Introducing layer of protection analysis for water safety risk assessments
Roland Alexander Bradshaw, George Leslie Illaszewicz and Yehoshuah Gershom Avrahamson

ABSTRACT

In pursuing their mandate of providing good and safe drinking water, water system operators and asset owners work continuously towards developing and maintaining the trust and confidence of their customers. The goal of developing and maintaining customer trust has led to an increased emphasis in the water sector to explicitly assess and manage risks. In this paper, we introduce Layers of Protection Analysis (LOPA) as an approach to assessing technical and organizational risk in the water industry. LOPA offers a robust, rational and defensible approach for assessing the adequacy of independent protection layers (IPLs), such as treatment units, standard operating procedures and incident response procedures, used to mitigate environmental and process risks in water supply systems. The strength of LOPA is not only its ability to facilitate a review of technical systems’ reliability, but also its versatility to be used for the review of organizational resilience under trying conditions and the opportunity to learn from failure. This is demonstrated in this paper with a review of more than 400 incidents affecting a large water utility serving some six million customers between 1997 and 2006.

Key words | asset management, independent protection layer, Layer of Protection Analysis, risk assessment, water

INTRODUCTION

In pursuing their mandate of providing good and safe drinking water, water system operators and asset owners work continuously towards developing and maintaining the trust and confidence of their customers. The goal of developing and maintaining customer trust has led to an increased emphasis in the water sector to explicitly assess and manage risks, particularly against a background of highly publicized water quality incidents in recent years. The provision of safe and reliable services requires a management approach that identifies and prioritizes all risks and supports decision-makers in taking the correct course of action. This need for a systematic and systemic assessment and management of public health risk has been documented in the Bonn Charter and the World Health Organization’s ‘Guidelines for Drinking Water Quality’, which introduces the concept of Drinking Water Safety Plans that are based on source-to-tap risk assessments (World Health Organization 2011).

By considering treatment process performance reliability and robustness within the overall methodology, a more complete understanding of the communal water supply, treatment and distribution assets can be obtained. This enhanced understanding can be used through the decision-making process to better identify and prioritize maintenance and optimization programs that, once implemented, will maximize the overall level of service of the water infrastructure. Qualitative risk analysis techniques can result in over- or under-protecting systems, and may run the risk of being unduly influenced by emotion or personal biases. Quantitative methods, on the other hand, can require significant resource investments.

In this paper, we introduce Layers of Protection Analysis (LOPA) as an approach to assessing technical and organizational risk in the water industry. The methodology and fundamental concepts behind LOPA offer a robust, rational and defensible method for assessing the adequacy of the mechanisms for mitigating environmental and process risks in water supply systems known as independent protection layers (IPLs). Building on process hazards analysis techniques, LOPA applies semi-quantitative measures in the evaluation of the frequency of potential incidents and the probability of corresponding failure in the IPLs. The LOPA methodology can therefore be used to identify safeguards that meet the IPL criteria of specificity, independence, dependability, and auditability, and to identify areas of concern or weaknesses. Treatment units, standard operating procedures (SOPs) and incident response procedures are all examples of IPLs.

BACKGROUND

Risk analysis and assessment techniques, developed in the water sector as a response to high profile contamination events, are widely used to aid the identification and management of hazards and their respective risks. These techniques were defined as a formal and systematic critical examination of the processes and engineering intentions of new facilities, meant to assess hazard potential of mal-operation or malfunction of individual items of equipment and the consequential effects. There are three emphases in asset risk management: to ensure that the proposed asset delivers the desired outcome in terms of its functionality; to optimize time, cost, quality, and residual risk within the project process; and to credibly and defensibly select and assure risk mitigation measures throughout asset operation.

Managing risk in the face of finite resources has long been an implicit component of asset management in the water sector. On-going demand for financial self-sufficiency and controlled pricing has created a climate where water utilities have to rigorously evaluate spending on operations and maintenance budgets, as well as capital investments, without compromising public health or their facilities’ impact on the environment. Screening out all risk to public health is unachievable, but conversely, permitting excessive levels of risk is not acceptable (Pollard et al. 2004). Thus, risk management is becoming an increasingly recognized approach to assess and prioritize levels of safety, investment and maintenance requirements.

In organizations with risk management systems, the systems are based on business processes that primarily result in some form of an asset management decision (British Standards Institution 2003). One of the key requirements of effective asset investment and maintenance decision-making is ensuring that data and processes are in alignment with strategic objectives. This decision-making process may include (Bradshaw 2008):

- setting assets’ operational objectives;
- deriving acceptability thresholds for risk and reliability that adequately define ‘system safety,’ including public health risks and occupational health and safety;
- developing dedicated risk registers to identify and define risk;
- assessing risks to prioritize capital, operations and maintenance investments;
- investigating and evaluating risk mitigation measures in terms of cost, benefit and residual risk;
- specifying safety criteria based on risk assessments;
- specifying engineering design criteria, e.g. technical reliability, materials;
- specifying data flow, monitoring and control design criteria for human-machine and machine-machine interfaces;
- designing operational processes and procedures;
- designing incident detection and response procedures; and
- defining normal and abnormal operating procedures.

In asset design, the control of public health risk and associated systems’ reliability is achieved through formulating performance specifications with an understanding of the consequences and probabilities of failure (Crossland et al. 1992; Deere et al. 2001). Specifying reliability requires the definition of a system and failure, and identification of hazards with Hazard Analysis Critical Control Points (HACCP) (Havelaar 1994; Deere & Davidson 1998, 1999a, 1999b), Hazard and Operability studies (HAZOP) (American Institute of Chemical Engineers 1992), or Failure Mode
Effect, and Criticality Analysis (FMECA) (American Institute of Chemical Engineers 1992; Strutt 2004).

Dunn (2004) defines three root causes for system failures: physical failure of equipment, failure due to human interaction, and failure within the organizational decision-making processes. Dunn (2004) proposes an asset integrity assessment process which is the meta process of risk management, environmental management, maintenance management, and safety management processes. The asset integrity assessment is a review against current standards and specifications that employs a risk matrix with defined probabilities and categories for consequences of failure to production, environment, and safety. The designed operating parameter envelope is reviewed against operating parameters, and the consequence of exceeding parameters is assessed. The routine maintenance program is assessed and compared to the risk profile from the design and operations review, but is also compared to individual needs for maintaining components (Dunn 2004).

The introduction of a socio-technical system’s perspective as described by Dunn (2004) broadens the scope for risk assessments. A methodology is required that considers a water system risks not only from a physical asset-centric perspective, but also accounting for human, information and intangible assets. Such a model provides a review of technical reliability and organizational resilience under trying conditions, as well as the opportunity to learn from failures with the objective of enhancing the safety and reliability of customer services. To this end, LOPA offers the water industry a powerful analytical tool for assessing the adequacy of IPLs used that mitigate risk.

LOPA builds upon process hazards analysis techniques, applying semi-quantitative measures to the evaluation of the frequency of potential incidents and the probability of failure of the IPLs. Originally developed within the process industry, LOPA provides a methodology that can be used to identify safeguards that meet the IPL criteria across physical, human, information and intangible assets. In the process industry, LOPA has been utilized to identify and develop appropriate safety integrity level (SIL) as per the requirements of safety standards such as IEC 61508, IEC 61511, or ANSI/ISA 84.00.01-2004. Treatment units, SOPs and incident response procedures can all be considered IPLs, as long as the following criteria are met.

- **Specificity** – An IPL is capable of detecting and preventing or mitigating the consequences of specified, potentially hazardous event(s), such as a runaway reaction, loss of containment, or an explosion.
- **Independence** – An IPL is independent of all the other protection layers associated with the identified potentially hazardous event. Independence requires that the performance of one IPL is not affected by the failure of another IPL or by the conditions that caused that IPL to fail. Most importantly, the IPL is independent of the initiating cause.
- **Dependability** – The protection provided by an IPL reduces the identified risk by a known and explicit amount.
- **Auditability** – An IPL is designed to permit regular periodic validation of the protective function.

Qualitative risk analysis techniques can result in over- or under-protecting systems, and may run the risk of being unduly influenced by emotion or personal biases. Quantitative methods, on the other hand, can require significant resource investments.

**METHODOLOGY**

The research preceding this paper consisted of a retrospective review of a series of incidents (419) that occurred between 1997 and 2006 in a large water utility considered representative of typical utilities (Bradshaw 2008). The characteristics of the water utility are representative of water utilities in terms of common processes and practices and the regulatory framework in which it operates. The review of the data set has also shown that it is representative of anticipated incidents relative to many other water utilities operating under the same regulatory framework.

The 419 incidents that occurred between 1997 and 2006 were investigated to understand their cause and effect relationships. A breakdown of the primary incident causes and primary incident effects over the 10-year period is presented for all 419 incidents in Table 1, verifying that the incidents are representative of expected events. The causes and effects are presented in descending order of occurrence. The most significant or primary cause and effect was extracted from the incident
narratives for each analyzed incident. The LOPA methodology is specifically investigated under ‘trying conditions’ and the effects of IPL principles as a means of generating organizational resilience during incident situations are carefully studied.

A more detailed analysis of 145 incidents that occurred between 2004 and 2006 was also conducted to understand the impacts incidents had on customers. The aim of this review was to understand how the organization responded and functioned during these incidents and to investigate how the organization coped under trying conditions. In the previous study, the following organizational attributes were considered important features of a reliable organization:

- a strong organizational culture of reliability;
- staff competencies via continuous learning and intensive training;
- effective and varied patterns of communication;
- adaptable decision-making dynamics and flexible organizational structures; and
- system and human redundancy (Bradshaw et al. 2006).

### Table 1 | Primary incident causes in the Regional Water Utility between 1997 and 2006

<table>
<thead>
<tr>
<th>Primary incident cause</th>
<th>10 year count</th>
<th>in %</th>
<th>Primary incident effect</th>
<th>10 year count</th>
<th>in %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst main</td>
<td>133</td>
<td>31.7%</td>
<td>Interruption to supply</td>
<td>120</td>
<td>28.6%</td>
</tr>
<tr>
<td>IT failure</td>
<td>47</td>
<td>11.2%</td>
<td>Discoloration</td>
<td>115</td>
<td>27.4%</td>
</tr>
<tr>
<td>Maintenance work</td>
<td>45</td>
<td>10.7%</td>
<td>Loss of monitoring and control</td>
<td>42</td>
<td>10.0%</td>
</tr>
<tr>
<td>Asset failure</td>
<td>41</td>
<td>9.8%</td>
<td>Potential biological pathogens present</td>
<td>24</td>
<td>5.7%</td>
</tr>
<tr>
<td>Power failure</td>
<td>25</td>
<td>6.0%</td>
<td>Chemicals present above guidelines</td>
<td>23</td>
<td>5.5%</td>
</tr>
<tr>
<td>Operational intervention</td>
<td>23</td>
<td>5.5%</td>
<td>Biological pathogens present, health effects envisaged</td>
<td>18</td>
<td>4.3%</td>
</tr>
<tr>
<td>3rd party</td>
<td>19</td>
<td>4.5%</td>
<td>Potential biological pathogens present, health effects envisaged</td>
<td>13</td>
<td>3.1%</td>
</tr>
<tr>
<td>Chlorination failure</td>
<td>18</td>
<td>4.3%</td>
<td>Biological pathogens present</td>
<td>12</td>
<td>2.9%</td>
</tr>
<tr>
<td>Asset contamination</td>
<td>15</td>
<td>3.6%</td>
<td>Empty service reservoir</td>
<td>11</td>
<td>2.6%</td>
</tr>
<tr>
<td>Unknown</td>
<td>13</td>
<td>3.1%</td>
<td>Loss of asset</td>
<td>8</td>
<td>1.9%</td>
</tr>
<tr>
<td>Treatment failure</td>
<td>12</td>
<td>2.9%</td>
<td>Damage to asset</td>
<td>5</td>
<td>1.2%</td>
</tr>
<tr>
<td>Raw water quality</td>
<td>8</td>
<td>1.9%</td>
<td>3rd party impact (gas)</td>
<td>4</td>
<td>1.0%</td>
</tr>
<tr>
<td>Asset damage</td>
<td>4</td>
<td>1.0%</td>
<td>Aesthetics above guidelines</td>
<td>4</td>
<td>1.0%</td>
</tr>
<tr>
<td>Monitoring and control failure</td>
<td>3</td>
<td>0.7%</td>
<td>Environmental</td>
<td>4</td>
<td>1.0%</td>
</tr>
<tr>
<td>Severe weather</td>
<td>3</td>
<td>0.7%</td>
<td>Chemicals present above guidelines, health effects envisaged</td>
<td>3</td>
<td>0.7%</td>
</tr>
<tr>
<td>High demand</td>
<td>2</td>
<td>0.5%</td>
<td>Low pressure</td>
<td>3</td>
<td>0.7%</td>
</tr>
<tr>
<td>Security</td>
<td>2</td>
<td>0.5%</td>
<td>3rd party damage</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>Adverse weather</td>
<td>1</td>
<td>0.2%</td>
<td>Disruption to normal processing of work</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>Chemical spillage</td>
<td>1</td>
<td>0.2%</td>
<td>Risk of cross contamination</td>
<td>2</td>
<td>0.5%</td>
</tr>
<tr>
<td>Chemical supply contamination</td>
<td>1</td>
<td>0.2%</td>
<td>3rd party accident</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Design failure</td>
<td>1</td>
<td>0.2%</td>
<td>Human safety</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Illegal connection</td>
<td>1</td>
<td>0.2%</td>
<td>Statutory monitoring failure</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Telemetry failure</td>
<td>1</td>
<td>0.2%</td>
<td>Supply of unchlorinated water</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Water quality</td>
<td>1</td>
<td>0.2%</td>
<td>Treatment failure</td>
<td>1</td>
<td>0.2%</td>
</tr>
<tr>
<td>Total</td>
<td>419</td>
<td>100.00%</td>
<td>Total</td>
<td>419</td>
<td>100.00%</td>
</tr>
</tbody>
</table>
In this study, the previous incidents were further reviewed using the following protocol:

1. Record all reference documentation, including hazards analysis documentation.
2. Document the process deviation and hazard scenario.
3. Identify all initiating causes for the process deviation and determine the frequency of each initiating cause.
4. Determine the consequence of the hazard scenario. This evaluation should include an examination of health and safety, environmental, and economic losses. The economic risk should be assessed to ensure that loss prevention goals are met. With an understanding of the frequency and consequence of the potential hazardous event, a risk matrix is used to determine whether the risk is acceptable or whether IPLs are required for further risk reduction. The risk matrix is developed, as part of the LOPA procedure, using risk criteria that provide consistency to the assessment of risk.
5. Evaluate the effectiveness of IPL in terms of independence, specificity, dependability, and auditability requirements.

Every incident was documented using the HACCP methodology from catchment to tap (Havelaar 1994), failure mode effect analysis (FMEA) to describe the cause and effect relationship of the incident and LOPA to characterize the technical and organizational IPL. The findings of this review were further analyzed using standard statistical procedures and validated with staff interviews.

RESULTS

Technical reliability

Based on the detailed analysis of 145 incidents between 2004 and 2006, a total of 170 incident impacts were recorded. Out of the 145 incidents, 59 (or 41%) resulted in a ‘loss of supply’ to customers. Out of the 145 incidents, the majority (107 or 74%) were recorded to have a no impact or only one impact category affecting customers indicating a generally successful provision of service. Regarding incidents with two or more impacts on customers, 10% of the 145 incidents caused a ‘loss of supply’ to customers followed by aesthetic problems – mainly due to discoloration – on resuming normal operations. In 6% of the incidents, potential pathogens were present in the drinking water in combination with chemical parameters exceeding guidelines. In 5% of the incidents, a ‘loss of supply’ for customers was recorded. These incidents should be examined in light of organizational goals to determine whether they represent an acceptable number of occurrences.

The majority of incidents (44%) were identified by customers reporting an unusual observation relating to their drinking water supply. The majority of customer contacts referred to ‘loss of supply’ and ‘aesthetic problems’ due to discoloration. Some incidents (6%) were identified by water quality laboratories confirming the presence of pollution or contamination in the drinking water. With a turnaround time of 24 hours for bacteriological tests, it is assumed that contaminated water has passed beyond the customer tap prior to the release of laboratory results. The majority of incident notifications therefore indicate that customers were exposed to incidents before reactive incident mitigation was carried out by the incident management team, suggesting a weakness in the system that warrants further consideration. Both methods of incident identification were established processes; in particular for ‘customer contact’, a dedicated call center is maintained to identify and characterize the symptoms of an incident.

Organizational reliability

A strong organizational culture of reliability is a necessary bulwark against the failures that instigate catastrophic consequences. It was observed that staff engaged in operations and incident management have a strong sense of the primary mission of the organization. Operations managers, engineers and operators share a common system of beliefs and perceptions when water safety is concerned. Failure scenarios are usually well understood and reflected in the monitoring program of water system assets. Past incidents are analyzed and failure prediction of future incidents is facilitated by anticipatory risk assessments.

Constant vigilance and concern for water safety and reliability dictates the behavior of staff. This is particularly relevant to field operators, but also to control room staff who acted with alertness, attentiveness and care in
monitoring the healthy operation of the water supply system. Employees are encouraged to take responsibility, particularly where problems are identified and immediate corrective action programs are required. With the introduction of information technology and an automated monitoring and control system, the majority of asset failures are identified by monitoring equipment and an alarm is raised. One major exception is the identification of water main bursts and water discoloration arising in the distribution network. Here, the organization relies on customers to report their service experience. An organization must be extremely responsive in such circumstances, where customers have been inconvenienced and allowed to learn that they are the only practical means to monitor such failures. Anything less than a rapid response will undermine customer confidence in the organization and their ability to provide safe and reliable services.

Staff competency

The review of incidents revealed that staff generally managed incidents and restored the system to safe operation with competence. Staff training is extensive and focuses on the requirements for maintaining a safe system. Operators are required to gain professional accreditation in the form of college certificates as a license to operate a water supply system. This training scheme is a customized training program for operators in that particular region. Training and certification are vitally important, but the content of that training is critical, including raising awareness of the substantial public health responsibility carried by operational personnel. In-house training and training on the job are also important components.

The performance of each task is evaluated with respect to formal rules, generalized guidelines and standardized frameworks. These are expressed in SOPs, risk assessments and method statements. The emphasis is on identifying potential sources of failure and preventative actions.

The communication of incidents to staff helps the organization to communicate the failure vulnerability of the system to relevant personnel. The water utility also learns by studying the failures, near failure and mistakes. Failures in one part of the organization can be used as a means of studying the failure susceptibility of the organization as a whole. Incident review meetings are designed to highlight and prompt cross-organizational learning in other parts of the business. The majority of incidents have occurred as a result of main bursts. There are many contributing factors for main bursts such as age, material, soil condition, installation and the operating regime. The structured collection and analysis of water mains failures provides data for multi-regression analyses and the derivation of risk profiles for the entire water distribution network. There is considerable merit to base failure analysis initially on frequent and tangible failures; however, there is also a need to build on this analytical base to predict more infrequent and subtle failures that possess greater disaster potential.

Effective and varied patterns of communication

Effective communication allows a complex system to become more understandable, predictable and controllable. Organizations with strongly developed IPLs create information-rich environments. In the organization, monitoring and control is increasingly performed with ‘Process Logic Controls’ and ‘Supervisory Control and Data Acquisition’ in remote control centers. These control centers are the hub for managing the system. In the first years of implementing the strategy of advanced monitoring and control, an increase of incidents was observed due to the failure of the underlying technologies. When monitoring and control equipment fails, the status of a system becomes unknown. Technological developments, such as status monitoring for control and monitoring equipment, have gradually reduced these incidents.

During an incident, inter-personnel communication is designed to be both bottom-up and top-down in order to ensure the rapid flow of information through the hierarchy of the incident management team. Rapid dissemination of information helps the organization respond to an incident with corrective action, thus preventing the escalation of the incident into an emergency. Of the management responses documented in the incident records, 72.4% were characterized by ‘effective communication’. Here, observations, decisions and water supply system performance were effectively communicated to all relevant staff and external bodies. In 6.9% of the incidents, the incident documentation identified aspects of excellent communication
that significantly contributed to the effectiveness of the incident management response. In 13.1% of the incidents, some areas of improvements were identified which meant that the incident was unnecessarily prolonged. In 6.2% of the incidents, ‘poor communication’ had a significant adverse impact on the overall performance of the incident management response.

Adaptable decision-making dynamics and flexible organizational structures

The incident documentation was studied to identify the ability of the organization to adapt its organizational structure to respond to the needs arising during an incident. It was found that in 88.3% of the incidents, the organization assumed an effective organizational structure to place it in the best possible position to effectively reduce the incident impact on customers and reinstate normal operations. In 9.7% of the incidents, the assumed organizational structure was deemed ‘adequate considering the circumstances’. In only 2.1% of the incidents was the incident management organization rated as ‘inflexible’. This suggests that the organizational structure assumed during the incident was inadequate to manage the complexity of the incident situation.

The incident assessment also focused on decision-making during incidents. It was found that 64.8% of the incident management efforts could be characterized as ‘good decision-making’. The decision taken during the incident significantly and pro-actively contributed to reducing the impact on customers and re-instate normal operations as soon as possible. In 24.8% of the incidents, the decision-making was ‘responsive to needs’ meaning that the incident management efforts pursued an effective course of action by reasonably practical means. The remainder of the incidents were, in hindsight, characteristic of poor judgment, poor decision-making, and were non-adaptive to the incident situation. These responses were identified as being ineffective to return the incident situation to normal operation, and provided an opportunity to learn lessons for enhancing the incident management response.

Overall, the organization demonstrated that decision-making under trying conditions effectively draws the necessary and correct conclusions from the data presented to the incident management team during an incident. This suggests that the quality of the decisions made is a reflection of the data availability during an incident, but also on the competence of the decision-makers involved during an incident. In 10.4% of the incidents, scope for improvements in data availability and/or competence in decision-making was identified. This aspect of personnel interaction clearly warrants dedicated attention.

System and human redundancy

The entire water supply system depends on duty standby systems or excess capacity to isolate failed assets and compensate for their loss. The use of systems’ redundancy was investigated as part of the incident management response. We define systems’ redundancy as any means of water supply capability capable of diversion to compensate for failed assets or installations. This definition considers systems’ redundancy to originate from fixed installations, but excludes bottled water and delivery via water tankers.

In 55.2% of the incidents, no systems’ redundancy was available to reduce the impact or avoid customer impact. In the majority of these incidents, the water utility resorted to the supply of bottled water. In 22.1% of the incidents, the use of systems’ redundancy did not avoid customer impact although it had a reducing effect. In 15.9% of the incidents, the use of systems’ redundancy significantly reduced the impact of incidents on customers and avoided the impact for a much larger customer base. Combined, this suggests that over 95% of incidents show the system redundancy successfully mitigating or reducing the impact on customers. In only 6.2% of the incidents, systems’ redundancy was available and used but had a low effect on reducing the incident impact.

Designing redundancy for a system can be counterproductive, as back-up functions can increase technical complexity, conceal errors and discourage individuals from performing their specified tasks (Sagan 1994). Although we did not find significant evidence of this, we believe that there is a potential for maintenance decisions to be deferred due to multiple technical redundancies; that is, duty standby systems have a significantly reduced probability of failure that may lead to an assessment of low risk and low priority in maintenance spending.
Human resource management practices that support reliability

In recruitment and selection, organizations with strongly developed IPLs select suitable and skilled candidates aiming to match, as closely as possible, the complexity of the environment with appropriate skills and competencies. An incident manager has to be able to cope with highly uncertain situations and demonstrate rational decision-making under trying conditions. The incident manager has to be able to communicate effectively with the staff and stakeholders involved in incidents. They also require a good understanding of the entire water supply system, whilst drawing on expert knowledge of the incident management team. On the other hand, an asset engineer requires a very different skill set. The asset engineer requires analytical skills and competencies in assessing technical systems' overall, as well as the technical means to provide and maintain safe and reliable drinking water within a system. Their job role is to be less reactive to incidents, but rather pro-active in assessing potential sources of failure. Increasingly, the asset engineer has to consider technical systems' risks communicated through a systemic risk assessment to the custodians of the risk management process. The asset engineer requires good communication skills, in particular to communicate with operators and operations management.

DISCUSSION

The aim of this review was to further understand how the organization responds and functions during incidents and under trying conditions. As such, the following organizational attributes were considered to be IPLs as defined in procedures for the analysis of layered protection:

- a strong organizational culture of reliability;
- staff competencies via targeted recruitment and selection, continuous learning, and intensive training;
- effective and varied patterns of communication;
- adaptable decision-making dynamics and flexible organizational structures; and
- system and human redundancy (Bradshaw et al. 2006).

All of these dimensions have been observed to contribute to the effective management of water safety and reliability of this particular organization. It was found that each dimension is important individually, but it is when acting together as a coherent configuration that incidents are effectively managed and future risks can be sufficiently understood and planned for.

We characterize and analyze each IPL in turn. With respect to IPL specificity, it was found that the organizational characteristics provide the capability to detect and prevent or mitigate the consequences of specified, potentially hazardous events. The organizational characteristics are integrated into a culture of organizational reliability. They can operate independently of all the other IPLs associated with the identified potentially hazardous event; therefore, the failure of one IPL does not affect other IPLs. The protection provided by the organizational characteristics significantly reduces the identified risk by a known and explicit amount. Lastly, the IPL is designed to permit regular periodic validation of the protective function.

As illustrated in this case study, LOPA offers the ability to assess the performance and adequacy of utility IPLs. As a result of the dependability and auditability characteristics of IPLs, the examination of historical performance should also correlate with the expected future behavior of the IPL under distress. This may permit utilities to identify weaknesses that can be proactively addressed, rather than remaining unaware of system threats that may damage the utility’s reputation or result in damages, injuries, illnesses or fatalities.

While LOPA permits utilities to assess their IPLs at their facilities, and with respect to the performance of their employees, its application is more limited within the distribution system infrastructure. Due to the size and inaccessibility of distribution system assets, as well as the complexities intrinsic in the mixed materials, ages, and sizes of pipes, there are fewer practical preventative IPLs that can be implemented beyond the mitigating IPLs discussed. This represents a clear limitation of LOPA in addressing system risks.

Irrespective, the methodology and fundamental concepts behind LOPA offer a robust, rational and defensible approach for assessing the adequacy of IPLs, such as
treatment units, SOPs and incident response procedures, used to mitigate environmental and process risks in water supply systems. Hence, the strength of LOPA is not only its ability to facilitate a review of technical systems’ reliability, but also its versatility to be used for the review of organizational resilience under trying conditions and the opportunity to learn from failure. As a result, LOPA ultimately enhances systems’ safety and reliability.

CONCLUSION

In this paper, Layer of Protection Analysis is introduced as a risk analysis and assessment instrument within water utilities. A data set of over 400 incidents that occurred in a large representative water utility between 1997 and 2006 was used to investigate organizational and technical barriers (IPLs) for their effectiveness to inhibit incident propagation.

The analysis of incidents for the utility suggests that IPL characteristics significantly contribute to reducing the public health impact of incidents. The utility has evolved its organizational and incident management structure to handle customer impacts as effectively and expeditiously as is practically possible. The regional water utility values clear objectives, ensures that they are well understood within the organization and by its partners, and has invested in its staff to ensure that people are performing the right roles and the right skills to work effectively.

REFERENCES


Deere, D. & Davidson, A. 1998 Safe drinking water: are food guidelines the answer? Water 11/12, 21–24.


Strutt, J. E. 2004 Reliability Data and Sources. Lectures in Risk Management for Water and Wastewater Engineers. Cranfield University, Cranfield, UK.


First received 19 March 2012; accepted in revised form 21 October 2012