The Future of Shared Responsibility Security for Water Utilities

Enhancing Cybersecurity Across the Water Sector with Connected Technologies and Practical Examples

[printed for WaterISAC event on 11-SEP-2025]

By:

Kenneth G. Crowther, PhD, Product Security Leader, Xylem, Kenneth.Crowther@xylem.com

Kristina Macro, P.E., Senior Project Manager, Xylem, kristina.macro@xylem.com

Richard Loeffler, Director of Digital Sales – US East, Xylem, Richard.Loeffler@xylem.com

Summary:

This whitepaper discusses enhancing cybersecurity in the water sector through connected technologies and practical examples. It emphasizes principles like defense in depth, shared responsibility, and continuous improvements. These principles involve multiple layers of security, joint efforts between service providers and users, and ongoing monitoring and updates.

Connected digital technology in water utilities allows for real-time monitoring and improved efficiency but introduces new security challenges. The document outlines security controls such as Identity and Access Management (IAM), encryption, network security, monitoring, vulnerability management, and compliance.

Examples of Xylem's cloud security implementations include OPC-UA for secure communication, secure SFTP servers for data transfer, transitioning to cloud-based services, using hardened modems as secure gateways, and other tailored examples for customers.

This whitepaper advocates for embracing connected technologies and robust security principles to protect critical infrastructure in the water sector. By implementing these measures, water utilities are more likely to ensure a safe and resilient future.

Principles of Modern Cybersecurity

Cybersecurity is an ever-evolving field, requiring continuous vigilance and adaptability. Water utilities, like many other sectors, must embrace comprehensive security measures to protect their critical infrastructure. Among the foundational concepts in modern cybersecurity are defense in depth (e.g., Kidd 2023), shared responsibility (e.g., Crowther 2024), and the continuous nature of cybersecurity (e.g., Abrahams et al 2024).

Defense in depth (sometimes called multi-barrier approach, castle doctrine, or security layered cake) involves implementing a community of security controls in multiple layers to protect the availability, integrity, and confidentiality of systems and data. This approach ensures that if one layer is compromised (e.g., someone gains access), subsequent layers provide additional protection (e.g., access does not grant privilege to change data and create a safety issue).

Shared responsibility prescribes that security is a joint effort between the service provider and the customer. For example, the cloud provider (e.g., Amazon Web Services) secures the hardware and system software, the vendor (e.g., Xylem) ensures the security of data and applications within the cloud environment, and the user (e.g., water utility) protects credentials and designs process safety assurances that don't rely only on digital controls. This is a modern example of how a community of controls is implemented when multiple parties are involved in maintaining the connected digital systems.

Cybersecurity is a ***continuous journey*** rather than a one-time fix. Threats evolve, and new vulnerabilities emerge, requiring ongoing monitoring, updates, and improvements to security measures. In this sense, software and digital services should be treated like every other critical asset and have maintenance schedules.

Value of Connected Digital Technology

Connected, digital technology has revolutionized water utilities by allowing for real-time monitoring, remote management, and improved operational efficiency. These digital transformations are decreasing maintenance expenses, improving operational efficiency, and enabling knowledge transfer to a younger workforce, among other improvements. (e.g., Daniel et al. 2023; Amankwaa, Heeks, and Browne 2024) However, this connectivity also introduces new security challenges, necessitating robust security measures. Last year, EPA issued a warning of increased cybersecurity at water utilities, a study showing 70% of inspected US water systems failed to meet basic security standards expected by the Safe Drinking Water Act, and an enforcement alert. (e.g., Tempest 2024) Cybersecurity in the water sector protects the value created by connected, digital technologies.

Layers of Security Controls in Connected Cloud Services

When connecting to a reputable vendor, water utilities benefit from multiple layers of security controls integrated into cloud services. These layers typically include (NIST 2025):

- ***Identity and Access Management (IAM)***: IAM ensures only authorized users or devices have access to systems and data. Every connection with a web resource should enable mutual authentication in which the device/human authenticates the external web service, and the web service authenticates the device. (Xylem 2025)
- ***Encryption***: Encryption is for protecting data both at rest and in transit through algorithms that ensure integrity of data and obscure the data from those who could intercept it. Modern protocols like HTTPS or OPC-UA are built with interoperability and security in mind, but legacy protocols like Modbus are not. (Stouffer et al 2023)
- ***Network Security***: Creating a defensible network architecture builds on IAM and secure communications. It starts with understanding your assets and data flows and mapping out connections. The idea is to divide the network into smaller segments to limit the spread of a potential cyber threat. Some gateways for cloud services are naturally configured to only connect to specific services and deny all other ports, protocols, and traffic from other entities. (Dragos 2023)
- ***Monitoring and Logging***: Monitoring and logging means keeping an eye on your digital systems—like connected sensors, controllers, and remote access tools—to detect unusual or unauthorized activity. Just like tracking pump performance, this helps you catch early signs of cyber threats, such as someone trying to access your system without permission. (Ebute 2024)
- ***Vulnerability Management***: Vulnerability management for connected digital assets means regularly checking your systems for weaknesses that hackers could exploit and fixing them before problems arise. It's like inspecting pipes for cracks, but instead you're looking for outdated software, weak passwords, or unprotected devices. (CISA 2016)
- ***Compliance and Auditing***: Compliance and audit for cybersecurity means making sure your connected digital systems follow industry rules or internal requirements. It's like a safety inspection, but focused on digital protections like access controls, software updates, and logging. To do it well, keep records of your cybersecurity practices, follow any required standards (like AWWA or EPA guidelines), and schedule regular reviews or audits to stay on track. (Sulaiman et al 2022)

Xylem Cloud Security Implementation Examples

Defense in depth can become expensive because each layer requires tools, skills, and resources to properly sustain. Consider for example the layer "monitoring and logging." To be most effective, this would require all devices (e.g., all sensors, actuators, controllers, work stations, etc.) to log events such as a user access or parameter change, to forward those logs to a collection system, to track those systems in a framework that traces log purpose and storage timeframe, and to have an operations center with adequate resources and processes to continuously monitor and respond to anomalous behaviors. A typical security operations center can cost over $1M to set up and almost as much annually to operate – and that is only one layer of the security layered cake required for effective defense in depth.

Security "Layered Cake" of a suitable cloud vendor includes $2M/yr of security.

	estimate per year
Certificate / key management	$10k - $50k
Vulnerability / patch management	$50k - $350k
Security Operations Center (SOC)	$100k - $1M
Logging and log aggregation	$5k - $20k
Access controls and certificate authority	$10k - $20k
Configuration control and system audit	$5k - $30k
Asset inventory and maintenance	$10k - $50k
Hardware / physical security	$100k - $500k

Table 1. Examples of defense in depth layers for a secure cloud service with estimated cost ranges.

The shared responsibility model improves the ability to implement the entire community of controls by properly spreading the responsibility for various controls across a broader community to make it economical. For example, any cloud service should come with the entire stack of controls included in the price of the service.

Xylem Vue is a secure-by-design platform, and we have a shared responsibility model of cybersecurity with the water utilities we work with. Several examples from utilities in the Northeast US demonstrate data integration and split responsibilities.

Example 1: Typical Deployment of Xylem Vue

Integrating data into the Xylem Vue platform to begin breaking down data silos at a utility is typically done with OPC-UA (Open Platform Communications Unified Architecture). OPC-UA clients only require a single *outbound* port to be open on a firewall because they can utilize the HTTP/2 protocol for communication with OPC services in the cloud. HTTP/2 allows for multiplexed streams over a single secure connection, meaning multiple requests and responses can be sent simultaneously over one port. This reduces the need for multiple open ports, enhancing security by minimizing potential attack vectors. The OPC-UA client initiates the connection, and once established, the server can send responses back through the same channel, enabling two-way communication. The inherent security

in this design comes from the use of encryption and authentication mechanisms within the OPC-UA protocol, ensuring that data is securely transmitted, and that both the client and server are verified entities. This combination of a single outbound port and robust security measures makes OPC-UA a secure and efficient choice for industrial communication. (Kohnhauser et al 2021, Kinnunen 2024)

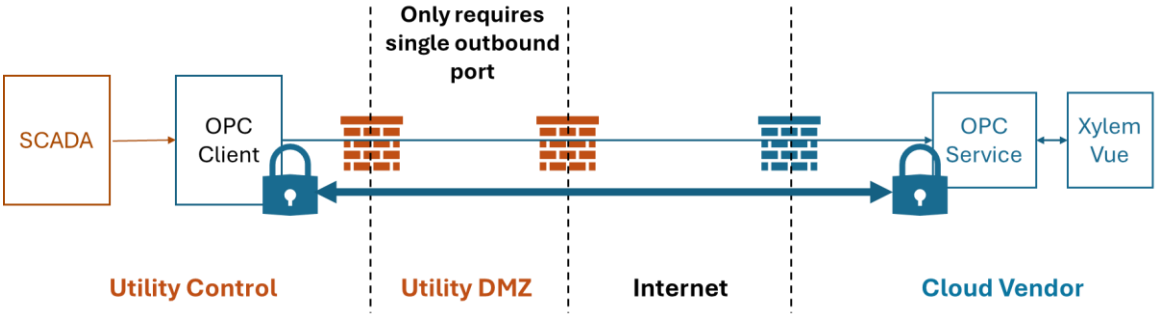

Figure 1. OPC-UA clients only require outbound port open on firewall, which reduces exposure and gives client control.

This is the typical way to extend the layers of security offered as part of a cloud service offer to a utility. OPC-UA was designed with interoperability and security in mind. It offers the following layers of security:

- **Mutual authentication** – Both client and cloud service must prove their identity through cryptographic certificates that act as identities that are difficult to spoof. It's like two people meeting for the first time and both are showing their government-issued identification before they begin to discuss their business.
- **Message encryption** – It's like stamping and sealing a letter in a locked briefcase – it is useless if intercepted, and if it arrives changed, you know someone tampered with it. Most utilities prioritize integrity (signing), but for remote communications you want both integrity (cryptographic signing) and confidentiality (encryption).
- **Session control by client (utility)** - The client machine initiates and ends conversations—reducing risk from rogue actors. Because you only need to open a single outbound port, no other entities or services can connect through the firewall into your control system network. While two-way communication is possible within the secure design, it is controlled and limited by the utility. Sort of like a phone call where only the caller can start and end the conversation to ensure no one else can interrupt.
- **Logging, monitoring, and response** – Each connection, failed connection, and change is logged and monitored. Least privilege set-up allows quick identification of anomalies and alerting for the utility.

Example 2: Secure SFTP Server Implementation

While OPC-UA is the default because of the built-in interoperability and layers of security, some utilities have a different set-up that lends itself to other security architectures. For example, one water utility in the Northeast had a system that collected data from their SCADA system and saved it into CSV files to share with analysts. Instead of setting up an OPC-UA client, we automated the process for these files to upload to a hardened file transfer server (SFTP) in a secure area that was independent of the control network.

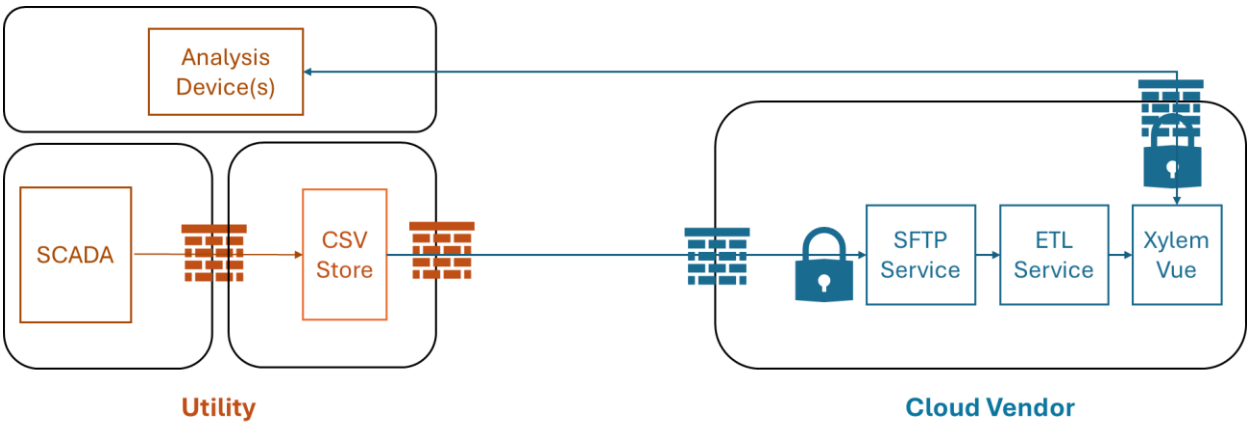

Figure 2. Secure architecture can tailor to existing security postures of utilities, such as external facing data store.

To automate remote analytics and alarms and to make it easier for analysts to obtain data, we set up a secure SFTP service in the cloud and provided specific instructions for sending their CSV data. The SFTP server is monitored 24/7 and is configured in a way that ensures all security layers described above (regular audit, vulnerability management, strict role-based access controls, log aggregation and continuous monitoring, and so forth). This segmentation and secure SFTP service provides the first layers of defense. However, before the data enters the Xylem Vue system it is also validated and prepared. This process is called ETL (Extract, Transform, Load) and provides added extra security measures that ensure new data will not pollute the system that creates analyses and alarms.

Customers can access their data, view analytics, customize additional analytics, and so forth within the scope of their roles and privileges granted to them by their admin. The overall process provides layers of controls that are customized around their existing business processes and adds both value from real-time digital analytics as well as improves their overall security posture with additional security evaluation and monitoring.

Example 3: Transition from On-Prem to Cloud-Based Services after Detailed Supplier Review

Another example involves a utility that initially requested an on-prem solution for their water utility management but wanted the vendor to maintain it. However, providing maintenance and security for an on-prem solution proved cost-prohibitive, whereas cloud services that were accompanied with additional security were cost-effective. The utility sent a detailed questionnaire about cloud security practices patterned after the NIST Cybersecurity Framework (NIST 2025) to evaluate cloud-based services.

Table 1. NIST Cybersecurity Framework (CSF) provides foundation for evaluating vendor cybersecurity.

NIST CSF SUBCATEGORY	*PR.PS-06:* Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle.
UTILITY QUESTION	Describe the system lifecycle process for in-house developed and acquired systems used for implementation and on-going maintenance to prevent, detect, and correct security weaknesses.
VENDOR RESPONSE	We enforce and audit secure development and implementation for all product or system releases consistent with *Xylem 72-02.21 Secure System and Software Lifecycle Management* (attached), …

While originally skeptical regarding moving to a "shared responsibility" model for cybersecurity, having transparent access to vendor controls provided an ability to better understand risks and hold the vendor accountable for consistent delivery. Use of a standard framework enables ease of communication. NIST CSF provides a foundation for investigating the security of operational systems (e.g., cloud services), the NIST Secure Software Development Framework (SSDF) provides a foundation for investigating the security that is built into a product that is delivered to the utility (e.g., purchased controller for on-premises installation).

Example 4: Hardened Modems as Secure Gateways

Another innovative solution involves the use of hardened modems that act as secure gateways. Some modems can be configured according to a checklist of controls to ensure they are always up to date, with all inbound and outbound ports closed and strictly limited connections from a short whitelist. Reconfiguration is only possible from a specified location over a VPN by an authorized user.

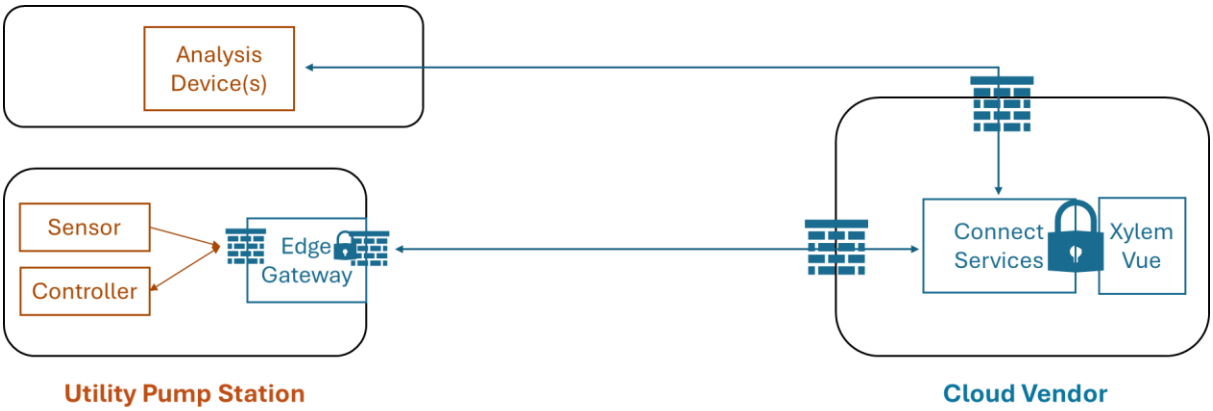

Figure 3. Specialized gateways can be hardened in ways to ensure secure communication.

This modem wraps insecure control network traffic (e.g., Modbus, DNP3, etc.) into a secure data or application protocol, such as MQTT over TLS, and sends traffic through a protected connection to a dedicated endpoint. The cloud service then has all layers of security controls that have been discussed. The layers of security on the cloud service can be extended to cover monitoring of the edge gateway and any devices that are able to forward device information through the gateway. As such, SCADA monitoring can even be extended to include firmware versions and patch status of controllers and other devices on the network.

Conclusion

The future of shared responsibility security for water utilities lies in embracing connected technologies and robust security principles. By implementing defense in depth, focusing on shared responsibility, and continuously evolving their cybersecurity practices, water utilities can protect their critical infrastructure while reaping the benefits of digital transformation.

Practical examples, such as OPC-UA, secure SFTP server setups, supplier reviews for transitions from on-prem to cloud-based services, and the use of hardened modems, demonstrate the feasibility and advantages of modern cybersecurity implementations that can be included in digital technology. As water utilities move forward, they should prioritize security in all aspects of operations, ensuring a safe and resilient future.

References:

Abrahams, T.O. et al, 2024. Continuous improvement in information security: A review of lessons from superannuation cybersecurity uplift programs. *International Journal of Science and Research Archives*.11(1): 1327-1337. DOI: 10.30574/ijsra.2024.11.1.0219

Amankwaa, G., et al., 2023. Powershifts, organizational value, and water management: digital transformation of Ghana's public water utility. *Utilities Policy*. 87. DOI: 10.1016/j.jup.2024.101724.

CISA (US Cybersecurity and Infrastructure Security Agency), 2016. *Volume 4 Vulnerability Management, Version 1.1*. Available online: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf.

Crowther, K.G., 2024. Blending shared responsibility and zero trust to secure the industrial internet of things, *IEEE Security & Privacy*, 22(5): 96-102, DOI: 10.1109/MSEC.2024.3432208.

Daniel, I. et al, 2023. A survey of water utilities' digital transformation: drivers, impacts, and enabling technologies. *NPJ Clean Water*. 2023(6):1-9. DOI: 10.1038/s41545-023-00265-7.

Dragos, 2023. *Implementing a Defensible Architecture: Using OT Asset Visibility and Firewalls to Protect Industrial Operations*. Available online: https://hub.dragos.com/white-paper-implementing-a-defensible-architecture.

Ebute, M.,2024. Continuous Monitoring and Assessment Mechanisms in Cybersecurity: Best Practices for Sustained Protection of Critical Assets. (July 31, 2024). Available online: https://ssrn.com/abstract=4912624.

Kidd, D., 2023. Cybersecurity Defense in Depth: Layered Strategies for Comprehensive Protection. *LinkedIn*. 10-OCT-2023. Available online: https://www.linkedin.com/pulse/cybersecurity-defense-depth-layered-strategies-protection-david-kidd/.

Kinnunen, H., 2024. *Cloud communications of Factory Automation System with OPC UA*. Master Thesis, Aalto University. https://aaltodoc.aalto.fi/server/api/core/bitstreams/b05cd408-470b-4aca-b0d4-1ce4d6727d92/content.

Kohnhauser, F., et al., 2021. On the security of IIOT deployments: An investigation of secure provisioning solutions for OPC UA. *IEEE Access*. DOI: 10.1109/ACCESS.2021.3096062.

NIST (US National Institute for Standards and Technology), 2025. *Cybersecurity Framework 2.0*. Available online: https://www.nist.gov/cyberframework. Accessed on 13-JUN-2025.

Stouffer et al, 2023. *Guide to Operational Technology (OT) Security*. NIST SP 800-82r3. DOI: 10.6028/NIST.SP.800-82r3

Sulaiman, N.R., et al, 2022. Cyber-information security compliance and violation behavior in organizations: A systematic review. *Social Sciences*. 11(9). DOI: 10.3390/socsci11090386

Tempest, O., 2024. EPA to ramp up cybersecurity inspections for water utilities. *Smart Water Magazine*. Available online: https://smartwatermagazine.com/news/smart-water-magazine/epa-ramp-cybersecurity-inspections-water-utilities.

Xylem, 2025. *Water Sector Cybersecurity: Effective Identity and Access Management (IAM) Practices*. Available online: https://www.xylem.com/en-xk/resources/blog-posts/water-utilities-cybersecurity-iam-practices/.

Xylem |'zīləm|

1) The tissue in plants that brings water upward from the roots;
2) a leading global water technology company.

We're a global team unified in a common purpose: creating advanced technology solutions to the world's water challenges. Developing new technologies that will improve the way water is used, conserved, and re-used in the future is central to our work. Our products and services move, treat, analyze, monitor and return water to the environment, in public utility, industrial, residential and commercial building services settings. Xylem also provides a leading portfolio of smart metering, network technologies and advanced analytics solutions for water, electric and gas utilities. In more than 150 countries, we have strong, long-standing relationships with customers who know us for our powerful combination of leading product brands and applications expertise with a strong focus on developing comprehensive, sustainable solutions.

For more information on how Xylem can help you, go to www.xylem.com

xylem
Let's Solve Water

Xylem, Inc.
11161 Harrel St
Mira Loma, CA 91752
Tel +1.951.681.3636
Email security@xylem.com
www.xylem.com