Engineering and Technology Journal e-ISSN: 2456-3358

Volume 07 Issue 09 September-2022, Page No.-1471-1476

DOI: 10.47191/etj/v7i9.06, I.F. – 6.484

© 2022, ETJ

A Case Study of Industrial Control System Network Security

Michael Kinzel[1], Te-Shun Chou[2]

[1]College of Technology, Indiana State University

[2]College of Engineering and Technology, East Carolina University

ABSTRACT: This case study presented the design of an Industrial Control System (ICS). The design focused on network security using network segmentation and redundancy. The objective was to relate theoretical network defense strategies to real-world applications. This case study highlighted the logical design of network segmentations within a redundant network architecture. The study demonstrated the possibility to implement a practical application by using multiple defense strategies simultaneously.

KEYWORDS: Network Security, Cybersecurity, Industrial Control System, Network Segmentation, Virtual Local Area Network, Information Technology, Operational Technology

I. INTRODUCTION

Threats to critical Information Technology (IT) infrastructures are visibly increasing dramatically every day. What is not so visible are the increasing threats to Operational Technology (OT) systems, which are integrated with IT systems. IT threats and vulnerabilities also affect OT infrastructures. ICSs are common OT systems that provide surveillance and control of industrial operations. They are used by almost every industry globally [1].

Threats to ICSs are not the same as those posed to IT systems because they have different vulnerabilities. Although defense strategies are different for the two systems, threats from the IT domain can horizontally slide across the organization and pose an equal risk to ICSs [2]. Because of this, there is some amount of overlap between the vulnerabilities and threats to each.

Defense strategies for an ICS must protect the system from human error, insider threats, and external attacks [3]. Defense strategies for these threats can be segmented into physical security and cybersecurity. Physical security relates to physical access to the system. Cybersecurity relates to how the ICS network is accessed and linked to the internet [4]. The preferred cybersecurity defense strategy is to incorporate security by design. Two design methods to increase security of an ICS are to incorporate dual/redundant systems and to segment the system into various tiered or layered networks.

This research addressed an optimal cybersecurity approach to secure an ICS network. Having completed the case study, we have found that physical and cybersecurity best practices should include a dual/redundant network with segmented Virtual Local Area Networks (VLAN) to maximize the CIA triad (confidentiality, integrity, and availability).

This paper is organized as follows: Section 2 introduces the ICS. Section 3 presents cybersecurity threats and vulnerabilities inherent within an ICS. Section 4 describes typical defense strategies. The application of these defense strategies are then illustrated using a case study in Section 5. Finally, we conclude our work in the last section on how network security can be designed into an ICS.

II. ICS

The differences between IT systems and ICSs are important to understand since most cybersecurity organizational policies and procedures are written by IT staff and may not provide equivalent protection for the ICS [5].

A. ICSs within the OT Domain

An ICS is a specialized type of OT system that has been around for over 50 years [3]. It provides organizations the ability to monitor and control industrial processes and is widely used in many industries. Types of ICSs include Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, as well as higher level Distributed Control Systems (DCSs) and Integrated Control and Safety Systems (ICSSs) [6]. Historically, ICSs were stand-alone systems that were isolated from external networks and typically used vendor specific proprietary protocols. These older stand-alone systems were physically separated from the external environment and were immune from external attacks [3]. Even if physically separated, they were not immune from insider attacks. As OT systems are continually integrated with IT systems, it's no longer practical to use network isolation as the primary means of security.

Rudimentary ICSs are based on nano or micro class PLCs that provide surveillance and control through a dedicated local Human Machine Interface (HMI). Modern ICSs rely on commercially available operating systems, open standards such as TCP/IP, and are interconnected within an enclosed plant [7]. A SCADA or DCS not only provides local control, but remote control as well. ICSs are now commonly interconnected to remote facilities and to the business enterprise network and have inherited the same or similar cybersecurity risks as IT systems. Even at its core, a PLC is programmed using computer language, the same as a PC [8]. Despite the vast similarities between ICS and IT, there are enough differences that the CIA triad may have different priorities between the two.

B. Differences Between IT Systems and ICSs

Performance requirements are much more stringent for an ICS than for a typical IT system. Delay or jitter may be tolerable for an IT network and only pose a nuisance to business operations. High availability is desired, but not necessarily required. Data confidentiality and integrity are also highly desired. Fault tolerance is not critical. IT in general does not pose a significant business risk during unplanned, but momentary downtime [5]. On the contrary, any type of performance degradation of an ICS can cause an uncontrollable process that could lead to human injury or loss of life. The severity of downtime may be intolerable, requiring system outages to be pre-planned well in advance to ensure continued regulatory compliance, production, and employee well-being/safety [5]. Availability and integrity are much more important for an ICS than for a typical IT system.

The physical systems for IT and ICS are often be different. IT systems typically include more than the minimum necessary capacity to support advanced applications, workload, growth, and unseen contingencies. Security technologies are often designed for, and easily integrated into IT systems. If there are performance or security concerns, an IT system may be upgraded or replaced easily [5]. All of which may be generally consistent for the IT domain, but it's very specific and bespoke to each ICS. ICSs are designed for a specific process and may not come with, or even support security technologies. ICS upgrades must be done carefully, due to proprietary software, protocols, and/or algorithms developed for the specific industrial process [7].

Lastly, the technology used in an ICS may have a design life measured in decades while an IT system may have a design life measured in years [9]. The security technologies put in place for an ICS may remain with minimal modifications for the entirety of the design life cycle.

III. THREATS AND VULNERABILITIES

The ICS's process information and/or physical process is an asset to the owning organization. Any potential damage or theft of an asset is a threat. Security threats to ICSs can be segmented into internal and external threats. These threats can exploit vulnerabilities in an ICS. Isolated and stand-alone ICSs are still vulnerable to insider attacks as the attacker often has physical access to the ICS user interface [7]. Integrated and networked ICSs have a much larger vulnerability due to a lager attack surface that extends outside the physical or virtual organizational boundaries.

A. Internal Threats

Threats to ICSs can be initiated within the organization itself and are therefore referred to as internal threats. Internal threats can originate with inadvertent or careless employee actions [3]. Internal threats can also originate from intentional misuse or malicious actions. As an example, unauthorized changes to a PLC [5].

B. External Threats

Threats that originate outside of the organization, or external threats, can include malware, hacking, and even terrorism [5]. Malware is a threat based on a system's vulnerability to malicious code. Malicious code can take the form of viruses, worms, spyware, trojan horses, etc. In most cases, malware is not the result of a directed attack, because it's not specifically targeted to the organization. A hacker is an external entity that probes, intrudes, and/or attempts to control the system. Hackers are often individuals or criminal groups seeking financial gain. Common attacks use ransomware [3]. External threats can also originate from individuals or groups attempting to injure critical infrastructure. Foreign governments also probe OT networks for weak links to support "red button functionality" [3].

C. Vulnerabilities

Both internal and external threats can exploit vulnerabilities originating from insufficient or inadequate policies and procedures, or poor design [10]. Threats can negatively impact the system and organizational operation. Some of the damage can include insertion of inaccurate or harmful data, changing or deleting alarm and safety setpoints, or stealing sensitive data or intellectual property [10]. As an example, once an external hacker enters the system, they can lock-out facility operators which can stop or shut-in production. External threats can also install malware to steal information or production recipes. In worse cases, dangerous situations can emerge if setpoints or controller thresholds are changed or deleted, removing safety devices from the production facility.

ICSs share many vulnerabilities with typical IT systems but can also include unique vulnerabilities. Some unique vulnerabilities include bypass logic, brute-force attacks, and vendor specific vulnerabilities. As an example, PLCs have a main memory for their program and a register memory for process variables. Generally, PLCs grant free read/write access to the register memory. Malware can allow infected PCs to change the PLC register values if they share a common network. This is referred to as a bypass logic attack [2]. Incorrect inputs and/or outputs can cause the system to crash or behave in an unsafe manner.

IV. DEFENSE STRATEGIES

ICS defense strategies depend on how the ICS is linked to the internet or other organizational networks [11]. Strategies can focus on local security of an ICS. Local security strategies include user access (e.g., passwords and employee accounts) and system access (e.g., flash drive capability). Strategies can also focus on network security of an ICS. Network security standards for IT systems may not necessarily provide security solutions for an ICS [7]. Two common standards for ICS network security are IEC 62443 [12] and NIST SP 800-82 [1].

Security solutions provided by the IT domain and operational controls can be incorporated into the ICS [13]. Common security solutions focus on prevention (restricting access) and remediation (ensuring system can be restored easily). Additionally, ICS unique defensive strategies include a secure topology design that includes gateways, firewalls, demilitarized zones (DMZ), and system redundancy [10].

A. IT Related Defense Strategies

The IT domain can provide security for the ICS by hardening the computer systems [13]. Additionally, the IT domain can disable the use of internet applications within the ICS [5]. Another IT related defense strategy is software configuration control. Configuration control involves the ability to identify and track changes to the software as well as maintain controller code, firmware versions, and hardware configurations [3]. Configuration control does not lessen the probability of an attack but increases the ability to respond and repair damage after an attack. These and other typical IT defense strategies including security policies and procedures, limiting applications, regularly scanning for viruses, and software updates may not provide adequate cybersecurity for the ICS.

The preferred IT related defense strategy is the zonal approach, which isolates the ICS as a controlled zone within the organizational IT network [7].

B. ICS Specific Defense Strategies

ICS security normally focuses on the PLC. PLC vendors offer several specific security solutions that include the deactivation of unused ports, services, and/or networking features [7]. Another PLC security solution is to limit access control to different areas. Two common areas are configuration and runtime. Additionally, network security through firewalls and Virtual Private Networks (VPN) can be enabled and integrated into the ICS topology [7].

Defense strategies should not rely on a single strategy. A common strategy is to bundle together several defense mechanisms in a layered approach [5]. Using a layered approach, the ICS is segmented into virtual zones and each zone has different security risks and mitigations. As an example, the outermost zone is the internet, which is accessible by everyone. The next layer is the corporate network, accessible by the organization's employees. Inside the corporate network are various site networks, which are only available to the local employees at each site. If possible, the ICS should remain within the site and would only be available to operations and engineering. Each of these three zones (corporate, site, control system) within an organization can be configured with firewalls, gateways, and DMZs that are bespoke for each zone [5].

V. CASE STUDY

A large production facility's ICS network is used to study the layered (zonal) approach to ICS security. The network design included dual redundancy to maximize the availability and integrity. The design incorporated layered (tiered) networks to maximize the integrity and confidentiality. For the purpose of concentrating on the actual ICS network design, procedural controls such as user access and firewalls are omitted from the study. Additionally, the higher level zones of the site and corporate enterprise network are also omitted.

A. Network Segmentation

A VLAN divides a physical network into smaller logical networks that use a different broadcast domain but is transparent to the end user [14]. The ICS used several VLANs to segment the physical network. Although there are several VLANs, they share a common ethernet physical link. VLANs were used for network separation for two reasons. First, from a network efficiency standpoint, it reduces the bandwidth and traffic due to broadcasting. Second and perhaps most important, segmenting the network using VLANs increases security (subnets could have been used, but VLANs were chosen for ease of design). VLANs increase security because each VLAN operates under its own security policy and allowable network traffic.

Segmentation improves the ICS integrity and availability. Any ICS controller or end device that lacked authentication protocols was segregated on its own VLAN. Integrity was maximized because these VLANs were isolated from inadvertent or malicious modification. Availability was maximized because a complete failure of any single VLAN did not prevent the system from safely shutting down.

The production plant's ICS is segmented into five VLANs labeled A through E:

- Management Network (A): Managerial functions, housekeeping, and configuration of the network and network devices.
- Control Network (B): Provides the information pathway between the PLC and PC servers.
- Process I/O Network (C): Transfers the Process Control System (PCS) Input/Output (I/O) data.
- Safety I/O Network (D): Transfers the Safety System I/O data.
- Supervisory Network (E): Transfers the HMI data to operator workstations/clients.

B. Redundancy

The ICS is completely redundant using system duality that maximizes system availability. Functionality is split between the PCS and Safety System. The PCS provided real time monitoring and control capabilities for facility operations. A separate safety system provided safety critical functionality during an abnormal process. Splitting out these two functions prevents system failures that occur in one system from affecting the other. Additionally, the safety system is Fail Safe, meaning that any hardware or network failure will cause the process to automatically revert to a safe state. As an example, the process variable "pressure" may be monitored by two pressure controllers, one for normal operations and a second pressure controller for safety functionality that only includes Pressure Safety Low (PSL) or Pressure Safety High (PSH) thresholds to prevent an unsafe condition.

Redundancy by duality included the use of two separate sets of hardware (arbitrarily designated as A and B or 1 and 2). The PCS included two PLCs, one that always runs as the Duty PLC and a secondary fail-over PLC that runs as Standby. The safety system also included two PLCs in a Duty/Standby configuration. In addition to the dual/redundant PLCs, the I/O switches included a Parallel Redundancy Protocol (PRP) ethernet protocol that automatically duplicated each packet for both of the physically separated PRP LANs "A" and "B".

Network redundancy improved the ICS availability and integrity. Availability was maximized because single point failures cannot cause system failure. Further, separate process and safety functions eliminate the ability of a complete failure of one system to cause complete ICS failure. Integrity was maximized because each I/O is duplicated and then interrogated by separate processors. Discrepant I/O is automatically alarmed.

C. Network Topology

The overall ICS network included I/O switches, field clients spread throughout the plant, network clients in the offices and control room, and a Virtual Machine (VM) host that ran all the VM based applications and process historian. The network topology is abstracted to represent both the physical and logical network in Figure 1.

The PLC cabinet housed the dual/redundant PCS and Safety System PLCs. Each PLC was connected to the Control VLAN. The two PCS PLCs connect to the Process I/O VLAN. The two Safety System PLCs connect to the Safety I/O VLAN. From the PLC cabinet, two dual/redundant PRP Local Area Network (LAN) rings connected each remote I/O switch. The I/O switches provided the local communication tie-in to various sensors and devices (e.g.: pumps and valves) throughout the plant.

A segregated Management VLAN was used together with the Control VLAN to link the PLC cabinet to the Control Room, and to the VM host cluster. The VM host cluster included several virtualized processes for engineering applications, domain controllers, and historization. The VM cluster also included the SCADA HMI VM. The SCADA HMI VM was used by operations for control and surveillance of the entire system. Due to data transmission challenges in an electrically noisy plant, media converters were used with the Supervisory VLAN to connect local clients in the plant to the Control VLAN using fiber optic cabling.

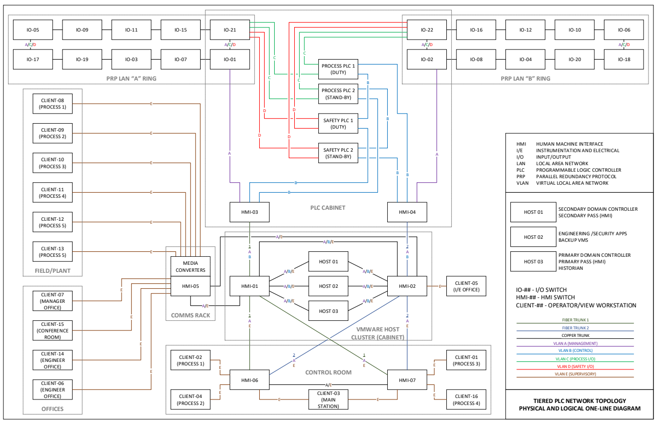

Figure 1: Tiered PLC Network Topology

D. PLC Network Redundancy and Segmentation

The PLC network redundancy is shown in Figure 2. The PCS and Safety System were isolated into separate PRP LANs and both LANs used dual redundant PLCs and ring network cabling. The PLC hardware, I/O, and controllers resided on the two separate VLANs C and D. Both of the separate PRP LANs used the common A VLAN to allow configuration of end devices. A separate B VLAN provided the communication link for the PLC I/O to be relayed to the PC servers and field clients. The B VLAN was also dual/redundant just the like the C and D VLANs. Each virtual network is logically separate.

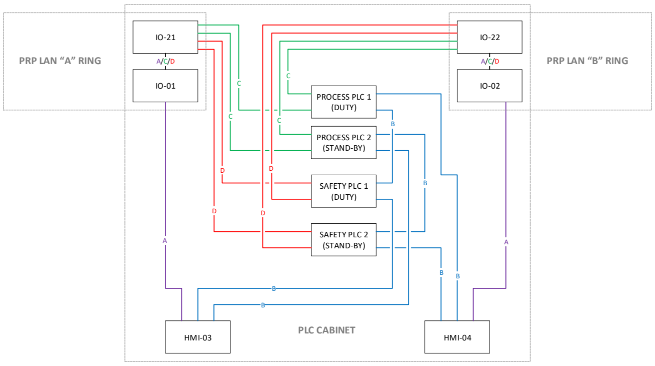

Figure 2: PLC Cabinet

As illustrated in Figure 3, each PRP LAN ring connected each of the remote I/O stations. A main trunk line was used to carry the three VLANs A, C, and D throughout the plant floor. I/O and controllers resided on separate networks. The PLC hardware is separated as well. The odd numbered switches were arbitrarily assigned to PRP LAN A and the even number switches were arbitrarily assigned to the PRP LAN B.

PRP provided availability assurances due to the dual/redundant design. PRP also provided data integrity since it time stamps all packets. PRP ensures that if two packets are sent to the same ring, the second (latter) packet is discarded. Since information is never lost, it's a "fault tolerant" design.

The physical loop design is incompatible with a logical looped network. However, the supervisory PLC blocks one of its two ports, so only one port is active at a time. If any individual segment fails, the supervisor automatically reinstates the port that was previously blocked and restores communications.

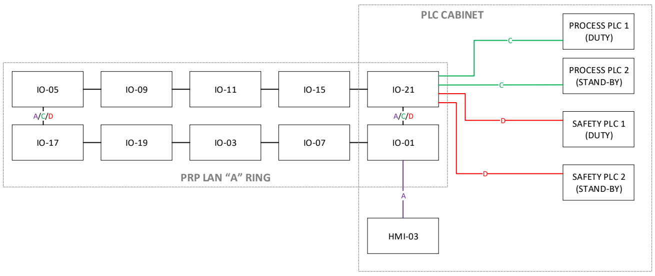

Figure 3: Field I/O Network & PRP LAN Ring

E. Operations and Control

Dual/redundant and segmented networks were used to connect the plant floor workstations to the main PLC cabinet and VM host cluster. The B VLAN connected the PLCs to the VMWare Host Cluster. The E VLAN originated at the VMWare cluster and was linked to all the field clients/HMIs. The network connections between each host within the VMware Cluster are depicted in Figure 4.

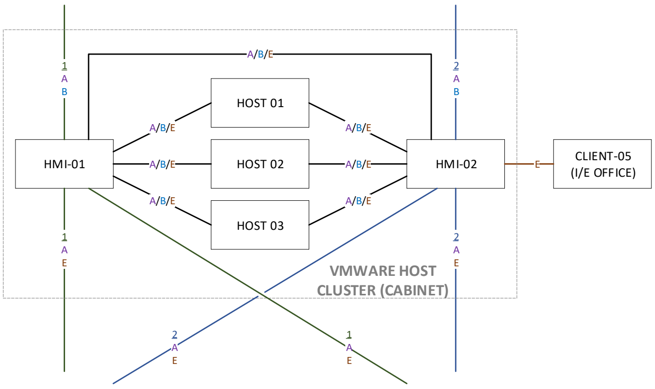

Figure 4: VM Cluster

The production facility's control room is illustrated in Figure 5. HMI-01, HMI-02, HMI-06, and HMI-07 were Layer-03 switches. Layer-03 switches can implement router functionality. Four of the five clients only used a single E VLAN connection to the HMI switch. The network topology is still fully dual/redundant manner since separate HMI switches (HMI-06 and HMI-07) are used. A fifth client (CLIENT-03) included a dual E VLAN connection to the two HMI switches HMI-06 and HMI-07. Each client used authentication mechanisms to limit access to ICS functionality. User authentication is a generally accepted method to ensure confidentiality.

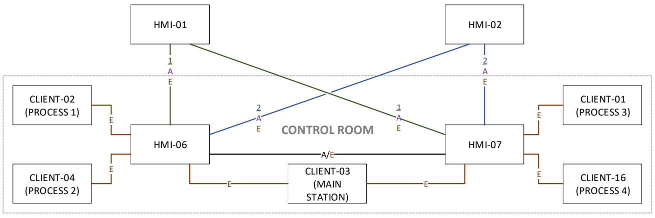

Figure 5: Control Room Network

F. Design Summary

The ICS design included dual redundant components segregated by multiple VLANs. The ICS is encapsulated within the plant's LAN. The plant used firewalls to segment the ICS from the corporate/enterprise network. Authentication controls were implemented for local access to the ICS. The use of a tiered defense strategy pairs specific security methods to specific network vulnerabilities.

- Availability was maximized through the use of a dual/redundant systems. A failure in any single system causes the standby system to take over (failover). Segmented VLANs also contributed to availability.
- Integrity was maximized through the use of separate PCS and safety systems. Each system includes identical or similar data points and discrepancies are automatically alarmed.
- VLANs were used to isolate field devices that did not support authentication protocols supporting high confidentiality.

VI. CONCLUSIONS

This paper used an ICS to demonstrate common infrastructure between the OT and IT domains. Despite the similarities between the IT and OT domains, threats to ICSs are not the same as those posed to IT systems, and therefore this paper presented different means to mitigate vulnerabilities and defend against attacks.

Security must protect ICSs from human error, insider threats, and external attacks. Security should be designed into an ICS. This paper discussed ICS defense strategies using network segmentation and network redundancy within the control system zone. Network segmentation is a standard approach to cybersecurity and can be combined with the use of dual/redundant networks to maximize the CIA triad of an ICS.

This case study presented an ICS design using techniques of both network segmentation and redundancy. Network segmentation provides availability and confidentiality. Redundancy offers the highest availability and integrity. Only using one of them is unable to achieve the highest security. Operational controls for an ICS's physical security is not investigated in depth because it is not the main focus during the initial stage of the ICS network design.

This case study contributed to both ICS design and cybersecurity practices by illustrating the actual implementation of practical defense strategies in an ICS. Dual/redundant design was illustrated at the component level. Network segmentation using VLANs was also illustrated at the component level. The design described in this case study can be used to further cybersecurity research and/or the implementation of cybersecurity methods in industrial applications.

REFERENCES

1. K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology, Gaithersburg, MD, 2015.
2. H. S. G. Pussewalage, V. Oleshchuk and P. Ranaweera, "PLC Security and Critical Infrastructure Protection," in 2013 IEEE 8th International Conference on Industrial and Information Systems (ICIIS), 2013.
3. M. Rothschild, "Secure Industrial Control Systems with Configuration Control," 26 May 2021. [Online]. Available: https://www.automation.com/en-us/articles/may-2021/secure-industrial-control-systems-configuratio.
4. J. Kaminski, "PLC Security," 11 January 2018. [Online]. Available: https://www.mroelectric.com/blog/plc-security/.
5. K. Fenrich, "Securing Your Control System POWID Symposium/17th ISA POWID/EPRI Controls & Instrumentation Conference," in 50th Annual ISA, Wickliffe, Ohio, 2007.
6. M. Lewis, "Cybersecurity for Industrial Control System Networks," InfosecWriters, 2015.
7. W. C. Yew, "PLC Device Security - Tailoring Needs," SANS Institute, 2021.
8. L. Teschler, "PLC Security in the Age of the IIOT," 25 april 2018. [Online]. Available: https://www.designworldonline.com/plc-security-in-the-age-of-the-iiot/.
9. J. P. Disso and T. Wilson, "Programmable Logic Controller (PLC) Security," 30 January 2015. [Online]. Available: https://blog.nettitude.com/uk/programmable-logic-controller-security.
10. Global Electronic Services, Inc., "Guide to Programmable Logic Controller Security," 2021. [Online]. Available: https://gesrepair.com/programmable-logic-controller-security/.
11. S. Francis, "How to secure your programmable logic controller," 12 January 2018. [Online]. Available: https://roboticsandautomationnews.com/2018/01/12/how-to-secure-your-programmable-logic-controller/15668/.
12. IEC, "Security for industrial automation and control systems," International Electrotechnical Commission, 2018.
13. M. Hashiguchi and K. Takamatsu, "Security Measures for Production Control Systems," Yokogawa, 2011.
14. Industrial Control Systems Cyber Emergency Response Team, "Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," Homeland Security, 2016.
15. Honeywell, "Protect Process Control Systems," Putman Media, 2013.
16. Cisco, "Networking and Security in Industrial Automation Environments," Cisco Systems, Inc., 2020.