White Paper

Industry
OT Cyber Security

An Argument for a Holistic Approach to Critical Infrastructure Security

Increased attacks on critical infrastructure and operational technology devices in robust physical infrastructure demand a holistic approach to fighting cyber-attacks.

Authors
Darren W Pulsipher
Chief Solution Architect
Dr. Ann Scott
Chief Edge Architect
Felix Reeb
Global Smart Railways Lead

Table of Contents

Cyber-attacks and ransomware attacks on critical infrastructure have increased dramatically over the few years. The sophistication of cyber criminals, the desire to leverage more OT data in business optimization and decision making, and the increased digitization of legacy infrastructure driving the increase in the number of devices gathering data and controlling the physical world have created a rich field for cyber-criminal to take advantage of [1]. Many organizations leverage their IT cyber-security best practices, tools, and architectures to secure the OT infrastructure without adequately understanding the operation model, or different requirements for OT devices, many of which are air-gapped and not designed for current security models and constant updating.

This ever-present battle between IT and OT's different approaches to cyber-security has relegated OT security solutions to a patchwork of tools and best practices that are disjointed and sometimes expose vulnerabilities for cyber-criminals to take advantage of. Air-gapping and isolation were sufficient in the past, but organizations must architect and design holistic approaches to OT physical and cyber security with the increase in cyber-attacks on physically controlled infrastructure and the emerging edge compute/devices for data-driven, real-time decision making.

This paper identifies the key drivers of securing critical infrastructure control systems and the problems with today's OT security solutions. It then describes the use cases for a holistic, complete security solution considering the operational models and unique physical environment of OT systems and devices. Then a high-level system architectural design shows how current common hardened off-the-shelf products can be integrated to provide a hardened security solution for critical infrastructure control systems and other OT systems.

Problem Statement

Over the last five years, there has been exponential growth in cyber-attack activity targeting critical infrastructure. An increasing number of these attacks have been successful in shutting down critical infrastructure all over the world [1]. Four factors are converging that increase the importance of hardened cyber-security position, namely: increased essential sophistication of infrastructure systems and ransomware attacks; IT security best practices do not map to OT security vulnerabilities and issues, government regulations and compliance, and the need to use data analytics to optimize critical infrastructure.

Increased Sophistication of Attacks

Cyber-criminals have increased the types of attacks and the frequency of attacks on critical infrastructure. Some recent successes have encouraged cyber-criminals and nation-states to increase their focus on critical infrastructure for monetary gain, terrorism, and physical attacks on other nation-states.

The STUXNET attack is one of the most famous cyber-attacks on Critical OT infrastructure. This sophisticated attack took advantage of the widespread traditional OT airgap network strategy and infiltrated OT systems worldwide using multiple zero-day vulnerabilities on USB flash drives.

This highly successful attack has emboldened several attacks over the last decade, including attacks on different critical infrastructure sectors, including the water sector, power grid, safety systems, and oil and gas [1]. See Figure 1 for a timeline of OT cyber-attacks over the last 20 years.

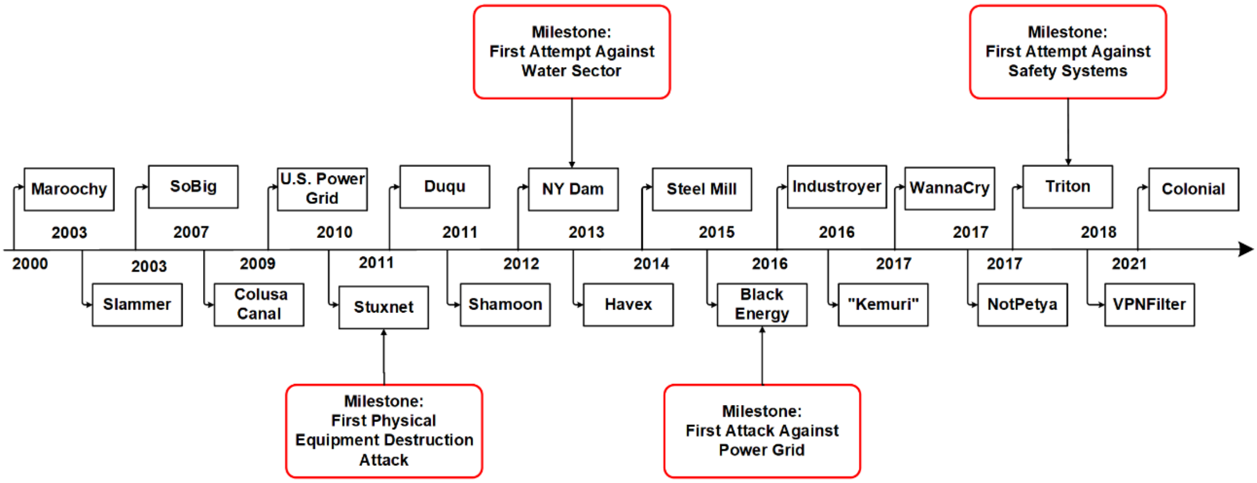

Figure 1 OT Cyber attacks [1]

OT Security Issues

OT infrastructure has different security issues than traditional IT infrastructure. Because OT infrastructure is typically made up of machines that manipulate the real world [motors, compressors, pumps, instrumentation (sensors), etc.], they can affect the physical world in which we live and potentially cause injury or death. The motivational foundation of infrastructure managers and OT operators is fundamentally different from IT in three key areas: functional safety is the highest priority, reliability of OT devices and network is vital to functional safety, and OT systems are made of highly heterogeneous OT devices designed for long service life (10-20 years).

Functional Safety is the highest priority of industrial control systems.

Functional safety is OT's primary concern when working with critical infrastructure systems. Functional safety refers to the physical world being affected by the OT infrastructure and the need for the designed functionality to continue regardless of external events. For example, landing lights on a runway when not properly working could cause delays at an airport or even loss of life.

Functional safety is so important to some organizations that systems are shut down to mitigate the risk of significant physical disasters in the sight of uncertainty. Most recently, an infection of a cyber virus in their IT network and potential exposure to the OT network motivated Colonial Pipeline to shut down operations and caused gas shortages across the mid-Atlantic coast of the United States.

Reliability of CI's (Darren - what is CI?) devices and network is vital to guarantee system safety.

Many OT critical infrastructure systems' "lack of control" can cause functional safety issues. Even though many critical systems have fail-safes to prevent physical destruction with the loss of machines or controllers (for example, hard-wired shut down systems for boilers), service disruption can cause secondary and tertiary side effects.

Even though these fail-safes protect the system, the secondary and tertiary side effects can be profound, like loss of electricity, gas shortages leading to increased gas prices, food processing plants shutting down leading to loss of tons of food, and increased prices at the store. Sometimes these secondary and tertiary effects are precisely the cybercriminals' goals.

Critical infrastructure has much higher demands on reliability and uptime than traditional IT infrastructure due to these scenarios.

Operational Technology (OT) Devices are different from IT devices.

IT security risk mitigation is very different from IT mitigation strategies, where traditionally infected nodes can simply be shut down, and the workloads migrated to other devices and/or locations. Several key differences between OT devices and IT devices compound the risk mitigation and management of OT infrastructure.

- Legacy infrastructure is measured in decades, not years – OT devices have a much longer lifecycle than IT devices.
- OT devices and networks are physically dispersed.
- Highly heterogeneous systems and functions, including machines, controllers, devices, networks, and capabilities.
- OT device vendors have proprietary systems with custom or outdated operating systems, communication protocols, and applications.
- Industrial communication protocols have not been designed with security in mind, for example, they often have no inherent encryption of data.
- Some legacy OT devices do not communicate over common network IP.
- The distributed nature of OT systems makes it challenging to manage and maintain them.
- Traditionally, OT networks are air-gapped from IT networks to prevent cyberattacks.
- Cyber-attacks are "jumping" air-gapped networks with zero-day vulnerabilities in software, firmware, and operating system patches.
- New cyberattacks are taking advantage of unpatched vulnerabilities in OT networks.

IT Security is not the same as OT security.

Most IT cybersecurity professionals leverage IT cybersecurity best practices on OT infrastructure without fully understanding their differences. The following two sections show the typical techniques for IT cyber security and the OT concerns that fundamentally differ from IT best practices.

IT cyber security techniques

Even though there are several different cybersecurity techniques, this paper will describe and compare and contrast these techniques with OT operators' concerns.

- Cyber Threat Detection – primarily focuses on network and host scanning for patterns of cyber intrusion.
- Cyber Prevention – primarily focuses on network management, network controls, and access management, including the proper configuration of routers, firewalls, and micro-segmented networks. This also includes malware and endpoint protection software.
- Risk remediation includes quarantine, investigation, and rebuild meaning systems can be off-line for extended periods of time.
- Patch and update management focuses on the high frequency of patch updates to firmware, operating systems, and software, and they often require "new" devices capable of supporting the increased load.

OT Operations Concerns

Typically, OT operations express concerns about injecting IT cyber security best practices into their OT networks. The following is a list of some common problems

- Cyber Threat Detection on OT networks needs to monitor different kinds of traffic than IT networks.
- OT networks contain highly heterogeneous devices. There are several hundred vendors and types of devices, OS(s), and applications. Where IT infrastructure is relatively homogeneous.
- Most of the data on OT networks can't be encrypted because the overhead of encrypting on old devices is too high.
- OT networks are protected because they are air-gapped networks.
- OT systems cannot be taken offline for repair without disruption to service. Additionally, there are safety and reliability concerns when systems are shut down and restarted.
- Software and firmware patches are risky for functional safety and security concerns. Patching impacts reliability and safety.
- OT systems are based on physically dispersed systems with long lifecycles and devices are often in use for 10-20 years.
- OT machine and device vendors have a protectionism position with proprietary systems. This disjointed industry is moving very slowly to standard infrastructure and security standards

Government Regulations

Because governments see critical infrastructure affecting their citizens' safety, economies, and national security, governments have begun to regulate OT and critical infrastructure cyber security. Governments are concerned not only with computing and data infrastructure but also physical infrastructure.

Some industries like transportation have adopted their cyber security frameworks to protect these industries from further catastrophic cyberattacks. The following is a brief list of the most prominent security frameworks with a quick overview of each framework.

TSA Cyber Security Framework [2]

This cyber security framework targets the transportation industry in the United States and heavily leverages the NIST cyber security standards. However, it does emphasize functional safety as part of the cyber security position and remediation plans.

TS50701 – European OT Cyber Security [3]

This European cyber security standard is very similar to the TSA cyber security framework, focusing on rail systems and their functional safety regarding cyber security, including several remediation strategies.

IEC 62443-4-2 - Component Security Assurance [4]

This international standard focuses on cyber security at the component level in OT infrastructure. It primarily focuses on individual machines, controllers, and devices, providing a common cyber security position across entities for automation and control purposes.

NIST SP 800-82r3 [5]

Most of the other standards have based their frameworks on this NIST standard. The primary goal is to implement a repeatable and auditable process to protect critical infrastructure through best practices in identifying, detecting, responding, and recovering. Additionally, the framework proposes five layers of architecture, including security management, physical security, network security, hardware security, and software security.

Business Intelligence through Data Analytics

Over the last decade, critical infrastructure has been augmented with intelligent IoT devices adding new types of sensors and compute power at the edge. This augmentation has increased the amount of data generated at the edge giving infrastructure managers additional information to manage their critical systems.

However, the increased volume of data requires more data analytics tools and compute resources that traditional OT infrastructure does not have available. Additionally, OT data in isolation does not provide a complete operational picture; injection of internal and external data is required. This desire to build more business decision information from OT data drives the breakdown of OT isolation.

Traditional Purdue Model

In the 1990s, a security and infrastructure model was created that most OT organizations still follow today. This model, named the Purdue model, describes the bridge between the IT and OT infrastructure through six levels that show a traditional air gap between the four levels of OT infrastructure and two groups in IT infrastructure. See Figure 2 for a high-level view of the traditional Purdue model.

The following is a brief description of each of the Levels.

- Level 0 – Devices that manipulate the physical world. Like pumps and motors.
- Level 1 – Devices that control level 0 machines, like PLC (Programmable logic controller)
- Level 2 – Control systems used to supervise the physical processes, basically controlling the Level 1 devices. This includes human-machine interfaces and engineering workstations.

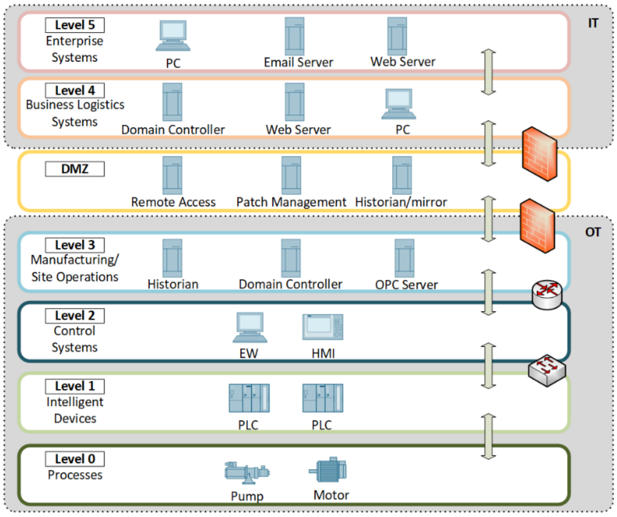

Figure 2 Purdue Model [1]

- Level 3 – Manufacturing and site operation machines used to manage production workflow and facility-wide control. These manage level 2 devices.
- DMZ – Demilitarized zone is used to prevent direct communications between IT and OT networks.
- Level 4 – Business and planning logistics system to oversee IT operations supporting OT processes. This includes MRP and ERP systems.
- Level 5 – The IT enterprise network used for production and resource data exchange.

This traditional Purdue has been in place over the last 30 years and is starting to show its age. As IoT devices become more intelligent, many lower levels 0-2 are starting to collapse, increasing capabilities at the edge. Additionally, these new devices are piercing through DMZ to talk directly to Levels 4 and 5 in the IT infrastructure [6].

Even though the Purdue model has served its purpose over the years, it is starting to break down as Cyber criminals are exploiting the hard-shell soft center paradigm of the model. Changes to the traditional OT isolation must be re-evaluated and re-engineered.

Understanding the OT Security Use Cases

Capturing actors and use cases of this system helps better understand the scope. Of the architecture and its impact on operations. The following two sections detail the system's actors and their use cases. See Figure 3 Use case Diagram for more information.

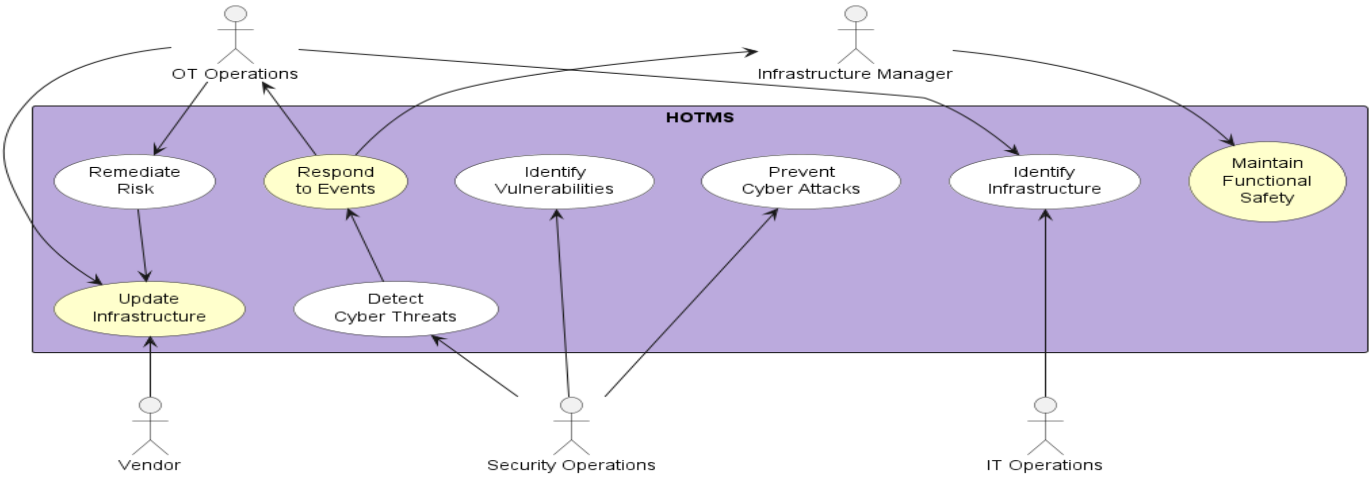

Figure 3 Use case Diagram

Actors

Understanding the key stakeholders and actors of an OT security solution is vital to understanding the scope of the system and its use cases. The primary actors are: IT operations, OT operations, infrastructure manager, security operations, and vendors are described in the following sections.

IT Operations

IT operations are responsible for managing network devices. And storage across the company's Infrastructure. Most IT organizations are also responsible for traditional disaster recovery and business continuity. However, this typically does not apply to OT operation's infrastructure.

OT Operations

Operations are responsible for operational technology infrastructure, primarily level 0 through Level 3 devices and network connectivity in the OT infrastructure. Typically come from the OT space, including understanding machines, controllers, and the devices that manage them. However, they are not responsible for the connectivity to the IT networks. And traditionally, they do not handle cyber security.

Infrastructure Manager

Infrastructure managers manage the infrastructure, including level 0 and level 1 machines and devices. They utilize Level 3 plant managers to evaluate the operating conditions of the machines and devices in the OT infrastructure. They are primarily responsible for critical infrastructure and functional safety of the plant.

Security Operations

Security operations are responsible for threat detection and threat prevention and remediation of cyber security threats against the company's assets. Traditionally focused on IT infrastructure, more emphasis is now being placed on IoT infrastructure and cybersecurity threats in this unique environment.

Vendor

Vendors play an essential role in OT infrastructure management because many vendors need access to machines and controllers to update and patch devices when things go wrong or updates are needed for the software. Firmware or hardware are required. Many times, this includes physical access to machines. Other times it could be connectivity or virtual access.

Primary Use Cases

The primary use cases show how the actors work with the system to achieve their goals. The following primary use cases are not comprehensive of all OT management but focus primarily on the use cases involved in securing OT infrastructure, devices, and data. They include identifying infrastructure, identifying vulnerabilities, preventing cyber-attacks, detecting cyber-attacks., remediating risk, updating infrastructure, responding to events, and maintaining functional safety.

Identify Infrastructure

The OT and IT operations teams work together to identify infrastructure in the OT environment. This should include taking inventory of machines, controllers, and devices from levels 0-3 of the Purdue architectural model.

This is typically handled through the automatic discovery of devices on the OT network. However, automatic discovery does not give the whole picture. Physical location and relationships between level 0-2 machines, controllers, and devices must be manually captured and added to the inventory management system.

The inventory management system should also contain firmware, operating systems, and software. The following are secondary use cases captured for the identifying infrastructure use case.

- Inventory Machines, Controllers, and Devices – This should include the relationships between machines, controllers, and devices.
- Inventory Operating Systems – Includes capturing

the OS version and patch levels. Used during risk assessment and remediation.

- Inventory Software – Includes software bill of materials (SBOM) and versions of each software package and its dependencies.
- Inventory Firmware – Includes software bill of materials (SBOM) and version for each firmware updated, baseline deployment, and any dependencies.
- Capture Device Location – Capture the machine, controller, and device location into the inventory management system, including longitude, latitude, and location name.
- Capture Network Topology – Understanding the current network topology should be able to be collected automatically.
- Monitor OT Devices – One of the critical aspects of identifying OT devices is monitoring the health and operational function of the devices. This is a pre-cursor to maintaining Functional Safety.

Identify and Assess Vulnerabilities

Identifying vulnerabilities is traditional cybersecurity IT best practice, which also has its place in the OT cybersecurity environment. Scanning network and security configurations in the OT environment is critical for preventing cyber-attacks in the future. After the vulnerabilities are found, there are several additional steps needed in order to understand how to respond. Some vulnerabilities can have an acceptable level of risk and do not require action, while others may warrant an immediate response. We recommend the following process:

1. Scan for Vulnerabilities - Vulnerability scans should include:
    a. hardware
    b. network, software, OS, and security configurations
    c. firewall, identity, and access management rules
    d. other security-centric controls.
2. Map Vulnerabilities - Industry vulnerabilities are published periodically and must be mapped to current software, hardware, and firmware entities.
3. Update Risk Management List - Potential risks are then created based on mapped vulnerabilities. These risks are managed through risk management processes.
4. Prioritize Risk - Risk need to be prioritized based on the impact on business goals, regulations, operating environment, and safety considerations. Organizations should have overall guidance on acceptable risk postures. For OT systems typically very little risk is acceptable, but this needs to be defined by the organization.
5. Mitigate Risk – There are several strategies to mitigate risks through process change, technology, or cultural change in the organization. Not all risks need to be mitigated. This decision must be made based on the overall organization's security posture.

Prevent Cyber-attack

Cyber-attack prevention comes in many different flavors, techniques, and strategies. Not all IT best practices apply to the OT space because of the traditionally limited access to OT networks. However, this is changing as OT devices share data more readily with IT networks and devices.

Because of the potential cross-over between OT and IT, a re-evaluation of IT prevention best practices should be part of the OT Cyber Prevention strategy. The following are some of the secondary use cases of the prevent cyber attack use cases.

Control Network Traffic – OT networks require more fine-grained control of communications between devices on the network. Firewall rules may not be sufficient to control traffic to prevent cyber threats.

Manage Endpoint Protection - endpoint protection like malware and personal firewalls on laptops and mobile devices are traditional IT strategies that can be applied to Level 1-2 OT devices.

Control Access to Devices – Not only does this use case include the traditional access control mechanisms from the IT world, but this should also include USB key access, network access, and downloading software to devices in all forms. All data from outside the OT network must pass through a secure airlock mechanism for software verification and security scanning before entering an OT device.

Multi-factor authentication for access management - multifactor authentication. It is critical for users coming onto the OT network, even if they've been authenticated on IT networks. Additionally, devices on the OT networks should be attested to certify their identity.

Encrypt communication on OT network - A common practice in IT networks is to encrypt all data in transit and at rest. OT networks have not encrypted their communication in the past because they were in a "closed" network. This false sense of security has led to many data leaks and ransomware scenarios.

Detect Cyber Threats

Traditionally cyber threat detection requires data analytics on large volumes of network logs, machine logs, and access logs. Because OT networks in the past have been isolated, many organizations have not spent the time or resources to monitor OT networks like their IT networks. This myopic view of the cyber threat landscape has led to some historic cyber breaches over the last ten years [1].

IT's cyber threat detection techniques should be leveraged to improve OT's detection capabilities. Additionally, OT and IT bridges and gateways should be monitored from both sides of the bridge to monitor and protect critical infrastructure.

The following are secondary use cases of the detect cyber threat use case.

Monitor and log OT network for cyber threats – This follows the traditional IT network best practices. It is essential to recognize that the traffic on the OT network should be more predictable, and it is easier to find nefarious traffic patterns in the logs.

Monitor Host machines, controllers, and devices for cyber threats - Because OT networks contain machines, controllers, and devices (Level 0-3 entities), it is essential to realize that automation might not be able to be performed on all of the entities.

Monitor and log access to OT networks - OT networks typically have strict controls. Accessed by devices, individuals, and applications. These strict controls should be monitored, and variances called out. This includes virtual and physical access to OT devices and networks.

Remediate Risk

One of the significant differences between OT and IT networks and infrastructure is the remediation of risk. What are the most often used remedies? Is isolation of infected devices from the rest of the network the best idea? Does this isolation decrease the infection throughout the IT infrastructure, both on-prem and in the cloud? Because most of the devices are homogeneous in an IT infrastructure, workloads can run on any set of machines at any time. However, this is not true for OT infrastructure, where specific applications, devices (level 2), and controllers (level 1) control specific machines (level 0) in the OT infrastructure. It is often impossible to migrate applications or control from one device to another because of the symbiotic relationship between entities in levels 0, 1, and 2. Traditional IT guaranteeing (Darren – remediating?) techniques come at a much higher risk to functional safety and must be dealt with differently. The following are secondary use cases of the remediate risk use case.

- Develop critical infrastructure action response strategies - Because each OT environment is different and functional safety requirements are unique, the infrastructure manager and OT operations must work together to develop critical infrastructure action responses when incidents occur.
- Evaluate Critical Infrastructure Risk - Even with action response plans, evaluating the real risk is essential so that critical infrastructure and functional safety requirements are understood before action plans are activated.
- Isolate the infected node's traffic - Traditional IT network node isolation should still be considered an essential tool to prevent infection from spreading in OT networks. However, the impact on the functional safety and operations of the system should be taken into account.
- Rebuild the infected node - The ability to rebuild levels 1,2 and 3 entities back to known good states after an infection is critical for disaster recovery plans.

Update Infrastructure

An Achilles Heel of OT infrastructure is the ability to effectively update entities in levels 1, 2, and 3 to prevent vulnerabilities from being leveraged by cyber-criminals. In the past, OT professionals relied on air-gapped networks to protect OT infrastructure from nefarious cyber-attacks over the Internet. However, cybercriminals have become more sophisticated in their attacks. They are easily circumventing traditional airgap networks.

One of the techniques used is "hopping the air gap" when updating devices and applications in OT networks. This has increased the fear of patching and allowing any new software in OT networks. In critical infrastructure, however, the risk must be calculated on leaving unpatched hardware and software stacks in OT networks, compared to patching and protecting OT infrastructure against known vulnerabilities. This should be part of the remediate risk use case risk mitigation plans.

This use case has several secondary use cases, as listed below.

Allow Vendor to connect to OT device - There are several vendors in OT devices and controllers (levels 1 and 2) that require manual updates from vendors, including using USB keys to transport updates, connecting to the device remotely, and downloading patches from their sites. This use case, although necessary, should be controlled and used with extreme caution.

Patch Software - Software updates should be made as quickly as possible based on the risk mitigation plan. Software bill of materials should be scanned and components compared with known vulnerabilities.

Patch Operating System - The risk mitigation plan and known vulnerabilities should include operating system updates. OSs may also run mixed-criticality applications at the same time, therefore, impacting multiple instances.

Patch Firmware - Firmware patches should be scanned for malicious code and compared to known vulnerabilities.

Update connection policies – Changing connection policies during updates of devices should be considered for specific periods, thus limiting the exposure of the OT network's protentional cyber threats.

Respond to Events

Many primary use cases rely on the "Respond to Events" use case to handle events they uncover. How the organization or system responds is defined in the "remediate risk" use cases specific to creating and managing the action response plan. Three categories of events need to be governed by the system:

Cyber events include any cyber threat detection, vulnerability notification, and vulnerability scan exposures.

Digital events - Digital events can be triggered by applications, services, or even individuals in control centers.

Physical events - Physical events occur from the physical world and are detected by sensors or individuals monitoring levels 0 and 1. Physical events can also occur due to natural disaster, theft, destruction of equipment, or other physically triggered events.

Maintain Functional Safety

One of the primary use cases specific to OT networks and critical infrastructure is the maintenance of functional safety of the plant, facility, or public infrastructure. Because OT networks manage physical devices, functional safety must be maintained to prevent loss of limb or life.

Some organizations must utilize additional techniques like digital twins or simulation before updating critical infrastructure. The following are the secondary use cases for the "Maintain Function Safety" use case:

- Monitor the health of the devices (Level 1-2) - monitoring the health of controllers and devices is critical for maintaining the safety of level 0 machines controlling the physical world.
- Monitor the health of the infrastructure (Level 0) - In highly critical systems, more than one sensor is required to monitor the health of machines (typically 2 of 3 voting). At Level 3, devices monitor the health of the physical world machines.
- Schedule maintenance downtimes as possible - An increase in artificial intelligence has given Infrastructure managers a better picture of preventive maintenance of level 0 machines, giving them the ability to schedule smaller windows of downtime for critical infrastructure to improve functional safety.
- Test Updates with a digital twin of the critical infrastructure – Another option commonly used method to decrease risk and improve functional safety is utilizing computing power to create a digital twin to simulate updating critical OT infrastructure.

Holistic Architectural Approach

Because OT infrastructure and operations have different goals and operating environments, traditional IT cyber security best practices do not always fit properly. There have been many efforts to try and utilize IT cybersecurity tools in the OT space, but there always seems to be some gaps that expose the OT infrastructure to cyber-attacks [7].

A holistic approach to OT cyber security must be developed to overcome the shortcomings of the current patch-quilt system that many OT organizations deploy today [8]. The architecture needs to handle the traditional IT cyber security use cases and the unique OT use cases simultaneously. Figure 4 High-level OT Security Architecture shows a proposed high-level diagram of the solution.

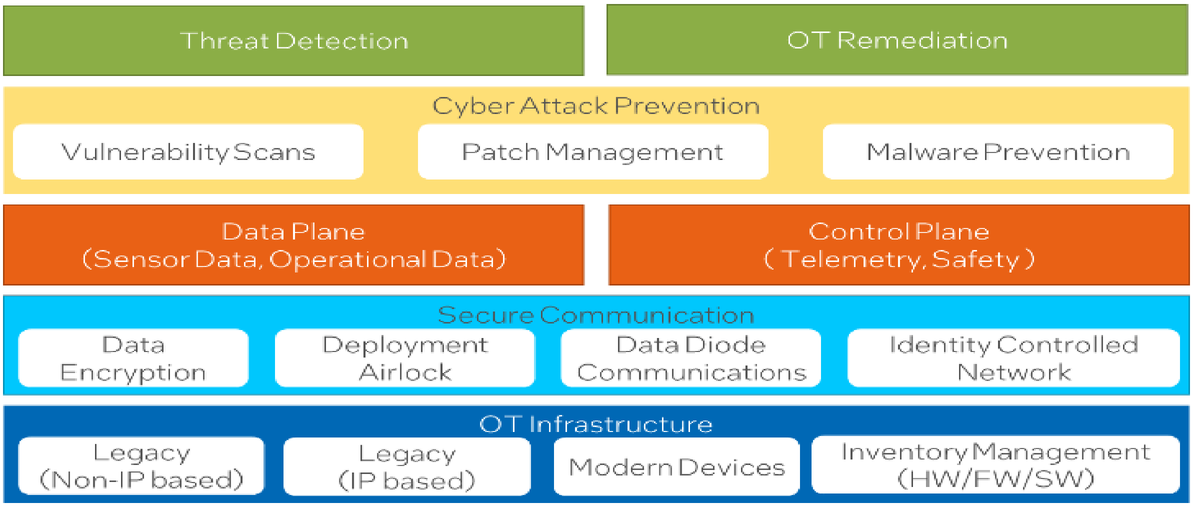

Figure 4 High-level OT Security Architecture

OT Infrastructure

Because OT infrastructure is highly heterogeneous, it is not sufficient to manage the OT infrastructure the same way as IT infrastructure. Leveraging the Purdue model's levels for infrastructure entities is a good starting point. However, because the life cycles of many Level 0 and 1 machines and controllers are decades, many entities are decades old and must be managed differently. The critical components of OT infrastructure are:

- Inventory Management (HW/FW/SW)
- Modern Devices
- Legacy Level 0-2 (Non-IP Based)

- Legacy Level 2-3 (IP Based)

Secure Communication

Functional safety drives many of the security positions in OT infrastructure. However, traditional OT networks relied on air gap networks to secure communications between machines, controllers, and devices. This security position has left a gap that exposes OT infrastructure to cyber-attacks, data leakage, and data spoofing. Recently, some new techniques have been used to overcome OT's myopic security position. These are represented as components of the secure communication subsystem.

- Data Encryption
- Secure Man Trap Deployments
- Data Diode Communications
- Identity Controlled Networking

Control Plane

Many OT designs focus on the control plan of the OT systems, which control and manage level 0-2 infrastructure entities. Since these are critical to functional safety, limited access to the control plane must be maintained and audited. Segmenting the control plane and data plane is essential in securing OT infrastructure. Network traffic over the control plane fundamentally differs from network traffic on the data plane.

Data Plane

In some respects, the data plane has been ignored in OT infrastructure, where machine telemetry, sensor data, and environmental data can be fused to provide insight into business operations, including predictive maintenance, to optimize scheduled downtime, optimizations of workflows, and increased functional safety.

Because many deep analytics tools are unavailable on legacy edge infrastructure, much of the OT Data must be moved to IT infrastructure or modern smart edge devices to perform this work. The reluctance to connect OT and their network is primarily due to the fear of IT-based cyber-attacks spilling over to OT infrastructure. Managing the data plane and control plane separately is vital to preventing cross-contamination.

Cyber Attack Prevention

Many traditional IT cyber-attack prevention tools and methodologies can be used in this subsystem with some augmentation in the patch management and vulnerability scans.

- Vulnerability Scans
- Patch Management
- Malware Prevention

Threat Detection

Many of the same techniques for threat detection can be utilized from IT for OT infrastructure. This includes state analytics on network, host, and system logs searching for known patterns of cyber intrusion. However, OT network traffic on the control plane is fundamentally different than traditional IT network traffic and much more predictable. This predictability can give threat detection algorithms better insight into network security, finding intrusions much faster.

OT Remediation

Remediation in OT infrastructure is fundamentally different than IT infrastructure. This is primarily due to the functional safety aspect of OT infrastructure. The traditional IT approach to remediation includes quarantining infected nodes and moving workloads to uninfected homogeneous infrastructure. Because OT infrastructure controls the physical world, functional safety is critical to OT operations.

OT remediation should enable different modes of remediation that may include degraded operations, isolation at levels 2 and 3 in the Purdue model, the shutdown of complete systems, or any number of safety protocols defined in the event response action plan. Because there are so many factors affecting OT remediation, it must be captured and managed. This subsystem is responsible for capturing and automating, where possible, the action responses for cyber, digital, and physical events in the environment.

Conclusion

Cyber-attacks on OT infrastructure are rising, and the sophistication of these attacks warrants immediate action to secure our critical infrastructure. Leveraging IT security best practices is a good start, but it does not cover all OT security concerns. Identifying those gaps and developing a holistic OT cyber security architecture is fundamental to protecting our critical infrastructure.

Most organizations and vendors fail to understand the OT and IT paradigms and have difficulty understanding the fundamental differences between them. Building a philosophical bridge between the two paradigms is critical in moving OT and critical infrastructure forward. Intel's committed to addressing these challenges and actively working on solutions together with our ecosystem partners .

References

[1] G. Makrakis, C. Kolias, G. Kambourakis, C. Rieger and J. Benjamin, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," *IEEE Access Access*, pp. 165295-165325, 2021.

[2] TSA, "Surface Transporation Cybersecurity Toolkit," TSA DHS, Dec 2021. [Online]. Available: https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit.

[3] EU Standards, "Railway applications -Cybersecurity," *CLC/TS 50701*, 2020.

[4] ISASecure, "Component Security Assurance (CSA) - version 1.0.0," 2019.

[5] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to Operational Technology (OT) 3," *NIST SP 800-92r3*, 20222.

[6] D. Greenfield, "Is the Purdue Model Still Relevant?," AutomationWorld, 12 May 2020. [Online]. Available: https://www.automationworld.com/factory/iiot/article/21132891/is-the-purdue-model-still-relevant.

[7] T. Nuth, "Fighting for holistic IT, OT security," 29 May 2017. [Online]. Available: https://www.controleng.com/articles/fighting-for-holistic-it-ot-security/.

[8] S. D. Antón and H. D. Schotten, "Putting Together the Pieces: A Concept for Holistic Industrial Intrusion Detection.," in *Proceedings of the European Conference on Cyber Warfare & Security*, Kaiserslautern, Germany, 2019.

[9] A. Akbarzadeh and S. Katsikas, "Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems," *IEEE Open Journal of the Industrial Electronics Society*, vol. 3, pp. 318-328, 2022.

[10] S. M. Belal, "The Top 7 Operational Technology Patch Management Best Practices," 2021. [Online]. Available: https://gca.isa.org/blog/the-top-7-operational-technology-patch-management-best-practices.

[11] CISA, "Critical Manufacturing Sector Security Guide," *Cybersecurity and Infrastructure Security Agency*, June 2020.

[12] *How secure is Your Plant: A Holistic OT Cybersecurity Toolkit for Industry 4.0.* [Film]. Engineering USA, 2021.

[13] V. Kumar and C. Gupta, "Cyber Security Issue in Smart Grid," in *2021 IEEE 4th International Conference on Computing, Power and Communication Technologies*, Roorkee, India, 2021.

[14] U. Masud, "OT Patch Management Strategy: Seven Best Practices," 2021. [Online]. Available: https://www.rockwellautomation.com/en-us/company/news/blogs/ot-patch-management-strategy--seven-best-practices.html.

[15] D. Palmer, "Manufacturing is becoming a major target for ransomware attacks," 13 Nov 2020. [Online]. Available: https://www.zdnet.com/article/manufacturing-is-becoming-a-major-target-for-ransomware-attacks.

[16] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski and J. McCarthy, "Cybersecurity Framework Manufacturing Profile," *NIST IR 8183*, p. 50, 2017.

[17] Verve, "Verve Industrial for OT/ICS Patch Management," 2022. [Online]. Available: https://verveindustrial.com/verve-security-center/patch-management/.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be secure.

* Other names and brands may be claimed as the property of others.