INSTITUTE FOR HOMELAND SECURITY

Who's in Charge of OT Security

Institute for Homeland Security

Sam Houston State University

Joe Weiss

CONTENTS

INTRODUCTION

IT attacks are only part of what should make CSOs, CISOs and Risk Officers lose sleep. While IT cyberattacks often make the news, potentially more dangerous are Operational Technology (OT) cyberattacks and failures. Not only can the latter cause include explosions, destruction, injuries and death, but the *way* we protect OT can do so as well.

OT monitors and controls physical processes. Automating OT is more efficient and reliable than manual operations, keeps better records, doesn't need multiple rest periods every day, or have labor issues. When properly programmed, it doesn't make mistakes humans will, helps assist with maintenance, and can warn of and mitigate danger.

However, if hackers can bypass security and "take over" systems, the very processes OT protects can become extremely hazardous. This is further compounded because some OT cyberattacks have been disguised as accidental OT issues. In more than one instance, a "failure of imagination has led security teams to misdiagnose cyberattacks as benign failures.

One contributor to these "misdiagnosis" has been because the network protectors of OT do not fully understand the OT operation, communication, vulnerabilities, and how to safely protect OT. Regrettably, this lack of understanding can be dangerous.

In this paper, we will look at:

- What is OT
- OT vs. IT
- OT-Specific Vulnerabilities
- IT Hurdles in protecting OT
- Recommendations on building OT protection teams

The goal of this paper is to help CSOs, CISOs, and Risk Managers be aware of OT cyber and safety issues so they can maximize IT and OT protection without endangering OT operation.

GAP ASSESSMENT

IT Vs OT

Information is the lifeblood of most modern companies. The guardians of that information are IT teams. They ensure information is kept secure and transferred securely to the right locations. But IT network output is typically information only, whether displayed, stored or printed. That information may result in an order for physical movement (such as a shipping order) but IT is about information.

OT differs in both its components and its “output”. The National Institute of Standards and Technology (NIST) defines “Operational Technology” as: *“Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.”*[i]

In short, “Operational” means that, when OT monitors and transmit signals, physical actions result. Conveyors turn on, robots actuate, turbines generate megawatts of power and heat, pumps move liquids, automated forklifts pick up and move loads, and heaters boil liquids – all monitored and controlled by OT. If you have worked around these processes, you know the dangers associated with them.

OT monitors and transmits data accurately in a specific period of time (generally not large amounts of data):

- Process sensors record flow, pressure, speed, strain, voltage, current, chemical composition, etc., transmitting that data to controllers for real time action. As a result, the controllers adjust their output to the control equipment.
- Within machines and systems, equipment (motors, pumps, actuators, and other devices) respond to input process sensor signals, creating chemical mixtures, pressures, temperatures, flows, delivery destinations, etc.
- When production is finished, material handling devices such as storage and retrieval systems and guided vehicles, each with their own control systems and sensors, move material to shipping or storage.
- Data about what was produced is sent back to the SCADA systems and from there to the IT systems.

- Continually during these processes, productivity and safety are monitored and safety issues annunciated and reported.

Critically, OT systems are a core part of every industrial, manufacturing, and transportation system. Their loss would immediately cripple the economy, the defense, and the personal security of citizens.

Both IT and OT use IT-style networking to communicate, and frequently over the same networks. After all, the communication processes are similar, few want to install two parallel networks, and IT systems must communicate with OT systems to process orders or measure output. In fact, most attacks on OT networks come through IT networks.

IT network attacks present a path to attack OT networks connected to them. Fortunately, some IT teams are aware of this risk. For example, an abundance of caution led JBS Foods, Colonial Pipeline, and other organizations to shut down their operations during recent IT ransomware attacks.[ii]

IT Security

Some, but not all, IT teams are well-prepared to protect their networked OT. Those without OT expertise are, at best, challenged to protect OT systems. This vulnerability is further exacerbated when security teams are remote from the OT for which they are responsible and / or not in communication with the OT “owners.”

Responsibility for OT security is frequently less well-defined than it is for IT, with responsibility potentially being the IT department, engineering, production, and / or elsewhere.

DISCUSSION

OT Incidents

As mentioned above, OT incidents have been and remain potentially hazardous. Following are several examples, with various causes. Each illustrates the ability of OT to suffer or cause damage if compromised. While some were cyberattacks, all illustrate the ability of OT to cause direct physical harm (explosions, fires, crashes) or depriving a population of utilities such as water, electricity, or fuel (i.e., natural gas).

We don't have to go far to find examples of OT involvement in accidents or incidents.

Unintentional OT Incidents

Some unintentional OT-related failures with fatalities include:

2005: Texas City, TX Tank Farm Explosions
Faulty process sensors led to an explosion which killed 15 and injured 180.

2010: DC Metro train crash
Caused by train control system losing view of a train coming into the station.

2018 – 2019: Boeing 737 Max Crashes
Caused by flight control software and angle of attack sensors.

2022: Union Pacific Salton Sea Train Crash
Caused by sensor and SCADA communication issues losing view of cars on track.

The impacts from these OT incidents range from millions to billions of dollars, not including deaths and injuries.

Malicious OT incidents

Examples of malicious OT incidents include:

Aurora

Electric grid stability requires synchronizing generator frequencies with the grid before connecting them to the grid. If generators are not synchronized, damage can occur to generators, grid systems, and any other Alternating Current (AC) equipment connected to the grid.[iii] To prove that generators were vulnerable to cyberattacks, the U.S. Department of Homeland Security (DHS) and Idaho National Laboratory (INL) conducted a test on March 4, 2007 to demonstrate that cyberattacks alone could cause physical impacts as significant as if dynamite was used (Figure 4).[iv,v] INL installed a 2.25 MW (3000 horsepower) generator and connected it to the test substation with a breaker in between. The breaker (as in other power systems) could be remotely operated (either in or out-of-phase).

INL used remote access (e.g., cyber) to open and close the diesel generator's circuit breakers (no malware involved) to create an out-of-phase condition from the grid. The out-of-phase condition resulted in very high torques causing the engine's physical destruction in a short period of time.[vi,vii ,viii]

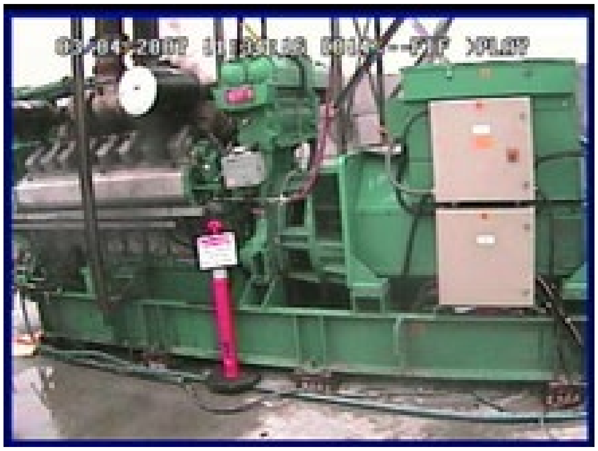


Figure 4 Aurora generator test

Other cyber / OT incidents which involved physical damage to OT include:

Stuxnet - Iran

The 2009-2010 Stuxnet attack on Iran's nuclear power program is well known. The virus was loaded onto a computer running the Microsoft operating system, then "wormed" its way to a computer connected to the Siemens PLCs. It then varied the speed of the centrifuges, causing them to become unstable while "telling" the operator displays that the centrifuges were operating in normally. Goodbye, centrifuges.

German Steel mill

In 2014, an "unnamed" German Steel Mill suffered a cyberattack that targeted the ICS of a blast furnace, causing the furnace to shut down improperly. This unstable and improper shutdown caused "massive damage" to the furnace.[ix]

Predatory Sparrow

On July 13, 2022, multiple Iranian steel facilities experienced a cyberattack that “caused the foundry to spew hot molten steel and fire onto the factory floor. The hacktivist group “Predatory Sparrow“ claimed responsibility [x]

Muleshoe, Texas Water System Attack

In January, 2024, Russian hackers breached the city of Muleshoe, Texas’ water tank software, which allows operators to interact with and control the tank. The tank overflowed for 30 to 45 minutes before officials took the machine offline and regained control of the system. Two nearby Texas cities reported cybersecurity concerns after similar incidents.

Unitronics controllers

In November 2023, Iranian IRGC-affiliated actors gained access to Israeli-made Unitronics PLCs in multiple US entities including water and wastewater utilities, food and beverage providers, and ports.

Network security (IT and OT) Causing OT incidents

Some incidents have been caused (though unintentionally) by IT/OT teams.

Security Patch - Gas Turbine

Cyber security changes can impact the reliability and safety of a system if the impacts on engineering and operations are not adequately evaluated. For example, a network security team developed a security patch to be installed on a gas turbine (typically used for power generation). The patch was tested for cyber security but was not evaluated for plant operation. Consequently, the patch caused a loss of view of the turbine control system displays. Further, the patch prevented the operator from being able ability to shut down the turbine from their console. As a result, the turbine had to be shut down using emergency protocols – not a process designed to maximize turbine life and a challenge to plant safety.

Inappropriate Cyber-Threat Testing – Utility Substation

Under the auspices of the CSO, a large utility performed security scans of several very critical substations. The security team initially scanned data center assets, but then expanded the scanning into NERC CIP transmission substations using Distributed Network Protocol polling,. The IT team had no previous substation scanning experience and did not notify the internal support groups are responsible for the substations. The inappropriate scanning affected hundreds of transmission level protective relays.

Port scanning with this new tool caused the real time protocol operation of the relays to stop and suspend operation at the CPU while the SCADA left the DNP / non-real time operations alone - the worst possible circumstance. To restore operation, hundreds of high-voltage relays had to be cut out and rebooted. In every case, all the devices at each substation were affected at the same time. What was a security scan appeared to be a DDOS attack resulting in equipment malfunction. This illustrates an almost catastrophic failure caused because IT was unaware of the differences between network security and control system device capabilities.

Background On Control System Safety Architecture

OT requires fast and accurate communication. With an eye to security, the Purdue Enterprise Reference Architecture was developed in the 1990s by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing.[xi] The Purdue model provides a framework for segmenting industrial control system networks from corporate enterprise networks and the internet, providing gaps between each layer.

The model used five zones (six including the Cloud) to segregate portions of OT systems. Level 0 is the actual process and process measurements in real time.

- Level 1 is basic control which is milliseconds to seconds.
- Level 2 are the plant networks which operate in seconds to few minutes.
- Level 3 are the production scheduling and quality assurance systems which operate in many minutes to hours.
- Level 3.5 is the Demilitarized Zone (DMZ) which is the interface between the engineering systems and the business networks. Not an original part of the Purdue model, it was added to ensure separation between OT and IT networks.
- Level 4, 5, and 6 (the cloud which isn’t shown) are the enterprise networks, long-term historians, and external parties which occur in days or months.

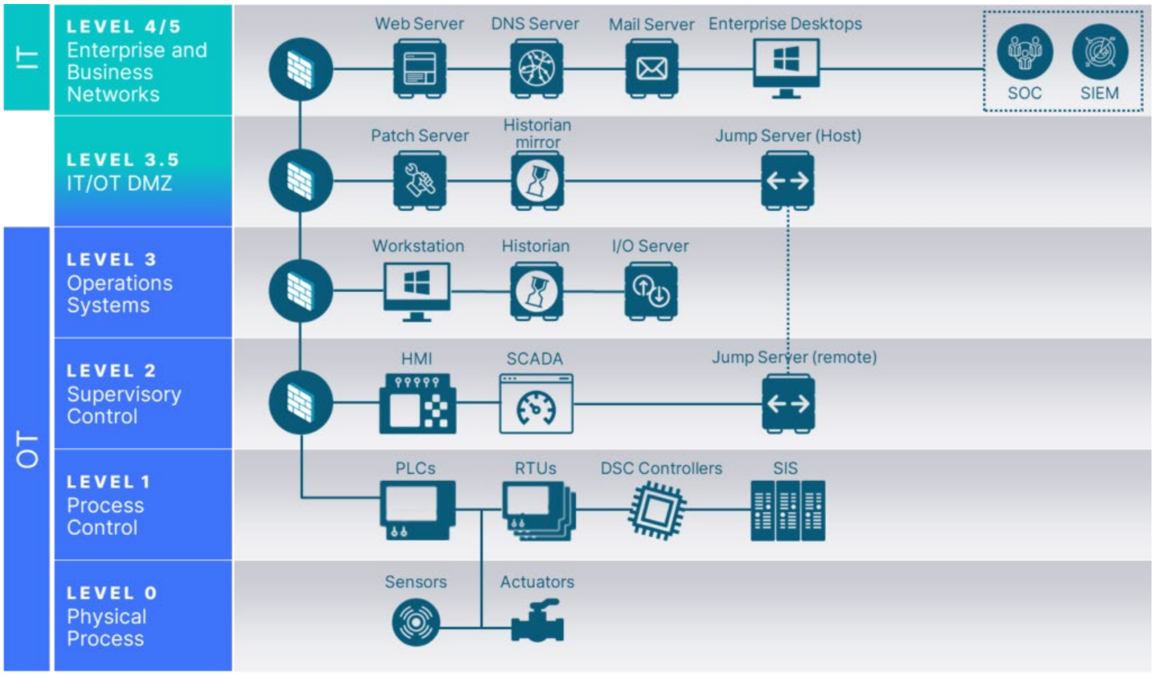


Figure 3 Purdue Reference Model

OT Vulnerabilities

The Purdue Architecture was intended to provide a model for enterprise control which end users, integrators and vendors can share in integrating applications at different layers in the enterprise. It was not intended to be a cyber security model. . However, cyber vulnerabilities exists at each layer of the Model.

Vulnerability 1 Communication

OT frequently requires information flow – primarily from sensors monitoring processes to controllers and from controllers to devices running processes. These devices operate at Purdue Levels 0 and 1 are owned by Engineering or Operations. Typically, there is little to no cyber security or authentication at this level.

The need for responsive control militates for rapid communication requiring 100% trust. This is at odds with “Zero Trust” security protocols.

Vulnerability 2 Design for Physical Changes

OT is designed to make things move, whether a train, a conveyor, or the temperature or pressure of a process. And things that move can be dangerous. This makes it a target for those wishing to cause damage or harm.

Vulnerability 3 Networked Sensors and Control Devices

Pressure, temperature, level, and other process sensors provide control, feedback, and process information. If they incorrectly read too low, the process pressure, temperature or level may be dangerously high. An example was the 2005 Texas City Refinery explosion.

Process (Level 0) sensors have historically been hardwired to Level 1 controllers. These in turn fed back to Level 2 HMIs or Distributed Control Systems (DCS) or SCADA systems and were monitored by Level 3 monitoring systems.

However, many sensors are now supplied with connectivity to communicate over Ethernet networks, although they contain no cybersecurity features, authentication, or cyber logging capabilities.

Within the Purdue Model, DCS and SCADA reside at Level 2. Yet Level 0 or 1 process sensors can now communicate directly to Level 3 or even higher This makes SCADA and DCS networks vulnerable to viruses or malicious payloads in Level 0 sensors.

In 2021, the Department of Energy (DOE)'s Oak Ridge National Laboratory, Pacific Northwest National Laboratory and National Renewable Energy Laboratory prepared a report on sensor issues in buildings. According to the DOE report:

> "…cybersecurity threats are increasing, and sensor data delivery could be hacked as a result. How hacked sensor data affects building control performance must be understood. A typical situation could include sensor data being modified by hackers and sent to the control loops, resulting in extreme control actions. To the best of the authors' knowledge, no such study has examined this challenge."

See also this author's paper "Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices" [xii]

Note that hacking process sensors is not new – it was demonstrated by Russian and other researchers at the 2015 ICS Cyber Security Conference. Moreover, published work from the US Air Force Institute of Technology (AFIT) demonstrated how process sensors from three different process sensor manufacturers could be hacked and detected.

Vulnerability 4 Existing (Legacy) systems

Systems based on Profibus and Foundation fieldbus generally are connected to gateways on the Local Area Network (LAN). With many of those systems still using unauthenticated and unencrypted communication, these insecure sensors/transmitters become exposed.

In January 2022, the Society of Automotive Engineers (SAE) held a session with MITRE to present the work of the MITRE Hardware (HW) special interest group identifying Common Weakness Enumeration (CWEs) for hardware to the SAE G32 Committee. MITRE stated that the Corporation's Common Vulnerabilities and Exposures (CVE) and (CWE) process was to identify mistakes in design or implementation. However:

1. Process sensors have no ability to use a token, a certificate, or signed firmware. An analog 4-20 milli-amp sensor has no capability to accomplish the requirement for a provable user identity.
2. The chipsets used in legacy or state-of-the-art digital sensors have no capability to accomplish the requirement for a provable user identity. Yet process sensors are not addressed by either the CVEs or CWEs.

Process Sensor Security Survey

The author performed a study on four process sensor vendors' 2023 Pressure Transmitter specification requirements using the terms "cyber", "security", authentication", encryption", "passwords", and "remote". The security terms were not used but the term "remote" was used more than 20 times in each specification sheet.

Readers may want to review the instrument data on your Level 0 OT devices as follows:

1. *Search your sensor documents for the terms: "cyber, security, passwords, authentication, encryption." See if those terms are mentioned in the documents.*
2. *Find out if those with Bluetooth or other remote connectivity are enabled by default.*

Vulnerability 5 Calibration

Process sensor maintenance (calibration) equipment, whether hand-held or using mobile apps, has access to the Internet without cybersecurity. According to one of the process sensor mobile app provider's advertisements, a key advantage of a mobile app solution over traditional handheld HART communicator is that you can use the mobile device you already own. In addition to already owning the main piece of hardware required, it is typically upgraded every couple of years for a very low cost (if not for free). In effect, users have more ways to access sensors, but not necessarily more security.

Network Security Vs. Engineering Control Systems

Table 1 below provides a detailed comparison between network security and Engineering (control systems).[xiii]

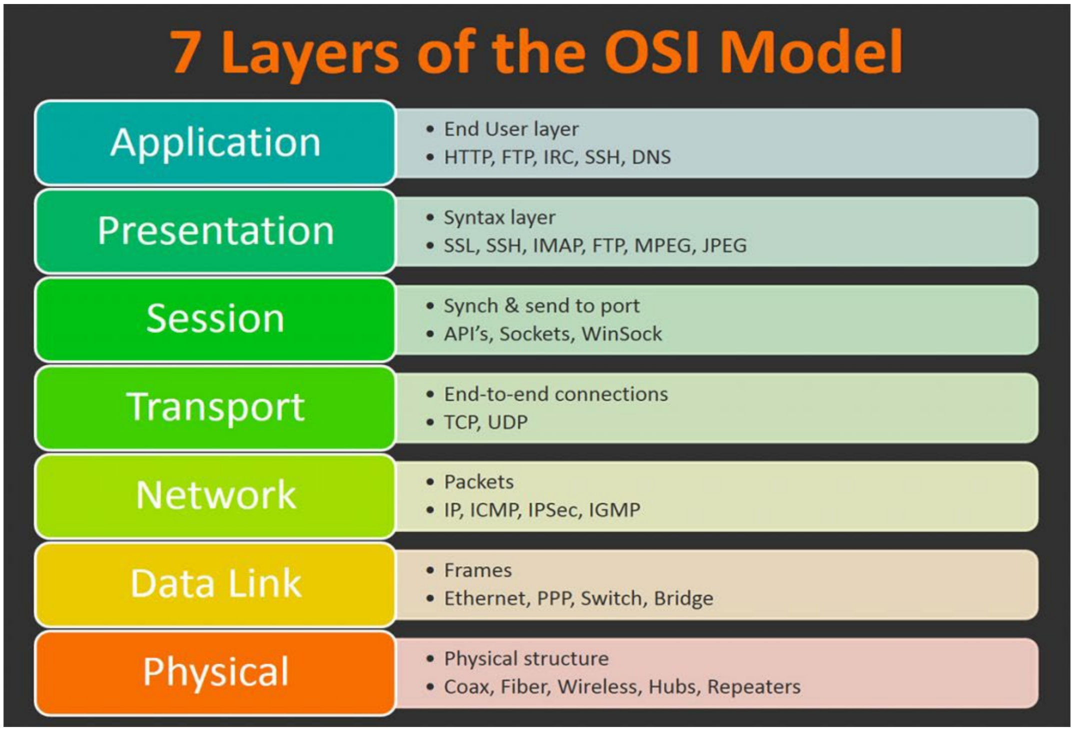
IT/OT	Engineering
Zero Trust	100% trust
Part of cyber security team	Generally not part of the security team
Worried about vulnerabilities	Worried about process and equipment
IP networks with security	Lower-level non-IP networks without security
Assume all comms go through IP networks	Can get to Level 0,1 devices without IP network
Vulnerability assessment required	Level 0,1 not applicable
Non-deterministic	Deterministic (timing is critical)
Advanced Persistent Threats (APT)	Design features with no security
Focus on malicious attacks	Focus on reliability/safety regardless of cause
Believe in airgaps	Airgaps don’t exist

Table 1: Differences between network security and Engineering

The OSI Model

Much network security is focused on the OSI (Open Systems Interconnection) model (Figure 2, below) that divides communication between computing systems into seven layers, or abstraction layers.[xiv] However, the OSI model does not address control system devices.

Effectively, IT people trained to the OSI model may not be aware of OT vulnerabilities.



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Figure 2 OSI 7-layer model

HURDLES IN PROTECTING OT

Safety And Security Are Not The Same

IT is typically focused on security. OT is primarily focused on safety. The two are not the same.

OT is often under the purview of IT because OT resides on networks. This creates unrealistic expectations for IT teams to be able to keep OT safe.

"Secure"

IT commonly uses a "CIA" security model based on three pillars: Confidentiality, Integrity, and Availability. CISA defines cybersecurity as the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. This is what we tend to think of when we think of "Security."

"Safe"

Operational Technology has a different triad: Safety, Reliability and Productivity. For OT, "Safe" is focused on not causing harm or damage to people, product, equipment, or the environment." A primary goal for OT systems is to be safe, controlling processes to prevent unsafe conditions.

OT: Secure and Safe

To be "safe", control systems must be both safe and secure. If a cyberattack can lead to a control system failure, the lack of security makes the system unsafe. This was the intent in the 2017 Triton attack on Saudi Arabia.

It is possible to be cyber-secure but not safe.
It is not possible to be safe without being cyber secure.

OT must be secure in order to be Safe.

Because cyber security involves electronic communications between systems, or systems and people (e.g., operator displays), cyber incidents can affect both the IT and OT triads.

For critical infrastructure and its associated control systems, cyber security is one of many risks that need to be addressed (along with physical, environmental, supply chain, and other threats).

OT Process Expertise

IT personnel with significant expertise in network security manage networks and their security and offer expertise. However, they will typically not have the expertise to understand OT as well (see the “IT-Cause OT Incidents,” above).

Most operational assets such as pumps, turbines, transformers, are “owned” by Operations or Engineering usually not under the purview of the CISO. Yet while they “own” the assets, they are often not responsible for cyber security which is under the purview of the CISO and may only have rudimentary network security training. This creates a gap in knowledge in the engineering and network security teams’ ability to manage OT cybersecurity.

Working in Isolation

IT staff cannot be solely in charge of OT cyber security. This is because, as shown in the two “IT-Caused OT Incidents” above, IT may inadvertently damage OT systems without support from engineering or operations. Likewise, engineers designing systems typically are focused on communications between devices, not security.

While one person must ultimately be in charge, the two teams (IT and OT) cannot work without input from each other.

Threat Vectors

When OT incidents cross from OT to IT systems, they obviously can affect both the OT and IT triads. This presents a challenge in that, while OT incidents are typically visible (because things break), cyberattacks underlying them may not be as visible, especially to the engineering side.

The difficulty of differentiating between cyber and OT incidents is more challenging because OT systems are increasingly linked using Internet Protocols, and incidents can occur due to any number of factors:

- OT component failure (heater, pump, actuator, etc.).
- PLC failure (controller).
- Improper programming.
- Communications failure.
- Operator error.
- Internal “bad actor” (hacker).
- External “bad actor” (hacker).

When an incident occurs in networked equipment, not performing a thorough root-cause analysis can lead to a false sense of security that an incident was not caused by a cyberattack or unintentional cyber issues.

To have an effective OT Cyber-Security program, you must be able to identify if OT incidents are cyber-related, and if so, whether the incident was accidental or malicious (this last may be difficult to determine).

Two events illustrate the difficulty of differentiating between cyber and control system attacks:

1. In the Stuxnet attacks, sophisticated cyber attackers made a cyberattack look like an equipment malfunction. Stuxnet was not identified as a cyberattack for more than a year.
2. At the Oldsmar, FL water treatment plant, an operator error was identified as a cyberattack. There are still OT cyber security experts calling Oldsmar a cyberattack.

Accurately identifying OT cyber events requires people who understand both OT and IT systems, working together.

Forensics

Unlike IT and OT network incidents which can be identified as being cyber-related (with cyber forensics and network security training) many control system cyber incidents are viewed as electrical or mechanical failures, simply because there are minimal cyber forensics at the process sensors and actuators for use by network security personnel.

Government and industry approaches on information sharing are focused on IP network cyber vulnerabilities, threats, and IP network cyber incidents, and much less on control system cyber incidents. Yet tens of thousands have been killed due to control system incidents, and the vast majority were not identified as “cyber-related” because they were not IP network compromises. It should also be noted that the use of IT technologies and testing can be inappropriate for use with control systems. The use of these inappropriate technologies and testing have shut down, or in some cases, damaged control systems.

Who Should be in Charge of OT Security?

Below is a summary of the traditional IT roles.

Security Roles

Security functions oftentimes are distributed across an enterprise's information resources, human capital and safety, risk, and engineering & operations departments. This can result in no one person in-charge, and no position fully responsible for overseeing the enterprise's strategic security framework.

Two well-known organizations which define security and standards are the American Society for Industrial Security (ASIS) and the National Institute of Standards and Technology (NIST). We will include their definitions for security roles below.

The ASIS International Standard refers to the "Senior Security Executive" as the senior official responsible: "To protect their assets, organizations often appoint a senior security executive (SSE) to implement a strategic security framework. This Standard provides organizational guidance on the establishment of an SSE role, addresses how to position this role within an organization and outlines responsibilities, key competencies, and critical success factors related to the SSE function."[xv]

The NIST standard works from an information technology or information resource management perspective, defining the "senior accountable official for risk management" as "the senior official…who has vision into all areas of the organization and is responsible for alignment of information security management processes with strategic, operational, and budgetary planning processes."[xvi]

Most Operational Technology is protected by IT teams Those in charge of these teams typically include:

Chief Information Security Officer (CISO)

For some enterprises, the CISO, is a senior-level executive who oversees an organization's information, cyber, and technology security. The CISO's responsibilities include developing, implementing, and enforcing security policies to protect critical data. The focus is on data.

Digital or cyber security, sometimes referred to as IT security, does have a cooperative inter-connected involvement. Some organizations have combined various elements of security programs within the CISO function. IT security typically address security-related risk issues across all layers of an organization's technology stack. This may include:

- Incident and crisis management.
- Information and privacy protection.
- Risk and compliance management.
- Security architecture.
- Organizational resiliency programs and assessment.

The CISO often reports to the Chief Information Officer (CIO)as the focus on information management and technology, not on overall risk. The organizational roles may overlap in an enterprise environment, but they differ when in an environment with operational facilities.

In many cases, CISOs have come through the ranks of IT or physical security. If via IT security, they will be familiar with network technologies including security. However, if they came up through physical security, they may not have as strong of a background in IT security concepts and technologies.

However, neither path may provide the CISO with grounding in the unique issues associated with control systems. This is because the term “OT” is more than just control system networks.

In most cases, the CSO’s staff are network security-related experts whose focus is the malicious compromise of IP networks.

Chief Security Officer (CSO)

From a physical security and risk management perspective, the head of security or CSO in some enterprises, is an organization's most senior executive accountable for the development and oversight of policies and programs intended for the mitigation and/or reduction of compliance, operational, strategic, financial and reputational security risk strategies relating to the protection of people, intellectual assets and tangible property. The focus here extends to tangible property which can include operational assets.

Below are accountabilities of the head of security, with items related to operational technology and control systems **in bold**. The include, but are not necessarily limited to:

- In cooperation with the organization’s executive leadership team(s), directs the development of an effective strategy to assess and mitigate risk (foreign and domestic), manage crises and incidents, **maintain continuity of operations**, and safeguard the organization.

- Directs staff in identifying, developing, implementing, and maintaining security processes, practices, and policies throughout the organization to **reduce risks**, respond to incidents, and limit exposure and liability in all areas of information, financial, **physica**l, personal, and reputational risk.
- Ensures the organization's compliance with the local, national, and international regulatory environments where applicable to the accountability of this role (i.e. privacy, data protection, and environmental, **health and safety**).
- Researches and deploys state-of-the-art technology solutions and innovative security management techniques to safeguard the organization's personnel and assets, including intellectual property and trade secrets**. Establishes appropriate standards and associated risk controls**.
- Through other internal policy committees, personnel and/or other external resources, coordinates and implements site security, operations, and activities to ensure protection of executives, managers, employees, customers, stakeholders, visitors, etc., as well as **all physical** and information assets, while ensuring optimal use of personnel and equipment.

Chief Risk Officer

A more recent development is the Chief Risk Officer (CRO), an executive in overall charge of an organization's risk management functions. Their responsibilities include:

Identifying, assessing, and mitigating risk, charge over risk management projects and technology, and risk management culture. In some cases, they are also over cybersecurity initiatives.

This gives them an executive role, allowing them to bring people together to address threats. If they can draw from and manage both IT and OT groups, this may give them an ideal position to combine IT and OT security and safety.

Where Are Engineering And Operations?

Those often missing from security discussions are the actual owners of the OT. Control systems are typically the responsibility of the engineers and technicians responsible for that equipment. These teams have relevant experience that Security teams lack with respect to unique aspects of control systems. While Security may be responsible for cyber security and associated workforce training, typical networking training is often different than what is required for Industrial Control / Operational Technology systems.

OT And IT Together

To maximize safety and security, IT and OT must both have input into the process. Whether we call it Cyber-Physical or Physical-Cyber, both need input into OT decisions involving networks.

Someone does need to be in charge, and it may be that the Chief Risk Officers has the overall purview and authority to ensure cooperation between IT and OT.

This is especially true with complex systems, as there have always been unintended system interactions. In fact, National Security Memo 22 states: “Critical infrastructure is diverse and complex, and includes distributed networks, varied organizational structures, operating models, interdependent systems, and governance constructs.”[xvii]

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has made security-by-design a major element to secure IT and OT networks without an apparent understanding of hardware physical-cyber system interactions. That is, all elements of a control system may be cyber secure, but that doesn’t mean the overall system is either safe or even cyber secure. Again, both sides must work together.

It should also be noted that the network security organizations’ lack of addressing safety extends beyond the United States. The Singapore Computer Emergency Response Team (CERT) aims to extend the OT cyber security workforce with the development of the Operational Technology Cybersecurity Competency Framework (OTCCF).[xviii] The OTCCF was developed jointly by CSA and Mercer with the support of SkillsFuture Singapore (SSG) and Infocomm Media Development Authority (IMDA). However, there was no mention of safety.

LESSONS LEARNED AND RECOMMENDATIONS

- There is little emphasis on the difference between IT and OT. This difference needs to be clarified and understood by IT and risk management teams.
- Teams need to plan to protect both IT and OT.
- Network security (IT and OT) security must always coordinate with engineering and operations when working with OT.
- Network security (IT and OT) and engineering / operations should bear joint responsibility and authority for cross-training, communication, and shared responsibility for security.
- Network security (IT and OT) should NOT use cyber security tools that haven't been thoroughly tested for use in OT environments.
- Engineering / Operations should not connect OT to networks to external networks without input from network security (IT and OT).
- It is not always clear what is or isn't a cyber event. It is often not clear what is a control system cyber incident.

CONCLUSIONS

Frequently, OT control system incidents may not be identified as cyber incidents or cyberattacks.

Attacks which use OT networks are in fact cyberattacks, and need to be recognized as such.

While they seem similar, control system cyber security is different than network IT and OT security.

CSO's need to work with engineering and operations to develop, implement, and maintain control system cyber programs as well as identify control system cyber incidents. Without understanding control system issues, cyber protections may not be sufficient to prevent cyberattacks that can damage hardware and cause injuries. On the other hand, inappropriate technologies or testing can, and have caused, the same impacts as hackers.

REFERENCES

[i] https://csrc.nist.gov/glossary/term/operational_technology

[ii] https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test, https://claroty.com/blog/jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test.

[iii] https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[iv] Joseph Weiss, Protection Industrial Control Systems from Electronic Threats, Momentum Press, ISBN 978-1-60650-197-9, 2010.

[v] Aurora test video can be found by searching for “Aurora Generator Test”, for example at https://www.youtube.com/watch?v=OhZb0Wl8kZc

[vi] https://www.youtube.com/watch?v=fJyWngDco3g

[vii] https://www.muckrock.com/foi/united-states-of-america-10/operation-aurora-11765/

[viii] For more details, see Power, “What You Need to Know (and Don’t) about the Aurora Vulnerability”, September 2013.

[ix] https://www.dovermicrosystems.com/case-study/german-steel-mill-cyberattack/.

[x] https://www.threatdown.com/blog/predatory-sparrow-massively-disrupts-steel-factories-while-keeping-workers-safe/

[xi] Theodore J. Williams (1993) "The Purdue enterprise reference architecture." Proceedings of the JSPE/IFIP TC5/WG5. 3 Workshop on the Design of Information Infrastructure Systems for Manufacturing. North-Holland Publishing Co.

[xii] Specific to buildings, my paper, “Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices” was published on the National Academies of Sciences website.

[xiii] Joe Weiss presentation to the Purdue Cerias Summer Series, July 15, 2020.

[xiv] https://www.bmc.com/blogs/osi-model-7-layers/

[xv] https://www.asisonline.org/publications--resources/standards--guidelines/senior-security-executive/

[xvi] https://csrc.nist.gov/glossary/term/senior_accountable_official_for_risk_management

[xvii] National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), April 30, 2024.

[xviii] linked-in 5/25/24

Challenges in Federal Facility Control System Cyber Security, Including Level 0 and 1 Devices (2023)

Division on Engineering and Physical Sciences; Federal Facilities Council; Board on Infrastructure and the Constructed Environment; Joseph Weiss

https://nap.nationalacademies.org/catalog/26511/challenges-in-federal-facility-control-system-cyber-security-including-level-0-and-1-devices.

INSTITUTE FOR HOMELAND SECURITY

Sam Houston State University

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Weiss,J. (2024)Who's in Charge of OT Security?(ReportNo.IHS/CR-2024-1033).The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/7M4DB