Original Article
Received/Accepted Dates
11.05.2023/15.07.2023
DOI 10.52096/usbd.7.30.33

International Journal of Social Sciences
Uluslararası Sosyal Bilimler Dergisi
www.sobider.net **ISSN: 2548-0685**

Integrating Cyber Resilience Strategies for OT Data Acquisition Devices

Noe Nevarez
Computer Science Department
Sam Houston State University, Huntsville, United States
nnevarez@shsu.edu

Yeşim Ülgen Sönmez
Dept. of Software Engineering
Faculty of Technology, Fırat University, Elazığ, Türkiye
phdyus@gmail.com, **ORCID:** 0000-0002-2090-0263

Abstract

Operational Technology (OT), Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA) devices have been around in some form since the 1960s and they control specific functions in many critical industries such as electrical power generation, oil refineries, and water treatment plants. Since most are integrated with IT-based protocols (e.g., TCP/IP), there has been an explosion of OT control systems to provide meaningful information to businesses. While OT and IT speak a common language, this has exposed OT to much more Cyber Attacks that were once applied only to IT-based systems. Data Acquisition Devices (DAS), such as those manufactured by Moxa, now have ethernet ports to provide this link between both networks. The combination of new ethernet-capable OT devices, and those using upgraded converters (e.g., Moxa) for older OT devices, has primarily increased the attack surface. This study proposes a secure layered architecture that can be deployed to limit security threats for ethernet-capable (DAS) devices. The current state of many organizations is the lack of visibility of their OT assets and a knowledge gap on how to secure them.

Keywords—Control systems, Cyber attacks, Cybersecurity resilience, Operational technology

Operasyonel Teknoloji Veri Toplama Cihazlari İçin Siber Direnç Stratejilerinin Entegrasyonu

Özet

Operasyonel Teknoloji (OT), Endüstriyel Kontrol Sistemleri (EKS) ve SCADA cihazları, 1960'lardan beri bir şekilde ortalıkta dolaşmaktadır ve elektrik enerjisi üretimi, petrol rafinerileri ve su arıtma tesisleri gibi birçok kritik endüstrideki belirli işlevleri kontrol ederler. Çoğu BT tabanlı protokollerle (ör. TCP/IP) entegre olduğundan, işletmelere anlamlı bilgiler sağlamak için OT kontrol sistemlerinde bir patlama oldu. OT ve BT ortak bir dil konuşsa da bu, OT'yi bir zamanlar yalnızca BT tabanlı sistemlere uygulanan Siber Saldırıların çok daha fazlasına maruz bıraktı. Moxa tarafından üretilenler gibi Veri Toplama Cihazları (VTC), artık her iki ağ arasında bu bağlantıyı sağlamak için ethernet bağlantı noktalarına sahiptir. Yeni ethernet özellikli OT cihazları ile eski OT cihazları için yükseltilmiş dönüştürücüler (örn. Moxa) kullananların kombinasyonu, öncelikle saldırı yüzeyini artırdı. Bu çalışma, ethernet özellikli (VTC) cihazlar için güvenlik tehditlerini sınırlamak üzere konuşlandırılabilecek güvenli, katmanlı bir mimari önermektedir. Birçok kuruluşun mevcut durumu, OT varlıklarının görünür olmaması ve bunların nasıl güvence altına alınacağına dair bilgi eksikliğidir.

Anahtar Kelimeler—Kontrol sistemleri, Siber saldırılar, Siber güvenlik dirençliliği, operasyonel teknoloji

1. INTRODUCTION

This study will be referring to OT/ICS/SCADA (Cook, Marnerides, Johnson & Pezaros, 2023; Hahn, 2016; Khadpe, Binnar & Kaz, 2020; Mubarak, Habaebi, Islam & Khan, 2021; Sangkhro & Agrawal, 2023; Sonkor & Soto, 2021) as OT for simplicity. ICS refers to control systems used in industrial processes and are often used in several critical infrastructure industries. Automation and control systems such as SCADA, Distributed Control Systems (DCS) are often referred to as OT. These systems are used to monitor and control critical infrastructures such as electricity, pipelines, water distribution, sewer systems and production control (Murray, Johnstone & Valli, 2017). Previously ICS were and therefore isolated from the outside world, making them less susceptible to cyber-attacks. But over the years, more and more components of the ICS environment have been

connected to the internet as well as the corporate network for convenience and accessibility. This has now exposed such systems to the same threats IT faces. However, cyberattacks against ICS can cause much greater physical damage. Therefore, there is a need to evaluate the current cyber security scenario in the ICS environment (Cook et al., 2023). Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology security (Galinec & Steingartner, (2017).

There has been a separation of IT and OT in terms of infrastructure and the staff that supports them. The main reason for this disparity is the unique knowledge base required and the operational requirements to manage OT. The goals of IT and OT are also different from a security and operations perspective. Both comply with the established CIA principle for securing their environment. However, the IT worker is mainly concerned with Confidentiality, Integrity, and Availability, in that order. The OT worker is mainly concerned with Availability that ensures uninterrupted operations. One contributing factor to Availability being the priority is that OT devices are used in many critical infrastructures where there is a high cost associated with system failures and the loss of life. Many organizations have inadequate OT digital protection and do not have the controls that are the normal point in IT organizations such as dashboard design, contingency courses, access control strategy, and verification strategy. OT framework administrators are primarily concerned about the availability and reliability of the framework, and less concerned about security in light of the fact that OT frameworks are verifiably limited to IT organizations (Sriram et al., 2023).

Most OT devices are built for operational efficiency, effectiveness, and stability. They are not built with security in mind, so security staff is often at a disadvantage when securing the OT environment and uses IT-based methods to protect systems which often causes undesirable results. For example, staff may try to use traditional scanning methods that use the TCP/IP to identify OT assets and vulnerabilities. The problem is that OT devices are quite diverse are use a variety of protocols to communicate and operate. So, the scan results can identify little to none of the devices unless there using IT-based protocols such as TCP/IP. Another problem is that IT scanners use "active" techniques to cause OT equipment to freeze, reset, reboot, or crash.

The OT Management tools of Today do not take into account Original Equipment Manufacturer (OEM) specific operating requirements. The tool would have to import this information from each

vendor, which is currently not widespread Today. Also, every region (*e.g., North America, South America, Europe, etc*.) may be governed by a different regulatory body for their electric utility industry. In North America, we use the North American Electric Reliability Corporation (NERC) to promote and ensure the reliability and adequacy of the electric utility system. Current OT Management tools are not built for compliance checks with NERC or any other governing body. This is a significant difference between what is available for IT compliance (e.g., NIST, PCI-DSS). The OT Service Management (OTSM) Model needs to be understood and how it differs from the ITSM. Only then can support staff offer secure solutions to protect OT-based components.

Today, older OT devices are becoming capable of communicating across Networks of all types. Data Acquisition Devices (e.g., Moxa 5100 Series) now have integrated ethernet ports which allows them to communicate across OT-to-IT network boundaries. The problem is that these devices do not support secure methods of data exchange or use secure protocols for remote management. For example, specific MOXA devices only support the Telnet for remote configuration. It is widely known that Telnet is an insecure application where the traffic is sent and received is readable in cleartext. Moxa devices are also web-enabled, using an HTTP server with a basic authentication webpage. It has been discovered that the passwords are stored using insecure hashing methods that a motivated hacker can easily crack. The Moxa support team does not have security patches readily available, so it lies on the security practitioner to formulate a solution to mitigate potential security threats.

2. LITERATURE REVIEW & BACKGROUND

This section provides an overview of different approaches to test and secure OT system components. In (Conklin, 2016), the author introduces a new metric, resilience, into the CIA Model. Resilience is the ability to handle system failures and disruptions to its critical processes. While resilient technologies are implemented in the context of operations, it is not for security. OT is thought of as less involved since they have long retention (i.e., 20 to 30 years) in the production environment. Thus, many OT devices are not networked capable and use older serial-based interfaces to communicate with monitoring stations. The US government has created documentation standards (i.e., NIST 800{53, 82, 160}) to provide guidelines implementing security

controls, layered security architecture, and developing cyber-resilient systems. The Department of Homeland security has its Cyber Resiliency Review model (C.R.R.) that advises how people can structure their security activities to manage resiliency better (Conklin, 2016). Examples of attacks were discussed involving a Water Treatment Plant, where the attacker was able to hack into the OT management system and change the levels of sodium hydroxide that would have poisoned people. Luckily, there were procedures to check the water later in the process. A resilient cyber strategy could have been deployed to better monitor and recover from such an event.

The study Cyber Security in the Energy World (Chee & Utomo, 2017) examines the changes in electric grid technologies as countries mitigate from the traditional power grid to the new Smart Digital Power Grid. The change into digital also means system components are more susceptible to cyber-attacks. One infamous attack occurred in the Iranian Nuclear Power Plant (a.k.a Stuxnet). The Stuxnet worm was inserted into an open USB port and targeted Data Acquisition Systems (DAS). The worm changed the system's parameters to spin the gas centrifuge faster than their actual operating limits. The authors also examine the importance of segregating power systems into different domains to ensure issues only affect one domain and not affect others (Chee & Utomo, 2017). This physical and logical segregation is considered the best practice for security. One example where an attack on an IT asset spilled over to the OT environment occurred in the Ukraine Power Grid Attack of 2015. In this case, the IT asset was the management system for reading data from the OT environment. The attacker used a method called Bad Data Injection (BDI), where the target gets false data into the DAS to either steal energy or induce a false response by the management system. Implementing a physical and logical separation strategy may have prevented this attack from the start.

In (Hupp, Hasandka, Carvalho & Saleem, 2020) the authors offer a new open source hardware security module that improves both information and operational security to better protect data and communications in the distribution network. This module improves system security through encryption, authentication, authorization, certificate management, and user access control. The main advancement of Module-OT is the addition of hardware encryption acceleration, which improves overall communication performance in terms of end-to-end latency (Hupp et al., 2020).

In (Maralli, Sudarsan & Ashok, 2019), the authors explain the fundamental differences and cyber threat impacts between OT and IT assets. OT technologies are designed to run (27/7/365) to support

the business needs. The costs of deploying risk-limiting safeguards outweigh the costs of recovering from a cyber-attack in an OT environment. A structured framework, like those offered by the government (e.g., NIST) or organizations such as ISA, ISO, or IEEE, can help determine weak spots in your infrastructure and suggest possible controls to limit risk. For example, performing routine security assessments is a must to verify compliance and identify security threats. Having a solid Vulnerability Management Program (VMP) will help identify OT and IT assets in your environment and help detect critical vulnerabilities and propose remediation solutions. Cyber-attacks on OT components have occurred in Sewage Treatment Plants, Rail Control Systems, Water Utilities, and Nuclear Power Plants. In all four attacks, the control systems were hacked to induce different responses by the SCADA Management System. The impacts were severe and caused significant damage to hardware and surrounding areas.

The Oldenburger Institute of Information Technology (OFFIS) did a test case using virtualized OT components to simulate real-world scenarios (Ansari, Castro, Weller, Babazadeh, Lehnhoff, 2019). The virtualized environment provided a testbed for OT functions and simulated cyberattacks. OFFIS took on this project after reading proposals from the US Department of Energy, where the agency was looking to develop a better Industrial Sensor. The requirements were to allow the continuous collection of sensor data, integrate with intelligent applications, and provide monitoring capabilities where cyberattacks could be detected. Three main components were virtualized:

- Remote Termina Unit (RTU.)
- Intelligent Electronic Device (IED.)
- Programmable Logic Controller (PLC)

The Remote Terminal Unit (RTU) has sensors for gathering data at various locations. The Intelligent Electronic Device (IED) provides automation logic, and the Programmable Logic Controller (PLC) provides continuous monitoring and makes decisions based on configured parameters. Protocols that are common to DAS devices are also simulated to facilitate Denial-of-Service attacks. All attacks were successfully executed and analyzed using the monitoring functions of the testbed. The virtualized environment is considered a significant step in understanding how OT devices function in electric power industries.

Modern Firewalls combine multiple prevention layers in their software suite to better protect data entering or leaving its interfaces. They are called Next Generation (NG.) Firewalls and combine

Stateful inspection, intrusion prevention, Layer 0-to-7 visibility, and can integrate with various third-party intelligence sources. In (Nyasore, Zavarsky, Swar, Naiyeju & Dabra, 2020), the firewall has all these features and can perform Deep Packet Inspection (DPI), which means it can also look at the payload. A layered security model is a requirement to help mitigate attacks that can slip through your defenses. Modbus is a common protocol used for communications between OT devices and management stations. Modbus was not built with security in mind, so many forms of attacks a hacker can execute. Therefore, it is essential to have a Next-Generation Firewall that can perform DPI as one of your security layers. Each study discussed common threats to OT environments and offered possible techniques and mitigation strategies to limit the damage when an event happens. Notice I said limit and not prevent. The reality is that no matter if you do everything right with securing your organization, there will still be about 5 to 10% of attacks that get through. However, implementing a layered security model and having competent security staff help identify those threats.

3.MULTI-LAYERED RESILIENT ARCHITECTURE

A layered approach has been documented in *NIST 800-82* – (Guide to Industrial Control Systems (ICS)) and is listed as the preferred architectural approach by the Department of Homeland Security (DHS). DHS performs Cyber Resilient Reviews (CRR) to evaluate an organization's operational resilience and cybersecurity (Alahmari, 2023). practices. The CRR analyzes resilience across ten domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness

10. Situational Awareness

The assessment report contains questions and answers according to industry best practices. Each domain is detailed in supplementary documentation that will guide security practitioners according to areas of weak development.

4. PROPOSED ARCHITECTURE FOR MOXA DAS

Modern DAS devices are now capable of communicating with the IT network. The benefits are that the business can retrieve essential data from their DAS devices to analyze trends and make strategic decisions for the future. We can deploy a Defense-in-Depth strategy to secure the data and OT management system (Fig. 1). The attacker will have to penetrate multiple components before they have access to the target asset.

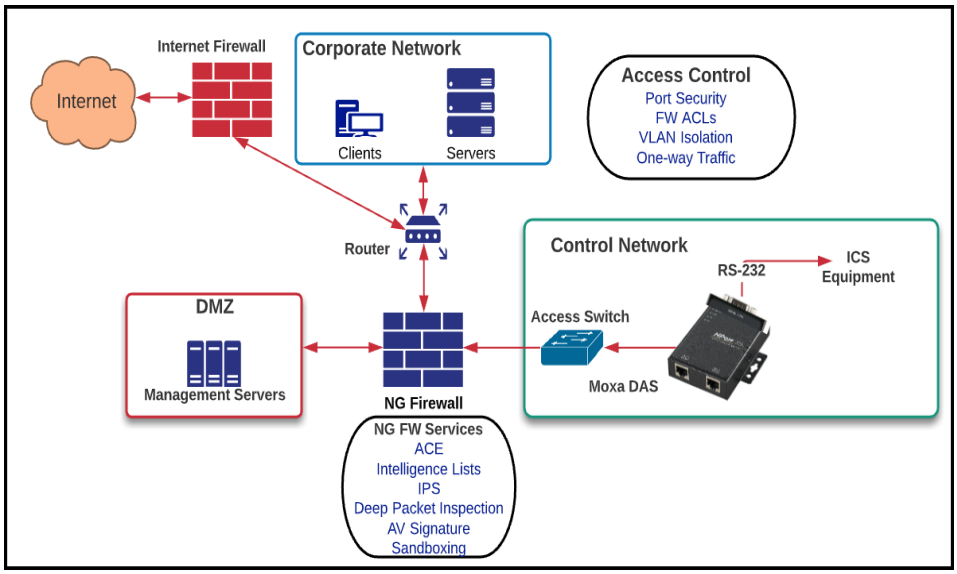

Fig. 1 Defense-in-Depth Architecture

The control network will contain Moxa DAS devices distributed across the company. These devices will be statically assigned an IP address in a dedicated VLAN for OT-only devices. This provides network segmentation and allows for greater access control by configuring a standard policy that gives a granular level of access. The Moxa DAS will be connected to an assigned network port on a switch with Port Security configured and logic (e.g., FW ACLs) so that traffic is only allowed

one-way, from Control Network to OT Management Device. All other switch ports are locked down and disabled. The Switch is physically secured and configured using an Access Control Server (e.g., Cisco ACS or ISE)

The Switch is connected to Next-Generation Firewall (NG-FW), which most mid-to-large organizations have available. The NG-FW has multiple interfaces configured in zones to isolate traffic only to their source zone. There will be zones for the Control Network, DMZ, and Corporate Network. Policy rules are created that specify what traffic can transverse the zones and to what destinations. The rules must be precise and include IP and service port information. Policies are then assigned to the policy rules that provide additional services: (IPS, DPI, AV, Anti-Spoofing). The NG-FW will be configured to pull real-time intelligence information from their intelligence repository and those from 3rd parties.

The DMZ zone will be an intermediary network that sits between both Corporate and Control zones. The OT Management device or SCADA controls The DMZ network is placed between the two firewalls so that any attacks would have to go through one firewall and then another that is hardened further. Management devices that provide services to corporate and control zones and publicly across the Internet can benefit from the DMZ. However, keeping all DMZ devices up-to-date with updates and patches is necessary to keep risk low.The router can handle heavier traffic loads and filters the traffic going to the Control Network NG-FW for traffic destined to the DMZ or Control Zones. This router provides packet filtering services using ACLs that restrict traffic based on Network IP or service ports. They also have features for blocking Denial of Service attacks, which adds another layer of security to our Network. The router has a connection out to the Internet firewall for those assets that are allowed. At no time will the Control Network have/need access to the Internet. Lastly, there needs to be a central data repository for each key component to send their security logs (e.g., SIEM). A security information and event management (SIEM) appliance should be deployed within this architecture to collect all logs and alert security staff for any suspicious activity. The only traffic allowed to the SIEM should be log traffic coming from allowed sources.

5. PENETRATION TESTS AND RESULTS

The proposed OT architecture was implemented in a medium-size company (1,500 users) that contained both IT and OT assets. The company underwent a penetration test by an outside security firm using the attack methodology shown below:

- Passive Recon
- Active Recon
- Network Attacks
- Application Attacks
- Black Box Attack

The reconnaissance starts by using passive techniques using information that was readily available over the Internet. This includes DNS information, externally accessible webpages using web crawlers, information repositories (e.g., shodan), and Social Media sites. Next, using active reconnaissance techniques using Vulnerability Scanners and custom scripts that try to find weaknesses. If weaknesses are found, a hacker can exploit them to gain access (a.k.a., Initial foothold). A Blackbox Attack occurs by an attacker finding a way to plug into your Network and start attacking without previous knowledge of the target.

The attacker was not able to penetrate the Control Network or DMZs. The log information that was gathered from the SIEM was able to alert support teams to their presence and notify the security team. A Denial-of-Service (DoS) attack was initiated by the Blackbox internally and was prevented by the router before even getting to the Control Networks NG-FW. The layered approach has kept the control environment secure from attacks since its implementation. The enhanced device logging has provided verbose log information for all traffic entering and leaving.

6. FUTURE OF OT MANAGEMENT

There are many changes needed to current OT management tools to provide organizations with the services that support the infrastructure's needs. First foremost, a tool needs to be able to discover all OT assets, no matter the vendor. With so many vendors using proprietary hardware and

protocols, it is difficult management tools to be equipped with plugin modules that identify the functions for every OT system component. Next, the tool needs to be able to identify devices across all layers of the OSI model (0-7). For example, many legacy devices are still running on serial interfaces (Layer 0). The tool needs to be able to identify serial assets in this situation. Lastly, many OT infrastructures are subject to regulatory requirements (e.g., NERC CIP, NIST) for operational security. The Electric Utility industry uses the North American Electric Reliability Corporation (NERC) to promote electric utility systems' reliability and power transmission in North America. Today's tools lack the integration of NERC regulatory requirements to automate configuration findings, and align those with NERC, and provide reporting documentation.

7. CONCLUSION

The knowledge required to understand what is needed to provide security for OT infrastructure is time-consuming but necessary. The tested architecture can be modified in many ways to increase the layers of security, but this will be based on the companies' objectives, budget, and technical support. IT Service Management (ITSM) tools are still considered much more evolved than OTSM, but I believe the gap is closing. With the attacks on OT, assets are rising dramatically, and leading security management vendors like Tenable are developing the next generation of OT Management Systems (e.g., Tenable. ot). Other mainstream vendors in this space will start to follow their lead.

Acknowledgment

The authors of this paper extend their appreciation to Dr. Cihan Varol for his contribution.

REFERENCES

Alahmari, M.S. (2023). *The Implications Of IT/OT Convergence Proposed By Industry 4.0 Model On The Current OT Cybersecurity Frameworks*, PhD Thesis, Marymount University, USA.

Ansari, S. Castro, F. Weller, D. Babazadeh, D. Lehnhoff, S. (2019). Towards Virtualization of Operational Technology to Enable Large-Scale System Testing, *IEEE EUROCON 2019 -18th International Conference on Smart Technologies*, Novi Sad, Serbia.

Conklin, A. (2016). IT vs OT Security: A Time to Consider a Change in CIA to Include Resilience, 49th Hawaii International Conference on System Sciences (HICSS) Koloa, HI, USA, 2642-2647.

Chee, G. K. Utomo, P.N. (2017). Cyber Security in the Energy World, in *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*, Singapore.

Cook, M. Marnerides, A. Johnson, C. and Pezaros, D.(2023). A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions, *IEEE Communications Surveys & Tutorials*.

Galinec, D and Steingartner, W. (2017). Combining cybersecurity and cyber defense to achieve cyber resilience, *2017 IEEE 14th International Scientific Conference on Informatics*, Poprad, Slovakia, 87-93.

Hahn, A. (2016).Operational Technology and Information Technology in Industrial Control Systems, *Cyber-security of SCADA and Other Industrial Control Systems*, 66.

Hupp, W. Hasandka, A. Carvalho, R. S. and Saleem, D. (2020). Module-OT: A Hardware Security Module for Operational Technology," *2020 IEEE Texas Power and Energy Conference (TPEC)*, College Station, TX, USA, 1-6.

Khadpe, M. Binnar, P. and Kazi, F. (2020). Malware Injection in Operational Technology Networks, *11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kharagpur, India,1-6.

Marali, M. Sudarsan, S. D. Ashok, G. (2019). Cyber security threats in industrial control systems and protection," in *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, Sathyamangalam, India.

Mubarak, S. Habaebi, M. H. Islam, M. R. and Khan, S. (2021). ICS Cyber Attack Detection with Ensemble Machine Learning and DPI using Cyber-kit Datasets, *2021 8th International Conference on Computer and Communication Engineering (ICCCE)*, Kuala Lumpur, Malaysia, 349-354.

Murray, G. Johnstone, M.N. and Valli, C. (2017). The convergence of IT and OT in critical infrastructure, *The Proceedings of 15th Australian Information Security Management Conference*, Edith Cowan University, Perth, Western Australia, 149-155.

Nyasore, O. N. Zavarsky, P. Swar, B. Naiyeju, R. Dabra, S. (2020). *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart*

Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Baltimore, MD, USA, 241-245.

Sangkhro, R. and Agrawal, A. K. (2023). Cybersecurity in Industrial Control Systems: A Review of the Current Trends and Challenges, *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, 355-359.

Sonkor, M. S. and Soto, B. G. (2021). Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective, *J. Constr. Eng. Manage*, (*147*)12.

Sriram, S. Rajeshkumar, G. Sadesh, S. Saranya, E. Saranya K. and K. Venu, K. (2023). Cyber Security Control Systems for Operational Technology, *2023, Second International Conference on Electronics and Renewable Systems (ICEARS)*, Tuticorin, India, 1-8.