International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

Securing Remote Access to SCADA During the Pandemic Era

Vilas Shewale

Independent Cybersecurity Researcher, USA

ABSTRACT: When COVID-19 arrived in the early part of 2020, it made clear for many operators that their old assumptions about engineers, vendor technicians and systems integrators accessing Supervisory Control and Data Acquisition systems had to go. Field offices shut down. Visits to site were cancelled. Downtime maintenance grew short because of a reduced workforce available on-site. Still, the gas pipes kept moving product, the lights were not shut off and the local water company was treating the supply to homes throughout its region. This document takes a look at the consequences of that transition for security and how the industry architects responded in patterns. It is informed by incidents occurring between 2020 and the spring of 2022 and references the advice put forth by the National Institute of Standards and Technology, CISA and the International Electrotechnical Commission during that timeframe. I suggest a phased approach to remote access: creating a specific Industrial Demilitarized Zone, requiring engineers or vendor technicians to "jump" to specific protected computers or systems hosted in that DMZ, multifactor authentication, systems for managing privileged accounts and the application of Zero Trust policies. My main idea is for the readers - operators of critical infrastructure - to have working patterns for making remote connections safer without interrupting the rate at which the facilities operate.

KEYWORDS: SCADA, industrial control systems, remote access, Zero Trust, pandemic, OT security, critical infrastructure.

I. INTRODUCTION

Most plants had to realize over March 2020 that their remote access was designed for few individuals that just "walked through the front door" of the control room or for when someone at vendor support has to step through your process by pointing your mouse. It was never meant to be the only path into operational technology. Some industrial companies had remote access capabilities (often, not more than an engineer at site that could support others remotely on specific tasks during off-hours) but almost as soon as stay-at-home orders went into effect, the "side door" that served a few specialists suddenly became the main way to get into SCADA systems-it had to carry the full weight of operations. Some companies had restricted remote access to change windows where operations needed hands-on modification of code, but almost literally weeks later it went to permanent open remote sessions for multiple engineering teams that are working from home. Instead of flying in technicians to conduct equipment commissioning, that has become screen-sharing calls through teams. Sometimes even contractors had to use their kitchen table while connecting into a control system HMI.

While this occurred, a worsening threat background occurred: more fishing campaigns against oil and energy companies and more ransomware operators that may have traditionally been targeting hospitals or law firms began to get into the energy sector: utilities, refineries, oil production firms, pipeline operators. It made the issue apparent when Colonial Pipeline had a ransomware issue May 2021, with those who pull into gas stations in the East Coast noticing [1].

This paper has three goals. The first is to highlight changes that were implemented in terms of remote access trends during the COVID-19 pandemic period. The second is to survey architectures that have popped up in response or grown up as we continue our industry. The third goal is to propose an architectural pattern for operations to reference. The paper utilizes some information from incident write-ups, advisories published by CISA (Cybersecurity and Infrastructure Security Agency) and NIST (National Institute of Standards and Technology) and standards from the IEC (International Electrotechnical Commission) 62443 series. I am aiming to talk in an architectural sense, than specific products, so operations could map the patterns described here onto whatever systems they run.

Two scope items that should be identified up front: The discussion here focuses on the remote access path going into the industrial control system and its network zones and conduits. Broadly speaking enterprise IT (information

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

technology) is out of scope here. Second, the essay and discussion from this point forward comes from the defender's viewpoint. Threat-actor tactics are presented to illustrate why one might choose a specific defensive move, than for completeness as an offensive threat.

II. BACKGROUND: SCADA AND THE PURDUE MODEL

SCADA refers to a family of systems that monitor and control any physical process on which information is available and controllable by digital computer systems. Pipeline operators use SCADA to view flow rate, pressure and valve status across hundreds of miles of pipeline. Electric utilities use SCADA to coordinate breakers, transformers and substations, while water authorities use SCADA for pumps, filtration and chlorination. In general, SCADA bridges the digital and physical world, as the flip of a bit causes a real-world actuator to move.

Figure 1 shows a diagram of how industrial networks are often organized using the Purdue Enterprise Reference Architecture (PERA), which categorizes the network into zones [2]. At the bottom are the physical devices, which includes sensors, actuators, motors and other input devices. Directly above the physical devices are the controllers, which include PLCs and RTUs, that manage the execution of tasks. Above the controllers is the supervisory layer where HMIs, historians and engineering workstations reside. Above the supervisory layer are the manufacturing operations systems, followed by the enterprise business networks at the top of the diagram. Above the manufacturing operations layer is a DMZ, where internet-facing assets, along with systems that are used by operational personnel but not on the operational level, are kept.

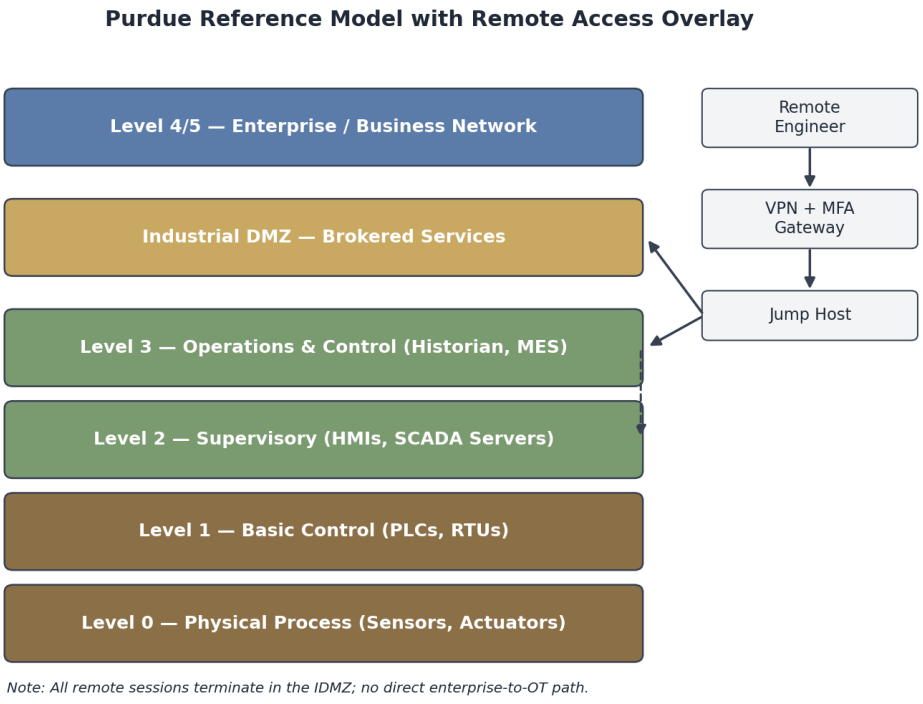

Figure 1. Purdue Reference Model with a remote access overlay. Remote sessions terminate in the industrial demilitarized zone (IDMZ); no direct path crosses from the enterprise to the operations layer.

Actually, that is not a rule of physics, it is a security paradigm. Most modern plants blur the edges of those boundaries in ways a historian writing about industrial security policy may indeed use, especially with unified OT monitoring across multiple Purdue levels and the advent of IoT analytics platforms spanning those layers. Edge computing even puts processing nodes outside those predefined zones of traffic flow. Nonetheless, that is how we talk about which communications should and should not cross zones and it is how the entire field of OT security discusses the problem, with both NIST SP 800-82 [3] and IEC 62443 [4] referencing the Purdue Model as the framework.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

Usually, before the COVID crisis, remote access means that someone from an outside company or a vendor would connect through the internet to the remote access point (the "VPN gateway"), log in with their credentials (their Active Directory log in) to access the jump host located within the OT DMZ, which would log the session and limit access to the appropriate systems and the jump host was also the only thing with all the passwords for the industrial control systems equipment on the floor. This worked when remote access was a few times a month or in a rare event, but not when workers became remote permanent.

III. THE PANDEMIC THREAT LANDSCAPE

Dragos tracked a spike in threat activity targeting industrial settings between the start of the COVID-19 pandemic and the close of 2021, noting in its 2021 Year in Review that its tracked threat groups had increased year over year while ransomware accounted for more than 65% of reported disruptions at industrial companies [5]. IBM's 2021 Cost of a Data Breach report found that the total cost of an average data breach rose to a record $4.24 million, an increase of 10% year-over-year and 29% higher than it was ten years prior [6]. Verizon's 2021 Data Breach Investigations Report revealed that in more than 80% of all observed breaches, credentials or phishing were used to gain initial entry [7].

The period's significant attacks-most notably on the Colonial pipeline and the meat processor JBS SA-show a trend toward exploiting weak authentication and unsegmented networks to seize control of critical operational technology. These were not the result of complex, novel cyber weapon zero-day exploits. The incidents highlight security vulnerabilities resulting from the failure to properly manage remote access security (e. g. , the use of old passwords or weak authentication) or a lack of network segmentation to contain threats (e. g. , when the control network was tied into a standard IT network).

3.1 Oldsmar Water Treatment, February 2021

In February 2021, an unauthorized actor gained access to a SCADA system at a water treatment facility in Oldsmar, Florida, briefly increasing the sodium hydroxide (caustic soda) concentration to dangerous levels. The intruder's access reportedly stemmed from a TeamViewer session using a password that was shared [8]. The attack was discovered and stopped in under five minutes by an observant employee monitoring the system, who noticed the computer cursor moving on his screen on its own. The event has sometimes been overlooked because no injuries occurred as a direct result of the intrusion, but it amplified security fears about insecure remote access to critical infrastructure, emphasizing the importance of keeping remote access channels to OT systems restricted. TeamViewer instances with shared passwords, unneeded remote-access tools lying dormant or lacking multi-factor authentication are common sight in OT environments, Oldsmar was a stark example of the negative outcomes of such risks.

3.2 Colonial Pipeline, May 2021

On May 4, 2021, Colonial Pipeline, a major operator of a 5,500-mile fuel line running from Texas to the Northeast, decided to shut down its systems following ransomware in its business network, to understand what was happening and to bring it back to business, the shutdown sparked gasoline shortages along the Eastern Coast. It had a swift congressional response and Transportation Security Administration regulations aimed at pipeline security were announced within weeks [9]. Later reporting discovered that the hack had started with stolen credentials to a legacy, abandoned account used for a VPN that lacked multi-factor authentication [1]. The two-factor requirement missing for that one particular account has stuck in my mind, I bet if that account had either been removed or upgraded, a control room post-mortem shared broadly would not be so painful to those working in the industry today.

3.3 JBS, June 2021

One example that demonstrated this escalation was when meat company JBS, one of the world's largest- paid $11 million in June to hackers behind an April ransomware attack that shut down plants in the United States, Canada and Australia. JBS represents how consumers are not on the receiving end of such attacks any more than other industries with connected, public infrastructure.

3.4 Log4Shell, December 2021

Back in December 2021, the security firm Praetorian discovered [11] a major vulnerability, CVE-2021-44228, in Apache Log4j, the most widely used logging tool for Java Applications. Even if not immediately obvious, the Java library is shipped with thousands of different commercial software products, including those that touch OT systems. When Praetorian announced Log4Shell, as it became known, IT teams quickly scrambled to find systems using it, contact vendors-who themselves were overwhelmed and had trouble tracing how widely distributed their product was- and to apply patches and remediation. All it took was one RCE in a major dependent tool to bring supply chains,

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

including OT supply chains, to their knees. OT managers experienced the fun of seeing their vendors scramble to reply, trying to figure out how many industrial control systems use this damn Java logging utility or even trying to figure out if any of theirs are running software even touching the Java logging utility in the first place. Once you are finished with all the inventory, you then run into problems with patch deployability and vendor patches that you may need to wait on, all with OT systems exposed for at least weeks after the patch. The OT/IT convergence has only made this worse.

Each event follows many similar themes: the attacker achieved access primarily through a compromised identity-reuse of weak passwords, absence of multi-factor authentication (MFA) and the exposure of remote management-as opposed to an exploit of complex code, like Eternal Blue or an advanced RCE. In numerous instances, there was not enough segregation between business IT networks and OT systems, resulting in wider impacts. When an operator of any size reads the news, they do not need any special expertise to identify the core problem: a compromise of a network remote access capability or an account identity.

IV. ARCHITECTURAL RESPONSES

There is really nothing that architectural response here has not popped up in various versions over the years, as such it is well covered in OT security texts, but it was a combination of operators, maybe in this region in this period, applying those technologies that were less in favor for 10 or more years and their willingness to challenge these older assumptions which brought it about in a few days time. That section touches on the individual pieces involved and how they stitch together, you can see the entire picture in Figure 2 below.

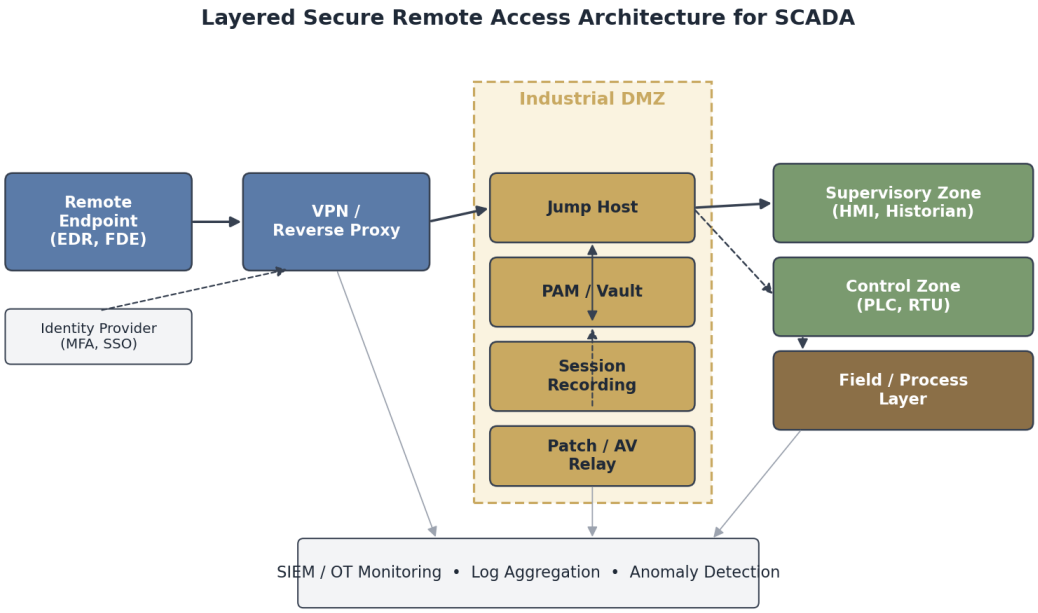

Figure 2. Layered secure remote access architecture for SCADA, combining an industrial demilitarized zone, jump host, privileged access management, session recording, and centralized monitoring.

4.1 The Industrial Demilitarized Zone

An industrial DMZ, placed between enterprise and operations, will broker all necessary traffic between those networks. Systems requiring OT side data (e. g. , historical database engines, MES databases / interfaces) will need to be replicated, virtualized, proxied or replicated out of the operations DMZ, instead of reaching directly into the operations network. Remote access will generally connect to systems in the industrial DMZ than reach directly into the OT DMZ or OT network. The fundamental rule is that nothing that is on the enterprise network is allowed to talk to any device that is within the OT network. NIST SP 800-82 has excellent coverage on this reasoning, [3] and the IEC 62443 security standards promote this logic within the zone and conduit security zones and conduit. [4]

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

4.2 Jump Hosts and Privileged Access

A jump host, also sometimes called a bastion host or secure access gateway, is the sole point through which an engineer or vendor interacts with industrial control system (ICS) devices. It uses high levels of authentication, logs sessions, limits the resources users can connect to and stores the logins necessary to access physical equipment that employees and vendors cannot see. They sign into their corporate ID on the workstation and it takes over inserting the credentials.

This structure effectively limits a broad range of access to an accessible point that security can monitor easily and simplifies password renewal processes instead of telling each third party to reset their unique credential information on every piece of gear they manage. Instead, a credential safe automatically updates logins and it communicates with the jump host. Security and IT organizations that already invested in managing privileges would not need significant new plumbing. They would just have to store OT credentials within their existing safe.

4.3 Multifactor Authentication

Most major OT security failures during the pandemic revolved around remote access methods such as RDP, VPNs, SSH, etc. , where, had MFA been in place, the damages could have been reduced if not avoided entirely. Repeatedly, over the course of 2020 and 2021 [12], CISA issued various advisories that repeated this finding, highlighting the risks of using single-factor authentication for remote access. The implementation costs associated with adding MFA to VPN hardware are not prohibitive, there are, however, significant challenges in an environment where shift rotations are common and employees may use a pool of workstations. If at all possible, users should authenticate using a hardware-backed factor, otherwise, SMS tokens may be substituted as an interim step. These are weaker but do at least prevent anyone with just a password from obtaining access to a system. By 2022, the generally expected requirement is for any external entry point into the OT network to include some form of second factor authentication. Specific cases should be justified with an acceptable risk rationale and expire after a time period designated by someone with the relevant authority for risk decisions.

4.4 Network Segmentation

Segmentation is the strategy of keeping an attacker out of one portion of the network even if they find a path into another part. Within an OT network, this involves separating control zones into boundaries along the suggested IEC 62443 lines, implementing firewalls on these lines or firewalls with only a unidirectional function if there is a need for an extreme zone barrier. Segmentation in the OT to enterprise zone is typically addressed by establishing and rigidly adhering to the IDMZ as the only method of connection between the OT network and the enterprise.

The shutdown of the Colonial Pipeline provides a relevant, though unwanted, illustration of segmentation benefits. Available reports suggest that the initial ransomware incident was contained to the IT network, however, Colonial had to halt operations of the entire pipeline, apparently because they could not sufficiently show that the control systems were isolated from IT within a sufficient time frame [1]. With stronger and documented evidence of segmentation, such a response time might not be necessary for the next operator unfortunate enough to find themselves in a similar dilemma.

4.5 Endpoint Hardening for Engineering Workstations

In time, remote working had engineers and vendors bridging in from home. The device they joined from is now an extension of the OT attack surface, with solutions including EDR tools, full-disk encryption, restricted local administrator rights and application allow-listing playing a function in controlling vulnerabilities on those endpoints. For laptops used solely for OT, engineers need to limit browsing, this machine accessing PLCs cannot also be where you read your personal e-mails. The ultimate approach for those firms able to pull it off: thin-client architecture or VDI so that the restricted OT environment can reside safely in the data center than on the laptops that their kids might also access while working from home.

4.6 Logging, Monitoring, and Anomaly Detection

And it generates far too many logs to inspect by eye. It is hoped that, by now, logs from remote access conduits are being funnel into a SIEM (Security Incident Event Management) or other OT network monitor and that the systems are looking for signs that might point to compromises: authentication outside expected times, remote sessions from overseas IP addresses, command chains running differently than in routine use. While the OT network monitoring market is smaller than for enterprise IT, many vendors specialized in this space have developed some excellent products and services and it reached its stride during COVID. It makes no difference which technology you prefer. What counts is that the traffic is under surveillance and monitored according to the standard behavior of your environment.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

V. ZERO TRUST AND THE FUTURE OF OT REMOTE ACCESS

Zero Trust security concepts have been around a long time-over 10 years before the COVID-19 pandemic shut the world down. The term was generally introduced in the work of Forrester analyst John Kindervag around 2010 [13]. NIST released Special Publication 800-207, "Zero Trust Architecture", in August 2020. NIST SP 800-207 documented how the U. S. Federal government plans to build its way toward Zero Trust Architecture, laying out common architectural components, design considerations and transition planning for adoption by U. S federal agencies [14]. US President Joe Biden signed Executive Order 14028 (Improving America's Cybersecurity) on May 11, 2021. E. O. 14028 directed all federal agencies to speed their migration towards Zero Trust by August 2024 and pressured vendors involved with the supply chains of government to adapt]15].

Trust is never granted because a client (e. g. , an employee's laptop) is inside the corporate firewall. Trust must be granted dynamically on a request-by-request basis based on identity, posture of the device and the sensitivity of the resource that a client wants access to. Request to read a process value should differ fundamentally from request to write a configuration, so the system must distinguish them. A few such common components have been organized in Figure 3.

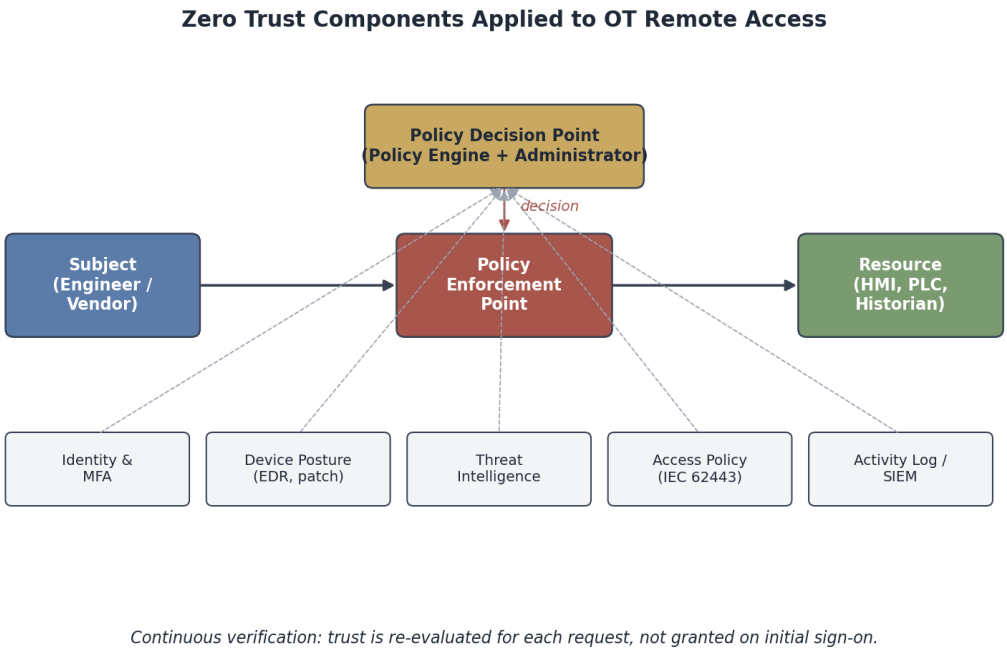

Figure 3. Zero Trust components applied to OT remote access. The Policy Decision Point evaluates each request against identity, device posture, threat signals, and access policy. The Policy Enforcement Point implements the decision.

The operating principles translate as follows into a SCADA system that allows only justified access from external points: Verify identity, not just location. Issue valid only until a few minutes are up. Check device, is it running, patched? The individual session should only be allowed access to the minimum set of systems required for the engineer. Log what has happened. Feeding log data into a threat intelligence system which identifies anomalous activities can quickly escalate the response by security personnel. It is the uncomfortable truth, that implementing Zero Trust is even more challenging than in traditional IT. But legacy OT equipment in operation will never fulfill certificate requirements or install agent-based devices.

Zero Trust therefore applies in depth, pushing controls closer to the edge and utilizing jump hosts and other protocol-aware security devices that are located at the boundary between a modern identity management system (with JWT certificates, SAML assertions, MFA, etc.) and an OT device that cannot support modern identity management (such as

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

PLCs commissioned in 2008). Zero Trust protects, but it has to manage, compensate and protect the endpoints (PLCs) which cannot provide any identity context, that will ultimately reside inside OT.

VI. IMPLEMENTATION CHALLENGES

The OT cybersecurity tools released over the last few years have created problems for operators since the pandemic began. None are fatal, but each merits attention because ignorance of the problem means inaction and inaction results in no progress.

First on this list are legacy controllers. Many exist that were specified decades ago for an OT environment that had no remote access on its horizon. Modern security protections like authentication, encryption and logging cannot be added. So the operator puts the controller in an isolation ward of security zones, firewalls and a monitored gateway. Vendor remote access second. OEMs want remote access on all machines so that they may maintain and warranty equipment.

Terms for vendor remote access often exceed that provided to the manufacturer's own employees. An operator may offer vendors vendor access by putting them in the same jump hosts for the operator's own personnel, managed by the operator with each vendor account. Some are stricter. Vendors require their access be through a ticket workflow that is "approved, " so there is a reason.

Operational tempo third. OT control centers are shift centers. Shift workers like to get to the screen as quickly as possible. MFA authentication, posture check and logging can take time to get through, which may or may not be intolerable based on the ease with which they are enabled. The operators that have done well securing their systems were the ones that were most able to carry out usably.
Last is budget and staff. Industrial cybersecurity teams remain the smallest of any I have seen at manufacturing firms. Adding many new tools without hiring many people just leaves the tools half-implemented. We tend to advise our customers honestly to invest in a couple of high-value tools they will manage properly instead of buying all of the tools that the industry is pushing.

VII. CONCLUSION

So, the pandemic did not make a new remote access problem. The remote access problem was there. But now people really were locked out of the building. The pace at which decisions about this happened, as is often the case with SCADA and IT/OT convergences, was wild. Many companies chose to keep it how they were, but do extra hard line work with their perimeters. Many of the companies I have observed embraced zero-trust. Other companies made decisions about nothing.

I have had to learn that by looking at bad things that have happened and the public disclosure that follows. The pattern I had seen was always effective- an industrial DMZ, use jump hosts, multifactor, segmentation, hardening clients, logging thoroughly, and, more often than not, it was always pretty simple stuff. What was lacking were either the buy-in or the people or the money needed to carry out that effectively. The pandemic window for that made for a significant opportunity. The operators who came out swinging instead of waiting out the storm did better.

As we look toward 2022 and beyond, one can see two primary trends in play here. The first trend is regulatory. The TSA pipeline rules, for example, were not invented at the beginning of the pipeline holiday. But they became imperative at that point, and they set the pace for additional pressure across other critical sectors. The other trend I am seeing is tech trend driven. Technologies such as identity-centric architecture will become even more prevalent throughout OT as we move away from legacy assets and into next generation equipment that is designed to support it. The fight will continue. However, the OT operators who used this as an impetus to completely rebuild all of their existing remote access procedures will face the next 10 years in a stronger situation than those that just deferred.

REFERENCES

[1] U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, “DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks,” Joint Advisory AA21-131A, May 2021.
[2] T. J. Williams, “The Purdue Enterprise Reference Architecture,” Computers in Industry, vol. 24, no. 2–3, pp. 141–158, 1994.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 5, Issue 2, March – April 2022 ||

DOI: 10.15680/IJCTECE.2022.0502006

[3] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Revision 2, May 2015.
[4] International Electrotechnical Commission, "IEC 62443: Security for Industrial Automation and Control Systems," multi-part series, 2013–2020.
[5] Dragos, Inc., "Year in Review 2021: ICS/OT Cybersecurity," February 2022.
[6] IBM Security and Ponemon Institute, "Cost of a Data Breach Report 2021," July 2021.
[7] Verizon, "2021 Data Breach Investigations Report," May 2021.
[8] Joint advisory from the Federal Bureau of Investigation, the U.S. Secret Service, and the Cybersecurity and Infrastructure Security Agency, "Compromise of U.S. Water Treatment Facility," February 2021.
[9] U.S. Department of Homeland Security, Transportation Security Administration, "Security Directive Pipeline-2021-01 and Pipeline-2021-02," May–July 2021.
[10] U.S. Federal Bureau of Investigation, public statement on the JBS USA cyber incident, June 2021.
[11] U.S. Cybersecurity and Infrastructure Security Agency, "Apache Log4j Vulnerability Guidance," Alert AA21-356A, December 2021.
[12] U.S. Cybersecurity and Infrastructure Security Agency, "Implementing Strong Authentication," guidance materials, 2020–2021.
[13] J. Kindervag, "No More Chewy Centers: Introducing the Zero Trust Model of Information Security," Forrester Research, September 2010.
[14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, August 2020.
[15] The White House, "Executive Order 14028: Improving the Nation's Cybersecurity," May 12, 2021.
[16] World Economic Forum, "The Global Risks Report 2021," 16th Edition, January 2021.
[17] European Union Agency for Cybersecurity (ENISA), "Threat Landscape 2021," October 2021.