Resilience for Smart Water Systems

Dayton Marchese, P.E., A.M.ASCE

Water Resources Engineer, Dept. of Research and Development, OptiRTC, Inc., 356 Boylston St., Boston, MA 02116; formerly, Research Environmental Engineer, US Army Engineer Research and Development Center, 696 Virginia Rd., Concord, MA 01742.

Andrew Jin

Engineering Intern, Environmental Laboratory, US Army Engineer Research and Development Center, 696 Virginia Rd., Concord, MA 01742.

Cate Fox-Lent

Research Civil Engineer, Environmental Laboratory, US Army Engineer Research and Development Center, 696 Virginia Rd., Concord, MA 01742.

Igor Linkov, Ph.D.

Risk and Decision Science Lead, Environmental Laboratory, US Army Engineer Research and Development Center, 696 Virginia Rd., Concord, MA 01742 (corresponding author). Email: igor.linkov@usace.army.mil

https://doi.org/10.1061/(ASCE)WR.1943-5452.0001130

Introduction

As the adoption of smart water systems increases, so does the importance of building resilience in these critical systems. Smart systems are often optimized to increase efficiency of water infrastructure and reduce costs, while resilience is required to enhance the system's ability to recover from disruptions and usually requires additional investment. Thus, there is an inherent tradeoff between resilience and efficiency that needs to be reconciled for development of efficient and resilient water infrastructure. This paper utilizes a resilience assessment framework (Linkov et al. 2013a) to identify and organize the various functions of smart water systems that improve resilience. First, an implementation of the resilience matrix framework is demonstrated for baseline water systems, exemplifying what has been done with traditional technologies to increase resilience in the water sector. Second, new vulnerabilities that are introduced as a result of implementing smart technology in water systems are discussed. Specifically, the new vulnerabilities of smart water infrastructure are primarily related to cyberattack. Finally, a representative subset of smart water technologies are organized using the resilience matrix framework, describing their functions with respect to system resilience. The resilience matrix framework can be used to identify ways in which smart water systems can improve performance in one area but introduce new weaknesses in another, thus impacting overall resilience.

Background

Smart Water Systems

Municipalities looking to become smart cities in an effort to enhance efficiency, sustainability, and resilience are increasingly turning to their water distribution utilities and stormwater management services for such opportunities. Smart water systems fall into the broader category of cyberphysical systems, which incorporate physical and software components to autonomously or semiautonomously perform the functions of data collection, systems controls, and adaptive decision making. These smart water systems utilize emerging technologies to provide adaptive and integrated water management (Hill et al. 2014). Many technologies may be included in smart water systems, such as sensors to detect blockages, leaks, or contaminants, software-enabled actuated valves to rapidly redirect water, and near real-time meters to better understand use and demand (Kerkez et al. 2016). The greater information provided by smart water systems can lead to better policies and operations to improve sustainability and efficiency of delivery. Additionally, smart technologies that provide real-time water quantity and quality monitoring and adaptive control of water storage and flows can improve resilience by enhancing recovery and preventing small disruptions from cascading into disasters (Mahmoud et al. 2018).

Vulnerabilities of Interdependent Infrastructure

Although smart technology improves resilience to many disruptions, rapid adoption of advanced technology without careful consideration for how it is implemented can introduce new vulnerabilities. The digital transmission of data from sensors to command systems to actuated controls, whether in isolated or wireless networks, can be intentionally exploited by malicious actors or malfunctions may go unnoticed until an emergency. Increasingly, digital connectivity of municipal water systems not only allows utilities to provide cost-effective drinking water and sanitary services to communities (NAIC 2010), it also supports other interconnected services such as energy, healthcare, and heating and cooling. Even when these other systems can function without clean, treated water, in the United States we have not built out a separate gray water network and so major interruptions to the delivery of potable water will often reduce performance of these other systems as well. Hence, the functionality provided by water infrastructure can have far-reaching implications on a community, state, and national level in that a major disruption to a water system could quickly spillover and reduce the efficiency of other services (NAIC 2016). In a similar way, water treatment and delivery systems are large consumers of electricity at the municipal level (Leinmiller and O'Mara 2017; USEPA 2010) and we have already seen that disruptions to the electrical grid can impact performance and delay postdisaster recovery efforts in the water sector. As a compounding factor, both water systems and electrical networks throughout the US suffer from aging and degraded infrastructure.

Resilience for Water Infrastructure

Initiatives such as the Presidential Policy Directive 21 (PPD-21) (PPD 2013) call for proactive steps to strengthen critical infrastructure through resilience thinking and advanced technology.

Resilience includes the ability of a system to either prevent or minimize the effects of disruptions that arise, and also to rapidly recover from or adapt to changing conditions associated with emerging threats. With the implementation of new technologies in critical infrastructure systems, it is important to have a framework to characterize the effect on resilience of the system. Successful resilience frameworks provide the user with a holistic view of how different types of disruptions can impact the system of interest (e.g., a water management system), alert the user of system vulnerabilities, and provide guidance in increasing resilience through targeted system changes (Folke et al. 2010). For example, water provision resilience (WPR) is a proposed indicator that attempts to characterize the resilience of a water system by evaluating the fraction of the population with access to safe water and its ability to maintain or improve that access over 50 years by combining water supply, finance, infrastructure, service, quality, and governance indicators (Milman and Short 2008). However, such an indicator does not necessarily help inform regulators and stakeholders about the costs and benefits of introducing new resilience measures, nor is it sensitive to differences in needs and requirements of different water utility districts.

Smart technology has turned water utilities into cyberphysical systems that have significantly changed the way water is treated and distributed by increasing connectivity, monitoring, and control capabilities (Kott and Linkov 2018). With these technologies, water distributers can more efficiently respond to demand changes, improve conservation efforts, detect contamination incidents, expedite crisis response and recovery, perform self-repair operations, and communicate with customers about their water usage (Rasekh et al. 2016). Additionally, smart technologies can be deployed to monitor the aging infrastructure and the data used to prioritize repair and replacement needs in municipal budgets, which may not have the capacity to implement wholesale upgrades.

Resilience Assessment

Resilience is not a novel topic; definitions range from the ability of materials to withstand short-term overload without sustaining permanent damage (Bruneau et al. 2003) to the persistence of populations and state variables in ecological systems facing disturbance (Holling 1973). For the design of critical infrastructure in social-technical systems, such as water distribution, an applicable definition of resilience was given by the National Academy of Sciences (NAS) for disaster resilience as the "ability to plan and prepare for, absorb, recover from, and more successfully adapt" to disruptive events (NAIC 2016). Whereas the dominant paradigm for systems design and management has been quantitative risk assessment (Park et al. 2013), resilience has a broader purview that allows researchers not only to predict and mitigate against potential hazards but also to characterize the system's ability to recover and adapt to novel and emerging threats (Linkov et al. 2014). Resilience analysis utilizes risk models for scenarios in which the probability of disruption is quantifiable, but when risk is incomputable (e.g., unprecedented or unpredictable threats), resilience analysis relies on qualitative characterization methods (Linkov et al. 2013b).

Although there is broad recognition of interdependencies (O'Rourke 2007), efforts to increase resilience are often implemented in only one or two operational domains (e.g., physical systems) and the interconnections among components in other domains (e.g., informational systems) are given less importance (Bruneau et al. 2003; Madni and Jackson 2009; Poff et al. 2016; Woods 2015). To bridge the domain gap, Linkov et al. (2013a) developed a two-dimensional matrix to assess the intersections of each of the four major system domains: physical (e.g., facilities), information (e.g., data), cognitive (e.g., decision makers), and social (e.g., users, customers, and stakeholders), with the four stages of resilience (prepare, absorb, recover, and adapt) as described in NAS and PPD-21 definitions (Linkov et al. 2013a). Each cell in the resilience matrix is used to consider the various efforts that take place in each domain at each event state that contribute to overall system resilience. By taking a holistic view of function across domains and stages, planners can use the resilience matrix to inform a diversified and effective approach to resilience improvement.

Baseline Water Systems Resilience

Table 1 shows baseline resilience functions for water infrastructure systems organized in the resilience matrix. Table 1 does not contain specific metrics and is not meant to provide an exhaustive list of resilience functions, but rather a demonstration of how the resilience matrix is used as an organizational framework for understanding the efforts of risk reduction, sustainability, and adaptive capacity in traditional water infrastructure. The authors used relevant literature and industry knowledge to demonstrate the baseline resilience functions in Table 1.

Smart Water Systems Vulnerabilities

The primary goal of smart systems in water applications is to enhance reliability, efficiency, sustainability, and resilience and this lifeline resource. To understand how resilience can be improved with smart technologies, consider the Lake Oroville spillway incident of February 4–25, 2017. The Lake Oroville spillway sustained major large concrete erosion during a period of high inflows, leading to the evacuation of thousands of residents and causing major damage (Department of Water Resources 2017; Schmidt 2017). The recent failures at the Oroville dam seem to be in the physical domain but were also found to be directly linked to failures in the cognitive domain. The root cause analyses report by Bea and Johnson (2017) found "'inappropriate standards' and guidelines, procedures, processes" by the Department of Water Resources (DWR), Division of Safety of Dams (DOSD) and the Federal Energy Regulatory Commission (FERC) that failed to address aging infrastructure, technological obsolescence, and life cycle flaws and defects. Studies of documentation and written testimony found known indicators including failed and cracked spillway gate anchor tendons, cracked reinforced concrete gate supporting structures, and severe gate binding (Bea and Johnson 2017). When the presence of these indicators is reported only in written reports, it increases the chance that they will be overlooked and their importance downplayed or forgotten over time. Instead, if the structure had been outfitted with sensors (where appropriate) and the data, along with each visual inspection, had been reported in a digital dashboard of current conditions for system managers, the issues would have remained at the forefront and likely been addressed sooner and/or progression of the degradation over time more clearly noted.

There are many smart cyberphysical technologies rapidly being adopted for use in water infrastructure (Taormina et al. 2017), including supervisory control and data acquisition (SCADA) systems, online continuous monitoring (OCM) sensors, and advanced metering infrastructure (AMI). SCADA systems provide utility operators an interface to monitor sensor data, and remotely control actuated devices (pumps, valves, switches, etc.). Over the past decade, SCADA systems have been implemented in most water treatment and distribution facilities, and have been accessible only on

Table 1. Baseline resilience matrix for water systems

Domain	Prepare	Absorb	Recover	Adapt
Physical	Reduce water demand	Utilize neighboring utilities for water resources	Implement flexible, temporary systems	Replace obsolete and damaged assets
	Build redundant piping structures[a]	Manually trigger safeguards to isolate and contain damage to specific components	Stockpile machinery, communications, and power systems	
	Perform preventative maintenance[b]			
Information	Evaluate resources with risk framework in American Water Works Association (AWWA) standards[c]	Restrict dissemination of critical facility information[d]	Make historical information regarding customer needs and status available to emergency crews	Evaluate incident point of entry, event process, vulnerabilities, and impacts
	Utilize information sharing frameworks (e.g., WaterISAC[c])			
	Implement cross-sector vulnerability assessment[b]			
	Determine water requirements using normal-state system capabilities and population information			
Cognitive	Identify gaps between projected needs and available resources	Adhere to the incident command system (ICS) model for clear lines of control and accountability[a]	Prioritize restoration of critical support services with cross-sector decision makers[3]	Utilize a compendium of lessons learned, best practices, expert knowledge, and tools in after-action analyses[d]
	Develop emergency response plans using tools, such as EPA Road to Resilience Toolkit[d]			
	Simulate catastrophic events across large geographic regions[d]			Assess performance after low probability, high impact events (e.g., Hurricane Sandy)
Social	Develop connections with other local utility personnel, information, and resources[b]	Ensure relevant personnel and resources are available, requesting support if needed[a]	Implement protocols for internal, external, and public/media communication of recovery procedures	Distribute after-action reports with lessons learned and input from various stakeholders and authorities to consumers
	Implement education campaigns for citizens on the community water demand relative to system capacity and environmental or economic thresholds	Enforce individual resilience efforts during disturbances[a]		Incentivize community members to implement more resilient systems

[a]USEPA (2011).
[b]Waste and Wastewater Sector Strategic Roadmap Work Group (2017).
[c]DHS and EPA (2015).
[d]NAIC (2016).

private networks without connections to other systems (Janke et al. 2014). SCADA systems are now increasingly being placed on the internet, allowing for remote access (Amin et al. 2013). The growing internet of things (IoT) allows nearly any device to be given a unique internet protocol (IP) address and continuously or regularly upload data to cloud storage services, vastly increasing the amount of data that can be collected and the number of management and analysis systems that can access the data for different purposes. The IoT further facilitates two-way communication between IP-indexed devices, paving the way for automatic responses to predetermined sensor thresholds without direct human interaction. Such improvements in communications technologies have facilitated the implementation of OCM sensors to detect contamination, intentional or otherwise, in the distribution system (Banna et al. 2014), and AMI that accurately captures, collects, and communicates end user consumption information in near real-time (Stewart et al. 2010), or at least much more frequently than manual or ad hoc methods. In this way, smart technologies can help preemptively detect and prevent some hazards, provide the tools for recovery from other hazards, and adapt to persistent and progressive threats, thus enhancing resilience.

Smart technologies give operators increased awareness, efficiency, and control over systems, but at the same time can expose systems to a new set of cyberthreats and the potential for far-reaching propagating failure (Marchese and Linkov 2017). Attacks on smart cyberphysical water systems have increased in recent years (Taormina et al. 2018). A prominent example of this was the 2000 Maroochy Water Systems breach in Queensland, Australia, in which a disgruntled worker released nearly 800,000 L of raw sewage into surrounding waterways by temporarily taking control of the SCADA system, causing major environmental and public health impacts (Abrams and Weiss 2008). Other targeted attacks on industrial water controls include the StuxNet malware, which operates undetected in smart infrastructure while infecting and reprograming programmable logic controllers (PLC) (Chen and Abu-Nimeh 2011). In the extreme case, black sky events (high impact, low probability events) can cause a combination of severe physical damage to utilities across multiple sectors. For example, in 2012, Hurricane Sandy engulfed a 152-acre wastewater treatment plant in New Jersey, causing sustained damage to critical machinery, 3 days of lost power, and $200 million in damages (NAIC 2016).

Security of cyberphysical systems is a well-researched field (Lee 2008; Ning and Liu 2012; Sridhar et al. 2012). Automated control research has new algorithms and models to determine the maximum number of attacks that can be detected and corrected within cyberphysical systems (Fawzi et al. 2014), optimal sensor placement (Krause et al. 2008), and performance of controllers during various cases of system knowledge (Amin et al. 2013). Yet new cybersecurity research far outpaces its incorporation in industry and government. Rasekh et al. (2016) discusses the inability of many water systems to identify and prevent both sophisticated attacks like advanced persistent threats, and also even the most basic of cyberthreat from unauthorized access (Rasekh et al. 2016).

The complexity of distributed systems makes understanding and recognizing cyber vulnerabilities difficult (Goldman et al. 2011). Furthermore, cybersecurity principles are rarely embedded or prioritized throughout an entire organization (Knowles et al. 2015), leaving those organizations and associated systems vulnerable to cyberattack. For example, Shodan, a search engine that scans the internet for publicly accessible internet-connected devices, has been used to locate and exploit water utility control systems, with nearly 2.2 million publicly accessible SCADA devices discoverable online (Bodenheim et al. 2014), most requiring no (or default) credentials to operate. Operators who use publicly accessible internet-connected devices should understand that mass scanning technologies like Shodan easily debunk this paradigm of security by obfuscation.

In general, the vulnerabilities introduced to water infrastructure as a result of smart technology implementation can be summarized as acting on the four operational domains described in the resilience matrix (Linkov et al. 2013b):

- Cyber-physical vulnerabilities—connecting physical infrastructure to communications and control technology can facilitate malicious attacks on, or accidental failures in, that infrastructure, causing propagating failure in other networked infrastructure (Marchese and Linkov 2017).
- Cyber-information vulnerabilities—smart water technologies provide the ability to access secure information remotely, which makes that information vulnerable to theft, loss, and contamination (Collier 2017).
- Cyber-cognitive vulnerabilities—decision-making entities of traditional water infrastructure systems are almost exclusively human operators. Implementing automated decision-making entities, especially those that self-adjust (e.g., machine learning algorithms), introduces the potential for catastrophic failures resulting from decisions made in situations that have not been vetted in operational simulations.
- Cyber-socio vulnerabilities—the implementation of smart technology in infrastructure often requires consumer information, both personal (e.g., names and addresses) and habitual (e.g., consumption patterns). This information can be accessed and used in a cyberattack or can be mishandled, resulting in loss of service (Coburn 2014).

Smart Water Systems Resilience

To describe systematically how advanced technologies can be used to increase resilience in the water sector, the authors utilize the resilience matrix framework (Linkov et al. 2013a). Among the many smart technologies being implemented, the authors have identified three with which to demonstrate the resilience matrix: (1) SCADA, (2) OCM sensors, and (3) AMI. In Table 2, cells contain resilience functions that are facilitated by SCADA, OCM sensors, or AMI, and that exist in one of the four operational domains and one of the four resilience stages. In addition, Table 2 assigns general cybersecurity functions that can further improve system resilience by mitigating vulnerabilities introduced by the smart water technologies. Table 2 was populated using published works from organizations including the National Infrastructure Advisory Council, Water Sector Coordinating Council, Environmental Protection Agency, and the Department of Homeland Security, and are meant only as examples of water sector resilience functions.

There is an apparent difference between the baseline resilience functions and the smart resilience functions with respect to redundancy, modularity, and connectivity. The baseline functions rely on redundancy (e.g., redundant piping and backup sensors) and modularity (e.g., separate water storage facilities) to prevent catastrophic damage, and may be slow to react. Conversely, smart technologies use connected sensors and actuators to respond quickly to disturbances, but may be susceptible to targeted cyberattack (Marchese and Linkov 2017). Throughout the cognitive domain, there are increased interjurisdictional and intersectional resilience considerations. Agencies and utilities are now realizing that resilience efforts are more effectively implemented when collaboration with other utilities, as well as local, state, and federal authorities are leveraged. This is especially true for smart technologies that can

Table 2. Resilience matrix for smart water systems

Domain	Prepare	Absorb	Recover	Adapt
Physical	SCADA: Install SCADA systems	SCADA: Automatically trigger containment and isolation safeguards on damaged components	SCADA: Use real-time diagnostics capabilities to identify damaged system components	SCADA: Integrate with new technologies or treatment processes
	OCM: Install online water quality sensors	OCM: Identify the presence of contaminants in real time	SCADA: Prioritize reestablishment of services to critical systems	SCADA: Perform postdisruption diagnostics on physical infrastructure components to better respond to future disruptions
	AMI: Install smart metering technology	AMI: Enforce tariffs and water restrictions to conserve water resources during emergency	OCM: Identify malfunctioning treatment units, control units, or sensors	
	Cyber: Implement cyber preparedness (encryption, firewalls, intrusion detection systems, antivirus, data backups, etc.)			
Information	OCM: Identify urban drainage hydrographs for inclusion in disaster response planning	SCADA: Provide a platform for emergency information to be distributed to stakeholders and decision makers	OCM: Use sensor data to optimize repair schedules and minimize loss	SCADA, OCM, and AMI: Analyze data and operating environment to anticipate future incidents and update design, operations, and maintenance
	AMI: Determine water requirements using specific usage data	OCM: Rapidly detect signal anomalies in distribution, pressure, water quality, etc.	AMI: Identify areas of high water use during postdisaster recovery period	Cyber: Implement machine learning algorithms to reduce damage from repeat threats
		Cyber: Isolate data contamination to prevent propagating losses	Cyber: Facilitate dynamic reconstitution and composition of water system software	
Cognitive	OCM: Plan optimal sensor placement using technologies such as TEVA-SPOT[a]	OCM: Use real-time metering data to improve existing hydraulic models and estimate contaminant transport[a]	SCADA: Implement rule-based automated decision making and repair after disturbances	OCM: Iteratively revise sensor placement, as necessary for emerging threats
	Cyber: Implement scenario-based cyber war gaming	Cyber: Increase contaminant containment with techniques such as role-based access controls	OCM: Use event-detection software such as CANARY to route emergency crews automatically to hazard sites[a]	Cyber: Generate and analyze postdisruption reports to identify trends and potential action to strengthen infrastructure performance
	Cyber: Train operators to respond to cyberthreats		AMI: Provide water-use data to decision makers during disaster response	
Social	AMI: Provide a community information dashboard to facilitate education for demand management, water conservation, and disaster response	AMI: Communicate water usage information and conservation efforts during emergencies to utilities, and allow consumers to monitor local contaminant levels during disruption	SCADA: Enable water systems to automatically notify customers of changes in quality or service disruptions	SCADA, OCM, and AMI: Use disaster response data to initiate public discussion over financial investment in water system upgrades

Note: Resilience functions within each cell are identified as deriving from either SCADA systems, online continuous monitoring (OCM) systems, advanced metering infrastructure (AMI), or through general cybersecurity practices (cyber).

[a]Storey et al. (2011).

facilitate the collection and distribution of data of interest to multiple users. Nonetheless, water utilities, as early adopters of smart technology, are becoming adaptable to lessons learned, not only from the water sector, but from other industries and sectors as well (Waste and Wastewater Sector Strategic Roadmap Work Group 2017).

Conclusions

Utilizing the resilience matrix approach (Linkov et al. 2013a), the authors organize the various domains and stages of each of the resilience efforts recommended by various agencies for stakeholders in the water sector. Although not comprehensive, the resilience matrix provides a framework for agencies and researchers to categorize resilience functions with an understanding of the implementation domain and objective, so that domains or resilience stages that are underrepresented can be identified and remedied. Moreover, this framework guides stakeholders from a static implementation of risk assessment to resilience thinking by identifying the temporal nature of disruptions of the water system.

Due to the rapidly growing use of advanced technology in the water sector, additional research and implementation is needed to address the interconnectivity of physical, information, cognitive, and social domains of water resilience. Specifically, the requirement to identify the increasing exposure of smart water systems to cyberthreats and to plan accordingly using resilience approaches is paramount. Although quantitative risk metrics are useful, increasing resilience in rapidly evolving fields can rely on characterization methods like the resilience matrix (Linkov et al. 2013b) to allow for timely assessment. Using these techniques, planners and engineers will be better prepared to respond to disturbances in the water sector and cascading failures in other infrastructure sectors.

References

Abrams, M., and J. Weiss. 2008. *Malicious control system cyber security attack case study—Maroochy water services, Australia*. McLean, VA: MITRE Corporation.

Amin, S., X. Litrico, S. Sastry, and A. M. Bayen. 2013. "Cyber security of water SCADA systems. I: Analysis and experimentation of stealthy deception attacks." *IEEE Trans. Control Syst. Technol.* 21 (5): 1963–1970. https://doi.org/10.1109/TCST.2012.2211873.

Banna, M. H., S. Imran, A. Francisque, H. Najjaran, R. Sadiq, M. Rodriguez, and M. Hoorfar. 2014. "Online drinking water quality monitoring: Review on available and emerging technologies." *Crit. Rev. Environ. Sci. Technol.* 44 (12): 1370–1421. https://doi.org/10.1080/10643389.2013.781936.

Bea, R. G., and T. Johnson. 2017. *Root causes analyses of the Oroville dam gated spillway failures and other developments*. Berkeley, CA: Cal Alumni Association.

Bodenheim, R., J. Butts, S. Dunlap, and B. Mullins. 2014. "Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices." *Int. J. Crit. Infrastruct. Prot.* 7 (2): 114–123. https://doi.org/10.1016/j.ijcip.2014.03.001.

Bruneau, M., S. E. Chang, R. T. Eguchi, G. C. Lee, T. D. O'Rourke, A. M. Reinhorn, M. Shinozuka, K. Tierney, W. A. Wallace, and D. Von Winterfeldt. 2003. "A framework to quantitatively assess and enhance the seismic resilience of communities." *Earthquake Spectra* 19 (4): 733–752. https://doi.org/10.1193/1.1623497.

Chen, T. M., and S. Abu-Nimeh. 2011. "Lessons from stuxnet." *Computer* 44 (4): 91–93. https://doi.org/10.1109/MC.2011.115.

Coburn, T. 2014. "The federal government's track record on cybersecurity and critical infrastructure." Accessed September 18, 2019. https://www.hsgac.senate.gov/download/the-federal-governments-track-record-on-cybersecurity-and-critical-infrastructure.

Collier, R. 2017. "NHS ransomware attack spreads worldwide." *Can. Med. Assoc. J.* 189 (22): E786–E787. https://doi.org/10.1503/cmaj.1095434.

Department of Water Resources. 2017 *Lake Oroville spillway incident: Timeline of major events February 4-25*. Sacramento, CA: California Dept. of Water Resources.

DHS and EPA (Department of Homeland Security and United States Environmental Protection Agency). 2015. *Water and wastewater systems sector-specific plan*. Washington, DC: US Dept. of Homeland Security.

Fawzi, H., P. Tabuada, and S. Diggavi. 2014. "Secure estimation and control for cyber-physical systems under adversarial attacks." *IEEE Trans. Autom. Control* 59 (6): 1454–1467. https://doi.org/10.1109/TAC.2014.2303233.

Folke, C., S. R. Carpenter, B. Walker, M. Scheffer, T. Chapin, and J. Rockstrom. 2010. "Resilience thinking: Integrating resilience, adaptability and transformability." *Ecol. Soc.* 15 (4): 20.

Goldman, H., R. McQuaid, and J. Picciotto. 2011. "Cyber resilience for mission assurance." In *2011 IEEE Int. Conf. on Technologies for Homeland Security, HST 2011*, 236–241. Piscataway, NJ: IEEE.

Hill, D., B. Kerkez, A. Rasekh, A. Ostfeld, B. Minsker, and M. K. Banks. 2014. "Sensing and cyberinfrastructure for smarter water management: The promise and challenge of ubiquity." *J. Water Resour. Plann. Manage.* 140 (7): 01814002. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000449.

Holling, C. S. 1973. "Resilience and stability of ecological systems." *Ann. Rev. Ecol. Syst.* 4 (1): 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245.

Janke, R., M. E. Tryby, and R. M. Clark. 2014. "Protecting water supply critical infrastructure: An overview." In *Securing water and wastewater systems*, 29–85. Cham, Switzerland: Springer.

Kerkez, B., et al. 2016. "Smarter stormwater systems." *Environ. Sci. Technol.* 50 (14): 7267–7273. https://doi.org/10.1021/acs.est.5b05870.

Knowles, W., D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones. 2015. "A survey of cyber security management in industrial control systems." *Int. J. Crit. Infrastruct. Prot.* 9 (Jun): 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002.

Kott, A., and I. Linkov. 2018. *Cyber resilience of systems and networks*. Amsterdam, Netherland: Springer.

Krause, A., J. Leskovec, C. Guestrin, J. Vanbriesen, and C. Faloutsos. 2008. "Efficient sensor placement optimization for securing large water distribution networks." *J. Water Resour. Plann. Manage.* 134 (6): 516–526. https://doi.org/10.1061/(ASCE)0733-9496(2008)134:6(516).

Lee, E. A. 2008. *Cyber physical systems: Design challenges*, 363–369. Piscataway, NJ: IEEE.

Leinmiller, M., and M. O'Mara. 2017. "Smart water: A key building block of the smart city of the future." Accessed December 18, 2017. https://www.waterworld.com/articles/print/volume-29/issue-12/water-utility-management/smart-water-a-key-building-block-of-the-smart-city-of-the-future.html.

Linkov, I., et al. 2014. "Changing the resilience paradigm." *Nat. Clim. Change* 4 (6): 407–409. https://doi.org/10.1038/nclimate2227.

Linkov, I., D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H. Allen, S. E. Flynn, and T. P. Seager. 2013a. "Measurable resilience for actionable policy." *Environ. Sci. Technol.* 47 (ii): 10108–10110. https://doi.org/10.1021/es403443n.

Linkov, I., D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott. 2013b. "Resilience metrics for cyber systems." *Environ. Syst. Decis.* 33 (4): 471–476. https://doi.org/10.1007/s10669-013-9485-y.

Madni, A. M., and S. Jackson. 2009. "Towards a conceptual framework for resilience engineering." *IEEE Syst. J.* 3 (2): 181–191. https://doi.org/10.1109/JSYST.2009.2017397.

Mahmoud, H. A., Z. Kapelan, and D. Savić. 2018. "Real-time operational response methodology for reducing failure impacts in water distribution systems." *J. Water Resour. Plann. Manage.* 144 (7): 04018029. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000956.

Marchese, D., and I. Linkov. 2017. "Can you be smart and resilient at the same time?" *Environ. Sci. Technol.* 51: 5867–5868. https://doi.org/10.1021/acs.est.7b01912.

Milman, A., and A. Short. 2008. "Incorporating resilience into sustainability indicators: An example for the urban water sector." *Global Environ. Change* 18 (4): 758–767.

NAIC (National Infrastructure Advisory Council). 2010. *A framework for establishing critical infrastructure resilience goals: Final report and recommendations*. Washington, DC: US Dept. of Homeland Security.
NAIC (National Infrastructure Advisory Council). 2016. *Water sector resilience: Final report rnd Recommendations*. Washington, DC: US Dept. of Homeland Security.
Ning, H., and H. Liu. 2012. "Cyber-physical-social based security architecture for future internet of things." *Adv. Internet Things* 2 (01): 1. https://doi.org/10.4236/ait.2012.21001.
O'Rourke, T. D. 2007. "Critical infrastructure, interdependencies, and resilience." *Nat. Acad. Eng.* 37 (1): 22.
Park, J., T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov. 2013. "Integrating risk and resilience approaches to catastrophe management in engineering systems." *Risk Anal.* 33 (3): 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x.
Poff, N. L., et al. 2016. "Sustainable water management under future uncertainty with eco-engineering decision scaling." *Nat. Clim. Change* 6 (1): 25. https://doi.org/10.1038/nclimate2765.
PPD (Presidential Policy Directive). 2013. *Critical infrastructure security and resilience*. PPD-21. Washington, DC: White House.
Rasekh, A., A. Hassanzadeh, S. Mulchandani, S. Modi, and M. K. Banks. 2016. "Smart water networks and cyber security." *J. Water Resour. Plann. Manage.* 142 (7): 01816004. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000646.
Schmidt, S. 2017. "188,000 evacuated as California's massive Oroville Dam threatens catastrophic floods." *The Washington Post*, February 13, 2017.
Sridhar, S., A. Hahn, and M. Govindarasu. 2012. "Cyber–physical system security for the electric power grid." *Proc. IEEE* 100 (1): 210–224. https://doi.org/10.1109/JPROC.2011.2165269.
Stewart, R. A., R. Willis, D. Giurco, G. Capati, R. A. Stewart, R. Willis, and D. Giurco. 2010. "Web-based knowledge management system: Linking smart metering to the future of urban water planning." *Aust. Planner* 47 (2): 66–74. https://doi.org/10.1080/07293681003767769.
Storey, M. V., B. Van Der Gaag, and B. P. Burns. 2011. "Advances in on-line drinking water quality monitoring and early warning systems." *Water Res.* 45 (2): 741–747. https://doi.org/10.1016/j.watres.2010.08.049.
Taormina, R., S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld. 2017. "Characterizing cyber-physical attacks on water distribution systems." *J. Water Resour. Plann. Manage.* 143 (5): 04017009. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000749.
Taormina, R., S. Galelli, N. O. Tippenhauer, E. Salomons, A. Ostfeld, D. G. Eliades, M. Aghashahi, R. Sundararajan, M. Pourahmadi, and M. K. Banks. 2018. "Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks." *J. Water Resour. Plann. Manage.* 144 (8): 04018048. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000969.
USEPA. 2010. *Evaluation of energy conservation measures for wastewater treatment facilities*. Rep. No. EPA 832-R-10-005 Environmental Protection Agency. Washington, DC: Office of Wastewater.
USEPA. 2011. *Planning for an emergency drinking water supply*. Washington, DC: USEPA.
Waste and Wastewater Sector Strategic Roadmap Work Group. 2017. "Roadmap to a secure and resilient water and wastewater sector." Accessed January 24, 2019. https://www.waterisac.org/sites/default/files/public/2017_CIPAC_Water_Sector_Roadmap_FINAL_051217.pdf.
Woods, D. D. 2015. "Four concepts for resilience and the implications for the future of resilience engineering." *Reliab. Eng. Syst. Saf.* 141 (Sep): 5–9. https://doi.org/10.1016/j.ress.2015.03.018.