencing, vehicle bollards, and other barriers are important for delaying intruders. However, at unstaffed facilities hardening features can be defeated with sufficient time. Thus, this example criterion was assigned a weight of 2 because of its moderately low importance.
8. Existing response capabilities	3	A rapid response of security personnel arriving on-site could prevent or limit the spread of contaminant injected by an intruder. Thus, this example criterion was assigned a weight of 3 because of its moderately high importance.
9. Ability to hydraulically isolate a facility	4	The ability to immediately hydraulically isolate a facility from the rest of the system through remote control valves, changing the hydraulic grade line in the vicinity of the facility, or via other operational changes, can prevent or limit the spread of contaminant injected by an intruder, typically before security personnel could arrive. Thus, this example criterion was assigned a weight of 4 because of its high importance.

Evaluation Criterion	Weight	Rationale for Weight
10. Facility flow	2	A facility with high flow generally serves a relatively large population, and thus a larger exposed population if that facility were contaminated. However, high flow also means a high dilution factor, and a significant amount of contaminant would need to be added to reach a harmful concentration. Thus, this example criterion was assigned a weight of 2 because of its moderately low importance due to these offsetting factors. Facility flows can be determined using operational data or a distribution system model, such as *EPANET*.
11. Critical service	2	This is a general assessment of the distribution system's ability to supply water to this facility's service area if the facility was isolated. Considerations include the number of customers that would be affected, the ability to maintain adequate system pressure, and the duration that service can be maintained with the facility off line. Maintaining service is important, but may not be as critical as minimizing contaminant spread. Thus, this example criterion was assigned a weight of 2 because of its moderately low importance.
12. Critical customers	4	Vulnerable populations such as children in schools, seniors in care facilities, and the immuno-compromised in healthcare facilities are considered critical because they may be impacted by lower concentrations of a contaminant compared to the general population. Thus, this example criterion was assigned a weight of 4 because of its high importance.

The last step of establishing the framework is to develop the scoring rationale for each criterion. Each criterion is scored on another four-point scale, and the characteristics for assigning a scoring value should be determined so that each facility can be objectively scored. A general four-point scale follows:

- 4 = high risk of intentional contamination
- 3 = moderate risk of intentional contamination
- 2 = low risk of intentional contamination
- 1 = minimal risk intentional contamination

Table 3-2 provides example scoring rationales for the criteria listed in Table 3-1.

Table 3-2: Example Scoring Rationale

Evaluation Criterion	Scoring Rationale
1. Frequency of unauthorized intrusions	4 = One or more times per year 3 = Once every 1 - 5 years 2 = Once every 6 – 10 years 1 = Less than once every 10 years
2. Access to distribution system water	4 = Easily accessible injection point (e.g., hatch in parking area) 3 = Need to enter a locked building to access distribution system water, and a pump is not needed to inject contaminant 2 = Need to enter a locked building to access distribution system water, and a pump is needed to inject contaminant 1 = Need to enter a locked building to access distribution system water, and a pump and climbing a ladder are needed to inject contaminant
3. Recognizability	4 = Easily recognized as a water treatment, pumping, or storage facility 3 = Not easily recognized as a water treatment, pumping, or storage facility, but does not appear to be a residence or office building either 2 = Appears to be a residence or office building but has some indications of a utility (e.g., signage, equipment) 1 = Indistinguishable from a residence or office building, or underground
4. Staffing	4 = Unstaffed, and visited less than once a day 3 = Unstaffed, and visited once or more a day 2 = Staffed during business hours (Monday-Friday, 8am-5pm) 1 = Staffed 24/7
5. Visibility	4 = No neighbors within 0.25 miles or more 3 = In a lightly populated area with few passersby 2 = In a moderately populated area with occasional passersby 1 = In a heavily populated area with many passersby
6. Existing security features – Detection[1]	4 = No intrusion detection 3 = Minimal intrusion detection (e.g., sensor on doors only, no form of back up communications) 2 = Comprehensive intrusion detection (e.g., sensors on doors and windows, glass break and motion sensors, redundant communications), but no video monitoring 1 = Comprehensive intrusion detection and video monitoring
7. Existing security features – Delay[1]	4 = No hardening 3 = Standard duty locks and barriers 2 = Mix of standard duty and heavy duty locks and barriers 1 = Heavy duty locks and barriers on all access points
8. Existing response capabilities	4 = Security staff would arrive on-site > 30 minutes after a detected intrusion 3 = Security staff would arrive on-site 10-30 minutes after a detected intrusion 2 = Security staff would arrive on-site 5-10 minutes after a detected intrusion 1 = Security staff would arrive on-site <5 minutes after a detected intrusion

Evaluation Criterion	Scoring Rationale
9. Ability to hydraulically isolate a facility	4 = Cannot isolate the facility 3 = Can isolate facility. It takes >15 minutes for valves to close or pumps to get up to speed or shut down 2 = Can isolate facility. It takes 5-15 minutes for valves to close or pumps to get up to speed or shut down 1 = Can isolate facility. It takes 5 minutes or less for valves to close or pumps to get up to speed or shut down
10. Facility flow[2]	4 = 75% to 100% of the utility's average daily flow 3 = 50 to 75% of the utility's average daily flow 2 = 25 to 50% of the utility's average daily flow 1 = Less than 25% of utility's average daily flow
11. Critical service	4 = Impossible to isolate facility without significant impacts to customers 3 = Limited ability to keep facility isolated (e.g., less than 12 hours) without significant impacts to customers 2 = Some impact on customers in surrounding areas, such as lower pressure 1 = Isolation has no impact on customers over an extended time period (e.g., more than 12 hours)
12. Critical customers[2]	4 = Relative to other utility facilities, this facility serves the most hospitals, schools, senior centers, and residences 3= Facility serves fewer hospitals, schools, senior centers, and residences 2= Facility serves industrial clients and residential customers without no hospitals, schools, or senior centers 1 = Facility serves primarily industrial customers (i.e., minimal residential and commercial customers) that don't make food or beverage products

Notes:
1. See the path analysis approach described in Appendix A for a more detailed analysis of the detection and delay criterion.
2. A hydraulic model can be used to identify facility flow and critical customers that are served by a specific utility facility.

3.2 Scoring the Facilities

The method used to score the facilities will depend on the amount of resources that the utility has to dedicate to this task. On-site assessments are preferred to ensure that actual site conditions are reflected in the facility scores. However, if resources are limited, facility scores may be informed by recorded drawings, recent reports, and ***vulnerability assessments***. For five example utility facilities, **Table 3-3** provides the characteristics related to each criterion and the associated scores for each facility using the evaluation framework described in Tables 3-1 and 3-2.

Table 3-3. Characteristics of Each Facility[1,2]

Evaluation Criterion	Pump Station K1	Elevated Tank A	Ground Tank E	Aboveground Reservoir K	Underground Reservoir S
1. Frequency of unauthorized intrusions	1 per year (4)	1 per 8 years (2)	1 per 4 years (3)	1 per 8 years (2)	1 per 11 years (1)
2. Access to distribution system water	Need to enter a locked building to access distribution water; a pump is required (2)	Need to enter a locked building to access distribution water; a pump is required (2)	Need to enter a locked building to access distribution water; a pump is required (2)	Need to enter a locked building to access distribution water; a pump and climbing a ladder are required (1)	Easily accessible injection point (4)
3. Recognizability	Highly recognizable (4)	Highly recognizable (4)	Highly recognizable (4)	Highly recognizable (4)	Not a recognizable reservoir, but has some signage (2)
4. Staffing	Unstaffed, but visited at least daily by utility personnel (3)	Unstaffed, but visited weekly (4)	Unstaffed, but visited weekly (4)	Unstaffed, but visited weekly (4)	Unstaffed, but visited weekly (4)
5. Visibility	In a populated area near busy road (1)	In a moderately populated area (2)	In a moderately populated area (2)	Near a busy road (1)	In a highly visible park/ residential area (1)
6. Existing security features – Detection	Sensors on all doors, but none on windows or hatches (3)	Sensors on the only access door (facility does not have windows) (2)	Sensors on all doors and hatches (facility does not have windows) (2)	None (4)	None (4)
7. Existing security features – Delay	Standard duty doors and locks; minimal protection on windows, hatches, and vents (3)	Heavy duty doors and locks; no windows or vents (1)	Standard duty doors and locks; minimal protection on hatches and vents; no windows (3)	No protection on hatches and vents; no doors or windows (4)	No protection on hatches and vents; no doors or windows (4)
8. Existing response capability	Average police response of 10 minutes (2)	Average police response of 10 minutes (2)	Average police response of 10 minutes (2)	Average police response of 10 minutes (2)	Average police response of 10 minutes (2)
9. Ability to hydraulically isolate a facility	Pumps and valves remotely controlled and valves close in 5 minutes (1)	Valves remotely controlled and close in 5 minutes (1)	Valves remotely controlled and close in 5 minutes (1)	Valves remotely controlled and close in 10 minutes (2)	Valves remotely controlled and close in 5 minutes (1)
10. Facility flow	Handles >75% of the utility's average daily flow (4)	Handles <25% of the utility's average daily flow (1)	Handles between 50% and 75% of the utility's average daily flow (3)	Handles between 25% and 50% of the utility's average daily flow (2)	Handles between 25% and 50% of the utility's average daily flow (2)

Evaluation Criterion	Pump Station K1	Elevated Tank A	Ground Tank E	Aboveground Reservoir K	Underground Reservoir S
11. Critical service	If the facility is isolated, its service area cannot be fed by other facilities without significant impacts to customers. (4)	If the facility is isolated, its service area can be fed by other facilities. (1)	If the facility is isolated, its service area can be fed by other facilities until storage runs out in less than 12 hours. (3)	If the facility is isolated, its service area can be fed by other facilities. (1)	If the facility is isolated, its service area can be fed by other facilities. (1)
12. Critical customers	Has a hospital in its service area (3)	Has a hospital, nursing home, and school in its service area (4)	Has a large elementary school in its service area (3)	Mainly non-food industrial customers (1)	Has a small elementary school in its service area (2)

Notes:
1. The score assigned to each criterion for each facility is shown in parenthesis following the description.
2. The score for each criterion is based on the site characteristics with respect to the scoring rationale shown in Table 3-2. For example, Pump Station K1 has experienced an unauthorized intrusion average of once per year, so it receives a score of 4, which corresponds to a frequency range of one or more times per year.

Next, the weighting factor for each criterion from Table 3-1 is applied to the corresponding value in Table 3-3 to produce the weighted scores for each example facility, as shown in **Table 3-4**.

Table 3-4. Weighted Scoring of Each Facility[1]

Evaluation Criterion	Weight	Pump Station K1	Elevated Tank A	Ground Tank E	Above-ground Reservoir K	Under-ground Reservoir S
1. Unauthorized intrusions	3	12	6	9	6	3
2. Access to distribution system water	4	8	8	8	4	16
3. Recognizability	1	4	4	4	4	2
4. Staffing	4	12	16	16	16	16
5. Visibility	1	1	2	2	1	1
6. Existing security features – Detection	4	12	8	8	16	16
7. Existing security features – Delay	2	6	2	6	8	8
8. Existing response capabilities	3	6	6	6	6	6
9. Ability to hydraulically isolate a facility	4	4	4	4	8	4
10. Facility flow	2	8	2	6	4	4
11. Critical service	2	8	2	6	6	2
12. Critical customers	4	12	16	12	4	8
Totals	---	93	76	87	83	86

Notes:
1. The weighted score for each criterion at the example facilities is the weight multiplied by its score from Table 3-3. For example, the weighted score for the Pump Station K1 unauthorized intrusions criterion is the weight (3) multiplied by the score from Table 3-3 (4), which equals 12.

3.3 Determining the Cost of ESM Improvements

The ESM improvements and costs required at each facility should be determined. Generally, ESM improvements consist of upgrades and enhancements to a facility's existing delay and detection security features to meet the physical security equipment target capability stated in Section 4. Consult Section 4.1 – Hardening and Section 4.2 – Intrusion Detection Equipment, herein, for guidance on these topics. The security enhancements and their associated costs for the example facilities listed in Table 3-4 are shown in **Table 3-5**.

Table 3-5. Cost of Enhancements at Each Facility

Facility	Enhancements	Cost of ESM Enhancements
Pump Station K1	• Contact alarms on all doors to the pump area • Contact alarm on stand pipe access hatch • Area motion detectors around the pump room • Heavy duty doors • Hardened windows • Video monitoring system proposed due to the relatively high frequency of intrusions at this facility.	$11,000
Elevated Tank A	• Ladder intrusion sensor	$1,200
Ground Tank E	• Ladder intrusion sensor	$1,200
Aboveground Reservoir K	• Hardened steel cover with access hatch and sensor to protect the reservoir vent	$3,500
Underground Reservoir S	• Hardened steel covers with access hatches and sensors to protect the reservoir vent and overflow pipes	$7,000

3.4 Prioritizing the Facilities

The facilities can be prioritized based on their cost per weighted score values, after enhancements and costs are determined. Facilities with the lowest cost per weighted score value should be given top priority because they can be protected at a relatively low cost as normalized by their relative risk of contamination. **Table 3-6** provides cost per weighted score values and relative rankings such that a ranking of "1" represents the highest priority.

Table 3-6. Cost and Weighted Score of Each Facility

Facility	Weighted Score	Cost of ESM Enhancements	Cost / Weighted Score	Priority Ranking[1]
Ground Tank E	87	$1,200	$13.79	1
Elevated Tank A	76	$1,200	$15.79	2
Aboveground Reservoir K	83	$3,500	$42.17	3
Underground Reservoir S	86	$7,000	$81.40	4
Pump Station K1	93	$11,000	$118.28	5

Notes:
1. The highest ranked facility (rank = 1) is the facility with the lowest cost per weighted score.

Plotting the cost of enhancements against the weighted score is useful for visualizing and comparing alternatives. For a graph with weighted score as the x-axis and the cost of enhancements as the y-axis, the facilities that fall in the bottom right of the graph represent the facilities that should be given highest

priority because they have a relatively high risk of intentional contamination and a relatively low cost. Facilities that are in the upper left of the graph should have the lowest priority because they have a relatively low risk of intentional contamination and a relatively high cost. **Figure 3-1** shows the cost of enhancements and weighted score for the example facilities, using the data from Table 3-6.

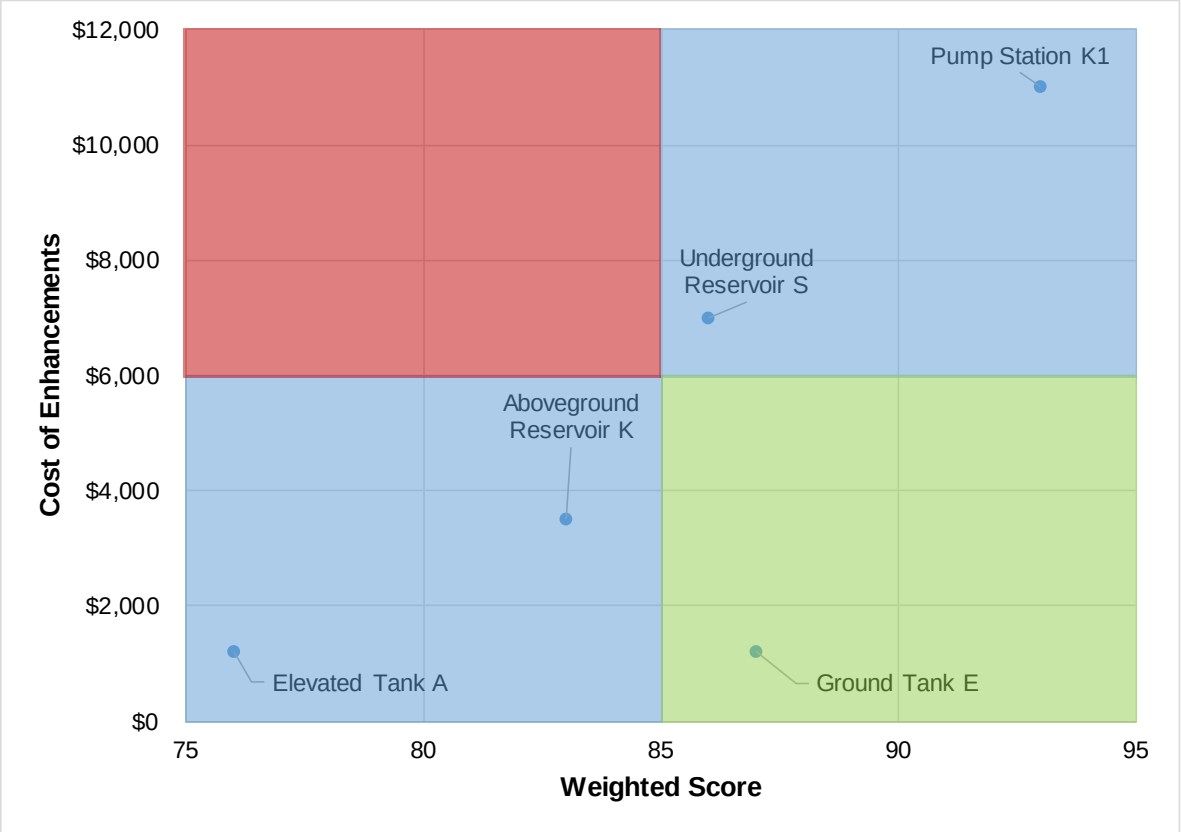


Figure 3-1. Cost and Risk Scores for the Example Facilities

Figure 3-1 shows that facilities with higher weighted scores (i.e., those that had a higher risk of intentional contamination) generally had costlier enhancements. The exception to this observation is Ground Tank E, which had a relatively high weighted score but a low cost of enhancement. Thus Ground Tank E is the highest priority for receiving security enhancements. In general, the cost per weighted score should be used to prioritize facilities, and professional judgment should be applied to account for considerations beyond intentional contamination (e.g., vandalism and theft).

Section 4: Physical Security Equipment

A utility facility can be equipped with physical security enhancements, such as hardening and intrusion detection equipment, to delay and detect unauthorized entry, thus reducing the risk of intentional contamination. Hardening includes physical barriers and heavy duty access ***hardware*** to slow the progress of an intruder. Intrusion detection equipment generates ***alerts*** if unauthorized access to the facility is detected, enabling utility personnel to initiate ***alert investigation procedures*** in a timely manner.

TARGET CAPABILITY

All access points to distribution system water at each utility facility are hardened and covered by intrusion detection equipment to reduce the risk of intentional contamination.

Layers of security with hardening and intrusion detection are recommended to protect distribution system facilities. Hardening delays the intruder and intrusion sensors alert utility personnel of the intrusion. For example, a small pump station without interior rooms should include exterior hardening consisting of perimeter fencing and metal exterior doors, and intrusion detection equipment consisting of door and motion sensors. A facility with an interior pump room should also include inner hardening and detection to protect and monitor the pump room (i.e., the pump room should be equipped with metal doors, heavy duty locks, and a door sensor). As an advanced feature, exterior detection equipment that senses when someone has climbed or breached the perimeter fence may also be considered for earlier detection of a potential intrusion.

Other advanced detection systems to supplement hardening and intrusion sensing may also be considered. Incident-based video monitoring or a ***video analytics*** system allows staff at a utility ***control center*** to visually assess the nature of an intrusion and determine whether contamination is a ***possible*** intent of the intrusion.

Table 4-1 describes enhancements to consider at common types of utility facilities.

Table 4-1. Example ESM Enhancements by Utility Facility Type

Facility Type	Typical Enhancements Recommended for ESM
Reservoirs and Ground Level Storage Tanks	• Vented enclosure over vents to prevent addition of contaminants • Barriers or vented enclosures for overflow pipes that are vulnerable to contamination
Elevated Storage Tanks	• Motion detectors or infrared cameras to detect intruders climbing the ladder • Ladder hatches with contact switches to monitor access points to ladders
All Facility Types (including pump stations and treatment plants)	• Contact switches for doors, hatches, and windows to detect intruders entering areas that provide access to water (e.g., pumps, pipes, vaults, and valves) • Hardened hatches and covers where sensors cannot be feasibly added • Secondary cover over hatches • Interior motion sensors to detect intruders entering through windows and vents in areas that provide access to water pumps and pipes • High-mast lighting • Cameras that are activated by motion detectors or contact switches • Lighting enhancements for camera systems where needed • Video and communication interfaces • Card access reader

This section describes considerations and details for selecting ESM counter measures:

- Subsection 4.1 provides guidance on hardening
- Subsection 4.2 provides guidance on intrusion detection equipment
- Subsection 4.3 provides guidance on video monitoring
- Subsection 4.4 provides guidance on video analytics

It should also be noted that non-security-related process improvements and engineering can reduce contamination risk by lowering the potential for public health consequences (e.g., installing remote control shutoffs at tanks and reservoirs, building redundancy in the supply system to allow for isolation of a facility during a suspected contamination incident).

4.1 Hardening

Hardening consists of physical barriers that delay an intruder from reaching their objective. Examples include heavy-duty doors and locks, site fencing, barbed wire, and vehicle barricades such as bollards and airport cabling. Glass windows can be barred or replaced with shatter-proof or bullet-proof glass or brick to harden a facility. Consult *Guidelines for the Physical Security of Water Utilities* for guidance on hardening.

4.2 Intrusion Detection Equipment

The following are established and emerging intrusion detection technologies. Consult *Guidelines for the Physical Security of Water Utilities* (Sections 2.0 through 7.0) for details on specific security technologies and methods that apply to the different types of utility facilities.

- **Door or Hatch Sensors**: These sensors use a magnetic proximity or mechanical limit switch to detect when a door, hatch, or rolling vehicle gate is opened. Magnetic proximity switches are less expensive than mechanical limit switches. Magnetic and mechanical sensors are less expensive than motion sensors.
- **Motion Sensors**: These sensors use ultrasonic, microwave (sometimes referred to as radar), and passive infrared technologies to detect motion in the area monitored by the sensor. Indoor motion sensors are more common than exterior motion sensors. However, exterior motion sensors are gaining acceptance, including ground-based radar – an emerging technology. Interior motion sensors are more expensive than door sensors, and exterior motion sensors are more expensive than interior motion sensors.
- **Glass Break Sensors**: These sensors utilize acoustic or shock sensing technology to detect the sound or shockwave from breaking glass, respectively. The cost of glass break sensors is comparable to that of door sensors.
- **Vibration Sensors**: These sensors are attached to the surface of an object and are tuned to sense the low frequency energy typically generated by a physical intrusion attempt such as sawing, drilling, ramming, or glass breaking. The cost of vibration sensors is comparable to that of motion sensors.
- **Perimeter Sensors**: Common perimeter systems include fence climbing and buried line sensors to detect exterior intrusions. These advanced applications are implemented as an additional layer of security to supplement facility hardening and intrusion detection. The cost of perimeter sensors is more than that of door sensors and will vary with the length of perimeter and type of sensor.

The following attributes and benchmarks should be considered when selecting enhancements. Details on design considerations can be found in *Guidelines for the Physical Security of Water Utilities*.

- **Detection Capability**: Motion sensors should be capable of detecting an individual (weighing 75 pounds or more) crossing the detection zone at speeds between 0.5 and 15 feet per second, or cutting or climbing a fence, if applicable. Door sensors should be capable of detecting when a door is opened enough for a person to enter. Vibration sensors should be capable of detecting sawing, drilling, ramming, glass breaking, and similar attempts at physical intrusion.
- **Minimum Invalid Alerts**: Interior intrusion sensors should have less than one ***invalid alert*** per interior sensor every three months, and perimeter (i.e., exterior) intrusion sensors should have less than one invalid alert per week per exterior sensor.
- **Detection Probability**: There should be at least a 95 percent confidence level that the sensor will detect an intrusion (i.e., of 100 actual intrusions, the sensor should detect at least 95).
- **Coverage**: Intrusion sensors should cover all points of access to a facility.
- **Environment**: Intrusion sensors should be suitable for the location, climate, and ambient temperature conditions where they are installed.
- **Backup Power**: A backup power system should provide at least four hours of sensor operation during a power failure. Powering a sensor from a standby generator or a 24-hour backup power system is also an option but may cost more than a 4-hour backup system.
- **Reliability**: All sensors should be included in the utility's preventive maintenance program to minimize ***sensor malfunctions*** and ensure that manufacturer-recommended routine maintenance for the sensors occurs.
- **Sustainability**: Operating and maintenance costs should be included in annual operating budgets. Spare parts may be warehoused to allow for immediate replacement, especially for devices with a long lead time from the manufacturer. The cost of replacement and the expected design life should be considered in the capital replacement budget.

4.3 Video Monitoring

If a utility wants to implement enhancements beyond the target capability of hardening and intrusion detection, incident-based video monitoring could be considered. An incident-based video monitoring system records continuous video data on a local storage device, receives intrusion alerts from sensors connected to the system or video analytics, and only transmits video clips of suspected intrusions to a utility control center. Incident-based video monitoring systems also allow the user to view live video imagery when needed (e.g., during an active investigation). An incident-based system is preferred over a closed-circuit television (CCTV) system because CCTV requires staff to continuously monitor multiple video feeds for suspicious behavior, and intrusions could be overlooked. Furthermore, CCTV requires that video data be transmitted continuously over the communications system, which generates a significant amount of data and usually requires hardwired communications infrastructure. An incident-based video system allows utility personnel to focus their efforts on detected incidents and requires transmitting less data over the communications system, allowing for wireless options. A typical video monitoring system consists of cameras, storage devices, and hardware as described below.

For more information on video monitoring systems, consult *Guidelines for the Physical Security of Water Utilities* (Section 11 of Appendix A).

4.3.1 Cameras

Cameras convert imagery into electronic signals via digital or analog means. Key considerations for selecting cameras including the following:

- **Digital vs. Analog:** Video cameras transmit imagery in a digital format using the Internet Protocol (IP) or in an analog format. Most new video systems are IP, although analog systems are

still available and often found in legacy applications. Compared to analog video, IP video typically has more options for storage, retrieval, and data compression. However, analog video may be preferred if the utility has an existing analog system that is working well and does not require functional upgrades. Analog-to-IP converters are available for video systems that have both types of cameras. Thus, the selection of analog vs. digital cameras depends on factors such as existing site conditions, ***information management*** requirements, and cabling needs, which are described below.

- **Connectivity:** Analog cameras use coaxial cabling and digital cameras use Ethernet cabling or a wireless connection. Coaxial cable can transmit video signals up to 1,500 feet, and copper Ethernet cabling requires a repeater for runs over 300 feet, although fiber optic Ethernet cabling may be used for Ethernet applications for distances up to two kilometers at 100 megabit per second or one kilometer at one gigabit per second. Copper Ethernet cabling is typically less expensive and easier to install than analog video cabling and fiber optic Ethernet cabling. Furthermore, power over Ethernet is an option for some IP cameras with copper Ethernet cabling, eliminating the need for separate power cabling. Wi-Fi is commonly used for wireless connections to digital cameras and has a transmission distance of 300 feet to 2,500 feet, depending on the Wi-Fi version used. See Section 5 for more information on wireless communications.
- **Fixed vs. Pan-Tilt-Zoom (PTZ)**: A PTZ camera housing includes a motorized mechanism that allows the lens to pan horizontally and vertically and zoom in or out, while a fixed camera includes a stationary lens. Fixed cameras are recommended for monitoring points of entry (e.g., doorways), and PTZ cameras are useful during an active investigation for determining intruder intent or the cause of an invalid alert. This selection depends on factors such as desired field of view, intended application, replacement frequency, and cost. PTZ cameras are more expensive than fixed cameras, and PTZ cameras have internal mechanisms that are subject to wear and have been found to have a ***useful life*** of approximately five years. However, fixed cameras, which have few moving parts, have been found to have a useful life of eight to 10 years.
- **Lighting**: Depending on camera capabilities, supplemental lighting may be required to allow the cameras to produce imagery with adequate resolution under low-light conditions. A utility should consider the cost of standard-grade cameras with supplemental lighting versus the cost of low-light cameras that do not require additional lighting. Infrared cameras may also be considered. For security applications where illumination only occurs when an intrusion is detected, instant-on lighting technologies such as light emitting diode, fluorescent, incandescent, or halogen, are required. Light emitting diode and fluorescent are typically preferred over the latter two because of higher energy efficiency. Technologies that have a warm-up period before illuminating, such as metal halide and sodium vapor, are only suitable for applications where they are energized continuously from dusk to dawn.
- **Resolution**: Typical camera resolutions include Common Intermediate Format (CIF), which is 352 x 288 pixels, Super Video Graphics Array (SVGA), which is 800 x 600 pixels, and high definition, which is 1920 x 1080 pixels.

CAMERA RESOLUTION GUIDELINES

Design guidelines for determining the appropriate resolution for a video application are as follows:

The object of interest should be at least the following number of pixels tall in the camera view:

- License Plate Recognition: A plate should be at least 24 pixels.
- Intrusion Detection: A person should be at least 48 pixels.
- Facial Recognition: A person should be at least 240 pixels.

Another design guideline for facial recognition is that the resolution should be at least 80 pixels per foot of scene width (e.g., a view of a ten-foot wide area should have a camera resolution of at least 800 pixels wide). For general recognition, a resolution of 30 pixels per foot of scene width should be adequate.

4.3.2 Video Storage

Video monitoring systems typically include equipment for short-term and archival storage of video data. ESM cameras are usually connected to a digital video recorder (DVR) or network video recorder (NVR) for temporary storage of continuous video from all cameras at the facility. Video data from incidents are transmitted to a utility control center and archived on a server or other storage device. Personnel at a utility control center also have the option of retrieving high resolution historical video from the NVR on an as-needed basis (i.e., while gathering post-incident evidence). This arrangement minimizes the transmission and storage of uneventful data. Details on video recorders and other storage options are provided below.

- **Video Recorders:** DVRs and NVRs are usually located in the same facility as their connected cameras and continuously save the high resolution video from all connected cameras. This configuration, also referred to as edge storage, minimizes the amount of video data transmitted from ESM sites to a utility control center. DVRs are connected to analog cameras and convert the incoming video signals into a digital format that is stored on their hard drive. NVRs are connected to the IP camera network and store the digital video data generated by the cameras. DVRs and NVRs are configured to save video data for only a preset duration to conserve storage space, and the *Guidelines for the Physical Security of Water Utilities* recommends a minimum of 30 days of continuous storage at five frames per second. However, many technologies are capable of 30 days of continuous storage at 30 frames per second. For publicly owned utilities, local ordinances may have storage duration requirements.
- **Other storage options:** At a utility control center, video data can be archived on servers or standalone storage devices such as a Redundant Array of Inexpensive Disks (RAID) device. Such a device includes multiple hard drives with redundant content on each drive such that the data on a failed drive can be recovered using data from the remaining drives. Other forms of network-based storage (e.g., storage area networks) or a cloud-based data storage service (via the Internet) are also options. A means of writing video data to optical media such as DVD or Blu-Ray may also be considered for archiving video of notable incidents for use by law enforcement or for training purposes.

4.3.3 Hardware

The video monitoring system consists of workstations and servers at a utility control center. Workstations enable utility personnel to view incident videos, monitor multiple facilities, and control PTZ cameras. Servers support the workstation functions, interface with remote NVRs and DVRs, and manage the storage of video data. Furthermore, workstations and servers should be equipped with adequate memory and processor speed to manage the high volume of data produced by the video cameras, preferably at a frame rate of 30 frames per second. However, a lesser frame rate may be used to reduce the amount of data transmitted to a utility control center and managed by the video monitoring system.

4.4 Video Analytics

Video analytic systems use algorithms that continuously analyze video images to identify an anomalous object, classify its size, characterize its behavior, and determine its location, which results in accurately detecting intrusions and greatly reducing the frequency of invalid alerts. Analytics systems can determine whether the object is a small animal, large animal, suitcase, package, human, car, truck, or railcar. Furthermore, analytics systems can identify behaviors such as a loiterer and a car that has illicitly entered a facility by closely following a utility vehicle (i.e., piggybacking). For example, a remote utility facility near a wooded area may have wildlife frequently approach its perimeter and cause invalid alerts from traditional intrusion sensors. However, a video analytics system would be able to distinguish between humans and animals to avoid this type of invalid alert. Other benefits of a video analytics system are that it eliminates the need for utility personnel to continuously monitor video for suspicious activity, and its location data can be used to point a camera at the intruder for assessment by utility personnel (Mix, Lynn, Gist, & Lai, 2017). An overview of three features of video analytic systems, "analytics at the edge," "behavioral analysis," and "meta tags", are provided below (Mix, Pickard, Gist, & Lai, 2011).

- **Analytics at the Edge**: This is a video analytics method whereby camera units provide video analytic detection within the camera unit, rather than at a separate computer.
- **Behavioral Analysis**: This video analytics method memorizes and learns typical environmental patterns like shadows, rain, snow, sunsets, etc. These systems do not need significant programming, but instead learn over time what is normal activity. Behavioral analysis ***software*** translates video feeds into data read by a computer to adapt and learn.
- **Meta Tags**: Meta tags are small pieces of data that are embedded and transmitted with video to include information about the scene such as the size, behavior, and location of the object.

When evaluating video analytics systems, scene characteristics such as water, shadows, shades, foliage, cars, people, and amount of movement can be critical to the overall effectiveness. Thus, a pilot-scale implementation of technologies from multiple vendors to evaluate their suitability for a utility's application is recommended. Utilities with similar systems could also be consulted. For video analytics systems, invalid alerts can be minimized by involving the video analytics vendor during the design and startup phases and by performing a diligent ***commissioning*** effort, as described in Section 4.5. Periodic recommissioning is also recommended to accommodate changes in background scenery and ensure that camera positions have not drifted.

LESSONS LEARNED IN VIDEO ANALYTICS

Advice from a utility that implemented a video analytics system:

- Be wary of areas frequented by people and other moving objects: A video camera viewing an exterior fence perimeter also viewed an adjacent jogging path. This situation had the undesired effect of causing numerous invalid alerts, wasting operator time to review the alerts, and reducing confidence in the ESM system. In retrospect, this camera view should not have included the jogging path. An alternate means of detection should be considered for areas with joggers, vehicles, moving foliage, blowing debris, etc.
- Consider allowing the video analytic vendor to access the system remotely: The video analytic vendor requested electronic access to the video analytic system to continue monitoring and tuning the system based on the type and quantity of alerts coming in. However, this electronic access request was denied due to security concerns with allowing an outside entity access to the security network. Determining an appropriate means to allow such access, while still complying with the utility's cybersecurity policies, would have allowed the vendor to adjust system settings and address invalid alerts in a timelier fashion.

4.5 Commissioning

A critical factor for successfully implementing ESM systems, especially video analytics systems and intrusion sensors, is the commissioning effort. A diligent commissioning effort is the most effective way to minimize invalid alerts. Commissioning is also essential for system sustainability and for staff and management to have confidence in the system. Confidence that the alerts received are ***valid alerts*** will ensure proper and timely investigations. For guidance on commissioning an ESM system, consult *Commissioning Security Equipment*.

Section 5: Communications

A typical communications system includes a ***wired*** or ***wireless technology*** to transmit and receive data between ESM equipment and end-users that view the data on designated devices, such as a workstation in a utility control center. Often utilities use more than one communications technology due to the resources and limitations at specific ***monitoring locations***. For example, a utility-owned wired network might be used to transmit data from ESM equipment located at larger utility facilities, while a third-party provided wireless network may be used to transmit data from locations without existing communications infrastructure.

TARGET CAPABILITY

There is a communications network to transmit data from ESM equipment installed at remote utility facilities to a utility control center.

A communications system can serve multiple SRS components, which can result in cost savings. However, the feasibility of a shared system will depend on each component's equipment locations and data transmission requirements. If it is impractical or cost-prohibitive to implement a single communications system that serves multiple components, separate communications systems – each dedicated to a component – can be implemented. Coordination with other components is strongly recommended to ensure that the communications system meets the requirements for each component and that overlapping effort and conflicts are minimized.

The overall process of evaluating communications alternatives consists of establishing evaluation criteria, identifying the available communications technologies for SRS sites, and selecting a technology (or technologies). After selecting a technology, the communications system can be designed and implemented. **Figure 5-1** provides an overview of this process.

Consult your ***Information Technology (IT)*** department early in the process when considering communications options. Their input can be useful when developing evaluation criteria and identifying available technologies, including existing utility communications systems that could be leveraged. They may also have lessons learned to share about previous experiences with communications technologies, which could be valuable during the selection process. A utility might also engage their ***Supervisory Control and Data Acquisition (SCADA)*** department when evaluating communications technologies.

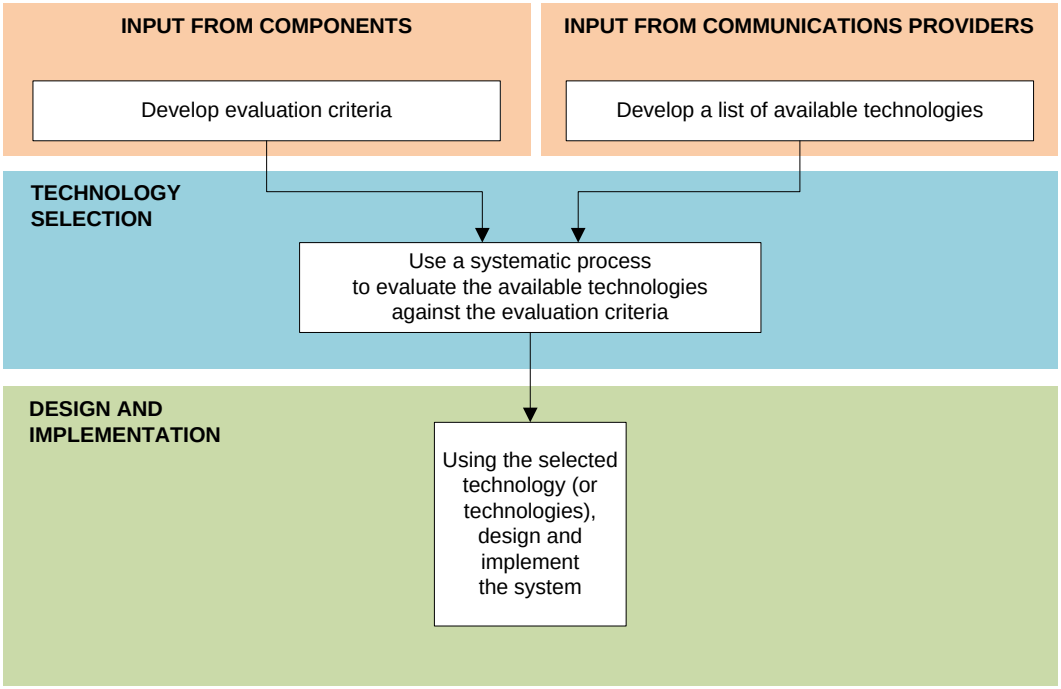


Figure 5-1. SRS Communications System Development Process

Consult the *Guidance for Designing Communications Systems* for more information on the SRS communications selection process and detailed descriptions of common communications technologies, which are summarized in **Table 5-1**. An overview of commonly used criteria for selecting communications technologies, which are also the column headings in Table 5-1, are shown below. Table 5-1 rates each technology as strong, moderate, or weak for each criterion, and the strong rating for each criterion is defined in its respective overview below:

- **Extent of use**: A measure of acceptance by utilities that reflects the degree of confidence that the water sector has in the technology. A strong rating for this criterion means widely accepted.
- **Data transmission rate**: The maximum, instantaneous rate of data that a technology can transmit. This metric is also referred to as bandwidth. A strong rating for this criterion means fast. Less than one megabit per second is generally considered slow. For a typical remote utility site with only a few standard definition cameras, one and 10 megabits per second would be considered moderate and fast, respectively.
- **Security**: For communications technologies, this refers to cybersecurity, specifically, a technology's susceptibility to malicious denial-of-service attacks, unauthorized access, and manipulation. A strong rating for this criterion means very secure. Technologies not exposed to the Internet and that provide data encryption are generally regarded as being very secure.
- **Reliability**: A technology's ability to continuously transmit data that is complete, uncorrupted, and in the order it was sent. A strong rating for this criterion means highly reliable. A 99.9% uptime is a typical guideline for security equipment for high reliability. This equates to about eight to nine hours of downtime per year to account for power and communications outages, planned maintenance, and breakage.
- **Distance**: The maximum extent that a technology can reliably transmit a packet of data without the aid of a signal repeater or amplifier, which applies to wireless technologies. A strong rating for this criterion means capable of transmitting long distances. The general guidelines for short, medium, and long ranges are less than 1,000 feet, 1,000 feet to a mile, and more than a mile, respectively.

- **Installation cost**: ***Implementation costs*** for a communication technology. A strong rating for this criterion means low cost. Installation costs will vary based on existing infrastructure at the facility, requirements by ***communications providers***, and hardware costs. Generally, the technologies that require minimal building wiring modifications have the lowest installation costs.
- **Provider fees**: The monthly cost for third party-provided communications systems. A strong rating for this criterion means low fees. Utility-owned communications systems will have strong ratings for this criterion because they do not incur provider fees.
- **Maintenance**: The cost and level of effort required to sustain the operation of a communications system. A strong rating for this criterion means low maintenance. Third-party provided communications systems will have strong ratings for this criterion because the provider is responsible for most system maintenance, so maintenance by utility personnel should be minimal.

To transmit and receive data, it is essential to include objective evaluation criteria (e.g., data transmission rate, distance) that measure how well the respective technology satisfies ***technical requirements***, which are system attributes and design features that are not readily apparent to the end user. A communications system's technical requirements should be developed to support the requirements of the information management system, which are discussed in Section 6.

Table 5-1. Commonly Available Communications Technologies

	Communication Technology	Extent of Use	Data Tr. Rate	Security	Reliability	Distance	Installation Cost	Provider Fees	Maintenance
Wired	**Plain Old Telephone System (POTS):** POTS is the basic form of wired voice communication. A conventional modem can be used over POTS for data communication, but is limited to 56 kilobits per second without data compression.	○	○	●	◒	●	●	◒	◒
Wired	**Digital Subscriber Line (DSL):** DSL uses existing POTS infrastructure for data transmission between facilities via the Internet, although some providers offer a private network option at additional cost. DSL is capable of transmission rates of up to five megabits per second to the end user and up to 768 kilobits per second from the end user.	◒	●	○	◒	●	●	◒	◒
Wired	**T-Carrier 1 (T1) Line:** A T1 line is a dedicated point-to-point data connection between facilities that is capable of transmission rates up to 1.54 megabits per second.	◒	●	●	●	●	○	○	●
Wired	**Frame Relay:** To the end user, frame relay appears to be a dedicated point-to-point data connection up to 1.5 megabits per second, similar to a T1 line. However, providers vary the size and routing of frame relay data packets to optimize usage of their infrastructure, resulting in a reduction in costs relative to that of T1 lines.	◒	●	●	●	●	○	◒	●
Wired	**Multi-Protocol Label Switching:** This newer technology is replacing T1 and frame relay connections and is capable of transmission rates up to 622 megabits per second.	●	●	●	●	●	◒	◒	●
Wired	**Transparent LAN Service:** This is also called “Metro Ethernet” and is an emerging technology that provides Ethernet data transmission rates between facilities of 10, 100, or 1000 megabits per second.	◒	●	●	●	●	●	◒	●
Wired	**Utility-Owned Fiber Optic:** This dedicated point-to-point data connection between facilities is capable of transmission rates up to 10 gigabits per second.	◒	●	●	●	●	○	●	○
Wireless	**Digital Cellular:** Digital cellular uses wireless transceivers to connect to a provider’s cellular network for data transmission. The cellular technologies, 3G and 4G, have transmission rates of up to 800 kilobits per second and 10 megabits per second, respectively. Upload and download data transmission rates are often asymmetric with upload rates being lower.	◒	●	◒	◒	●	●	◒	●
Wireless	**Utility-Owned Wireless:** Utility-owned wireless uses utility equipment and infrastructure for data transmission over unlicensed or licensed frequency bands. Transmission rates vary widely depending on the modulation technology and frequency band (9.6 kilobits per second for low-speed, narrowband technologies and up to 7 gigabits per second for high-speed Wi-Fi). This category also includes microwave technologies.	●	●	◒	◒	◒	○	●	○

Attribute Key: ● Strong ◒ Moderate ○ Weak

Section 6: Information Management

Once alert data has been transmitted to a utility control center, alert information should be promptly displayed on a ***user interface*** and disseminated electronically to designated personnel. This information should also be stored for post-incident analysis. The process of selecting and implementing an ***information management system*** is similar to that used for a communications system (see Figure 5-1), with an additional up-front step for developing ***functional requirements***, which are key features and attributes of the system that are readily apparent to the end user. A description of each step required to develop an information management system, is provided in the subsections below.

TARGET CAPABILITY

There is an information management system that provides a timely display and efficient storage of data from ESM equipment.

Considerations for developing an ESM information management system are described in the following subsections:

- Subsection 6.1 describes a process for developing ESM information management requirements
- Subsection 6.2 describes a process for evaluating alternatives for ESM information management
- Subsection 6.3 provides guidance for designing an ESM information management system
- Subsection 6.4 describes the process for implementing an ESM information management system

6.1 Developing Requirements

Developing functional and technical requirements for an information management system is an important first step to establish information management functions that are necessary to support the ESM component. Typical functional requirements related to the ESM information management system are listed below.

- Display alerts in real-time
- Access alert data via a quick, easy, and intuitive process
- Access alert data from fixed workstations and mobile devices, etc.
- Create custom reports
- Export data in a format that can be used by external software
- Archive alert data for a certain duration
- Access archived alert data

To support the functional requirements, the ESM information management system will also have technical requirements such as data storage capacities for hardware at remote facilities and at a utility control center. For example, video recorders can be located at ESM facilities for temporarily storing high resolution video from all of the cameras at the facility, and video associated with specific alerts may be archived at a utility control center. Image resolution, frame rate, number of cameras, and duration of storage are variables that determine the capacity required for the video recorder. Furthermore, the frequency of alerts, the duration of video per alert, image resolution, frame rate, and days of desired storage are variables that determine the data storage capacity required at the utility control center. Data security is another technical requirement that is essential for all ESM information management systems.

The *Information Management Requirements Development Tool*, a software package designed to help users define and prioritize requirements for an information management system, can be used to develop

and document the requirements for an ESM information management system. This tool is populated with common functional and technical requirements for an information management system designed to support ESM operations. It also provides a feature for generating a consolidated list of functional and technical requirements that can be used to develop design and/or bid documents as appropriate.

6.2 Evaluating Alternatives for ESM Information Management

A variety of alternatives are available for ESM information management. Reviewing technology with security and video management consultants and communications providers may be helpful for identifying and evaluating available alternatives. If an SRS ***dashboard*** is being developed, ESM requirements can be integrated into the dashboard design. See *Dashboard Design Guidance for Water Quality Surveillance and Response Systems* for more information on dashboards. If a utility does not have an SRS dashboard, the utility could consider incorporating ESM functionality into existing SCADA or an access control system.

However, if a utility is considering integrating ESM video into a dashboard, existing SCADA, or access control system, the utility should confirm that the hardware and software are compatible and capable of handling the large amounts of data associated with video applications. Alternately, a utility may choose to implement video monitoring as a standalone system on its own network. This configuration isolates video data from other systems, and allows either system to be updated without affecting the other. However, use of a dedicated system for ESM video will necessitate the maintenance of additional hardware and network infrastructure. If video and alert management interfaces are not integrated, the workstations used to view each should be co-located such that utility personnel can view both screens simultaneously. If ESM information management splits across multiple systems, care should be taken to ensure that facility names and other metadata are consistent among the systems.

After information management alternatives have been established, criteria should be developed to evaluate and compare alternatives. The criteria can be based on the requirements developed in Section 6.1 and include overarching measures and utility-specific considerations. Utility-specific criteria can include level of expertise with a system and compatibility with other communications systems and existing information management systems. As a starting point, the following common evaluation criteria should be considered when selecting an information management system: ability to meet ESM requirements, extent of use, security, reliability, compatibility, installation cost, and maintenance requirements. Criteria can be added, revised, or deleted based on utility needs and constraints.

After developing evaluation criteria, the utility can perform a high-level screening of the alternatives to eliminate any that clearly would not meet the criteria, especially budget constraints. Of the remaining alternatives, the option that is evaluated most favorably is selected and designed, as described in Section 6.3.

6.3 Designing an ESM Information Management System

After selecting an approach to ESM information management, a detailed design is developed that includes: the storage required for alert and video data (if applicable), a detailed ***architecture*** that incorporates computer hardware and storage devices, and user interface screen designs. The steps to develop a detailed design are described below.

6.3.1 Estimating Required Storage

Estimated data generation rates can be used to determine the necessary storage capacity. The minimum storage required is the product of the frequency of incidents, the duration that data is retained, and the data per incident (alert and video). ***Historical data*** may be used to approximate the frequency of

incidents, and ESM data should be retained for a minimum of 30 days before being deleted or moved into long-term storage, although local ordinances may have different storage duration requirements. A factor of safety of at least 25% should be applied to the estimated data storage requirement to account for uncertainty in the estimated data generation rate.

The amount of data per incident includes calculations for alerts and video. The alert data per incident depends on overhead, encryption, and other factors described in the *Guidance for Designing Communications Systems*, Section A.1. The amount of video data per incident depends on the image resolution, frame rate, compression rate, and whether continuous video or clips of intrusions are being stored as described in *Guidance for Designing Communications Systems*, Section A.2.2 in the appendix.

Dedicated storage hardware for video data can also be considered because of the data intensive demands of most video systems, especially if the video and alert systems (e.g., dashboard, SCADA, or access control system) are not integrated. For more information on video storage, refer to Section 4.3.2 above.

6.3.2 Developing a Detailed Architecture

The detailed architecture should provide an overview of all ESM hardware including the intrusion detection devices, ***data collectors***, servers, storage hardware, and user interfaces. A description of each follows:

- **Intrusion detection devices**: Devices that detect an intrusion and generate an alert (e.g., motion sensors and door contact switches). The alert signal is typically a ***contact closure signal*** where the sensor completes or disconnects an electrical circuit when alert conditions are sensed. See Section 4 for details.
- **Data collectors**: Hardware at the ESM facility that is directly connected to intrusion detection devices. A data collector converts the raw data from intrusion detection devices to a format that can be processed by ESM servers. A data collector is usually a device capable of accepting contact closure inputs, wireless signals, or Ethernet data. Access control system modules, programmable logic controllers, and remote telemetry units are examples of data collectors.
- **Cameras**: Video cameras convert images to an analog or digital signal and can be fixed or PTZ. See Section 4 for details.
- **Video Recorders**: Hardware at the ESM facility that is directly connected to video cameras. Video recorders convert the raw data from cameras to a format that can be processed by video monitoring servers. Video recorders also provide temporary local storage of video data generated by their connected cameras.
- **Servers**: A high-end computer that is capable of managing the information from the data collectors and provides data to user-interface PCs and storage devices. The server also can include storage. Section 4.3.3 includes an overview of considerations for video servers.
- **Storage**: Data can be stored in servers or in standalone storage devices. See Section 4.3.2 for video storage details.
- **User interfaces**: Workstations and mobile devices that allow utility personnel to view alert information and video. Typically, user interfaces will include workstations at operations and security centers and mobile phones or tablets used by off-site utility personnel.

For the example shown in **Figure 6-1** below, continuous video data from all cameras are stored at the remote facility on the video recorder, and video clips from incidents are transmitted to the video monitoring server in a utility control center and archived in a RAID device. Alert data is transmitted to the alert management server for processing and ultimately stored on the RAID device. Data communications between facilities are shown as a cloud for this architecture diagram, and are discussed

in more detail in Section 5. The data collector does not include storage for this example. Alerts and video are displayed on a single ESM workstation for this example, although configurations with multiple ESM workstations are common.

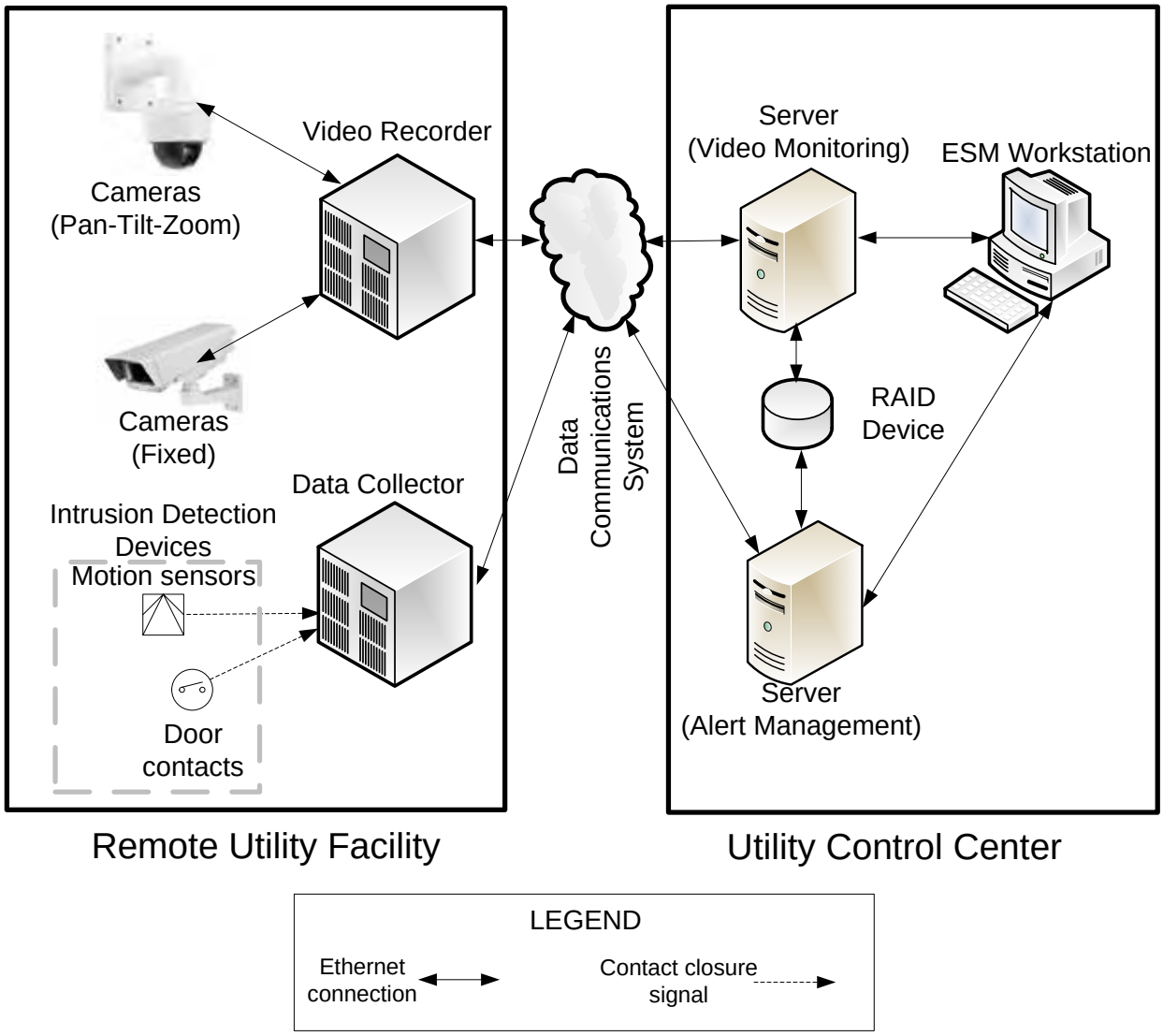


Figure 6-1. Example ESM Information Management Architecture

6.3.3 User Interface Screens

Utility personnel rely on the user interface to obtain the information necessary to investigate alerts. As a first step, an alert screen hierarchy, which describes the organization and connectivity of the user interface screens, should be established. The hierarchy should be informed by the alert investigation procedure developed in the Section 7, and general design guidelines are described below. Typically, there is an overview screen that shows all monitored facilities and provides single-click access to detailed facility-specific screens when more information on a facility is needed (e.g., when investigating an intrusion alert). Screens that show individual camera views may also be included. An example of an alert screen hierarchy is shown in **Figure 6-2** below.

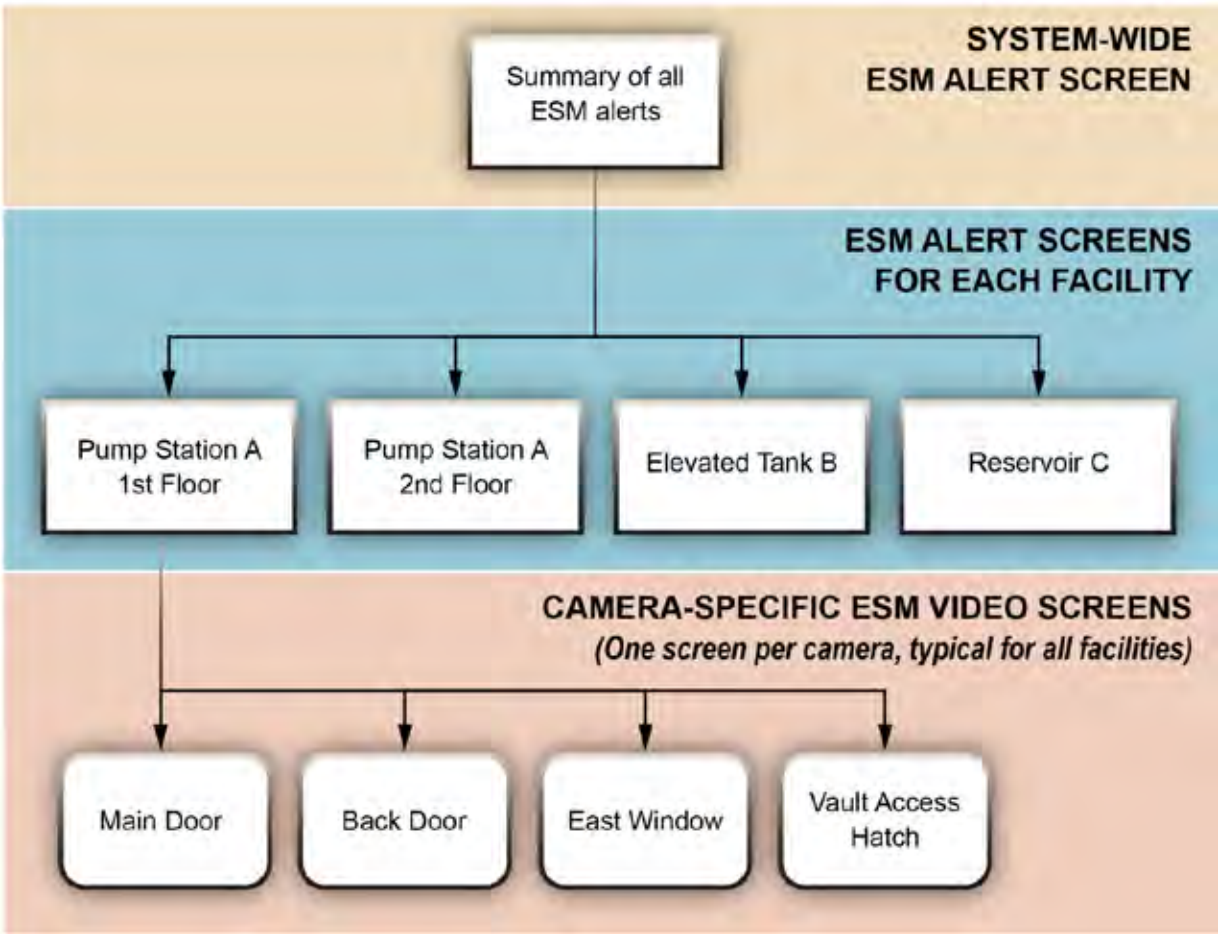


Figure 6-2. Example Screen Hierarchy for an ESM Information Management System

After establishing a screen hierarchy, the layout for each ESM user interface screen should be developed. First, a schema of alert parameters is developed such as time of alert, facility with the alert, and location of the alert within the facility (e.g., north door). Next, all of the intrusion sensors are listed for each facility and included in a system-wide alert screen. Then screens are developed for each ESM site to display facility-specific alarm information, followed by screens that show dedicated camera views.

For the system-wide alert screen, utilities with only a few facilities could use text-based descriptions of sites and alerts. However, utilities with dozens of facilities might consider a screen that shows a map of the utility's service area, with icons for the ESM sites. Similarly, for the facility-specific alert screens, sites with only a few intrusion detection devices could include text-based alert descriptions, while a large facility with numerous points of entry could show a plan view of the facility to show the locations of monitored doors, motion sensor zones, and video camera views.

An example that includes a system-wide alert screen, facility-specific screen, and camera-specific screen is provided in **Figure 6-3**. This figure shows the progression of screens that utility personnel would typically follow when investigating an ESM alert. The example commences with utility staff receiving an alert notification triggered by a door opening at an ESM facility. The ensuing investigation is guided by an alert investigation procedure developed for ESM as described in Section 7. Although other activities may be included in the investigation, such as contacting law enforcement, this example focuses solely on use of the user interface screens and references the numbered items listed below:

- Item 1: The ESM alert is received on the ESM Overview screen, which indicates that the Main Door has been opened at Pump Station A. The user clicks on the Pump Station A – 1st Floor facility detail screen for more information.
- Item 2: The Pump Station A –1st Floor screen shows video snapshots of all cameras at the site and highlights the Main Door, where the alert has been detected. The user clicks on the Main Door camera detail screen link for more information.
- Item 3: The Main Door camera detail screen shows a large image of the area. From this screen, the user can view live video and control the pan, tilt, and zoom of the camera to survey the area around the main door. The live video may allow utility personnel to determine the intruder's intent. The user also has the option of clicking Replay Alert to view recorded video of the door opening and the person entering. Replaying the alert can indicate if a utility employee inadvertently caused the alert.

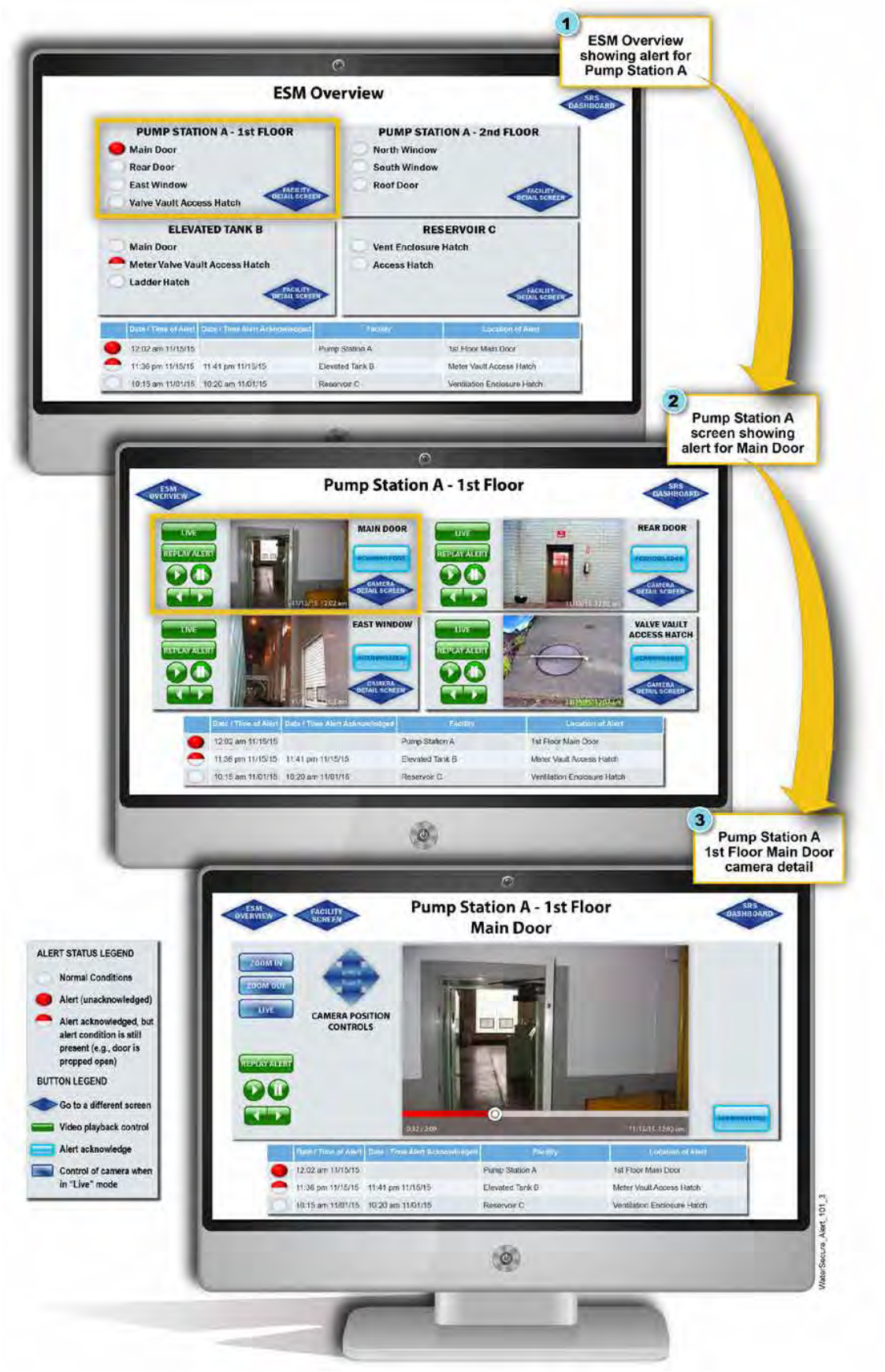


Figure 6-3. Example ESM Screens

6.4 Implementing an ESM Information Management System

The first step in implementing an ESM information management system is to develop contract documents based on the design developed under the previous step. These contract documents are used to solicit bids and select a contractor. Then, the contractor submits pre-installation design documents for utility review. After the utility approves the submitted documents, the contractor installs and commissions the system. Alternately, the utility could implement the information management system themselves using a similar approach, although the contractor procurement step would not be needed.

Using information from the design step, the utility must develop contract drawings and specifications and issue these documents for bidding by contractors. The contract documents must include requirements for a robust submittal and review process, a thorough and transparent commissioning effort, and performance benchmarks and other measures of quality to ensure that the information management system performs at an acceptable level before operational use. It may also be beneficial to include requirements for the contractor to provide a certain number of hours of post-installation support and associated travel costs to address issues that may occur after system commissioning.

If the utility has the option of soliciting only preapproved contractors (e.g., through a statewide contract for communications services and equipment), this approach is strongly recommended (Mix, Golembeski, & Baranowski, 2011). This can lead to a shorter bidding process and lower costs through a negotiated statewide pricing agreement.

Prior to installation, the contractor must submit design documentation including screen mock-ups, architecture options, and technical data on the hardware and software being provided. The utility ***IT design team*** and design engineers should review the submitted documentation to ensure conformance with the contract documents. After the utility approves the design documentation, the contractor installs the information management system. During installation, the utility should have a qualified inspector on site to ensure that installation and commissioning are performed as shown on the submittals and conform to the contract documents.

For more information on designing and implementing an information management system, consult Section 4 of *Guidance for Developing Integrated Water Quality Surveillance and Response Systems*.

Section 7: ESM Alert Investigation Procedure

An ESM alert investigation procedure should be developed to guide the systematic investigation of ESM alerts. The objective of an ***alert investigation*** is to determine if the suspected intrusion could lead to water contamination at the monitored facility.

TARGET CAPABILITY

A procedure has been developed, documented, and put into practice to facilitate the timely and efficient investigation of ESM alerts to determine whether an alert indicates an intrusion that could have resulted in contamination of distribution system water. The procedure provides a clear and comprehensive sequence of steps for the investigation of alerts, and assigns responsibilities for carrying out each step. The procedure is provided to personnel responsible for supporting investigations in a user-friendly format, such as a checklist. Personnel are trained on proper implementation of the procedure and related tools.

This section describes considerations for developing an ESM alert investigation procedure and covers the following topics:

- Subsection 7.1 provides guidance on developing an effective alert investigation procedure
- Subsection 7.2 provides guidance on developing tools to support the investigation
- Subsection 7.3 provides guidance on preparing to implement the procedure as part of real-time monitoring

7.1 Developing an Effective Alert Investigation Procedure

This section describes a methodical process for developing an ESM alert investigation procedure. The steps of the process, listed below, are described in the following subsections.

- Defining Potential Alert Causes: develop a discrete list of alert causes used to classify each alert
- Establishing an Alert Investigation Process: develop a detailed, sequential listing of steps for investigating alerts
- Assigning Roles and Responsibilities: establish a listing of all personnel who have a role in alert investigations and a summary of their responsibilities

The *ESM Alert Investigation Procedure Template* includes an editable table and process flow diagram that can be used to document the utility's role during an ESM alert investigation. The template can be opened in Word by clicking the icon in the callout box.

This template can be used to develop an ESM alert investigation procedure.

Defining Potential Alert Causes

The objective of the alert investigation process is to identify the cause of an alert. At the highest level, alerts should be categorized as invalid or valid. Valid alerts for ESM are defined as alerts attributable to an unauthorized entry to a utility facility with access to drinking water. **Table 7-1** lists and describes the most common causes of ESM alerts, based on experience from utilities that have implemented ESM (EPA, 2014). The causes are grouped into invalid (not due to unauthorized entry) and valid.

Table 7-1. Common Causes of ESM Alerts

---	Alert Cause	Description
Invalid Alerts	Employee Error	Employee or contractor forgot to call in to a utility control center after entering an ESM-monitored facility.
		Employee or contractor forgot to disarm the security system after entering an ESM-monitored facility.
		Employee or contractor left a door propped open at an ESM-monitored facility.
	Equipment Issue	Sensor malfunction
		Communications fault
		Power failure
	Environmental	Wildlife or windblown debris activated a motion sensor.
Valid Alerts	Non-contamination	Vandalism
		Theft
		Other non-contamination-related malevolent acts
	Possible contamination	Signs of contamination at the location of the ESM alert
		Intruder entered an area with access to distribution system water, and investigators cannot rule out the possibility that the intruder contaminated the water.

Establishing an Alert Investigation Process

With potential causes of ESM alerts defined, the next step is to develop an alert investigation process to guide investigators through a detailed sequence of steps in order to determine the cause of an alert. In general, the process begins with receipt and acknowledgement of an alert and ends with a determination regarding whether or not water contamination is possible. The steps between involve a review of available information to investigate potential causes of the alert. The alert investigation process is generally structured to consider the most likely causes first, allowing contamination to be quickly ruled out for the majority of alerts. However, if the cause of the alert cannot be determined through this review, the process concludes with the determination that contamination is possible.

ALERT INVESTIGATION AND USER INTERFACE SCREENS

The alert investigation procedure should inform the development of user interface screens to ensure that the screens provide the information needed by utility personnel at each step of the investigation. See Section 6.3.3 for more information on user interface screens.

The type of information typically documented in an alert investigation process includes:

- Detailed instructions for completing the step
- The name and role of specific individual(s) responsible for completing the step
- Information resources that should be consulted during the step
- Actions that should be taken, including personnel who should be notified, upon completion of the step

During the development of an ESM alert investigation process, the utility should coordinate with the various law enforcement agencies whose jurisdictions are included in the utility's service area. This provides a forum for establishing the responsibilities of law enforcement during the investigation of an ESM alert. It also provides law enforcement personnel with the opportunity to become familiar with drinking water facilities within their jurisdiction.

The alert investigation process can be visually depicted in a diagram that shows the progression of steps through the entire process. This simplified representation of the alert investigation process allows individuals with responsibilities for discrete steps to see how their activities support the overall investigation.

Figure 7-1 provides an example of an ESM alert investigation process flow diagram. The major steps and decision points are shown in the flowchart on the left side of the figure and additional detail on the actions implemented is shown to the right. In general, utility operations and security personnel are responsible for determining if an ESM alert is valid and indicative of a possible intentional contamination incident. Law enforcement can also be involved during on-site investigations. If the utility concludes that an ESM alert is invalid, the investigation is closed. However, if contamination is considered possible, the ***SRS Manager*** is notified.

A range of estimated times for properly trained personnel to complete steps in the investigation is shown to the left of the flowchart in Figure 7-1. These times are based on experience at utilities that have implemented ESM (EPA, 2014). The total time for utility personnel to complete an ESM alert investigation could range from two to 72 minutes, depending on the number of steps in the investigation process that need to be completed before a conclusion can be reached regarding whether or not contamination is possible.

For ESM locations with video monitoring, determining that contamination is possible may occur as soon as video from the site is available, which could be a minute or less after the intrusion occurs. However, if video is not available or does not show signs of possible contamination, an on-site investigation may be necessary to look for signs of contamination, which may take 33-72 minutes to complete.

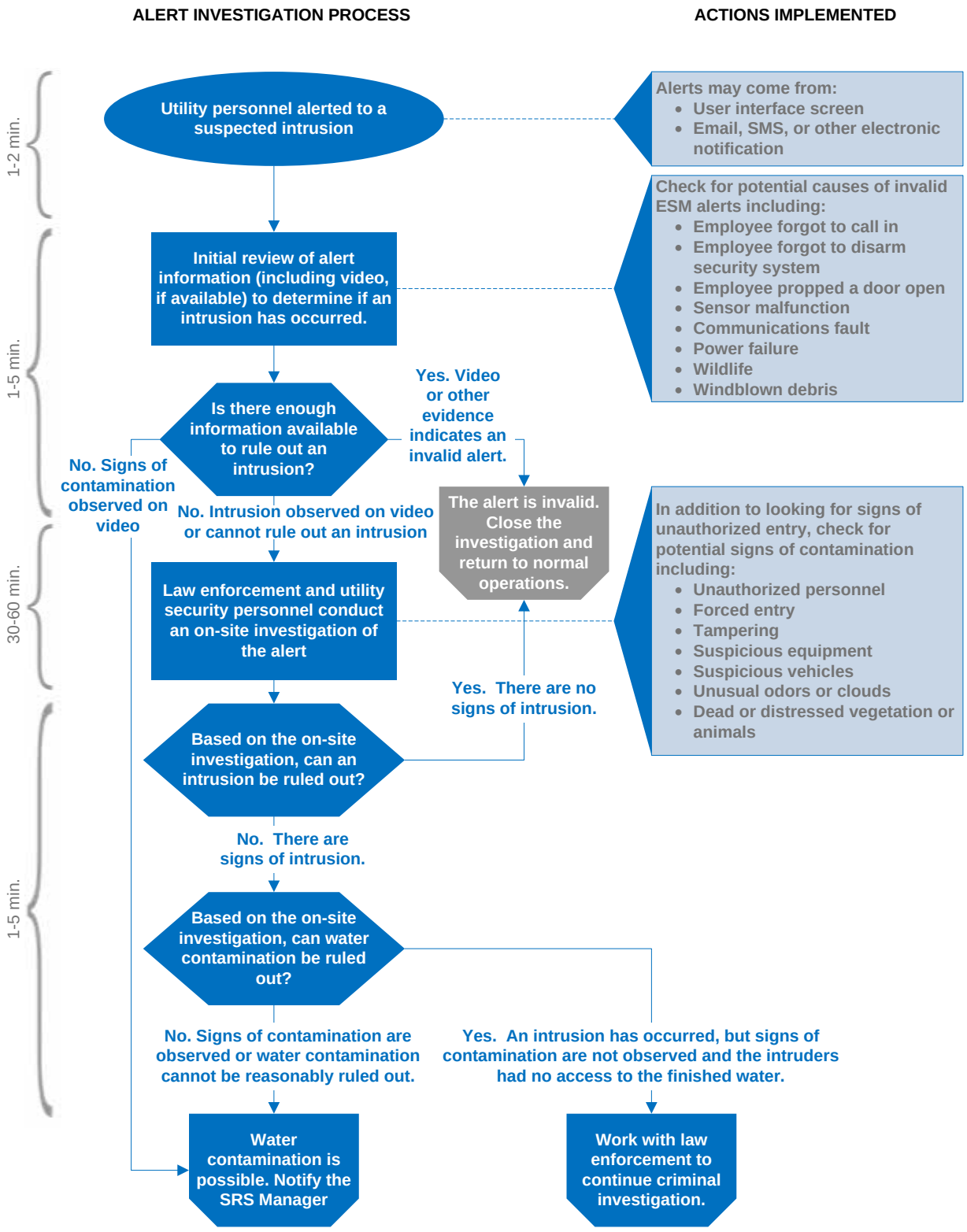


Figure 7-1. Example Alert Investigation Process Flow Diagram for ESM Alerts

The specific actions included in the alert investigation process depend largely on the availability of relevant information and how it can be accessed (e.g., through an ESM workstation or by calling separate utility departments). It is important to identify these information resources as the alert investigation process is being developed. The data available through existing information management systems may impact the activities included in the alert investigation process, and conversely the alert investigation process may point to the need to make additional information resources available to investigators or to improve access to existing information. Desired updates to information management systems should be noted during development of the alert investigation procedure. This information is particularly useful for developing requirements if a new information management system will be implemented or if existing systems will be updated.

When performing the initial review of alert information, utility personnel should first check the most likely causes of invalid alerts to minimize the investigation effort. Thus, the initial step is to review video from the site, if available, to determine if the video shows signs of intrusion and contamination or a benign cause for the alert (e.g., wildlife or windblown debris). Typically, the next step is to check the utility's call-in log to determine if an employee has called in from the site, but forgot to disarm the security system. Next, utility personnel should check the maintenance log for utility work or problematic intrusion detection sensors at the site. Lastly, the user interface screen is checked for power and communications outages at the site. If the ESM alert is from an interior door sensor, personnel can check the door status history on the user interface screen to determine if the door has been propped open, causing an invalid alert, although personnel should still be dispatched to the site to close the monitored door. A propped exterior door would still warrant an investigation because the open door could have allowed an intruder to gain access to the facility.

If an on-site investigation is required, the process of searching and clearing the facility is best performed by law enforcement and security staff. Additionally, investigators should look for the unusual site conditions listed in Figure 7-1 when conducting their investigation, which are discussed in further detail below.

- **Unauthorized personnel**: Note the number of intruders and their sex, height, weight, and potentially distinctive attributes.
- **Forced entry**: Cut fences, cut locks, damaged doors or windows
- **Tampering**: Damaged utility equipment
- **Suspicious equipment**: Weapons, explosives, empty containers, portable pumps, discarded personal protective equipment
- **Suspicious vehicles**: Make, model, color, license plate, and other unusual characteristics such as large dents in vehicle and other noticeable damage
- **Unusual cloud or odors**: Possible sign of a hazardous chemical or gas
- **Dead or distressed vegetation or animals**: Possible sign of a hazardous chemical

If the investigation determines that contamination may be possible, the SRS manager will be notified and will activate a ***Distribution System Contamination Response Plan***. This plan includes procedures to establish the credibility of the possible contamination incident, minimize public health and economic consequences by implementing ***response actions*** such as operational changes (e.g., close valves, turn off pumps) or public notification, and guide the remediation and recovery effort. The credibility of an ESM alert can quickly escalate, requiring notifications to external partners, such as the drinking water primacy agency. Consult *Developing a Distribution System Contamination Response Plan* for more information.

VERBAL AND WRITTEN THREATS

A utility may also want to develop procedures for and train its employees on investigating verbal and written threats. Procedures and checklists for a utility's customer service representatives to respond to such threats can be found in *Designing Customer Complaint Surveillance For Water Quality Surveillance and Response*.

Assigning Roles and Responsibilities

Table 7-2 lists utility and law enforcement personnel who may have a role during the investigation of an ESM alert and describes their potential responsibilities.

Table 7-2. Example of Generic Roles and Responsibilities for ESM Alert Investigations

Role	Alert Investigation Responsibilities
Utility Control Center Operator	• Monitor all SCADA alerts 24/7/365, including intrusion alerts. • Perform the initial review of alert information to determine if the intrusion alert is invalid. • Notify utility security personnel if an intrusion is suspected. • Notify local law enforcement of ESM alerts that may require their involvement. • Notify the SRS Manager if signs of contamination are observed on video. (Some utilities may prefer that utility security personnel perform these functions to minimize distracting operators from their primary duties of controlling and monitoring the distribution and treatment systems.)
Utility Security Personnel	• If the utility control center operator does not acknowledge the intrusion alert, perform the initial review of alert information to determine if the intrusion alert is invalid. • Lead the investigation of all ESM alerts. This includes assessing the validity of ESM alerts and performing on-site investigations. • Coordinate site investigation activities with distribution field crews and local law enforcement, as necessary. • If an intrusion is confirmed, determine whether the intruder could have accessed the water supply. • Make the determination regarding whether or not a security incident presented the intruder with an opportunity to contaminate the drinking water.
Distribution Supervisor	• Coordinate the site activities of field crews who may support utility security personnel during the on-site investigation of a security incident. • Review distribution system work activity to determine whether an ESM alert could have been inadvertently caused by utility personnel. (Distribution supervisors and field crews may need to be trained in security procedures because they could be the first to arrive at a potential crime scene, and security duties may need to be added to their formal job descriptions.)
Distribution Field Crews	• Perform site activities to support utility security personnel in the on-site investigation of a security breach.
Local Law Enforcement	• Conduct an investigation at the site of a security incident, if warranted. • Interview potential witnesses to a security incident. • Initiate a criminal investigation, if an unlawful intrusion has been confirmed.

Arrangements should also be made to provide coverage of alert investigation responsibilities at all times, through approaches such as these:

- Training personnel from all shifts on the alert investigation procedure
- Assigning backup personnel for each activity in the case that the primary investigator is unavailable
- Cross-training investigators on multiple roles
- Assigning personnel to be on call for critical investigation functions, particularly those requiring a decision about the possibility of water contamination

THIRD PARTY SECURITY SERVICES

A third-party security service may be considered for utilities that prefer not to hire security staff or install and maintain security equipment. Third-party monitoring services typically monitor for alerts 24/7 and provide their own communications infrastructure. Some services also dispatch guards to respond to alerts. Although the upfront costs for using a third-party security service may be minimal, the utility's operating budget will need to account for the recurring fees. If a third-party security service is used, the service's operating procedures would need to be coordinated with the utility's personnel to have a sustainable and robust process. For example, utility personnel may need to be present to unlock the facility gate and building entrance door for all on-site investigations by the security service.

7.2 Developing Investigation Tools

While the detailed alert investigation procedure described in Section 7.1 is necessary, the detailed documentation of this procedure is generally not used during ***real-time*** alert investigations. This section describes the following tools that can be developed to assist investigators in efficiently carrying out their responsibilities:

- Checklists
- Record of Alert Investigations
- Quick Reference Guides

Checklists

Alert investigation checklists are job aids that guide personnel through their investigative responsibilities and document investigation findings. Checklists can help ensure consistency among investigators, verify that all activities are completed, and reduce the time required to conduct alert investigations. They generally list the activities assigned to specific roles, and thus more than one checklist may be developed to support the ESM alert investigation procedure.

Depending on the number of utility roles involved in an investigation and the overall complexity of the ESM alert investigation process, a utility may prefer to have a single or multiple checklists. For the flow diagram shown in Figure 7-1, multiple checklists could be used. The *ESM Alert Investigation Procedure Template* contains editable ESM alert investigation checklists for the control center operator and on-site investigator.

Record of Alert Investigations

A record of alert investigations provides documentation of key information, including the actions implemented during the investigation as well as the likely cause of the alert. This record can be used to monitor the frequency of alerts by cause (Section 7.1). It can also serve as a resource during investigation of future alerts.

There are a variety of ways to document alert investigations. For example, a simple approach uses a spreadsheet maintained on a shared drive that can be accessed by all investigators as well as the SRS Manager. Use of an electronic tool, such as a spreadsheet, can facilitate standardization of data entry through use of predefined pull-down lists and data entry masks. **Figure 7-2** provides an example record that shows useful fields to capture.

Alert Investigation Information							
Alert Date/Time	**Alert Location**	**Point of Intrusion**	**Investiga-tor**	**Investiga-tion Start Date / Time**	**Investiga-tion End Date / Time**	**Conclusion**	**Notes**
5/4/14 2:15 AM	Pump Station A	Main door	Jean Smith	5/4/14 2:16 AM	5/4/14 2:30 AM	Invalid alert: Employee did not disarm security system	Gary Miller called in.
5/6/14 8:05 AM	Elevated Tank B	Meter Valve Vault Access Hatch	John Brown	5/6/14 8:06 AM	5/6/14 8:30 AM	Invalid alert: Sensor malfunction	Hatch sensor has been flaky over the past month, but instrument shop has not repaired it.
5/6/14 4:05 PM	Reservoir C	Access Hatch	Tasha Lee	5/6/14 4:07 PM	5/6/14 4:30 PM	Invalid alert: Employee did not call-in	Chris Nguyen seen on video and later called in.

Figure 7-2. Example of Alert Investigation Records

If a dashboard will be used to support the SRS, electronic alert investigation tracking may be incorporated into the design. For example, electronic checklists can be developed, and the information entered can automatically be saved in a database, facilitating further analysis and use of the records. If ESM alerts are incorporated into a SCADA or access control system, these types of applications typically include alert tracking. See *Dashboard Design Guidance for Water Quality Surveillance and Response Systems* for more information on this option.

Quick Reference Guides

While many alert investigation activities become second nature to investigators, additional tools may be useful for guiding investigators through complex or less frequently implemented tasks. Development of quick reference guides, in which key information is concisely summarized in an easily accessible form such as a factsheet, ensure investigators can quickly and easily get the information they need. Examples of quick reference guides that can be useful for ESM include:

- A list of contact information for all individuals whom investigators may need to contact during alert investigations.
- Site-specific guidelines for investigating suspected intrusions, which include details such as a summary of points of entry, locations that could provide access to water, rendezvous locations, and actions an investigator should not take for safety or security reasons.
- Job aids that include annotated overhead views of each site including locations of video cameras, intrusion detection sensors, and other site features.
- Call-in scripts for utility personnel to use when notifying 911 or other external agencies of the intrusion. An example 911 script is provided in the callout box below.

EXAMPLE 911 SCRIPT

My name is [**name of Utility Control Center Operator on duty**], and I am the Senior Operator for the [**Utility Name**]. We are in the process of investigating a possible intrusion at our [**name of location**] at [**address or location of the facility**]. We are requesting police response at this location for our [**utility staff and/or utility security**] that is already [**en route or onsite**].

Our alarm system indicates that there have been [**single or multiple door alarms or single or multiple motion alarms**]. [**If video is available: I have viewed a video clip of the possible intrusion, and it shows [describe what is shown on the video clip]**]. We suspect that criminal activity may have occurred, or may still be occurring, at this location and that hazardous conditions may exist.

Our team leader for this investigation is [**name of utility staff and/or utility security dispatched to the scene**] who will meet the arriving law enforcement personnel and coordinate their support. Police can contact me at [**land-line and cell phone numbers**] for further information. Where do you want [**name of utility staff and/or utility security dispatched to the scene**] to meet the responding officers?

7.3 Preparing for Real-time Alert Investigations

This section describes a suggested process for putting the ESM alert investigation procedure into practice. The benefits of ESM can be fully realized only if ESM alerts are investigated in real time and responded to appropriately. The following topics are covered under this section:

- Training
- Real-time operation

Training

Proper training on the alert investigation procedure ensures that all utility personnel with a role in the investigation of ESM alerts are aware of their responsibilities and have the knowledge and expertise needed to implement those responsibilities. It is suggested that training on the alert investigation procedure include the following:

- An overview of the purpose and design of the ESM component
- A description of the local law enforcement agencies that have jurisdictions within the utility's service area
- A detailed description of the alert investigation procedure and the role of each participant
- A review of checklists, quick reference guides, information management systems, and other tools available to support ESM alert investigations
- Instructions for using the record of alert investigations, both for entering new records and retrieving previous records to support new alert investigations

Section 6 of *Guidance for Developing Integrated Water Quality Surveillance and Response Systems* provides guidance on implementing a training and exercise program. In general, classroom training is conducted first to orient personnel to the procedure and their responsibilities during ESM alert investigations. Once they are comfortable with the procedure, drills and exercises give them the opportunity to practice implementing their responsibilities in a controlled environment. The *SRS Exercise Development Toolbox* is an interactive software program designed to help utilities design, conduct, and evaluate exercises specific to ESM and the other SRS components.

A utility may also consider training utility security staff on the existing equipment, infrastructure, and overall layout at each ESM site. This can improve investigators' ability to discern unusual conditions from normal operations. Such training can also be offered to local law enforcement to enhance their understanding of the operations and equipment that occur at utility facilities.

CASE STUDY

A utility developed a training video for each police district in the utility's service area. These videos were intended to assist police officers with monitoring critical utility facilities by describing site-specific features and potential signs of contamination at the utility locations in the applicable district. The training videos were well-received, and the police districts and police academy currently use these videos in their ongoing training cycles.

Real-time Operation

After the ESM system has been commissioned and training has occurred, real-time operation of this component should commence. During real-time operation, ESM alerts are investigated as they are generated, and the *Distribution System Contamination Response Plan* is activated if drinking water contamination is considered possible. The transition from commissioning to real-time operation should be clearly communicated to all utility personnel with a role in ESM alert investigations. This includes establishing a date for the transition as well as providing expectations for how alert investigations will be performed and documented.

To sustain real-time operation, a culture of security should be promoted such that all utility personnel understand and contribute to the security of the organization (AWWA, 2014). A key part of a security culture is the integration of alert investigation procedures into existing job functions and responsibilities to the extent possible. Leveraging existing expertise in this manner will reduce the amount of new training required and can result in increased acceptance of new responsibilities for investigating ESM alerts. Sufficient time must be allocated for personnel to investigate ESM alerts as they are generated.

Other important aspects of security culture include maintenance of the alert investigation procedure and training. Maintenance involves periodic review of the steps performed to verify that they are working as intended. Furthermore, the alert investigation record should be reviewed to ensure that the procedure is being correctly implemented. Ongoing drills, exercises, and training are important to ensure that staff remain familiar with their responsibilities and to address any changes, such as updates to the procedure or investigation tools. Consider including local law enforcement in drills and exercises to build a stronger relationship and improve coordination with the utility. Finally, it is important to thoroughly train new staff on their responsibilities for supporting the investigation of ESM alerts.

MAINTAINING THE ALERT INVESTIGATION PROCEDURES

Routine updates to the alert investigation procedure and tools are necessary to maintain their usefulness. Recommendations for procedure maintenance include these tasks:

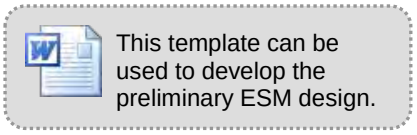
- Designate one or more individuals with responsibility for maintaining alert investigation materials.
- Establish a review schedule (annual review should suffice in most cases, although the procedure and tools should be developed for new utility facilities as soon as they are commissioned).
- Review the alert investigation record, conduct tabletop exercises, and solicit feedback from investigators to identify necessary updates.
- Establish a protocol for submission and tracking of change requests.

Section 8: Preliminary ESM Design

The information presented in the previous sections of this document can guide development of a preliminary ESM design that supports a utility's design goals and performance objectives. If ESM will be a component in a multi-component SRS, the design of the integrated system will likely be guided by a project management team. In this case, guidelines for design of the individual components should be provided to the component implementation teams, and should include:

- Overarching design goals and performance objectives for the SRS.
- Existing resources that could be leveraged to implement the SRS components, including personnel, procedures, equipment, and information management systems.
- Project constraints, such as budget ceilings, schedule milestones, and policy restrictions.
- Instructions or specific guidelines for the development of preliminary component designs.

It is also useful to develop a preliminary ESM alert investigation procedure prior to developing a preliminary ESM design. Information in this procedure can inform various aspects of the design, such as information management requirements.



Regardless of whether ESM will be developed as a stand-alone component or as part of a multi-component SRS, the preliminary ESM design should be documented in sufficient detail to assess whether or not it can achieve the design goals established for the component within project constraints. A *Preliminary ESM Design Template* can be opened and edited in Word by clicking the icon in the callout box. This template covers the following aspects of ESM design:

- Component implementation team: Identify personnel from the utility and local law enforcement organizations who will have a role in the design and implementation of ESM. Document the role, responsibilities, and estimated time commitment of each team member.
- Design goals and performance objectives: Use the overarching design goals and performance objectives established for the SRS to develop specific ESM goals and performance objectives to guide the design process.
- Preliminary site and physical security equipment selection: Identify sites for installing ESM equipment based on each site's risk of contamination and the cost required to upgrade the site's physical security equipment to an acceptable level as established by the performance objectives.
- Preliminary communications: Identify all communications systems that could be used for transmitting ESM data. This could include SCADA, access control, or business networks. Document the performance of existing systems and identify sites where the existing communications system might require replacement or upgrades.
- Preliminary information management requirements: Identify all information management systems that would be used during operation of ESM. This will likely include utility systems that will be accessed during the investigation of ESM alerts and possible interfaces with local law enforcement. Develop an information flow diagram depicting user-to-machine and machine-to-machine interactions. Document requirements for any new or modified information management systems.
- Initial training requirements: Develop a training plan to educate personnel about their responsibilities during operation of ESM.
- Budget: Develop a line item budget for the ESM component. It is recommended that the budget include implementation as well as ***operation and maintenance (O&M) costs***, which can be used

to develop a ***lifecycle cost*** estimate. The budget should indicate the year in which each cost is incurred. Contingencies should be included to avoid cost overruns.

- Schedule: Develop a schedule that shows the planned sequencing of activities as well as any key dependencies. The schedule may reflect a phased implementation over multiple years, which may be advantageous or necessary to overcome resource (financial or personnel) limitations.

In some cases, multiple design alternatives may emerge. A ***benefit-cost analysis*** should be performed to identify the preferred option. The resource *Framework for Comparing Alternative Water Quality Surveillance and Response Systems* provides an objective process for comparing design alternatives with respect to their lifecycle costs and capability.

Resources

Overview of ESM Design

Vulnerability Self-Assessment Tool

The Vulnerability Self-Assessment Tool (VSAT) helps water and wastewater utilities of all sizes to identify vulnerabilities to both man-made and natural hazards and evaluate potential improvements to enhance their security and resiliency. Version VSAT 6.0, released in 2015, is also consistent with the ANSI/AWWA Standard for Risk and Resilience Management of Water and Wastewater Systems, termed the J100 Standard.
https://yosemite.epa.gov/ow/SReg.nsf/description/VSAT

Enhanced Security Monitoring Primer for Water Quality Surveillance and Response Systems

This document provides an overview of the Enhanced Security Monitoring (ESM) component and presents information about the goals and objectives of ESM in the context of a Water Quality Surveillance and Response System. It also defines the design elements that are necessary for a functional ESM component. EPA 817-B-15-002B, May 2015.
http://www.epa.gov/sites/production/files/2015-06/documents/enhanced_security_monitoring_primer.pdf

Water Quality Surveillance and Response System Primer

This document provides an overview of Water Quality Surveillance and Response Systems (SRS) for drinking water distribution systems. It defines the components of an SRS, describes common design goals and performance objectives for an SRS, and provides an overview of the approach for implementing an SRS. EPA 817-B-15-002, May 2015.
http://www.epa.gov/sites/production/files/2015-06/documents/water_quality_sureveillance_and_response_system_primer.pdf

Site Selection

Framework for Comparing Alternatives for Water Quality Surveillance and Response Systems

This document provides guidance for selecting the most appropriate design from a set of viable alternatives. It guides the user through an objective, stepwise analysis for ranking multiple alternatives and describes, in general terms, the types of information necessary to compare the alternatives. EPA 817-B-15-003, June 2015.
http://www.epa.gov/sites/production/files/2015-07/documents/framework_for_comparing_alternatives_for_water_quality_surveillance_and_response_systems.pdf

EPANET

A software application that models water distribution piping systems. EPANET performs extended period simulation of the water movement and quality behavior within pressurized pipe networks by calculating parameters such as the flow in each pipe, pressure at each node, height of the water in each tank, and water age. Furthermore, EPANET can model the movement and fate of a reactive material as it grows (e.g., a disinfection by-product) or decays (e.g., chlorine residual) over time.
https://www.epa.gov/water-research/epanet

Physical Security Equipment

Guidelines for the Physical Security of Water Utilities

Guidelines for water utilities that recommend physical and electronic security measures for systems intended to protect against threats with specified motivation, tools, equipment, and weapons. Additional requirements and security equipment may be necessary to defend against threats with greater capabilities. December 2006.
http://www.waterboards.ca.gov/drinking_water/certlic/drinkingwater/documents/security/WISE-Phase3WaterUtilityGuidelines.pdf

Commissioning Security Equipment – Getting it Right the First Time

Discusses commissioning of security systems and provides a step-wise commissioning process and forms for use by drinking water utilities. The objectives of commissioning are to ensure that systems perform as designed and meet the owner's needs. Although this document focuses on security equipment and reducing invalid alerts, its nine-step approach is also applicable to a communications system. EPA 817-R-12-002, February 2012.
https://www.epa.gov/sites/production/files/2015-06/documents/commissioning_security_systems_for_drinking_water_utilities.pdf

Communications

Guidance for Designing Communications Systems for Water Quality Surveillance and Response Systems

This guidance document describes an approach for evaluating and selecting communications technologies to support the transmission of data generated by ESM. The document provides users with a description of attributes that should be considered when evaluating communications systems alternatives and a general assessment of common technologies relative to these attributes. EPA 817-B-16-002, September 2016.
https://www.epa.gov/sites/production/files/2017-04/documents/srs_communications_guidance_081016.pdf

Information Management

Information Management Requirements Development Tool

This tool is designed to help users develop information management requirements to support operation of a Water Quality Surveillance and Response System (SRS). Specifically, this tool (1) assists SRS component teams with development of component functional requirements, (2) assists information technology (IT) personnel with development of technical requirements, and (3) allows the IT design team to efficiently consolidate and review all requirements. EPA 817-B-15-004, October 2015.
https://www.epa.gov/waterqualitysurveillance/information-management-requirements-development-tool

Dashboard Design Guidance for Water Quality Surveillance and Response Systems

A dashboard is a visually oriented user interface that integrates data from multiple Water Quality Surveillance and Response System (SRS) components to provide a holistic view of distribution system water quality. This document provides information about useful features and functions that can be incorporated into an SRS dashboard. It also provides example user interface designs. EPA 817-B-15-007, November 2015.
http://www.epa.gov/sites/production/files/2015-12/documents/srs_dashboard_guidance_112015.pdf

Guidance for Developing Integrated Water Quality Surveillance and Response Systems

This document provides guidance for applying system engineering principles to the design and implementation of a Water Quality Surveillance and Response System (SRS) to ensure that the SRS functions as an integrated whole and is designed to effectively perform its intended function. Section 4 provides guidance on developing information management system requirements, selecting an information management system, and IT master planning. Section 6 provides guidance on developing a training and exercise program to support SRS operations. EPA 817-B-15-006, October 2015.
http://www.epa.gov/sites/production/files/2015-12/documents/guidance_for_developing_integrated_wq_srss_110415.pdf

Alert Investigation Procedure

ESM Alert Investigation Procedure Template (Word File)

The alert investigation procedure template includes an editable flow diagram, table, and checklists that can be used to document the utility's role in an ESM alert investigation process. August 2017.
Click this link to open the template

Developing a Distribution System Contamination Response Plan

This resource provides an editable template for developing a utility-specific Distribution System Contamination Response Plan. Elements of this plan include investigation of a possible distribution system contamination incident, planning for site characterization, implementing operational response actions, issuing public notification, and planning for remediation and recovery. An accompanying guide helps the user populate the template to customize the plan to a specific utility. *In press*.
https://www.epa.gov/waterqualitysurveillance/consequence-management-resources

Designing Customer Complaint Surveillance For Water Quality Surveillance and Response Systems

This document describes the Customer Complaint Surveillance component and its design elements, including Complaint Collection, Information Management and Analysis, and Alert Investigation Procedure. EPA 817-B-17-002, November 2017.
https://www.epa.gov/waterqualitysurveillance/customer-complaint-surveillance-resources

SRS Exercise Development Toolbox

The Exercise Development Toolbox helps drinking water utilities to design and conduct exercises in order to evaluate procedures developed to support a Water Quality Surveillance and Response System (SRS). These exercises can be used to refine SRS procedures and train personnel in the proper implementation of those procedures. The toolbox guides users through the process of learning about training programs, developing realistic contamination scenarios, designing SRS discussion-based and operations-based exercises, and creating exercise documents. EPA 2016.
https://www.epa.gov/waterqualitysurveillance/water-quality-surveillance-and-response-system-exercise-development-toolbox

Preliminary ESM Design

Preliminary ESM Design Template (Word File)

This Word template can be used to document aspects of ESM component design such as the component implementation team, design goals and performance objectives, preliminary site and

physical security equipment, preliminary communications, preliminary information management requirements, initial training requirements, budget, and schedule. August 2017.
Click this link to open the template

References

AWWA, 2014. ANSI/AWWA G430-14: Security Practices for Operations and Management. AWWA, Denver.

EPA, 2014. *Water Security Initiative: Evaluation of the Enhanced Security Monitoring Component of the Cincinnati Contamination Warning System Pilot*, 817-R-14-001C. Washington, D.C.

Mix, N., Lynn, R., Gist, F., Lai, A. Advancements in Security Technology – Detection, Assessment, and Automation. *Opflow. In press*.

Mix, N., Golembeski, J., Baranowski, C., 2011. Understanding Information Security Terminology and Governance for Drinking Water and Waste Water Utilities. *Proceedings of the Water Security Congress*. Nashville, Tennessee. (Manuscript for Abstract ID 35294)

Mix, N., Pickard, B., Gist, F., Lai, A., 2011. Security Equipment History, Trends, Use and Functionality – From Tried & True to Emerging & Cutting Edge. *Proceedings of the Water Security Congress*. Nashville, Tennessee. (Manuscript for Abstract ID 35292)

Glossary

alert. An indication from an SRS surveillance component that an anomaly has been detected. Alerts may be visual or audible, and may initiate automatic notifications such as pager, text, or email messages.

alert investigation. The process of investigating the validity and potential causes of an alert generated by an SRS surveillance component.

alert investigation checklist. A form that lists a sequence of steps to follow when investigating an SRS alert. This form ensures consistency with an alert investigation procedure and provides documentation of the investigation of each alert.

alert investigation procedure. A documented process that guides the investigation of an SRS alert. A typical procedure defines roles and responsibilities for alert investigations, includes an investigation process diagram, and provides one or more checklists to guide investigators through their roles in the process.

anomaly. A deviation from an established baseline. Detection of an anomaly by an SRS surveillance component generates an alert.

architecture. The fundamental organization of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution. The architecture of an information management system is conceptualized as three tiers: source data systems, analytical infrastructure, and presentation.

benefit-cost analysis. An evaluation of the benefits and costs of a project or program, such as an SRS, to assess whether the investment is justifiable considering both financial and qualitative factors.

commissioning. The process of testing a newly installed or modified system for proper operation, configuration, and calibration.

communications provider. An entity that allows customers to use its network to transmit data. This includes third-party service providers such as cellular or telecommunications carriers and cable television companies.

component. One of the primary functional areas of an SRS. There are four surveillance components: Online Water Quality Monitoring; Enhanced Security Monitoring; Customer Complaint Surveillance; and Public Health Surveillance. There are two response components: Consequence Management and Sampling and Analysis.

consequence. An adverse public health or economic impact resulting from a contamination incident.

constraints. Requirements or limitations that may impact the viability of an alternative. The primary constraints for an SRS project are typically schedule, budget, and policy issues (for example, zoning restrictions, IT restriction, and union prohibitions).

contact closure signal. A signal generated by a device that connects or disconnects an electrical circuit to indicate a change of state. Intrusion sensors typically generate this type of signal and change state when a door, hatch, window, etc. is opened or if motion is sensed.

contamination incident. The presence of a contaminant in a drinking water distribution system that has the potential to cause harm to a utility or the community served by the utility. Contamination incidents may have natural (e.g., toxins produced by a source water algal bloom), accidental (e.g., chemicals introduced through an accidental cross-connection) or intentional (e.g., purposeful injection of a contaminant at a fire hydrant) causes.

control center. A utility facility that houses operators who monitor and control treatment and distribution system operation, as well as other personnel with monitoring or control responsibilities. Control centers often receive system alerts related to operations, water quality, security, and some of the SRS surveillance components.

dashboard. A visually oriented user interface that integrates data from multiple SRS components to provide a holistic view of distribution system water quality. The integrated display of information in a dashboard allows for more efficient and effective management of distribution system water quality and the timely investigation of water quality incidents.

data collector. Hardware that transmits and receives signals from field devices and converts the information for use by a designated software application running on a server. Typical data collectors include access control system modules, programmable logic controllers, and remote telemetry units.

design elements. The functional areas that comprise each component of an SRS. In some cases, design elements are divided into design sub-elements. In general, the information presented in SRS guidance and products is organized by design elements and sub-elements.

design goal. The specific benefits to be realized through deployment of an SRS and each of its components. A fundamental design goal of an SRS is detecting and responding to distribution system contamination incidents. Additional design goals for an SRS are established by a utility and often include benefits to routine utility operations.

Distribution System Contamination Response Plan. A planned decision-making framework that establishes roles and responsibilities and guides the investigative and response actions following a determination that distribution system contamination is possible.

distribution system water. Treated drinking water within a distribution system.

Enhanced Security Monitoring (ESM). One of the surveillance components of an SRS. ESM includes the equipment and procedures used to detect and respond to security breaches at distribution system facilities that are vulnerable to contamination.

facility. A utility structure used for storing, treating, or pumping water. The terms “facility” and “site” are used interchangeably in this document, although in practice, it may be possible for a site to include multiple facilities. For example, a large utility site may include elevated storage tank and pump station facilities.

functional requirement. A type of information management requirement that defines key features and attributes of an information management system that are visible to the end user. Examples of functional requirements include the manner in which data is accessed, types of tables and plots that can be produced through the user interface, the manner in which component alerts are transmitted to investigators, and the ability to generate custom reports.

hardening. Practices for deterring and delaying unauthorized entry to a site, such as installing fencing and locks and clearing vegetation around the perimeter of the facility.

hardware. Physical IT assets such as servers or user workstations.

historical data. Data that has been generated and stored, including recent data that is readily available in an information management system as well as older data that has been stored or archived in a historian.

implementation costs. Costs to procure and install equipment, IT components, and other assets necessary to build an operational system.

information management. The processes involved in the collection, storage, access, and visualization of information. In the context of an SRS, information includes the raw data generated by SRS surveillance components, alerts generated by the components, ancillary information used to support data analysis or alert investigation, details entered during alert investigations, and documentation of Consequence Management activities.

information management system. The combination of hardware, software, tools, and processes that collectively supports an SRS and provides users with information needed to monitor real-time system conditions. The system allows users to efficiently identify, investigate, and respond to water quality incidents.

information technology (IT). Hardware, software, and data networks that store, manage, and process information.

intrusion detection equipment. Devices that detect a door opening, motion, glass break, or vibration that can alert utility personnel of unauthorized access into drinking water distribution system facilities. Video monitoring is also a type of intrusion detection equipment.

invalid alert. An alert from an SRS surveillance component that is not due to a water quality incident or public health incident.

IT design team. Personnel responsible for selecting, designing, and implementing the SRS information management system.

lifecycle cost. The total cost of a system, component, or asset over its useful life. Lifecycle cost includes the cost of implementation, operation and maintenance, and renewal.

monitoring location. A specific point in the water distribution system where SRS component data is collected, such as the location of OWQM sensor hardware or an ESM video surveillance camera.

operation and maintenance (O&M) costs. Expenses incurred to sustain operation of a system at an acceptable level of performance. O&M costs are typically reported on an annual basis, and include labor and other expenditures, such as supplies and purchased services.

performance objectives. Measurable indicators of how well an SRS or its components meet established design goals.

possible. In the context of the threat level determination process, water contamination is considered possible if the cause of an alert from one of the surveillance components cannot be identified or determined to be benign.

real-time. A mode of operation in which data describing the current state of a system is available in sufficient time for analysis and subsequent use to support assessment, control, and decision functions related to the monitored system.

reservoir. A structure designed to store very large volumes of distribution system water, which may be located underground, in-ground, or at grade.

response action. An action taken by a utility, public health agency or another response partner to minimize the consequences of an undesirable water quality incident. Response actions may include issuing a public notification, changing system operations, or flushing the system.

risk assessment. A method of quantifying the risk of a threat to an asset by evaluating the threat's likelihood of attacking the asset, the probability that the attack will be successful based on the asset's vulnerability to and countermeasures against such an attack, and the consequences that would result from a successful attack. The current standard risk methodology for the water sector is AWWA's J100 manual.

sensor malfunction. A condition in which the data produced by a sensor unit is inaccurate and does not match current conditions.

site. A utility property that includes facilities for storing, treating, or pumping water. The terms "facility" and "site" are used interchangeably in this document, although in practice, it may be possible for a site to include multiple facilities. For example, a large utility site may include elevated storage tank and pump station facilities.

software. A program that runs on a computer and performs certain functions.

SRS Manager. See Water Quality Surveillance and Response System (SRS) Manager.

Supervisory Control and Data Acquisition (SCADA). A system that collects data from various sensors at a drinking water treatment plant and locations in a distribution system and sends this data to a central information management system.

tank. A structure designed to store large volumes of distribution system water, which may be at grade or elevated.

target capability. A level of performance or an outcome for a design element that is necessary for an effective SRS component.

technical requirement. A type of information management requirement that defines system attributes and design features that are often not readily apparent to the end user but are essential to meeting functional requirements or other design constraints. Examples include attributes such as system availability, information security and privacy, back-up and recovery, data storage needs, and integration requirements.

useful life. The period of time that an asset can be economically maintained.

user interface. A visually oriented interface that allows a user to interact with an information management system. A user interface typically facilitates data access and analysis.

valid alert. Alerts due to water contamination, verified water quality incidents, intrusions at utility facilities, or public health incidents.

video analytics. An incident-based video monitoring system that uses algorithms that continuously analyze video images to identify anomalous objects, classify their sizes, characterize their behaviors, and determine their locations.

vulnerability assessment (VA). Assessments required under the Bioterrorism Act of 2002 for all community water systems with a population over 3,300 customers. The purpose of a VA is to identify susceptibility to potential threats and evaluate corrective actions that can reduce or mitigate the risk of serious consequences from adversarial actions.

water quality incident. An incident that results in an undesirable change in water quality (e.g., low residual disinfectant, rusty water, taste & odor, etc.). Contamination incidents are a subset of water quality incidents.

Water Quality Surveillance and Response System (SRS). A system that employs one or more surveillance components to monitor and manage source water and distribution system water quality in real time. An SRS utilizes a variety of data analysis techniques to detect water quality anomalies and generate alerts. Procedures guide the investigation of alerts and the response to validated water quality incidents that might impact operations, public health, or utility infrastructure.

Water Quality Surveillance and Response System (SRS) Manager. A role within an SRS typically filled by a mid- to upper-level manager from a drinking water utility. Responsibilities of this position include receiving notification of valid alerts, coordinating the threat level determination process, integrating information across the different surveillance components, and activating the Consequence Management Plan.

wired technology. A method of transmitting data that uses a solid material such as copper or fiber optic cabling as the transmission media.

wireless technology. A method of transmitting data that uses electromagnetic waves as the transmission media.

Appendix A: Determining Detection and Delay Scores Using Path Analysis

The following is a three-step method for scoring the detection and delay criterion described in Section 3 by analyzing the various paths that an intruder could take to contaminate distribution system water at a facility.

A.1 Developing a Scoring Rationale

The first step in a path analysis is to develop a scoring rationale for detection and delay, which will be applied to each path identified in the second step. **Table A-1** shows an example criterion. The utility has the option of adjusting the scoring rationales to accommodate their system's characteristics.

Table A-1: Example Scoring Rationale

Evaluation Criterion	Scoring Rationale
1. Existing security features – Detection	4 = Sensors are not installed along the path. 3 = Sensors are installed on some segments of the path. 2 = Sensors are installed on most segments of the path. 1 = Sensors are installed on all segments of the path. Note: Subtract 1 from the score if video is included in any segment of the path.
2. Existing security features – Delay	4 = Hardening features are not installed along the path. 3 = Hardening features are installed on some segments of the path. 2 = Hardening features are installed on most segments of the path. 1 = Hardening features are installed on all segments of the path. Note: The delay score may be adjusted based on how difficult it would be for an intruder to overcome a hardening feature, such as climbing an adjacent building to get over a fence.

A.2 Determining Paths

The second step in a path analysis is to determine the various paths that an intruder could take to access the distribution system water. Four paths are shown in **Figure A-1** for an example utility facility. In general, it is not necessary to consider all possible paths, only those that represent the most efficient pathways to the target through all combinations of barriers.

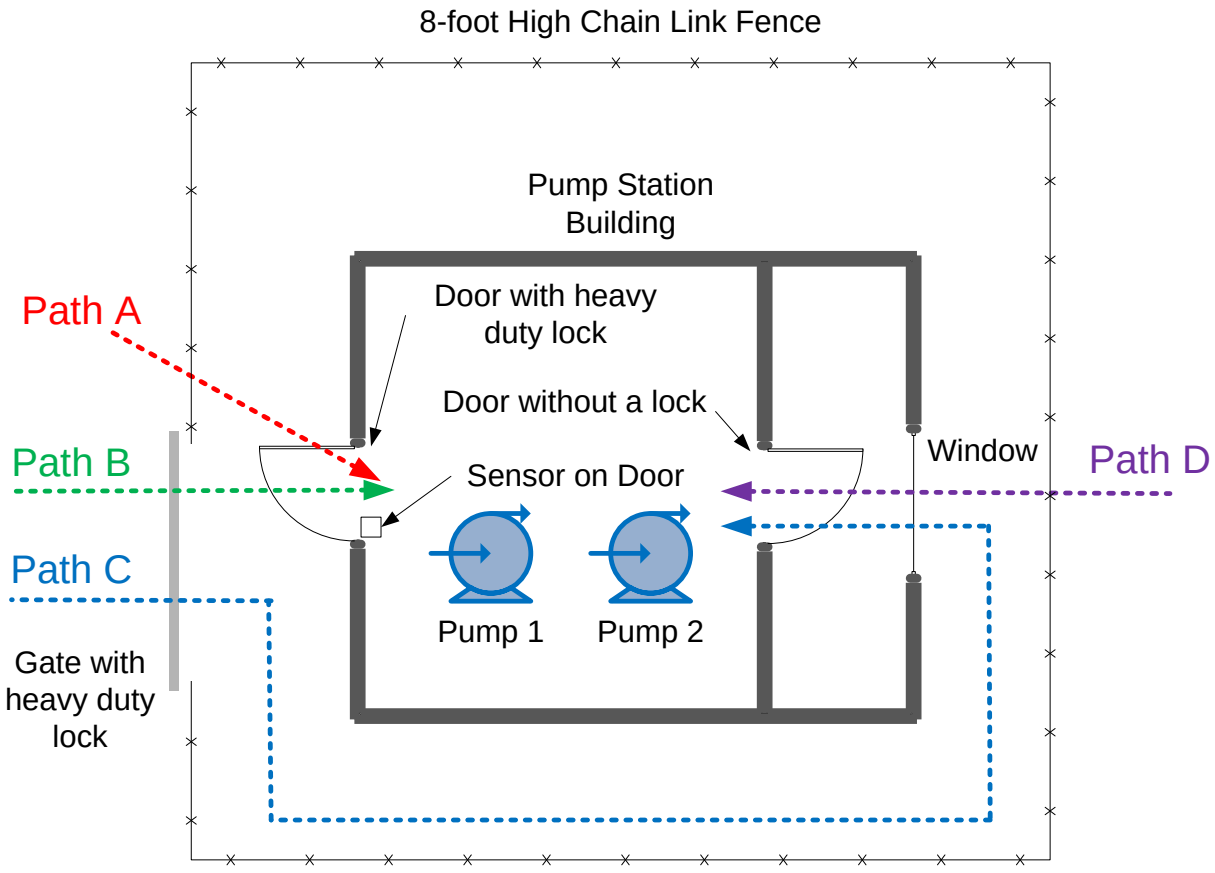


Figure A-1. Path Analysis Example

A.3 Scoring Each Path

Lastly, each path is analyzed for its delay and detection characteristics and scored based on the scoring rationale established in Table A-1. **Tables A-2** and **A-3** describe the scoring for each path and the average values for detection and delay.

Table A-2: Scoring Each Path for Detection Characteristics

Path	Detection Characteristics
A	• Fence does not have a perimeter detection system. • Exterior door is equipped with a sensor. • Only one of 2 segments of Path A have detection equipment, so detection score = 3.
B	• Gate does not have a sensor. • Exterior door is secured with a heavy duty lock. • Only one of 2 segments of Path B have detection equipment, so detection score = 3.
C	• Gate does not have a sensor. • Window does not have a sensor. • Interior door does not have a sensor. • None of three segments of Path C has detection equipment, so detection score = 4.
D	• Fence does not have a perimeter detection system. • Window does not have a sensor. • Interior door does not have a sensor. • None of three segments of Path D has detection equipment, so detection score = 4.
Average	The average detection score is (3+3+4+4)/4 = 3.5.

Table A-3: Scoring Each Path for Delay Characteristics

Path	Delay Characteristics
A	• Fence is 8’ high. • Exterior door is secured with a heavy-duty lock. • Both segments of Path A are hardened, so delay score = 1.
B	• Gate is secured with a heavy-duty lock. • Exterior door is secured with a heavy-duty lock. • Both segments of Path B are hardened, so delay score = 1.
C	• Gate is secured with a heavy-duty lock. • Window is made of standard-duty glass. • Interior door does not have a lock. • One of three segments of Path C is hardened, so delay score = 3.
D	• Fence is 8’ high. • Window is made of standard-duty glass. • Interior door does not have a lock. • One of three segments of Path D is hardened, so delay score = 3.
Average	The average delay score is (1+1+3+3)/4 = 2.

Thus, the detection and delay scores for this example pump station should be 3.5 and 2, respectively, when applying the method described in Section 3 to prioritize facilities for ESM enhancements. A path analysis is useful for detailed analysis of the security features at a facility but can be time consuming for larger facilities with numerous points of entry and multiple locations where an intruder could access distribution system water. However, the advantage of the path analysis is it can accurately identify exactly where physical security enhancements are needed. In the above example, an intruder could access distribution system water undetected via Path C and Path D. At minimum, intrusion detection is needed on the window to optimally achieve the ESM design goals of detecting intrusions that could lead to water contamination incidents and enhancing physical security.