Increasing robustness and resilience of water delivery infrastructure

Stephen Reese, Ollie Gagnon – Idaho National Laboratory
Gaurav Kumar Srivastava, Martin Otto – Siemens Foundational Technologies, Siemens Corporation

Focal Area

Within the energy for water space, there is a need to establish a national testing capability for water treatment and delivery infrastructure to address knowledge and technology gaps. Water systems are vulnerable to product loss, contamination, or physical compromise due to aging or poorly maintained infrastructure, natural disasters, industrial accidents, and malicious acts. A national testing capability would increase water system resilience and help water utilities focus investments on high-consequence components and systems most prone to failure or compromise.

Existing Challenge

Supply water is a national critical function.[1] Water Systems enable the continuous operation of critical government and business functions and are essential to human health, safety, and economic security.[2] The water sector represents lifeline infrastructure[3] essential to the operation of most critical infrastructure sectors (including power generation), and it is a dependency undergirding multiple other national critical functions. There are ~148,000 public water systems[4] and ~50,000 water utilities in the U.S. versus only ~3,000 electric utilities.[5] 92% of those water systems serve less than 10,000 people (small systems),[6] and 88% of them are publicly owned.[5]

The preponderance of small, publicly owned systems makes water a target rich, predominantly resource poor sector. Physical infrastructure and operational technology (OT) systems in the sector are inviting targets to malign actors. Many utilities are unable to properly maintain the systems they have, let alone invest in upgrades to make their systems more secure and resilient. Approximately 15% (~8.3 km^3 annually) of treated water is lost due to leaks and failing infrastructure.[7,8] These losses equate to ~44.6 trillion BTUs of wasted energy annually.[9] In addition to maintenance deficiencies caused by budgetary limitations, there has been a notable increase in cyber-attacks on water infrastructure in the US in recent years, particularly by nation-state actors and their proxies.[10,11,12,13]

Consequently, there has been widespread federal interest in water sector cybersecurity. Joint seal guidance – issued by the EPA (Environmental Protection Agency), DHS CISA (Department of Homeland Security's Cybersecurity and Infrastructure Security Agency), and the FBI (Federal Bureau of Investigation) – was followed by White House-driven efforts to enlist states to develop cyber and physical security plans for water systems. These initiatives are evident in a March 28, 2024, request from the National Security Council[14] to state governors to prepare an action plan outlining how states aim to eliminate high-risk cybersecurity gaps. In May 2024, the Water Sector Coordinating Council (WSCC)[a] issued a letter to EPA's Office of Water and Office of

[a] The WSCC is a collection of water sector associations tasked with working with government to improve water critical infrastructure security and resilience.[15,16]

INL/PRO-25-88671

Research and Development and to DHS's Science and Technology Directorate and Cybersecurity and Infrastructure Security Agency stating, in part:

> "Currently, there is no large-scale, OT [Operational Technology]-enabled water system environment that can be disrupted or destructively tested. Current testing is limited to emulation and simulation. The WSCC believes there is a need to establish an adaptable testing and training environment that can respond to the evolving level of automation in the water sector, including the assessment of new OT and other digital tools. In the absence of such a capability, some utilities will only be able to respond to cyber-physical incidents instead of pre-emptively mitigating the potential impacts or preventing them outright."

Water utilities are faced with competing demands between maintenance and infrastructure replacement, system upgrades, and cyber security requirements. Limited budgets generally make addressing all these areas impractical. Research and testing are needed to help water providers prioritize their investments where they will have the most impact, to identify equipment or systems that will meet or exceed performance requirements, and to develop and refine realistic operator training to enhance utility readiness and minimize downtime due to disruptions.

Near-Term Opportunity (3-5 year timeframe)

The Idaho National Laboratory (INL) houses the Water Security Test Bed (WSTB), a large-scale platform for testing water system decontamination methods. The remote, secure WSTB offers the ability to test equipment to failure without putting a population at risk – as would be the case for any testing down with a municipal water system. Further, the WSTB is co-located with the INL's Electricity Grid and Wireless Test Beds, enabling testing of infrastructure interdependencies (e.g., water systems' reliance on grid-supplied power, wireless sensors and instrumentation in water systems). With upgrades, this established test capability can test control system and automation solutions at scale – whether individual components or hardware or software systems. Further, INL offers a suite of National Security related infrastructure security and resilience analysis capabilities and experts. Siemens provides a fundamental, industry-leading research capability to inform and augment analysis and testing done at INL, as well as the product development capability to field new solutions that can then be tested and verified at scale at the WSTB.

There is a national need to establish a sustained program focused on testing water components and systems, validation of water quality protocols, and training for utility operators and OT personnel. Simply directing budget-challenged water providers to add trained IT/OT staff and to upgrade their systems to the most modern, secure state is not a viable solution. A testing program that reveals what systems or components are relatively rugged or hardened against tampering versus those links in the system that, once compromised, lead to significant infrastructure damage and/or service interruption is critical. Utilities need information on which systems or components to focus their limited resources – where investment can have the biggest impact on the security and resilience of their systems. This approach supports nationally focused approaches – Secure by Design and Cyber-Informed Engineering – to mitigate risks in cyber-physical systems. By establishing a national, risk-informed testing and training capability for water systems, the approach also advances the Executive Order "Achieving Efficiency Through

State and Local Preparedness" [17] by enabling states and municipalities to make data-driven infrastructure investments while leveraging federal resources and expertise. This collaborative model embodies the Order's directive for the federal government to support and strengthen state and local efforts to build efficient, secure, and resilient critical infrastructure systems.

Success Measure

The most impactful success measure of a research program focused on cyber-physical water system resilience will be a reduction in water losses, hardening of water systems, and building resilience to the impacts of cyber-initiated attacks and natural disasters. Near term success will be indicated by the establishment of a national testing and training capability for water system resilience that informs and guides government policy and utility modernization. Long term results will be seen in growth of the number of operators trained to identify and preempt intrusions and in increases in large and small utilities' level and sophistication of planning for security and resilience upgrades.

References

1. "National Critical Functions," Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/national-critical-functions-set, accessed 10/2/2025.
2. "Community Lifeline," Federal Emergency Management Administration, https://www.fema.gov/emergency-managers/practitioners/lifelines, accessed 10/21/2025.
3. "National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience," Department of Homeland Security, https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf, accessed 10/2/2025.
4. "Information about Public Water Systems," US EPA, https://www.epa.gov/dwreginfo/information-about-public-water-systems, accessed 10/2/2025.
5. "Comparing Water & Electricity Delivery Systems," Pacific Northwest National Laboratory, https://www.pnnl.gov/sites/default/files/media/file/WaterUtilities.pdf, accessed 10/2/2025.
6. "Small Drinking Water System Variances," US EPA, https://www.epa.gov/sdwa/small-drinking-water-system-variances, accessed 10/2/2025.
7. "Water Leaks: A Costly and Risky Problem," Seven Seas Water Group, https://sevenseaswater.com/water-leaks-a-costly-problem/, Oct. 21, 2024.
8. "A Comprehensive Assessment of America's Infrastructure: 2025 Report Card for America's Infrastructure," American Society of Civil Engineers, https://infrastructurereportcard.org/wp-content/uploads/2025/03/Full-Report-2025-Natl-IRC-WEB.pdf, 2025.
9. Twomey & Webber, "Evaluating the energy intensity of the US public water system," Proceedings of the ASME 2011 5th International Conference on Energy Sustainability, August 7-10, 2011, Washington DC.
10. "Throwback Attack: How the Bowman Avenue Dam Became the Target of Iranian Hackers," Control Engineering, https://www.controleng.com/throwback-attack-how-the-modest-bowman-avenue-dam-became-the-target-of-iranian-hackers/, accessed 10/2/2025.
11. "Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group," CBS News, https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/, accessed 10/2/2025.

12. "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities," DHS CISA, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a, accessed 10/2/2025.
13. "Mandiant: Notorious Russian hacking unit linked to breach of Texas water facility," Cyberscoop, https://cyberscoop.com/sandworm-apt44-texas-water-facility/, accessed 10/2/2025.
14. "NSC issues new letter to US governors requesting water system action plans," Association of State Drinking Water Administrators, https://www.asdwa.org/2024/04/01/nsc-issues-new-letter-to-us-governors-requesting-water-system-action-plans/, accessed 10/2/2025.
15. "Water Sector: Council Charters and Membership," DHS CISA, https://www.cisa.gov/water-sector-council-charters-and-membership, accessed 10/10/2025.
16. "Water Sector Coordinating Council Discusses Cybersecurity with EPA, DHS," National Association of Clean Water Agencies (NACWA), https://www.nacwa.org/news-publications/news-detail/2022/05/26/water-sector-coordinating-council-discusses-cybersecurity-with-epa-dhs, accessed 10/10/2025.
17. "Achieving Efficiency Through State and Local Preparedness," Executive Order, The White House, March 19, 2025, https://www.whitehouse.gov/presidential-actions/2025/03/achieving-efficiency-through-state-and-local-preparedness/.