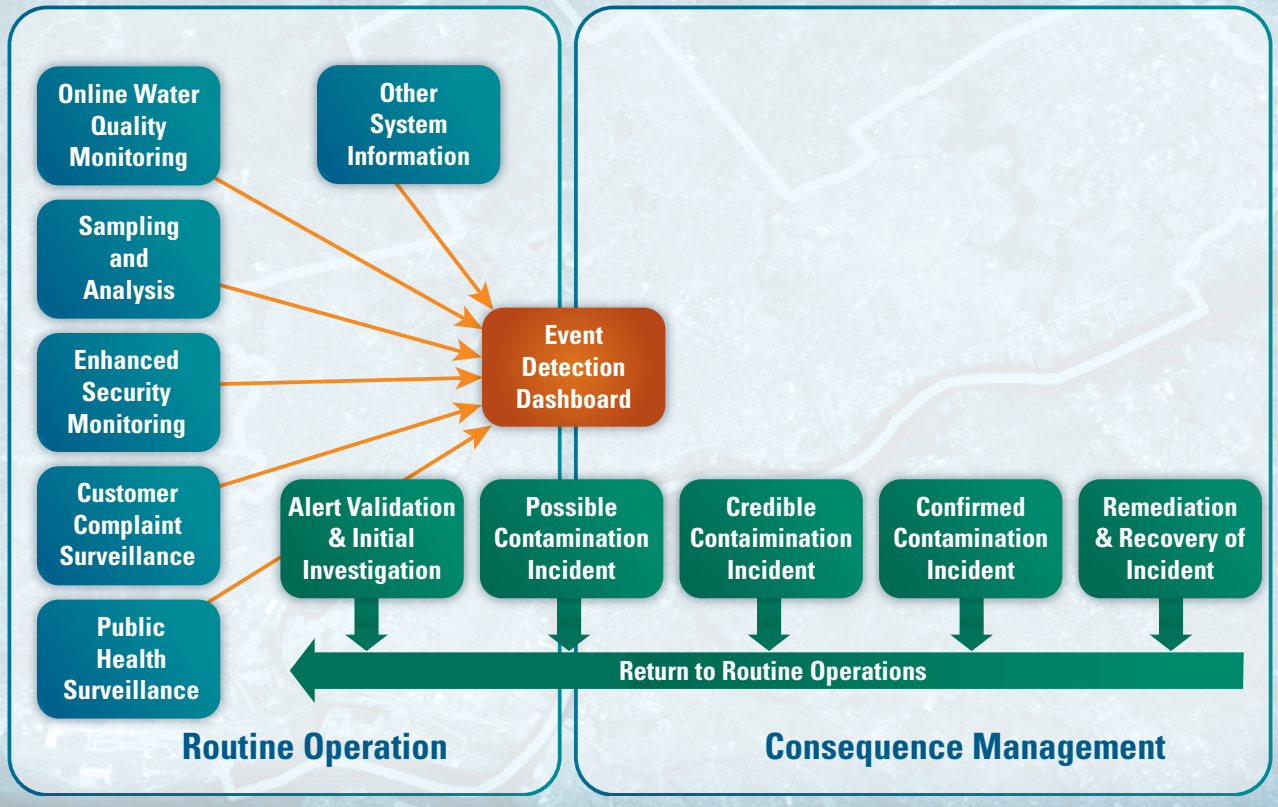
Philadelphia Water Department

May 2013

Philadelphia Water Department
Contamination Warning System Demonstration Pilot Project:

Enhanced Security Monitoring





WBG012313172402PHL

CH2MHILL®

EPA Disclaimer

Although the information in this document has been funded wholly or in part by the United States Environmental Protection Agency under the Water Security Initiative program, it may not necessarily reflect the views of the agency and no official endorsement should be inferred.

When referencing this white paper in another document, please use the following citation:

Philadelphia Water Department and CH2M HILL. May 2013. Philadelphia Water Department Contamination Warning System Demonstration Pilot Project: Enhanced Security Monitoring. White Paper Submitted to EPA as part of the Water Security Initiative Grant Awarded to Philadelphia Water Department.

This paper can also be downloaded from www.ch2mhill.com/iws.

Acknowledgments

The Philadelphia Water Department would like to recognize the following individuals and organizations for their assistance and contributions in the development of this document:

EPA Water Security Division

- Brian Pickard, PE, BCEE
- Captain Nelson Mix, PE, CHMM

Contractor Support

- Forrest Gist, PE, CH2M HILL
- Brian Lee, PE, CH2M HILL
- Randy Lynn, CH2M HILL
- Christopher Wiggins, CH2M HILL
- Priyanka Uppu, R2T
- Lynn Scofield, CH2M HILL
- Yakir Hasit, PhD, PE, CH2M HILL

Questions concerning this document should be addressed to:

Jim Golembeski, PE
Philadelphia Water Department
1101 Market Street
ARAMARK Tower, 5th Floor
Philadelphia, PA 19107-2994
Phone: 215-685-6194
E-mail: Jim.Golembeski@phila.gov

Gary Burlingame
Philadelphia Water Department
Bureau of Laboratory Services
1500 E Hunting Park Avenue
Philadelphia, PA 19124
Phone: 215-685-1402
E-mail: Gary.Burlingame@phila.gov

Yakir Hasit, PhD, PE
CH2M HILL
1717 Arch Street
Suite 4400
Philadelphia, PA 19103
Phone: 215-640-9027
E-mail: Yakir.Hasit@ch2m.com

Abstract

The Philadelphia Water Department (PWD) developed a comprehensive contamination warning system (CWS) for its drinking water system under a Water Security (WS) initiative grant from the U.S. Environmental Protection Agency (EPA). The enhanced security monitoring (ESM) objective is to detect and respond to security breaches at locations vulnerable to contamination. This objective is accomplished through the development of equipment installations, procedures, and staff knowledge that effectively integrate into the utility's security and contamination warning system.

This paper provides general information on establishing enhanced security monitoring at a water utility, and presents an overview of the steps for identifying and assessing upgrade needs, evaluating technologies, designing security monitoring systems, bidding, and commissioning. PWD's recommendations and experience is offered in support of ESM.

Project Background

PWD developed a comprehensive CWS for its drinking water system under a WS initiative grant. The WS initiative is a program developed by the EPA in partnership with drinking water utilities and other key stakeholders in response to Homeland Security Presidential Directive 9. The WS initiative involves designing, deploying, and evaluating a model CWS for drinking water security. A CWS is a systematic approach to the collection of information from various sources, including monitoring and surveillance programs, to detect contamination events in drinking water early enough to reduce public health or economic consequences. The WS initiative goal is to develop water security CWS guidance that can be applied by drinking water utilities nationwide.

The CWS project has six major components:

1. Online water quality monitoring
2. Sampling and analysis
3. Enhanced security monitoring
4. Customer complaint surveillance
5. Public health surveillance
6. Consequence management

ESM includes the systems, equipment, and procedures used to detect and respond to security breaches at locations vulnerable to contamination. The monitoring approach includes detection by physical security components, such as sensors, alarms, and cameras, as well as eyewitness accounts, threats made by perpetrators and actionable intelligence from law enforcement, and the response methods linked to these. The ESM component of the WS initiative pilot is designed to help differentiate security alarms and notifications related to a contamination incident from those related to other activities such as vandalism, trespassing, or an unintentional alarm activation.

During the course of the ESM project for PWD, several fundamental process steps were followed that are applicable to any utility seeking to upgrade its security:

1. Identify water distribution sites/facilities for security upgrade.
2. Review existing security infrastructure, if any.
3. Determine potential security upgrades and establish a basis of design.
4. Evaluate appropriate security technology.
5. Select equipment and design the system.
6. Conduct the bidding and installation processes.
7. Commission and test the system.
8. Identify lessons learned.

Although each security upgrade project is unique and will have distinctive challenges, the process steps noted above are universal in their applicability to any security upgrade. Each process step was followed during the course of the project. The results and observations from each step are noted below to assist other utilities wishing to follow the same process and learn from PWD's experience.

CH2M HILL served as the project contractor and supported PWD in development of its CWS. CH2M HILL supported PWD in ESM equipment site selection, technology evaluation, and implementation of the upgraded system.

Facility Types and Site Selection

PWD's facilities span a wide variety of facility types, including intakes, storage tanks, reservoirs, pumping stations, and the Load Control facility. Some of the facilities date to the early twentieth century and are historical buildings. Others are more modern facilities, such as the Load Control facility, where all water-related supervisory control and data acquisition (SCADA) displays are monitored/controlled 24 hours a day and water distribution issues are evaluated and responses initiated.

The original project methodology was to identify facilities that would receive ESM equipment using the results of the Threat Ensemble Vulnerability Assessment–Sensor Placement and Optimization Tool (TEVA-SPOT) analysis to identify the most critical facilities. TEVA-SPOT is a computational tool developed in part by Sandia National Laboratories that allows a utility to optimize its sensor placement within a water distribution system. Instead of using TEVA-SPOT, PWD stakeholders identified facilities using the results of its own vulnerability assessment and knowledge of the size of the service area associated with each site. It was decided that, although TEVA-SPOT analyses would provide useful information, PWD's broad experience and deep understanding of each facility from hydraulic, security, and criticality perspectives would provide a more simplified means of ranking each facility for inclusion in the project. As a result, the facilities were ranked in order of priority and importance by PWD's vulnerability assessment. The overall list of facilities was grouped into 2 phases: a small pilot phase (Phase 1) consisting of 3 different types of sites (Tank, Reservoir, Pumping Station) plus Load Control monitoring upgrades, and a larger subsequent phase (Phase 2) consisting of the remainder of the sites. Eventually, Phase 3, consisting of source water intake and pumping facilities, was initiated and self-funded by PWD.

Existing PWD Security Monitoring Infrastructure

At project initiation, PWD had several analog video surveillance camera systems haphazardly located at some of the water facilities. The systems consisted of analog Panasonic cameras and an onsite Panasonic analog video recorder to store video data from each camera. Some video was transmitted to a security workstation computer at Load Control. The system has worked well and has been largely trouble-free.

PWD physical security alarm data are received and managed primarily at the PWD Load Control facility. Security intrusion alarm conditions are detected by discrete door and window contact sensors and motion sensors. The sensors are monitored by remote terminal units (RTUs), and the data are transmitted by modem phone lines to the SCADA server at Load Control. The system incorporates a keypad mounted within each facility and door contact sensors. Upon entering a facility, users must enter their unique personal identification number (PIN) access codes within a designated period; otherwise a SCADA alarm is initiated and transmitted to Load Control.

No utility-wide security network existed before the project. Instead, video data was sent over a Verizon T1 line using Internet protocol (IP).

Proposed New Systems and Basis of Design

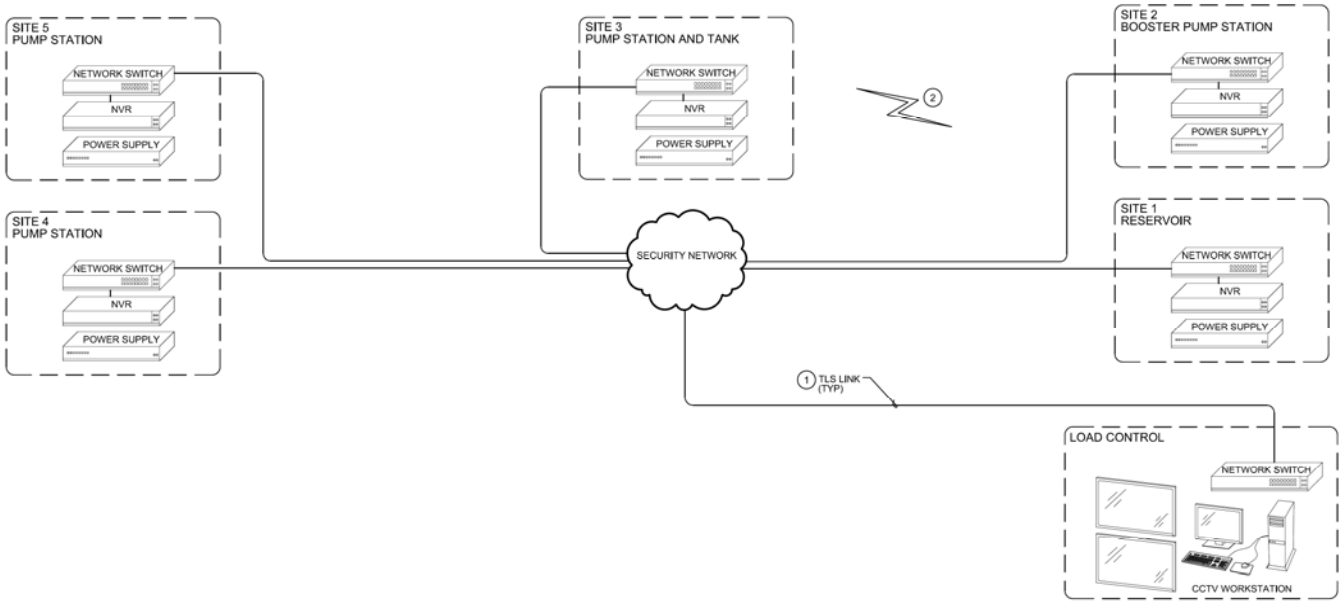
During the initial planning for the ESM project, several key concepts were discussed and determined. The early planning led to a set of design parameters or goals that guided the subsequent design of the system. For example, one fundamental design parameter of the closed circuit television (CCTV) system was that it view and record usable video that could be reviewed in the event of a security breach. The video is primarily to interpret intent, rather than attempting to identify individuals. As such, perimeter camera coverage was provided at building entrances, approachways, or viewing areas where there is access to the water and/or other critical assets. As another goal, the project team wanted the security components, such as surveillance cameras, to be visible to discourage intruders,

but still “aesthetically pleasing” so as to complement the building from an architectural perspective. The team also needed to keep the existing SCADA system and video systems separate to ensure the SCADA system could not be hacked into via the network connection used for the video.

System Architecture – The basis of design for the overall security system network architecture was to develop and incorporate a new broadband network across the PWD sites, serving new video surveillance and network recording equipment, integrating alarm outputs/inputs from the existing SCADA run security systems, and adding new video monitoring controls at Load Control.

Broadband Network – The basis of design for the ESM systems was to link the separate sites using a broadband network of sufficient bandwidth to serve all of the additional cameras and other security components so that all components can be viewed from Load Control (Figure 1). The decision was made to lease high-speed fiber-optic network service from Verizon, using its Transparent LAN Service (TLS). The service provides bandwidth values of 10Mb/s, 100Mb/s, and 1Gb/s. For most sites, a transmission speed of 10Mb/s was selected, providing adequate bandwidth for all video cameras yet still permitting additional unused bandwidth capacity if additional cameras are installed. The TLS lines represent an ongoing monthly fee that PWD incurs to maintain video connectivity to Load Control.

FIGURE 1
ESM Network Architecture



Partial network diagram; not all sites are depicted.

Video Review and Monitoring – Within the ESM upgrades, the basis of design philosophy was to provide complete CCTV viewing capability at the Load Control facility. To accomplish this, a new video server running Panasonic video management software, a new CCTV workstation, and two 42-inch plasma monitors have been provided, as well as a 19-inch desktop monitor and CCTV joystick (Figure 2). The video server and workstation equipment have been carefully located so that the Load Control operator is able to simultaneously view the CCTV images along with the SCADA displays. During a security event, the Load Control operator can view and assess the video images to determine whether to contact 911 or to initiate further investigation by a PWD roving engineer. Careful consideration has been given to minimize the impact of the CCTV system and any resulting security alarms with the Load Control operator’s workload. A large graphical map display of the utility has been arranged on one of the CCTV monitors. A mouse click on any facility on the utility map results in site area of that facility being displayed, along with corresponding camera thumbnails for review.

FIGURE 2
ESM Display Monitors at Load Control

SCADA Integration – The ESM system relies on the SCADA keypads that control access into the facilities. Upon entering a facility, PWD staff is instructed to enter their unique PIN sequence onto the entry keypad within a specified period. If a valid PIN is not entered within a specific period, a SCADA alarm is generated, and PWD response procedures are initiated.

An enhancement identified during the ESM project and incorporated as a basis of design was the interconnection between SCADA and CCTV. In all, four alarms are transmitted between the SCADA and CCTV systems at each site receiving ESM upgrades:

- Alarms Transmitted from CCTV to SCADA – The following alarm conditions are transmitted from the CCTV video system by a dry contact relay output to a designated RTU, where they may be viewed on the SCADA system:
  - Loss of Power – The CCTV system has lost normal power and is running on uninterruptible power supply at the site.
  - Equipment Trouble – The CCTV system network video recorder has experienced a system failure at the site.
  - Loss of Connectivity – The CCTV system has experienced loss of video at one or more cameras, indicating a camera has gone down or is experiencing a trouble condition at the site.
- Alarms Transmitted from SCADA to CCTV: The following alarm condition is transmitted from the SCADA system by a dry relay contact output from a designated RTU, where it is monitored by the CCTV video system:
  - Unacknowledged Door Alarm – A valid PIN was not entered at the entry keypad at the site, causing a SCADA alarm to be generated and transmitted to the CCTV system.

Technology Evaluation

The security upgrades to the ESM system included CCTV, network video recording, and intrusion detection. For each security subsystem, an evaluation was made to determine the most appropriate technology to be used. The results of these evaluations are described below.

CCTV – The CCTV system was selected to be an IP-based system, taking advantage of technology advances in IP cameras, recording, and networking. IP video (as opposed to analog video) offers the advantages of greater options for video transmission modes, enables more flexible storage and retrieval of video, and can be more easily compressed into smaller file sizes resulting in lower bandwidth. In general, CCTV system equipment manufactured by Panasonic, or compatible with Panasonic, was chosen so that the new video system could more easily interface with PWD's existing video equipment.

Network Video Recording – An early design decision was made to use local storage rather than centralized storage. This decision had the advantage of reducing the amount of bandwidth transmitted throughout the video network and localizing any component failures to only one site. As a result, the camera images at each site were digitally recorded locally on a network video recorder (NVR) located at that site, and then transmitted on demand back to Load Control.

Intrusion Detection – Intrusion detection largely consisted of door sensors that are interconnected to SCADA. Where door sensors were non-existent, missing, or needed to be replaced, sensors were added within the ESM project at appropriate locations. The intent is that all exterior doors be monitored with door contact sensors. In some locations, additional intrusion detection sensors were added where the threat of intrusion by an adversary existed. The intrusion detection motion sensors are described further in this report.

Access Control – Access control is served by means of keypads interconnected to the SCADA system.

Integration with CWS Dashboard – There is no direct integration of the ESM system with the CWS dashboard. PWD opted against linking the SCADA and ESM systems to continue to operate SCADA as a standalone system. Because there may be greater potential for false alarms from the ESM component than from other components, whether due to maintenance workers inadvertently activating motion sensors, unacknowledged door alarms, or other reasons, PWD decided that filtering alarms through the Load Control Operator presented a better option than sending all alarms to the dashboard. The possibility of allowing each ESM camera to be viewed through the dashboard was considered, but it was not pursued because of associated bandwidth requirements. Other utilities may want to consider the complications that may arise with multiple users attempting to control pan-tilt-zoom (PTZ) cameras over a dashboard.

Upon receiving a security alarm through SCADA (such as a door forced alarm), the Load Control Operator observes video of the appropriate site and contacts the roving engineer. The roving engineer reports to the Load Control Operator whether it appears that there has been a contamination incident. The Load Control Operator then decides whether to escalate (contacting 911 and the Load Control Standby) the incident. The Load Control Standby can then create an “event” and upload video clips to the dashboard if warranted.

Design Process and Selected Equipment

Once the basis of design parameters and technology evaluations have been completed, the design process can begin. A project decision was made to keep the design plan drawings conceptually simple but to add detail to the technical specifications and to the schematic one-line diagrams. The benefit of this decision is that the design process can proceed rapidly, with minimal drawing development time and subsequent review time. During the shop drawing submittal process, drawing enhancements were incorporated to the final set of plan drawings. The technical specifications could be reused for each phase of the project while incorporating lessons learned or issues in subsequent versions of the specifications to improve them.

At this stage of the design process, component selections were made regarding each item of ESM equipment to be used in the system.

- **Network Switches** – At each site, a point-of-presence network switch was added. The network switches provide a point of demarcation between the PWD systems and the incoming Verizon TLS lines, linking the cameras and video recording equipment together at the site. The network switches are industrially hardened units manufactured by Cisco (model WS-C3750 rack-mounted units). These units were selected because of their interoperability with City of Philadelphia Office of Innovation and Technology (OIT) standards and their wide compatibility with the various network configurations and standards.
- **Network Video Recorders** – The NVRs for each site were sufficiently sized to provide storage capacity for all cameras at 10 images per second, 4CIF resolution (704 × 576 pixels), for at least 30 days. After 30 days, the video images may be archived or overwritten (oldest recordings are overwritten first), depending upon PWD’s preference. As a standard, 2-terabyte hard disks have been used at each site for video storage. Panasonic WJ-ND400 NVRs have been selected for interoperability with PWD’s video equipment.

- **Fixed and Pan/Tilt/Zoom Cameras** – A combination of fixed and PTZ cameras was selected for the ESM facilities. For many facilities, at least one PTZ camera was installed, with the camera set to ”tour mode.” Tour mode means that the camera automatically and continually sweeps across a pre-programmed area of coverage. Most of the PTZ cameras have a 36x optical zoom capability, which allows very clear manual zoom capability at long ranges. During the installation commissioning process, preset camera call-up positions have been programmed and tested so that areas of interest can be called up and viewed quickly within the overall area of coverage for the PTZ cameras. All cameras have been focused to provide sharp picture clarity under daytime and nighttime conditions. The Panasonic model WV-NW960 was selected for PTZ camera use.
- **Low Light Day/Night Cameras** – Wherever possible, day/night cameras were selected so that the cameras can operate under ambient lighting conditions. Low-light, day/night technology enables the camera images to appear as color during conditions with good ambient lighting, and black and white images under low light conditions, permitting better nighttime visibility. Day/night cameras manufactured by Panasonic were used for the PWD ESM project because of their interoperability with the Panasonic equipment in use by PWD. A design decision made early within the project was to minimize adding new lighting at the project locations. This camera selection avoided lighting complaints and the resulting installation, energy, and maintenance costs inherent with adding new lighting. Panasonic WN-NW484S cameras were selected for day/night mini-dome use.
- **Infrared/Thermal Cameras** – At certain locations, infrared/thermal cameras were used as they do not require ambient lighting to operate. Thermal cameras use heat signatures rather than ambient lighting, showing variations in temperature as white and gray areas. Warm objects (such as humans) appear white, while ambient temperatures (such as roadways and foliage) appear gray or black. Thermal cameras manufactured by FLIR Systems were used for the PWD ESM project because of their industry reputation for effectiveness and durability.
- **IR Illuminators** – Where FLIR Systems cameras are not practical, the use of infrared (IR) illuminators was considered. IR illuminators shine a light within the IR wavelength to illuminate an area for camera viewing. Cameras calibrated for IR illuminators can see the light, but the human eye cannot see the IR wavelength. To a casual observer, an IR illuminator looks similar to a red light at a traffic intersection.
- **Backup Power** – An important consideration within the ESM design for PWD was backup power. Philadelphia experiences frequent lightning strikes in summer. This, coupled with snow conditions during winter that disrupt power lines, can make power reliability uncertain. Therefore, at each site an uninterruptible power supply was incorporated into the design. The duration of the power supplies typically is 1 hour of backup time, but this may differ depending upon the site. Units manufactured by Eaton PowerWare and TrippLite were selected because of their previous use and reputation within the Philadelphia area.
- **Surge Suppression** – In addition to backup power, surge suppression was an important consideration. Surge suppression ensures that voltage fluctuations and transient power disturbances are not transmitted onto the system equipment. Incoming alternating current power, Ethernet connections, and exterior IP camera connections were all protected from surges using units manufactured by Ditek.
- **Wireless Systems** – For some sites, cameras are used in areas that would require trenching/excavation to add new conduit. At these sites, wireless radio communication equipment was used. The radio communication transmits the video from a transmitter unit, located near the camera, to a receiver unit, located near the video storage equipment. Nonlicensed, line-of-sight equipment manufactured by Firetide was chosen for robust performance, bandwidth, and reputation. Shrubs or trees that grow within the line of sight of the radio unit will need to be pruned from time to time so that they do not obstruct the radio signal.
- **Motion Detection** – To provide additional detection capabilities, various types of motion detection sensors were added to various sites.
  - Tank ladders at some sites incorporated motion detection to detect the presence of an individual attempting to climb the ladder. Discrete motion sensors were used in these applications. The motion sensors have tended to drift down over time, in which their original target area of the tank ladder has

drifted down so that they now detect persons underneath the ladder, causing nuisance alarms. This issue is being investigated. The motion detection units are manufactured by Xtralis.

- Video motion detection software was incorporated at some sites at tank ladder installations to detect an individual attempting to climb a tank ladder. The video analytic software can detect unusual motion within a predefined area of coverage, and based on pixel changes and motion within the area it can issue an alarm. The video motion software is manufactured by Panasonic and integrated within the NVR firmware.
- At one site, an array of motion sensors was installed at the perimeter of the site area. This site is unique in that it uses a floating membrane cover. The goal of the motion sensors is to detect the presence of an intruder on the perimeter of the site before the intruder reaches and accesses the membrane cover area. Despite the fact that the motion sensors were selected based on their performance for outdoor use, they have been problematic. They are susceptible to detecting cars on the adjacent roadway, causing nuisance alarms. Tuning of the sensors is ongoing. The motion detection units are manufactured by Xtralis.

Bidding and Installation Process

The pilot phase (Phase 1) employed a prequalification process that requested information from the potential bidders including firm size, number of local personnel, firm references, similar projects completed, and certified qualifications. All of the vendors were required to sign a confidentiality agreement and only then were they able to get further details of the basic design plans and specs. Following the submittal of prequalification documents, four representative bidders were invited to bid on the Phase 1, 2 and 3 projects; three firms submitted bids. Two were local Pennsylvania security integration firms, and the third was a large, national security system integrator.

A competitive bidding process was followed for each phase. The three bidding firms were invited to a prebid meeting whereby they could tour the ESM project sites and thereby take notes and photos. A 2-week period following the prebid meeting was established for bidders to assemble their bid quotations. During this period, the design consultant (CH2M HILL) responded to technical questions.

During the pilot phase, unit pricing was requested of the bidders. The unit pricing formed the basis of a detailed cost estimate developed for Phases 2 and 3 using the unit pricing received within Phase 1. It turned out that the prices received for Phase 2 were much lower than expected.

Through the competitive bidding process used for Phases 1, 2, and 3, each of the three system integrators was awarded some portion of the project. Each system integrator had unique strengths and weaknesses. For example, one did well at adhering to the agreed-upon project schedule but not so well at managing client-requested changes. Another did well at identifying creative solutions to resolve issues but was unable to drive the installation progress to meet the schedule objectives.

In retrospect, by using three separate system integrators for Phases 1, 2, and 3, PWD was able to evaluate and use the best skill sets from each system integrator contractor to fine-tune and calibrate the overall ESM system. What might have been a disadvantage instead turned to an advantage during the project.

Commissioning

Following installation, a thorough commissioning and startup process was conducted before turning over the project to PWD.

Each phase underwent a point-by-point, camera-by-camera startup and testing process of commissioning. This has the benefit of showing the client exactly what components it is getting, demonstrating the performance of the system while confirming that all systems and components are operating as designed, meeting the owner's needs, and minimizing nuisance alarms. At one site, a pole-mounted CCTV camera was not connected to uninterruptible power. This was discovered during the uninterruptible power supply battery tests which remove power to the system and demonstrate the system can remain completely operational under battery power. This issue was soon corrected so that all PWD ESM components operate on backup power in the event of a primary power loss.

At another site, a camera was found to be mounted adjacent to a flag pole light. During nighttime camera image review, in which every camera view was observed for night time image clarity, it was discovered that the camera was blinded by the light illuminating the flag. This issue was corrected so that the camera view was usable in both daytime and nighttime. These examples illustrate issues that might not have been discovered quickly without a thorough commissioning process.

Lessons Learned

A lessons-learned session was held at the conclusion of the three phases. As might be expected, over the course of a multi-year, comprehensive project with several complex elements, several lessons learned can be extended to other utilities for their benefit.

Importance of an Information Technology Capable System Integrator – One lesson learned on the project is the importance of having a capable information technology system integrator. When installing and configuring a network, there are many network settings that can dramatically affect the performance, reliability, and operability of the network. For example, at two sites the communications failed completely after a power outage because network configuration setting changes were not saved to read-only memory by the system integrator. When network equipment was restarted after a power outage, instead of starting in a ”configured” mode, it came up in a “default” mode (without saved settings) when the power was restored. After the problem was discovered, it was corrected, and the settings at all other sites were checked and saved.

Involve the System Integrator at Project Inception – Another lesson learned is the importance of involving the information technology system integrator at the beginning of the project and continuing his or her involvement throughout the project. For example, the decision to use Verizon TLS lines to interconnect the various sites with Load Control was made early in the project. Making the network adjustments enabling the incoming TLS lines to reliably connect to the local network switches at each site has been somewhat problematic. It took multiple visits and many collaboration meetings between Verizon technicians and the system integrator technicians to work out the details. Additionally, the ongoing monthly cost of the TLS lines has been expensive. Having a system integrator on board earlier to interface with Verizon could have resulted in the video network performance parameters and settings being more clearly defined up front, possibly reducing costs for the leased lines.

Use a Single Brand to Ensure Compatibility – Ensuring system compatibility through the use of a single brand is another lesson learned. Throughout the project, Panasonic equipment was specified for cameras, network video recorder equipment, and video software. This made the installation and startup of the systems much more rapid and trouble-free than if multiple, unrelated equipment manufacturers were used. For example, the project has used thermal cameras manufactured by FLIR Systems. The cameras are very well known in the industry and are a market leader for that type of camera. However, because the cameras are not completely integrated under the Panasonic umbrella of components, there were difficulties in getting the FLIR Systems PTZ cameras to operate as desired using the Panasonic software. These issues required firmware updates of the internal camera software to get the desired PTZ camera response. The firmware upgrades took time and effort to resolve.

Use of Preapproved Vendors under Statewide Contract – Bid packages were sent to preapproved vendors under a Statewide Contract. This strategy allowed a much more rapid bidding process, avoiding the lengthy public bid advertisement stage and the resulting non-secure release of security bid documents to the public that occurs with public bids. Allowing the public to receive security bid documents is not the preferred way to safeguard these important documents during a bid process. By using the Statewide Contract mechanism, PWD avoided these issues and streamlined the bid process.

Problems with Motion Detection – External motion detection sensors have had problems. For example, the ladder motion switches have drifted down over time. Twice they detected people walking by, causing false alarms. The ladder motion sensors are undergoing review for possible replacement with a strain gauge sensor mounted directly on the ladder, rather than using discrete motion sensors. An example illustrating the difficulty of exterior motion sensors is their susceptibility to nuisance alarms by detecting cars on the adjacent roadway. The lesson learned for the PWD ESM project is that, during the design phase, the benefits of exterior sensors must be

carefully weighed against the drawbacks of potential nuisance alarms. Motion sensors must undergo a tuning and thorough testing process during final commissioning to correct any issues and to demonstrate their effectiveness.

Conclusion

The ESM project was a successful one for PWD. Through the process of upgrading the security monitoring system, PWD gained valuable experience that is useful to any utility seeking to upgrade its facility. Additionally, during the ESM upgrade, a series of fundamental steps were followed that can be used for any utility seeking to upgrade its electronic security system. These fundamental steps include:

1. Select sites for upgrade.
2. Review the existing security infrastructure.
3. Identify potential security upgrades and establish a basis of design.
4. Evaluate appropriate security technology.
5. Select equipment and design the system.
6. Develop a bidding and installation process.
7. Commission and test the system.
8. Identify lessons learned.

While every security project is unique and has certain differences, these steps are universal in their applicability to all utilities.

Abbreviations and Acronyms

CWS	Contamination warning system
CCTV	Closed-circuit television
EPA	United States Environmental Protection Agency
ESM	Enhanced Security Monitoring
Gb/s	Gigabytes per second
IP	Internet protocol
IR	Infrared
LAN	Local area network
Mb/s	Megabytes per second
NVR	Network video recorder
OIT	Office of Innovation and Technology
PIN	Personal identification number
PTZ	Pan/tilt/zoom
PWD	Philadelphia Water Department
RTU	Remote terminal units
SCADA	Supervisory Control and Data Acquisition
TEVA-SPOT	Threat Ensemble Vulnerability Assessment–Sensor Placement and Optimization Tool
TLS	Transparent LAN Service
WS	Water Security

Bibliography

Additional information on PWD's ESM design and implementation can be found at the following sources:

Baranowski, C., J.E. Golembeski, and N. Mix. 2011. "Understanding Water Sector Information Security Terminology and Governance." *Proc., Water Security Congress, AWWA, Nashville, TN.*

Mix, N., B. Pickard, A. Lai, and F. Gist. 2011. "Technology Advances put Security Measures within Reach." *Opflow*, 37(8):12-15. August.

Gist, F., A. Lai, N. Mix, and B. Pickard. 2011. "Security Equipment History, Trends, Use and Functionality-From Tried & True to Emerging & Cutting Edge." *Proc., Water Security Congress, AWWA, Nashville, TN.* See Conference Proceedings.

Mix, N., B. Pickard, F. Gist, and J. Sizcka. 2012. "Commissioning Process Ensures Security System Performance." *Opflow*, 38(8):14-15. August.