Achieving Visibility and Control in OT Systems: Remote Maintenance, Securing Remote Access, and the Zero-Trust Approach

By Erik Peterson, Cybercore Integration Center, Idaho National Laboratory

Operational Technology (OT) systems are critical to the functioning of many industries, ranging from manufacturing to utilities. As the convergence of Information Technology (IT) and OT systems accelerates, the need to secure these systems becomes increasingly important. Remote maintenance and secure remote access are practical steps to achieve visibility and control in OT systems, working for both internal and third-party Service Level Agreement (SLA) vendors.

As organizations continue to rely on OT systems to streamline operations, they also face significant cybersecurity risks. The consequences of a successful cyberattack on an OT system can be devastating, including production shutdowns, equipment damage, and even threats to human safety. The interconnectedness of IT and OT systems has only amplified these risks, making it crucial for organizations to implement robust security measures to protect their critical infrastructure.

The increased reliance on remote work in the wake of the COVID-19 pandemic has further highlighted the need for secure remote access to OT systems. With employees accessing these systems from remote locations, the risk of unauthorized access and data breaches has risen significantly. As such, organizations must implement secure remote access protocols that ensure only authorized personnel can access their OT systems, and data transmissions remain secure. In this paper, we will explore the challenges associated with securing remote access to OT systems and provide practical solutions to mitigate these risks.

Remote Maintenance and Securing Remote Access in OT Systems

When building a new OT network internally, organizations can incorporate remote maintenance and secure remote access from the ground up. This involves implementing strong access controls, multi-factor authentication, secure communication channels, and ongoing monitoring (Stouffer, Pillitteri, & Lightman, 2015). For retrofitting an existing solution, organizations must first assess their current network, identify vulnerabilities, and develop a plan to address these weaknesses. This may involve updating hardware, software, and network infrastructure to support secure remote access and maintenance.

Remote maintenance and secure remote access are critical components of ensuring the efficient functioning of OT systems. However, these processes can also introduce several challenges, particularly when it comes to securing the remote access pathways. This section explores some real-world examples of problems related to remote maintenance and securing remote access in OT systems.

One notable example is the cyberattack on the Ukrainian power grid in December 2015. In this attack, the hackers gained access to the control systems of three power distribution companies through phishing emails that contained malicious attachments. Once inside the system, the attackers were able to carry out a coordinated attack that resulted in a power outage for over 200,000 customers. The attack was made possible by the lack of proper security controls in the remote access pathway used by the power grid operators.

Another example is the NotPetya ransomware attack that affected several multinational corporations, including the pharmaceutical company Merck, in June 2017. The attackers were able to gain access to Merck's network through a vulnerability in the company's remote access tools. Once inside the system, the ransomware spread rapidly, encrypting critical files and disrupting the company's operations for weeks. The attack highlights the importance of securing remote access tools and implementing proper access controls.

Finally, in 2020, the COVID-19 pandemic forced many organizations to shift to remote work, including those that rely on OT systems. This shift has increased the use of remote access pathways, making them more vulnerable to cyberattacks. In one example, a ransomware attack targeted a major US pipeline company in May 2021, causing a shutdown of its operations for several days. The attack was traced back to a vulnerability in the company's remote access pathway, highlighting the need for robust security controls in these pathways.

For third-party SLA vendors, organizations should establish clear expectations and requirements regarding the security of remote access and maintenance. Vendors should provide secure communication channels, access controls, and robust monitoring systems. Additionally, organizations should conduct regular security audits of the vendor's infrastructure to ensure compliance with industry standards and best practices (Almulla et al., 2020).

When comparing internal vs. third-party SLA vendor network security requirements, consider the following aspects:

Access Control:

- Internal: Organizations can implement and manage their own access control policies and systems.

- Third-party: Organizations must ensure the vendor complies with the organization's access control requirements and follows best practices.

Authentication and Authorization:

- Internal: Organizations have full control over user authentication and authorization mechanisms.
- Third-party: Organizations must verify the vendor uses strong authentication mechanisms (e.g., multi-factor authentication) and enforces least-privilege access.

Network Segmentation:

- Internal: Organizations can design and implement their own network segmentation strategy.
- Third-party: Organizations should ensure the vendor's network is adequately segmented and isolated from other clients' environments.

Security Monitoring and Incident Response:

- Internal: Organizations can deploy their own security monitoring and incident response systems, tailored to their specific needs.
- Third-party: Organizations must verify the vendor has robust security monitoring and incident response capabilities, and that those capabilities meet or exceed the organization's expectations.

Security Updates and Patch Management:

- Internal: Organizations have full control over their security update and patch management processes.
- Third-party: Organizations must ensure the vendor regularly applies security updates and patches to infrastructure.

Compliance and Auditing:

- Internal: Organizations can perform their own security audits and ensure compliance with industry standards and regulations.
- Third-party: Organizations must verify the vendor's compliance with industry standards and regulations and may need to conduct regular security audits of the vendor's infrastructure.

When evaluating network security requirements for internal versus third-party SLA vendor OT systems, several aspects must be considered. These aspects include access control, authentication mechanisms, monitoring and auditing, incident response, and risk management.

Access control is critical for securing OT systems, and organizations must implement appropriate controls to ensure only authorized personnel can access the systems. Internal systems may have a more straightforward access control framework, as the organization has complete

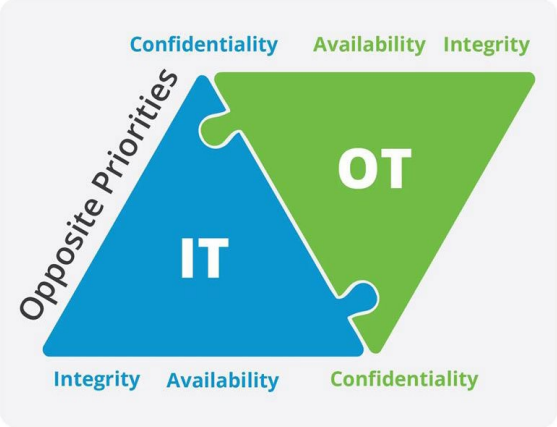

Figure 1. – The information security CIA Triad (Confidentiality, Availability, Integrity).

control over the user accounts and access permissions. In contrast, third-party vendors may have a more complex access control framework, requiring the organization to rely on the vendor's authentication mechanisms and access controls. The use of multi-factor authentication and role-based access controls can help mitigate the risks associated with unauthorized access.

Monitoring and auditing are also essential for maintaining the security of OT systems. Organizations should implement real-time monitoring to detect anomalous behavior and security events. Additionally, audit logs should be maintained to track access and system activity. Internal systems may have more comprehensive monitoring and auditing frameworks, as the organization has direct control over these processes. In contrast, third-party vendors may have limited monitoring and auditing capabilities, requiring the organization to rely on the vendor's reporting and logging mechanisms.

Incident response is another critical aspect to consider when evaluating network security requirements. In the event of a security incident, organizations must have appropriate incident response plans in place to minimize the impact of the incident. Internal systems may have more robust incident response frameworks, as the organization has control over the response process. In contrast, third-party vendors may have limited incident response capabilities, requiring the organization to rely on the vendor's response plans and procedures.

Finally, risk management is a critical aspect of securing OT systems. Organizations must implement appropriate risk management practices to identify and mitigate potential risks. Internal systems may have more comprehensive risk management frameworks, as the organization has direct control over the risk management process. In contrast, third-party vendors may have limited risk management capabilities, requiring the organization to rely on the vendor's risk management practices and procedures.

Implementing the Zero-Trust Approach in OT Systems

A zero-trust approach involves treating every user and device as a potential threat, requiring constant verification and least-privilege access control to resources. This approach can enhance security in OT systems by minimizing the attack surface and reducing the likelihood of unauthorized access (Gilad, 2020).

In a zero-trust model, all access requests are continuously evaluated and monitored for risk, even if the user or device has previously been authenticated. This approach helps to detect and respond to any suspicious activity or anomalies that may indicate a security breach. By implementing continuous monitoring and real-time analytics, organizations can quickly identify and mitigate threats, minimizing the potential damage and reducing the time to recover from a security incident.

Another important aspect of the zero-trust approach is the use of encryption to protect data in transit and at rest. Encryption helps to prevent unauthorized access to sensitive information by ensuring only authorized users with the appropriate encryption keys can access the data. Additionally, data encryption can also help to protect against data theft or loss due to physical theft, accidental loss, or cyberattacks. By implementing a zero-trust model with strong encryption, organizations can significantly reduce the risk of data breaches and protect critical OT systems and assets from potential threats.

Assessing Current OT Systems

To implement a zero-trust approach, organizations should first assess their existing OT systems to understand the risks and vulnerabilities. This includes evaluating network architecture, hardware, software, and communication protocols. Vulnerabilities should be addressed to establish a strong foundation for the zero-trust implementation.

“Zero Trust” is an approach to cybersecurity that assumes all users and devices, whether inside or outside the network perimeter, are potentially malicious and should not be trusted by default. This approach has gained increasing attention in recent years, particularly in the context of OT systems, where traditional perimeter-based security measures are often insufficient. In this section, we explore the implementation of the zero-trust approach in OT systems.

One study by Katsaros et al. (2021) proposes a zero-trust architecture for securing Industrial Control Systems (ICS), which are a type of OT system. The architecture consists of several layers, each with its own security controls, such as firewalls, intrusion detection systems, and access control mechanisms. The authors argue the zero-trust approach can help mitigate the risks associated with insider threats, supply chain attacks, and other types of advanced persistent threats.

Another study by Njilla and Sallabi (2021) proposes a zero-trust framework for securing remote access to OT systems. The framework includes several components, such as identity and access management, multi-factor authentication, and continuous monitoring. The authors argue the zero-trust approach can help organizations mitigate the risks associated with remote access, including unauthorized access and data breaches.

A third study by Roy et al. (2020) proposes a zero-trust architecture for securing critical infrastructure, which includes OT systems. The architecture consists of several layers, including network segmentation, identity and access management, and threat intelligence. The authors argue the zero-trust approach can help organizations mitigate the risks associated with cyberattacks, including ransomware attacks and data exfiltration.

Designing Zero-Trust Architecture

Next, organizations should design a zero-trust architecture, focusing on segmentation, access control, and continuous monitoring. This includes implementing micro-segmentation, enforcing least-privilege access, and deploying security solutions that monitor user and device behavior in real-time (Stouffer et al., 2015).

A zero-trust architecture for OT systems would include several layers of security controls designed to protect against both insider and outsider threats. These layers could include:

- Identity and access management: This layer would include measures such as multi-factor authentication and identity verification to ensure only authorized users are able to access the system. This layer would also include access control mechanisms that restrict access to specific resources based on the user's role and permissions.
- Network segmentation: This layer would involve breaking up the network into smaller segments and controlling traffic between them. This helps to limit the impact of a potential breach by containing it within a single segment. Network segmentation can be accomplished through techniques such as virtual local area network (VLANs), firewalls, and virtual private networks (VPNs).
- Threat intelligence: This layer involves using advanced analytics and machine learning to detect and respond to potential security threats in real-time. Threat intelligence can be used to detect anomalies in network traffic, identify potential breaches, and generate alerts for security teams.
- Secure remote access: This layer involves implementing secure remote access protocols, such as virtual desktop infrastructure (VDI) and remote desktop

protocol (RDP), to ensure only authorized personnel can access the OT system from remote locations. This layer would also include measures such as VPNs and multi-factor authentication to protect against unauthorized access.

As OT systems become more interconnected and exposed to cyber threats, organizations must take proactive steps to ensure their security. Implementing remote maintenance and secure remote access, as well as adopting a zero-trust approach, can significantly enhance the visibility and control of OT systems.

In addition to implementing remote maintenance and secure remote access, organizations must also prioritize regular security assessments and audits to ensure the continued protection of their OT systems. Conducting routine assessments can help identify potential vulnerabilities and gaps in the system that can be exploited by cybercriminals. Additionally, performing audits can ensure security controls are properly implemented and adhered to, and any issues or weaknesses are promptly addressed.

Another important consideration for OT system security is employee training and awareness. Organizations must invest in educating their staff on potential cyber threats and how to identify and respond to them. Regular training and awareness programs can help employees understand the importance of security and their role in protecting the organization's critical infrastructure. This can also help prevent human error, which is often a significant contributing factor to security breaches in OT systems. By implementing a comprehensive security training program, organizations can create a security-focused culture and mitigate the risk of cyber threats to their OT systems.

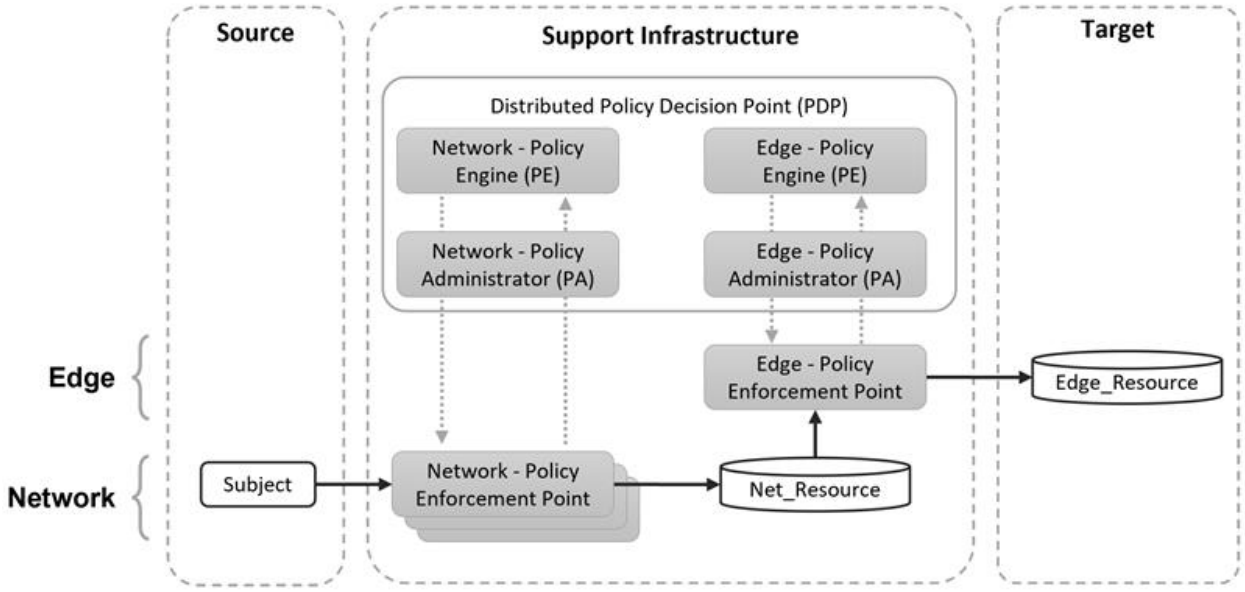

Figure 2. – Zero-trust diagram.

References

S. Almulla, Y. Iraqi, and A. Jones, "Review of security challenges, attacks and potential solutions in smart grid networks," IET Smart Grid, vol. 3, no. 2, pp. 202-215, 2020.

Y. Gilad, "Zero trust security for OT networks," in Industrial Cybersecurity, Cham, Switzerland: Springer, 2020, pp. 291-312.

Stouffer, K., Pillitteri, V., Lightman, S., et al., "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg, MD, 2015.

ISA/IEC. (2020). ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems Security. International Society of Automation / International Electrotechnical Commission.

SANS Institute, "Securing Industrial Control Systems: A Unified Security Model," SANS Institute, 2021.

H. S. Nye, "How hackers attacked Ukraine's power grid," IEEE Spectrum, vol. 53, no. 2, pp. 26-31, Feb. 2016.

E. A. Boyle, "Why the NotPetya cyber-attack is a wake-up call for companies," IEEE Spectrum, Jun. 28, 2017.

S. J. Vaughan-Nichols, "Ransomware hits Colonial Pipeline, forcing closure," ZDNet, May 10, 2021.

S. S. Osterman, "Access control for critical infrastructure: Best practices for securing OT environments," IEEE Security & Privacy, vol. 17, no. 1, pp. 42-51, Jan/Feb. 2019.

S. S. Osterman, "OT security monitoring and auditing: Best practices for securing critical infrastructure," IEEE Security & Privacy, vol. 16, no. 5, pp. 39-47, Sep/Oct. 2018.

T. M. Chen and C. H. Chu, "An adaptive framework for incident response in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 14, no. 4, pp. 1614-1624, Apr. 2018.

J. C. Miller, "A risk management framework for critical infrastructure protection," IEEE Security & Privacy, vol. 10, no. 6, pp. 62-67, Nov/Dec. 2012.

Katsaros, K. V., Tsoumas, B. D., & Douligeris, C. (2021). A Zero-Trust Architecture for Securing Industrial Control Systems. IEEE Transactions on Industrial Informatics, 17(2), 1174-1182.

Njilla, L., & Sallabi, F. (2021). Zero Trust Framework for Securing Remote Access to Operational Technology Systems. International Journal of Advanced Computer Science and Applications, 12(1), 7-17.

Roy, S., Sarkar, A., & Das, S. K. (2020). Zero Trust Architecture for Securing Critical Infrastructure. International Journal of Computer Science and Information Security, 18(11), 73-80.

C. Szegedi, "Zero Trust Architecture - A Modern Security Model for the Digital Enterprise," Acta Polytechnica Hungarica, vol. 16, no. 2, pp. 157-176, 2019.

Y. Chen, X. Zhang, and M. Zhou, "Zero-Trust Architecture: A Comprehensive Survey," IEEE Access, vol. 7, pp. 101042-101062, 2019.

S. Yoo, J. Ahn, and J. H. Park, "Zero-Trust Security Architecture Based on Threat Intelligence for the Industrial Internet of Things," IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4057-4064, 2020.

K. V. Katsaros, B. D. Tsoumas, and C. Douligeris, "A Zero-Trust Architecture for Securing Industrial Control Systems," IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 1174-1182, 2021.