



Morley

Advancing the Culture of Security and Preparedness in the Water Sector

The water sector is typically very adaptable and responsive to marketplace gaps that require a common baseline, including such issues as treatment chemicals, tanks, pipes, and appurtenances. In fact, since the founding of AWWA in 1881, it has developed 196 consensus standards and 52 manuals of practice that establish a common baseline for utility management and operations to promote clean, safe water. As noted in

AWWA’s original constitution, the organization’s mission covers “the exchange of information pertaining to the management of waterworks, for the mutual advancement of consumers and water companies, and for the purpose of securing economy and uniformity in the operations of water-works.” These self-organizing efforts by the water sector to address marketplace gaps predate all public health laws and regulations in the United States associated with water.

Initiatives that support the security and resiliency of the water sector are a continuation of AWWA’s charter and mission. In fact, the water sector has become a model for other critical infrastructure sectors seeking to integrate security and resilience principles. It is the only one of the 18 critical infrastructure and key resource (CIKR) sectors, as defined by the Department of Homeland Security (DHS), that has voluntarily completed two rounds of reporting on metrics

FIGURE 1 The seven-step RAMCAP process



RAMCAP—risk analysis and management for critical asset protection

associated with its sector-specific plan. The water sector has also strongly embraced the water/wastewater agency response network (WARN) model for providing mutual aid and assistance (to be addressed in a future column) and has collaborated with the DHS to develop the “Roadmap to Secure Control Systems in the Water Sector.” More recently the sector has developed two voluntary, consensus-based standards to further support utilities in becoming more secure and resilient, specifically ANSI/AWWA G430: Security Practices for Operations and Management and ANSI/ASME-ITI/AWWA J-100: Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems.

Standard G430 defines the minimum requirements for a protective security program at drinking water or wastewater utilities and promotes the protection of employee safety, public health, public safety, and public confidence. This is one of the Utility Management G-Series standards that are designed to cover the principal activities of a typical water and/or wastewater utility. This standard is intended to apply to all water or wastewater utilities, regardless of size, location, ownership, or regulatory status. G430 builds on the long-standing practice among utilities of using a multiple-barrier approach for the protection of public health and safety. The requirements of the standard are designed to support a protective utility-specific security program that will result in consistent and measurable outcomes (McLaughlin, 2010). One key requirement of G430 is the updating of vulnerability assessments to address any changes that have occurred.

Standard J100 was developed by ASME Innovative Technologies Institute LLC (ASME-ITI) and AWWA to provide a consistent and technically sound methodology to identify, analyze, quantify, and communicate the risks of specific malevolent attacks and natural hazards against water and wastewater systems. J100 provides a significant update to the methodologies applied in response to the requirements of the 2002 Bioterrorism Act by establishing an all-hazards risk and resilience assessment and management process. This standard also supports decision-making for prioritizing resources to reduce risk and enhance resilience.

“With the publication of this national voluntary standard, we close an intense effort of idea distillation and definition and begin a period of growth and refinement,” said Dave Binning, chair of the J100 committee. “Now the real work begins. I believe that an important result of this standard will be to provide a common language and framework which the water sector—operators, associations, consultants, tool developers, and regulators—can use to measure risk and resilience for systems that may face natural or targeted incidents. I hope this standard will help develop more quantifiable information that is essential in the development of affordable, secure and resilient water and wastewater systems,” he concluded.

RAMCAP Overview. RAMCAP is a process for analyzing and managing the risks associated with naturally occurring hazards and malevolent attacks against critical infrastructure. When applied to the water sector, it provides a consistent, efficient, and technically sound methodology to identify, analyze, quantify, and communicate the level of risk and resilience (i.e., the ability to withstand disruption or to quickly return to an acceptable level of service after an interruption) and the benefits of risk reduction and resilience enhancement. Because of the rigor and consistency in estimating risks, resilience, and benefits quantitatively, the results of the evaluation can also be compared across the water sector and between critical infrastructure sectors.

The RAMCAP process is composed of seven interrelated analytic steps (Figure 1). There are three key upgrades in RAMCAP that differentiate it from earlier methodologies used by the water sector. These are as follows:

1. RAMCAP provides guidance for calculating the probability of attack (or P_A in the RAM-WTM [Risk Assessment Methodology for Water UtilitiesTM] equation).
2. RAMCAP provides guidance for calculating the probability of a specific natural hazard occurring at a given utility (e.g., earthquake, tornado, hurricane).
3. RAMCAP provides guidance for calculating both asset and utility resilience.

Probability of attack. In a RAMCAP analysis, specific reference threat scenarios are provided, or the utility may also apply other threats given unique local conditions

or circumstances. Previously, utilities lacked any credible justification for using a P_A value other than 1 for malevolent attacks such as terrorism. As a result, the findings of early risk assessment were heavily biased toward countermeasures aimed at thwarting acts of physical intrusion/destruction. RAMCAP provides a reasoned approach to estimating the probability of a malevolent incident so that the probability of malevolent attack in the risk equation is calculated to be less than 1 but more than 0 (because such acts cannot be ruled out completely). The method allows for this greater granularity by separating utilities based on community size and facility type.

Natural hazards. Another key component of RAMCAP is that it balances the threat from malevolent attacks with the threat from natural hazards. The water sector clearly has ample data with which to estimate the probability of various natural disasters at specific geographic locations in the United States, and the risk equation can now reflect that physical barriers (guns, gates, and guards) cannot protect against these hazards. An all-hazards risk management approach is necessary—and in the long term more sustainable—because most actions taken to prepare for natural hazards assist in responding to most malevolent incidents as well.

Resilience. Also missing from the earlier risk assessments as a characterization of resilience, i.e., the ability of an asset or system to withstand an attack or natural hazard without an interruption to the performance of its function, or, if the function is interrupted, to restore the function rapidly. At the asset level, this is driven by time or

severity of service outage that translates into lost revenue. However, the standard also includes a utility-resilience index that provides a macro-level assessment of the utility's resilience and therefore is also an indicator of the utility's preparedness needs.

Standard J100 received final recognition from ANSI May 4, 2010, and will have an effective date of July 1, 2010. AWWA and ASME-ITI are in the process of developing a training course that will provide implementation guidance to utilities and practitioners. The course is expected to be available in mid-July, and those completing it will receive both continuing education units and a certificate of proficiency in Standard J100.

These standards and related efforts reflect the commitment and stewardship of the water sector to ensure that a vital element of the nation's economy (Hoover, 1941) is secure and resilient as it integrates the realities of a post-9/11 and Hurricane Katrina world into its culture.

—Kevin M. Morley is AWWA's security and preparedness manager, 1300 Eye St. NW, Ste. 701 W, Washington, DC 20005-3314. Morley can be reached at kmorley@awwa.org.

REFERENCES

- Hoover, J.E., 1941. Water Supply Facilities and National Defense. *Jour. AWWA*, 33:1861.
- McLaughlin, J., 2010. Going "All In" on All Hazards. *Jour. AWWA*, 102:1:33.
- WSCCCSWG (Water Sector Coordinating Council Cyber Security Working Group) Roadmap to Secure Control Systems in the Water Sector. AWWA and US Department of Homeland Security, Denver. www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf (accessed May 2010).