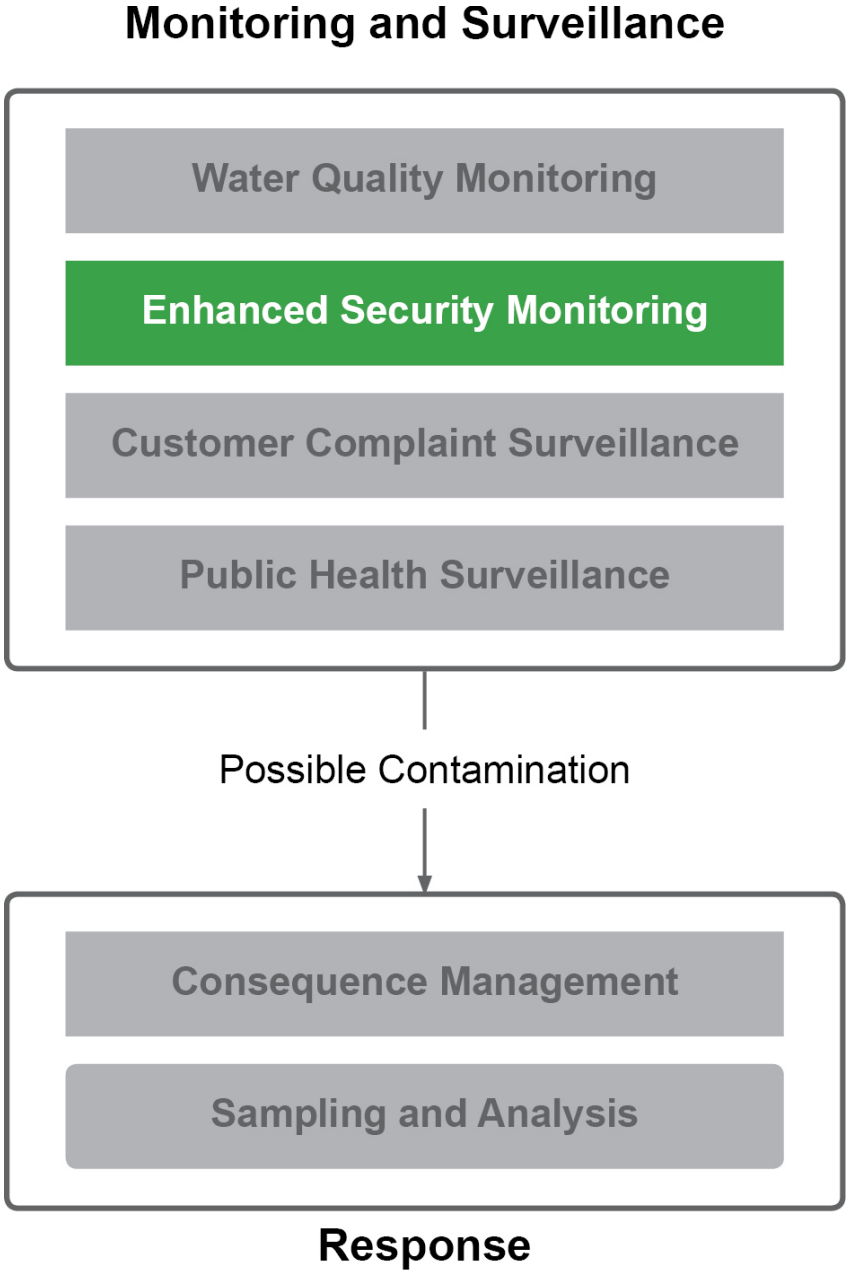
United States Environmental Protection Agency

Water Security Initiative: Evaluation of the Enhanced Security Monitoring Component of the Cincinnati Contamination Warning System Pilot



Office of Water (MC-140) EPA-817-R-14-001C April 2014

Disclaimer

The Water Security Division of the Office of Ground Water and Drinking Water has reviewed and approved this document for publication. This document does not impose legally binding requirements on any party. The findings in this report are intended solely to recommend or suggest and do not imply any requirements. Neither the U.S. Government nor any of its employees, contractors or their employees make any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use of or the results of such use of any information, apparatus, product, or process discussed in this report or represents that its use by such party would not infringe on privately owned rights. Mention of trade names or commercial products does not constitute endorsement or recommendation for use.

Questions concerning this document should be addressed to:

Nelson Mix, PE, CHMM
U.S. EPA Water Security Division
1200 Pennsylvania Ave, NW
Mail Code 4608T
Washington, DC 20460
(202) 564-7951
Mix.Nelson@epa.gov

or

Steve Allgeier
U.S. EPA Water Security Division
26 West Martin Luther King Drive
Mail Code 140
Cincinnati, OH 45268
(513) 569-7131
Allgeier.Steve@epa.gov

Acknowledgements

The Water Security Division of the Office of Ground Water and Drinking Water would like to recognize the following individuals and organizations for their assistance, contributions, and review during the development of this document.

- Jim Holly, Greater Cincinnati Water Works
- Yeongho Lee, Greater Cincinnati Water Works
- Jeff Swertfeger, Greater Cincinnati Water Works
- Jim Golembeski, Philadelphia Water Department
- Kyle Parks, Dallas Public Works
- Curt Baranowski, U.S. Environmental Protection Agency
- David Harvey, U.S. Environmental Protection Agency

Executive Summary

The goal of the Water Security Initiative (WSI) is to design and demonstrate an effective multi-component warning system for timely detection and response to drinking water contamination threats and incidents. A contamination warning system (CWS) integrates information from multiple monitoring and surveillance components to alert the water utility to possible contamination, and uses a consequence management plan to guide response actions.

System design objectives for an effective CWS are: spatial coverage, contaminant coverage, alert occurrence, timeliness of detection and response, operational reliability and sustainability. Metrics for the enhanced security monitoring (ESM) component were defined relative to the system metrics common to all components in the CWS, but the component metric definitions provide an additional level of detail relevant to the ESM component. Evaluation techniques used to quantitatively or qualitatively evaluate each of the metrics include analysis of empirical data from routine operations, drills and exercises, modeling and simulations, forums, and an analysis of lifecycle costs. This report describes the evaluation of data collected from the ESM component from the period of January 2008 – June 2010.

The major outputs from the evaluation of the Cincinnati pilot include:

1. *Cincinnati Pilot System Status*, which describes the post-implementation status of the Cincinnati pilot following the installation of all monitoring and surveillance components.
2. *Component Evaluations*, which include analysis of performance metrics for each component of the Cincinnati pilot.
3. *System Evaluation*, which integrates the results of the component evaluations, the simulation study, and the benefit-cost analysis.

The reports that present the results from the evaluation of the system and each of its six components are available in an Adobe portfolio, *Water Security Initiative: Comprehensive Evaluation of the Cincinnati Contamination Warning System Pilot* (USEPA 2014a).

Enhanced Security Monitoring Component Design

Unlike traditional hardening practices, ESM includes systems, equipment and procedures to detect intrusions at high risk facilities in real time and respond promptly to prevent, interrupt, or reduce the impact of an attempted contamination incident.

ESM includes intrusion sensors and video monitoring equipment to detect intrusions that could precede a potential contamination incident. Intrusion alerts and video are transmitted to the Greater Cincinnati Water Works (GCWW) Control Center, where alerts are continuously monitored by utility personnel. After an incident is detected, assessment procedures include the use of video cameras to view the intrusion at video-monitored sites, and onsite investigation methods to determine whether contamination is Possible. Additionally, video evidence can be used to minimize unnecessary site investigations when invalid alerts are observed. Under the contamination warning system model, ESM is designed to help discern between intrusions that may be related to a contamination incident and those resulting from benign causes (e.g., an employee forgetting to call in).

The ESM design also includes procedures for responding to intrusions reported by eyewitnesses and threat notifications from perpetrators.

For more information on ESM design, see Section 2.0. A summary of the results used to evaluate whether the ESM met each of the design objectives relevant to this component is provided below.

Methodology

Several methods were used to evaluate ESM performance. Data was tracked over time to illustrate the change in performance as the component evolved during the evaluation period. Statistical methods were also used to summarize large volumes of data collected over either the entire or various segments of the evaluation period. Data was also evaluated and summarized for each reporting period over the evaluation period. In this evaluation, the term reporting period is used to refer to one month of data that spans from the 16th of the indicated month to the 15th of the following month. Thus, the January 2008 reporting period refers to the data collected between January 16th 2008 and February 15th 2008. Additionally, four drills designed around mock contamination incidents were used to practice and evaluate the full range of procedures, from initial detection through response.

Because there were no contamination incidents during the evaluation period, there is no empirical data to fully evaluate the detection capabilities of the component. To fill this gap, a computer model of the Cincinnati CWS was developed and challenged with a large ensemble of simulated contamination incidents in a simulation study. An ensemble of 2,015 contamination scenarios representing a broad range of contaminants and injection locations throughout the distribution system was used to evaluate the effectiveness of the CWS in minimizing public health and utility infrastructure consequences. The simulations were also used for a benefit-cost analysis, which compares the monetized value of costs and benefits and calculates the net present value of the CWS. Costs include implementation costs and routine operation and maintenance labor and expenses, which were assumed over a 20 year lifecycle of the CWS. Benefits included reduction in consequences (illness, fatalities and infrastructure damage) and dual-use benefits from routine operations.

Design Objective: Spatial Coverage

ESM was limited in its ability to detect contamination incidents throughout the distribution system since only specific utility locations are monitored for intrusions that may lead to contamination. However, the sites that were monitored by ESM have the potential to impact a large portion of the distribution system and general population, indicating the importance of monitoring these locations. Overall, the simulation model indicated that the ESM sites covered water supplied to 99 percent of the retail population and 96 percent of the retail service area. The model also showed that the three ESM pump station sites supplied water to 81 to 93 percent of the retail service population and 70 to 80 percent of the retail service area. These relatively large populations and wide service areas supported the design decision to install video monitoring equipment at these three high-risk sites. For more information on spatial coverage and the simulation model see Sections 3.3 and 6.2.

Design Objective: Contaminant Coverage

ESM was primarily concerned with detecting and responding to the physical intrusions which could have led to a potential contamination incident. As a result, the identification of a specific contaminant and recognition of a contaminant's class were not significant considerations during the design of the component's monitoring equipment. However, a contaminant's volume and method of injection were considered when designing ESM enhancements and when developing scenarios to challenge the ESM component of the CWS simulation model. For more information on contaminant coverage see Sections 4.3 and 5.3.

Design Objective: Alert Occurrence

Alert occurrence tracks the frequency of alerts to determine how well the security equipment and procedures discriminate between real intrusions and invalid alerts caused by environmental factors (wind, etc) or utility employees/contractors not following security procedures. Metrics for this design objective include both invalid and valid alert rates, and were characterized using empirical data gathered during the real-time monitoring phase. Invalid alerts occurred frequently at the beginning of the evaluation period due primarily to communication-related errors. The invalid alerts caused by utility employees or contractors not following security procedures resulted in average invalid alert rates of 0.42 door/hatch props per 100 valid entries per door, 1.4 no call-in incidents per 100 valid entries at video sites, and 0.23 no call-in incidents per 100 entries at non-video sites. All ESM intrusion detection devices performed better than the industry standard minimum of 90 days between invalid alerts (*Guideline for the Physical Security of Water Utilities*, ASCE/AWWA, 2006). Area motion sensors were the most prone to invalid alerts at 136 days between alerts, and door/hatch sensors were the least prone at 1,168 days between invalid alerts. For more information on alert occurrence see Sections 4.4, 5.4 and 6.4.

Design Objective: Timeliness of Detection

For ESM, the timeliness of detection metrics measured the amount of time required to perform key steps in the investigation to determine a Possible contamination incident. Factors that impact this objective include: time for alert transmission, time to recognize alerts and time to investigate alerts. These metrics were characterized for invalid alerts using empirical data. Average times for ESM investigation steps included five seconds for intrusion alert transmission, 3.2 minutes for video clip viewing and 26 minutes for validation of Possible contamination. The average times for video clip transmission were one to three minutes using digital cellular communications and 37 seconds using T-carrier 1 (T1) or digital subscriber line (DSL) connections.

Data from ESM drills was used to evaluate the time required to investigate valid alerts. **Figure ES-1** summarizes the average times for the investigation steps during the four ESM drills that were conducted**.** The average total time to investigate an ESM alert was 40 minutes, with a range of 35 to 50 minutes.

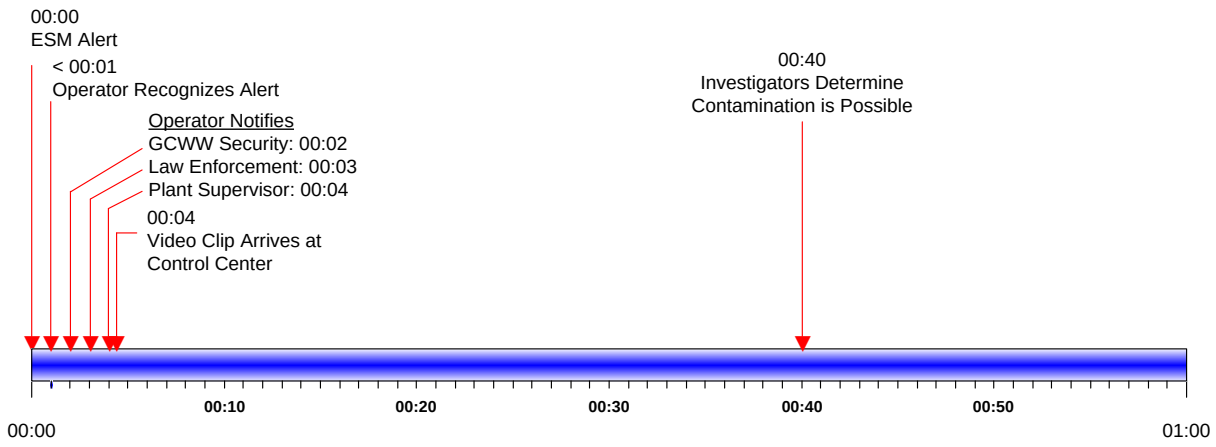


Figure ES-1. Timeline Progression of Alert Investigations during ESM Drills

Data from the ESM drills were used to develop input parameters for the simulation model, specifically the time to validate Possible contamination, the time to interrupt an injection and duration of an uninterrupted injection values. The model results demonstrated two critical benefits of installing video at a site: earlier

determination that contamination is Possible and quicker potential interruption of an injection. For more information on timeliness of detection see Sections 4.5, 5.5 and 6.5.

Design Objective: Operational Reliability

Operational reliability metrics quantify the percent of time that the ESM component is working as designed. Availability, data completeness, and invalid alert metrics were used to evaluate the reliability of the ESM system, as measured by the analysis of empirical data. The ESM component exhibited excellent operational reliability during the evaluation period. Intrusion alert and video communications systems, intrusion detection equipment and video equipment had availabilities above 99 percent. The only exceptions were for outages caused by the digital cellular provider and the pan-tilt-zoom cameras failing as they approached the end of their design life. For more information on operational reliability see Sections 4.6, 5.6 and 6.6.

Design Objective: Sustainability

Sustainability is a key objective in the design of a CWS and each of its components, which for the purpose of this evaluation is defined in terms of the cost-benefit trade-off. Costs are estimated over the 20-year life cycle of the system to provide an estimate of the total cost of ownership and include the implementation costs, enhancement costs, operation and maintenance costs, renewal and replacement costs, and the salvage value. The benefits derived from the system are defined in terms of primary and dual-use benefits. Metrics that were evaluated under this design objective include: costs, benefits and acceptability. The costs used in the calculation of the 20-year lifecycle costs for the ESM component are presented in **Table ES-1**. These costs were tracked as empirical data during the design and implementation phase of project design, and were analyzed through a benefit-cost analysis. It is important to note that the Cincinnati CWS was a research effort, and as such incurred higher costs than would be expected for a typical large utility installation.

Table ES-1. Cost Elements used in the Calculation of the 20-Year Lifecycle Cost

Parameter	Value
Implementation Costs	$1,388,869
Annual O&M Costs	$38,002
Renewal and Replacement Costs[1]	$257,332
Salvage Value[1]	($19,124)

[1] Calculated using major pieces of equipment.

To calculate the total 20-year lifecycle cost of the ESM component, all costs and monetized benefits were adjusted to 2007 dollars using the change in the Consumer Price Index between 2007 and the year that the cost or benefit was realized. Subsequently, the implementation costs, renewal and replacement costs, and annual O&M costs were combined to determine the total lifecycle cost:

ESM Total Lifecycle Cost: **$2,195,081**

A similar ESM implementation at another utility should be less expensive when compared to the Cincinnati pilot as it could benefit from lessons learned and would not incur research-related costs.

Dual-use benefits and user acceptability were evaluated through documentation of qualitative data during drills and exercises, and during forums with the utility including lessons learned workshops. Dual-use benefits identified included: 1) more efficient investigations, staff utilization and education; 2) deterrent to trespassing, vandalism and theft; 3) improved integration with law enforcement; and 4) increased employee safety. User acceptability was demonstrated through 100% utility participation in drills and

exercises, which required substantially more effort than routine investigations. GCWW personnel reported that they were able to better appreciate and understand standard operating procedures (SOPs) through responding to simulated water contamination incidents. Finally, the GCWW has maintained the ESM equipment since the conclusion of the Cooperative Research and Development Agreement in June 2009, and has instructed employees to implement the Cincinnati Pilot Operational Strategy for suspected intrusions at all sites within the GCWW service area. For more information on sustainability, see Section 6.7.

Table of Contents

List of Figures

List of Tables

Section 1.0: Introduction

The purpose of this document is to describe the evaluation of the enhanced security monitoring (ESM) component of the Cincinnati pilot, the first such pilot deployed by the US Environmental Protection Agency's (EPA) Water Security Initiative (WSI). This evaluation was implemented by examining the performance of the ESM component relative to the design objectives established for the contamination warning system (CWS).

1.1 CWS Design Objectives

The Cincinnati CWS was designed to meet six overarching objectives, which are described in detail in *WaterSentinel System Architecture* (USEPA, 2005) and are presented briefly below:

- **Spatial Coverage**. The objective for spatial coverage is to monitor the entire population served by the drinking water utility. It depends on the location and density of monitoring points in the distribution system, and the hydraulic connectivity of each monitoring location to downstream regions and populations.
- **Contaminant Coverage**. The objective for contaminant coverage is to provide detection capabilities for all priority contaminants. This design objective is further defined by binning the priority contaminants into 12 classes according to the means by which they might be detected (USEPA, 2005). Use of these detection classes to inform design provides more comprehensive coverage of contaminants of concern than would be achieved by designing the system around a handful of specific contaminants. Contaminant coverage depends on the specific data streams analyzed by each monitoring and surveillance component, as well as the specific attributes of each component.
- **Alert Occurrence**. The objective of this aspect of system design is to minimize the rate of invalid alerts (alerts unrelated to contamination or other anomalous conditions) while maintaining the ability of the system to detect real incidents. It depends on the quality of the underlying data as well as the event detection systems that continuously analyze that data for anomalies.
- **Timeliness of Detection and Response**. The objective of this aspect of system design is to provide initial detection of a contamination incident in a timeframe that allows for the implementation of response actions that result in significant consequences reduction. For monitoring and surveillance components, such as ESM, this design objective addresses only detection of an anomaly and investigation of the subsequent alert. Timeliness of response is addressed under consequence management and sampling and analysis.
- **Operational Reliability**. The objective for operational reliability is to achieve a sufficiently high degree of system availability, data completeness and data accuracy such that the probability of missing a contamination incident becomes exceedingly low. It depends on the redundancies built into the CWS and each of its components.
- **Sustainability**. The objective of this aspect of system design is to develop a CWS that provides benefits to the utility and partner organizations while minimizing the costs. This can be achieved through leveraging existing systems and resources that can be readily integrated into the design of the CWS. Furthermore, a design that results in dual-use applications that benefit the utility in day-to-day operations, while also providing the capability to detect intentional or accidental contamination incidents, will also improve sustainability.

The design objectives provide a basis for evaluation of each component, in this case ESM, as well as the entire integrated system. Because the deployment of a drinking water CWS is a new concept, design

standards or benchmarks are unavailable. Thus, it is necessary to evaluate the performance of the pilot CWS in Cincinnati against the design objectives relative to the baseline state of the utility prior to CWS deployment.

1.2 Role of ESM in the Cincinnati CWS

Under the WSI, a multi-component design was developed to meet the above design objectives. Specifically, the WSI CWS architecture utilizes four monitoring and surveillance components common to the drinking water industry and public health sector: ESM, water quality monitoring, customer complaint surveillance, and public health surveillance. Information from these four components are integrated under a consequence management plan, which is supported by sampling and analysis activities, to establish the credibility of Possible contamination incidents and to initiate response actions intended to mitigate consequences.

As one of the four monitoring and surveillance components, ESM includes systems, equipment and procedures to detect intrusions at high risk facilities in real time and respond promptly to prevent, interrupt, or reduce the impact of an attempted contamination incident. If an intrusion is detected, an alert is generated and assessment procedures, such as video footage review and onsite investigations, are used to determine whether the alert can be explained by a benign cause (e.g., an employee forgetting to call in). If it cannot, contamination is considered Possible, and the consequence management plan is activated to determine the credibility of the incident and respond appropriately.

1.3 Objectives

The overall objective of this report is to demonstrate how well the ESM component functioned as part of the CWS deployed in Cincinnati (i.e., how effectively the component achieved the design objectives). This evaluation will describe how the deployed ESM component could reliably detect a possible drinking water contamination incident based on the operational strategy established for the Cincinnati pilot. Although no known contamination incidents occurred during the pilot period, data collection during routine operation, drills and exercises, and computer simulations yielded sufficient data to evaluate the performance of the ESM component against each of the stated design objectives. In summary, this document will discuss the approach used for analysis of this information and present the results that characterize the overall operation, performance and sustainability of the ESM component of the Cincinnati CWS.

1.4 Document Organization

This document contains the following sections:

- **Section 2: Overview of the ESM Component**. This section introduces the ESM component of the Cincinnati CWS and describes each of the major design elements that make up the component. A summary of significant modifications to the component that had a demonstrable impact on performance is presented at the end of this section.
- **Section 3: Methodology**. This section describes the data sources and techniques used to evaluate the ESM component.
- **Sections 4 through 6: Evaluation of ESM Performance against the Design Objectives**. Each of these sections addresses one of the design objectives listed in Section 1.1. Each section introduces the metrics that was used to evaluate the ESM component against that design objective. Each supporting evaluation metric is discussed in a dedicated subsection, including an overview of the analysis methodology employed for that metric followed by presentation and

discussion of the results. Each section concludes with a summary of ESM component performance relative to the design objective.

- **Section 7: Summary and Conclusions**. This section provides an assessment of how well the ESM component of the Cincinnati CWS met the design objectives.
- **Section 8: References**. This section lists all sources and documents cited throughout this report.
- **Section 9: Abbreviations**. This section lists all acronyms approved for use in the ESM component evaluation.
- **Section 10: Glossary**. This section defines terms used throughout the ESM component evaluation.

Section 2.0: Overview of the ESM Component

The Cincinnati CWS added security equipment at selected facility locations in the distribution system and modified existing security practices. Prior to the implementation of the CWS, the physical security systems and processes in place for the Greater Cincinnati Water Works (GCWW) distribution facilities were primarily intended to delay entry of unauthorized individuals and detect intrusion. Major enhancements included the placement of intrusion detection equipment at areas with access to the finished drinking water (e.g. hatches and ladders), the addition of video at high-risk pump station locations, and the development of the Cincinnati Pilot Operational Strategy to streamline the processes of alert investigation. The Cincinnati Pilot Operational Strategy for ESM describes the roles and responsibilities of various job functions as well as the standard operating procedures for the employees involved in its operation.

The ESM component of the Cincinnati CWS was fully deployed and operational by May 2007 and a detailed description of the system at this point in the project can be found in *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status* (USEPA, 2008). During the next phase of the Cincinnati Pilot, from February 2008 through June 2010, the system was evaluated and modified in an effort to improve performance. Sections 2.1 through 2.3 provide an overview of the three ESM design elements, with an emphasis on changes to the component during the evaluation period. Section 2.4 summarizes all significant modifications to the ESM component that are relevant to the interpretation of the evaluation results presented in this report. The three main ESM design elements for the Cincinnati Pilot are described in greater detail in **Table 2-1.**

Table 2-1. Enhanced Security Monitoring Design Element

Design Element	Description
1. Physical Security Equipment	Door/hatch sensors, motion sensors and cameras designed and installed to detect intrusion and help discriminate between potential contamination threats and routine access to facilities.
2. Data Management and Communications	Communication technology which would allow video of sufficiently good quality to be transmitted in a time frame which could assist in determining if a contamination incident occurred.
3. Component Response Procedures	Written standard operating procedures exist for every step in responding to a security monitoring alert. These procedures outline effective and timely communications, including clear guidance on appropriate response actions for stopping or limiting the spread of a contamination incident.

2.1 Physical Security Equipment

Monitoring equipment was installed at three pumping stations, four finished water reservoirs (one underground and three above-ground) and five elevated or ground storage tanks. The pumping stations were equipped with door/hatch sensors, motion sensors, video cameras and a video monitoring system to supplement the existing door sensors. Hardening the security of the vents was performed at reservoir sites in addition to the installation of monitoring equipment. The hardened vents were equipped with intrusion sensors on the access hatches and a level switch to detect an attempt at flooding the enclosure to introduce contamination into the finished water. The ESM improvements were in addition to the existing door/hatch sensors at the pumping stations, reservoirs, and elevated and ground storage tanks.

2.2 Data Management and Communications

Data management systems and communications were installed to transmit intrusion alert and video data from the remote ESM sites to the utility control center. **Figure 2-1** contrasts the Pre-Existing GCWW Supervisory Control and Data Acquisition (SCADA) Protected Network with Post-ESM enhancements that resulted in all video monitored ESM locations using the Water Security Parallel SCADA Protected Network. This was specifically designed for the CWS and was isolated from the GCWW SCADA Protected Network. The video monitored ESM sites initially used a secure digital cellular network to transmit intrusion alert and video data from the remote sites to operator workstations at the utility control center. The digital cellular network was later replaced by T carrier 1 (T1) and digital subscriber lines (DSL) due to issues encountered regarding video data transmission. (See Section 2.4 regarding this modification.) All non-video monitored ESM locations used the existing GCWW network for transmitting intrusion alert data from the remote sites to operator workstations in the utility control center.

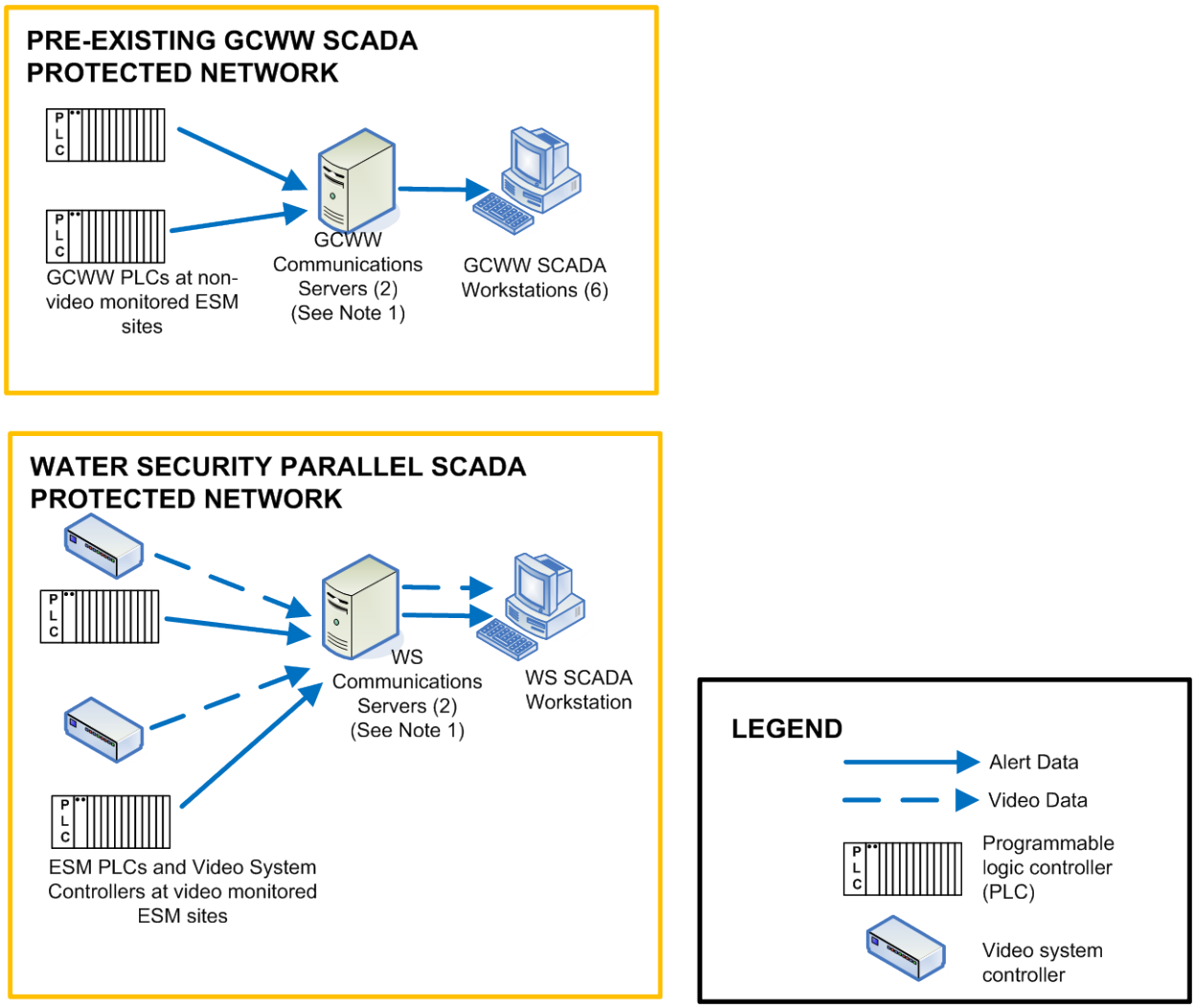


Figure 2-1. ESM Communication Networks

Note 1: Only the ESM portions of the GCWW SCADA Protected Network and Water Security Parallel SCADA Protected Network are shown.

The GCWW and Water Security SCADA communications servers host Human Machine Interface (HMI) software to monitor and control the ESM systems via their respective SCADA workstations located in the utility control center. There is also a Water Security SCADA workstation in the security control center for security staff use. The Water Security System SCADA HMI application provides user interfaces that allow operators and security staff to view intrusion alerts, video clips of intrusions and current camera images; select the refresh rate of the current camera images, select a camera preset for pan-tilt-zoom (PTZ) cameras, and arm/disarm the intrusion alert system at each ESM site. The GCWW SCADA HMI provides user interfaces that allow operators to view intrusion alerts at non-video monitored ESM sites in addition to their primary function of monitoring and controlling the water treatment and distribution systems. The communications servers are also referred to as input/output (I/O) servers.

2.3 Component Response Procedures

When an intrusion is detected at an ESM site, GCWW implements the Cincinnati Pilot Operational Strategy that guides the initial investigation into potential causes of the alert. This Operational Strategy establishes procedures, roles, responsibilities, information flow paths, and checklists to provide a systematic process for reviewing relevant information to rule out benign causes of the alert. Many GCWW employees with various job functions are involved in the continued operation and maintenance of the ESM component. **Table 2-2** describes the role of various job functions, and corresponding GCWW users, in the routine operation of the ESM component of the Cincinnati CWS.

Specifically the following steps are performed:

- Determine whether the intrusion is a valid entry based on employee call-in logs.
- Determine whether the intrusion is an invalid alert caused by GCWW activity based on video data, when available, or observations of concurrent alerts, if any. **Table 2-3** shows the different indicators of an invalid alert. A detected entry that is not categorized as a valid entry or invalid alert is considered a suspected intrusion.
- GCWW Distribution Division and Security personnel and local law enforcement are dispatched to the site of all suspected intrusions and an investigation checklist is filled out by the control center operator and utility security guard. Each checklist is based on the Cincinnati Pilot Operational Strategy and guides the user through the steps of an investigation. The checklist provides fields for recording incident and event times.
- The operator reviews available video data to assess the nature of the intrusion and potential for tampering or contamination. Any findings are communicated to the on-site investigators.
- Once onsite, the investigators verify site safety, look for signs of intrusion and determine if contamination of the water supply is Possible.
- If investigators determine that contamination is Possible, the Water Utility Emergency Response Manager (WUERM) is contacted.

If the initial investigation does not reveal an obvious cause for the alert, contamination is considered Possible and the investigation is turned over to the WUERM, who will take additional steps to determine whether or not contamination is Credible.

While no major changes were made in the Cincinnati Pilot Operational Strategy during the evaluation period, the process underwent several minor revisions based on the results of drills and exercises and experience with routine operation of the system. Most of the modifications to the operational strategy were clarifications of roles and responsibilities and streamlined the investigation process.

Table 2-2. Roles and Responsibilities for Routine Operation of the ESM Component

GCWW User	Role in Routine Operation of ESM
Control Center Operator	• Receive intrusion alerts. • Make the initial determination regarding whether or not the intrusion alert has detected an apparent intruder. • Notify GCWW Security if there is an apparent intruder. • Notify Plant Supervisor if there is an apparent intruder. • Notify local law enforcement if there is an apparent intruder. • Notify the WEURM if investigators determine that contamination is Possible.
Plant Supervisor	• Investigate, or identify an employee from Distribution Division to investigate, the facility with the intrusion alert for signs of intrusion/contamination along with security personnel (if available) and local law enforcement. • Provide access to the facility for law enforcement officials. • Determine if an intrusion has occurred if the GCWW security guard is not available. • Determine if an intruder had access to the water supply. • Request the GCWW control center operator to contact the WUERM of a Possible contamination incident.
GCWW Security Personnel	• Receive witness accounts of possible intrusion. • Determine if public witness accounts of possible intrusion are legitimate. • Notify the Control Center Operator of a possible intruder due to a witness account. • Investigate the facility with the intrusion alert for an apparent intruder, along with Distribution Division personnel and local law enforcement agency. • Provide access to facility for law enforcement officials. • Log the incident if the investigation determines that either intrusion or access to the water supply did not occur. • Determine if an intrusion has occurred. • Determine if an intrusion has provided access to the water supply if the plant supervisor is not available.
Local law enforcement	• Conduct the onsite investigation of the intrusion alert with GCWW Security, Distribution Division, or both, if warranted.
All GCWW employees	• Notify GCWW Security after witnessing possible intruders.
WUERM	• Assume the lead in the credibility determination process, as outlined in the Cincinnati Pilot Consequence Management Plan, once the Possible contamination incident has been reported. • Implement the Cincinnati Pilot Consequence Management Plan as necessary.

Table 2-3. Invalid Alert Indicators

Intrusion Alert Type	Invalid Alert Indicator	Invalid Alert Type
All Alerts at Video-monitored Sites	Employee is seen in the video clip.	No call-in
Door or hatch	A door intrusion alert or alerts are generated immediately after the system was armed.	Door prop
Area motion sensor	Video clip showed nothing in the area monitored by the motion sensor.	Equipment-caused
Ladder	A radio fault or tank water level alert accompanies a ladder intrusion alert.[1]	Radio fault caused ladder
Ladder	A door alert does not precede a ladder intrusion alert.[2]	Equipment-caused

Notes:
1. There were two indications of problems with the radio signal at ladder sites. One was a radio fault from the wireless module, and the other was a tank water level alert that occurred within a few seconds of the ladder intrusion alert. When either of these conditions occurred, the alert was considered false and caused by radio issues.
2. The only way for an intruder to gain access to the ladder was to first enter the facility through the door. There were no windows at the ladder facilities. If a door alert did not precede the ladder alert, the alert was considered false, and caused by an issue with the ladder sensor.

2.4 Summary of Significant ESM Component Modifications

The modifications discussed in the previous subsections were implemented to improve the performance of the ESM component. The impact of these component modifications on performance can be observed in the metrics used to evaluate the degree to which the ESM component met the design objectives described in Section 1.1. **Table 2-4** summarizes these modifications and will serve as a reference when discussing the results of the evaluation presented in Sections 4 through 7.

Table 2-4. ESM Component Modifications

ID	Design Element	Component Modification		Date
1	Physical Security Equipment	Modification	The ladder motion sensor power supplies were rewired to the GCWW SCADA uninterruptible power supply (UPS) or replaced by 12 volt direct current UPS units.	March 2008
		Cause	The ladder motion sensors were powered by non-UPS power supplies and the sensors would reboot after loss of power, resulting in invalid alerts.	
2	Physical Security Equipment	Modification	The ladder motion sensors were removed and ladder hatches with contact sensors were installed at elevated storage tanks.	December 5, 2008
		Cause	The Hamilton County Sherriff requested this modification during the ESM Drill 1 debriefing, so law enforcement and emergency responders could have a better idea of potential onsite threats. The ladder hatch provided responders with a more conclusive means of knowing whether an intruder had climbed the ladder and could still be in the upper level of a storage tank.	

ID	Design Element	Component Modification		Date
3	Physical Security Equipment	Modification	A contact switch was installed at a hatch at Pump Station C.	March 5, 2009
		Cause	CWS Full Scale Exercise (FSE) 2 featured a point of contamination at Pump Station C that was not known to the ESM team during the design phase and was therefore left unmonitored. Adding a contact switch to the hatch that allowed access to this point of contamination addressed this vulnerability.	
4	Physical Security Equipment	Modification	The video system server software was upgraded to version 4.0.	June 2008
		Cause	The video system's automatic video clip deletion feature was not available in version 3.0. Upgrading to version 4 allowed video clips stored for a predetermined time to be automatically deleted. This functionality allows for improved disk space management.	
5	Physical Security Equipment	Modification	The data transmission packet size was adjusted in the video monitoring system from 20,000 bytes to 1,400 bytes.	January 6, 2009
		Cause	The video clip packets were not successfully transmitted by the Cincinnati Bell network.	
6	Data Management and Communications	Modification	The GCWW instrument shop raised its SCADA communications antenna from the side to the top of a storage tank.	October 2008
		Cause	GCWW suspected that trees between the storage tank antenna and pump station antenna were interfering with the radio signal, causing radio faults. The GCWW SCADA equipment often sent a false ladder alert when a radio fault occurred.	
7	Data Management and Communications	Modification	Reprogrammed remote telemetry units to wait five seconds after a ladder alert before transmission of ladder alert to the GCWW HMI. If a radio alert occurred during the waiting period, the ladder alert was not transmitted.	December 2008
		Cause	Local radio interference between the storage tank antenna and the pump station antenna caused radio faults. The GCWW SCADA equipment often sent an invalid ladder alert when a radio fault occurred.	
8	Data Management and Communications	Modification	All video system traffic was rerouted through an existing GCWW WAN (Wide Area Network) T1 connection or a newly installed DSL connection. Digital cellular connections from these pump station locations were discontinued.	• PS C: September 24, 2009 • PS B: December 29, 2009 • PS A: January 25, 2010
		Cause	There was a digital cellular network issue that caused all digital cellular video traffic from the video monitored sites to be blocked.	

2.5 Timeline of ESM Development Phases and Evaluation-related Activities

Figure 2-2 presents a summary timeline for deployment of the ESM component, including milestone dates indicating the occurrence of significant component modifications and drills and exercises. The timeline also shows the completion date for design and implementation activities, along with the subsequent real-time monitoring phases of deployment.

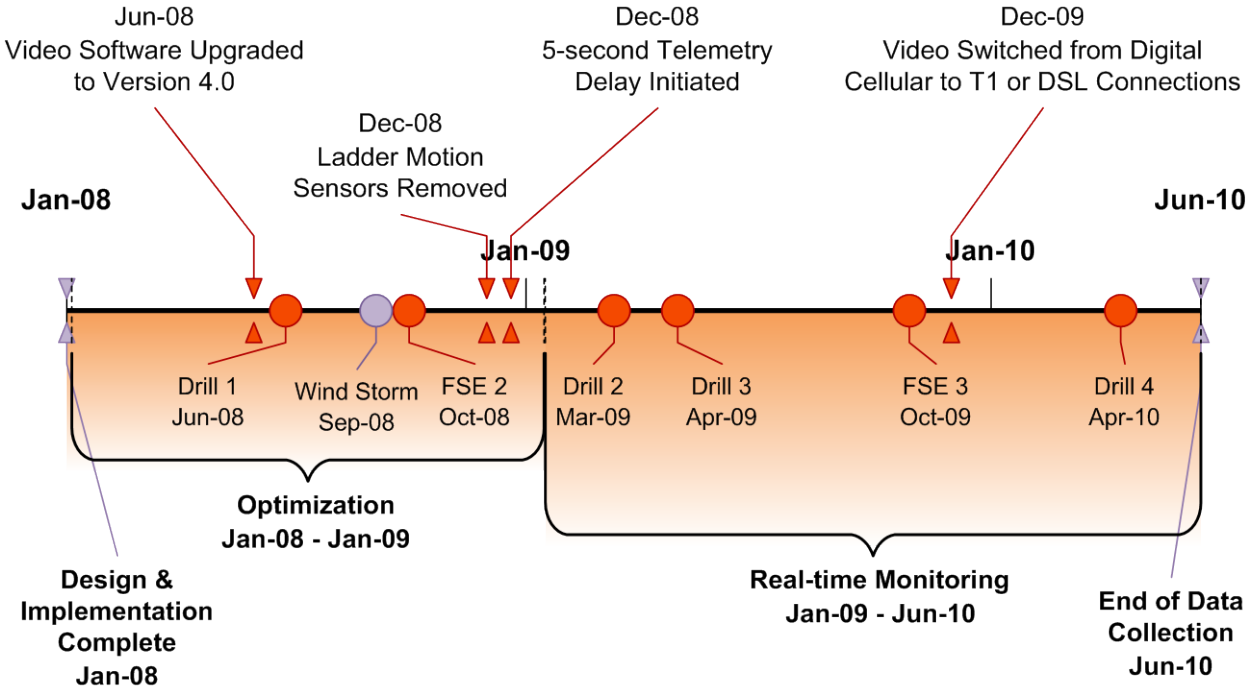


Figure 2-2. Timeline of ESM Component Activities

Section 3.0: Methodology

The following section describes the evaluation techniques for the ESM component. The analysis of the ESM component was conducted using five evaluation techniques: empirical data from routine operations, results from drills and exercises, results from the simulation study, findings from ESM feedback forums, and analysis of lifecycle costs.

3.1 Analysis of Empirical Data from Routine Operations

Data from ESM routine operations was collected monthly from February 16, 2008, to June 10, 2010. In this evaluation, the term "reporting period" is used to refer to a month of data which spans from the 16th of one month to the 15th of the next month. For example, the February 2008 reporting period refers to the data collected between February 16, 2008 and March 15, 2008. Where applicable, results are summarized by reporting period to illustrate temporal trends in the data.

Investigation data and timelines were collected through ESM investigation checklists. To facilitate and document ESM intrusion alert investigations, lead investigators were required to fill out a checklist indicating completion of procedures, summarizing findings and detailing the investigation time. Since full deployment of the ESM system in February 2008, investigators have been expected to respond to intrusion alerts from ESM sites in real time and then to complete checklists.

Empirical data from routine operations were collected by querying electronic logs from the CWS SCADA, ESM video and GCWW SCADA systems throughout the evaluation period. The electronic log data included intrusion alert start and end times, communication system downtimes and equipment downtimes. Data were also obtained from paper call-in logs to document the number of valid entries at each ESM location.

Intrusion alerts were categorized as either valid, indicating an actual intrusion incident, or invalid, indicating no actual intrusion had occurred, or that the intrusion was authorized. An example of an invalid alert would be if a GCWW employee triggered an intrusion alert while performing normal duties but forgot to call the utility control center to verify entry into a facility. Under the same circumstances, if the employee had called in to the control room upon entry, the incident would have been considered an authorized entry into a facility, not an intrusion alert. For analysis, invalid alerts were grouped by root cause: security procedure violations, equipment issues and environmental causes.

3.2 Drills and Exercises

During the evaluation period, drills were conducted to give the GCWW opportunities to practice standard operating procedures for recognizing and responding to ESM intrusion alerts, and to coordinate with external response partners, such as local law enforcement. Post-drill discussions provided the opportunity to refine ESM standard operating procedures that needed further clarification or detail.

Three FSEs were also conducted to allow GCWW and its response partners to practice procedures and coordinating at a multi-component, multi-organizational level. In total, four component drills and two FSEs, which included ESM involvement, were conducted for the purpose of component evaluation. These are discussed below and include:

- ESM Drill 1 (June 26, 2008)
- CWS FSE 2 (October 1, 2008)
- ESM Drill 2 (March 11, 2009)

- ESM Drill 3 (April 30, 2009)
- CWS FSE 3 (October 21, 2009)
- ESM Drill 4 (April 13, 2010)

3.2.1 CWS Full Scale Exercise 2 (October 1, 2008)

Description: A FSE was conducted on October 1, 2008, to test all Cincinnati Pilot CWS components, except ESM. The ESM component played a minor role during FSE 2. GCWW Security personnel were instructed to contact local law enforcement and the Cincinnati Fire Department's Hazardous Materials Removal Team (HazMat) to request assistance in securing the site and conducting the onsite investigation. There was no ESM intrusion during the exercise.

The FSE 2 simulated contamination at an access point at an ESM facility that was not known to the ESM team during the design phase and was therefore left unmonitored. Following this exercise, the ESM team installed equipment to monitor this point of access to the distribution system, as mentioned in Table 2-4.

Relevant Participants: FSE 2 involved only one person from GCWW Security for ESM.

3.2.2 CWS Full Scale Exercise 3 (October 21, 2009)

Description: The FSE 3 scenario involved the injection of a contaminant into the GCWW drinking water system through a fire hydrant. The ESM component played a minor role during FSE 3, and involved one member of GCWW Security conducting a security sweep of the impacted area, checking the status of the Water Information Sharing and Analysis Center (WaterISAC) website, and reporting his findings to the WUERM. This player's actions were not anticipated and were viewed as positive. There was no ESM intrusion planned for this exercise.

Relevant Participants: FSE 3 involved only one person from GCWW Security for ESM.

3.2.3 ESM Drills (1-4)

Description: The objectives of the ESM drills were to evaluate the investigation procedures and the interactions among local law enforcement and GCWW Security and Distribution Division personnel. Drill responders investigated an ESM intrusion alert to determine if drinking water contamination was Possible. For Drills 1 through 3, these objectives were evaluated by initiating an intrusion alert at an ESM facility and observing how GCWW and local law enforcement detected and responded. For ESM Drill 4, these objectives were evaluated by simulating a witness account and verbal threat of a possible intrusion at a GCWW facility. In addition to evaluating procedures and observing interactions, the elapsed times between actions were also recorded. Section 6.5.3 discusses ESM drill results.

Variations among drills included whether the site had video monitoring, whether the intrusion occurred during business or non-business hours, the local law enforcement agency involved and the number of GCWW and law enforcement participants. **Table 3-1** summarizes the variations among drills.

Relevant Participants: ESM relevant participants are listed in Table 3-1.

Table 3-1. ESM Drill Variations

Variations	Drill 1	Drill 2	Drill 3	Drill 4
	6/26/08	3/11/09	4/30/09	4/13/10
Time of Drill (N = Normal business hours, A = After hours)	N	N	N	A
Site has video monitoring?	N	Y	Y	Y[1]
Local Law Enforcement Agency (C = Cincinnati Police, H = Hamilton County Sherriff's Dept., S = Simulated by Drill Observer)	H[2]	C	S	S
Drill Participants				
GCWW Control Center Operator	1	1	1	1
GCWW Plant Supervisor	1	1	1	1
GCWW Security Guard	1	1	1	2
Law Enforcement	1	2	0[3]	0

Notes:
1. The site of ESM Drill 4 had video monitoring, but for the drill scenario, the video monitoring was assumed to be out-of-service.
2. Members of the Anderson Township Fire Department and HazMat and Cincinnati Fire Department/HazMat were drill observers and participated in the post-drill discussion and debriefing.
3. The GCWW Head of Security, a 20+ year veteran of the Cincinnati Police Department, simulated the role of law enforcement.

3.3 Simulation Study

Evaluation of certain design objectives relies on the occurrence of contamination incidents with known and varied characteristics. Because contamination incidents are extremely rare, there is insufficient empirical data to fully evaluate the detection capabilities of the Cincinnati CWS. To fill this gap, a computer model of the Cincinnati CWS was developed and challenged with a large ensemble of simulated contamination incidents in a simulation study. For the ESM component, simulation study data was used to evaluate the following design objectives:

- **Spatial Coverage:** ESM was limited in its ability to detect contamination incidents throughout the distribution system since only specific utility locations are monitored for intrusions that may lead to contamination in the ESM component. However, the consequences if a contamination incident did occur at an ESM site may be widespread. Thus, the CWS model was used to evaluate the population and area impacted if a simulated contamination incident were to occur at each of the ESM-monitored sites. The results were used to analyze the importance of installing ESM equipment at the monitored sites, especially the ones chosen for video monitoring.
- **Timeliness of Detection:** Analyses conducted to evaluate this design objective quantified the time between the start of contaminant injection and when investigators determined that contamination was Possible. Analyses was also conducted to determine if the response times of GCWW and law enforcement personnel to an ESM alert were short enough to prevent or interrupt an intentional contamination incident.

A broad range of contaminant types, producing a range of symptoms, was utilized in the simulation study to characterize the detection capabilities of the monitoring and surveillance components of a CWS. For the purpose of the simulation study, a representative set of 17 contaminants was selected from the comprehensive contaminant list that formed the basis for CWS design. These contaminants are grouped into the broad categories listed below (the number in parentheses indicates the number of contaminants from that category that were simulated during the study).

- Nuisance Chemicals (2): these chemical contaminants have a relatively low toxicity and thus generally do not pose an immediate threat to public health. However, contamination with these chemicals can make the drinking water supply unusable.
- Toxic Chemicals (8): these chemicals are highly toxic and pose an acute risk to public health at relatively low concentrations.
- Biological Agents (7): these contaminants of biological origin include pathogens and toxins that pose a risk to public health at relatively low concentrations.

Development of a detailed CWS model required extensive data collection and documentation of assumptions regarding component and system operations. To the extent possible, model decision logic and parameter values were developed from data generated through operation of the Cincinnati CWS, although input from subject matter experts and available research was utilized as well.

The simulation study used several interrelated models, three of which were relevant to the evaluation of ESM: EPANET, Health Impacts and Human Behavior (HI/HB) and the ESM component model. Each model was further broken down into modules that simulated a particular process or attribute of the model. The function of each of these models, and their relevance to the evaluation of ESM, is discussed below.

EPANET

EPANET is a common hydraulic and water quality modeling application widely used in the water industry to simulate contaminant transport through a drinking water distribution system. In the simulation study, it was used to produce contaminant concentration profiles at every node in the GCWW distribution system model, based on the characteristics of each contamination scenario in the ensemble. The concentration profiles were used to determine the number of miles of pipe contaminated during each scenario, which is one measure of the consequences of that contamination scenario.

Health Impacts and Human Behavior Model

The HI/HB model used the concentration profiles generated by EPANET to simulate exposure of customers in the GCWW service area to contaminated drinking water. Depending on the type of contaminant, exposures occurred during one showering event in the morning (for the inhalation exposure route), or during five consumption events spread throughout the day (for the ingestion exposure route). The HI/HB model used the dose received during exposure events to predict infections, onset of symptoms, health-seeking behaviors of symptomatic customers and fatalities.

The primary output from the HI/HB model was a case table of affected customers. This captured the time at which each affected customer transitioned to mild, moderate and severe symptom categories. Additionally, the HI/HB model outputted the times at which exposed individuals would pursue various health-seeking behaviors, such as visiting their doctor or calling the poison control center. The case table was used to determine the public health consequences of each scenario, specifically the total number of illnesses and fatalities. Furthermore, EPANET and the HI/HB model were run twice for each scenario; once without the CWS in operation and once with the CWS in operation. The paired results from these runs were used to calculate the reduction in consequences due to CWS operations for each simulated contamination scenario.

Enhanced Security Monitoring Component Model

The ESM model consists of two modules: Event Detection and Alert Validation. The Event Detection module was based on the component as deployed and currently operating in the Cincinnati CWS. Site-specific contamination scenarios were developed for each utility facility with ESM capabilities. The simulation study was designed such that scenarios originating at ESM facilities could potentially be interrupted prior to contaminant injection, thus achieving 100% reduction in consequences.

Outputs of the ESM Event Detection module provided inputs to the ESM Alert Validation module. The primary outputs from the ESM Event Detection module were time of alert, location of alert and type of alert (video or non-video sites). This information was used by the ESM Alert Validation module to determine whether contamination was Possible. The procedures included in this module were representative of the alert investigation process that response partners and GCWW utilize in the Cincinnati CWS.

The following assumptions used in the design of the ESM model are important to consider when evaluating the simulation study results presented in this report:

- All contamination scenarios were modeled as "pump and run" incidents. Specifically, it was assumed that the perpetrator would set up the contaminant injection, turn on the pump and then leave. Thus, the first responders (utility/police) eventually discovered the equipment, which quickly established that contamination was Credible or Confirmed.
- ESM always detected scenarios with an injection location at an ESM facility, regardless of the contaminant used in the scenario.
- No benign causes for ESM alerts were found during investigations. The practical implication of this assumption is that in the simulations, the investigation was not prematurely terminated.

3.4 Forums

Throughout implementation and optimization of the ESM system, the EPA, GCWW, and contract support personnel met monthly to review data and component operation, and to discuss modifications. The monthly meetings provided regular, timely feedback on the ESM component. In addition, two lessons learned workshops and an exit interview were conducted as follows:

- **Lessons Learned Workshop, June 17, 2008,** was limited to nine EPA and contractor support personnel responsible for the design and implementation of the ESM. The object of the workshop was to revisit key decisions made during the process and solicit specific feedback on successes and challenges encountered.
- **Lessons Learned Workshop, August 12, 2009,** included 15 EPA, GCWW, and contract support personnel involved in the design, implementation, and daily operation of the ESM system. The object of the workshop was to elicit specific lessons learned information from the Cincinnati Pilot utility through discussions and to gather feedback concerning how lessons learned may be shared with the drinking water sector.
- **Exit Interviews, June 2010,** was limited to key GCWW members of the ESM evaluation team to provide a final opportunity to learn and document GCWW's perceptions and experiences with ESM since assuming full ownership in June 2009.

3.5 Analysis of Lifecycle Costs

A systematic process was used to evaluate the overall cost of the ESM component over the 20-year life cycle of the Cincinnati CWS. The analysis includes implementation costs, component modification costs, annual operations and maintenance (O&M) costs, renewal and replacement costs, and the salvage value of major pieces of equipment at the end of the life cycle.

Implementation costs include labor and other expenditures (equipment, supplies and purchased services) for installing the ESM component. Implementation costs were summarized in *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status* (USEPA, 2008), which was used as a primary data

source for this analysis. In that report, overarching project management costs incurred during the implementation process were captured as a separate line item. However, in this analysis, the project management costs were equally distributed among the six components of the CWS, and are presented as a separate line item for each component. Component modification costs include all labor and expenditures incurred after the completion of major implementation activities in December 2007 that were not attributable to O&M costs. These modification costs were tracked on a monthly basis, summed at the end of the evaluation period and added to the overall implementation costs.

It should be noted that implementation costs for the Cincinnati CWS may be higher than those for other utilities given that this project was the first comprehensive, large-scale CWS of its kind and had no experience base to draw from. Costs that would not likely apply to future implementers (but which were incurred for the Cincinnati CWS) include overhead for EPA and its contractors, cost associated with deploying alternative designs and additional data collection and reporting requirements. Other utilities planning for a similar large-scale CWS installation would have the benefit of lessons learned and an experience base developed through implementation of the Cincinnati CWS.

Annual O&M costs include labor and other expenditures (supplies and purchased services) necessary to operate and maintain the component and investigate alerts. O&M costs were obtained from procurement records, maintenance logs, investigation checklists and training logs. Procurement records provided the cost of supplies, repairs and replacement parts, while maintenance logs tracked the staff time spent maintaining the ESM component. To account for the maintenance of documents, the cost incurred to update documented procedures following drills and exercises conducted during the evaluation phase of the pilot was used to estimate the annualized cost. Investigation checklists and training logs tracked the staff hours spent on investigating alerts and training, respectively. The total O&M costs were annualized by calculating the sum of labor and other expenditures incurred over the course of a year.

Labor hours for both implementation and O&M were tracked over the entire evaluation period. Labor hours were converted to dollars using estimated local labor rates for the different institutions involved in the implementation or O&M of the ESM component.

The renewal and replacement costs are based on the cost of replacing major pieces of equipment at the end of their useful life. The useful life of ESM equipment was estimated using field experience, manufacturer-provided data, and input from subject matter experts. Equipment was assumed to be replaced at the end of its useful life over the 20-year life cycle of the Cincinnati CWS. The salvage value is based on the estimated value of each major piece of equipment at the end of the life cycle of the Cincinnati CWS. The salvage value was estimated for all equipment with an initial value greater than ~$1,000. Straight line depreciation was used to estimate the salvage value for all major pieces of ESM equipment based on the lifespan of each item.

All of the cost parameters described above (implementation costs, component modification costs, O&M costs, renewal and replacement costs, and salvage value) were used to calculate the total 20-year lifecycle cost for the ESM component, as presented in Section 6.7.

Section 4.0: Video Monitored Sites

The following section provides a description of the video monitored sites followed by the results of the evaluation of this data stream. This analysis includes an evaluation of metrics that characterize how these sites achieve the design objectives described in Section 1.1. Specific metrics are described for each of the design objectives.

4.1 Description

The introduction of video monitoring equipment was a significant security enhancement at selected facilities. An event-based video system was chosen over the continuously streaming video system typically found in conventional closed circuit television systems because of its ability to function on low bandwidth communication networks. The system transmitted only short duration video clips in response to a detected security incident, thus imposing only a brief data load on the communications system. Incident detection at the selected locations was provided by contact switches on external doors and by area motion detectors along interior walls that have windows or ventilation louvers. Once a switch or motion detector was triggered, video clips were transmitted to the control center for assessment by operations personnel. Video may provide personnel with visual evidence to validate whether an intrusion or contamination incident is actually occurring without having to conduct an onsite investigation.

4.2 Design Objective: Spatial Coverage

While the ESM video sites each covered only one access point to the distribution system, limiting their detection capability and spatial coverage, the consequences of a contamination incident at these sites would be widespread. Sites that had the highest number of theoretical fatalities from simulated attacks using the Threat Ensemble Vulnerability Assessment (TEVA) analytical framework were chosen for video monitoring ESM enhancements. Using this methodology, three pump stations were selected for ESM video monitoring enhancements. Intrusion detection devices and video monitoring were installed at all points of entry that could allow an intruder access to the water supply at these locations. Pump stations provided an opportunity for testing the limits of the video technology due to their relatively large areas and multiple points of intrusion, which in some cases included long banks of windows.

4.3 Design Objective: Contaminant Coverage

The ESM component did not consider specific contaminants or detection classes of contaminants; however, the volume of contaminants and method of contaminant injection were considered during the ESM design of the video monitored sites. All video monitored sites were pump stations, and the design assumed that a perpetrator would need to gain access to a pressurized line and use an injection pump to overcome the system pressure. In assuming the use of an injection pump, the design also assumed a perpetrator would inject a liquid or slurry from a 55-gallon drum or tank truck. As a result, all points of entry that could allow access for such equipment were monitored.

4.4 Design Objective: Alert Occurrence

4.4.1 Invalid Alerts

For the Cincinnati pilot evaluation, intrusion alerts are categorized as either a valid alert, indicating an actual contamination incident, or an invalid alert. A valid alert is an observed deviation from the base state of a monitored data stream that is not a result of a contamination incident. Invalid alerts are results

from a component that indicate an anomaly is present when there is no contamination or valid alert. Invalid alerts are of great concern to any security system, as they are one of the most significant impediments to system effectiveness. A large number of invalid alerts erodes a utility's confidence in an intrusion alert system and significantly increase the labor hours associated with intrusion alert investigations.

For the ESM component, an invalid alert specifically refers to an intrusion that has been detected, but no actual intrusion has occurred. An example of an invalid alert would be if a GCWW employee triggered an intrusion alert while performing normal duties but forgot to call the utility control center to verify entry into a facility. Under the same circumstances, if the employee had called in to the control room upon entry, the incident would have been considered a valid entry into a facility, not an intrusion alert. For analysis, invalid alerts were grouped by root cause: security procedure violations, equipment issues and environmental causes.

Invalid alerts caused by security procedure violations were categorized as either "no call-in" or "door prop." These security procedure categories were also divided by type of facility, including staffed pump station, frequently visited unstaffed pump station, and infrequently visited unstaffed pump station. Invalid alerts caused by equipment issues were categorized by equipment type, including "door/hatch sensors" and "area motion sensors." Ladder motion sensors at video-monitored sites are discussed in Section 5.4 along with the ladder motion sensors installed at non-video monitored sites. Environmental causes were the third category of invalid alert causes. Because only a handful of invalid alerts were attributed to environmental factors, this category was omitted from the analysis. Only two devices were installed at outdoor locations at video monitored sites.

To generalize the invalid alert data, the security procedure violation metrics were normalized by number of valid entries and, where applicable, number of doors. Invalid alerts due to equipment issues were normalized by the number of sensors.

To implement the above categorizations of invalid alerts, Section 4.4.1 is organized as follows:

- Security Procedure Violations – Door Props
    - Unstaffed and infrequently visited pump station
    - Staffed pump station
    - Unstaffed and frequently visited pump station
- Security Procedure Violations – No Call-Ins
    - Unstaffed and infrequently visited pump station
    - Staffed pump station
    - Unstaffed and frequently visited pump station
- Equipment-Caused Invalid Alert
    - Area Motion Sensors
- Door/Hatch Sensors

Security Procedure Violations-Door Props

Definition: A *security procedure violation* occurred when an employee did not follow security procedures and an invalid alert was generated. A door prop was a type of security procedure invalid alert that occurred when authorized personnel left a door propped open that should have been closed when personnel left the facility.

Standard operating procedures require that the utility control center operator arm the ESM system at a facility after being notified by personnel that they had left the premises. A door prop invalid alert was generated when the ESM system was armed and detected that a secure door was left open. All intrusion detection devices at video sites use the ESM system for displaying intrusion alerts at the utility control

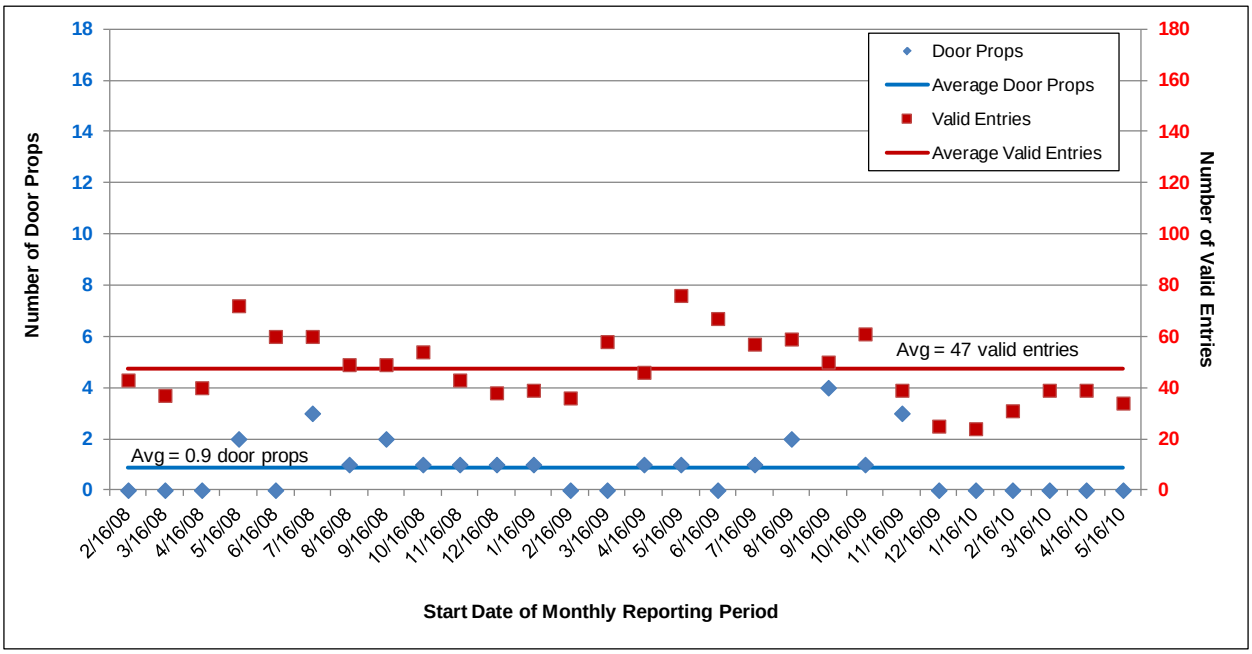
center. The ESM system can be enabled by the utility control center operator using their HMI. If the utility control center operator is not notified, the ESM systems at all video-monitored sites are programmed to arm automatically at a preset time.

Analysis Methodology: This metric was segregated by the site types listed in Section 4.4.1. Each pump station was associated with one of the following categories of facilities:

- Unstaffed and infrequently visited: Pump Station A
- Staffed: Pump Station B
- Unstaffed and frequently visited: Pump Station C

The segregation by site type allowed for individual analysis, as well as comparison among site types. Furthermore, the door prop data was normalized by the number of monitored doors and the number of valid entries to each facility. Facilities with many doors may have a higher probability of door prop instances, just as a frequently visited facility may be more likely to have a door propped open.

Results: **Figure 4-1** shows the door prop metrics for Pump Station A, an unstaffed and infrequently visited pump station where all employees must call the utility control center to announce arrival, regardless of time of day. In general, Pump Station A is visited less often than Pump Stations B and C.



Note: The average number of door props was 0.9, the average number of valid entries 47 per reporting period.

Figure 4-1. Pump Station A (Unstaffed, Infrequently Visited): Door Props

There were, on average, 0.9 door props per reporting period at Pump Station A. There was a relationship between the door props and valid entries. Of the six reporting periods that had an above average number of door props, four reporting periods also had a higher than average number of valid entries.

The number of invalid alerts due to door props did not decrease over the course of the evaluation period, likely because ESM did not implement any significant changes to the security procedures and because of a door that was prone to propping throughout the evaluation period. There was a minimal learning curve associated with training the utility staff on the ESM procedures at this unstaffed facility. The pre-ESM standard operating procedures required that personnel shut all doors at the facility except one seldom-used interior door which had a problem with alignment and only closed when excessive force was applied.

This condition existed before installation of the ESM system at Pump Station A and continued throughout the evaluation period.

There was an increase in door props during the August 2009 to November 2009 reporting periods. Contractors and utility personnel were working on a project that required frequent use of the misaligned door that required excessive force to close. The door was repeatedly left ajar inadvertently, resulting in multiple invalid alerts.

Figure 4-2 shows the door prop metrics for Pump Station B, a staffed pump station. The valid entries shown in Figure 4-2 are the number of after-hours visits that were called in to the utility control center. Since the Pump Station B is normally staffed, employees did not call in during business hours.

There were, on average, more door props and valid entries at the staffed facility compared to the unstaffed, infrequently visited facility. The door props and valid entries for Pump Station B were 3.6 and 63 compared to 0.9 and 47 for Pump Station A.

There was a slight relationship between door props and valid entries at Pump Station B. Of the ten reporting periods that had an above average number of door props, four reporting periods also had a higher than average number of valid entries.

The number of invalid alerts due to door props decreased over the course of the evaluation period for Pump Station B. Training and familiarizing utility and contractor personnel of the new practice of closing all ESM-monitored interior and exterior doors reduced invalid alerts at this staffed facility. With ESM, interior doors that led to the pump floor or anywhere an intruder could access the water were monitored.

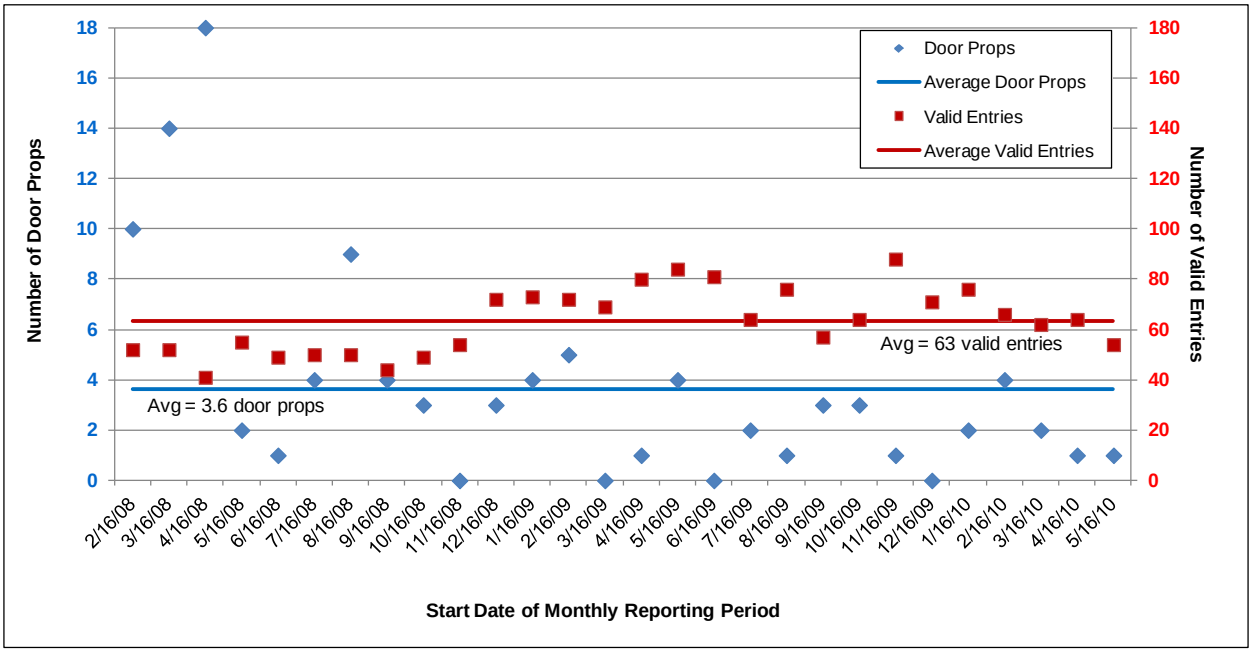
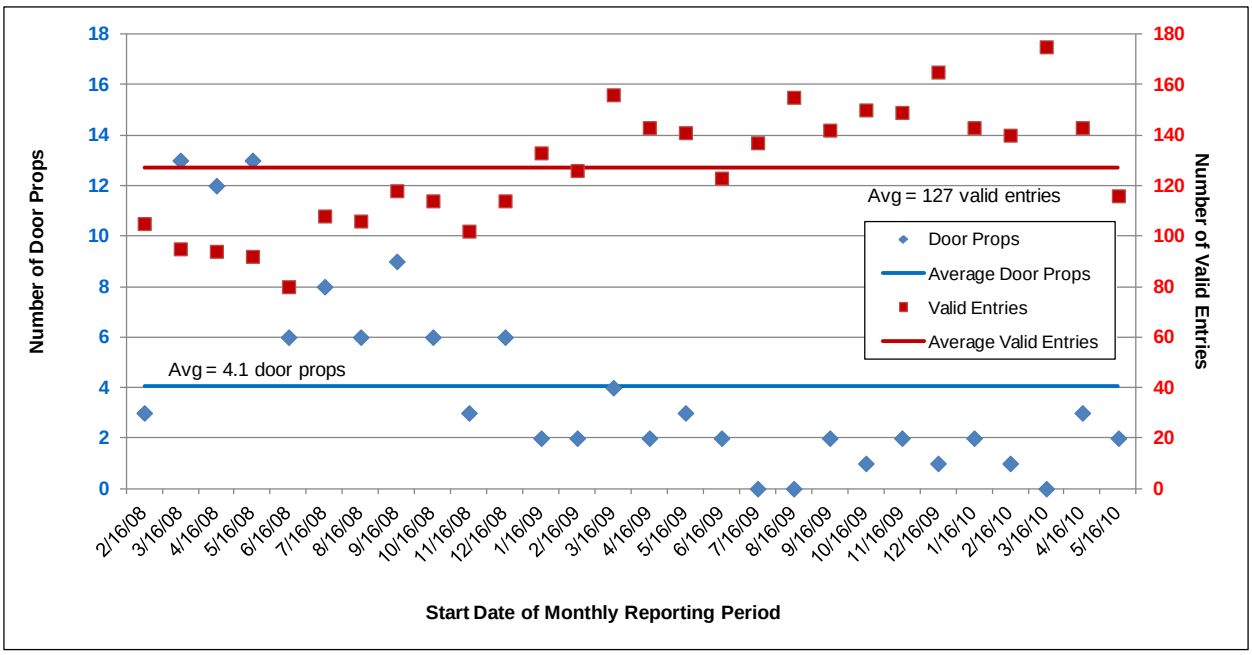


Figure 4-2. Pump Station B (Staffed): Door Props

Figure 4-3 shows the door prop metrics for Pump Station C, an unstaffed and frequently visited pump station where all employees must call the utility control center to announce arrival, regardless of time of day. Although Pump Station C is no longer staffed, utility employees and contractors visit the site often for capital improvements, maintenance work and training.



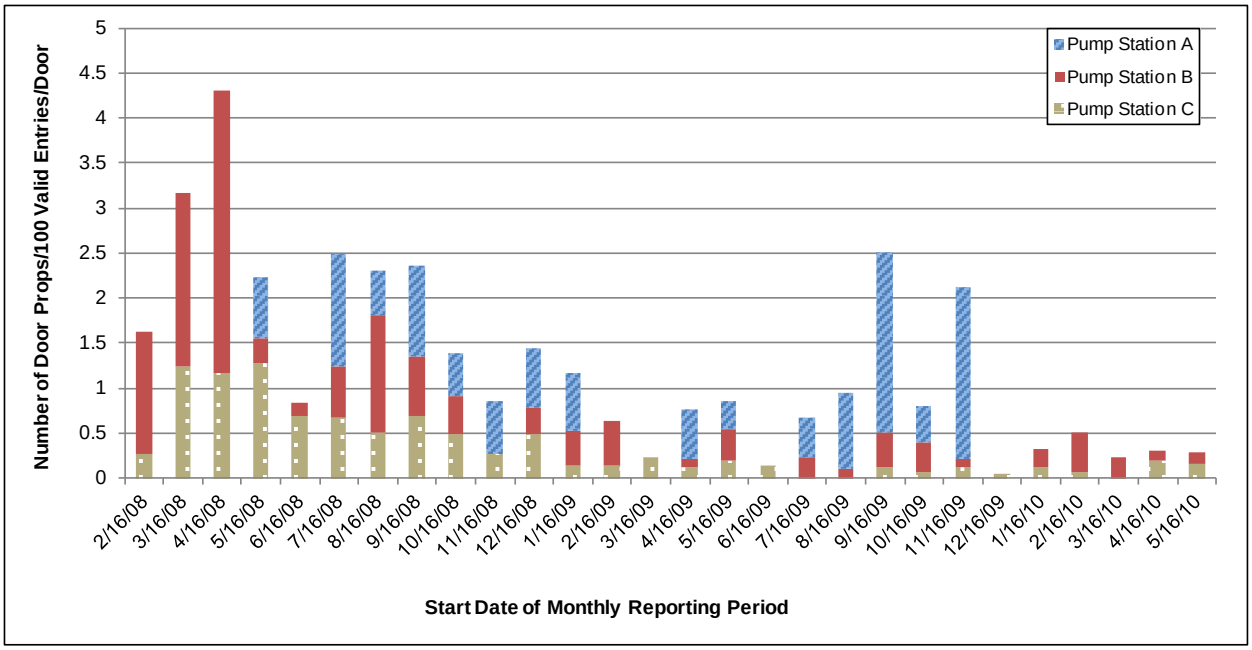
Note: There was a noticeable downward trend in door props over the evaluation period.

Figure 4-3. Pump Station C (Unstaffed, Frequently Visited): Door Props

There were, on average, more valid entries and more door props at the unstaffed, frequently visited facility (4.1 and 127) compared to the unstaffed, infrequently visited facility (0.9 and 47) and staffed facility (3.6 and 63). There was no relationship between door props and valid entries at Pump Station C. Of the nine reporting periods that had an above average number of door props, none had a higher than average number of valid entries.

Similar to Pump Station B, the number of invalid alerts due to door props for Pump Station C decreased over the course of the evaluation period. Training and familiarizing utility and contractor personnel of the new practice of closing all ESM-monitored interior and exterior doors reduced invalid alerts at this staffed facility. Before ESM, only exterior doors to a pump station were monitored. With ESM, interior doors that led to the pump floor or anywhere an intruder could access the water were monitored.

Figure 4-4 shows the door prop metrics normalized by number of valid entries and monitored doors at each pump station. The normalization factors were chosen because a larger number of valid entries and monitored doors could increase the probability of door prop occurrence. Furthermore, each pump station had different numbers of valid entries and monitored doors. **Table 4-1** summarizes the data shown in Figure 4-4.



Note: Employee education reduced the number of door props over time, except at Pump Station A where there were no new standard practices as a result of ESM.

Figure 4-4. Pump Stations: Door Props/100 Valid Entries/Door

Table 4-1. Summary of Pump Station Door Prop Data

Location	Average Door Props per Reporting Period	Normalized Average Door Props per 100 Valid Entries per Door	Average Valid Entries per Reporting Period
Pump Station A (unstaffed, infrequently visited)	0.9	0.44	47
Pump Station B (staffed)	3.6	0.49	63
Pump Station C (unstaffed, frequently visited)	4.1	0.34	127
All Stations, Combined Average	2.9	0.42	79

Pump Station C had the highest average door props per reporting period at 4.1, but after normalization, Pump Station B had the highest average per reporting period per 100 valid entries per door, at 0.49/100 valid entries/door.

The number of normalized door props for Pump Stations B and C tended to decrease over the evaluation period. Training and familiarizing utility and contractor personnel of the new practice of closing all ESM-monitored interior and exterior doors reduced door prop invalid alerts at the facilities. See the discussion following Figures 4-2 and 4-3 for details.

The number of normalized door props for Pump Station A did not decrease over the evaluation period, likely because ESM did not implement any significant changes to the security procedures at Pump Station A. There were above average values of normalized door props at Pump Station A during the August 2009 to November 2009 reporting periods because of project work. The project required frequent use of a door that was prone to propping. See the discussion following Figure 4-1 for details.

The average normalized door props for the Pump Stations ranged from 0.34 to 0.49 door props/100 valid entries/door. When averaging all pump stations, there were 2.9 door props and 79 valid entries per reporting period.

Security Procedure Violations - No Call-Ins

Definition: A *no call-in security procedure violation* occurred when GCWW personnel did not follow established procedures for calling in to the utility control center within a designated time span of entering a facility. An intrusion alert was generated automatically when anyone entered a facility, but an entry was considered valid if an employee called in within a designated time span. Personnel at the utility control center could observe a no call-in incident when the video clip showed an employee entering the facility. If video data were not available, a no call-in incident could be verified when onsite investigators or local law enforcement arrived at the facility and witnessed the employees at the site.

Analysis Methodology: This metric was segregated by the site types listed in Section 4.4.1. The site types include the following categories of facilities:

- Unstaffed and infrequently visited
- Unstaffed and frequently visited
- Staffed

Segregation by site type allowed analysis of each type individually and also comparison among types. Furthermore, the no call-in data were normalized by the number of valid entries to a pump station, since a frequently visited facility would have a higher probability of an employee not calling in.

Results: Figure 4-5 shows the no call-in metrics for Pump Station A, an unstaffed and infrequently visited pump station where all employees must call the utility control center to announce arrival, regardless of time of day. In general, Pump Station A is visited less often than Pump Stations B and C.

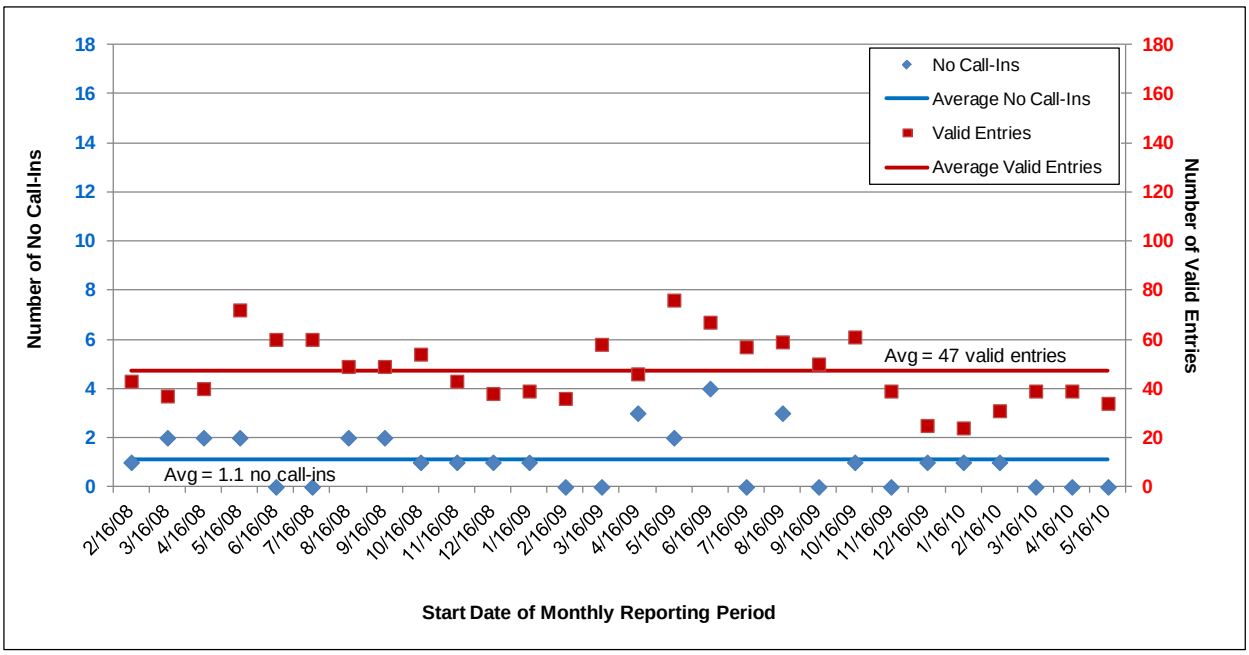


Figure 4-5. Pump Station A (Unstaffed, Infrequently Visited): No Call-Ins

The average number of no call-ins per reporting period was 1.1. There was no relationship between the no call-ins and valid entries. Of the nine reporting periods that had an above average number of no call-ins, only three also had a higher than average number of valid entries. The number of invalid alerts due to no call-ins did not decrease over the course of the evaluation period, likely due to ESM not implementing any significant changes to the utility's call-in procedures.

Figure 4-6 shows the no call-in metrics for Pump Station B, a staffed pump station. The valid entries shown are the number of after-hours visits called in to the utility control center. Since Pump Station B is normally staffed, employees did not call in during business hours.

There were, on average, more no call-ins and valid entries at the staffed facility compared to the unstaffed, infrequently visited facility. The no call-ins and valid entries per reporting period for Pump Station B were 1.6 and 63, compared to 1.1 and 47 for Pump Station A.

There was no relationship between the no call-ins and valid entries at Pump Station B. Of the nine reporting periods that had an above average number of no call-ins, only one reporting period also had a higher than average number of valid entries.

There were a higher number of no call-ins during the first seven reporting periods of the evaluation period compared to the last 21 reporting periods. There were no significant changes to the utility's call-in policy during the evaluation that could have affected the frequency of no call-ins. However, the utility's efforts to reiterate the call-in policy to employees was an ongoing process.

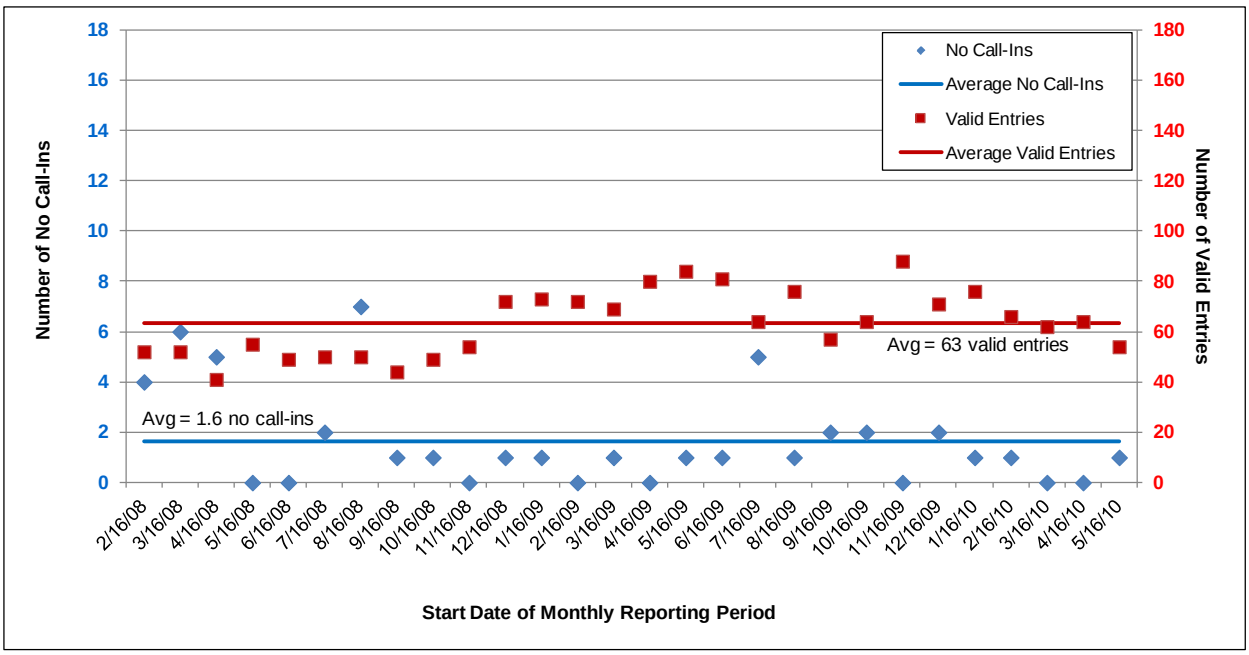


Figure 4-6. Pump Station B (Staffed): No Call-Ins

Figure 4-7 shows the no call-in metrics for Pump Station C, an unstaffed and frequently visited station where all employees must call the utility control center to announce arrival, regardless of time of day. Although Pump Station C is no longer staffed, utility employees and contractors visit the site often for capital improvements, maintenance work, and training.

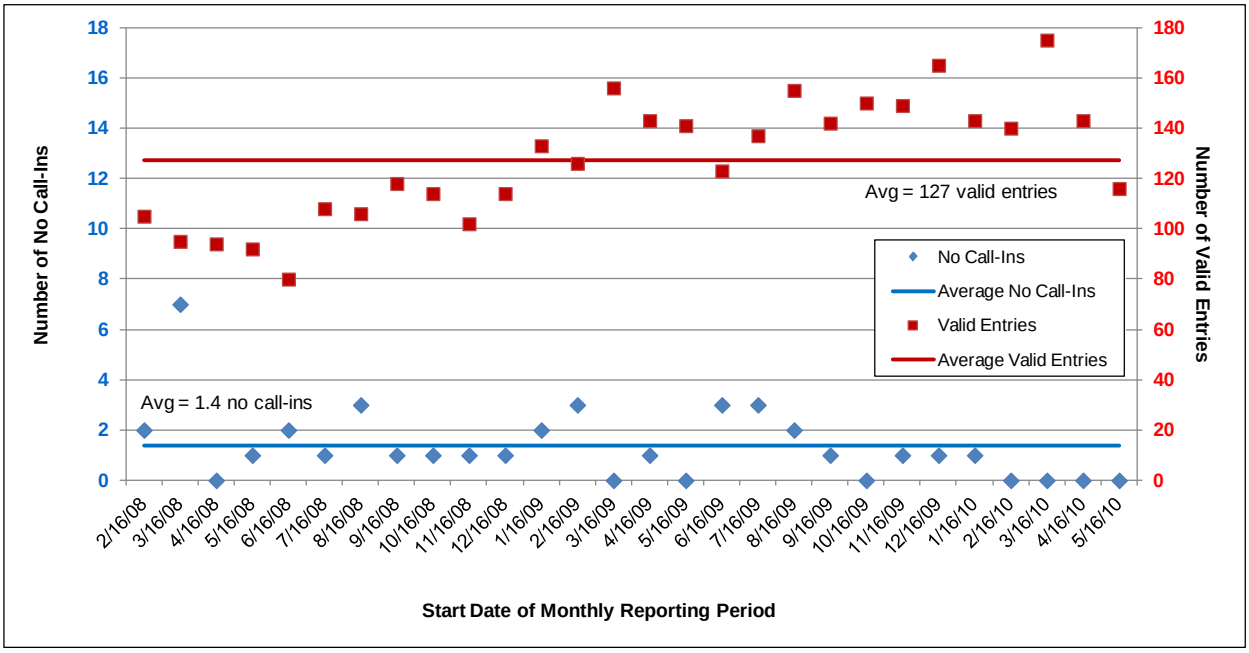


Figure 4-7. Pump Station C (Unstaffed, Frequently Visited): No Call-Ins

There were, on average, more no call-ins and valid entries at the unstaffed and frequently visited facility (1.4 and 127) compared to the unstaffed, infrequently visited facility (1.1 and 47) but not compared to the staffed facility (1.6 and 63). There was no relationship between the no call-ins and valid entries at Pump

Station C. Of the nine reporting periods that had an above average number of no call-ins, only two also had a higher than average number of valid entries.

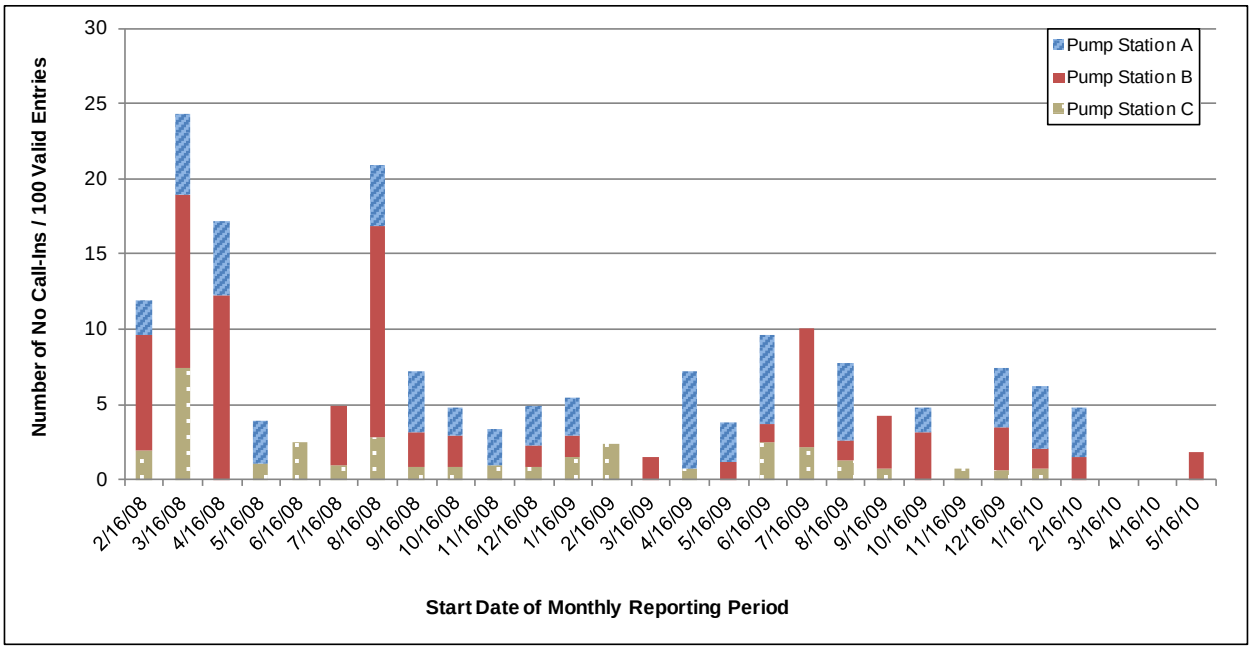
Except for the March 2008 reporting period, which had seven no call-ins, the number of invalid alerts due to no call-ins did not decrease over the course of the evaluation period, likely because ESM did not implement any significant changes to the utility's call-in procedures at Pump Station C. The decrease in the March 2008 reporting period in no call-ins was a random occurrence rather than a systemic trend.

Figure 4-8 shows the no call-in metrics normalized by number of valid entries at each pump station. The normalization factor was chosen, because having a larger number of valid entries could increase the probability of no call-in occurrence. Furthermore, each pump station had different amounts of valid entries. **Table 4-2** summarizes the data shown in Figure 4-8, and includes the average no call-in metrics for comparison among the pump stations.

Pump Station B had the highest non-normalized and normalized average no call-ins per reporting period at 1.6 and 2.99/100 valid entries.

The number of normalized no call-ins for Pump Stations A and C did not decrease over the evaluation period. This was likely because ESM did not implement any significant changes to the utility's call-in procedures. However, the number of normalized no call-ins for Pump Station B decreased over the evaluation period. The utility's efforts to reiterate the call-in policy to employees was an ongoing process.

The average normalized no call-ins for the Pump Stations ranged from 1.19 to 2.37 no call-ins/100 valid entries. When averaging all pump stations there were 1.4 no call-ins and 79 valid entries per reporting period.



Note: There was a reduction in the number of normalized no call-in incidents over time at Pump Station B, but not for the other pump stations.

Figure 4-8. Pump Stations: No Call-Ins/100 Valid Entries

Table 4-2. Summary of Pump Station No Call-In Data

Location	Average Number of No Call-Ins per Reporting Period	Normalized Average Number of No Call-Ins per 100 Valid Entries	Average Number of Valid Entries per Reporting Period
Pump Station A (unstaffed, infrequently visited)	1.1	2.37	47
Pump Station B (staffed)	1.6	2.99	63
Pump Station C (unstaffed, frequently visited)	1.4	1.19	127
All Stations, Combined Average	1.4	2.18	79

Equipment-Caused Invalid Alerts

Definition: An *equipment-caused invalid alert* occurred when an equipment issue caused an intrusion detection device to trigger an alert when there was no intrusion. The following section will discuss invalid alerts caused by equipment issues with the door/hatch and area motion sensors. The analysis for the ladder motion sensors installed at the pump stations will be included in the ladder motion sensor discussion for the non-video monitored sites in Section 5.4.

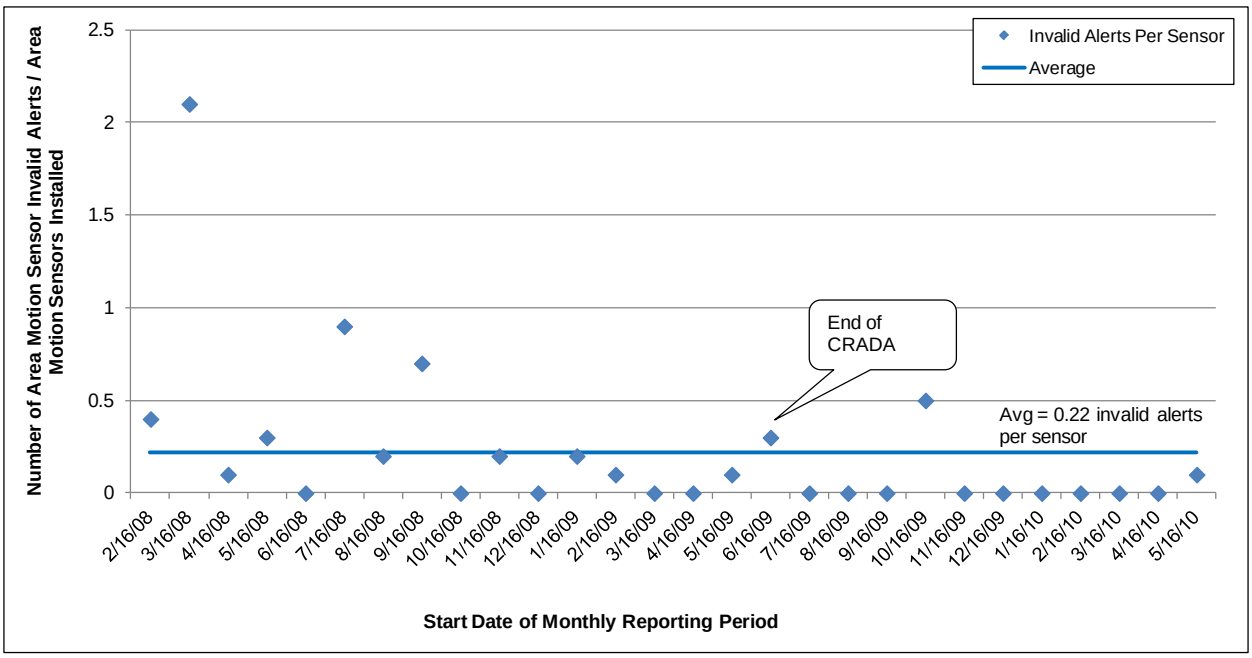
Analysis Methodology: This metric was segregated by the site types listed in Section 4.4.1. The site types include area motion sensors and door/hatch sensors.

The segregation of equipment by type allowed for an analysis of each type individually, and for comparison among types. The number of equipment-caused invalid alerts was normalized by the number of sensors for each type, since a higher number of installed sensors increased the probability of having an invalid alert. The analysis for equipment caused invalid alerts was not divided by site, since the cause of these invalid alerts were equipment specific rather than site-dependent.

Results: Figure 4-9 shows the normalized equipment-caused alert metrics for area motion sensors. The end of the Cooperative Research and Development Agreement (CRADA) on June 15, 2009, is noted on the graph since this was the point at which all maintenance activity was turned over from EPA to the utility. EPA addressed all known equipment issues before the end of the CRADA to minimize the initial maintenance burden on utility staff.

Equipment-caused area motion sensor invalid alerts decreased over the course of the evaluation period. Area motion sensor range and sensitivity configuration during sensor installation was lacking. Improper configuration led to high invalid alert rates early in the evaluation period. Over the course of the CRADA, sensors with high invalid alert rates had their ranges and sensitivities adjusted. Final range and sensitivity adjustments were completed during May 2009 reporting period, prior to the end of the CRADA.

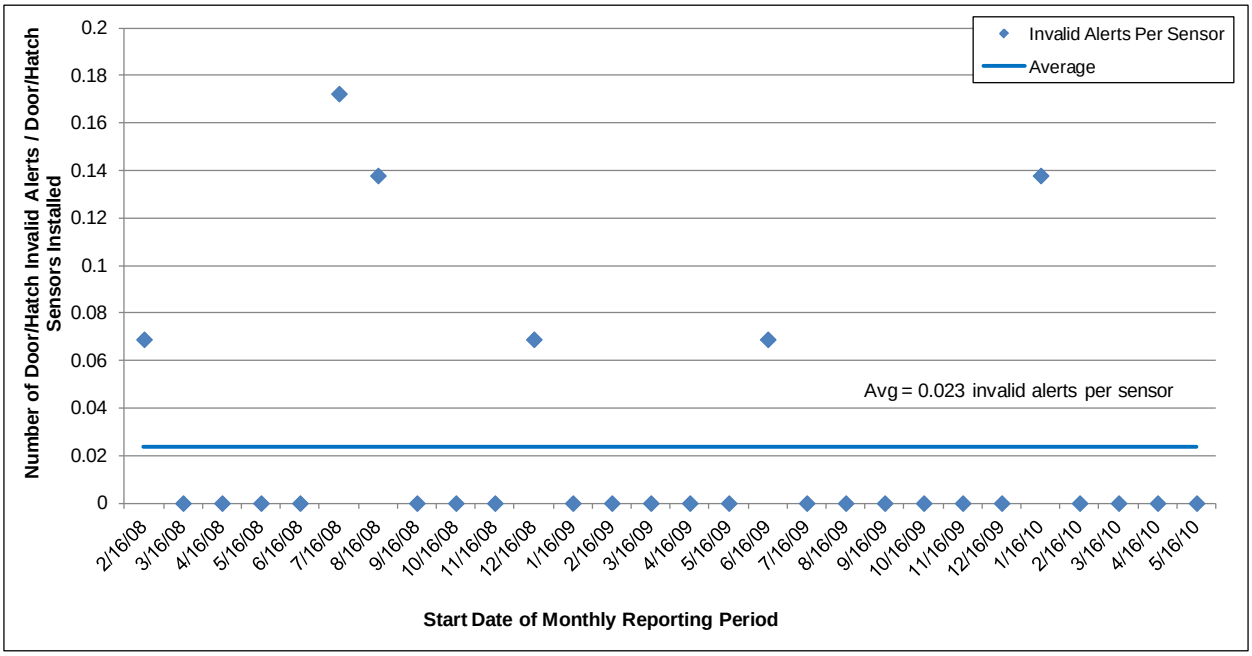
Two post-CRADA reporting periods, June 2009 and October 2009, showed equipment-caused area motion sensor invalid alerts. The invalid alert during the June 2009 reporting period was likely due to a warm air mass moving through an open window. An area motion sensor generates an alert only when its infrared detector senses a warm moving object at the same time that its microwave detector senses a moving object, regardless of temperature. If an area motion sensor is overly sensitive, the minute motion of objects caused by wind combined by motion of a warm air mass could generate an invalid alert. The invalid alert during the October 2009 reporting period appears to have been caused by an issue with the CWS SCADA system.



Note: Motion Sensor invalid alerts can be decreased with range and sensitivity adjustments.

Figure 4-9. Area Motion Sensors Invalid Alert Rate

Figure 4-10 presents the number of door/hatch sensor invalid alerts normalized by the number of door/hatch sensors (similar to the area motion sensor analysis), since a higher number of installed sensors increases the probability of having an invalid alert. The analysis is not divided by site, since the causes of these invalid alerts are not site-specific.



Note: The average per reporting period was 0.023 invalid alerts per door/hatch sensor compared to 0.22 for motion sensors at video sites.

Figure 4-10. Door/Hatch Sensors Invalid Alert Rate at Video Sites

All door/hatch sensors monitored by the ESM system were new except for an existing door sensor and hatch sensor at Pump Station A. The existing door and hatch sensors at Pump Station A accounted for 74

percent of the door/hatch sensor invalid alerts. The door sensor's target mounting bracket bent with use, causing the sensor to produce invalid alerts. The remedy for the problem was to bend the bracket back into shape. The hatch sensor at Pump Station A was also prone to invalid alerts. The hatch sensor was a reed type switch that was not an industrial grade device.

New sensors accounted for the remaining 26 percent of the door/hatch sensor invalid alerts. A new sensor on a door at Pump Station A caused an alert during the February 2008 reporting period. This was an isolated incident for this sensor. A new sensor on a door at Pump Station B caused alerts during the January 2010 reporting period and required adjustment.

Table 4-3 shows the average times between invalid alerts and the invalid alerts per sensor per year for area motion and door/hatch sensors. Industry standards from the *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA, 2006), and also device costs, are provided in Table 4-3.

Table 4-3. Equipment Caused Invalid Alerts: Average Times Between Alerts

	Area Motion Sensors	Door/Hatch Sensors	ASCE/AWWA Guideline
Days between Invalid Alerts per Sensor	136	1,168	90 (minimum)
Invalid Alerts per Sensor per Year	2.7	0.31	4 (maximum)
Cost per Device (2007 list prices)	$450	$260	n/a

The door/hatch sensors had more than eight times the number of days between invalid alerts per sensor for about 60 percent of the cost of a motion sensor. The area motion sensors and door/hatch sensors installed at video sites both satisfied the American Society of Civil Engineers (ASCE) and American Water Works Association (AWWA) guidelines for invalid alert rates. Although the door/hatch sensors have a significantly lower invalid alert rate and are a fraction of the cost of an area motion sensor, the door/hatch sensor can detect an intrusion only through a single door or hatch, but an area motion sensor can detect intrusions over a large area.

4.4.2 Summary

The alert occurrence design objective was evaluated by examining the invalid alert metrics, which measure a security system's effectiveness. The invalid alerts were categorized into security procedure violations and equipment caused invalid alerts. Security procedure violations were further categorized into door prop and no call-in incidents.

The analysis of the security procedure violations caused by door props showed the non-normalized and normalized averages per reporting period were three door props and 0.42 door props/100 valid entries/doors. Sites that had new ESM procedures for securing doors showed a decrease in the number of door props over the course of the evaluation period. This was due to the time required to train and familiarize utility and contractor personnel of the new practice of closing all ESM-monitored interior and exterior doors.

The analysis of the security procedure violations caused by employees not calling in when arriving at a facility showed the non-normalized and normalized averages per reporting period for no call-in invalid alerts were 1.4 no call-ins and 2.18 no call-ins/100 valid entries. The utility's call-in procedure has always been in place, so the decreasing trend observed with the door props was not observed for no call-ins at two of the three video sites. The decreasing no call-in trend at the other video site indicated that the utility's efforts to reiterate the call-in policy to employees was an ongoing process.

For equipment-caused invalid alerts, the area motion sensors had the highest average invalid alert rate per reporting period at 0.22 invalid alerts per sensor, which equated to 136 days between invalid alerts per sensor. Comparatively, for door/hatch sensors the rates were 0.023 invalid alerts per sensor and 1,186 days between invalid alerts per sensor. Both sensors met the ASCE/AWWA (2006) guideline of a minimum of 90 days between invalid alerts per sensor. The area motion sensors invalid alerts trended downward over the course of the evaluation period. Sensors that received inadequate sensitivity and range configuration during installation were adjusted over the course of the evaluation as the sensors that were prone to invalid alerts were identified. The door/hatch sensors had more than eight times the number of days between invalid alerts than the area motion sensors, and cost only 60 percent as much as the motion sensors.

Table 4-4 presents the percentage of each type of invalid alert at the video monitored sites. Security procedure and equipment caused invalid alerts are both shown for comparison.

Table 4-4. Pump Station Invalid Alerts by Type

Invalid Alert Type	Percentage (%)
Door Prop (Security Procedure)	56%
No Call-In (Security Procedure)	26%
Area Motion (Equipment Caused)	14%
Door Switch (Equipment Caused)	4%
TOTAL	100%

Most invalid alerts were caused by door props. Equipment (door switch and area motion detectors) caused 18 percent and security procedure violations caused 82 percent of all invalid alerts at pump stations. Ladder motion sensor invalid alerts installed at pump stations are discussed in the non-video site ladder motion sensor section in Section 5.4.

4.5 Design Objective: Timeliness of Detection

Timeliness of detection refers to the time for video to be transmitted and reviewed during an intrusion or Possible contamination incident. Factors that affect this objective include time for a video clip to arrive at the utility control center, time for the clip to be viewed by utility personnel, and time for determination of Possible contamination to be made. Installation of cameras allowed GCWW staff to view intrusion alert locations remotely and to determine quickly the validity of the alert. Video also allowed staff to more confidently confirm a contamination attempt and to take response actions that normally would not be completed, such as turning off pumps to prevent the spread of contamination. Without video, the response time may be longer. Intrusion alert data collected at the pump stations is discussed in Section 6.4.1.

4.5.1 Time for Video Clip Transmission

Definition: Time for video clip transmission is the time required for a video clip to be transmitted from the pump station site to the utility control center. This metric measured how effectively the video system provided video information to utility personnel. Timely video clip transmission may provide utility staff with evidence of a Possible contamination incident before dispatching investigators to the site.

Analysis Methodology: The time to transmit a video clip and the time to transmit a video clip normalized by file size for each pump station per reporting period are shown.

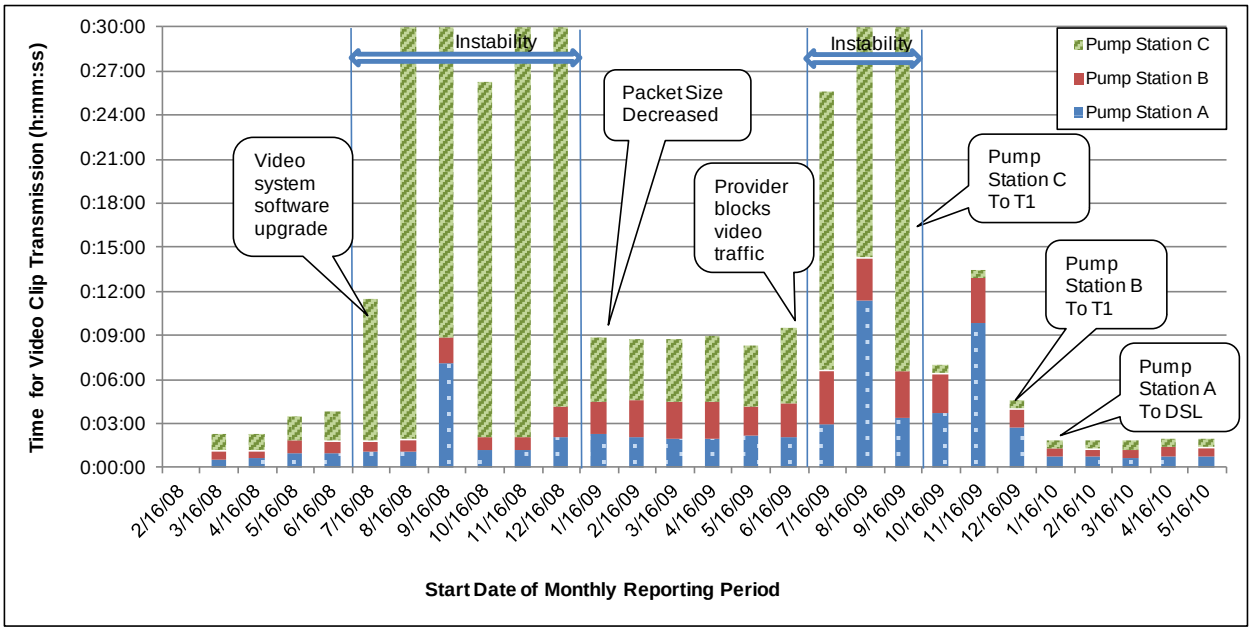
Results: Video system performance varied greatly over the evaluation period because of communications and software issues. These issues are shown in **Table 4-5**, which documents the timeline of events that affected video performance. Table 4-5 also discusses the modifications that were implemented to work around or resolve these issues.

Table 4-5. Timeline of Events Affecting Video Data Transmission Time

Date	Video Transmission Event	Event Details
February – June 2008	Video System Version 3 was running with video clip transmission times of about 1 minute.	• Version 3 could not automatically delete video clips that were stored for a predetermined time. As a result, video clips accumulated until either manually deleted or the hard drive ran out of space.
June 2008	Upgraded to Video System Version 4.	• Video system was configured to automatically delete video clips older than six months.
		• Minor usability issues were also addressed in the Version 4 upgrade.
June 2008 – January 2009	Video clip transmission times increased significantly, especially at Pump Station C.	• Signal strength problems occurred at Pump Station C, likely because of adjacent structures and large nearby trees obstructing the signal path to the cell tower. • Engineers were unable to determine whether increased transmission time was due to the system software upgrade or to the digital cellular provider imposing restrictions on the utility's "unlimited" data plan.
January 2009	The video data transmission packet size was decreased from 20,000 bytes to 1,400 bytes to remedy the signal strength effect on clip transmission times.	• Reducing packet size increased the likelihood a data packet would be transmitted successfully, which was critical for locations with low signal strength. • Reducing packet size also increased the time required to transmit a video clip. Each successfully transmitted packet contained less information, requiring transmittal of more packets to deliver the video clip file, taking longer. • The slight increase in the video clip transmission time for Pump Stations A and B can be attributed to this phenomenon.
January – June 2009	Video clip transmission times stabilized.	• Video clip transmission times were roughly three minutes, two minutes longer than during the pre-June 2008 period of stability.
June 2009	The digital cellular provider blocked user datagram protocol (UDP) traffic on the port used by the video system.	• Video clip transmission times increased significantly for Pump Stations A and C, and increased slightly the transmission time for Pump Station B.
July – August 2009	To work around the UDP blockage, the video system was reconfigured to use the transmission control protocol (TCP).	• Performance was erratic under the TCP configuration. • Under low signal strength conditions, the TCP protocol performed poorly compared to UDP. This was an issue at Pump Station C. • GCWW was reluctant to continue relying on the digital cellular provider for video traffic and initiated plans to switch the video sites to T1 and DSL landline connections.
September 2009	Pump Station C communications were successfully switched to a T1 line.	• There was an existing T1 line at Pump Station C.

Date	Video Transmission Event	Event Details
December 2009	Pump Station B communications were successfully switched to a T1 line.	• There was an existing T1 line at Pump Station B.
January 2010	Communications at the pump station A were successfully switched to the new line.	• There was not an existing T1 line at Pump Station A, but there was an existing phone line. A new DSL connection was installed at Pump Station A.
January – June 2010	The video clip duration doubled.	• The landline connections improved video data performance. All three pump stations had the lowest video clip transmission times over the entire evaluation period. Because of improved performance and stability of the communications system for video traffic, GCWW doubled the video clip duration so that the point of intrusion could be monitored for a longer period after the intrusion.

Figure 4-11 shows the time for a video clip to be transmitted from each video monitored site to the utility control center, and calls out significant video system events discussed in Table 4-5.



Note: There were only two periods of instability: July 16, 2008–January 15, 2009, and July 16, 2009–October 15, 2009.

Figure 4-11. Pump Stations: Time for Video Clip Transmission

All three pump stations used digital cellular communications until they were switched to a T1 or DSL connection. While using digital cellular communications, Pump Station C generally had a longer video clip transmission time than the two other sites. Signal strength problems occurred at Pump Station C, likely because of adjacent structures and large nearby trees obstructing the signal path to the cell tower.

The start of the first period of video instability coincided with a version upgrade to the video system software, which was during the July 2008 reporting period. The first period of video instability concluded after the packet size parameter was adjusted on the video system, which was during the January 2009 reporting period. Smaller packet sizes are less prone to radio interference, but take longer to transmit a large amount of data. This workaround solution reduced the video transmission time, but the

root cause behind the first period of instability was not determined. The likely causes were changes to the video system software as a result of the version upgrade or restrictions from the digital cellular provider.

The video sites were switched to T1 or DSL connections after the digital cellular provider started blocking video traffic during the June 2009 reporting period. **Table 4-6** summarizes the average video clip transmission times during the periods of stability.

Table 4-6. Video Clip Transmission during Periods of Stable Communications

Date	Average Video Clip Transmission Time (seconds)
February–June 2008	59
January–June 2009	177
January–June 2010	37

During the second period of stability, the video clip transmission time was three times longer than that of the first period of stability. The data packet size was reduced to restore system stability. Smaller packet sizes require more time to transmit a large amount of data. During the third period of stability, the video clip transmission time was 38 percent less than that of the first period of stability and 79 percent less than that of the second period. The video clip transmission time data for the third period of stability was skewed by the fact that the utility doubled the video clip duration during the January 2010 reporting period.

As noted, the video clip duration was doubled during the January 2010 reporting period. Initially, the video clip was about 240 kilobytes, and after the January 2010 reporting period, about 380 kilobytes. Thus, to give an accurate comparison of video transmission times before and after January 2010, the video transmission times were normalized by video clip file size. **Table 4-7** lists the normalized video clip transmission times during the periods of stable communications.

Table 4-7. Normalized Video Clip Transmission - Periods of Stable Communications

Date	Normalized Average Video Clip Transmission Time (seconds per 100 kilobytes)
February–June 2008	24
January–June 2009	74
January–June 2010	10

During the third period of stability, the video clip transmission time normalized by clip file size is 58 percent less than that of the first period of stability and 86 percent less than that of the second period of stability. When the video clip transmission time is not normalized, the improved performance using the T1 and DSL lines is understated. As noted, the non-normalized reductions in transmission time during the third period of stability are 38 percent less than the first period of stability and 79 percent less than the second.

4.5.2 Time for Video Clip Viewing

Definition: *Video clip view time* is the time between an intrusion and the time utility personnel start viewing the accompanying video clip. This metric measured how effectively the utility staff used the video system to support investigations.

Analysis Methodology: The view time of video clips used to support an onsite investigation or to verify an invalid alert were analyzed. The view times of video clips that were not part of an investigation were not considered to avoid skewing this analysis, because such clips were typically viewed multiple days after intrusion when an operator inadvertently clicked on the clip or when viewed for training purposes. Video clips that were not part of an investigation were usually generated when an employee called into the utility control center, but the operator did not disarm the ESM system. When the ESM system was armed, video clips were generated of all entries. A video clip that was part of an investigation was typically viewed within 30 minutes after an intrusion. View times from the ESM drills at video-monitored sites also were analyzed.

Results: The video clips that supported an onsite investigation or were used to verify an invalid alert during the evaluation period were viewed an average of 3 minutes 14 seconds after the intrusion (excluding two outliers). The outlier clips were viewed hours after the investigation had concluded and were likely used for debriefs.

Twelve video clips were used as part of onsite investigations or to verify invalid alerts, including the two outliers noted. Thirty-one onsite investigations were performed at the video-monitored sites. The use of video to support investigations was reduced by the utility control center operators' lack of confidence in the video system following the periods of video instability discussed in Section 4.5.1. After the issues with video clip transmission were resolved following the transition to T1 and DSL connections, there were no recorded onsite investigations at the video-monitored sites, so empirical data after the transition were not available.

Data on the video clip view times were also collected during the ESM drills at video-monitored sites. The utility control center operator viewed the video clips as soon as they were completely downloaded, six minutes after the intrusion in ESM Drill 2 and two minutes after the intrusion in Drill 3. Drills 2 and 3 occurred before the T1/DSL transition. During Drill 4, the utility control center operator switched the video system to "live" mode after receiving the alert but before the video clip fully downloaded. Live mode allowed the operator to view the inside of the facility with only a few seconds of delay, as a result of the DSL connection at the drill site. The delay would be longer and the imagery more sporadic with a slower connection. During the Drill 4 debriefing, the utility security and operations staff mentioned their high level of confidence in the video system since the T1/DSL transition. The Drill 4 events showed that live video can be useful tool for responding to an intrusion, although the live mode requires a communications link that can support the bandwidth demand. The live video also requires immediate operator attention, which may be challenging if the operator is involved in a critical task. Event-based video clips are still an essential response tool since the clip captures the actual intrusion at the point of entry, has less bandwidth demand, and does not require immediate operator attention.

4.5.3 Summary

The timeliness of detection design objective was evaluated by examining the video data transmission times and video clip view times.

The time for video clip transmission varied greatly over the course of the evaluation period because of complex data transmission problems caused by software issues, localized signal strength problems and digital cellular provider interruptions. After the digital cellular provider blocked video traffic during the June 2009 reporting period, the utility transitioned the video monitored sites to T1 and DSL connections. The transition began during the September 2009 reporting period and concluded during the January 2010 reporting period. By the end of the evaluation period, transmission time was consistently at the lowest level, and the utility no longer reported major issues with the system. Engineers were able to double video clip transmission time with the landline connections, which was not possible with the slower digital cellular network.

The video clip transmission metric was characterized by three extended periods of stability: February 16 through June 15, 2008, January 16 through June 15, 2009, and January 16, 2010 through the end of the evaluation period. The first two periods used digital cellular communications, and the third, T1 and DSL connections. Video clip transmission times were one minute for the first period, three minutes for the second and 37 seconds for the third. When normalized by video clip file size, the transmission times were 24, 74 and 10 seconds per 100 kilobytes. During the third period of stability until the end of the evaluation, the clip duration was doubled in length because of improved video system performance and a desire expressed by the utility to view the point of intrusion for a longer duration.

The view times for video clips that supported an onsite investigation or were used to verify an invalid alert averaged 3 minutes and 14 seconds after the intrusion.

Data on the video clip view times also were collected during the ESM drills at video-monitored sites. The utility control center operator viewed the video clips as soon as they were completely downloaded, six minutes after the intrusion during Drill 2 and two minutes after the intrusion during Drill 3. During Drill 4, the utility control center operator switched the video system to "live" mode during the drill to view the inside of the facility which is near-real-time with a few second delay, rather than waiting for the video clip to download. The utility security and operations staff mentioned their high level of confidence in the video system since the T1/DSL transition during the Drill 4 debriefing.

4.6 Design Objective: Operational Reliability

Analysis of the reliability of the ESM considers both operation and performance metrics. Operation metrics measured the system's ability to continuously monitor for intrusions, and included availability and data completeness. Performance metrics measured the accuracy of ESM equipment and procedures in discriminating between an actual intrusion incident and normal variability in underlying data (i.e., invalid alerts).

4.6.1 Availability of Intrusion Alert Communication Systems

Definition: Availability of intrusion alert communication system is the percentage of time that intrusion alert data are successfully transmitted.

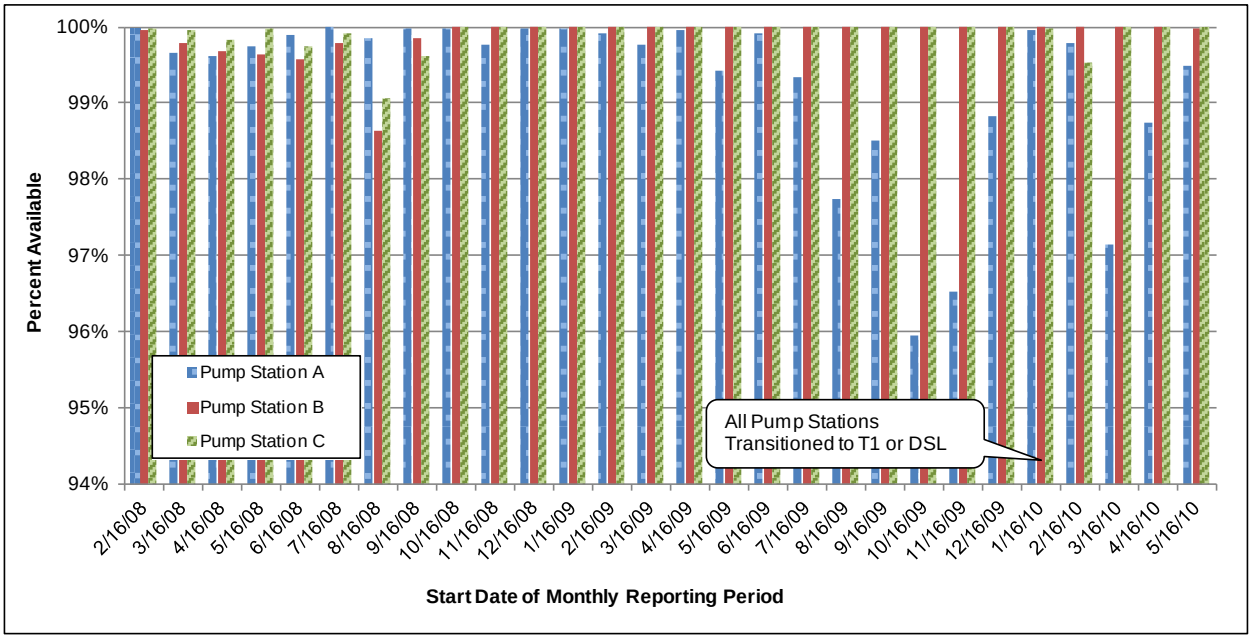
Analysis Methodology: The availability of the communications system for intrusion alert data transmission for each pump station per reporting period is shown. The calculation for each pump station is:

$$\frac{(\text{Potential Alarm Communication Hours Available - Alert Communication Hours Unavailable})}{\text{Potential Alarm Communication Hours Available}} \times 100$$

Potential number of intrusion alert communication hours available is the number of hours in a given reporting period. *Intrusion alert communication hours unavailable* are the number of hours that the intrusion alert communications system was not working properly at each pump station per reporting period and included downtime due to communications system failure as well as for maintenance.

Results: **Figure 4-12** shows the communications system availability for intrusion alert data at the three pump station locations with digital cellular, T1 or DSL communications. **Table 4-8** summarizes the data depicted in Figure 4-12. When intrusion alert data and video data are transmitted over the same communications link, the two data types use different protocols, ports and data packet sizes. Thus, the issues that caused unavailability and slow responsiveness with video communications may not have necessarily affected intrusion alert communications. The availability of intrusion alert data

communications exceeded 95 percent and the difference between digital cellular and T1/DSL communications was minimal.



Note: The availability of intrusion alert data communications exceeded 95% and the difference between digital cellular and T1/DSL communications was minimal.

Figure 4-12. Pump Stations: Communications System Availability Intrusion Alerts

Table 4-8. Communications Availability for Intrusion Alert Data

Pump Station	Digital Cellular (February 2008–December 2010)	T1 or DSL (January–June 2010)	Entire Evaluation Period (February 2008–June 2010)
Pump Station A	99.32%	99.02%	99.26%
Pump Station B	99.87%	100%	99.89%
Pump Station C	99.92%	99.90%	99.91%
All Pump Stations	99.70%	99.64%	99.69%

All three pump stations had an average intrusion alert data communications availability of greater than 99 percent regardless of communications method. There were three reasons for the high levels of availability: (1) Intrusion alert data consist of relatively small data packets compared to video data; (2) Smaller packets are less prone to interference; and (3) Smaller packets are less likely to be noticed by a communications provider that may be looking for ways to manage the amount of bandwidth allotted per user.

The T1/DSL transition increased the average availability by 0.13 percent at Pump Station B but reduced the average availability at Pump Station A by 0.3 percent and at Pump Station C by 0.02 percent. Sporadic DSL and T1 outages at Pump Stations A and C were the causes.

There were reporting periods that experienced deviations from the otherwise high level of availability, as explained by **Table 4-9.**

Table 4-9. Incidents That Reduced Intrusion Alert Communications Availability

Reporting Period	Pump Stations	Description
August 2008	A, B, C	A severe windstorm occurred on September 14, 2008. • Prolonged power outages exceeded the battery charge duration of the UPS in the ESM control panels. • The prolonged power outages may have also caused downtime with the digital cellular network.
August 2009	A	Two 8-hour (approximate) cellular network outages. • Not caused by a power failure at the Pump Station. • May have been due to troubleshooting attempts by the digital cellular provider or the utility to remedy the video port blocking issue described in Section 4.4.1.
October 2009	A	Multiple cellular network outages, each lasting about 50 minutes.
November 2009–April 2010	A	Sporadic cellular network outages until the end of the evaluation period, regardless of digital cellular or DSL communications.

4.6.2 Availability of Video Communication Systems

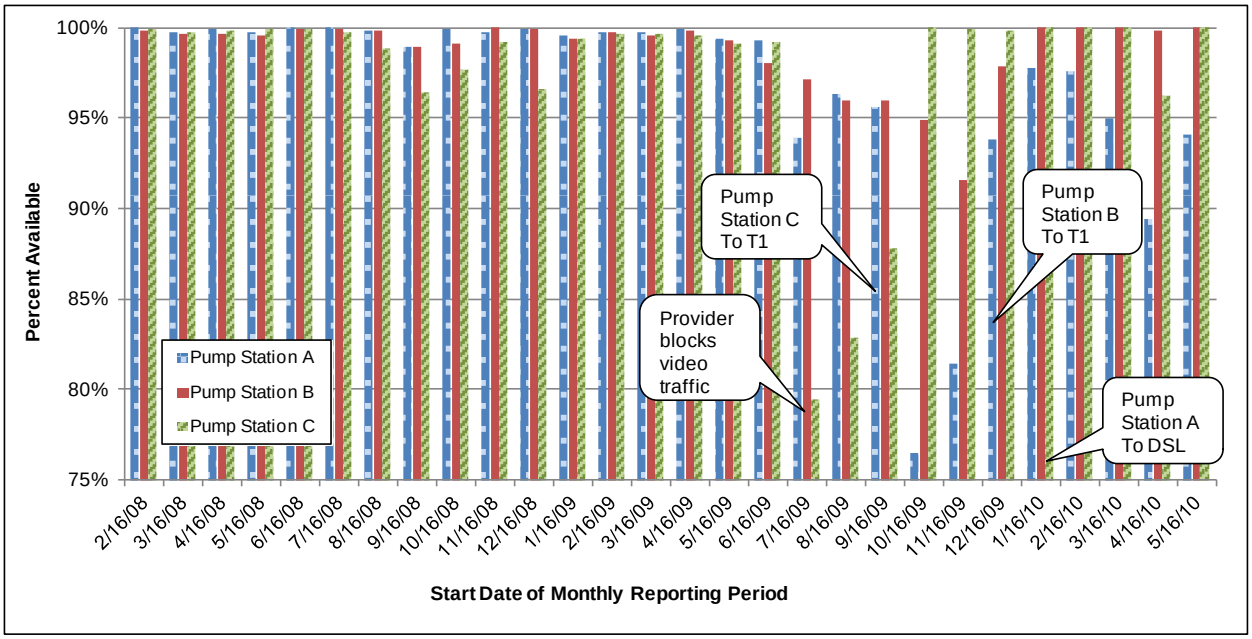
Definition: *Availability of video communication systems* is the percentage of time that video data are successfully transmitted.

Analysis Methodology: The communications system availability for video transmission for each pump station per reporting period is shown. The calculation for percent availability for each pump station is:

$$\frac{(\text{Potential Video Communication Hours Available} - \text{Video Communication Hours Unavailable})}{\text{Potential Video Communication Hours Available}} \times 100$$

Potential number of video communication hours available is the number of hours in the reporting period. *Video communication hours unavailable* is the number of hours that the video communications was not working properly at each pump station per reporting period.

Results: **Figure 4-13** shows the communications system availability for video data at the three locations with digital cellular, T1 or DSL communications. **Table 4-10** summarizes the data shown in Figure 4-13.



Note: There were three extended periods of stability: February 16, 2008 to June 16, 2008, January 16, 2009 to June 16, 2009, and January 16, 2010 to the end of the evaluation period.

Figure 4-13. Pump Stations: Availability of Video Communication Systems

Table 4-10. Communications Availability for Video Data

Pump Station	February 16–June 15, 2008	January 16–June 15, 2009	January 16, 2010–End of Evaluation	Total Evaluation
	Percent Available	Percent Available	Percent Available	Percent Available
Pump Station A	99.87%	99.60%	94.75%	96.66%
Pump Station B	99.72%	99.32%	99.96%	98.76%
Pump Station C	99.87%	99.44%	99.24%	97.51%
All Pump Stations	99.82%	99.45%	97.98%	97.64%

The pump stations had average availabilities above 99 percent during the first two periods of stability, when digital cellular service was used. During the third period of stability, there was a reduction in availability for Pump Stations A and C and an increase in availability for Pump Station B. There were sporadic outages with the DSL connection at Pump Station A. There were sporadic outages with the T1 connection at Pump Station C, but fewer than those experienced by Pump Station A.

Reporting periods that experienced long video clip transmission times also had lesser-than-average levels of video communications availability. See Section 4.5.1 for more discussion on the suspected causes behind periods of video system instability and how the issues were addressed.

4.6.3 Availability of Intrusion Detection Equipment

Definition: *Availability of intrusion detection equipment* is the percentage of time that door sensors, area motion sensors and ladder motion sensors are functioning properly.

The availability of the PLC and I/O servers also was analyzed because those devices played important roles in delivering intrusion alert data to the utility staff at the control center. PLCs transmitted intrusion alerts from intrusion detection devices to the I/O servers, which provided data to the utility staff's HMI.

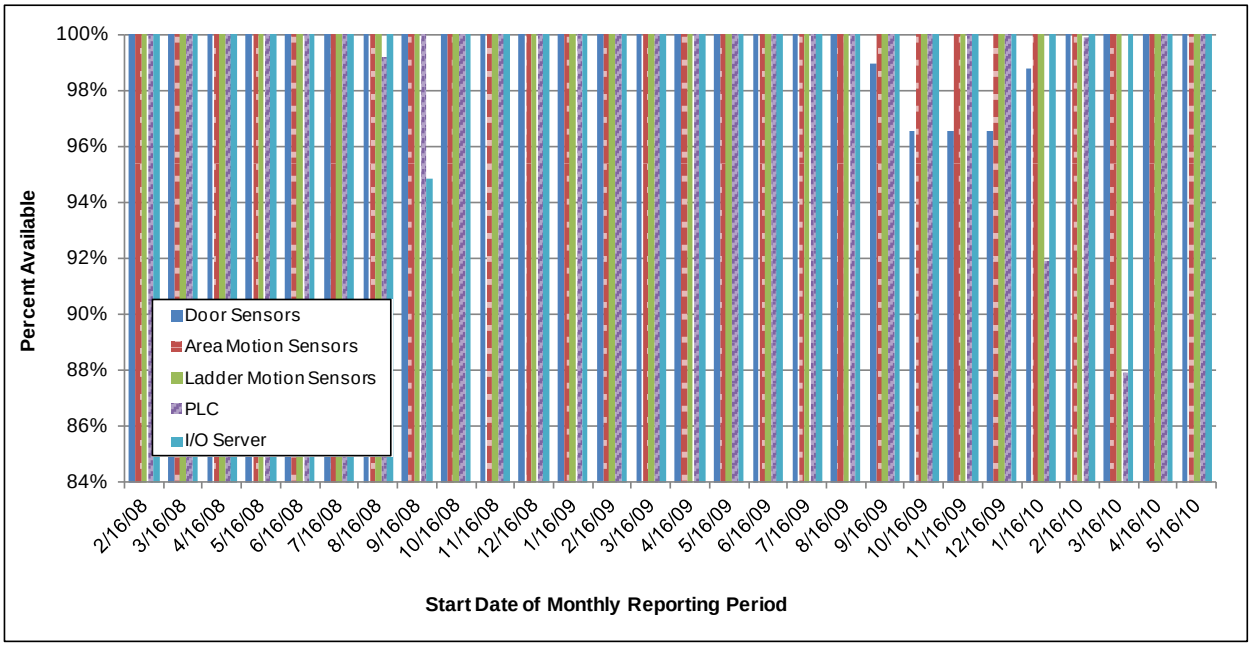
There was one PLC per pump station and a redundant pair of I/O servers (primary and secondary) that communicated with all three PLCs. Intrusion detection device downtime caused by a PLC or I/O server outage was only recorded under the PLC or I/O server category and not recorded as downtime for the attached detection devices.

Analysis Methodology: The equipment availability for the different types of intrusion detection devices at video sites for each reporting period is shown. The calculation for percent available for each type of intrusion detection device is:

$$\frac{(\text{Potential Equipment Hours Available} - \text{Equipment Hours Unavailable})}{\text{Potential Equipment Hours Available}} \times 100$$

Potential equipment hours available is the number of hours in the reporting period multiplied by the number of equipment of that type installed at the pump stations. *Equipment hours unavailable* is the number of hours that the equipment was not working for each type of equipment per reporting period.

Results: **Figure 4-14** shows the availability for the intrusion detection devices used at pump stations over time, and **Table 4-11** summarizes the data.



Note: The intrusion detection devices were 100% available for most of the entire evaluation period. PLC outages toward the end of the evaluation period caused the most significant downtime.

Figure 4-14. Intrusion Detection Equipment Availability

Table 4-11. Intrusion Detection Equipment Availability

Intrusion Detection Equipment	Average Percent Availability
Door Sensors	99.55%
Area Motion Sensors	100%
Ladder Motion Sensors	100%
PLC	99.25%
I/O Server	99.81%

The area and ladder motion sensors at the pump stations were 100 percent available throughout the evaluation. Despite occasional periods of downtime for door sensors, PLCs and I/O server had average availabilities above 99 percent. These periods of downtime are further explained in **Table 4-12**.

Table 4-12. Incidents That Reduced Intrusion Detection Equipment Availability

Reporting Period	Intrusion Detection Equipment	Description
August 2008	PLCs	A severe windstorm occurred on September 14, 2008. • Prolonged power outages exceeded the battery charge duration of the UPS in the ESM control panels. • The PLC at each pump station is enclosed in and powered from that site's ESM control panel.
September 2008	I/O Server	Compatibility issues with a PLC firmware upgrade caused the I/O server computers to stop running.
September 2009 – January 2010	Door Sensor	A door alert at Pump Station A was not triggered when the door was opened. • Likely caused by utility personnel inadvertently disabling the door alert while employees were at the site and not re-enabling it when work was completed. • New operators were being trained at this time. • The intrusion alert log does not track if an alert is disabled, so the exact cause of unavailability is unknown. A motion detector monitored the door entryway, so intrusions at Pump Station A were still detected during the period of unavailability. • The door sensor unavailability went unnoticed for multiple reporting periods, because intrusions were still detected.
January 2010	Door Sensor	A door alert at Pump Station B was triggered even when the door was not being opened. • The utility's instrument shop adjusted the sensor.
January 2010	PLC	Suspected power issues at Pump Stations A and B.
March 2010	PLC	Suspected power and PLC hardware issues at Pump Station B.

At the end of the CRADA, June 15, 2009, ESM equipment was turned over from the EPA to the utility and was incorporated into the utility's maintenance program and emergency procedures for minimizing the impact of power and communications outages.

4.6.4 Availability of Video Equipment

Definition: *Availability of video equipment* is the percentage of time that the fixed and PTZ cameras were functioning properly. Video devices were not categorized as intrusion detection devices since the

devices are not used to detect intrusions, but to confirm whether the intruder is a legitimate threat and also if contamination may be Possible.

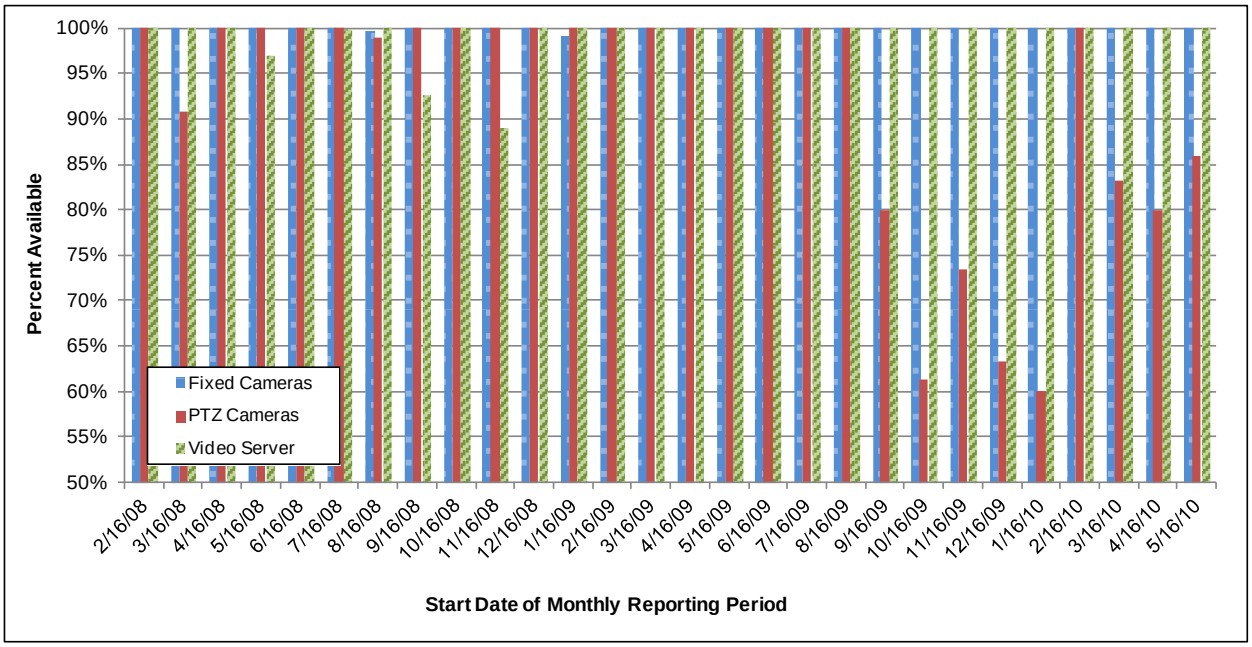
The availability of the video server also was analyzed because the server gathered video data transmitted from the remote sites and delivered the video clips to the utility staff's HMI. Video server downtime caused by a video server outage was recorded under the video server category and not as downtime for the attached cameras. The video server application runs on the secondary I/O server. See Section 4.5.3 for a discussion of the I/O servers.

Analysis Methodology: The availability for each type of camera and for the overall video system is shown per reporting period. The calculation for percent available for each type of equipment is:

$$\frac{(\text{Potential Equipment Hours Available} - \text{Equipment Hours Unavailable})}{\text{Potential Equipment Hours Available}} \times 100$$

Potential equipment hours available is the number of hours in the reporting period multiplied by the number of pieces of equipment installed at the pump station. *Equipment hours unavailable* is the number of hours that the equipment was not working properly for each type of equipment per reporting period. Six fixed cameras, five PTZ cameras and one video server served all the pump stations.

Results: Figure 4-15 shows the availability for the video equipment used at pump stations over time, and **Table 4-13** summarizes the data. The availability of the video server also is shown because it gathers video data transmitted from the remote sites and delivers the video clips to the utility staff's HMI. Video server downtime caused by a video server outage was recorded under the video server category, not as downtime for the attached cameras.



Note: PTZ cameras experienced numerous outages from the reporting period beginning September 16, 2009 until the end of the evaluation.

Figure 4-15. Video Equipment Availability

Table 4-13. Intrusion Detection Equipment Availability

Intrusion Detection Equipment	Percent Available
Fixed Cameras	99.96%
PTZ Cameras	92.03%
Video Server	99.23%

Fixed cameras and the video server had average availabilities above 99 percent. PTZ cameras had numerous outages, causing the average availability to be about 92 percent. The PTZ cameras were commissioned between January and April 2007 and were approaching three years in service when the cameras started experiencing issues during the September 2009 reporting period. The utility's experience with this type of PTZ camera at non-ESM facilities indicated that the design life typically ended after three to five years of service. **Table 4-14** explains the periods of downtime for video equipment.

Table 4-14. Incidents that Reduced Video Equipment Availability

Reporting Periods	Equipment	Description
March 2008	PTZ cameras at Pump Station B	Two cameras at Pump Station B displayed as gray screens.
May 2008	Video Server	A video system version upgrade required stopping the video server application.
August 2008	Fixed and PTZ cameras at all locations	A severe windstorm occurred on September 14, 2008. • Prolonged power outages exceeded the battery charge duration of the UPS in the ESM control panels. • The cameras at the pump stations are powered from each site's ESM control panel.
September 2008	Video Server	Compatibility issues with a PLC firmware upgrade caused the secondary I/O server computer to stop running. The video server application runs on the secondary I/O server computer.
November 2008	Video Server	Scheduled CWS SCADA programming updates were implemented on the secondary I/O server, requiring the video server application to be stopped.
January 2009	Fixed camera at Pump station A	The camera at Pump Station A was taken out of service temporarily to re-pressurize the camera enclosure.
September 2009 – January 2010	PTZ camera at Pump Station B	Two cameras at Pump Station B were not zooming to the appropriate points of intrusion. The cameras were also out of focus. The cameras sent video clips at times when there were no intrusions.
March 2010	PTZ camera at Pump station C	A camera at Pump Station C displayed as a black screen.

4.6.5 Data Completeness

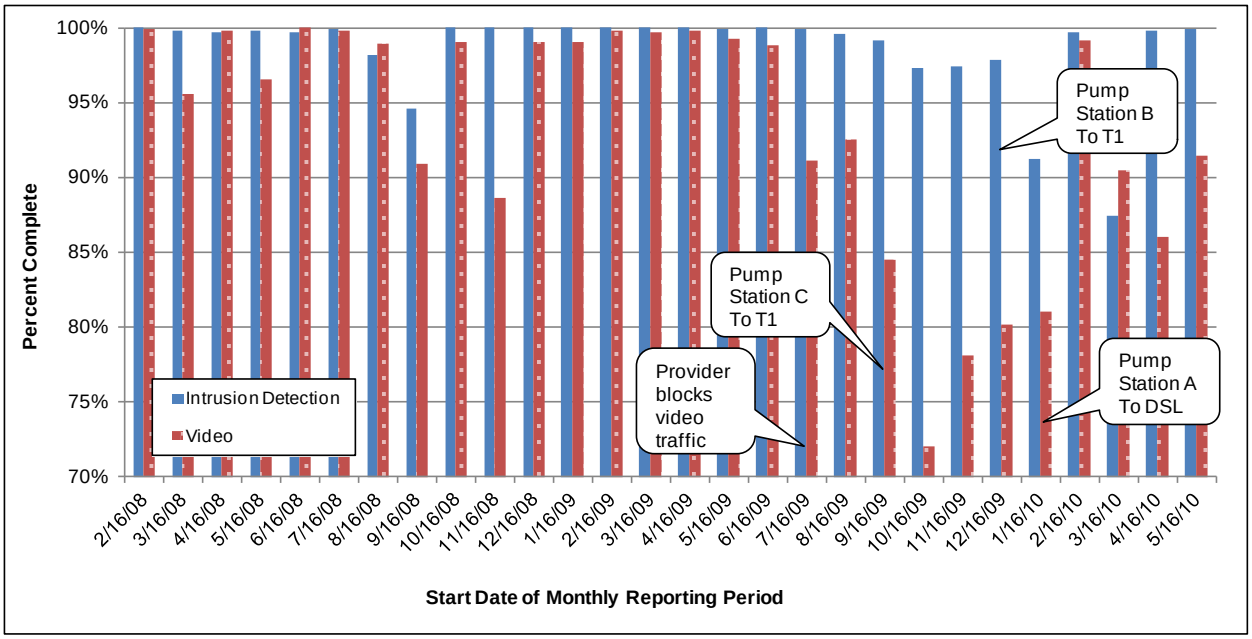
Definition: *Data completeness* is the amount of data hours that can be used to support component operations, expressed as a percentage of all data generated by the component.

Analysis Methodology: The data completeness for intrusion detection equipment and video equipment is shown. The calculation for data completeness is:

$$\frac{(\text{Potential Data Hours Available} - \text{Data Hours Unavailable})}{\text{Potential Data Hours Available}} \times 100$$

Potential data hours available is calculated using the number of intrusion detection or video data streams multiplied by the number of hours in the reporting period. *Data hours unavailable* is the number of hours the data stream was not working properly for each type of equipment per reporting period.

Results: **Figure 4-16** shows the completeness for all intrusion and video data streams over time, and **Table 4-15** summarizes the data.



Note: Data completeness for video data fell to 72% after the digital cellular provider blocked video traffic after the June 2009 reporting period. PTZ camera failures kept video data completeness low after the T1/DSL transition in January 16, 2010.

Figure 4-16. Data Completeness: Pump Stations

Table 4-15. Data Completeness: Pump Stations

Data Stream	Percent Available
Intrusion Detection	98.59%
Video	93.23%

Data completeness includes downtime from communications and equipment faults. Each data stream represents the output from an individual intrusion detection device or camera. For equipment connected to multiple intrusion detection devices or cameras, any PLC, I/O server, or video server equipment

downtime would cause a loss of data from all of the intrusion detection devices or cameras data streams connected to them. For example, if a PLC, I/O server, or video server were to experience downtime, the following systems shown in **Table 4-16** would also be affected.

Table 4-16. Intrusion Detection Device Downtime Effects

Equipment	Number of Connected Devices
PLC: Pump Station A	9 intrusion detection devices
PLC: Pump Station B	23 intrusion detection devices
PLC: Pump Station C	18 intrusion detection devices
I/O Server	50 pump station intrusion detection devices
Video Server	11 cameras

Video data completeness values combine the trends shown in Figures 4-13 and 4-15, which show the video communications availability and video equipment availability. Figures 4-12 and 4-14 are the equivalent graphs for intrusion detection communications and equipment availability, respectively. The lowest data completeness was 72 percent. This was observed during the October 2009 reporting period, which had a 76 percent video communications availability that was compounded by a 55 percent PTZ camera availability.

The data completeness for intrusion detection data streams was 98.59 percent. The intrusion detection data streams had fewer communications and hardware issues compared to the video data streams. Power outages, PLC hardware and firmware issues, communications outages and possible operator error caused reductions in intrusion detection data completeness. See Tables 4-9 and 4-12 for discussions on the incidents that reduced intrusion alert communications and intrusion detection equipment availability.

The data completeness for video data streams was 93.23 percent. Communications outages, power outages, software and CWS SCADA updates, and camera hardware issues caused reductions in video data completeness. See Tables 4-5 and 4-14 for discussions on the incidents that reduced video communications and video equipment availability.

4.6.6 Summary

The operational reliability design objective was evaluated by examining the video and intrusion alert communications availability, equipment availability and data completeness.

As discussed in Section 4.5.1, the three periods of video system stability experienced high levels of video communications availability. When digital cellular communications were used, average video communications availabilities were 99.82 percent in the first period of stability and 99.45 percent in the second. The third period, which used T1 and DSL connections, displayed a lower overall average availability of 97.98 percent, primarily because of sporadic DSL and T1 outages at Pump Stations A and C. The slight decrease in availability and increase in video data transmission performance after the T1/DSL transition, which was discussed in Section 4.5.1, underscores the independence of the availability and performance metrics. System improvements that improve performance may also cause more system downtime. The reduction in system availability after the T1/DSL transition was minimal.

The intrusion alert data transmission was relatively stable and experienced a high level of performance. Whether using digital cellular T1 or DSL connections, the average intrusion alert data communications availability was above 99 percent. Although the intrusion alert data used the same communications systems as the video data, the intrusion alert data used smaller packets and different protocols. The

smaller packets were less prone to interference and were less likely to be noticed by a communications provider that may be looking for ways to manage the amount of bandwidth allotted per user.

The intrusion detection equipment, which included area and ladder motion sensors, door/hatch sensors, PLCs and an I/O server, all had average availabilities above 99 percent. For the video equipment, the fixed cameras and video server had average availabilities above 99 percent, but the PTZ cameras experienced numerous outages during the last nine reporting periods of the evaluation, resulting in an average availability of 92 percent. This observation of the PTZ camera outages for ESM was in-line with the utility's previous experience with this type of PTZ camera, where similar cameras at non-ESM facilities were found to last about three to five years before failing.

The data completeness metric considers communications and equipment availability. The high level of intrusion detection equipment availability led to an average data completeness of 98.6 percent, but the communications and PTZ camera issues and caused the video equipment data completeness to average 93 percent.

Section 5.0: Non-Video Monitored Sites

The following section provides a description of the non-video monitored sites followed by the results of the evaluation of this data stream. This analysis includes an evaluation of metrics that characterize how these sites achieve the design objectives described in Section 1.1. Specific metrics are described for each of the design objectives.

5.1 Description

Non-video sites that received ESM equipment included four reservoirs (one underground and three above-ground), four elevated storage tank, and one ground-level storage tank. For reservoirs, rectangular fabricated aluminum structures were added over the existing vents to eliminate direct access to the vents. The structures were fitted with sidewalk style hatches to provide access to the vents for inspection and cleaning. Two types of intrusion detection devices were installed at each vent enclosure. One was a contact switch on the hatch that sends an intrusion alert when the hatch is opened. The other was a liquid-level switch installed at the base of the enclosure sidewall. The liquid-level switches were provided to detect a situation in which a liquid contaminant would be introduced by plugging the drain holes and the louvers of the enclosure. The liquid level switch inside the enclosure would send an intrusion alert to the control center if the fluid level in the structure rises to the detection level. The existing access hatches on the reservoirs were previously fitted with contact switches. The intrusion alert contacts at the vent enclosure were wired in series with the existing access hatch alert contacts.

Each elevated and ground-level storage tank provides access to finished (treated) water at the top of the storage bowl via a ladder in either the center column or a side column (in the case of the ground level storage tank). The entrance doors to the tank were protected by existing contact switches, so motion sensors were installed on the ladders to indicate if an intruder was attempting to access the water at the top of the storage bowl. The tanks' bottom areas typically contain equipment in addition to the ladder, so the motion sensors were installed at least 30 feet up the ladder to reduce invalid alerts from movement by personnel at floor-level (i.e., only an intruder climbing the ladder would be sensed). Both the door contact switch and the ladder motion sensor alerts would be transmitted to the operators at the utility control center. This approach provided two sources of alerts, which helped to screen out invalid alerts arising from motion sensor oversensitivity and from utility personnel who enter the tank base and forget to call the control center.

5.2 Design Objective: Spatial Coverage

As with video monitored sites, ESM non-video monitored sites each covered only one access point to the distribution system, thus limiting their detection capability and system-wide spatial coverage. However, the consequences if a contamination incident did occur at an ESM site may be widespread. To protect against contamination incidents, non-video monitored sites were equipped with intrusion detection devices at all points of entry that could allow an intruder access to the water supply. This supplemented their existing intrusion detection devices, which were primarily intended to detect theft and vandalism incidents.

5.3 Design Objective: Contaminant Coverage

ESM did not consider specific contaminants or detection classes of contaminants, but the volume of contaminants and method of contaminant injection were considered during ESM design of the non-video monitored sites. For elevated and ground storage tanks, the design assumed a contaminant volume that

could fit into an intruder's backpack for ease of ladder climbing. A pumped contaminant is possible but less convenient, since the perpetrator would need to climb the ladder while transporting a hose to the upper level of the tank. For reservoir vents, the design assumed that a perpetrator would use a hose to pump the contaminant into the vent, since pouring liquid directly into the vent would be prevented by the shrouds over them. For pump-injected contaminations, a 55-gallon drum or tank truck was assumed. Based on these assumptions, all applicable points of contamination at the non-video sites were monitored.

5.4 Design Objective: Alert Occurrence

See Section 4.4.1 for a general discussion of invalid alerts.

5.4.1 Invalid Alerts

Invalid alerts caused by security procedure violations were segregated into "no call-in" and "hatch left propped open (hatch prop)" categories. Each security procedure category was divided by type of facility, including ladder and reservoir sites. Invalid alerts caused by equipment issues were categorized by equipment type including "hatch sensors" and "ladder motion sensors." The ladder motion sensors installed at video sites are discussed below with the ladder motion sensors installed at non-video monitored sites. Environmental causes were the third category of invalid alert causes, but since only a handful of invalid alerts were attributed to environmental factors, this category was not included in the analysis. None of the intrusion sensors at non-video sites were outdoors.

To generalize the invalid alert data, the security procedure violation metrics were normalized by the number of valid entries and where applicable, the number of hatches. Invalid alerts due to equipment issues were normalized by the number of sensors.

To implement the above categorizations of invalid alerts, this section is organized as follows:

- Security Procedure Violations – Hatch Props
  - Ladder sites
  - Reservoir sites
- Security Procedure Violations – No Call-Ins
  - Ladder sites
  - Reservoir sites
- Equipment-Caused Invalid Alert
  - Ladder Motion Sensors
  - Ladder Hatch Sensors
- Reservoir Hatch Sensors

Security Procedure Violations: Hatch Props

Definition: A *security procedure violation* occurred when an employee did not follow security procedures and an invalid alert was generated. A hatch prop was a type of security procedure invalid alert that occurred when authorized personnel left a hatch propped open that should have been closed when they left the facility.

Standard operating procedures require that the utility control center operator enable the intrusion alerts at a facility after personnel notify the operator that they have left the premises. A hatch prop invalid alert occurred when the intrusion alert on the GCWW SCADA system was enabled, and the system detected that a secure hatch was left open. All intrusion detection devices at non-video monitored sites use the GCWW SCADA system for displaying intrusion alerts at the utility control center. The intrusion alert on the GCWW SCADA system can be enabled by the utility control center operator using an HMI.

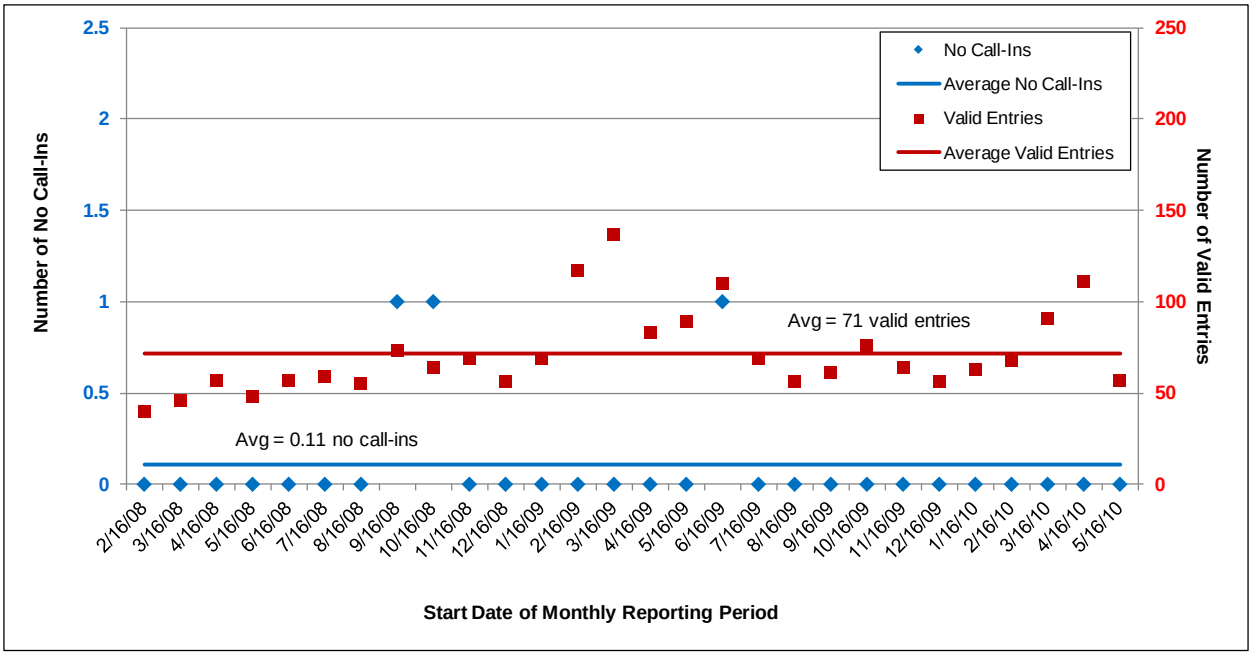
Analysis Methodology and Results: No hatch props were observed at non-video sites during the entire evaluation period.

Security Procedure Violations: No Call-Ins

Definition: A *no call-in security procedure violation* occurred when GCWW personnel did not follow established procedures for calling the utility control center within a designated time span of entering a facility. An intrusion alert is generated automatically when anyone enters a facility, but the alert is considered a valid entry if an employee called in a designated time span. For non-video monitored sites, a no call-in incident could be verified when onsite investigators or local law enforcement arrived at the facility and witnessed the employees at the site.

Analysis Methodology: This metric was segregated by ladder sites and reservoir sites. Segregation by site type allowed the analysis of each type individually and also comparison among types. The no call-in data were normalized by the number of valid entries to a site, since a frequently visited facility would have a higher probability of an employee not calling in.

Results: **Figure 5-1** shows the "no call-in" metrics for the ladder sites. Since all ladder sites are unstaffed, all employees must call the utility control center to announce arrival, regardless of time of day.



Note: There were only three no call-in incidents at ladder sites.

Figure 5-1. Ladder Sites: No Call-Ins

Reporting periods with a no call-in incident did not usually have an above average number of valid entries. One of three reporting periods that had a no call-in incident also had an above average number of valid entries.

The number of invalid alerts due to no call-ins did not decrease over the course of the evaluation period, likely because ESM did not implement significant changes to the utility's call-in procedures.

Figure 5-2 shows the no call-in metrics that are normalized by the number of valid entries at the ladder sites. This normalization factor was chosen because having a larger number of valid entries could increase the probability of no call-in occurrence.

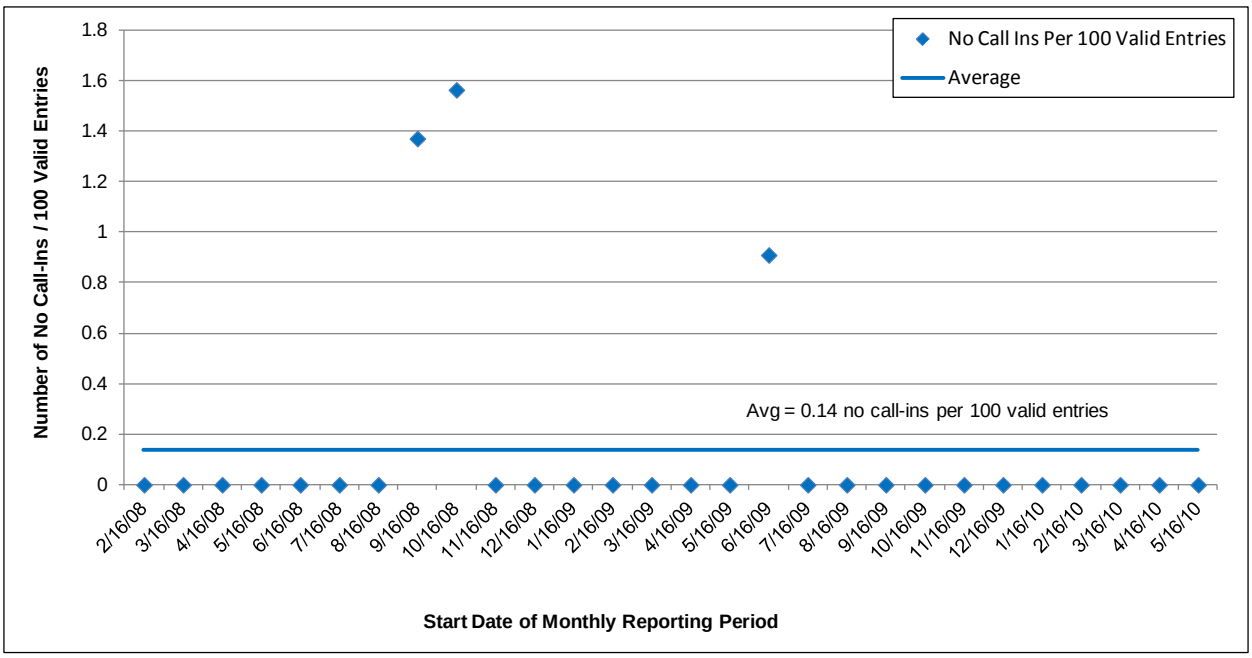
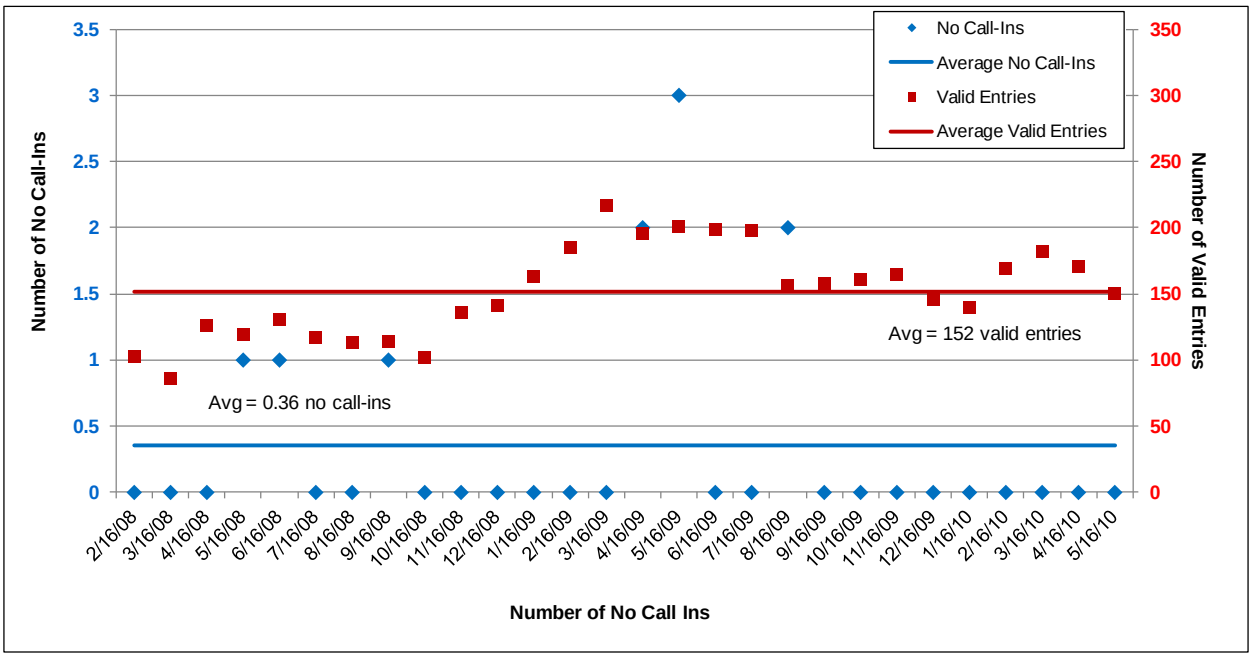


Figure 5-2. Ladder Sites: No Call-Ins/Valid Entries

The ladder sites had significantly less normalized no call-ins compared to the pump stations (previously discussed in Section 4.4.1). The pump station with the lowest average normalized no call-ins had 1.19 no call-ins/100 valid entries compared to 0.14 for the ladder sites.

Figure 5-3 shows the "no call-in" metrics for the reservoir sites. Since all reservoir sites are unstaffed, all employees must call the utility control center to announce arrival, regardless of time of day.



Note: There were only ten no call-in incidents at reservoir sites.

Figure 5-3. Reservoir Sites: No Call-Ins

Reporting periods with a no call-in incident usually did not have an above average number of valid entries. Three of six reporting periods had a no call-in incident and also an above average number of valid entries.

The number of invalid alerts due to no call-ins did not decrease over the course of the evaluation period, likely because ESM did not implement any significant changes to the utility's call-in procedures. The utility's efforts to reiterate the call-in policy to employees was an ongoing process.

Figure 5-4 shows the no call-in metrics normalized by the number of valid entries at the reservoir sites. A normalization factor was chosen, because having a larger number of valid entries could increase the probability of no call-in occurrence.

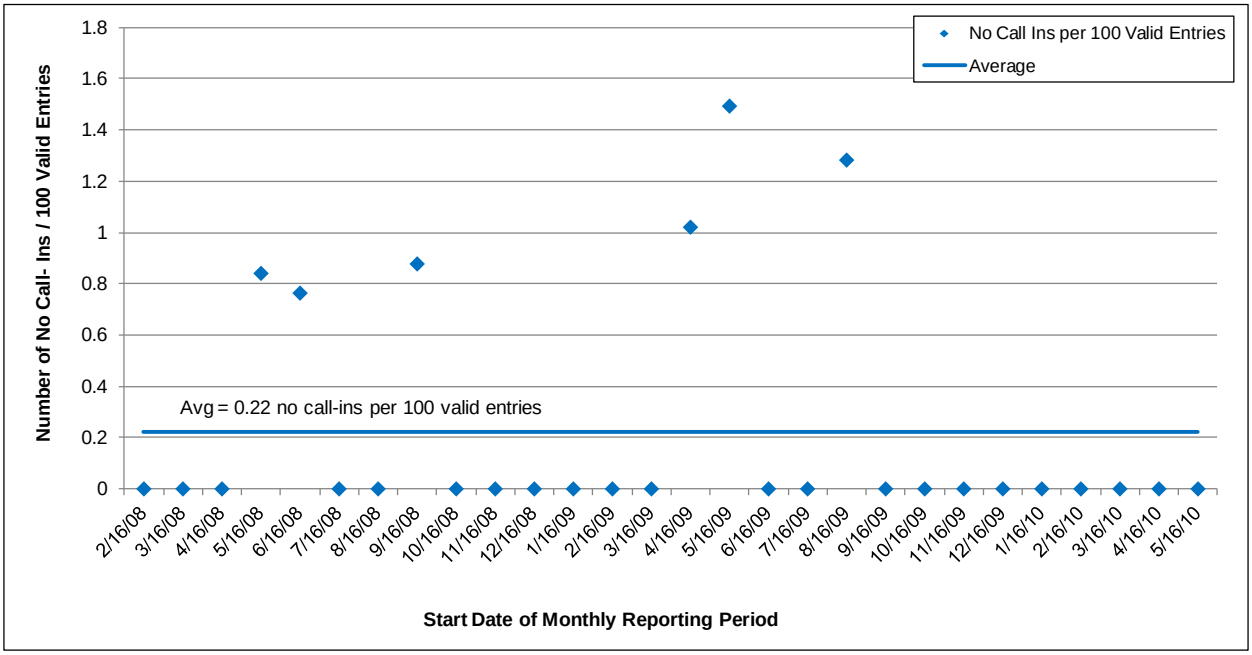


Figure 5-4. Reservoir Sites: No Call-Ins/Valid Entries

Invalid alerts due to no call-ins at reservoir sites only occurred during the Spring and Summer months at a frequency of approximately one per 100 valid entries. Similar to the non-normalized no call-ins, the normalized number of invalid alerts due to no call-ins did not decrease over the course of the evaluation period. This was likely because ESM did not implement any significant changes to the utility's call-in procedures. The utility's efforts to reiterate the call-in policy to employees was an ongoing process.

The reservoir sites had significantly less normalized no call-ins compared to the pump stations and more normalized no call-ins compared to the ladder sites. The pump station with the lowest average normalized no call-ins had 1.19 no call-ins/100 valid entries compared to 0.22 for the reservoir sites. The ladder sites had 0.14 no call-ins/100 valid entries.

Table 5-1 compares the non-normalized and normalized no call-in metrics for the ladder and reservoir sites. Pump Station A and C metrics from the video monitored sites are also shown in the table for comparison with the ladder and reservoir metrics. Pump Station A had the lowest average non-normalized no call-ins, while the Pump Station C video monitored site had the lowest average normalized no call-ins.

The ladder sites had fewer non-normalized and normalized average no call-ins than did the reservoir and pump station sites. The ladder sites were visited less frequently than the pump stations and reservoirs.

Table 5-1. Summary of Non-Video Site No Call-In Data

Location	Average Number of No Call-ins per Reporting Period	Normalized Average Number of No Call-Ins per 100 Valid Entries	Average Valid Entries
Ladder Sites	0.11	0.14	71 (14)[1]
Reservoir Sites	0.36	0.22	151 (38)[1]
Non-Video Sites, Combined Average	0.23	0.18	112
Pump Station A	1.1	2.37	47
Pump Station C	1.4	1.19	127

1. For ladder and reservoir sites, the average valid entries per site are shown in parentheses. The lowest pump station averages are shown for comparison.

Equipment-Caused Invalid Alerts

Definition: An *equipment-caused invalid alert* occurs when an equipment issue caused an intrusion detection device to trigger an alert when there was no intrusion. The following section discusses invalid alerts at non-video sites caused by equipment issues with ladder motion, ladder hatch, and reservoir hatch sensors. The discussion on ladder motion sensors includes the two ladder motion sensors installed at video monitored sites.

The ladder sensors at non-video sites have a unique equipment-caused invalid alert, the radio fault. The radio fault is a feature of the GCWW SCADA network. The non-video sites used the existing GCWW SCADA network for transmitting the ESM intrusion alerts to the utility control center. Certain GCWW remote sites used wireless I/O modules to transmit data to a facility with a hardwired connection to the GCWW SCADA network. Three of the five ladder sites at non-video locations used wireless I/O modules. An invalid ladder alert was triggered when the wireless I/O module experienced a loss in signal strength, which could result from signal path blockage or radio interference. Usually a radio fault was transmitted to the GCWW SCADA network with the ladder alert following loss in signal strength, but there were also occasions where a radio fault was not generated but a false tank level alert accompanied the false ladder alert. Both conditions were used to determine when a ladder alert was caused by a radio issue.

The four other ladder sites were not subject to radio fault invalid alerts. Two of the five ladder sites at non-video locations were at a facility with a hardwired connection to the GCWW SCADA network and did not use wireless I/O modules. The two ladder sites at video locations were connected to the ESM system, which was not part of the GCWW SCADA network.

Analysis Methodology: This metric was segregated by the site types listed in Section 4.4.1. The site types include the following types of equipment:

- Ladder motion sensors
- Ladder hatch sensors
- Reservoir hatch sensors

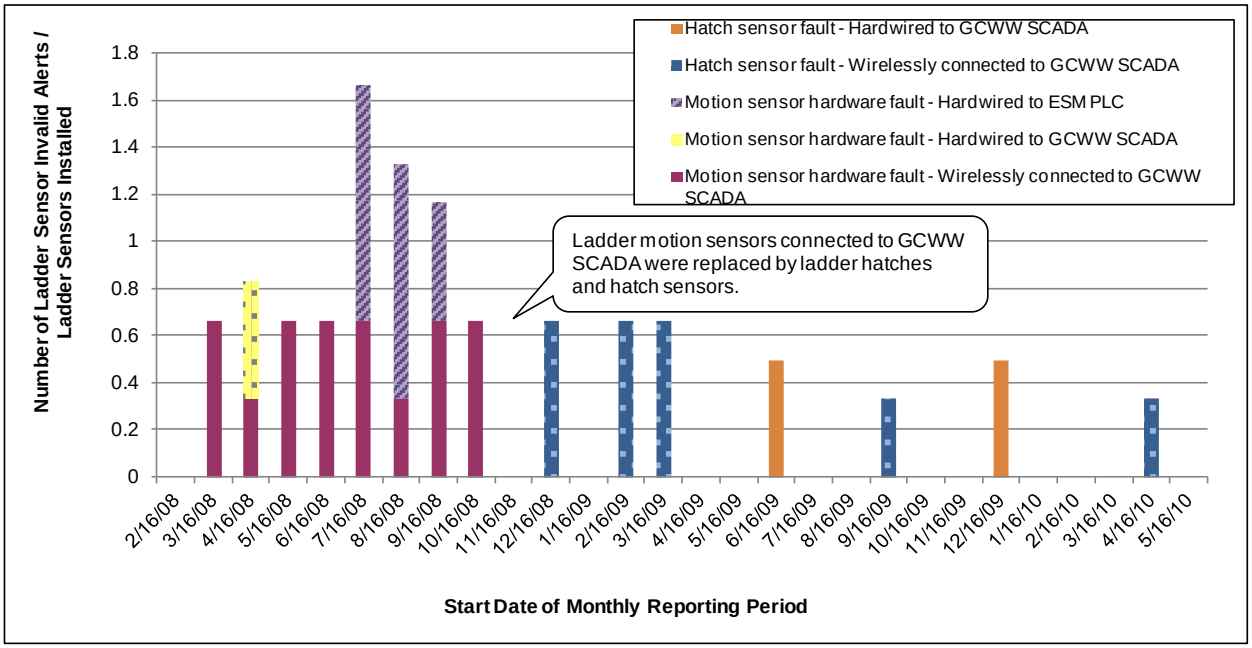
There were no equipment-caused invalid alerts at the reservoir sites, and subsequently no analysis for reservoir hatch sensors was performed.

The segregation of equipment by type allowed for an analysis of each type individually and also allowed for comparison among types. The number of equipment-caused invalid alerts was normalized by the number of sensors for each type, since a higher number of installed sensors increased the probability of having an invalid alert. The analysis for equipment-caused invalid alerts was not divided by site, since the causes of these invalid alerts were equipment-specific, rather than site-dependent.

These equipment-caused invalid alerts for ladder sensors were categorized as wirelessly connected to GCWW SCADA, wired to GCWW SCADA, and wired to ESM PLC. Because there were ladder sensor invalid alerts caused by the wireless connection on the GCWW communications network, the radio fault generated alerts also were analyzed.

Data for ladder motion sensors at non-video sites were not available over the entire evaluation period, as the ladder motion sensors were removed in December 2008. Discussion following Drill 1 indicated that interior motion sensors did not provide enough information about the intrusion, including whether an intruder had actually climbed the ladder to get access to the water. Therefore, the ladder motion sensors were replaced with ladder hatches and ladder guards that were monitored by hatch sensors, which would more definitively indicate whether the ladder was climbed to gain access to the drinking water. The exterior ladder motion sensors, however, remained in service. After December 2008, the ladder hatch sensors invalid alerts were analyzed in place of the ladder motion alerts at the non-video sites.

Results: **Figure 5-5** shows the normalized equipment-caused invalid alert metrics for ladder motion and ladder hatch sensors. The reporting period when the ladder motion sensors at non-video sites were replaced by ladder hatch sensors (December 2008) is noted on the graph. **Table 5-2** summarizes the data on Figure 5-5. For comparison purposes, Table 5-2 also includes equipment-caused invalid alert data for area motion sensors and door/hatch sensors from the video sites. Table 5-2 also presents industry standards for invalid alert rates from the *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA, 2006).



Note: Replacing the ladder motion sensors at non-video sites with ladder hatches reduced the number of ladder invalid alerts. The ladder motion sensors connected to the ESM PLC were not replaced with ladder hatches.

Figure 5-5. Ladder Sensor Invalid Alerts Caused By Sensor Faults

Table 5-2. Sensor Caused Invalid Alerts: Average Times Between Invalid Alerts

Sensor	Days Between Invalid Alerts per Sensor	Invalid Alerts per Sensor per Year
Ladder Motion Sensors—Wirelessly connected to GCWW SCADA	65	5.6
Ladder Motion Sensors—Hardwired to GCWW SCADA	608	0.6
Indoor Ladder Motion Sensors (Average of all motion sensors connected to GCWW SCADA)	101	3.6
Ladder Motion Sensors—Hardwired to ESM PLC (CWS SCADA) (Outdoors)	338	1.1
Ladder Motion Sensors—Total	160	2.3
Ladder Hatch Sensors—Wirelessly connected to GCWW SCADA	203	1.8
Ladder Hatch Sensors—Hardwired to GCWW SCADA	541	0.67
Ladder Hatch Sensors—Total	271	1.3
Reservoir Hatch Sensors	Note 1	Note 1
Area Motion Sensors—Video Sites	136	2.7
Door/Hatch Sensors—Video Sites	1,168	0.31
ASCE/AWWA (2006) Guideline	90 (minimum)	4 (maximum)

1. There were no invalid alerts for this equipment type over the evaluation period, so the value of this metric could not be calculated.

Overall the ladder hatch sensors were less prone to equipment-caused invalid alerts than ladder motion sensors. The ladder hatch sensors averaged 271 days between invalid alerts while the ladder motion sensors averaged 160 days between invalid alerts.

The ladder hatch sensors were more prone to equipment-caused invalid alerts than the door/hatch sensors installed at video sites. The ladder hatch sensor was the same physical sensor as the door/hatch sensor, but installation on a ladder hatch was more complex than installation on a door and required post-installation repositioning at some locations. Utility staff required training on the new ladder hatches to ensure that the hatches were completely closed. There was a slight decreasing trend in the ladder hatch alerts as training was provided to utility staff on the new procedures.

The outdoor ladder motion sensors at video sites (hardwired to ESM PLC) did not have a higher invalid alert rate compared to the indoor ladder motion sensors. Most of the indoor ladder motion sensors were connected wirelessly to the GCWW SCADA system. GCWW suspected that many of the equipment-caused sensor invalid alerts may have actually been caused by wireless communications errors that were undetected by the wireless I/O module's radio fault. The inconsistent nature of the radio fault function on GCWW wireless communication equipment is discussed above under "Definition."

Most ladder motion sensor and ladder hatch sensor equipment-caused invalid alerts met the ASCE/AWWA (2006) guidelines. The exception was the ladder motion sensors that were wirelessly connected to the GCWW SCADA system. These devices averaged 65 days between invalid alerts compared to the ASCE/AWWA (2006) minimum of 90 days. Issues with the radio fault function on the wireless I/O modules were suspected as discussed in the previous paragraph. The average sensor-caused invalid alert rate for all indoor motion sensors was 101 days between invalid alerts, which met the ASCE/AWWA (2006) guidelines. For ladder motion and ladder hatch sensors, the hardwired sensors had

significantly less invalid alerts than wirelessly connected counterparts. Issues with the radio fault function on the wireless I/O modules were suspected. See the above paragraphs for a discussion.

Figure 5-6 shows the normalized radio fault caused invalid alert metrics for ladder motion and ladder hatch sensors. The reporting period when the GCWW SCADA programming was modified (December 2008) is noted on the graph.

The number of radio-caused invalid alerts was much greater than the equipment-caused invalid alerts at ladder sites. There was less than one equipment-caused invalid alert per ladder site per reporting period, compared to five radio-caused invalid alerts per ladder site per reporting period.

The GCWW SCADA programming changes reprogrammed the utility's remote telemetry unit to wait five seconds after a ladder alert before transmission of the ladder alert to the utility's HMI. If a radio fault occurred during the five second waiting period, the ladder alert was not transmitted. This change reduced invalid alerts while not impacting the system's ability to detect real intrusion incidents.

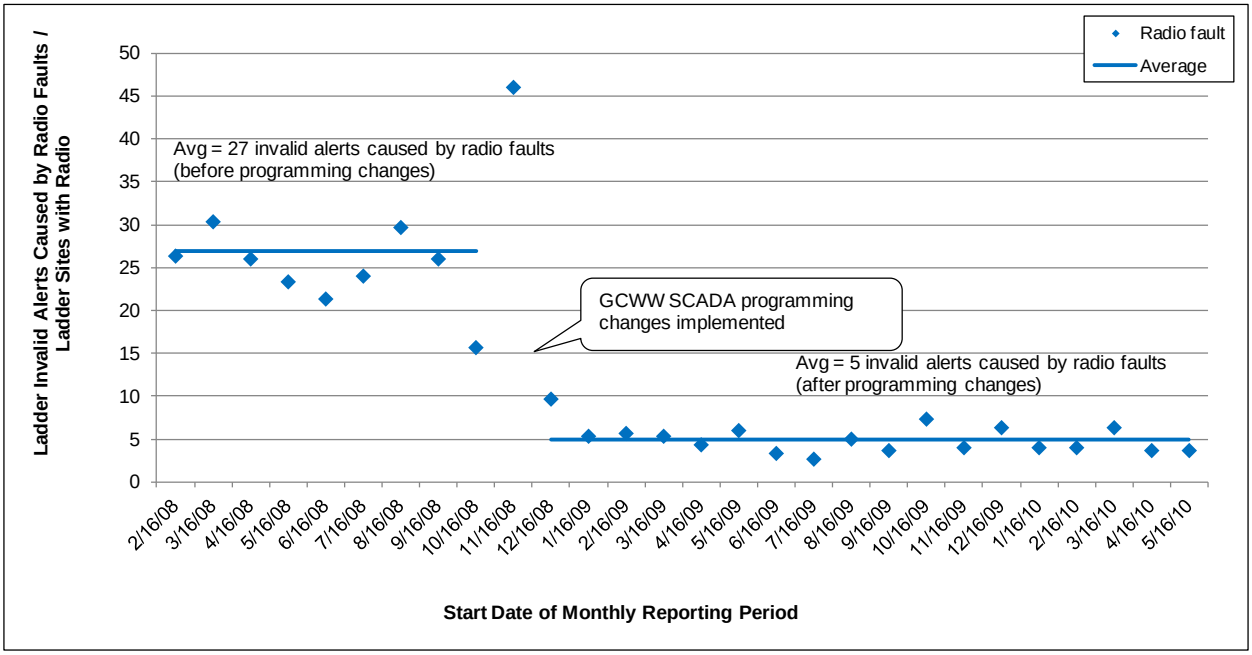


Figure 5-6. Ladder Sensor Invalid Alerts Caused By Radio Faults

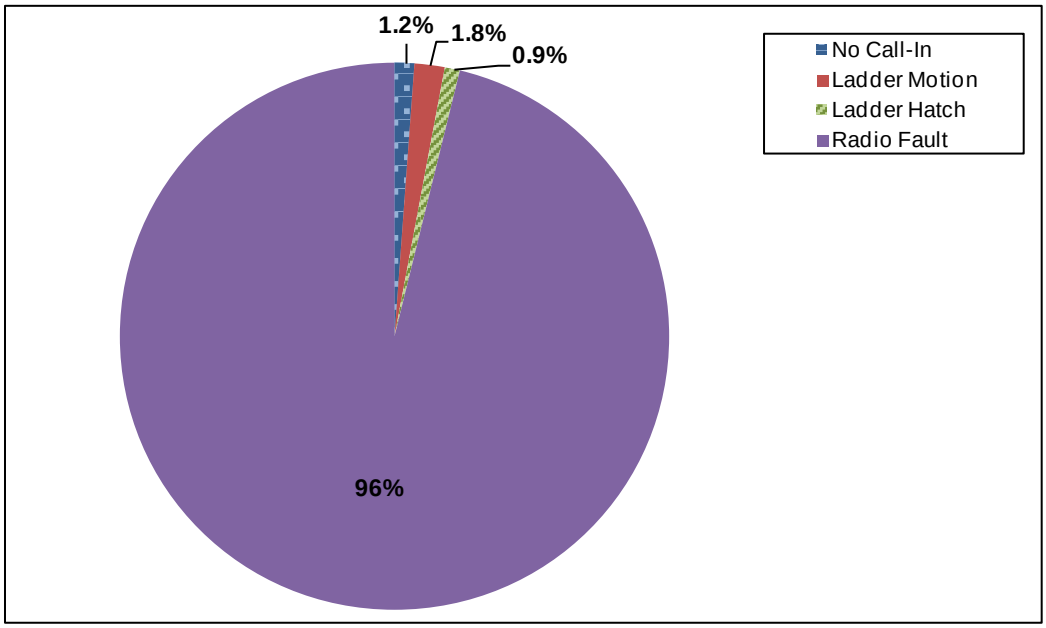
Table 5-3 shows the invalid alert rates and costs for ladder motion and ladder hatch sensors. For comparison purposes, Table 5-3 also includes the invalid alert rates and costs for the area motion sensors and door/hatch sensors in addition to the industry standards from the *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA, 2006).

Table 5-3. Equipment Caused Invalid Alerts: Average Times between Invalid Alerts

	Area Motion Sensors	Door/Hatch Sensors	Ladder Motion Sensors	Ladder Hatch Sensor	ASCE/AWWA Guideline
Days Between Invalid Alerts per Sensor	136	1,168	160	271	90 (minimum)
Invalid Alerts per Sensor per Year	2.7	0.31	2.3	1.3	4 (maximum)
Cost per Device (2007 list prices)	$450	$260	$1,660	$260	n/a

The ladder motion sensors were costly and appeared to be relatively prone to invalid alerts. Undetected radio faults may have caused an overestimation of equipment-caused invalid alerts for the ladder motion sensors. This topic is discussed under "Definition" and in the analysis following Figure 5-8.

Figure 5-7 presents the percentage of each type of invalid alert at the non-video monitored sites, which included security procedure (no call-in) and equipment caused (ladder motion sensor, hatch sensor and radio fault) invalid alerts.



Note: Most invalid alerts were radio faults.

Figure 5-7. Non-Video Site Invalid Alerts by Type

Radio faults caused 96 percent of all invalid alerts at non-video sites. There were no security procedure violations caused by door or hatch props at non-video sites. There were no equipment invalid alerts from hatches at non-video sites. The ladder sensors installed at pump stations were included in this analysis.

Table 5-4 presents the percentage of invalid alerts from each non-video monitored site.

Table 5-4. Non-Video Site Invalid Alerts by Location

Invalid Alert Type	Percentage
Elevated Tank A	20.71%
Elevated Tank B	51.70%
Elevated Tank C	0.27%
Ground Tank D	0.09%
Elevated Tank E	25.89%
Reservoir A	0.36%
Reservoir B	0%
Reservoir C	0.09%
Reservoir D	0.45%
Ladder Motion Alerts at Pump Stations	0.45%
Total	100.00%

Note: Most invalid alerts were at Elevated Tanks with wireless I/O modules.

The elevated tanks that used wireless I/O modules to connect to the GCWW SCADA system were Elevated Tanks A, B, and E, which accounted for 98 percent of all invalid alerts at non-video sites. Wireless I/O modules experienced frequent invalid alerts caused by radio faults. See the definition discussion of Section 5.5.4 and the discussions following Figures 5-5 and 5-6 for details on the wireless I/O modules and radio faults.

5.4.2 Summary

The alert occurrence design objective was evaluated by examining the invalid alert rates, which measure a security system's effectiveness. The invalid alerts were categorized into security procedure violations and equipment caused invalid alerts.

For the security procedure violation invalid alerts, data showed the non-normalized and normalized averages per reporting period were 0.11 no call-ins and 0.14 no call-ins/100 valid entries at ladder sites, and 0.36 no call-ins and 0.22 no call-ins/100 valid entries at reservoir sites. These no call-in amounts were an order of magnitude lower than the lowest pump station average no call-in values, which are shown in Table 5-1. Despite the utility's ongoing efforts to reiterate the call-in policy to employees, there was a slight increasing trend in no call-ins at the reservoir sites. The other type of security procedure violation invalid alert was the hatch prop. There were no hatch props at the non-video sites during the evaluation.

For equipment-caused invalid alerts, the reservoir hatch sensors had no invalid alerts during the evaluation. Ladders at non-video sites originally were monitored by ladder motion sensors. The ladder motion sensors at non-video sites were replaced by ladder hatch sensors during the December 2008 reporting period as a result of recommendations from ESM Drill 1. See Table 2-4 in Section 2.3 for a discussion on this component modification. Overall the ladder hatch sensors had a lower equipment-caused invalid alert rate than the ladder motion sensors, averaging 271 days between invalid alerts per sensor compared to 169 days per sensor for the ladder motion sensors. Both sensors met the ASCE/AWWA (2006) guideline of a minimum of 90 days between invalid alerts per sensor. Ladder sites that used a wireless connection to the GCWW SCADA system also experienced a significant number of radio-caused invalid alerts. Initially there were about 27 radio-caused invalid alerts per sensor, which was

reduced to five radio-caused invalid alerts per sensor after GCWW SCADA programming changes were implemented. The equipment-caused (non-radio related) invalid alert rate was less than one invalid alert per sensor. Radio faults caused 96 percent of all invalid alerts at non-video sites. Most of invalid alerts at non-video sites occurred at the locations that used wireless equipment that were prone to radio faults.

5.5 Design Objective: Timeliness of Detection

For non-video monitored sites, timeliness of detection is the time to determine Possible contamination. The timely determination by utility personnel is vital to ensuring a potential contamination incident is addressed as quickly as possible once the intrusion detection equipment has alerted. Intrusion alert data was collected at non-video monitored sites, and is discussed in Section 6.4.1 where these metrics are compared with those from video monitored sites.

5.6 Design Objective: Operational Reliability

See Section 4.6 for the definition of the operational reliability design objective.

5.6.1 Availability of Intrusion Alert Communication System

Definition: Availability of intrusion alert communication system is the percentage of time that intrusion alert data were successfully transmitted.

Analysis Methodology: The communications system availability for all non-video sites per reporting period is shown. The calculation for percent available is:

$$\frac{(\text{Potential Communication Hours Available} - \text{Communication Hours Unavailable})}{\text{Potential Communication Hours Available}} \times 100$$

Potential communication hours available for all non-video sites is the number of hours in the reporting period multiplied by the number of non-video sites. *Communication hours unavailable* is the number of hours the communications was not working properly at each non-video site per reporting period.

Results: Figure 5-8 shows the communications system availability for intrusion alert data at the non-video monitored sites. Each non-video site had only one ESM intrusion alert, so the ESM alerts were added to the existing GCWW SCADA communications network without adversely affecting communications of the existing GCWW data. Since non-video sites used the existing GCWW SCADA system, the digital cellular issues that hampered the video-monitored sites did not affect intrusion alert communications.

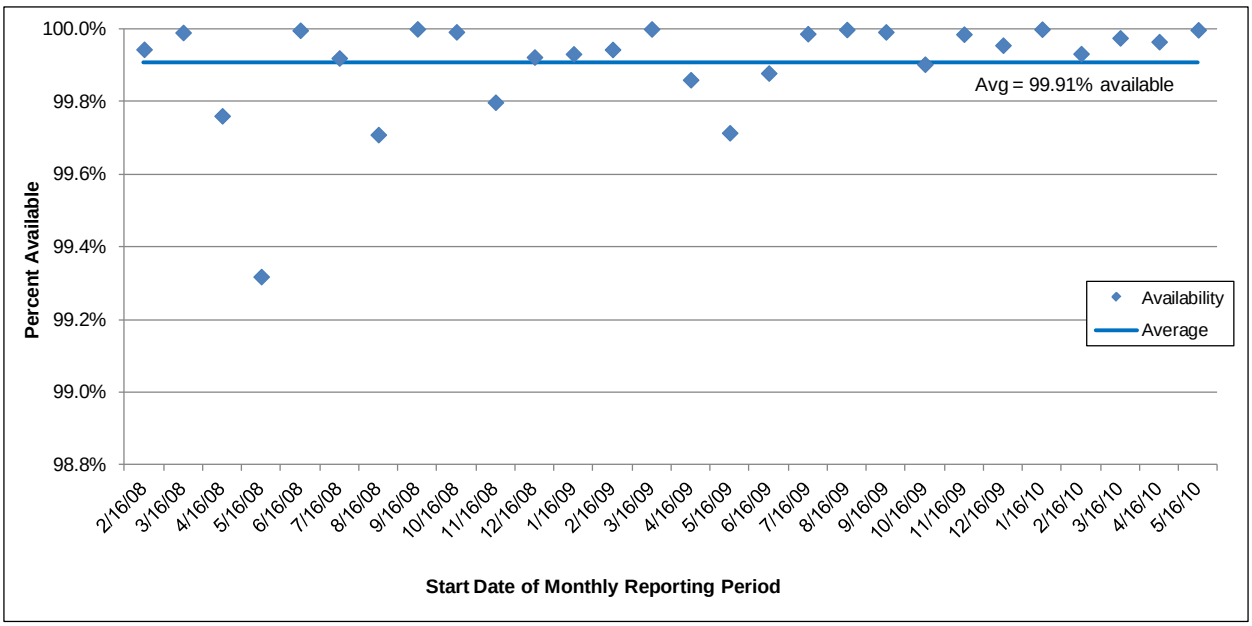


Figure 5-8. Communications System Availability: Non-Video Sites

All reporting periods had availability greater than 99.3 percent. Twenty of 28 reporting periods were above the average availability of 99.91 percent. Only one reporting period, which had an availability of 99.3 percent, was less than 99.7 percent.

5.6.2 Availability of Intrusion Detection Equipment

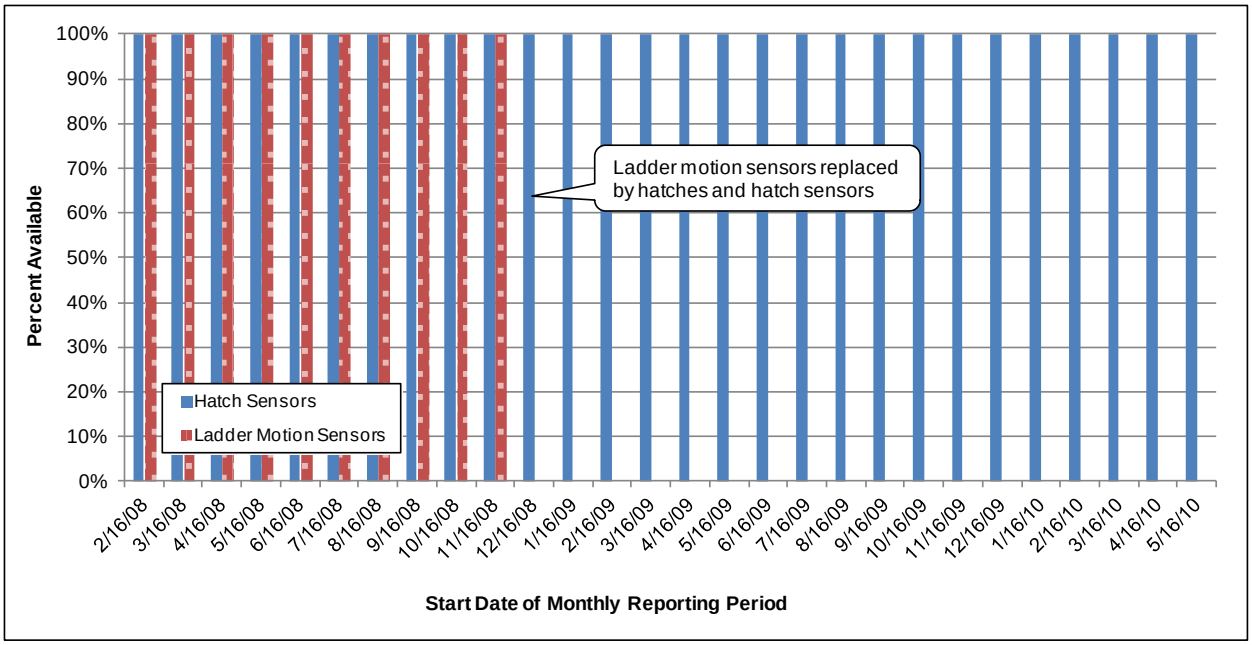
Definition: Availability of intrusion detection equipment was defined as the percentage of time that the hatch sensors, level sensors and ladder motion sensors were functioning properly. The hatch and level sensors were wired in series, so the sensors were treated as one device for this report.

Analysis Methodology: The equipment availability for the different types of intrusion detection devices at non-video sites for each reporting period is shown. The calculation for percent available for each type of intrusion detection device is:

$$\frac{(\text{Potential Equipment Hours Available} - \text{Equipment Hours Unavailable})}{\text{Potential Equipment Hours Available}} \times 100$$

Potential equipment hours available is the number of hours in the reporting period multiplied by the number of equipment of that type installed at the non-video sites. *Equipment hours unavailable* is the number of hours that the equipment was not working for each type of equipment per reporting period.

Results: **Figure 5-9** shows the availability for the intrusion detection devices used at non-video sites, including ladder motion sensors and hatch sensors.



Note: Hatch contact sensors and ladder motion sensors were always available.

Figure 5-9. Intrusion Detection Equipment Availability - Non-Video Sites

No intrusion detection equipment failures occurred during the evaluation period. During the December 2008 reporting period, hatch sensors replaced ladder motion sensors at the non-video sites, based on feedback from ESM Drill 1 (see Table 2-4).

5.6.3 Data Completeness

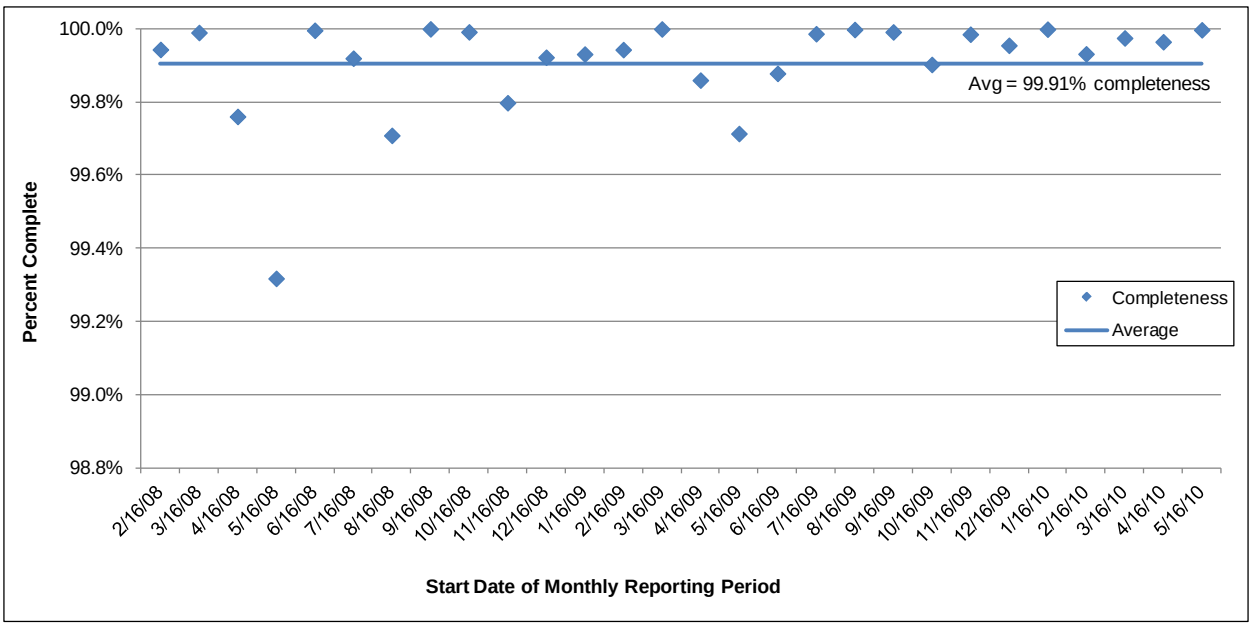
Definition: *Data completeness* is the number of data hours that can be used to support component operations, expressed as a percentage of all data generated by the component.

Analysis Methodology: The data completeness for intrusion detection equipment at non-video sites is shown. The calculation for data completeness is:

$$\frac{(\text{Potential Data Hours Available} - \text{Data Hours Unavailable})}{\text{Potential Data Hours Available}} \times 100$$

Potential number of data hours available is calculated using the number of intrusion detection data streams multiplied by the number of hours in the reporting period. *Data hours unavailable* is the number of hours that the data stream was not working properly per reporting period. Each data stream represents the output from an individual intrusion detection device. Additionally, downtime due to communications outages caused all the intrusion alert data streams from that location to be considered invalid.

Results: Figure 5-10 shows the completeness for all non-video intrusion alert data streams. The data completeness metric includes downtime from communications and equipment faults. Each data stream represents the output from an individual intrusion detection device.



Note: The data completeness was equal to the communications availability, because the equipment availability at non-video sites was 100%.

Figure 5-10. Data Completeness for Non-Video Sites

The data completeness values combined the trends shown in Figures 5-8 and 5-9, which show the communications availability and intrusion equipment availability. The data completeness was equal to the communications availability shown on Figure 5-8, because the equipment availability at non-video sites was 100 percent.

5.6.4 Summary

The operational reliability design objective was evaluated by examining the intrusion alert communications availability, equipment availability, and data completeness. At the non-video monitored sites, intrusion alert data transmission availability averaged 99.91 percent per reporting period, with the lowest reporting period averaging 99.3 percent. The intrusion detection equipment availability was 100 percent over the evaluation period, so the data completeness was the same as the intrusion alert data transmission availability. Intrusion alert data transmission at the non-video sites was not subject to the digital cellular issues that affected video data communications because the non-video sites used the GCWW SCADA network to transmit data.

Section 6.0: Performance of the Integrated Component

The previous two sections provided a description of metrics and results related to aspects unique to video monitored and non-video monitored sites. The analysis in the section includes an evaluation of metrics that pertain to the integrated component and how it achieves the design objectives described in Section 1.1. Specific metrics are described for each of the design objectives.

6.1 Description

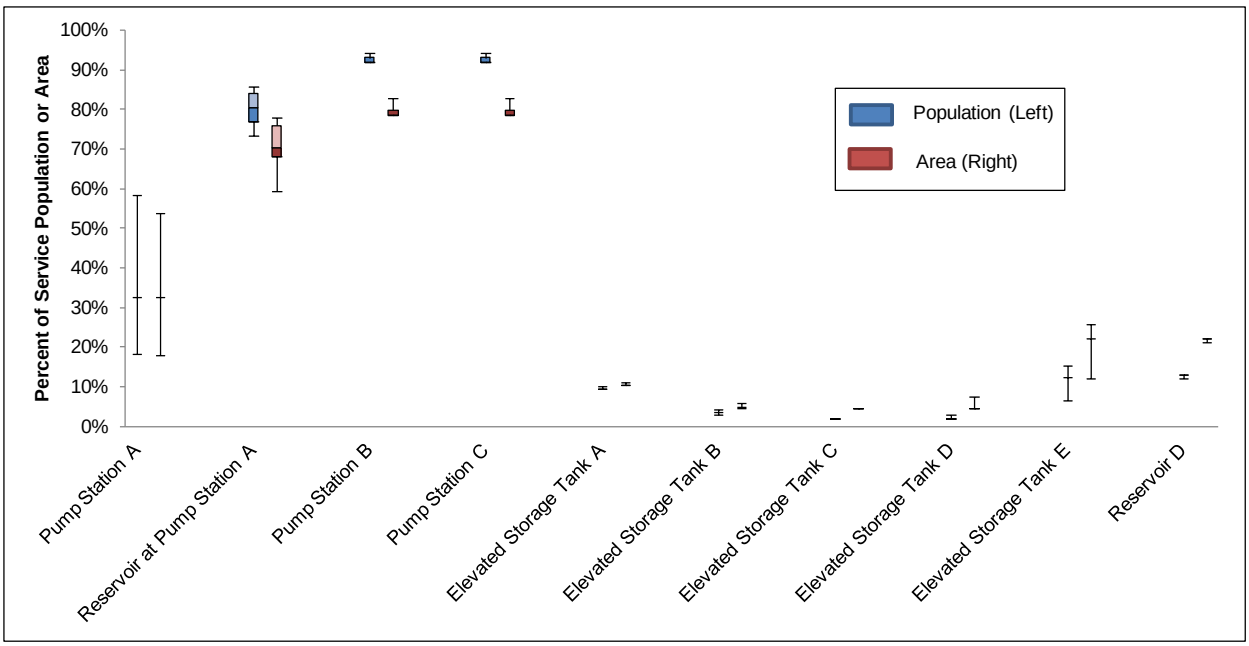
Proper integration of all ESM security processes is crucial to implementing a comprehensive CWS which will provide an effective defense against a contamination incident in a utility's distribution system. Refer to Sections 4.1 and 5.1 for more detailed discussions of each security system that form the integrated ESM component.

6.2 Design Objective: Spatial Coverage

Definition: Each ESM site covered only one access point to the distribution system, thus limiting their detection capability and spatial coverage. However, the consequences if a contamination incident did occur at an ESM site may be widespread. This analysis considered each ESM site and estimated the service area impacted should each site experience a contamination incident.

Analysis Methodology: The CWS simulation model was used to estimate the service area protected by an ESM-equipped site by determining the area and population that would be impacted by an uninterrupted contaminant injection at the ESM site. The model calculates the contaminant spread from an injection location until the contaminant concentration is not detectable or harmful, and the area affected by the incident is called the Zone of Influence (ZOI). The area of and population within the ZOI for each scenario originating at an ESM site were tabulated, and the percentile values for individual sites were calculated to examine the distribution of data. Additionally, a non-overlapping superset of the ZOIs from each ESM scenario was developed to determine the overall population and area coverage for the ESM component.

Results: There were 170 scenarios that involved ESM locations, and the statistics for the population and area for each ESM location are presented below in **Figure 6-1**. Variations in ZOI were due to differences in hydraulics and contaminant toxicity. Overall, the model indicated that the ESM component covered 99 percent of the retail population and 96 percent of the retail service area.



Notes:
- Elevated Storage Tanks A and D: 10th, 25th, 50th and 75th percentiles are the lower bar, 90th is the upper bar
- Reservoir D: 10th percentile is the lower bar, 25th, 50th, 75th and 90th percentiles are the upper bar.
- The simulated contamination scenarios at Reservoirs A, B and C did not result in detectable or harmful levels of contaminant introduced into the system.

Figure 6-1. Percent Population and Area of Zone of Influence at ESM Sites

Figure 6-1 shows that the Pump Stations B and C, and Reservoir at Pump Station A had the largest ZOIs, with median values of 81 to 93 percent population and 70 to 80 percent area of the retail service area impacted, thus supporting the design decision to install a higher level of surveillance capability (video monitoring equipment) at these sites. Pump Station A, Elevated Storage Tank E and Reservoir D had smaller ZOIs with medians of 12 to 33 percent population and 22 to 33 percent area. Lastly, the Elevated Storage Tanks A, B, C and D had the smallest ZOIs with medians of two to nine percent population and five to ten percent area. Some sites with lesser ZOIs were chosen for ESM improvements so all site types were represented in the Cincinnati pilot, even if the estimated consequences of contamination were not as high as that of other sites.

6.3 Design Objective: Contaminant Coverage

See Sections 4.3 and 5.3 for the contaminant coverage considerations of video and non-video monitored sites. ESM focuses on detection of physical intrusions, and is therefore independent of contaminant type; therefore contaminant coverage was not considered.

6.4 Design Objective: Alert Occurrence

6.4.1 Invalid Alerts

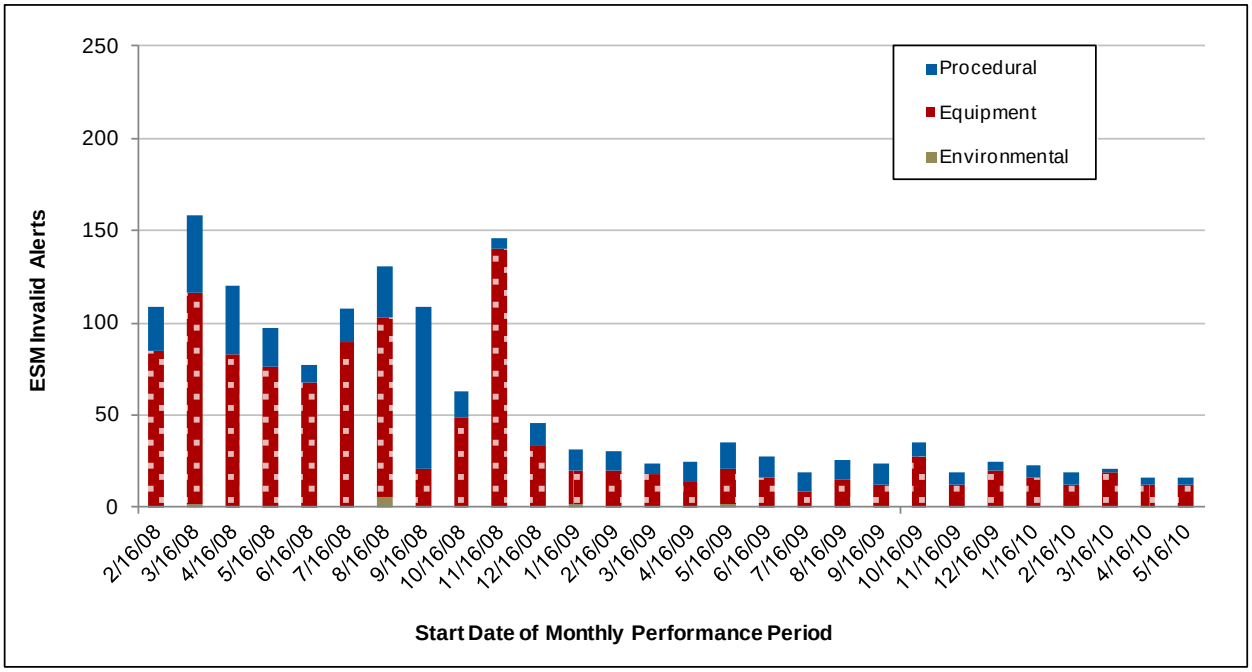
Definitions: See Sections 4.4.1 and 5.4.1 for definitions of invalid alerts at the video and non-video monitored sites.

Analysis Methodology: For an integrated evaluation of invalid alerts video and non-video monitored sites, invalid alert data was analyzed on a time-series basis and also by overall percentages averaged over the evaluation period.

Results: Figure 6-2 shows the number of invalid alerts at all ESM sites over the evaluation period. The invalid alerts were categorized by overall root causes: procedural, equipment and environmental.

Equipment-caused invalid alerts dropped significantly starting with the November 2008 reporting period. SCADA programming changes implemented during the December 2008 reporting period reduced the number of invalid alerts caused by radio faults at ladder sites. Replacement of ladder motion sensors with ladder hatch sensors during December 2008 reporting period reduced the number of equipment-caused invalid alerts.

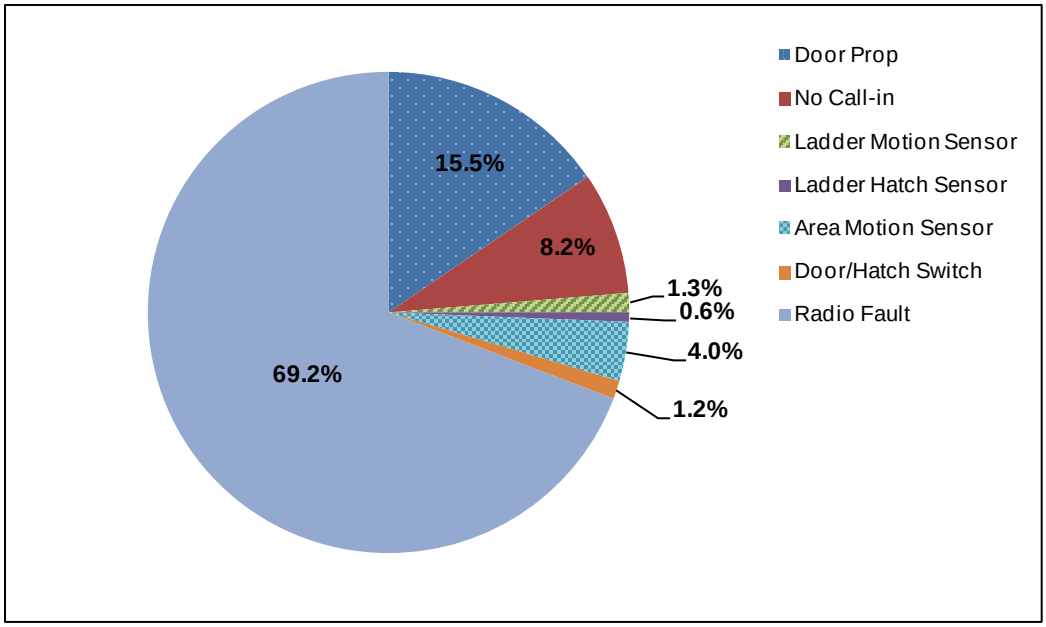
Procedure-caused invalid alerts had a decreasing trend over time. Training of staff on new ESM procedures reduced this type of invalid alert.



Note: Employee training and security equipment adjustment reduced invalid alerts.

Figure 6-2. ESM Invalid Alerts

Figure 6-3 shows the percentages of invalid alerts at all ESM sites over the evaluation period. The invalid alerts were categorized by detailed root causes: door prop, no call-in, motion sensor, door/hatch sensor and radio fault.

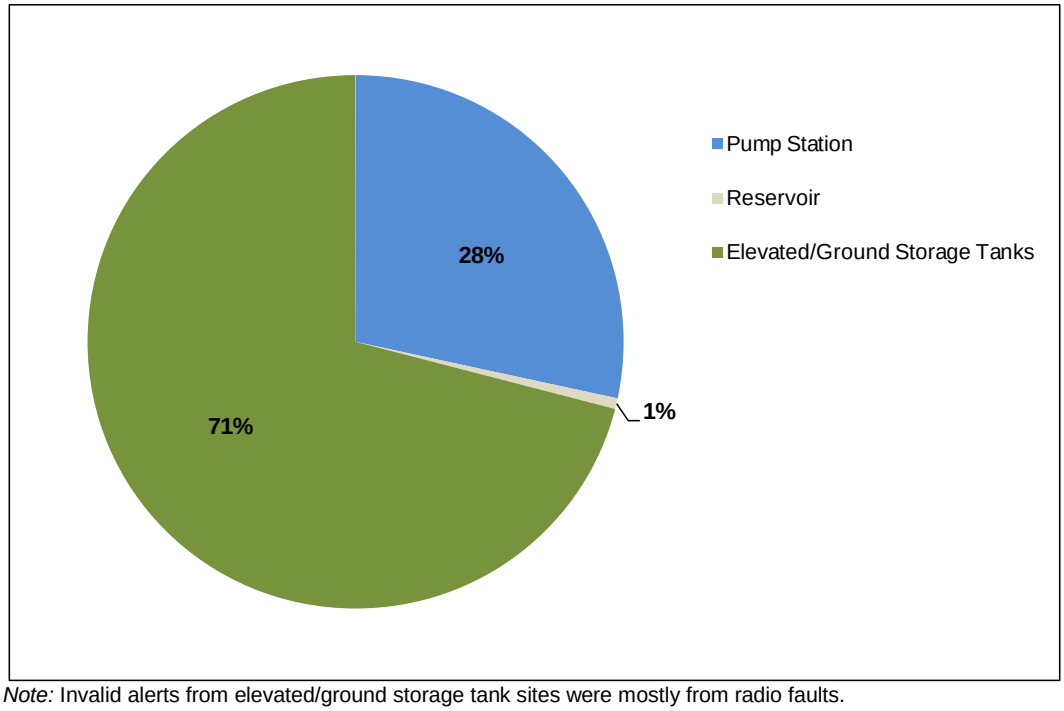


Note: Most invalid alerts were caused by radio faults.

Figure 6-3. Invalid Alerts by Type

After radio faults, door props were the next highest percentage of invalid alerts. Many doors monitored by the ESM system were not previously required to be closed. Training of staff on ESM procedures reduced this type of invalid alert over time.

Figure 6-4 shows the percentages of invalid alerts at all ESM site types over the evaluation period. The invalid alerts were categorized by locations: pump station, reservoir and elevated/ground storage tanks.



Note: Invalid alerts from elevated/ground storage tank sites were mostly from radio faults.

Figure 6-4. Invalid Alerts by Site Type

The elevated/ground storage tank sites had the highest percentage of invalid alerts due to the high number of radio faults. The pump stations had the next highest percentage of invalid alerts. The pump stations had a high number of door props and no call-in incidents.

6.4.2 Summary

The alert occurrence design objective was evaluated by examining the invalid alert rates for video and non-video monitored sites. The overall number of invalid alerts had a decreasing trend over the evaluation period, as employee training and equipment adjustment reduced the number of procedural and equipment-caused invalid alerts. Radio faults were the most common type of invalid alert, accounting for 69.2% of alerts received over the course of the evaluation period. Door props represented the next highest percentage of alerts received at 15.5%. Most invalid alerts were received from elevated/ground storage tank (71%) and pump station (28%) locations; only 1% of invalid alerts were received from reservoir locations.

6.5 Design Objective: Timeliness of Detection

For all ESM sites, the timeliness of detection evaluation metrics include the time for an alert to arrive at the utility control center, the time for the alert to be observed by utility personnel, the time for the alert to be investigated by utility personnel and the level of usage of the investigation checklists. The time for video clip transmission and viewing was specific to video sites and was discussed in Section 4.5.1 and 4.5.2. The timely transmission of alerts, the subsequent viewing of information by utility personnel, and a rapid investigation of the site are vital to ensure that a potential contamination incident is validated as quickly as possible after intrusion detection equipment has generated an alert. Proper use of the investigation checklists ensures that the utility personnel follow the response procedures as stated in the Cincinnati Pilot Operational Strategy.

6.5.1 Time for Intrusion Alert Transmission

Definition: *Time for intrusion alert transmission* is the time required for an alert to be transmitted from an ESM site to the utility control center and be available for utility personnel review.

Analysis Methodology: Reported transmission times by ESM site per reporting period were analyzed.

Results: The average time for alert transmission from non-video sites to the utility control center was about five seconds over the entire evaluation period. Non-video sites used the GCWW SCADA system for transmitting alerts. The video sites used digital cellular communications until transitioned to T1 and DSL connections during the January 2010 reporting period. Alert transmission time for video sites was about five seconds using digital cellular communications, decreasing to 4.5 seconds after the T1 and DSL transition.

Summary: Transmission time for alerts from the ESM sites to the utility control center was about five seconds for the entire evaluation. The transition from digital cellular to T1 and DSL connections at video sites improved alert transmission time only slightly.

6.5.2 Time to Initiate an Investigation

Definition: *Time to initiate an investigation* is the time between when an alert is received at the utility control center and when the investigation by utility personnel begins.

Analysis Methodology: The times to initiate an investigation per reporting period were analyzed. Data from investigation checklists were used to calculate investigation initiation times.

Results: Overall, the investigation process was initiated as per utility policy.

6.5.3 Time to Validate Possible Contamination

Definition: *Time to validate Possible contamination* is the time between when an alert investigation begins and when utility personnel have determined whether contamination is Possible. ESM is unique because it is the only component theoretically capable of preventing intentional contamination, if a timely response ensues. The CWS simulation model also captured two contaminant injection-related timeliness metrics: the time to interrupt an injection, which is the time between when an injection started and when on-site investigators could interrupt the injection, and the duration of an uninterrupted injection.

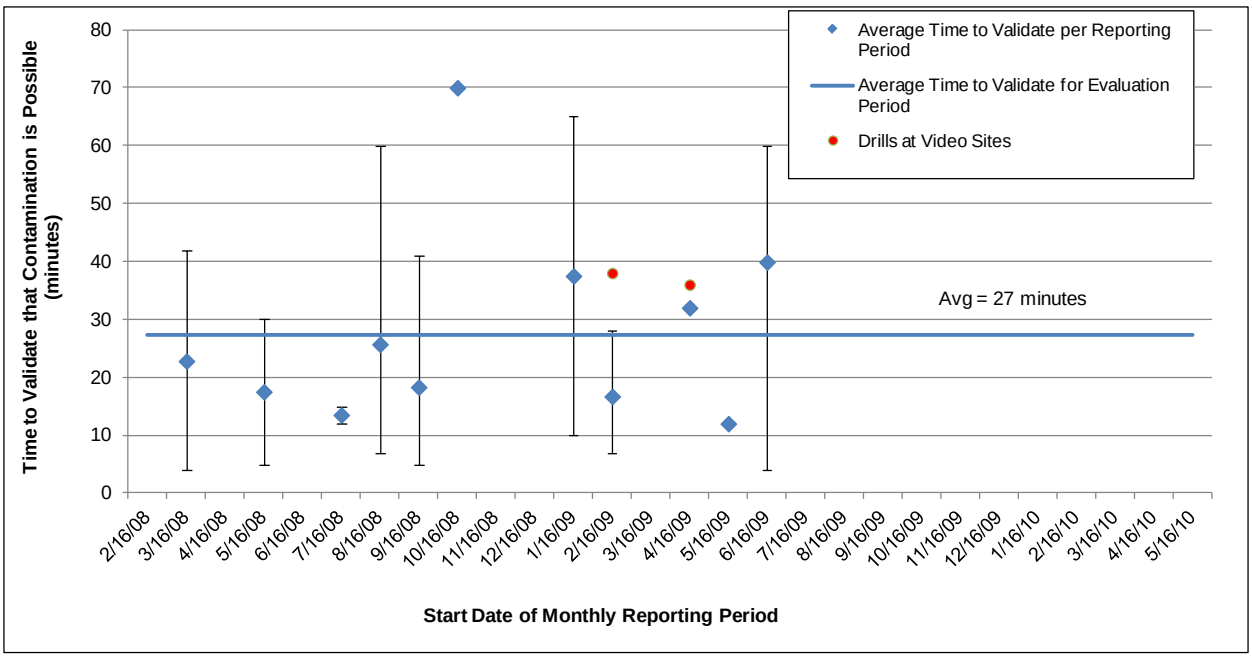
Time to validate Possible contamination metrics were obtained through three separate methods—obtained empirically during routine operations, observed during ESM drills, and simulated through the CWS model. As such, the Analysis Methodology and Results for each method is described separately below.

Routine Operations

Analysis Methodology: Average, minimum and maximum times to complete alert investigations per reporting period were evaluated for the video monitored and non-video monitored facilities. Data from investigation checklists were used to calculate alert validation times.

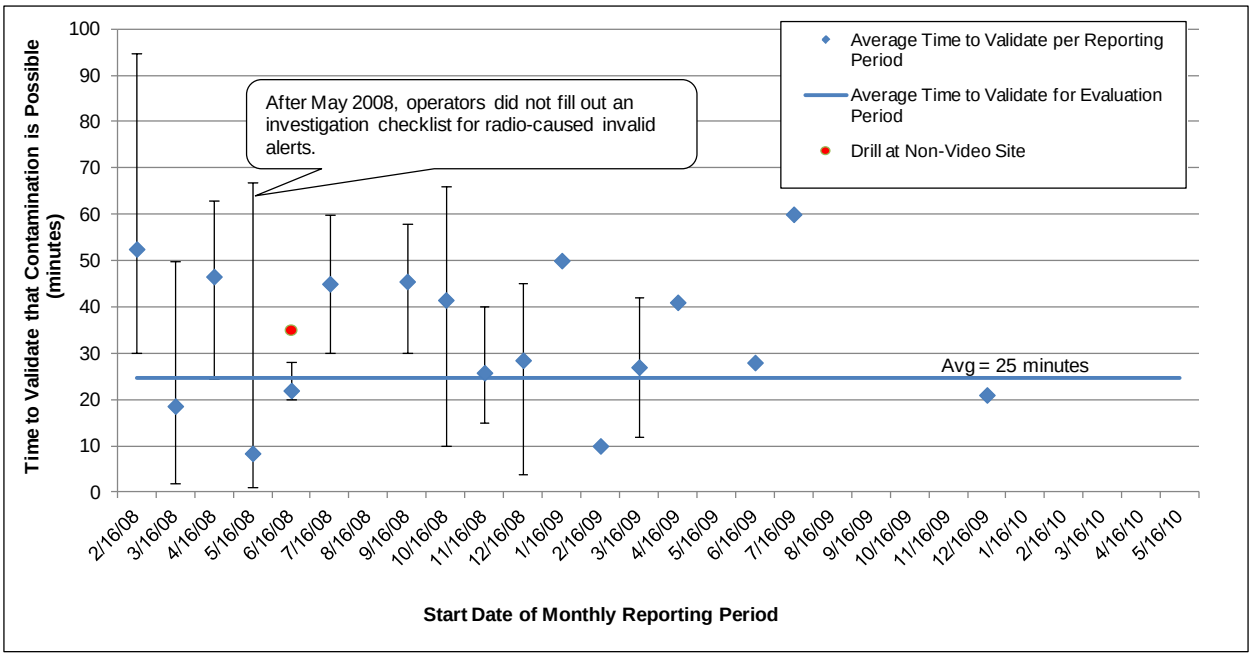
Results: The times to validate Possible contamination for video and non-video monitored sites during routine operation are shown in **Figures 6-5 and 6-6**, respectively. None of the routine operation alert investigations reached the Possible stage, so the investigation time to reach a Possible determination could not be captured empirically. Alert response investigation times observed during ESM drills, all of which did reach the Possible stage, are discussed in the next results section.

During the design phase, the video monitoring was intended to reduce the amount of time to validate an alert, since operators and security personnel could use video clips to verify if an invalid alert was caused by an employee or a potential contamination incident. In the case of an invalid alert, a video clip could prevent an unnecessary field investigation of a site. **Table 6-1** summarizes the data from the figures.



Note: The error bars represent the maximum and minimum validation times per reporting period. The average alert validation time was 27 minutes during the evaluation period and 37 minutes during drills at video monitored sites. There were no investigations at video monitored ESM sites after July 16, 2009.

Figure 6-5. Time to Validate if Contamination is Possible at Video Monitored Sites



Note: The error bars represent the maximum and minimum validation times per reporting period. The average alert validation time was 25 minutes during the evaluation period. The validation time was estimated at 35 minutes during the drill at a non-video monitored site.

Figure 6-6. Time to Validate if Contamination is Possible at Non-Video Monitored Sites

Table 6-1. Time to Validate Possible Contamination

ESM Site Type	Average	Minimum	Maximum
Video Monitored Sites	27 minutes	4 minutes	70 minutes
Non-Video Monitored Sites	25 minutes	1 minutes	95 minutes

Contrary to the design intent, the video sites had a longer average time to validate if contamination was Possible compared to the non-video sites by an average of about two minutes. Potential causes include:

- The non-video validation time data from the May 2008 reporting period may have caused the non-video validation time to be underestimated. The reporting period included 32 investigations of 85 total non-video site investigations over the entire evaluation period. There were multiple investigations during this reporting period that were only a few minutes long, causing the average for this reporting period to be only 8.4 minutes. These short investigations at non-video sites were caused by the operator observing a ladder sensor alert followed by a radio alert, and then concluding that the ladder alert was caused by the radio alert. An onsite investigation was not conducted, but the operator filled out an investigation checklist anyway. Data from investigation checklists were included in calculating alert investigation and validation times. After the May 2008 reporting period, operators did not fill out an investigation checklist when a radio alert caused an invalid ladder alert. If the average for non-video monitored sites was recalculated without the May 2008 reporting period, the average validation time at non-video would increase to 34.7 minutes, instead of 25 minutes.
- Extended periods of video communications downtime increased validation time at video sites. When video clips were not being transmitted to the utility control center in a timely manner, onsite investigations for all suspected intrusions were required.
- The video sites are significantly larger facilities than the non-video sites, and require more time to conduct a thorough investigation. For example, video sites were large multi-level pump stations while non-video sites included smaller structures associated with elevated storage tanks and reservoirs. During Drill 1, which was at a non-video site, the time for site investigators to validate if contamination was Possible was ten minutes less than that of Drill 2, which was at a large pump station.

For video monitored sites, the minimum and maximum validation times were four minutes and 70 minutes, respectively. The validation times included approximately two minutes to download the video clip. The minimum occurred when the video clip showed that an employee caused the alert, so an onsite investigation was not needed. The maximum time occurred when an onsite investigation was needed.

For non-video monitored sites, the minimum and maximum validation times were one minute and 95 minutes, respectively. The minimum occurred when a ladder alert was accompanied by a radio alert, indicating that the invalid alert was caused by radio problems so an onsite investigation was not needed. The radio alert usually arrived within a few seconds of the ladder alert. The maximum validation time was higher for non-video monitored sites, because the sites are farther than the video monitored sites, from where the plant supervisor and security guard are normally stationed.

ESM Drills

Analysis Methodology: Average, minimum and maximum times for each investigation step that was performed during the four ESM drills were evaluated using checklists from drill observers. This data was used to develop time to validate Possible contamination metrics, which were not available empirically from routine operations.

Results: This section covers alert response investigation times observed during four ESM drills, all of which reached the Possible stage. Each of the drills is described below.

ESM Drill 1 was conducted on June 26, 2008, during business hours at an elevated tank equipped with intrusion sensors only (no video equipment). Two scenarios were presented. During the first scenario, responders arrived and saw an open gate and door. During the second scenario, the door accessing the elevated tank was closed. Safety discussions ensued among the responding personnel pertaining to the possibility of an intruder still being at an advantageous position, high on the tank, with the capability and intent to deter response. One of the major outcomes of the drill was replacing motion sensors on the ladders with ladder guards equipped with intrusion contact switches. This change provided responders with the knowledge of whether or not an intruder had actually climbed the ladder to access the top of the tank. **Figure 6-7** shows the timeline progression of the key activities completed during the ESM alert investigation for ESM Drill 1. Note that the timeline was normalized so the start of the investigation occurs at time 0. The time to fully investigate the alert during the first scenario was 35 minutes.

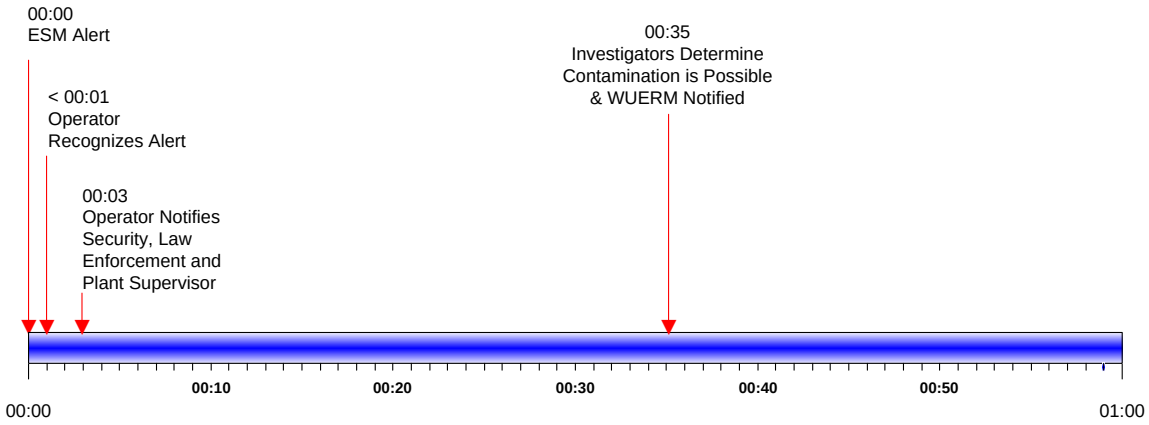


Figure 6-7. Timeline Progression for ESM Alert Investigation - ESM Drill 1

ESM Drill 2 was conducted on March 11, 2009 to evaluate alert recognition and investigative procedures associated with the component during the business hours of the utility, at a pump house which was equipped with video equipment. Video showed two individuals, appearing to be employees or maintenance workers, entering the site with a 55-gallon drum and a garden hose. Two scenarios were discussed with the responders. In the first scenario, video conclusively showed the intrusion. In the second scenario, the video was unavailable or garbled. The 'inconclusive video' scenario prompted discussion about safety and procedures that differed from the 'conclusive video' scenario. **Figure 6-8** shows the timeline progression of the key activities completed during the ESM alert investigation for ESM Drill 2. Note that the timeline was normalized so the start of the investigation occurs at time 0. The time to fully investigate the alert was 38 minutes.

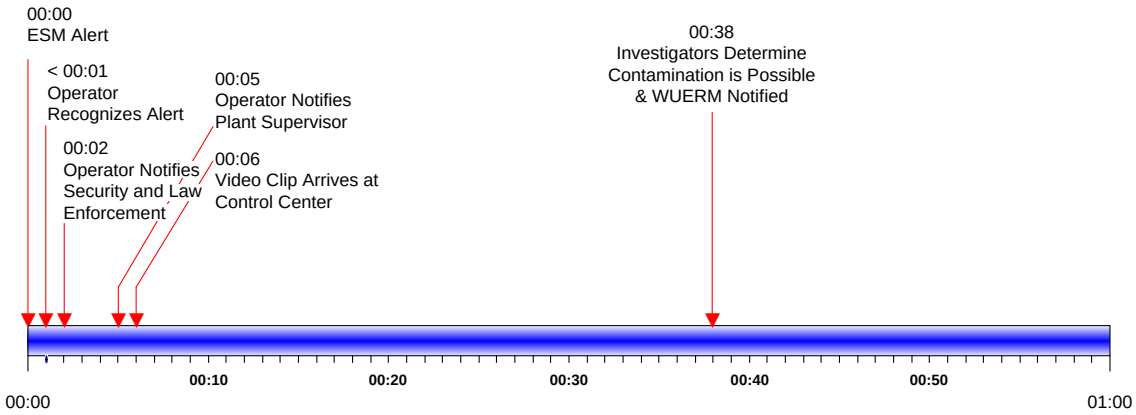


Figure 6-8. Timeline Progression for ESM Alert Investigation - ESM Drill 2

The ESM After-Hours Drill was conducted April 30, 2009 to May 1, 2009 at a reservoir which was equipped with video. The video conclusively showed intrusion, and one of the drill observers played the role of a local law enforcement responder. **Figure 6-9** shows the timeline progression of the key activities completed during the ESM alert investigation for ESM Drill 3. Note that the timeline was normalized so the start of the investigation occurs at time 0. The time to fully investigate the alert was 36 minutes.

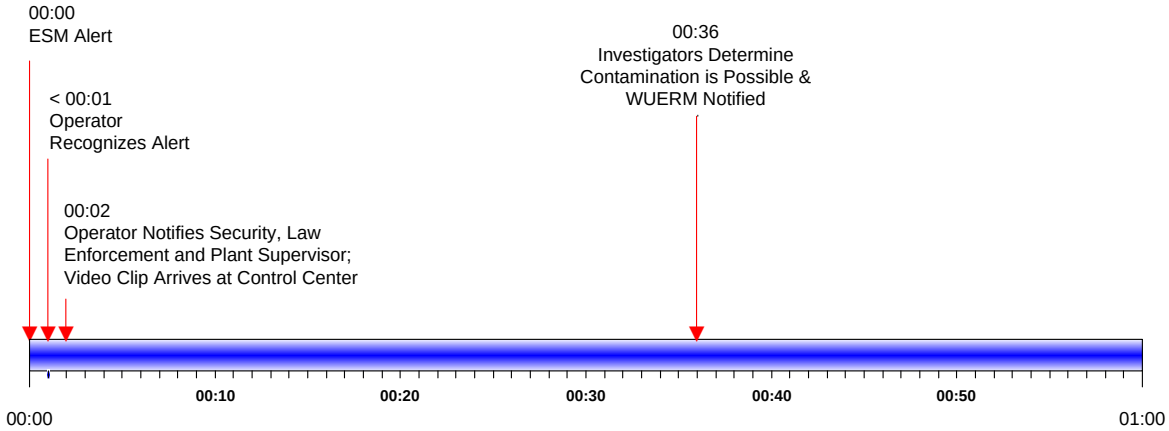


Figure 6-9. Timeline Progression for ESM Alert Investigation - ESM After-Hours Drill 3

ESM Drill 4 was conducted on April 13, 2010 to evaluate GCWW's response to an ESM incident stemming from a witness account, corroborated with a threat. The drill was at the same video monitored reservoir site as Drill 3. The scenario was a contractor (who was part of a cleaning crew) witnessing an individual tampering with the door, and then fleeing. No intrusion alerts were triggered, nor video captured. During the investigation, as responders were about to enter the facility, drill evaluators injected that the GCWW contact center received a threat that the water had been contaminated at that location.

Figure 6-10 shows the timeline progression of the key activities completed during the ESM alert investigation for ESM Drill 4. Note that the timeline was normalized so the start of the investigation occurs at time 0. The time to fully investigate the alert was 50 minutes.

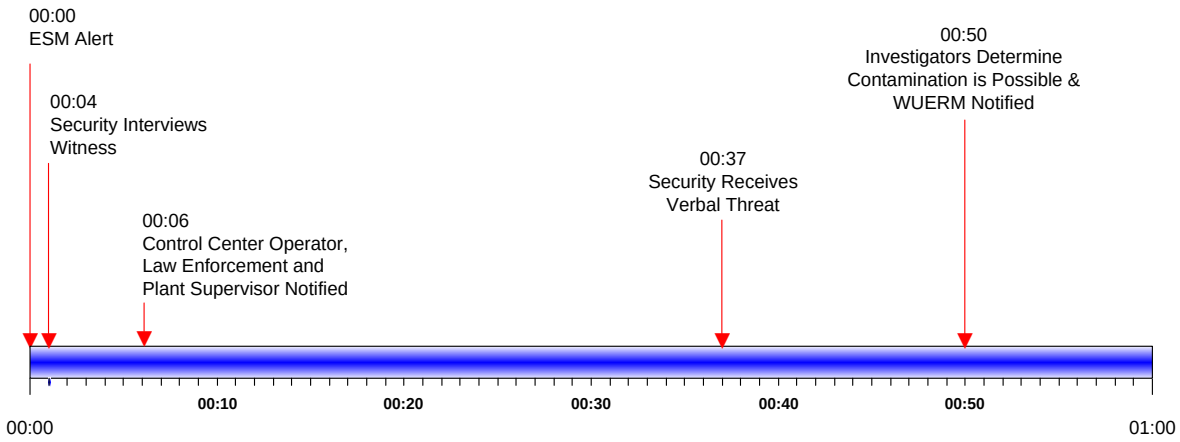


Figure 6-10. Timeline Progression for ESM Alert Investigation - ESM Drill 4

Table 6-2 provides a summary of the average time spent on each alert investigation activity and range (MIN to MAX). The average time to investigate an ESM alert was 40 minutes with a range of 35 to 50 minutes. Information on each drill scenario is also presented in Section 3.2.3.

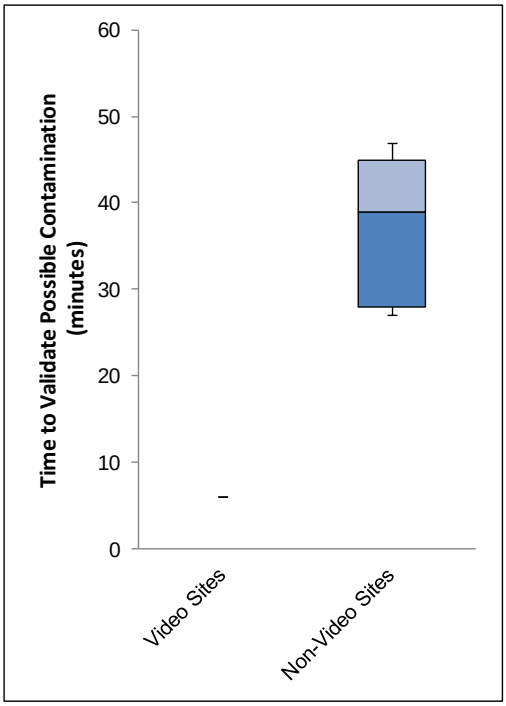
Table 6-2. Time to Implement Key Activities During Drill ESM Alert Investigations

Activity	Average (minutes)	MIN to MAX
Time to Investigate ESM Alert	**40**	**35 to 50**
Time elapsed between start of ESM alert and operator recognition of alert	<1	--
Time for video clip to arrive at control center	4	2 to 6
Time for operator to notify local law enforcement	3	2 to 6
Time for operator to notify GCWW Security	2	2 to 3
Time for operator to notify Plant Supervisor	4	2 to 6

CWS Simulation Model

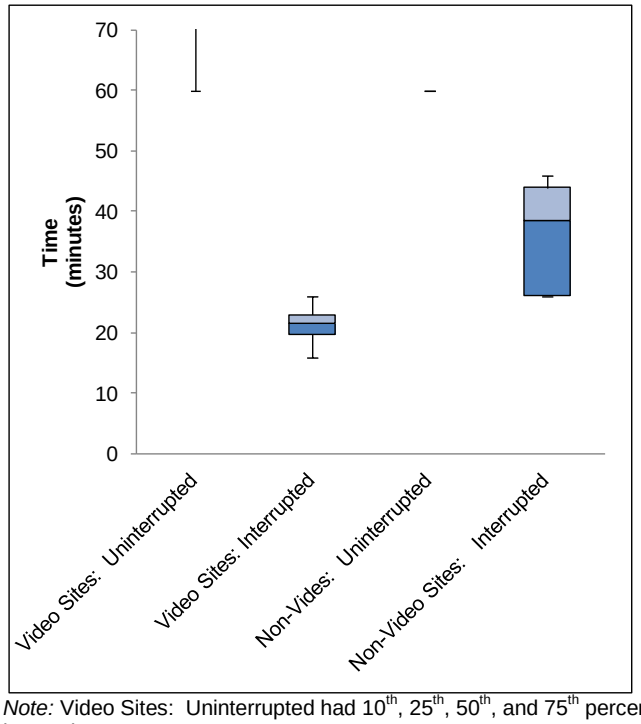
Analysis Methodology: The CWS simulation model was used to further compare the time to validate Possible contamination metric between video and non-video sites. The time to interrupt an injection metric was generated by the CWS simulation model for video and non-video sites, and the duration of an uninterrupted injection metric was also presented for comparison.

Results: The CWS simulation model was used to simulate the time to validate Possible contamination metric to supplement the empirical findings from routine operations and drills. The time to interrupt an injection and duration of an uninterrupted injection metrics were also modeled since empirical data was not available for these metrics. The CWS model metrics for time to validate Possible contamination and time to interrupt an injection are shown in **Figures 6-11 and 6-12**, respectively.



Note: All data points for video sites were six minutes.

Figure 6-11. Simulated Time to Validate Possible Contamination



Note: Video Sites: Uninterrupted had 10th, 25th, 50th, and 75th percentiles of 60 minutes, and a 90th percentile of 414 minutes, which is not shown.

Figure 6-12. Simulated Time to Interrupt an Injection

Figure 6-11 shows the difference between the video and non-video sites for the time to validate Possible contamination. All of the scenarios at video sites had a time of six minutes since the simulated investigation timeline for a video site had no variables.

The time to validate contamination at non-video sites varied with 25th, 50th and 75th percentile values at 28, 39, and 45 minutes, respectively. Non-video sites required an on-site investigation to determine that contamination was Possible, and the variability was due to differences in travel time and the necessary time to investigate the site for different ESM facility types.

Thus, contamination was deemed Possible approximately 30 minutes sooner at video sites compared to non-video sites, which underscores the benefit of installing video monitoring systems.

Figure 6-12 indicates that a few of the scenarios at video sites had uninterrupted injection durations of more than 60 minutes, which was due to facility characteristics at video sites that allowed for longer injection times. CWS simulation model developers determined that an uninterrupted injection duration shorter than 60 minutes would likely result in a contaminant slug that was too small to impact a large number of people because there would be only a very small window of time when the contaminant would be at a node for potential exposure.

The differences in the investigation procedures between video and non-video sites led to a more timely injection interruption at the video sites. For non-video sites, the on-site investigation begins after the plant supervisor and local law enforcement are both on-site, with law enforcement arriving ten minutes after being notified and the supervisor arriving within 20-30 minutes, depending on the distance of the site from the assumed starting point. However, for video sites, the law enforcement officer does not wait for the supervisor to arrive and initiates the on-site investigation immediately since there is video confirmation of an actual intrusion, thus shortening the time to interrupt the injection by approximately 10-20 minutes.

These model results demonstrate two critical benefits of installing video at a site: earlier determination that contamination is possible and sooner interruption of an injection. Early determination of potential contamination could initiate operational changes (such as isolation or hydraulic grade changes) to minimize contaminant spread, and timely injection interruption reduces the amount of contaminant introduced into the system.

6.5.4 Summary

The timeliness of detection design objective was evaluated by examining alert transmission time and time to validate Possible contamination. Transmission time for alerts from the ESM sites to the utility control center was about five seconds for the entire evaluation. The transition of communication type from digital cellular to T1 and DSL connections at video sites improved alert transmission time only slightly, from 5 to 4.5 seconds.

The average time to validate whether contamination was Possible took 27 minutes at video monitored sites and 25 minutes at the non-video monitored sites. This was contrary to the design intent of video monitoring, which was to reduce validation time since the operations and security personnel could use the video clips to determine an invalid alert or Possible contamination incident without having to conduct an onsite investigation. Possible reasons for this result include inconsistencies in the way operators were filling out investigation checklists, video communication issues and the additional time required to investigate the larger areas of the video-monitored sites.

The average validation times from routine operations were slightly less than the validation times from the ESM drills that simulated an intrusion. The drills at non-video site had a validation time of about 35 minutes, while the drill at a video site averaged 37 minutes. The average validation times from routine operations were shorter because they included alerts where onsite investigation was not required.

CWS simulation model results showed that investigators would determine that contamination was Possible approximately 30 minutes sooner for alerts at video sites when compared to that of non-video sites. This simulation finding underscores the benefit of installing video monitoring systems, given that the majority of uninterrupted injection durations were on the order of 60 minutes.

6.6 Design Objective: Operational Reliability

See Section 4.6 for a discussion on the operational reliability design objective.

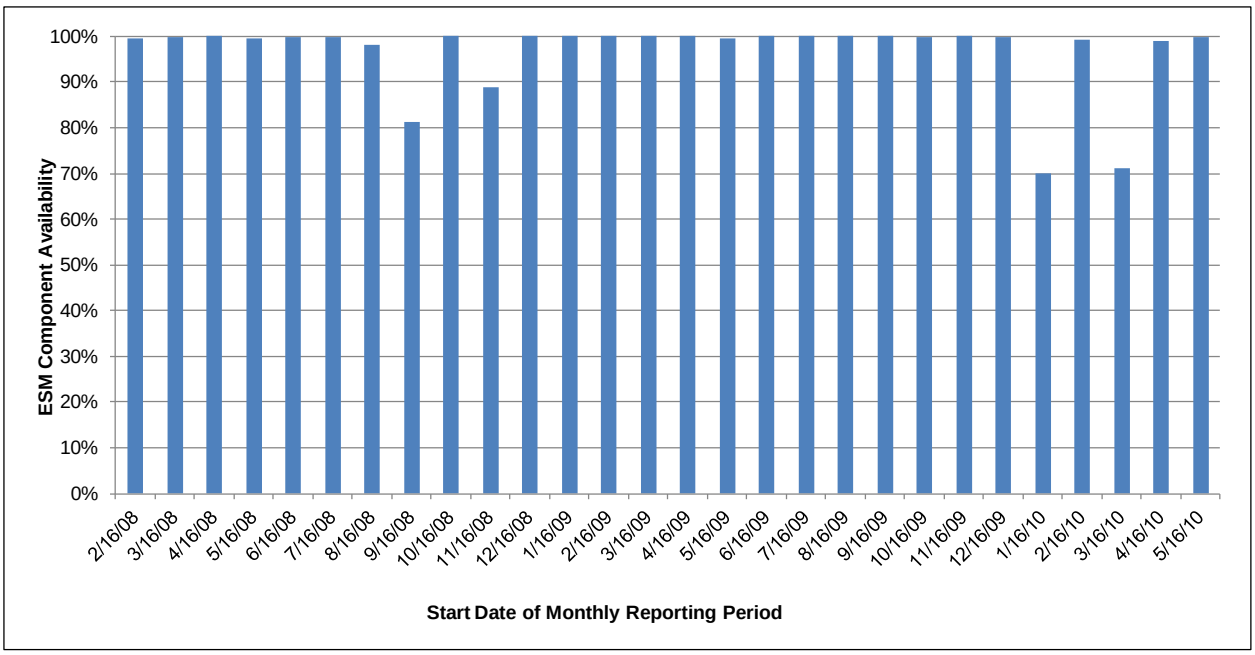
6.6.1 System Availability

Definition: The ESM component is considered available when the physical security equipment, communications equipment, and the data management design elements are all operational concurrently. If any of the design elements is unavailable, then the ESM component is considered unavailable during that time period.

Analysis Methodology: Any period of downtime greater than one hour for the ESM component was considered unavailable. ESM availability is the total number of hours available divided by the total possible hours available. The downtime criteria for the ESM design elements were defined as follows:

- *Physical Security Equipment*: Less than 75% of intrusion detection devices are producing a valid data stream.
- *Communications Equipment*: Less than 75% of ESM data streams are successfully transmitted.
- *Data Management*: Less than 75% of ESM data streams are successfully displayed on the human-machine interface application in the GCWW control center.

Results: Figure 6-13 below shows the ESM component availability for each reporting period. Overall, the ESM component was available 97% of the time, with 99% or greater availability during 23 out of the 28 reporting periods. Reporting periods with less than 99% availability resulted from downtime due to PLC failure and I/O server downtime caused by programming updates and hardware issues.



Note: The average ESM component availability during the evaluation period was 97 percent.

Figure 6-13. ESM Component Availability

6.7 Design Objective: Sustainability

Sustainability is a key objective in the design of a CWS and each of its components, which for the purpose of this evaluation is defined in terms of the cost-benefit trade-off. Costs are estimated over the 20 year life cycle of the CWS and include the capital cost to implement the CWS and the cost to operate and maintain the CWS. The benefits derived from the CWS are defined in terms of primary and dual-use benefits. The primary benefit of a CWS is the potential reduction in consequences in the event of a contamination incident; however, such a benefit may be rarely, if ever, realized. Thus, dual-use benefits that provide value to routine utility operations are an important driver for sustainability. Ultimately, sustainability can be demonstrated through utility and partner acceptability with the protocols and procedures necessary to operate and maintain the CWS. The three metrics that will be evaluated to assess how well the Cincinnati CWS met the design objective of sustainability are: Costs, Benefits, and Acceptability. The following subsections define each metric, describe how it was evaluated, and present the results.

6.7.1 Costs

Definition: Costs are evaluated over the 20 year life cycle of the Cincinnati CWS, and comprise costs incurred to design, deploy, operate, and maintain the ESM component since its inception.

Analysis Methodology: Parameters used to quantify the implementation cost of the ESM component were extracted from the *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status* (USEPA, 2008). The cost of modifications to the ESM component made after the completion of implementation activities were tracked as they were incurred. O&M costs were tracked on a monthly basis over the duration of the evaluation period. Renewal and replacement costs, along with the salvage value at the end of the Cincinnati CWS life cycle were estimated using vendor supplied data, field experience and expert judgment. Note that all costs reported in this section are rounded to the nearest dollar. Section 3.5 provides additional details regarding the methodology used to estimate each of these cost elements.

Results: The methodology described in Section 3.5, was applied to determine the value of the major cost elements used to calculate the total lifecycle cost of the ESM component for 20 years, which are presented in **Table 6-3**. It is important to note that the Cincinnati CWS was a research effort, and as such incurred higher costs than would be expected for a typical large utility installation. A similar ESM component implementation at another utility should be less expensive as it could benefit from lessons learned and would not incur research-related costs. Additional information regarding the data used to determine the value of each cost element is presented below.

Table 6-3. Cost Elements used in the Calculation of 20 Year Lifecycle Cost

Parameter	Value
Implementation Costs	$1,388,869
Annual O&M Costs	$38,002
Renewal and Replacement Costs	$257,332
Salvage Value	($19,124)

Table 6-4 below presents the implementation cost for each ESM design element, with labor costs presented separately from the cost of equipment, supplies, and purchased services.

Table 6-4. Implementation Costs

Design Element	Labor	Equipment, Supplies, Purchased Services[1]	Component Modifications[1] (deletions in parentheses)	Total Implementation Costs[1]
Project Management[1]	$102,749	-	-	$102,749
Physical Security Equipment	$617,156	$405,617	$27,121 ($18,505)	$1,031,389
Data Management and Communication	$85,886	-	-	$85,886
Procedures	$168,846	-	-	$168,846
TOTAL:	**$974,636**	**$405,617**	**$8,616**	**$1,388,869**

[1] Project management costs incurred during implementation were distributed evenly among the CWS components.

The first design element, project management, includes overhead activities necessary to design and implement the component. The physical security equipment design element includes the cost of conducting a vulnerability assessment on all pump stations, ground level tanks and elevated storage tanks at GCWW. Enhancements were identified during the assessment, and consisted of door/hatch sensors, motion sensors, ladder hatch gates and cameras for identified facilities. The third design element, data management and communication, includes the cost of implementing a parallel SCADA system for transmitting digital video recordings to the utility control system for viewing when an alert is received. The final design element, procedures, includes the cost of developing procedures that guide the routine operation of the component and alert investigations, along with training on those procedures.

Overall, the physical security equipment design element had the highest implementation cost (74 percent). Implementation costs for project management, data management and collection and for development of the procedures for routine operation and training on those procedures were significantly lower at 7, 6 and 12 percent, respectively.

The component modification costs represent the labor, equipment, supplies and purchased services associated with enhancements to the ESM component after completion of major implementation activities in December 2007. The modification costs include additional expenses incurred to install 24 volt dc UPS and batteries for ladder motion sensors; fabricate and install ladder hatches and ladder guards; install an additional hatch sensor; and implement communications and control system improvements. The cost of four ladder motion sensors and their installation was subtracted from the total implementation costs as these items were removed from utility facilities based on recommendations from ESM Drill 1. The ladder motion sensors were replaced with hatch sensors.

The annual labor hours and costs of operating and maintaining the ESM component, broken out by design element, are shown in **Table 6-5**.

Table 6-5. Annual O&M Costs

Design Element[1]	Total Labor (hours/year)	Total Labor Cost ($/year)	Supplies and Purchased Services ($/year)	Total O&M Cost ($/year)
Physical Security Equipment	201	$9,359	$1,901	$11,260
Data Management and Communication[2]	-	-	$15,840	$15,840
Procedures	210	$10,902	-	$10,902
TOTAL:	**411**	**$20,261**	**$17,741**	**$38,002**

[1] Overarching project management costs were only incurred during implementation of the ESM component and are not applicable for annual O&M costs.
[2] Recurring communication cost is split between Water Quality Monitoring and ESM.

O&M for the physical security equipment involves routine maintenance and troubleshooting of any equipment problems. Most of the O&M labor hours reported under "Procedures" are spent on the routine investigation of ESM alerts. **Table 6-6** shows the investigation labor hours, representing the amount of effort that utility control center operator and field investigators spend when responding to intrusion alerts at ESM sites. The utility control center operator receives the alert and then notifies the personnel assigned to conduct the onsite investigation.

The field investigators had 24 percent more labor than the utility control center operators. In many cases, the plant supervisor and guard both investigated a site, doubling the amount of field investigator labor. There were only a few investigations at ESM sites from the start of the July 2009 reporting period through the end of the evaluation. The utility's operators and security guards continued responding to suspected intrusion alerts throughout the period. However, almost all suspected intrusions were at non-ESM sites, so the investigations were not included in this evaluation.

Investigation labor hours per alert varied greatly because of the widespread geographic distribution of the ESM monitored sites throughout the utility's service area.

Table 6-6. Investigation Labor Hours per Reporting Period and Investigation

Personnel	Average Labor Hours per Investigation	Average Labor Hours per Period	Total Labor Hours
Utility Control Center Operators	0.40	1.64	46
Field Investigators	0.49	2.05	57
Total	**0.89**	**3.69**	**103**

Two of the major cost elements presented in Table 6-3, the renewal and replacement costs and salvage value, were based on costs associated with major pieces of equipment installed for the ESM component. The useful life of these items was estimated at 3, 5, 7, 10, or 15 years based on field experience, manufacturer-provided data and input from subject matter experts. For the items with a useful life of three years, it was assumed that the equipment would need to be replaced six times during the 20-year life cycle of the CWS, items with a useful life of five years were assumed to be replaced three times, and items with a useful life of seven years were assumed to be replaced twice. The equipment with a useful life of 10 or 15 years would only be replaced once. These items and their total costs are presented in **Table 6-7**.

Table 6-7. Equipment Costs

Equipment Item	Useful Life (years)	Unit Capital Costs	Quantity (# of Units)	Total Cost
Security Lighting	15	$311	28	$8,708
Door/Hatch Sensors	15	$260	33	$8,580
Ladder Sensors	10	$1,660	2	$3,320
Area Motion Sensors	10	$450	10	$4,500
Cameras - PTZ	3	$4,026	5	$20,130
Cameras - Fixed	7	$1,037	6	$6,222
Video System (Longwatch, RVE hardware and VCC)	5	$11,000	3	$33,000
			TOTAL:	**$84,460**

To calculate the total 20 year lifecycle cost of the ESM component, all costs and monetized benefits were adjusted to 2007 dollars using the change in the Consumer Price Index between 2007 and the year that the cost or benefit was realized. Subsequently, the implementation costs, renewal and replacement costs, and annual O&M costs were combined, and the salvage value was subtracted to determine the total 20-year lifecycle cost:

ESM Total Lifecycle Cost: **$2,195,081**

Note that in this calculation, the implementation costs and salvage value were treated as one-time balance adjustments, the O&M costs recurred annually, and the renewal and replacement costs for major equipment items were incurred at regular intervals based on the useful life of each item.

6.7.2 Benefits

Definition: The benefits of CWS deployment can be considered in two broad categories: primary and dual-use. Primary benefits relate to the application of the CWS to detect contamination incidents, and can be quantified in terms of a reduction in consequences. Primary benefits are evaluated at the system and are thus discussed in the system evaluation report *Water Security Initiative: Evaluation of the Cincinnati*

Contamination Warning System Pilot (USEPA, 2014b). Dual-use benefits are derived through application of the CWS to any purpose other than detection of intentional and unintentional drinking water contamination incidents. Dual-use benefits realized by the ESM component are presented in this section.

Analysis Methodology: Information collected from forums, such as data review meetings, lessons learned workshops, and interviews were used to identify dual-use applications of the ESM component of the CWS.

Results: Operation of the ESM component of the CWS has resulted in benefits beyond the detection of intentional and unintentional contamination incidents. These key dual-use benefits and examples identified by the utility include:

1. More efficient investigations/staff utilization and education:
    - ESM assists operational staff in determining whether a facility has been restored and secured to proper conditions after maintenance activities. For example, after work is performed inside a storage tank, it is imperative that all access hatches be closed to ensure the quality of the water. An examination of the facility ESM conditions, including monitored hatches, by operational staff ensures that the facility is restored to proper conditions.
    - Through ESM, operational staff gain familiarity and proficiency with security-related SOPs, reducing the number of invalid alerts caused by procedural errors.
    - As camera technology and cost improve, camera use in conducting security checks of facilities in place of staff visits can reduce field time, thereby making security staff available for higher priority activities.
    - Implementation of an optimally defined ESM system at remote utility facilities, areas subject to frequent power outages, or locations that serve as a single connection to a major area such as a wholesale customer, allow for remote site investigations and provide police responders better information. Remote site investigations provide faster investigations and reduce or eliminate staff visits to the site. An optimally defined ESM system includes perimeter fencing, access alerts, motion sensors, alert-activated cameras (both external and internal) and an uninterruptible power supply.
2. Deterrent effect:
    - Additional intrusion detection devices such as video cameras could serve as a deterrent to and allow detection of vandalism or theft incidents. Vandals are less likely to target a site with a video camera, and thieves are more likely to target sites without as much security.
3. Integration with law enforcement:
    - ESM can assist police conducting investigations in the vicinity of utility facilities equipped with external video cameras. The cameras can be used to identify people of interest, time frames, activities and other conditions that support the collection of forensic evidence for crimes not related to the water utility. For example, a utility video camera could capture on video a thief who has robbed a nearby business.
    - In high-crime areas, access to ESM information including cameras could be provided to police (e.g., in a local Fusion Center). This would enable police to closely monitor criminal activities in the area.

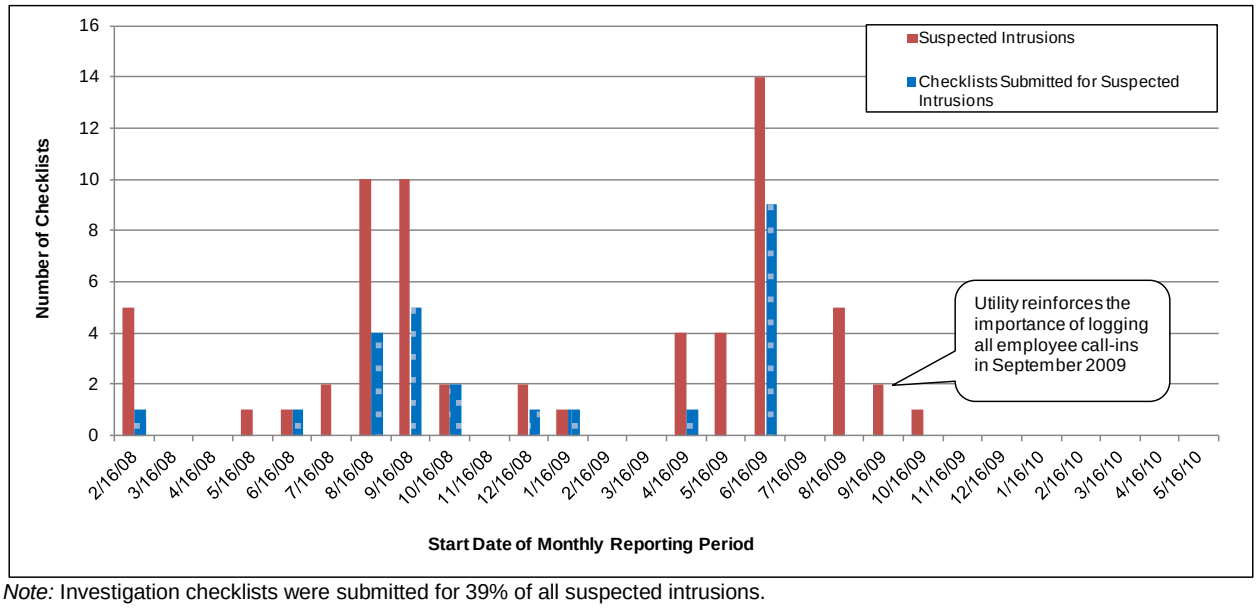
4. Increased employee safety:
    - ESM can allow utility staff to know the location of employees. If an employee is at a location for an unusually long amount of time, it could be an indication that an employee is injured or impaired.

6.7.3 Acceptability - Investigation Checklist Usage

Definition: Investigation checklist usage is the number of investigation checklists submitted for suspected intrusion incidents. The Operational Strategy for the Cincinnati CWS required that the utility control center operator complete an investigation checklist for all suspected intrusion incidents and that the security guard complete a checklist for all suspected intrusion incidents that the guard investigated. The investigation checklist guides the user through the steps of an investigation and provides fields for recording incident and event times.

Analysis Methodology: The number of suspected intrusions and the number of investigation checklists provided for suspected intrusions was evaluated.

Results: Figure 6-14 and Table 6-8 show the investigation checklist usage and the number of suspected intrusions.



Note: Investigation checklists were submitted for 39% of all suspected intrusions.

Figure 6-14. Detected Entries by Category

Table 6-8. Investigation Checklists Submitted for Suspected Intrusions

Detected Entry Category	Amount Over Evaluation Period
Investigation Checklist Submitted for Suspected Intrusions	25
No Investigation Checklist Submitted for Suspected Intrusion	39
Total Suspected Intrusions	64
Valid Entries at ESM sites	12,905

Note: There was an average of 460 valid entries at ESM sites per reporting period.

Investigation checklists were submitted for 39 percent of all suspected intrusions. It is likely that many, if not all, of the 39 suspected intrusions without a corresponding investigation checklist were due to the utility control center not logging a valid entry, especially given that there were 12,905 valid entries at ESM sites during the 28-month evaluation period. It should be noted that suspected intrusions without an investigation checklist began decreasing, eventually to zero after utility management re-emphasized the importance of logging all entries in September 2009.

The months of June, July and August tended to have the most suspected intrusions. Two factors increased the likelihood of an operator not logging an employee call-in during the summer months. First, high water demand required the utility control center operator to perform more operational tasks than during other months of the year. Second, increased construction and maintenance activities elevated the number of valid entries to be logged.

At the conclusion of the CRADA, the utility personnel were instructed to continue to complete investigation checklists for all suspected intrusions at ESM and non-ESM sites, indicating system-wide adoption of the Cincinnati Pilot Operational Strategy.

6.7.4 Summary

The sustainability design objective was evaluated by examining costs, benefits and acceptability. Total lifecycle costs for 20 years were calculated by adding the cost of implementing the system, annual operations and maintenance, renewal and replacement costs, and then subtracting the estimated salvage value. The total 20 year lifecycle cost was $2,195,081. The cost to develop, design, procure, install, and modify the ESM hardware/software for video monitored and non-video monitored sites was a total implementation cost of $1,388,869. The annual O&M cost of the ESM component was $38,002. The renewal and replacement cost was $257,332.

Implementation costs were derived from a matrix that analyzed labor, procured goods and services and modification costs segregated by project management, equipment, communications, and the cost to develop investigative procedures. The O&M costs were mostly labor hours spent on the routine investigation of ESM alerts. The renewal and replacement costs and salvage value were based on costs associated with major pieces of equipment installed for the ESM component. The useful life of each piece of equipment was estimated to be between three and 15 years and varied based on field experience, manufacturer-provided data, and input from subject matter experts.

Investigation labor hours per alert varied greatly due to the widespread geographic distribution of the ESM monitored sites throughout the utility's service area. The average labor for investigations per reporting period was 3.69 hours, and the average per investigation was 0.89 hour. The average labor hours for field investigators was slightly greater than that of the utility control center operators mainly

because of occasions when there was more than one field investigator participating in the onsite investigation.

The benefits described are based on qualitative information, and related to increased efficiency, deterrence and integration. Quantifiable consequences are discussed in the report *Water Security Initiative: Evaluation of the Cincinnati Contamination Warning System Pilot* (USEPA, 2013).

To evaluate the acceptability of the ESM component, analysis of the investigation checklist usage showed 25 suspected intrusions at ESM sites that resulted in an investigation and completion of an investigation checklist, although not all suspected intrusions resulted in completion of an investigation and corresponding checklist. The most likely explanation for the suspected intrusions without an investigation checklist was that an employee called into the utility control center, but the operator overlooked entering the call into the log book. Those entries should have been counted as valid. After the conclusion of the CRADA, utility personnel were instructed to complete investigation checklists for all suspected intrusions at ESM and non-ESM sites, indicating system-wide adoption of the Cincinnati Pilot Operational Strategy.

Section 7.0: Summary and Conclusions

As described earlier, this document serves to provide a comprehensive evaluation of how effectively the ESM component of the Cincinnati pilot achieved the five applicable CWS design objectives used to characterize performance: spatial coverage, contaminant coverage, timeliness of contaminant detection, operational reliability and sustainability. To conduct the evaluation, data sources including empirical data, drill and exercise data, simulation study results, forums (including monthly staff interviews and a lessons-learned workshop), and cost data were utilized.

7.1 Design Objective: Spatial Coverage

ESM was limited in its ability to detect contamination incidents throughout the distribution system since only specific utility locations are monitored for intrusions that may lead to contamination. However, the sites that were monitored by ESM impacted a very large portion of the population and service area, indicating the importance of monitoring these locations. Overall, the simulation study model indicated that the ESM sites covered water supplied to 99 percent of the retail population and 96 percent of the retail service area. The model also showed that the three ESM pump station sites supplied water to 81 to 93 percent of the retail service population and 70 to 80 percent of the retail service area. These relatively large populations and wide service areas supported the design decision to install video monitoring equipment at these three sites.

7.2 Design Objective: Contaminant Coverage

Although the ESM component did not consider specific contaminants or detection classes of contaminants, the volume of contaminants, general levels of contaminant toxicity, and method of contaminant injection were considered during the ESM design of the video and non-video monitored sites.

7.3 Design Objective: Alert Occurrence

Table 7-1 summarizes the alert occurrence metrics.

Door prop invalid alerts diminished as utility staff and contractors were trained on new ESM procedures for securing doors at the facilities.

The ladder and area motion invalid alerts were found to have a higher frequency of invalid alerts compared to door/hatch sensors. Ladder and area motion invalid alerts diminished as sensors with high invalid alert rates were identified and adjusted. Ladder motion sensors were replaced by ladder hatches and ladder hatch sensors based on recommendations from ESM Drill 1.

The intrusion detection devices met the *Guidelines for the Physical Security of Water Utilities* (ASCE/AWWA, 2006) guideline of at least 90 days between invalid alerts per sensor.

Table 7-1. Evaluation of Alert Occurrence Metrics

Description	Video Sites	Non-Video Sites
Invalid Alerts—Door/Hatch Props	0.42 per 100 valid entries per door	None
Invalid Alerts—No Call-Ins	1.4 per 100 valid entries	0.23 per 100 valid entries

Description	Video Sites	Non-Video Sites
Invalid Alerts—Door/Hatch Sensors	1,168 days between invalid alerts per sensor	
Invalid Alerts—Area Motion Sensors	136 sensor days between invalid alerts per sensor	N/A
Invalid Alerts—Ladder Motion Sensors	160 days between invalid alerts per sensor	
Invalid Alerts—Ladder Hatch Sensors	271 days between invalid alerts per sensor	

7.4 Design Objective: Timeliness of Detection

Table 7-2 summarizes the timeliness of detection metrics.

Table 7-2. Evaluation of Timeliness of Detection Metrics

Description	Video Sites	Non-Video Sites
Time for Alert Transmission	5 seconds	
Time to Initiate an Investigation	2 minutes	
Investigation Checklist Usage	25 investigation checklists were submitted for suspected intrusions at ESM sites. The utility has adopted use of investigation checklists at all sites.[1]	
Time for Video Clip Transmission	One to three minutes (using digital cellular communications) 37 seconds (using T1 and DSL communications and video clip is doubled in duration)	N/A
Time to View Video Clip	3.23 minutes	N/A
Time to Validate Contamination is Possible	27 minutes	25 minutes

1 – There were 39 out of 64 suspected intrusions during the evaluation period that did not have an investigation checklist. The most likely explanation for the suspected intrusions without an investigation checklist was that an employee called into the utility control center, but the operator overlooked entering the call into the log book. Those entries should have been counted as valid. There were 12,905 valid entries at ESM sites during the evaluation period.

The alert transmission times were relatively constant throughout the evaluation. The video clip transmission time varied because of communications issues. The digital cellular communication system initially used to transmit the alert and video data from video sites eventually was replaced by T1 and DSL connections.

The video clips that supported an onsite investigation or were used to verify an invalid alert were viewed an average of 3 minutes and 14 seconds after the intrusion.

Utility staff took longer to investigate video sites than non-video sites. This was contrary to the design intent of the video monitored sites. Possible reasons included inconsistencies in the way operators filled out investigation checklists, communications issues delaying transmission of the video clip and video monitored sites being larger than non-video sites and requiring more time to investigate thoroughly.

Data from the CWS simulation model simulated the time to validate possible contamination, the time to interrupt an injection and duration of an uninterrupted injection for ESM sites with and without video. The model results showed that contamination was determined to be possible 30 minutes sooner and injections were interrupted 10-20 minutes earlier at video sites when compared to that of non-video sites.

7.5 Design Objective: Operational Reliability

Table 7-3 summarizes the operational reliability metrics.

Communications system availability typically was above 99 percent for alert data transmission but varied greatly for video data transmission. There were issues with video communications throughout the evaluation, including the blocking of video traffic by the digital cellular provider. Communications from video monitored sites were transitioned to T1 and DSL connections after video traffic was blocked.

Table 7-3. Evaluation of Reliability Metrics

Description	Video Sites	Non-Video Sites
Communications System Availability—Alerts	96–100% Avg. = 99.69%	99.3–100% Avg. = 99.91%
Communications System Availability—Video	77–100% Avg. = 97.64%	N/A
Intrusion Detection Equipment Availability	88–100%[1]	100% Avg. = 100%
Video Equipment Availability	60–100%[1]	N/A
Data Completeness—Intrusion Detection	87–100% Avg. = 98.59%	99.3-100% Avg. = 99.91%
Data Completeness—Video	71-100% Avg. = 93.23%	N/A

1 - Average varied by equipment.

The availability of intrusion detection equipment typically was greater than 99 percent, although PLC outages caused downtime. Cameras started out with availability greater than 99 percent but experienced extended periods of downtime toward the end of the evaluation period, as the PTZ cameras approached the end of the design life.

7.6 Design Objective: Sustainability

The costs, benefits and acceptability associated with operating, maintaining, modifying and evaluating the ESM system are summarized in **Table 7-4**.

After the conclusion of the CRADA, the utility staff was instructed to complete investigation checklists for all suspected intrusions at ESM and non-ESM sites, indicating system-wide adoption of the Cincinnati Pilot Operational Strategy. A similar ESM implementation at another utility should be less expensive when compared to the Cincinnati pilot as it could benefit from lessons learned and would not incur research-related costs.

Table 7-4. Summary of Sustainability Metrics

Description	Value
Costs	
Implementation Costs	$1,388,869
Annual O&M Costs	$38,002
Renewal and Replacement Costs	$257,332
Salvage Value	($19,124)
Labor Hours per Investigation	0.89 hours
Average for Investigation Labor Hours per Reporting Period	3.69 hours
Total Investigation Labor Hours	103 hours
Total 20 Year Lifecycle Costs[1]	$2,195,081

Description	Value
Benefits	
More efficient investigations/ staff utilization and education	Qualitative
Deterrent effect	Qualitative
Integration with law enforcement	Qualitative
Increased employee safety	Qualitative
Acceptability	
Investigation Checklist Usage	0-100% Avg. = 39%[1]

1 - Actual costs were adjusted to 2007 dollars to calculate the total 20 year lifecycle cost.

Section 8.0: References

ASCE/AWWA. 2006. *Guidelines for the Physical Security of Water Utilities*. ASCE/AWWA Draft American National Standard for Trial Use.

U.S. Environmental Protection Agency. 2008. *Water Security Initiative: Cincinnati Pilot Post-Implementation System Status*. EPA 817-R-08-004.

U.S. Environmental Protection Agency. 2014a. *Water Security Initiative: Comprehensive Evaluation of the Cincinnati Contamination Warning System Pilot* EPA 817-R-14-001.

U.S. Environmental Protection Agency. 2014b. *Water Security Initiative: Evaluation of the Cincinnati Contamination Warning System Pilot* EPA 817-R-14-001A.

Section 9.0: Abbreviations

The list below includes acronyms approved for use in the ESM component evaluation. Acronyms are defined at first use in the document.

ASCE	American Society of Civil Engineers
AWWA	American Water Works Association
CRADA	Cooperative Research and Development Agreement
CWS	Contamination Warning System
DSL	Digital Subscriber Line
EPA	United States Environmental Protection Agency
ESM	Enhanced Security Monitoring
FSE	Full Scale Exercise
GCWW	Greater Cincinnati Water Works
HazMat	Hazardous Materials Removal Team
HMI	Human Machine Interface
I/O	Input/Output
O&M	Operation and Maintenance
PHS	Public Health Surveillance
PLC	Programmable Logic Controller
PTZ	Pan-Tilt-Zoom
SCADA	Supervisory Control and Data Acquisition
SOP	Standard Operating Procedure
T1	T-carrier 1
TCP	Transmission Control Protocol
TEVA	Threat Ensemble Vulnerability Assessment
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
WAN	Wide Area Network
WaterISAC	Water Information Sharing and Analysis Center
WUERM	Water Utility Emergency Response Manager
ZOI	Zone of Influence

Section 10.0: Glossary

Alert. Information from a monitoring and surveillance component indicating an anomaly in the system, which warrants further investigation to determine if the alert is valid.

Alert Investigation. A systematic process, documented in a standard operating procedure, for determining whether or not an alert is valid and identifying the cause of the alert. If an alert cause cannot be identified, contamination is possible.

Anomaly. Deviations from an established baseline. For example, a water quality anomaly is a deviation from typical water quality patterns observed over an extended period.

Baseline. Normal conditions that result from typical system operation. The baseline includes predictable fluctuations in measured parameters that result from known changes to the system. For example, a water quality baseline includes the effects of draining and filling tanks, pump operation and seasonal changes in water demand, all of which may alter water quality in a somewhat predictable fashion.

Benefit. An outcome associated with the implementation and operation of a contamination warning system that promotes the welfare of the utility and the community it serves. Benefits are classified as either primary or dual-use.

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

Component response procedures. Documentation of roles and responsibilities, process flows, and procedural activities for a specified component of the contamination warning system, including the investigation of alerts from the component. Standard operating procedures for each monitoring and surveillance component are integrated into an operational strategy for the contamination warning system.

Confirmed. In the context of the threat level determination process, contamination is confirmed when the analysis of all available information from the contamination warning system has provided definitive, or nearly definitive, evidence of the presence of a specific contaminant or class of contaminant in the distribution system. While positive results from laboratory analysis of a sample collected from the distribution system can be a basis for confirming contamination, a preponderance of evidence, without the benefit of laboratory results, can lead to this same determination.

Consequence management. Actions taken to plan for and respond to possible contamination incidents. This includes the threat level determination process, which uses information from all monitoring and surveillance components as well as sampling and analysis to determine if contamination is credible or confirmed. Response actions, including operational changes, public notification and public health response, are implemented to minimize public health and economic impacts, and ultimately return the utility to normal operations.

Consequence management plan. Documentation that provides a decision-making framework to guide investigative and response activities implemented in response to a possible contamination incident.

Contamination incident. The introduction of a contaminant in the distribution system with the potential to cause harm to the utility or the community served by the utility. A contamination incident may be intentional or accidental.

Contamination scenario. Within the context of the simulation study, parameters that define a specific contamination incident, including: injection location, injection rate, injection duration, time the injection is initiated and the contaminant that is injected.

Contamination warning system. An integrated system of monitoring and surveillance components designed to detect contamination in a drinking water distribution system. The system relies on integration of information from these monitoring and surveillance activities along with timely investigative and response actions during consequence management to minimize the consequences of a contamination incident.

Costs, implementation. Installed cost of equipment, IT components and subsystems necessary to deploy an operational system. Implementation costs include labor and other expenditures (equipment, supplies, and purchased services).

Cost, life cycle. The total cost of a system, component or equipment over its useful or practical life. Life cycle cost includes the cost of implementation, operation & maintenance and renewal & replacement.

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

Costs, renewal & replacement. Costs associated with refurbishing or replacing major pieces of equipment (e.g., water quality sensors, laboratory instruments, IT hardware, etc.) that reach the end of their useful life before the end of the contamination warning system lifecycle.

Coverage, contaminant. Specific contaminants that can potentially be detected by each monitoring and surveillance component, including sampling & analysis, of a contamination warning system.

Coverage, spatial. The areas within the distribution system that are monitored by, or protected by, each monitoring and surveillance component of a contamination warning system.

Credible. In the context of the threat level determination process, a water contamination threat is characterized as credible if information collected during the investigation of possible contamination corroborates information from the validated contamination warning system alert.

Data completeness. The amount of data that can be used to support system or component operations, expressed as a percentage of all data generated by the system or component. Data may be lost due to QC failures, data transmission errors and faulty equipment among other causes.

Distribution system model. A mathematical representation of a drinking water distribution system, including pipes, junctions, valves, pumps, tanks, reservoirs, etc. The model characterizes flow and pressure of water through the system. Distribution system models may include a water quality model that can predict the fate and transport of a material throughout the distribution system.

Door/Hatch Prop. An occurrence when personnel left a door or hatch open that should have been closed. An example of such an occurrence could be when utility staff used an object to prevent a door

from closing for ease of entry or exit during maintenance activities and left the facility without closing the door.

Dual-use benefit. A positive application of a piece of equipment, procedure, or capability that was deployed as part of the contamination warning system, in the normal operations of the utility.

Ensemble. The comprehensive set of contamination scenarios evaluated during the simulation study.

Event detection system. A system designed specifically to detect anomalies from the various monitoring and surveillance components of a contamination warning system. An event detection system may take a variety of forms, ranging from a complex set of computer algorithms to a simple set of heuristics that are manually implemented.

Evaluation period. The period from January 16, 2008 to June 15, 2010 when data was actively collected for the evaluation of the Cincinnati CWS.

Hydraulic connectivity. Points or areas within a distribution system that are on a common flow path.

Incident Commander. In the Incident Command System, the individual responsible for all aspects of an emergency response; including quickly developing incident objectives, managing incident operations, and allocating resources.

Incident timeline. The cumulative time from the beginning of a contamination incident until response actions are effectively implemented. Elements of the incident timeline include: time for detection, time for alert validation; time for threat level determination, and time to implement response actions.

Injection duration. The cumulative time over which the bulk volume of a contaminant is injected into the distribution system at a specific location for a given scenario within the simulation study.

Injection location. The specific node in the distribution system model where the bulk contaminant is injected into the distribution system for a given scenario within the simulation study.

Injection rate. The mass flow rate at which the bulk volume of a contaminant is injected into the distribution system at a specific location for a given scenario within the simulation study.

Invalid alert. An alert from a monitoring and surveillance component that is not due to an anomaly and is not associated with an incident or condition of interest to the utility.

Job function. A description of the duties and responsibilities of a specific job within an organization.

Metric. A standard or statistic for measuring or quantifying an attribute of the contamination warning system or its components.

Model. A mathematical representation of a physical system.

Model parameters. Fixed values in a model that define important aspects of the physical system.

Module. A sub-component of a model that typically represents a specific function of the real-world system being modeled.

Monetizable. A cost or benefit whose monetary value can be reliably estimated from the available information.

Monitoring & surveillance component. Element of a contamination warning system used to detect unusual water quality conditions, potentially including contamination incidents. The four monitoring & surveillance components of a contamination warning system include: 1) online water quality monitoring, 2) enhanced security monitoring, 3) customer complaint surveillance and 4) public health surveillance.

Net present value. The difference between the present value of benefits and costs, normalized to a common year.

No call-in. An occurrence when GCWW personnel did not follow established procedures for calling in to the utility control center within a designated time span of entering a facility. An intrusion alert was generated automatically when anyone entered a facility, but an entry was considered valid if an employee called in within a designated time span. Personnel at the utility control center could observe a no call-in incident when the video clip showed an employee entering the facility. If video data were not available, a no call-in incident could be verified when onsite investigators or local law enforcement arrived at the facility and witnessed the employees at the site.

Node. A mathematical representation of a junction between two or more distribution system pipes, or a terminal point in a pipe in a water distribution system model. Water may be withdrawn from the system at nodes, representing a portion of the system demand.

Nuisance chemicals. Chemical contaminants with a relatively low toxicity, which thus generally do not pose an immediate threat to public health. However, contamination with these chemicals can make the drinking water supply unusable.

Operational strategy. Documentation that integrates the standard operating procedures that guide routine operation of the monitoring and surveillance components of a drinking water contamination warning system. The operational strategy establishes specific roles and responsibilities for the component and procedures for investigating alerts.

Optimization phase. Period in the contamination warning system deployment timeline between the completion of system installation and real-time monitoring. During this phase the system is operational, but not expected to produce actionable alerts. Instead, this phase provides an opportunity to learn the system and optimize performance (e.g., fix or replace malfunctioning equipment, eliminate software bugs, test procedures and reduce occurrence of invalid alerts).

Pan-tilt-zoom camera. A camera that is capable of rotating 360 degrees horizontally and 90 degrees vertically. Furthermore, the camera view can be zoomed-in or widened to the extent of the lens and mechanism. Pan-tilt-zoom cameras installed for the Cincinnati pilot were programmed to focus on preset locations when the associated door or motion sensor detected an intrusion.

Pathogens. Microorganisms that cause infections and subsequent illness and mortality in the exposed population.

Possible. In the context of the threat level determination process, a water contamination threat is characterized as possible if the cause of a validated contamination warning system alert is unknown.

Primary benefits. Benefits that are derived from the reduction in consequences associated with a contamination incident due to deployment of a contamination warning system.

Priority contaminant. A contaminant that has been identified by the EPA for monitoring under the Water Security Initiative. Priority contaminants may be initially detected through one of the monitoring and surveillance components and confirmed through laboratory analysis of samples collected during the investigation of a possible contamination incident.

Process flow. The central element of a standard operating procedure that guides routine monitoring and surveillance activities in a contamination warning system. The process flow is represented in a flow diagram that shows the step-by-step process for investigation alerts, identifying the potential cause of the alert and determining whether contamination is possible.

Radio fault. The radio fault is a feature of the GCWW SCADA network. The non-video sites used the existing GCWW SCADA network for transmitting the ESM intrusion alerts to the utility control center. Certain GCWW remote sites used wireless I/O modules to transmit data to a facility with a hardwired connection to the GCWW SCADA network. Three of the five ladder sites at non-video locations used wireless I/O modules. An invalid ladder alert was triggered when the wireless I/O module experienced a loss in signal strength, which could result from signal path blockage or radio interference. Usually a radio fault was transmitted to the GCWW SCADA network with the ladder alert following loss in signal strength, but there were also occasions where a radio fault was not generated but a false tank level alert accompanied the false ladder alert. Both conditions were used to determine when a ladder alert was caused by a radio issue.

Real-time monitoring phase. Period in the contamination warning system deployment timeline following the optimization phase. During this phase, the system is fully operational and is producing actionable alerts. Utility staff and partners now respond to alerts in real-time and in full accordance with standard operating procedures documented in the operational strategy. Optimization of the system still occurs as part of a continuous improvement process, however the system is no longer considered to be developmental.

Routine operation. The day-to-day monitoring and surveillance activities of the contamination warning system that are guided by the operational strategy. To the extent possible, routine operation of the contamination warning system is integrated into the routine operations of the drinking water utility.

Salvage value. Estimated value of assets at the end of the useful life of the system.

Scenario subset. A group of scenarios that represent a portion of the full ensemble. Typically, scenario subsets will be defined by specific values or ranges of values for scenario parameters.

Security breach. An unauthorized intrusion into a secured facility that may be discovered through direct observation, an alert or signs of intrusion (e.g., cut locks, open doors, cut fences).

Simulation study. A study designed to systematically characterize the detection capabilities of the Cincinnati drinking water contamination warning system. In this study, a computer model of the contamination warning system is challenged with an ensemble of 2,023 simulated contamination scenarios. The output from these simulations provides estimates of the consequences resulting from each contamination scenario, including fatalities, illnesses and extent of distribution system contamination. Consequences are estimated under two cases, with and without the contamination warning system in operation. The difference provides an estimate of the reduction in consequences.

Time for confirmed determination. A portion of the incident timeline that begins with the determination that contamination is credible and ends with contamination either being confirmed or ruled

out. This includes the time required to perform lab analyses, collect additional information, and analyze the collective information to determine if the preponderance of evidence confirms the incident.

Time for contaminant detection. A portion of the incident timeline that begins with the start of contamination injection and ends with the generation and recognition of an alert. The time for contaminant detection may be subdivided for specific components to capture important elements of this portion of the incident timeline (e.g., sample processing time, data transmission time, event detection time, etc.).

Time for credible determination. A portion of the incident timeline that begins with the recognition of a possible contamination incident and ends with a determination regarding whether contamination is credible. This includes the time required to perform multi-component investigation and data integration, implement field investigations (such as site characterization and sampling), and collect additional information to support the investigation.

Time for initial alert validation. A portion of the incident timeline that begins with the recognition of an alert and ends with a determination regarding whether or not contamination is possible.

Toxic chemicals. Highly toxic chemicals that pose an acute risk to public health at relatively low concentrations.

Valid Alert. Alerts due to water contamination, system events (i.e., work in the distribution system for CCS or WQM), or public health incidents (for PHS), or an occurrence where an actual intrusion incident happened (ESM).

Video Clip. A data file of video imagery of a preset duration and resolution. A video clip of each detected intrusion was transmitted to the utility control center for assessment by operations personnel. This minimized the load on the communications system while provide personnel with visual evidence to validate whether an intrusion or contamination incident was actually occurring without having to conduct an onsite investigation.

Water Utility Emergency Response Manager. A role within the Cincinnati contamination warning system filled by a mid-level manager from the drinking water utility. Responsibilities of this position include: receiving notification of validated alerts, verifying that a valid alert indicates possible contamination, coordinating the threat level determination process, integrating information across the different monitoring and surveillance components, and activating the consequence management plan. In the early stages of responding to possible contamination, the Water Utility Emergency Response Manager may serve as Incident Commander.