Securing operational technologies

White paper

A holistic security approach towards Operational Technologies (OT)

Computer networks play a central role in business as more organizations are becoming fully digital and heavily-reliant on technology to carry out business tasks. Connecting Operational Technologies (OT) to applications hosted in Information Technologies (IT) data centers and in the Cloud is a critical factor for reaping benefits of the fourth industrial revolution, where large amounts of data can be stored and processed for various purposes. At the same time, there are many newly introduced security concerns, as OT networks have traditionally been isolated from the IT networks and the Internet for the security and reliability. The purpose of this paper is to provide a framework for security of OT networks so that they can become a business enabler and play a role in creating a competitive edge.

Basic definitions and acronyms

OT is a collective name for hardware and software used in different industries including but not limited to manufacturing, oil and gas, utilities, healthcare, and others. Gartner defines Operational Technology as "hardware and software that detects or causes a change, through the direct monitoring and/or control of physical devices, processes and events." Many IT security professionals may not be familiar with these terms as they seldom have to use them. The following definitions show some of these technologies, which are collectively referred to as OT.

- **Industrial Controls Systems (ICS) -** Devices and systems used to control industrial processes.
- **Process Control Networks (PCN) -** A communications network that connects different components of OT to enable real time data collection and controls or industrial processes.
- **Supervisory Control and Data Acquisition (SCADA) -** A combination of sensors, communication methods, controllers and software to collect data at a central location. SCADA is typically architected as a distributed system spread across geographical areas. Examples include oil and gas pipelines.
- **Distributed Control Systems (DCS) -** A distributed industrial control system with many autonomous controllers but no centralized supervisory control. This is in contrast to SCADA where controls are usually centralized. DCS may be more complex with large systems needing higher reliability and security with many autonomous controllers and control loops. Examples include large manufacturing plants, oil refineries.
- **Programmable Logic Controllers (PLC) -** Specialized industrial computers connected to physical manufacturing processes, robotic devices, operations, data collection, and fault detection. PLCs have specialized real-time operating systems as well as graphical/visual programming methods known as Ladder Diagrams. PLCs have digital and analog inputs/outputs to connect with physical devices. These devices could be very small as well as large rack-mounted machines.
- **Remote Terminal Units (RTU) -** Devices directly connected to sensors or actuators.
- **Human-Machine Interface (HMI) -** Sometimes also referred to as man-machine interface are typically software components to interact with PLCs and other controllers. Consider this as a graphical user interface to industrial processes, installed on a regular server or desktops connected to PLCs and other OT technologies.

The OT industry also uses other terms as well. The above list is not exhaustive and is presented here to establish a common terminology for further discussion in this white paper.

Operational Technology Security - Business imperatives

Why should business and security leaders pay more attention to the security of OT systems? There are many reasons as explained below. The essential business need is to use data from OT technologies and convert it into an asset to gain competitive advantage. Innovation in many industries relying on OT systems depend on data and analytics, which in turn require massive storage and processing capabilities in the Cloud. Security of this data and analytics, as well as broader network connectivity, has become a major business imperative for safety and reliability of OT systems and the physical processes these systems support. There are five current business imperatives related to OT.

1. **OT as enabling technology for fourth industrial revolution** - The fourth industrial revolution, also known as industry 4.0, is building on human progress of the past with rapid changes in the 21st century to revolutionize the way we live and blurring the lines among physical and digital worlds. Technologies like Artificial Intelligence (AI), Internet of Things (IoT), massive communication, Cloud and information processing/storage technologies are fueling this revolution. We are fundamentally changing the way industries work, and operational technologies are a big part of it. Businesses that use OT have their survival at stake if they are not part of this.
2. **IT/OT convergence -** To enable use of technologies like IoT, Cloud computing, and artificial intelligence, convergence and connectivity of IT and OT systems is needed. It provides huge benefits of collecting massive amounts of data from OT systems, storing and processing this data in the Cloud, and using it for improving OT processes. At the same time, IT/OT convergence creates new security challenges that were isolated to IT systems in the past.
3. **Emergence of ransomware targeting OT -** As a recent phenomenon, ransomware attacks against OT systems are a major threat, not only from a financial perspective but also in terms of personal security and disruption of day-to-day functions. While ransomware is on top of mind for business executives at this point in time, OT has been a target for malware for many years resulting in disruptions to production systems.
4. **IP enabled OT systems -** In the past, OT systems were kept isolated. They used different communication protocols than the public Internet. With a need for IT/OT convergence, many newer OT technologies support the same IP protocols that are used on the Internet and present some security challenges.
5. **Secure semote access for vendors -** For faster support, more and more vendors request remote access to OT systems in addition to local/physical access.

How Operational Technology is different from traditional Information Technology

OT has traditionally been related to processes and systems that touch the physical world and is different from IT in a number of ways. Given these differences, many security aspects of OT systems are also different from IT systems.

1. **Longer lifespan** - While software and hardware used in IT systems has a short life, OT systems may remain in use for decades. People who designed and built these OT systems may have retired, taking their knowledge of these technologies with them. In many cases updates and patches are not available for these systems. They may also be prone to new threats that did not exist at the time when these systems were built. For this reason, the strategy to secure these systems needs to be innovative and different from IT systems where security updates and patches are readily available.
2. **Different solution objectives: Availability vs. confidentiality** - When it comes to information security triad (Confidentiality, Integrity and Availability or commonly known as CIA), the objectives of IT systems are highly weighted towards confidentiality and protecting data. On the other hand, availability is the primary objective of OT systems to keep industrial processes operational. Due to this fundamental difference in the primary objective, the security strategy is also different.
3. **Potential for cascading impact -** While typical incidents in IT systems impact one or a small number of businesses, OT incidents can cascade to much larger and broader impacts on businesses and society. For example, security incidents resulting in outages for electrical grids or disruption of fuel pipelines can impact an entire region of the country.
4. **IT and OT different reporting structure -** Traditionally IT and OT are managed separately, not only from a technical perspective but also from an administrative perspective. IT and OT are two different organizations. With a need for converged IT/OT, organizational changes are needed to align.
5. **Antiquated network architecture -** Many OT networks are designed as isolated with minimal connectivity to broader Internet and Cloud services. Newer requirements for massive data collection and use of AI and analytics technologies in the Cloud require a new architecture model. The IT networks, on the other hand, have evolved over time and don't suffer from this issue.
6. **Fragility of OT equipment** - Many of the OT devices don't respond well to vulnerability scanning tools and may stop working or malfunction as a result of scanner activity.
7. **Lack of patching -** Patching tools and practices, commonly used in IT networks, usually don't work in OT networks because of implication on physical processes in case a patch results in undesirable results.

A recent research report, OT:ICEFALL [22] shows “insecure by design” implementation of many OT systems including insecure engineering protocols, weak cryptography, broken authentication, insecure firmware updates and remote code execution. The IT systems are relatively more mature in these basic areas compared to OT systems.

While many concepts of security for IT and OT networks overlap, due to these differences, strategy of security of OT networks may vary for different industries.

OT security - State of the affairs from Verizon DBIR

Leveraging incident data collected for the Verizon 2022 Data Breach Investigation Report (DBIR) [26] provides unique insight into some of the types of real-world incidents that have impacted OT systems. However, it should be noted that the DBIR does not collect or codify ALL known incidents, but uses a sampling approach in concert with combining various data sources to create the DBIR dataset.

Figure 1: Major motives behind OT incidents from DBIR data set.

Figure 1 demonstrates the main motives associated with incidents impacting OT systems, which follows similar trends as the general dataset, with criminals targeting systems for financial gain, such as through the use of Ransomware which occurred in 34% of the incidents. It is difficult to know whether or not the OT systems were the primary target for these incidents or if they were simply secondary impact to the main objective, which was to impact the business to coerce the owners and operators to pay the ransom. The next most common motives are Espionage and Grudge/Ideology, with Espionage largely consisting of nation state or nation-state affiliated actors and Grudges and Ideology coming from a variety of different actors.

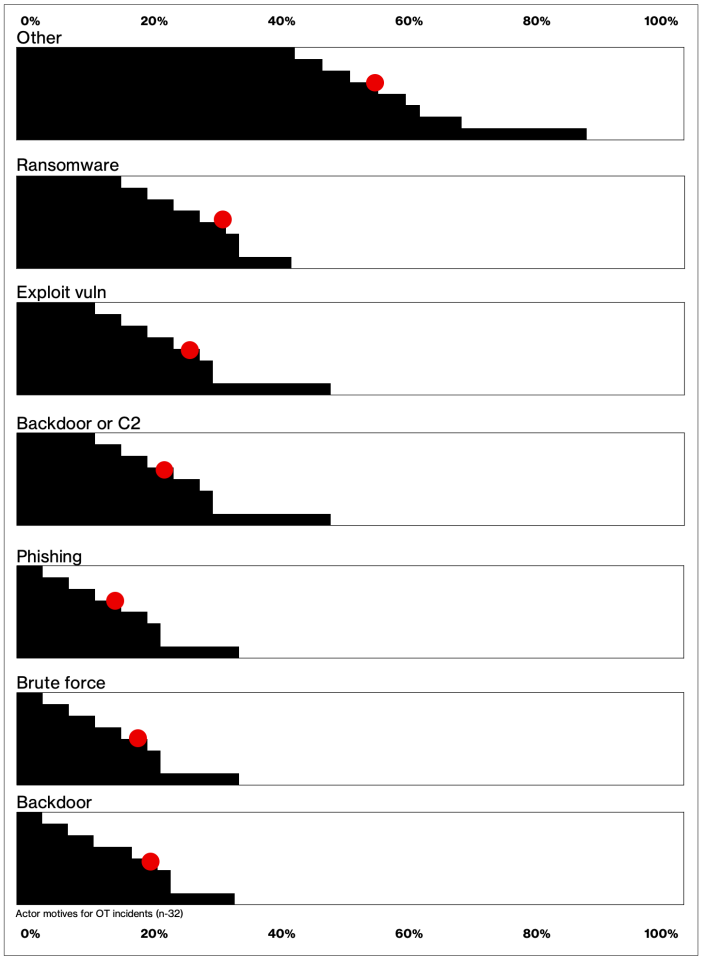

Figure 2: Actions against OT systems from DBIR data set.

In terms of Actions, Figure 2, Ransomware tops the cases that show up in the DBIR data, followed by other Actions such as the using exploits against vulnerabilities, phishing and targeting of weak credentials through brute forcing. Complementing the types of actions, there is also the vector which captures how actions occurred, with 25% of incidents involving direct access to the impacted system and 20% of incidents occurring through some form of Remote Sharing Desktop application, either natively supported within the Operating System (OS) or through third party applications. In addition, 15% of the OT incidents occurred through Email, which might indicate improper separation between the OT environments and the business environments enabling actors to move from corporate systems to more sensitive networks.

MITRE ICS ATT&CK Navigator

MITRE ATT&CK Navigator is an online tool [12]. It provides techniques and tactics used by attackers at different stages. The following is a screenshot of this tool for industrial controls systems. As stated in the tool help, you can use it to "visualize your defensive coverage, your red/blue team planning". You can use color coding in the Navigator to identify capabilities, gaps, as well as use it as a communications tool.

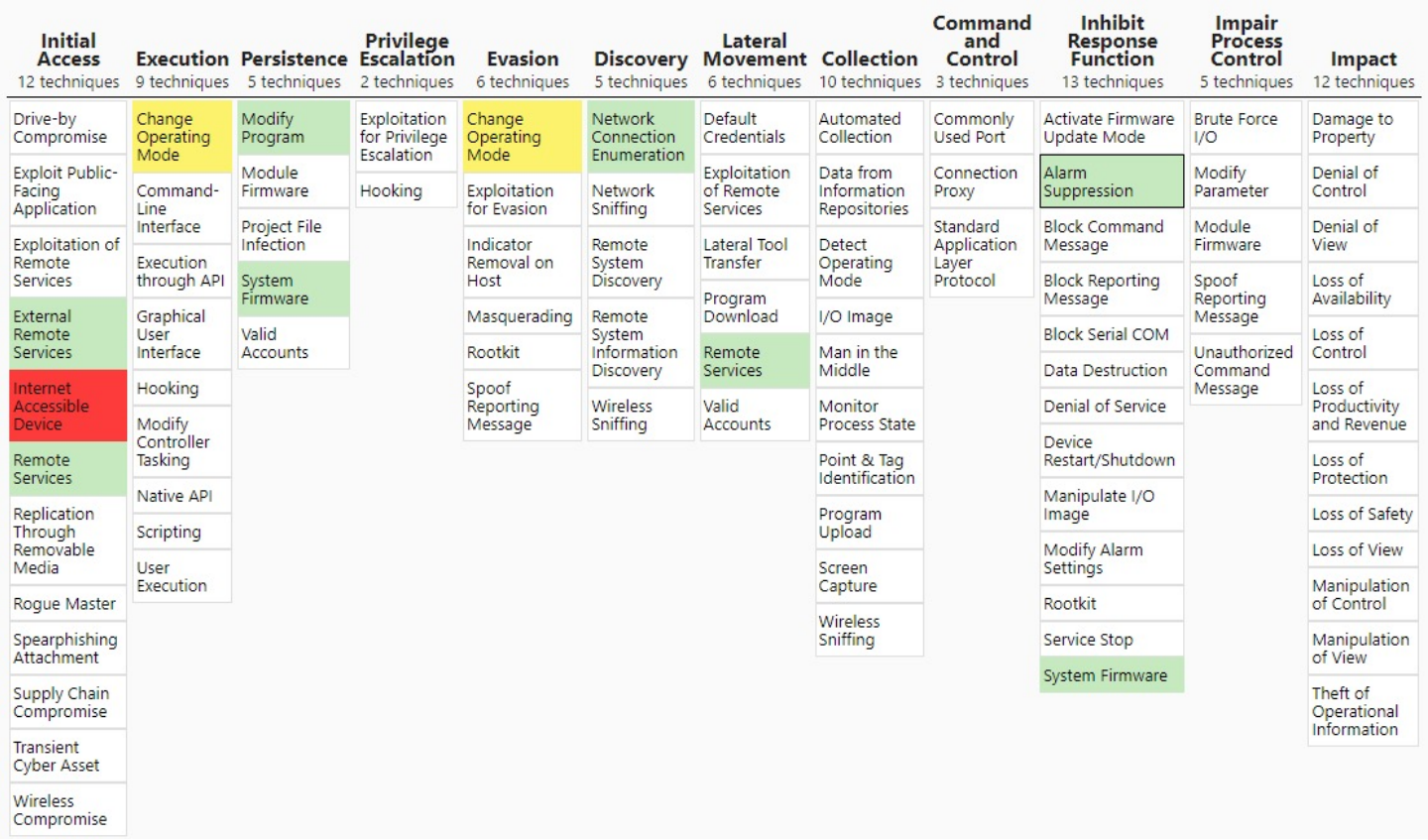

Figure 3: MITRE ATT&CK Navigator tool

The advantage of using the MITRE ATT&CK Navigator tool is that it is well understood in security communications with accepted definitions of the common terminology used. It also provides pointers to create a strategy for OT security. For example, there are five techniquest under "Discovery," which help identify security tools that one can implement to discover attackers within an OT network.

Initial access vectors for exploitation

MITRE ATT&CK provides a great list of initial access vectors for OT systems, twelve to be precise. The National Security Agency (NSA) and Cybersecurity & Infrastructure Security Agency (CISA) published an advisory [13] outlining some areas of initial entry points, tactics, techniques, and procedures. Some of these are listed below:

- Using IT systems to pivot to OT systems by getting an initial entry point in IT systems using spear phishing
- Use of ransomware in both IT and OT systems
- Access to Programmable Logic Controllers (PLCs) connected to the Internet with no authentication or default passwords
- Using standard network protocols to get access to controllers
- Program download to controllers

OT security assessments performed by Verizon's Cyber Security Consulting Services Services also provide insights into vulnerabilities that enable initial attacker entry points. Four top vulnerabilities observed by Verizon are as follows:

1. Lack of network segmentation
2. Poor access controls
3. Issues with physical security
4. Lack of maintaining a robust hardware and software inventory

A well-established OT security program, starting with asset management and access controls, can help avoid these entry points.

OT security architecture

As OT systems connect with physical processes and manufacturing, security of these systems has implications for safety as well as significant loss in revenue. The Purdue Model is a layered network segmentation model proposed in early 1990s and has served as a reference architecture for many years.

The Purdue Model

The Purdue Model is a layered model segmented into different levels as described below and in the following diagram. Each layer sits on top of the other and implements specific functionality of manufacturing processes.

- Level 4 and level 5 is a typical IT network including access to the Internet, hosting business applications, such as Enterprise Resource Planning (ERP)
- Corporate Demilitarized Zone (DMZ) segments IT and OT networks. Sometimes it is also called level 3.5 as it sits between level 3 and level 4
- Level 3 implements a Manufacturing Execution System (MES) or sometimes also called a Manufacturing Operations Management Systems (MOMS). Typically data historian systems are also implemented at this level to time stamp and store process data for longer periods of time
- Level 2 has most of the supervisory controls devices, SCADA and HMI systems
- Level 1 provides basic controls for sensors and actuators. This level may have intelligent devices such as PLCs and RTUs
- Level 0 is connection to physical processes, sensors for collecting data, actuators for controls

IT Environment	**Level 5**	**Internet DMZ**
	Level 4	Corporate network, enterprise, applications, domain controllers, ERP
OT Environment	**Corporate DMZ**	Application Servers, Jump hosts
	Level 3	Site manufacturing operations, Historian
	Level 2	Supervisory Controls: HMI, SCADA
	Level 1	Basic controls, PLCs
	Level 0	Processes: sensors and actuators

Figure 4: High level conceptual diagram of Purdue Model

While the actual implementation of the Purdue Model may vary from business to business, the main concepts are the same.

Architecture to enable industry fourth industrial revolution

With the advent of Cloud technologies, the need for collecting and analyzing large amounts of data, modern robotics with real time controls, and newer methods of connectivity including 5G and edge computing, the Purdue Model requires rethinking. In a modern architecture, the sensor devices are getting much more intelligent and have the capability of sending data directly to applications hosted in Cloud. Use of 5G combined with application in edge is also fueling ultra low latency needed for real time controls.

At the same time, options like zero trust access enable stricter security controls and present opportunities for simplifying the layered architecture. A number of new architectures are being proposed to better enable needs for industry 4.0 (massive data collection and analytics, AI, use of virtually unlimited processing and storage in Cloud, etc.). Businesses need to reevaluate their OT network strategy to modernize the older networks and take advantage of newer technologies that were not available at the time the Purdue Model was created.

Figure 5: Building blocks of an OT strategy

Building OT security strategy

Frameworks are very helpful in ensuring a consistent approach towards managing any cybersecurity program, including OT. Principles from existing frameworks (NIST CSF, NIST 800-53, ISO 27K, IEC 62443, NIST 800-82, NERC CIP) are a good starting point for building a customized OT security strategy for an organization.

A simplified strategy for OT security must include at least the following components wrapped in a governance structure.

1. Comprehensive asset management to keep track of what you have, how old it is, its end of life status, and software or firmware versions, etc.
2. Assessments of current state of the OT network and identification of security gaps.
3. Designing a layered network architecture with IT DMZ providing simpler access to applications hosted in the Cloud. Data-diodes [16] are useful technologies for unidirectional flow of data.
4. Continuous threat monitoring for detecting suspicious activity in OT networks both at network and application levels.
5. Use of deception technologies [17] for early breach detection.
6. A well designed and tested incident response plan.

The following subsections briefly elaborate on these components of OT security strategy.

OT asset management

Comprehensive asset management is an essential component of OT security strategy. The asset management includes not only hardware but also software and firmware versions for each component. Vulnerability management goes hand in hand with asset management.

An asset register is a good starting point for asset management. The following is just a sample of information stored in an asset register. However, organizations can maintain the structure of an asset register that suits their purpose, as long as it enables an organization to know hardware and software versions, vendor contact information, end-of-life information, and ownership status of these assets.

Asset ID	Vendor	Type	Model	Software Version	Last software update	Purpose	Physical location	Owner

An asset register should enable an organization to identify and prioritize vulnerabilities related to installed technologies, apply patches, and quickly identify owners in case of an incident.

Assessing the current state of OT networks

A good strategy starts with understanding the current state. OT networks are no exception. A good current state assessment helps identify gaps, improve processes, and recommendations for improvements. Following are some of the major areas that should be considered for inclusion in the current state assessment.

1. Maturity of asset management.
2. Physical security controls.
3. Currency of patches, updates, end of life status.
4. Network connectivity, network segmentation, and DMZ.
5. Understanding OT attack surface including but not limited to scanning public IP address space and using Shodan to identify OT devices accessible from the Internet.
6. Vendor support process.
7. Use of protocols, survey of all unused ports, status of firewall rules.
8. Security of wireless networks.
9. Use of dual-purpose and multi-purpose systems (e.g. a system used as part of OT infrastructure as well as for checking emails by operators).
10. Supply chain risk.
11. Threat monitoring capabilities.
12. Incident response planning and maturity.

While current state assessments can be performed internally, a good practice is to invite an external vendor with expertise in performing these assessments and for making recommendations to bring OT networks up to prevailing industry standards.

OT network architecture

Network segmentation and creating zones/layers for different parts of the OT network is a standard practice. The Purdue Model, as discussed earlier, provides a good blueprint and starting point and has been used in OT networks for more than two decades. It divides the OT network into multiple zones with defined boundaries and services to be included in each zone.

- **Data flow diagrams -** Along with physical network design, virtual connectivity of different OT network components and updated data flow diagrams are very important to ensure that the concept of layered approach and zones is properly implemented.
- **Maintaining DMZ -** Modern OT networks require connectivity to corporate networks, Cloud services, and the Internet. Maintaining proper DMZ environments for both the corporate network and the Internet is essential for OT security.

- **Strong access control -** In our observations, one common vulnerability leading to breaches is weak access control to OT systems from within the OT network, corporate networks, and vendors. Going beyond multi-factor authentication, zero trust access technologies are now readily available and should be explored.
- **Use of Data Diodes -** Data diodes [16] are technologies that provide a unidirectional flow of information in computer networks. For collecting data outside of OT networks, these technologies are very useful in ensuring that data flow outside of the OT environment is enabled but attackers are not able to use this connectivity to get into the OT network.

A careful network architecture not only enables and simplifies the connectivity of OT components but also helps in implementing reasonable security measures to protect the OT network.

Continuous Threat Monitoring

Threat monitoring in OT networks has similarities with threat monitoring in the IT network. At the same time, there are differences that security and business leaders should consider. For example, many protocols used in OT networks are quite different from those used in IT networks. For that reason, not only do the monitoring technologies for OT networks need to be compatible with these protocols but also the people working in security operations centers (SOC) need to be proficient in these protocols to better understand the context of an alert.

MITRE ATT&CK Navigator [12] is very useful in understanding techniques for attacking OT networks and using appropriate methods to detect attacker activity. In general, continuous monitoring should include the following components, at minimum.

1. Vulnerability management including feeding the vulnerability data into monitoring systems.
2. ICS Advisories - CISA provides ICS advisories [3] for products that should be made part of a comprehensive program for asset and patch management.
3. Integrating Threat Intelligence into monitoring systems and performing threat hunting on a regular basis.
4. Building an OT SOC or integrating OT telemetry into a converged IT SOC.
5. Passive monitoring of OT network traffic using an Intrusion Detection System (IDS) that understands OT protocols.

Timely detection of security incidents in OT networks provides an opportunity for quick response and continuous operation of critical processes.

Using deception technologies

Deception technologies [17] are an evolution of older “honeypots” and provide mechanisms for early breach detection. The basic concept behind deception technologies is an assumption that an attacker has already breached a network and is working inside it. Deception technologies include simulation of OT devices, also known as decoys, to lure attackers into interaction with these. When an attacker interacts with these “fake” OT devices, alerts are triggered, enabling detection of a network breach.

Many vendors provide deception technologies that use decoys to mimic PLCs, controllers, and other OT devices. Use of deception is an essential part of OT security strategy.

OT incident response

A robust incident response process starts with creating an incident response plan and testing the plan on regular intervals. OT incident response plan should include:

1. Identifying stakeholders.
2. Building a “first responders” team to effectively take initial steps in the incident response lifecycle.
3. Conduct tabletop exercises.
4. Backup and recovery of systems configurations and data.
5. Capturing and storing OT network data for forensic purposes in case a data breach occurs.

A good incident response plan minimizes damages, shortens down time, and builds confidence among stakeholders.

Private 5G and Edge Compute in OT

Newer applications in OT environments (e.g. real time robotics controls) require high data speed, ultra low latency, and massive connectivity for OT and Industrial IoT devices. In many ways 5G technology with edge computing capabilities is the best answer to these requirements. Private 5G options are available for customers with such application needs.

Although there are many ways to design private 5G networks, the following diagram shows one possible option with a local 5G edge installed within the OT environment enabling applications hosting with a very short round trip time.

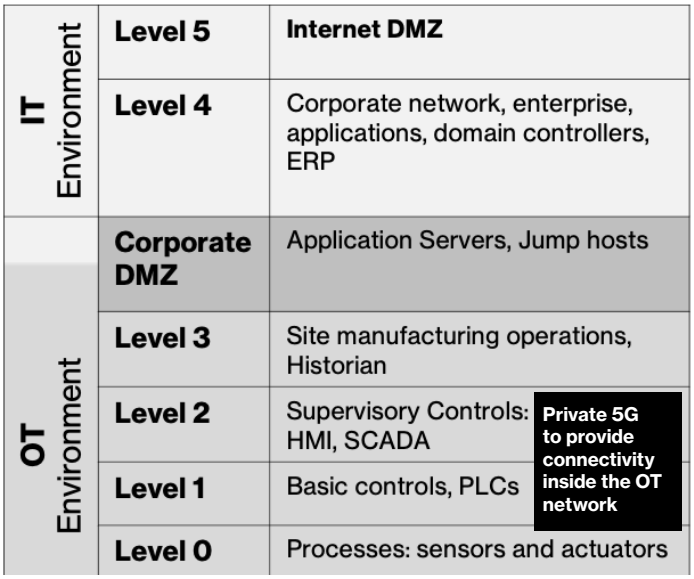

Figure 6: A proposed approach for using private 5G in OT networks

While some private 5G core controls can be managed through Cloud services, the end-to-end data paths from source to destination terminate within the OT network, providing the full control for a layered approach for network segmentation. In other design patterns, data can also be sent to the Cloud for long term storage, pattern detection and trend analysis.

NIST special publication 800-82, Guide to industrial control systems (ICS) security [19] provides guidelines for placement of firewalls. The guidelines can also be utilized in the design of private 5G network segments inside an OT network.

It should be noted that when it comes to use of wireless technologies inside an OT network, Wi-Fi is another option. A good comparison of Wi-Fi and 5G technologies is available in a separate Verizon white paper "Manufacturers get industrial strength security with private 5G" [25].

OT security recommended practices

Following are the best practices for OT systems as recommended by CISA, NIST and other public/private organizations [1][2][5]. Some recommendations are also included based upon lessons learned from Verizon's OT security assessments.

1. Create policy, standards and processes for OT systems as part of the governance structure. OT Policies and Procedures are necessary for continuity of an effective security program especially for multiple sites and global enterprises.
2. Identify OT processes that rely on IT infrastructure to understand inter-dependency of IT and OT.
3. Create a strong asset management program to know what you have.
4. Ensure physical security and access controls to OT systems. This also aligns with Verizon's top 4 findings and is often overlooked.
5. Build a process to check available patches to ICS and other OT systems. Once a patch is released, prioritize and test the patch and then apply it.
6. As part of hardening, disable all unnecessary ports and protocols at device level. Retest after applying patches to make sure a patch does not reopen previously closed ports.
7. Change all default passwords. Periodically check devices for default passwords.
8. Implement endpoint detection and response technologies where support for these technologies is available.
9. Backup data and configuration of OT systems. Test backups periodically to ensure you are able to restore devices from backup in a reliable and timely manner.
10. Regularly (quarterly or biannually) identify and secure all internal network and Internet connections. Each network connection must have a strong justification, including vendor access to OT systems.
11. Build an OT DMZ zone for any network/Internet connection. Apply proper network segmentations.
12. Review firewall policies on a quarterly basis to justify all open ports and protocols.
13. Ensure OT systems are not dual use (e.g. a computer running an OT application should not be used to check emails).
14. Create a vulnerability assessment and management program for OT systems. Subscribe to CISA Known Exploited Vulnerability database as part of the program to keep updated about and prioritize OT system vulnerabilities.
15. Integrate OT security monitoring into SOC.
16. Build, maintain and test an OT incident response/recovery plan.
17. Periodically evaluate supply chain security for OT systems including hardware and software products, vendors, and contractors.
18. Create processes to manually operate critical systems in case of a ransomware attack.
19. Maintain a Cybersecurity Awareness and Training program for those who have access to OT systems.

The above list of recommended practices is based upon practical experience and is useful for building any OT security program.

Technologies for securing OT systems

Following are security technologies and their purpose in security of OT systems and networks.

1. **Endpoint Detection and Response (EDR) -** Where available, provide continuous monitoring of end point vulnerabilities, threat detection, and mitigation.
2. **Firewalls -** Network segmentation, building a DMZ, minimize network flows to known OT systems on specific ports.
3. **OT Intrusion Detection System (IDS) -** Passive detection of OT threats, asset detection and inventory, protocol detection, open ports detection. Some OT protocols use Secure Socket Layer/Transport Layer Security (SSL/TLS) for transport security. OT IDS is also useful to detect if any weak ciphers are used in SSL/TLS implementations.
4. **Strong access controls -** Older methods included multi-factor authentication to get access to OT systems. However now we recommend exploring zero trust technologies based upon NIST 800-207 publication [18].
5. **Deception technologies -** Early detection of presence of attackers inside the OT networks.
6. **SOC -** Continuous monitoring of threats and detection of security incidents
7. **Incident response tools -** Responding to security incidents and restoring systems to their regular operations. Performing forensic analysis.
8. **Data Diodes -** These are technologies used to enable one way traffic for data collection and IDS taps to ensure data flows in one direction only.
9. **Asset tracking and vulnerability management -** We can't manage what we don't know. A system for full asset discovery and tracking is crucial for effective vulnerability management. Some commercial off the shelf products can help but a comprehensive strategy for asset tracking is required. Vulnerability management in OT systems is not the same as for IT systems, for the reasons mentioned earlier in this white paper.

A well designed OT security program will include a combination of many technologies listed above as part of the OT secure architecture.

Verizon OT services

Verizon provides a broad range of network and security services, for both IT and OT. These services include, but are not limited to the following:

1. Cyber Security Consulting Services - These services are usually delivered on a project basis with a defined scope and a statement of work.
    a. Current State Assessments of Operations Technologies and Industrial Control Systems (OTACS assessment).
    b. OT network design and modernization, including use of emerging technologies like 5G to help implement ultra low latency applications, collect massive amounts of data and connect large numbers of devices.
    c. OT Incident Response with Rapid Response Retainer (RRR) service.
    d. OT threat and vulnerability management utilizing customers' existing tools as well as implementing new solutions.
2. Managed Network Services (MNS) providing full lifecycle management of LAN and WAN networking as well as network equipment.
3. Managed Network Access Controls (NAC) in collaboration with industry leading Verizon partners.
4. Managed security services for threat detection.
5. Deception technologies as part of the overall threat detection program.
6. Passive IDS, full packet capture and analysis capabilities with Verizon Network Detection and Response (NDR) service.
7. Strategy, design and implementation of Zero Trust Access solutions that align with NIST 800-207 [18].
8. Private 5G and Multi-access Edge Compute (MEC) integration for ultra low latency and cutting edge OT applications.

Please contact otsecurity@verizon.com for more information and explore possibilities of enhancing OT network security with these services.

References

Following is a list of references for further reading. All trademarks and service marks are property of their respective registered owners.

1. CISA - Recommended Cybersecurity Practices for Industrial Control Systems
2. CISA - Rising ransomware threat to operational technology assets
3. CISA - ICS advisories
4. ICSJWG - Industrial Controls Systems Joint Working Group
5. NIST - Tips and tactics for control systems cybersecurity
6. Department of Energy - Cybersecurity Capability Maturity Model (C2M2)
7. Gartner - Operational Technical Security, Focus on Security Industrial Control and Automation Systems
8. International Society of Automation - OT Security Dozen: Series on Building an OT/ICS Cybersecurity Program
9. Wikipedia - Ladder Logic
10. Wikipedia - Programmable Logic Controllers
11. Wikipedia - Distributed Control Systems
12. MITRE ATT&CK Navigator
13. NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
14. Shodan - A tool for finding Internet accessible OT devices
15. CISA Known Exploited Vulnerabilities Catalog
16. Unidirectional networks
17. Deception technologies
18. NIST 800-207 Zero Trust Architecture
19. NIST 800-82 Guide to Industrial Control Systems Security
20. International Electrotechnical Commission (IEC) Understanding IEC 62443
21. International Society of Automation ISA99, Industrial Automation and Control Systems Security
22. OT: ICEFALL - The legacy of “insecure by design” and its implications for certifications and risk management
23. A database of OT incidents, attacks, and malfunctions
24. RISI Online incident database
25. Verizon White Paper - Manufacturers get industrial strength security with private 5G
26. Verizon 2022 Data Breach Investigations Report (DBIR)

Authors and contributors

Author

Rafeeq Rehman
Distinguished Architect Cybersecurity

Additional Content Contributors

Brian LeeVan
Principal Consultant, Professional Services

Jeff Harrison
Sr. Mgr PS Consulting

Mike Hannan
Principal Architect, Solution Architecture

Philippe Langlois
Senior Principal, Threat Intelligence

Steven Gevers
Sr. Mgr PS Consulting

Stuart Wilson
Manager Product Development and Management