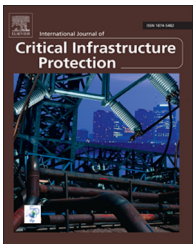
Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip



Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis

Stephen Papa[a,b], *William Casper*[a,b], *Tyler Moore*[a,*]

[a]*Computer Science and Engineering Department, Bobby Lyle School of Engineering, Southern Methodist University, P.O. Box 750122, Dallas, TX 75275, USA*

[b]*Lockheed Martin Aeronautics, 1 Lockheed Boulevard, Fort Worth, TX 76101, USA*

ARTICLE INFO

Article history:
Received 14 January 2013
Accepted 29 April 2013
Available online 4 May 2013

Keywords:
Industrial control system security
Wastewater facilities
Security economics
Cost-benefit analysis

ABSTRACT

It has been widely reported that industrial control systems underpinning critical infrastructures ranging from power plants to oil refineries are vulnerable to cyber attacks. A slew of countermeasures have been proposed to secure these systems, but their adoption has been disappointingly slow according to many experts. Operators have been reluctant to spend large sums of money to protect against threats that have only rarely materialized as attacks. But many security countermeasures are dual-use, in that they help protect against service failures caused by hackers and by accidents. In many critical infrastructure sectors, accidents caused by equipment failures and nature occur regularly, and investments for detecting and possibly preventing accidents and attacks could be more easily justified than investments for detecting and preventing attacks alone. This paper presents a cost-benefit analysis for adopting security countermeasures that reduce the incidence of sewer overflows in wastewater facilities. The paper estimates the expected annual losses at wastewater facilities due to large overflows exceeding 10,000 gallons using publicly-available data on overflows, cleanup costs, property damage and regulatory fines. Also, it estimates the costs of adopting security countermeasures in wastewater facilities in eight large U.S. cities. The results of the analysis indicate that, in many cases, even a modest 20% reduction in large overflows can render the adoption of countermeasures cost-effective.

1. Introduction

Supervisory control and data acquisition (SCADA) systems and industrial control systems (ICSs) are widely used to control systems such as water supply systems, wastewater collection and treatment facilities, refineries, oil and gas pipelines, factories, ships and subways. These systems have evolved from direct human control to computer-based control over the last several decades. Once computer-based control became common practice, a migration from proprietary to standards-based systems, protocols and interfaces occurred. Today, many systems have adopted standard wireline and RF physical interfaces, and the TCP/IP protocol is commonly used to move command and status messages within these systems. To ease management, the trend has been to connect these control networks to company intranets, which are normally connected to the Internet.

Unfortunately, SCADA systems and ICSs were not designed to defend against even the simplest network attacks. Operational commands, controller software updates, and operational status messages are not authenticated [32]. As a result, these systems are vulnerable to command

*Corresponding author.
E-mail address: tylerm@smu.edu (T. Moore).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.05.002

injection [9] and middle-person attacks [18]. A programmable logic controller (PLC) attack was at the heart of the Stuxnet virus that targeted Iranian uranium hexafluoride centrifuges [15]. Effectively, Stuxnet used a middle-person attack to change the PLC logic to report normal centrifuge operations to plant operators while issuing control commands that damaged the centrifuges.

Research efforts focused on control systems security typically take for granted that an attack will occur and instead focus on adopting security countermeasures to thwart attacks. However, attacks have been so rare in practice that asset owners and operators are reluctant to invest in adequate defenses. This paper studies one particular critical infrastructure sector – wastewater collection and treatment systems – and investigates whether the expense of security countermeasures can be justified, provided that they can also be used to prevent accidents as well as attacks. The wastewater sector is selected precisely because the intended effect of a cyber attack is the same as a relatively common failure mode – a sewer overflow. Furthermore, systems for detecting malicious overflows in wastewater systems can also detect accidental ones.

The next section, Section 2, outlines the threat model for wastewater facilities and explains how security countermeasures can be deployed in a representative system to detect and prevent sewer overflows. Section 3 presents a framework for calculating the expected costs of large sewer overflows. Detailed public data from the California Water Board is used to estimate the incidence of large sewer overflows. Reports of legal settlements are collated to estimate the cost of property damage, and EPA data on Clean Water Act violations are examined to estimate the cost of regulatory fines as well as the probability of drawing the ire of regulators. Also, an estimate for the cost of comprehensive security countermeasures is provided. Section 4 presents a cost-benefit analysis based on the findings discussed in Section 3. The net expected utility is assessed by comparing the costs with the benefits of experiencing fewer overflows. Because wastewater facilities vary greatly in complexity, a detailed analysis is provided for facilities in eight U.S. cities, with the results demonstrating that some cities are likely to view the costs as acceptable whereas other cities will not. Section 5 reviews related work in the field and Section 6 discusses key limitations of the analysis and outlines opportunities for future research.

2. System model

This section describes the threat model for wastewater facilities considered in this paper. It explains the countermeasures that have been proposed and how a representative wastewater facility may be secured using the available countermeasures.

2.1. *Threat model*

The threat model includes all sewage system overflow failures occurring at wastewater facilities, regardless of intent. The wide range of common failures includes electrical equipment failures (sensors, pumps and control electronics), blockages and structural failures. However, an overflow can also be triggered by an actor with malicious intent. The primary methods of attack on industrial control systems include command injection, service-denial and middle-person attacks [9,18,32]. Regardless of whether the attacker's motivation is wealth, fame, notoriety or terror, invariably the aim of an attack is to disrupt system operations. In this paper, we do not differentiate sanitary sewer overflows (SSOs) from combined sewer overflows (CSOs) that may be caused by accidents or attacks. A CSO involves a single collection system for both stormwater and sanitary wastewater, and an SSO involves only wastewater, but we refer to both as sewer overflows (SOs). Note that overflows typically cannot be prevented even if they detected, notably the overflows caused by excessive storm water inflow.

In the case of wastewater facilities, the most likely and disruptive method of attack is to trigger a sewer system overflow. A famous attack on a wastewater collection system is the Maroochy Water Service Breach [1]. In this attack, a SCADA system installer injected commands to a lift station, triggering millions of liters of SOs on at least 46 separate occasions. While the incidents persisted for nearly two months, we view it as a single, sustained attack rather than 46 separate attacks because it was carried out by the same perpetrator. The person responsible, Vitek Boten, was sentenced to two years in prison and was levied fines to help cover the cleanup costs; his motive was to obtain a consulting job with the utility to stop the SO incidents.

In general, the PLCs that control lift station pumps are the most logical targets for causing overflows. Attack methods include turning off one or more pumps, under pumping, or repeatedly cycling power to the pumps in order to cause motor damage and malfunctions. These attacks can be executed by modifying the PLC control logic, by injecting malicious control commands, or by modifying operator commands. PLCs are vulnerable to attack because they often have no mechanisms for authenticating commands.

2.2. *Countermeasures to prevent sewage overflows*

Two complementary types of countermeasures have been proposed to protect against attacks on control systems. The more proactive approach is to improve the integrity of control elements such as PLCs and RTUs in a SCADA system and the communications channels they rely on to transmit messages. For example, researchers have proposed retrofitting communications channels with devices to encrypt communications at the link level [14,25,33]. Alternatively, integrity can be achieved at the system level by deploying new sensors and PLCs that incorporate trusted hardware (e.g., trust anchors [17]). While the approach offers a high level of protection against attacks, adding systems such as trust anchors are expensive and do not, on their own, aid in detecting system failures or attacks.

A second class of countermeasures is much more reactive. Instead of preventing attacks by improving system and communications integrity, attacks and failures can be detected by monitoring systems for aberrant behavior. Several researchers have proposed intrusion detection

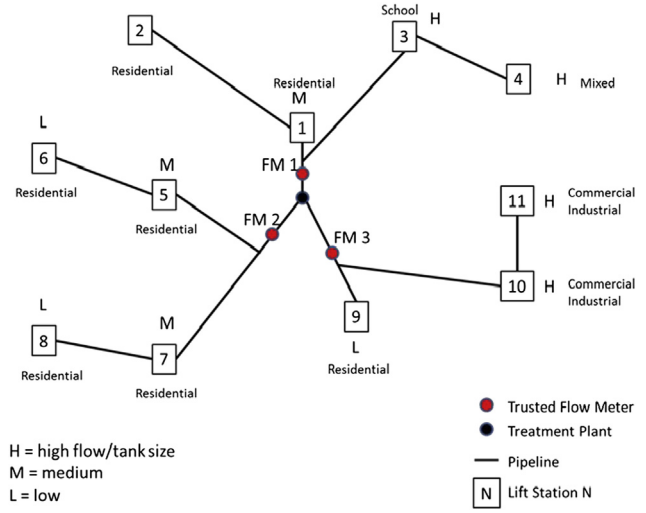


Fig. 1 – Reference wastewater facility (trust anchors placed in flow meters are in red).(For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

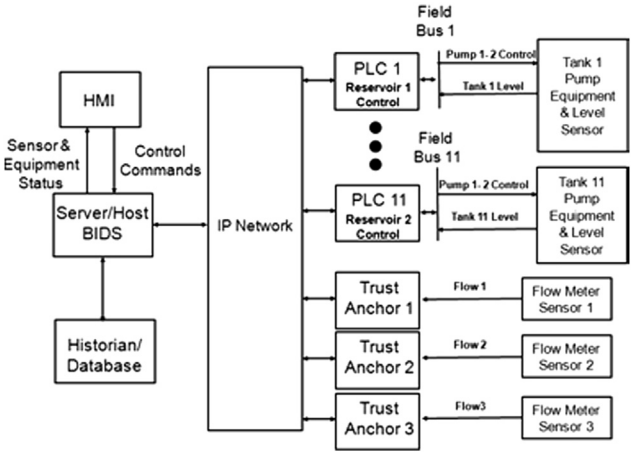


Fig. 2 – Reference wastewater facility hardware.

systems for use in industrial control environments (see, e.g., [7,9,13,18,32,34]). Typically, these intrusion detection systems are individually tailored to the systems being protected.

Approaches that improve system integrity, such as trust anchors (TAs), can be leveraged as a source of unmodified signal data. For instance, in the case of wastewater facilities, trusted flow meter data in the reference system can be used with untrusted data from PLCs (tank levels and pump control status) along with known pump characteristics, pipeline lengths and flow speeds to model the system behavior of a reference wastewater facility. One or more system models then predict system signals based on the known PLC control logic and characteristics of the physical system. In each case, failures can be detected when observed behavior deviates substantially from the estimated behavior. Crucially, detection mechanisms can identify failures caused by accident as well as by strategic attacks, often with enough lead time to mitigate widespread calamity.

2.3. *Securing a wastewater facility*

We make the discussion of available countermeasures concrete by considering how a joint deployment of trust anchors and a behavioral intrusion detection system (BIDS) might work in the representative wastewater facility presented in Fig. 1. This system is modeled after a city wastewater collection system that feeds into a single wastewater treatment facility. The system consists of eleven lift stations (indicated by square nodes in the figure), each of which relies on a PLC to control two pumps, a storage tank, and a tank-level sensor. Additionally, three flow meter sensors are available for monitoring the pipelines entering the treatment plant.

Fig. 2 shows the wastewater facility from a different perspective, using a block diagram of the hardware elements and connections. This diagram also indicates how the security countermeasures can be integrated into the system. It can be seen in the top right of the figure that each of the eleven PLCs relies on a tank-level signal from a sensor to automatically determine when to turn on and off the two pumps under its control. Rules for turning pumps on and off can vary by lift station PLC, and can be modified by the operator. Additionally, three flow meters transmit to the operator information about the flow rates to the treatment plant. The flow meters can be augmented with trust anchors to ensure that the flow rates are not manipulated.

The PLC and trust anchors transmit readings to the operator and the BIDS via the IP network. The BIDS automatically checks for anomalous readings that indicate an overflow may occur. The operator, based on either manual inspection of readings or alerts from the BIDS, can decide to override PLC commands and turn pumps on or off to react to conditions in the larger system context, or to dispatch maintenance crews if a failure is suspected. As part of normal operation, the system saves the operational status from flow meters, PLCs and operator commands in a historian database for future analysis and as input to the BIDS.

This raises a key question: how might an overflow be detected using the BIDS and trust anchors?

For instance, the pump flows from lift station 1 (LS1) and lift station 3 (LS3) combined with the flow between the lift stations and flow meter 1 (FM1) can be used to estimate the flow for comparison with the trusted FM1 measurement. If the estimated and measured flows fall within an acceptable range, then the two lift stations LM1 and LM3 and the pipelines that feed FM1are deemed to have not failed or become compromised. After this initial assessment, the flows from LS2 based on the pump status of LS 1 and LS2 can be used to estimate the level of the LS1 tank. The integrity of the pipelines and LS2 are verified if the reported level and the estimated level are acceptably close. LS4 and its pipelines to LS3 can be verified in a similar fashion. This process is repeated for the collection segments monitored by FM2 and FM3.

When the estimated signal values (flow or tank levels) deviate substantially from the reported signal values, then a blockage, pump failure, PLC failure or attack on the lift station could be to blame. The BIDS can raise an alarm and notify the operator. Furthermore, the BIDS can often determine which

component has failed. For instance, if the error in predicted flow versus measured flow is approximately equal to the output flow of a feed pump, then that pump must have failed. If instead all four pumps report similar output rates, then it can only be concluded that one of the four pumps has failed without pinpointing the exact pump that has failed. When the error is not proportional to the output of a pump, then there may be a blockage or structural failure between the lift station and the flow meter, or between lift stations.

We have verified that the BIDS is effective at detecting failures by running Matlab simulations of the reference system with three trusted flow meters. We have also verified that the BIDS can detect simulated PLC attacks and pump failures, giving us confidence that a pump failure or other medium-to-large flow problem can be detected, isolated and reported.

While the combination of the BIDS and trust anchors offers a powerful way to detect failures and cyber attacks early, the question remains whether it is economically feasible to deploy these countermeasures. The next section sets out to answer this question.

3. Empirical estimation of expected sewage overflow costs

A number of costs are incurred when a wastewater facility experiences a sewer overflow. We follow the approach of Anderson et al. [2] and divide these costs according to the direct losses experienced by the facility, indirect losses imposed on society, and defense costs that mitigate SOs. Direct losses associated with an overflow incident include cleanup costs, collateral property damage (buildings/environmental/property), regulatory fines and penalties, and adverse health impacts sustained by the victims. Additional indirect losses associated with an incident include lost business, environmental impact and distress to individuals who suffer as a result of the overflow.

Table 1 enumerates the different types of costs and assigns them to the appropriate category.

Table 1 – Cost breakdown of sewage overflows, data availability and the corresponding variable used in the model.

Cost category	Data?	Variable
Direct losses		
Cleanup costs	✓	c_{cln}
Property damage	✓	c_{dam}
Regulatory costs (e.g., fines and settlements)	✓	c_{EPA}
Lost business for victims	✗	
Victim health costs	✗	
Indirect losses		
Lost business for non-victims	✗	
Broader environmental impact	✗	
Psychological distress	✗	
Defense costs		
Integrity protection (e.g., trust anchors)	✓	c_{sec}
Incident detection (e.g., BIDS)		

In the following subsections, we present appropriate data sources in order to estimate the costs when possible. Derived data is used to calculate the expected annual cost of SOs using the following formula:

$$ALE_0 = E(n_{SO}) \times (c_{cln} + p_{dam}c_{dam} + p_{EPA}c_{EPA}) \quad (1)$$

Here $E(n_{SO})$ represents the expected number of SOs exceeding 10,000 gallons for a utility per year, which is computed in Section 3.1. For each expected overflow, we tally the cost of cleanup (c_{cln}), the expected cost of property damage ($p_{dam}c_{dam}$), and the expected cost of regulatory penalties ($p_{EPA}c_{EPA}$), which are computed in Section 3.2.

3.1. Estimating the incidence of sewage overflows

We exhaustively searched public sources in order to estimate the historical probability of cyber attacks targeting wastewater facilities. However, the search turned up only one well-publicized attack on a wastewater system [1]. The Repository for Industrial Security Incidents (RISI) [20] provides reports about additional water and wastewater system incidents between 2000 and 2009. Based on the limited publicly-available information, these incidents appear to have been triggered by a mix of software and hardware equipment failures, system failures, network failures, sabotage, and operator or maintainer errors. Notably, there is no indication that the reported incidents were actually cyber attacks on wastewater facilities [20,26]. Thus, we conclude that, although wastewater systems are vulnerable to attack, the empirical probability of a cyber attack is extremely low based on its past incidence. This is consistent with the finding that cyber attacks on SCADA systems in general have also been very rare, even if the attacks that have been executed, such as Stuxnet, have attracted significant notoriety [1,26]. The extremely low incidence of published SCADA cyber attacks in general points to a similarly low probability that wastewater facilities in particular would be targeted. Of course, the absence of attacks in the past is no guarantee that such attacks will not happen in the future, but it does mean that investments in systems that protect against attacks are unlikely to be justified on a cost-benefit basis of preventing malicious attacks alone. Therefore, we empirically examine the probability of a non-malicious sewage overflow in order to see if countermeasures that protect against malicious and accidental overflows could be economically justified.

The most reliable and comprehensive data on overflows in the United States comes from the California Water Board, which reports that 4738 SOs occurred in the state during FY 2011 [21]. However, the size of an overflow can vary greatly. Just 2% of overflow incidents – those exceeding 10,000 gallons – account for 84% of the total volume of spilled sewage. Of course, not all overflows can be prevented by early detection.

The California Water Board distinguishes between four broad categories of overflows: operational, condition, structural, and other. Operational overflows arise from acts of nature such as debris clogs, while condition failures are often caused by outdated infrastructures. These types of overflows are unlikely to be prevented by early detection. However, structural overflows, where components such as pump stations fail, are often detectable before the overflows exceed

10,000 gallons. Likewise, most failures in the "other" category are detectable, such as operator and maintenance errors.

We choose to only track the incidence of SOs exceeding 10,000 gallons. As stated above, these account for the vast bulk of overflow volume, and are therefore the best targets for prevention. California experienced 96 SOs exceeding 10,000 gallons in FY 2011, approximately 46 of which should be detectable by a system like BIDS. A 10,000 gallon SO is also a reasonable threshold for detecting failures using a device such as BIDS because sensor measurements (flow meter and tank level) have to be filtered to reduce false alarms and instantaneous measurement errors.

The approximately 16,000 sewer systems in the United States vary considerably in their size and, therefore, in their likelihood of experiencing a large overflow. Fortunately, the California Water Board reports that there are 110,593 total miles of sewer lines. This can be used to compute an estimate of the number of detectable overflows in SO exceeding 10,000 gallons using the following formula as a function of sewer line miles m:

$$n_{SO}(m) = \frac{46 \text{ detectable large SOs}}{110,593 \text{ sewer miles}} = 4.16 \times 10^{-4} \times m \quad (2)$$

We searched public records in order to determine the average number of miles of sewer mains for cities with populations over 100,000. We started with U.S. Census data from the 2010 census [27] to obtain a list of 273 cities that met the criterion. We browsed the city websites for information. Often, the cities have sewer information categorized in the water, wastewater or public works section of their websites. These sections are usually associated with departments or public utility portions of the websites. Searches were issued using the keywords of "sewer," "sewerage," "sewer mains," "sewer miles" and "wastewater treatment." Frequently, there were statistical summaries on the amount of water lines and sewer lines in miles for each city area. Some cities have outsourced all of their water distribution and treatment efforts to separate utilities. These utilities are independently-controlled entities with their own websites, and these websites often list information about the sewer mains that were serviced. We were able to access information for 135 of the 273 cities. An average of 1300 miles of sewer mains per city with a population over 100,000 was reported for these 135 cities. Using this value of 1300 miles in Eq. (2) yields $n_{SO}(1300) = 0.541 = n_{SO}$.

3.2. Estimating the cost of sewage overflows

We now review the available data regarding the various types of costs associated with sewage overflows in order to derive robust estimates. We follow the structure set out in Table 1: direct losses resulting from the overflow, including cleanup costs, property damage and regulatory fines; and indirect losses affecting others not directly impacted by the overflows.

3.2.1. Direct losses for cleanup

For spills that only require cleanup (no property damage), the best public data available is from a 2000 U.S. Environmental Protection Agency (EPA) report [8]. Based on this EPA report, the average cost of cleanup (labor and materials) was approximately $2130 per event in 2000. Adjusting for inflation from 2000–2012, the average cost per event is estimated to be $2854 [31]. However, this is not an appropriate estimate of the cleanup costs for large SOs because larger events are much more likely to cause property damage.

The California Sanitation Risk Management Association (CSRMA), a large non-profit organization that includes 40 city and regional wastewater utilities, provides credible wastewater cleanup information. According to CSRMA, the average cleanup cost is $22,554 per SO event based on 133 claims made in 2011 [5,6]. Even so, this data is also likely an underestimate because the CSRMA is a cooperative of mostly smaller wastewater districts. However, since this is the best data we have, we set $c_{cln} = \$22,554$.

3.2.2. Direct losses due to property damage

Spills that result in property damage have costs that vary widely depending on the location and the volume of the SO. The majority of all property damage claims are paid by insurance, and the remaining claims are settled in lawsuits. Many large wastewater utilities are city or county government owned entities and are self-insured. Smaller utilities either purchase insurance or join a larger pool to distribute their individual risk of a large loss.

The last category of costs is legal and non-insurance settlements. An exhaustive Internet search covering lawsuit data associated with SOs, public utility records and media reports of property damage settlements only identified nineteen claims. To find these incidents, a significant number of keyword searches on google.com and bing.com were performed and the highest 100–400 websites for each search term were reviewed for related loss data. Search terms included "sewer overflow," "wastewater overflow," "SSO," "CSO," along with "property" and "property damage." All unique instances of reported property damage settlements were used to create a database from these data sources. These incidents included damage sustained by single homes, multiple homes, an apartment complex and a business. The data is summarized in Table 2. The average cost due to legal and non-insurance settlements amounts to $1,403,345.

The next question is: how often does property damage occur? Nine of the nineteen cases with confirmed property damage were reported in 2011–2012. A lower bound on the probability of property damage is given by:

Table 2 – Non-insurance settlement costs.

Cases	Property damage estimates from non-insurance settlements			
#	Minimum	Median	Mean	Maximum
19	$11,331	$151,000	$1,403,345	$11,600,000

$$p_{\text{dam}} \leq \frac{9 \text{ SOs with damage in the U.S. in 2011–12}}{\left(\frac{46 \text{ SOs in California in 2012}}{12.1\% \text{ US population in California}}\right) \times 2 \text{ years}} = 1.18\% \quad (3)$$

Of course, this is likely a gross underestimate because a 10,000 gallon sewage spill is very likely to damage property. However, many property damage claims are settled out of court in a way that does not attract news coverage. Consequently, the true value for p_{dam} is somewhere between 1.18% and 100%. While we lack data to support it, a plausible conservative estimate for the probability of incurring property damage in a large overflow is $p_{\text{dam}} = 25\%$.

We also note that the RISI incident information provides independent cost estimates associated with six incidents. Three incidents cost less than $10,000, two incidents cost between $10,000 and $100,000, and one incident cost over $10 million [20,26]. This is fairly consistent with the data we collected.

3.2.3. *Direct losses due to regulatory fines*

The EPA levies fines on cities, municipalities and special utility districts for violations of the 1972 Clean Water Act, which includes sewage overflow incidents. In addition to federal penalties levied by the EPA, legal settlements of these violations often involve the offender agreeing to environmental enhancement projects; these are referred to as Supplemental Environmental Policy (SEP) agreements. SEP costs are typically a small fraction of the total estimated costs to comply with EPA recommendations for system upgrades. Indeed, SEPs can be thought of a way to compensate society for the harm imposed by the Clean Water Act violation.

The EPA maintains a database of Clean Water Act infractions with the associated costs for resolving violations from 2001–2012 [30]. Table 3 summarizes the penalties, SEP value and compliance costs associated with Clean Water Act violations. The table presents summary statistics from 46 of the 85 total Clean Water Act violations specifically caused by SOs. We obtained this subset by filtering the search results from the EPA database using two parameters. First, we set the Facility Characteristics SIC Code to 4952, which is the Standard Industrial Classification (SIC) code for sewerage systems. Second, we set the Case Attribute Primary Law to CWA – Clean Water Act. All the other parameters were kept at their default values. Additionally, we validated many of the EPA fines by inspecting independent legal settlement information [10,12].

The average EPA penalty assessed was $341,205 and the average SEP value was $2,546,344. We can safely assume that EPA fines would only occur in the case of large overflows exceeding 10,000 gallons. Consequently, we can estimate the probability that a large overflow receives an EPA fine as

$$p_{\text{EPA}} = \frac{46 \text{ EPA violations in the U.S. in 2000–11}}{\left(\frac{46 \text{ SOs in California in 2012}}{12.1\% \text{ U.S. population in California}}\right) \times 12 \text{ years}} = 1.01\% \quad (4)$$

3.2.4. *Indirect losses*

The primary indirect loss associated with SOs is the pollution of the environment. Businesses that are impacted by an SO may incur lost revenue due to cleanup, lost customers due to health concerns, and damaged inventory or equipment. Additionally, victims may suffer psychological distress as a result of the SO or concerns about future overflows.

Overflows often reach rivers, watersheds or the sea, causing additional environmental losses and health hazards. Lakes, rivers, beaches and fisheries can become contaminated from SOs. An SO can cause water contamination of water as described in a 2004 report to the U.S. Congress [29]; the long list of contaminants includes microbial pathogens, viruses, parasites, metals, synthetic organic chemicals, toxins and bacteria. All these indirect costs are difficult to quantify, but a small percentage of the costs are likely to be captured in the lawsuit loss and regulatory fine data provided with the direct loss data.

Finally, it is worth noting that typical home insurance policies do not normally cover sewer overflow damage. An additional rider is usually needed for such coverage at an annual cost of $40–$60 [24]. The low cost indicates that insurance companies have determined that there is a low risk for sewer overflow damages that are the homeowner's responsibility.

3.3. *Estimating defense costs*

Table 4 provides a summary of the estimates of the non-recurring costs and the annual recurring costs associated with the addition of trust anchors and BIDS hardware and software to the reference wastewater facility described in Section 2.3. The recurring expenses include trust anchor (TA) hardware, system-specific TA and BIDS software, and initial operator training.

A Matlab system simulation revealed that the minimal number of trust anchors required to support the BIDS is three (flow meters). With these three trusted flow measurements and data from the PLC controlling each lift station, the BIDS can detect a pump failure from data inconsistencies resulting from a cyber attack on the PLC.

4. Cost-benefit analysis

Having estimated the various costs associated with sewer overflows and the associated countermeasures, we are now in a position to evaluate the effectiveness of the

Table 3 – Regulatory fines and compliance costs for Clean Water Act violations arising from SOs.

46 Incidents	Regulatory fines and compliance costs			
2001–2012	Minimum	Median	Mean	Maximum
Federal penalties	$0	$122,500	$341,205	$2,200,000
SEP value	$10,800	$305,000	$2,546,344	$42,000,000
Compliance costs	$0	$72,000,000	$679,600,000	$4,700,000,000

countermeasures. We can calculate the current expected annual loss by inserting the empirically-derived estimates into Eq. (1). Upon doing this, we find that ALE_0=$217,675 for a utility managing 1300 miles of sewer lines, the average for large U.S. cities. Fig. 3 (left) plots the expected annual loss ALE_0 as a function of the number of miles of sewer pipe managed by a utility. Three lines are included in the plot for different probabilities of experiencing property damage p_{dam}. The dotted line uses the lower bound estimate of 1.18%, showing expected losses ranging from $3000 for a town with 100 miles of sewer lines to $85,000 for a city with 3000 miles of sewer lines. In contrast, for the upper bound of probability $p_{dam}=1$, a city with 3000 miles of sewer faces an expected annual loss of $1.8 million. The loss falls to $500,000 when there is only a 25% chance that an overflow causes property damage.

The benefits of security are notoriously difficult to measure. We follow the practice in the security economics literature by measuring security benefits as the amount of loss avoided [4]. The expected annual loss when investing in countermeasures is given by

$$ALE_S = (1-r) \times ALE_0 \quad (5)$$

where r represents the fraction of large overflows that can be prevented by early detection. We have no reliable data on what this rate should be because few utilities have adopted failure detection systems. However, a value of $r=0.4$ seems plausible.

Our next task is to examine the impact of varying r on the viability of countermeasures. But first, we must also include the cost of countermeasures in determining whether a countermeasure is worth adopting. To this end, we calculate the expected net benefit of security as

$$ENBIS = ALE_0 - ALE_S - c_{sec} \quad (6)$$

A standard approach in cost-benefit analysis is to identify the cost at which a countermeasure breaks even. To do that, we can set $ENBIS=0$ and solve for c_{sec}. Upon substituting from Eq. (5), the security countermeasures breakeven when $c_{sec}=r \times ALE_0$. Fig. 3 (right) plots the breakeven cost for a city with average sewer lines and a 25% chance of property damage as a function of the overflow prevention rate r. For a 40% prevention rate, the breakeven cost is just under $100,000 per year, rising linearly. Countermeasures that cost more than $200,000 require complete prevention to be economically viable for a typical utility.

But what exactly constitutes a typical utility? And how do the estimated costs of countermeasures stack up? We now examine the expected costs facing U.S. cities.

To determine the viability of adding protection measures, it is necessary to estimate the costs of adding the hardware and software to the wastewater facilities of several cities. We selected eight major U.S. cities – Atlanta, Baltimore, Los Angles, New Orleans, New York, Orlando, San Francisco and Washington DC – in order to estimate the cost of protection for a diverse range of system layouts. We compared the system layout in each city to the reference wastewater facility and scaled the protection equipment costs appropriately. The scaling was based on the number of standalone lift stations and combined lift stations/wastewater facilities (WFs) that were identified. Because SCADA systems have 20–30 year hardware replacement lifecycles, we adopted a 20-year lifecycle to calculate the total cost and average operational cost per year of the countermeasures. Of course, the

Table 4 – Cost estimates for reference system development and installation of TAs and BIDS.

Non-recurring Costs	TA HW, SW, BIDS and training	$79,095
Recurring (Annual) costs	TA HW, SW, training and key updates	$ 7850

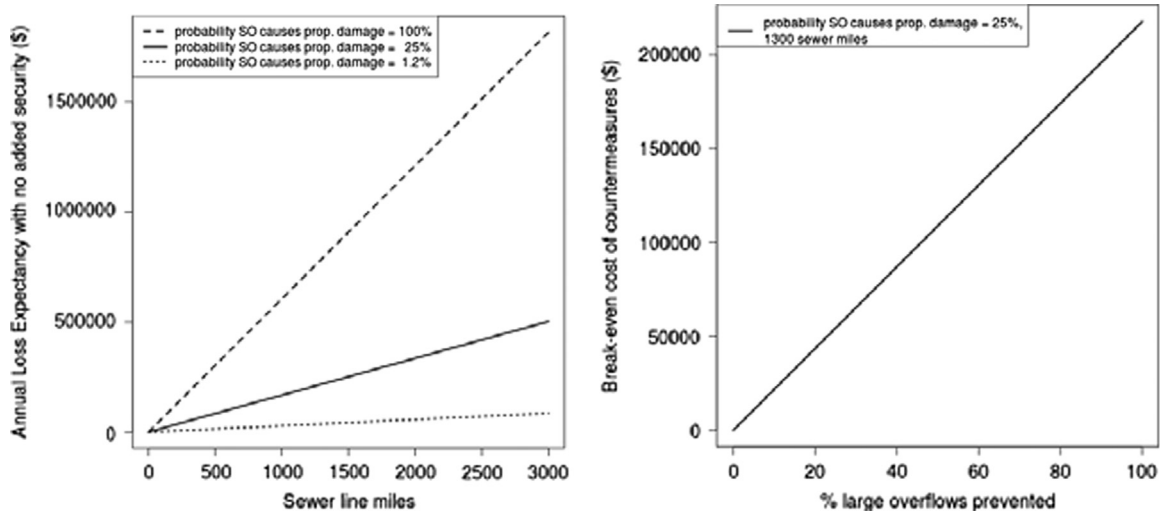


Fig. 3 – The expected loss ALE_0 for a utility expressed as a function of the length of sewer lines managed, shown for varying probabilities of experiencing property damage (left); the breakeven costs of countermeasures expressed as a function of the percentage of large overflows prevented through improved detection (right).

Table 5 – Estimated costs of countermeasures for wastewater facilities in eight cities plus the reference system shown in Fig. 1. The annual expected loss is shown for each city along with the expected net benefit of countermeasures based on a 40% risk reduction and $p_{dam} = 0.25$.

System	Pump stations	No. WFs	Lift/WF	Minimum no. TAs	Cost Fac.	Initial cost	Op. cost (20 Years)	Cost/year	Sewer miles	ALE_0	ENBIS
Reference	11	1	11	3	1	$79K	$157K	$20K	–	–	–
Atlanta	16	4	4	5	2	$158K	$314K	$39K	2125	$356K	$103K
Washington, DC	25	1	25	7	3	$237K	$471K	$59K	1800	$301K	$62K
San Francisco	56	2	28	16	6	$475K	$942K	$118K	993	$166K	($51K)
New Orleans	83	2	42	23	8	$633K	$1256K	$157K	1600	$268K	($50K)
New York	93	14	7	26	9	$712K	$1,413K	$177K	6000	$100K	$225K
Baltimore	116	1	116	32	11	$870K	$1727K	$216K	3100	$519K	($9K)
Los Angeles	154	11	14	42	14	$1107K	$2198K	$275K	6700	$1122K	$174K
Orlando	200	4	50	55	19	$1502K	$2983K	$373K	895	$150K	($314K)

true cost of upgrading facilities in these cities may vary, based on local conditions and proprietary information about the facilities. Nevertheless, the purpose of this exercise is to examine how differences in wastewater facilities, geography and city populations can lead to different cost-benefit outcomes.

Table 5 presents the results. The annual costs varied considerably, ranging from $20,000 to $373,000. The table also shows the sewer miles managed by each city. While positively correlated, some cities have far more pumping stations and lifts than the length of sewer lines would suggest. This invariably has to do with local geography and the age of the city. One consequence of this, however, is that protective countermeasures are much more economically feasible for some cities than for others. Table 5 also includes an estimate of the expected annual loss without added protection (ALE_0), which is tied to the sewer line length in each city. Finally, we can compute whether the protection mechanisms are viable using *ENBIS*. For a 40% risk reduction and 25% probability of suffering property damage, four of the cities should invest and four should not.

Fig. 4 explores the relationship between sewer miles, cost of protection and *ENBIS* using a scatter plot. Each point represents a city; points to the right indicate that the city has more sewer miles and points towards the top indicate that the city has higher protection costs. The points are scaled according to the size of the gain (or loss) from investing in protection. It is clear that the cities in the upper left quadrant fare worst, which makes sense because their costs are high but their risk of large overflows are lower. But the figure also shows that that even relatively expensive protection mechanisms can be economically viable if the risk of a large overflow is substantial, as is the case for New York and Los Angeles. Individual utilities can, of course, inspect their overflow history in order to determine if the risk of overflow is substantial enough to invest in better detection.

As mentioned above, it is not known how effective the protection mechanisms would be in preventing overflows. We can deal with this situation by measuring the viability of countermeasures for a wide range of detection rates. Because each city faces different costs and benefits, it is helpful to normalize the benefit measure. We use the standard metric called *ROSI* (return on security investment), defined as:

$$ROSI = \frac{ENBIS}{c_{sec}} = \frac{r \times ALE_0 - c_{sec}}{c_{sec}} \tag{7}$$

Table 6 plots the *ROSI* values for detection rates ranging from 10% to 100% effectiveness for each of the eight cities. Positive percentages indicate that investments in protection are worthwhile, while negative numbers suggest that the added protection costs too much compared with the reduction in risk. Note that, if the countermeasures reduce large overflows by 10%, then none of the cities would find the protection cost-effective. After 20% of the overflows are prevented, the protection becomes viable for Atlanta, Washington, DC and New Orleans. Note also that the infrastructure of Orlando is so complex for its size that even preventing all sewer overflows would not make the countermeasures cost-effective. Consequently, we can safely conclude that protection mechanisms may be reasonable for some, but never all, wastewater utilities.

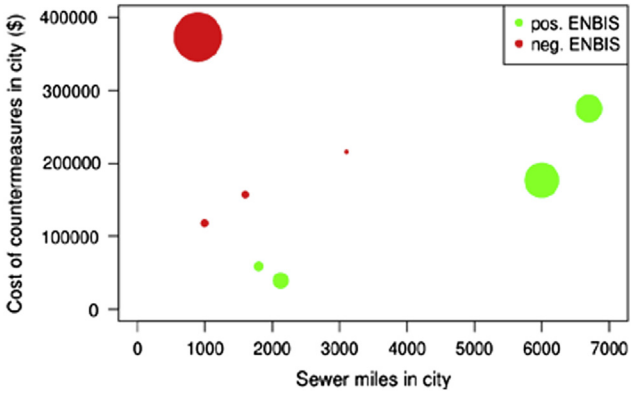


Fig. 4 – Comparison of the number of sewer miles with the costs of deploying countermeasures for the eight representative cities. The size of a point indicates the magnitude of the net benefit (or cost) of deploying countermeasures.

5. Related work

Critical infrastructures are susceptible to disruption. While failures triggered by accidents and acts of nature have long presented a challenge, during the past decade researchers and practitioners have become cognizant of the threats posed by malicious parties with regard to exploiting vulnerabilities in industrial control systems [11]. The vulnerabilities in control systems affect a broad range of industries, including electric utilities, refineries and wastewater facilities.

Researchers have proposed two main approaches to protect against threats to industrial control systems and the critical infrastructure assets they manage. The first is to improve the integrity of the systems and communications channels, ranging from less-expensive retrofits (e.g., [14,25,33]) to more comprehensive replacement solutions (e.g., trust anchors [17]). The second approach is to build systems that can detect attacks and, hopefully, stop them from succeeding, borrowing ideas from intrusion detection systems used in IP networks [7,9,18,27,32,34]. When applied to SCADA systems, intrusion detection systems can identify unauthenticated command injections, response injections and denial-of-service attacks [9]. Papa et al. [16] proposed a risk assessment methodology that determines the most vulnerable assets within a system. The results were then used to recommend the least disruptive and most cost-effective configurations of trust anchors and intrusion detection systems [19]. We have leveraged this approach in estimating the configuration required to secure wastewater facilities in the eight representative cities.

The research literature referenced above has argued that vulnerabilities in industrial control systems, once found, must be fixed. Given the reliance of society on the critical infrastructure, this is an understandable position. However, the proposed countermeasures come at substantial cost, and infrastructure owners and operators have pushed back, arguing that attacks that exploit the vulnerabilities are exceedingly rare, if they happen at all.

Table 6 – Return on security investment (ROSI) for eight cities for various percentages of overflows prevented using countermeasures. Positive numbers indicate a viable investment.

	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Atlanta	−9	81	172	262	353	443	534	624	715	805
Washington, DC	−49	2	53	104	156	207	258	309	360	411
San Francisco	−86	−72	−58	−44	−30	−15	−1	13	27	41
New Orleans	−83	−66	−49	−32	−15	2	19	36	53	70
New York	−43	14	70	127	184	241	298	354	411	468
Baltimore	−76	−52	−28	−4	20	44	68	92	116	140
Los Angeles	−59	−18	22	63	104	145	185	226	267	308
Orlando	−96	−92	−88	−84	−80	−76	−72	−68	−64	−60

Recent research in security economics [2,3,4] can shed light on this problem in two ways. First, researchers have argued that insecurity is a form of negative externality, which suggests that companies often lack an appropriate incentive to improve security [3]. In the context of our study, asset owners and operators may not wish to invest enough in protecting against insecurity when the harmful consequences of an attack are primarily borne by society. The second way in which security economics can help is in quantifying the costs of insecurity and the benefits of improved security. In Section 3, we applied the cost framework used in [2] in the context of cyber crime to estimate the costs associated with sewage overflows. We also used loss expectancy and return on security investment metrics consistent with [4].

Cost-benefit analysis has been applied in the context of combating terrorism. For example, Stewart and Mueller [22] have presented a cost-benefit analysis for securing bridges from terrorist attacks. Similar to our study, this threat has been realized very rarely if at all. But unlike wastewater systems, Stewart and Mueller could not rely on a non-malicious threat of failure to estimate probabilities. Stewart and Mueller have also examined aviation security countermeasures [23], comparing the effectiveness of different techniques. We adopt a similar approach in piecing together empirical estimates of probabilities and costs using information gleaned from public sources.

6. Conclusions

Detecting non-malicious failures could make security countermeasures economically viable for wastewater facilities. Absent improved failure detection mechanisms, we estimate that the expected annual loss due to sewer overflows exceeding 10,000 gallons is approximately $200,000 for U.S. cities with populations exceeding 100,000. The cost to a utility depends on the complexity of its wastewater facility. Some utilities will find that investing in security mechanisms that improve early detection of overflows is justified.

The current study has some limitations that should be addressed in future work. For one, the robustness of the data could be improved. We were limited by the information obtained from public resources. Notably, there is uncertainty regarding the probability that large overflows will cause property damage and the estimates for cleanup costs are likely understated. Furthermore, we chose to use average values of cost estimates, even though the distribution of losses is highly skewed. Using median values instead would have biased the estimates downward, but in the end we decided that using mean values was more appropriate given the risk aversion exhibited by many asset owners and operators. Finally, while we did not account for attacks that triggered overflows due to their historical rarity, we would like to be able to derive some measure of their expected cost, which may be substantial.

We are optimistic that the approach adopted in this paper – justifying security improvements by quantifying their ability to prevent accidents – can be applied to other critical infrastructure sectors. High value assets such as petroleum refineries and power plants are promising targets for cost-benefit analyses. The number of these facilities is more limited – 144 refineries and 6313 electrical power plants in the U.S. [28] – compared with more than 16,000 wastewater treatment facilities. The available incident data related to these assets should show higher incident rates and higher cost per incident that may justify investments that prevent failures regardless of whether they are accidental or malicious.

REFERENCES

[1] M. Abrams and J. Weiss, Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, M. Abrams and J. Weiss, Malicious Control System Cyber Security Attack Case Study: Maroochy Water Services, (www.csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf), 2008.

[2] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. van Eeten, M. Levi, T. Moore, S. Savage, Measuring the cost of cybercrime, Proceedings of the Workshop on the Economics of Information Security, 2012.

[3] R. Anderson, T. Moore, The economics of information security, Science 314 (5799) (2006) 610–613.

[4] R. Böhme, T. Nowey, Economic security metrics, in: I. Eusgeld, F. Freiling, R. Reussner (Eds.), Dependability Metrics, Springer, Heidelberg, Germany, 2008, pp. 176–187.

[5] California Sanitation Risk Management Authority, Pooled Liability Program Committee Agenda, San Francisco, California (www.csrma.org/docs/meeting-agendas/Agenda-PL-110512.pdf), 2011.

[6] California Sanitation Risk Management Authority, Member Directory, San Francisco, California (csrma.org/template/members.asp?id=366), 2012.

[7] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner and A. Valdes, Using model-based intrusion detection for SCADA networks, Proceedings of the SCADA Security Scientific Symposium, 2007, pp. 127–134.

[8] Environmental Protection Agency, Environomics, Benefits of Abating Sanitary Sewer Overflows (SSOs), U.S. , Washington, DC (archive.nacwa.org/getfile05d1.pdf?fn=ra01-4f.pdf), 2000.

[9] W. Gao, T. Morris, B. Reaves, D. Richey, On SCADA control system command and response injection and intrusion detection, Proceedings of the APWG eCrime Researchers Summit, 2010, pp. 1–9.

[10] Globe Business Publishing, Lexology, London, United Kingdom (www.lexology.com/library/MoreLikeThis.aspx?g=7183714f-d1b3-439c-bbbc-259f0c1d5074&SameJurisdiction=1), 2012.

[11] V. Igure, S. Laughter, R. Williams, Security issues in SCADA networks, Computers and Security 25 (7) (2006) 498–506.

[12] LawyersandSettlements.com, Knoxville Utilities Board, Santa Cruz, California (www.lawyersandsettlements.com/settlements/02648/sewage.html), 2012.

[13] O. Linda, T. Vollmer, M. Manic, Neural network based intrusion detection system for critical infrastructures, Proceedings of the International Joint Conference on Neural Networks, 2009, pp. 1827–1834.

[14] M. Majdalawieh, F. Parisi-Presicce, D. Wijesekera, DNPSec: Distributed Network Protocol Version 3 (DNP3) security framework, in: T. Sobh, K. Elleithy (Eds.), Advances in Computer, Information, Systems Sciences and Engineering, Springer-Verlag, Heidelberg, Germany, 2006, pp. 227–234.

[15] P. Marks, Stuxnet Analysis Finds More Holes in Critical Software, New Scientist, March 25, 2011.
[16] S. Papa, W. Casper, S. Nair, Availability-based risk analysis for SCADA embedded computer systems, Proceedings of the World Congress in Computer Science, Computer Engineering and Applied Computing, 2011, pp. 541–547.
[17] S. Papa, W. Casper, S. Nair, Placement of trust anchors in embedded computer systems, Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust, 2011, pp. 111–116.
[18] S. Papa, W. Casper, S. Nair, A transfer function based intrusion detection system for SCADA systems, Proceedings of the IEEE International Conference on Technologies for Homeland Security, 2012, pp. 93–98.
[19] S. Papa, W. Casper, S. Nair, Security fusion implementation and optimization in SCADA systems, Proceedings of the IEEE International Conference on Technologies for Homeland Security, 2012, pp. 620–625.
[20] Repository for Industrial Security Incidents, Quarterly Report on Cyber Security Incidents and Trends Affecting Industrial Control Systems (Sample Copy) (www.securityincidents.org), November 30, 2009.
[21] State Water Resources Control Board, Statewide Sanitary Sewer Overflow Reduction Program Annual Compliance Report, Fiscal Year 2011–2012, Sacramento, California (www.waterboards.ca.gov/water_issues/programs/sso/docs/compliance_report_fy1112.pdf), 2012.
[22] M. Stewart, J. Mueller, Assessing the risks, costs and benefits of counter-terrorism protective measures for infrastructure, CIP Report 10 (5) (2011) November.
[23] M. Stewart, J. Mueller, Terrorism risks and cost-benefit analysis of aviation security, Risk Analysis 33 (5) (2013) 893–908.
[24] Timeshare User's Group, Sewer overflow insurance rider cost source, Orange Park, Florida (www.tugbbs.com/forums/showthread.php?t=145439), 2005.
[25] P. Tsang, S. Smith, YASIR: A low-latency, high-integrity security retrofit for legacy SCADA systems, Proceedings of the Twenty-Third IFIP TC-11 International Information Security Conference, 2008, pp. 445–459.
[26] Z. Tudor, M. Fabro, What went wrong? A study of actual industrial cyber security incidents, presented at the Industrial Control Systems Joint Working Group Spring Conference (www.us-cert.gov/control_systems/icsjwg/presentations/spring2010/02%20-%20Zach%20Tudor.pdf), 2010.
[27] U.S. Census Bureau, People and Households, Washington, DC (www.census.gov/people), 2012.
[28] U.S. Energy Information Administration, Number and Capacity of Petroleum Refineries, Washington, DC (www.eia.gov/dnav/pet/pet_pnp_cap1_dcu_nus_a.htm), 2012.
[29] U.S. Environmental Protection Agency, Report to Congress on the Impacts and Control of CSOs and SSOs, Chapter 6, Washington, DC (www.epa.gov/npdes/pubs/csossoRTC2004_chapter06.pdf), 2004.
[30] U.S. Environmental Protection Agency, Enforcement and Compliance History Online (ECHO), Washington, DC (www.epa-echo.gov/echo/compliance_report_sep.html), 2012.
[31] U.S. Inflation Calculator (www.usinflationcalculator.com).
[32] J. Verba, M. Milvich, Idaho National Laboratory supervisory control and data acquisition intrusion detection system (SCADA IDS), Proceedings of the IEEE Conference on Technologies for Homeland Security, 2008, pp. 469–473.
[33] A. Wright, J. Kinast, J. McCarty, Low-latency cryptographic protection for SCADA communications, Proceedings of the Second International Conference on Applied Cryptography and Network Security, 2004, pp. 263–277.
[34] D. Yang, A. Usynin, J. Hines, Anomaly-based intrusion detection for SCADA systems, Proceedings of the Fifth International Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies, 2006, pp. 12–16.