Module 2: Information Technology (IT), Operational Technology (OT), and Their Vulnerabilities
Introduction

• In this module, the concept of Operational Technology will be introduced.

• The cyber similarities and differences of OT to the more familiar IT will be discussed.

• Case Studies will be presented to illustrate OT vulnerabilities:
  - PIPEDREAM Attack
  - Stuxnet Virus
  - Wind Farm Vulnerabilities
The Concepts of Safety and Security

Tactics, Techniques and Procedures (TTPs) are put in place to protect assets, both people and property, from harm. Harm may be accidental (safety) or intentional (security).

Discussion: Are Physical Security and Cybersecurity Separate?
- What about removable media?
- What about physical access control?
- Are Safety and Security TTPs mutually supportive or in conflict?
Information and Operational Technology (IT/OT)

IT refers to the familiar office and home computer systems. OT refers to production processes, often with massive moving parts such as engines, generators, wind farms and ships.

**Information Technology**
- Business Processes (e.g., Cargo Manifests, Tracking, Production.....)
- Email and Web
- Human Resources

**Operational Technology**
- Navigation and Propulsion
- Cargo Loading and Unloading
- Kinetic Systems: Engines, Centrifuges, Wind Farms

**Diagram**
- Asset Protection
- Safety
- Security
- Physical
- Cyber

Information Technology

Operational Technology
Typical Information Technology (IT)

- Business Systems, Cargo Mgt., Billing, Inventory
- Networking, Web, Email
- LAN, Router
- Removable Media (A source of malware)

Financial, HR
IT Characteristics

Technology for information access and processing

- Email, web services, data access and processing, logistics, finance and business systems.
- Operates over unsecure networks
- Usually, can sustain some outage
- Frequent updates, patches, new releases
- **But compromising the IT network can provide a path to exploit the OT network**
- **Exploiting a weakness in IT to access either IT or OT is referred to as Initial Access (IA). IA may either be an end in itself, or a first step to downloading malware.**
Operational Technology (OT)

OT refers to the Industrial Production Processes and the technology that manages them

Some processes are shown here. These are Critical Infrastructure examples:

- Electric Grid: Power Generation and Distribution
- Chemical Plants and LNG Facilities
- Maritime Transportation System
Critical Infrastructure (CI)

Critical Infrastructure are vital systems and assets that, if compromised, would have a debilitating effect on security and safety of the U.S.*

- Examples include:
  - Chemical
  - Water
  - Transportation (incl. MTS)
  - Energy
  - Gov’t incl U.S. Election Systems**
  - 16 CI sectors in all

* https://www.cisa.gov/critical-infrastructure-sectors
** https://www.eac.gov/sites/default/files/eac_assets/1/6/starting_point_us_election_systems_as_Critical_Infrastructure.pdf, January 6, 2017
OT: Production Processes and the Technology that Manages Them

- In order to manage these processes, they must be equipped with **Sensors** to measure and report key **Variables**, such as output voltages, generator and motor speeds (rpm), gas pressure, temperature, locations of cranes, containers, RR cars, etc.
- These measurement values must be reported to automated or manual **Control** systems for adjustment when out of tolerance.
OT: Production Processes and the Technology that Manages Them (cont.)

• If the Controller determines that a Variable needs to be adjusted, it communicates with an **Actuator** to achieve that. The Actuator might be a control motor, an electrical switch or relay, a valve, etc.

**Controller**
(e.g., Programmable Logic Controller)

**Sensors and Actuators**
for control of Voltage, Temperature, Position, etc.

**Processes**
OT: Automating Control of Production Processes

Sensor measurements are reported to a controller, which issues commands to keep processes within set values. The Programmable Logic Controller (PLC) is the brains of this “Feedback Control Process”.

1. Measure critical process variables
2. Report values to PLC
3. PLC issues control commands
4. Process brought under control
OT: The Human Machine Interface (HMI)

*But what if the PLC can’t control the process variations?* Human observation and intervention from the HMI are critical to the operational control process. The HMI observes the sensor data remotely and determines whether the PLC settings are adequate. Special maintenance operations are also done from the HMI.
OT: The Architecture of the Control Processes

The top three layers are referred to as the Industrial Control System (ICS)/Supervisory Control and Data Acquisition or SCADA, for short. Since the processes may extend for hundreds of miles, Remote Access by the Centralized HMI is necessary. This remote access introduces a cyber attack vulnerability.

1. **Human Machine Interface (HMI)**
2. **Programmable Logic Controller (PLC)**
3. **Sensors and Actuators**
   - for observation and control of key process variables

**Processes**
SCADA Systems

- SCADA systems supervises the control of an **automated** industrial plant.
- The data may be received by the **SCADA server** from **Remote Transmission Units** or **Programmable Logic Controllers (PLC)**, which interact with sensors on equipment.
- For efficient operation, the processes are automated and centrally controlled. There may also be **Remote Operations Centers**.
- These elements are all networked and are vulnerable to a cyber attack, especially the servers and PLCs.
Interaction of IT and OT in Controlling Physical Processes

Common practices for IT security may not apply to OT, especially in applying patches (Terminology Note: Industrial Control Systems (ICS), and SCADA may be used interchangeably or as ICS/SCADA).

Some Key Security Points

- Processes include Ship Systems, Electrical Grids, etc., controlled by Industrial Control Systems (ICS) called SCADA
- Historically OT has been physically isolated (air gapped) from IT networks, and so security has not been an issue
- But now OT is automated and accessed remotely via IT networks. Hence it is vulnerable to a remote attack

  - As the process outputs are time-critical, **OT cannot sustain unplanned outages**, or **unscheduled patches**, contrary to common IT practice!
  - Unlike IT, there is danger of “kinetic” harm (big, heavy things moving and spinning out of control)
Cybersecurity of IT and OT in Process Control

In addition to an IT vs. OT dilemma, there is also a safety vs. security dilemma

• IT has many cybersecurity safeguards, e.g., virus controls, encryption, frequent patches...
• OT has not, in general, been designed with cybersecurity as a high priority
• Existing OT may not have the resource capacity to add on IT-type safeguards
• From a physical safety perspective, strong cybersecurity may not even be desirable due to increased operational delay, failure modes...

A hypothetical example...
Suppose you are sitting at the bridge of a 15,000 TEU container ship. You see an alarm on the HMI that says engine temperature is dangerously high.

You quickly hit “cut engines”. You get a response, “Please enter your username and password.”

You finally find and enter your password and then get a window that says, “Please enter the make of your first car.”

You enter all this, and get, “Please insert your encryption key”

You then hear a very loud noise from below
Since the HMI, and the facilities and vessels it may need to access, may be thousands of miles apart, communications is via the internet, and often over a satellite (SATCOM) link. The communications link terminates in the IT part of the system.
Here, the OT functions are added, including the **Data Historian (DH)**. The DH stores all the sensor data for observation and analysis by centralized and distributed HMIs. **The DH plays an important role in SCADA cybersecurity.**

**Land-Based Facilities**  
HMI (Control Center) operators observing operational data stored in the on-board Data Historian (DH) over a Sat Comms link

**Facility and Shipboard Processes**

- Navigation
- Propulsion
- Port Systems

**SCADA**

- Programmable Logic Controllers
- **Data Historian (DH)**

**Processes**

**IT Services**

**Satellite Comms Link**
Since the IT/OT functions may be remote from the HMI, they must be accessible via the internet. Hence, they are vulnerable to hacking. The hacker might use remote access via the internet (Hacker 1) or might be an insider (Hacker 2). All the red links must be secure!
Efficiencies and Vulnerabilities Introduced by IT/OT Integration

The IT and OT worlds are sufficiently different such that Tactics, Techniques and Procedures (TTPs) for one may not work in the other.

- Integration of IT and OT allows efficient, automated bridge and remote access to all systems
- Remote access allows:
  - Timely updates and access to IT systems
  - Centralized expertise to be accessible to SCADA for ships at sea, remote facilities
  - But also allows cyber criminal, alien nation/state access to OT systems
- Whereas IT is regularly patched by downloads, OT may be decades old with many vintages, legacy systems, out-of-date software and patches. Hard to patch on-the-fly.
- Systems may not have been designed with cybersecurity in mind
- Third-party vendors traditionally have been “trusted agents” with “Delegated Access Privileges”. These concepts are no longer appropriate without significant safeguards. For example, how does a Facility Security Officer know that a third-party vendor’s laptop is free of malware?
Case Study: PIPEDREAM, A New and Evolving Critical Threat to Operational Technology

Alert (AA22-103A)

APT Cyber Tools Targeting ICS/SCADA Devices

Original release date: April 13, 2022 | Last revised: April 14, 2022
Case Study: PIPEDREAM, A New and Evolving Critical Threat to Operational Technology

• On April 13, 2022, the Cybersecurity and Infrastructure Security Agency (CISA) issued an alert (Alert AA22-103A) entitled “APT Cyber Tools Targeting ICS/SCADA Devices” (APT is Advanced Persistent Threat). It is likely a State-Sponsored Threat aka INCONTROLLER.

• This threat, while modeled on PLCs manufactured by Schneider Electric Company and the Omron (Automation) Corporation, uses standardized protocols and therefore can communicate with any PLC that uses these protocols.

• While the current PIPEDREAM focusses on Schneider and Omron, these systems, protocols, and architectures are used by ICS/SCADA in all sectors.

• Hence, the threat is very broadly based!
PIPEDREAM contains many functions and is evolving in its capabilities. The objectives of PIPEDREAM are disruption, sabotage, and possible destruction of ICS/SCADA including critical infrastructure. The major categories of tools and functions are shown below:

- **TAGRUN**: A tool for scanning ICS servers to determine their structure and read or change data; performs reconnaissance for details of production processes and control systems.

- **CODECALL**: Using standard ICS/SCADA protocols to scan and attack Schneider Electric Company PLCs.

- **OMSHELL**: Uses appropriate protocols, designed to attack Omron PLCs.

The PIPEDREAM attack tools may be configured to appear as a terminal on the IT/OT network:
PIPEDREAM Attack on MTS and other Critical Infrastructure

Initial Access may be through a password attack on IT. PIPEDREAM may appear to the OT as simply another network terminal. (In this diagram, no network protection is yet shown).
CISA-Recommended Actions to Mitigate PIPEDREAM

On the first page of its April 13, 2022 Alert, CISA recommended several immediate actions, as shown in the blue box. **Mitigations** are actions taken to reduce **Risk**, either by reducing the **Likelihood** of a successful attack, or its **Consequences**. (More in Module 5)

**Actions to Take Today to Protect ICS/SCADA Devices:**
- Enforce multifactor authentication for all remote access to ICS networks and devices whenever possible.
- Change all passwords to ICS/SCADA devices and systems on a consistent schedule, especially all default passwords, to device-unique strong passwords to mitigate password brute force attacks and to give defender monitoring systems opportunities to detect common attacks.
- Leverage a properly installed continuous OT monitoring solution to log and alert on malicious indicators and behaviors.

- Multi-Factor Authentication reduces likelihood of a successful Initial Attack
- Changing passwords, especially default passwords, also reduces likelihood of IA
- Installing and using **logs** are critical to detect a successful malicious access or download
Case Study: The Stuxnet Virus - 2010

The Stuxnet virus attack was a cyber attack on the OT of a major Iranian nuclear installation. It resulted in substantial *kinetic* harm.

- Attack OT SCADA of Iran nuclear facility, specifically centrifuges for uranium enrichment
- Malware seeks and attacks control software on Siemens centrifuges (Siemens S7 software)
- Malware introduced, perhaps via USB Flash Drive
- Causes centrifuges to spin out of control and self-destruct (*kinetic harm*)
- In the meantime, the Operations Center (HMI) sees all conditions “Normal”
Stuxnet Attack: IT, OT, and Process

Information Technology
Breached to introduce malware

Operational Technology
• Human Machine Interface
• SCADA including PLC

Process
Uranium enrichment centrifuges
Stuxnet Attack Vector as an OT Attack

Threat Vector

1. OT breached, and malware inserted via infected flash drive
2. PLC commands actuators to make centrifuges to “Go Slow, Go Fast, Go Slow…”
3. PLC to HMI: “Everything Normal
4. Centrifuges Burn Out

Human Machine Interface
The Stuxnet Virus – 2010 (cont.)

- Affected 200,000 computers and 1000 machines
- No known retaliation admitted, but since Stuxnet, Iran has emerged as a major cyber threat

Epilog
- Cyber Attack Takes Down 25% Of Iranian Internet February 8, 2020
- Iran responsible for interfering with US elections Oct. 3, 2020
  - Sent emails telling registered voters “not to vote”
  - An Advanced Persistent Threat (APT)
    - [https://us-cert.cisa.gov/ncas/alerts/aa20-296b](https://us-cert.cisa.gov/ncas/alerts/aa20-296b)
Case Study: Offshore Wind Farms (OSWF)
OSWF are an emerging energy critical infrastructure with safety and security implications

- The U.S. plans to implement 30 megawatts of offshore wind power by 2030 to supply 20% of electricity needs

Considerations:
- Environmental/Ecological due to presence of hundreds of structures
- Hazards to navigation
- Radar interference
- Cybersecurity?
Cybersecurity of OSWF

OSWF architecture and vulnerability are similar to Stuxnet. A cyber attack could cause similar destruction

Stuxnet
- OT controlled process speed
- Caused self-destruct of centrifuge

OSWF
- OT controls turbine speed by adjusting pitch and yaw of blades
- Loss of control can result in system destruction
This material is based upon work supported by the U.S. Department of Homeland Security under Cooperative Agreement No. 2014-ST-061-ML0001.