Operational Technology:
Network Topology and Risk Tolerance

By David Brearley
Operational Technology Cybersecurity Director, Columbia, SC

Water utilities, a key component of the United States' critical infrastructure, are challenged with controlling operating costs while maintaining resilient and safe operations.

Operational technology systems, or control systems, are widely accepted as a critical component to operations. These OT systems enable operations of highly complex and distributed processes not readily achieved through human interaction.

Advances in process technology have increased the number of connected OT devices, simultaneously growing the amount of information created exponentially. This increased availability of data has fostered an explosion of capacity and efficiency gains.

These advances come with their own inherent challenges. Large, comprehensive systems also, by their very nature, create a large 'surface' vulnerable to cyberattack. This attack surface necessitates the application of cybersecurity, monitoring and maintenance to keep the process operational and infrastructure safe.

At its core, cybersecurity is the act of risk management, balancing the investments made to secure systems versus the potential impact of a cyber event. For a utility to develop cybersecurity risk tolerance metrics, it must consider not only the potential consequences, but also the costs of security. Security costs are comprised of financial investments, both capital, maintenance and operational.

These costs address the requirements of implementing system security improvements, as well as the continuous monitoring and maintenance.

No One-Size-Fits-All Approach

There is no such thing as a perfectly secure system, and cybersecurity is not a one-size fits all approach. Various best practices and national and international standards for OT Cybersecurity exist (such as ISA-62443 and NIST 800-82). However, many utilities are unable to achieve full compliance with the standards due to financial, staffing or other constraints. Even those systems owned by entities with significant financial capabilities such as the federal government must also accept some level of risk.

Consequently, it is recommended that owners follow a risk-management framework to identify and evaluate risks. Once determined, an organization must either accept, transfer or mitigate risks to create an OT system that is within its acceptable risk tolerance.

Network topology is one of the primary design elements within the risk, impact and cost evaluation process. Differing topologies provide options and opportunities for controlling the size of attack surface, the scope and breadth of the attack, and the tools available to detect, respond and recover. Additionally, evaluation of operational impacts (both gains and losses) should be considered when selecting a topology that balances operational gains (e.g. efficiencies, data visibility, mobility) and risk tolerance goals.

Exploring the risks, benefits and challenges of widely utilized network structures provides an understanding of key characteristics to assist in making an informed selection of network topological implementations. The selected topology should provide for risk mitigation that meets acceptable tolerances.

Examples of network topologies commonly found within water utilities vary from isolated systems to fully integrated, up to and including cloud hosted solutions.

Air-Gapped Control Systems

Traditionally, water utilities have utilized the concept of a physical separation (an air gap) of the OT network from other networks as the primary means of protection. Frequently, it is the only means of protection.

In the past, control systems have utilized self-limiting communications protocols, which were typically proprietary with an air gap that was accepted as a secure architecture. Modern control systems have transitioned to rely on open network communications protocols (IP based) and operating systems (Windows).

These open architectures are leveraged to decrease OT device cost, while increasing the integration with other systems in order to achieve goals focused on situational awareness and efficiency.

Today, the use of an air gap as the only means of cybersecurity risk management is no longer recognized as an accepted methodology for securing a control system. An air gap primarily attempts to provide boundary protection against an outside actor entering the network; it does not provide any protections against internal actors or when the air gap is breached. Stuxnet is the most famous and malicious example of a breach of an air gapped control system affected by a virus. However, not all breaches are intentionally malicious and often may occur when outside sources introduce laptops onto a site network, plug in a cell phone for charging or plug in removable media (like a USB Flash drive) to patch or install new software. Each breach has the potential for adverse impacts to the network.

True air-gapped systems cannot receive updates (including patches, operating system or firmware updates or antivirus/anti-malware definition updates) without a breach. Air-gapped systems also limit access to data available for situational awareness and increased efficiencies by maintaining process control data as a disparate data set contained only within the control system environment.

Maintaining the air gap relies on the application of policies and procedures for all interactions with the system, which are typically human-centric constructs that require voluntary compliance. Unfortunately, human interactions with systems are attributed to approximately thirty percent of successful cyberattacks.

Data Diodes - A One-Way Connection

A variant of the air-gapped network is utilizing a data diode, which creates a one-way connection where communications are physically restricted from entering the control system network but allows for a defined communications path leaving the network.

Much like physically air-gapped systems, data diodes utilized as the only means of security are still faced with the risks associated with inside actors, maintenance challenges and manual enforcement. Data diodes do not represent a significant increase of the infrastructure investments, and have minimal maintenance cost. Some utilities use the addition of a data diode as a steppingstone on the path to a modern OT / business integrated environment.

While air-gapped systems are focused on the external threat, they do nothing in the way of addressing those that are internal. Without additional protective measures, an inside actor can inflict intentional or unintentional harm to the OT systems. For many utilities this is an acceptable balance of costs and risks; the challenges related to limited data integration and voluntary policy enforcement outweigh the costs associated with more integrated architectures.

Modern OT systems achieve a balance of risk and data integration to promote operational efficiencies and security through network design, system-based policy enforcement and network monitoring.

Operational efficiencies and situational awareness are maximized through OT system data integration with business systems including, but not limited to, LIMS, CMMS, WIMS and GIS. Large integrated networks increase the number of threat vectors to the control system, the cost and complexity of the implementation, and the resource costs associated with monitoring and maintaining that system. Consequently, utilities must carefully weigh the value of efficiency gains against risk and costs.

Defense In Depth Techniques

For complex integrated networks, risk management is achieved through the application of defense in depth techniques. These methodologies offer boundary protection, layers of defense against insider and outsider threats and may also limit the scope of an attack when a network is compromised. Defense in depth relies on an array of techniques which range from technology, topology, people, policies and procedures (voluntarily and systemically enforced), network monitoring and system maintenance.

Within this model, network traffic is contained inside a zone with data integration flows allowed to traverse network zone boundaries through a specific, limiting conduit. Any cross zone-boundary traffic must have a business purpose that outweighs the risks. These allowable exceptions are configured with directional traffic flow moving from the trusted OT network to the untrusted exterior networks. The untrusted networks must never be allowed to communicate directly with trusted networks.

For data that must be transmitted from an untrusted network into a trusted network, an intermediary network (demilitarized zone - DMZ) should be utilized. This intermediary network provides a buffer with its own security and monitoring, along with the ability for quick disconnects from foreign networks in the event of an emergency. For this implementation, it is critical that the OT network and its associated devices must not rely upon outside resources to maintain normal operations.

The topology within each network zone may be further compartmentalized with additional zones and conduits.

Applying defense in depth within the network topology requires the control of data flows using a zone and conduit model.

The segmentation of OT zones should carefully consider interactional requirements between systems as well as their importance to the operations. Well-designed network zones limit exposure, the initial impact of a breach into a zone and provide additional security features on network protected critical assets. It should be noted that network segmentation increases individual device configuration and the complexity of the network architecture.

Additionally, communications between zones require monitoring of the network traffic to properly maintain security. Resources are required for completing this security mosaic and these complexities increase equipment costs, configuration and maintenance times and require additional skillsets because the planning, design and implementation are ineffective if the alarms go unheeded.

You have to be right 100% of the time, the cyber criminals only have to be right once!

Integrated networks also require policies and procedures for interaction with the OT systems to codify the security requirements and methodologies. While technology does not remove the human component from the equation, many policies and procedures can be enforced automatically through the system. The OT systems implemented, with all their varied interconnections, are designed to increase the efficiency and decision-making processes that are required to be executed by individuals.

A network topology designed for defense in depth offers layers of protection but has no specific first or last line of defense. Regardless of the threat vector or entry point, the defense in depth network allows for the deterrence, detection, defense, and response and recovery from an event. These techniques can be applied to both on-premise and cloud-hosted environments.

Risk mitigation begins with understanding the threats and potential consequences. “One size fits all” cannot apply when it comes to cybersecurity in OT systems. Each utility must perform its own analysis and must do so with openness and honesty. It takes commitment from organizational leadership to develop a vision of how OT systems will be leveraged within the utility. Policies and procedures must enforce the vision including risk-informed engineering. Budget and staff need to be committed to implement, monitor and maintain the systems to achieve the vision within acceptable risk tolerance.

In conclusion, disaster recovery and emergency response plans must be developed for when an event occurs. Risk cannot be eliminated, only mitigated to within acceptable tolerances, and disasters do not arrive when it is convenient. Finally, since risks and threats are continuously evolving, risk management must also be incorporated as a continuous lifecycle, requiring utilities to review and update risk mitigations for changes in risk tolerance or threat vectors on an ongoing basis.

Contact David Brearley at **david.brearley@hdrinc.com,**
+1 (704) 338-6853 for more information.