Exercise 2

OT Systems & Devices

Dr Diarmuid Ó Briain

Version: 2.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

This page is intentionally blank

Exercise Scenario

1 Exploring OT at an Airport

1.1 Exercise #1: OT at the airport

Figure 1: Consider OT devices at an airport

Scenario: Consider a holiday flight you have taken, enjoyable? Yes. Now go back and consider the OT devices you interacted with, but in your excitement you probably did not notice.

Task: As an exercise, think about the airport and try to imagine where you might find OT devices that are hiding in plain sight.

For example:

- Escalators
- Moving walkways
- Baggage conveyor belt
- Automatic doors
- Security scanner

OT devices within OT are at work to keep the operation of the airport smooth.

1.2 Question #1: Where do you find OT?

Which of the following industrial locations use OT devices?

- Airport
- Dam
- Salmon farm
- Cake factory
- Power station
- Train station
- Pharmaceutical plant
- Creamery
- All of the above

2 SCADA and vulnerabilities

SCADA has brought with it improvement through the incorporation of technologies such as Local Area Network (LAN) and Human Machine Interfaces (HMI) as well as the advances since the 1980s to today, moving things into the Internet of Things (IoT) and beyond. Adding the Internet creates a Cyber concern. Present day alerting has allowed Structured Query Language (SQL) web based applications allows for full remote access and reaction to a SCADA system.

2.1 Question #2: SCADA vulnerabilities

Which of these technological changes are increasing cybersecurity vulnerability for SCADA systems?

- Flashing lights on nuclear plant control boards
- Advancements in IoT
- Ethernet & Internet connectivity
- Physical control switches

3 Distributed Control System (DCS)

Large facilities, such as a large factory, use many DCS systems because they support redundancy. When one system goes down, another system can pick up. If one line goes down, another line can pick up. Ethernet has also been introduced with a Virtual Private Network (VPN) from the vendor which allows for on the fly and real-time repairing and monitoring. Bringing Ethernet and VPNs to the system introduce new attack vectors for the industrial facility.

3.1 Question #3: SCADA versus DCS

What is the difference between a DCS and SCADA?

- There is no difference
- SCADA is designed to cover a large geographical distance
- SCADA systems are event driven
- A DCS is state driven

4 Safety Instrumented Systems (SIS)

4.1 Question #4: SIS

Why are Safety Instrumented Systems (SIS) considered "passive"?

- They are ineffective in an emergency
- They rely on a HMI to operate in an emergency
- They do not respond until they are called into action
- They do not expose the industrial environment to any threat

5 Programmable Logic Controllers (PLC)

Imagine a factory without a fire suppression system and fire management was exercised via fire extinguishers located next to generators, heaters, and other production equipment that generates heat. Consider a Data Centre (DC) with biometric controlled access. Who is going to extinguish the fire? Will they have access? Would it be safe for them to enter the DC in the event of a fire to extinguish it? There could be people, without biometric access, available who could tackle the fire but are rendered unable to due to access. There can be large variances between safety standards, the EU, the US and right across the world.

5.1 Question #5: PLC

Which of these is NOT an example of something controlled by a PLC?

- Temperature sensor
- Robot arm actuator
- Pressure valve
- Fire hose
- None of the above

6 Fieldbus

Consider an assembly line making generic antennas that required some to have PL259 connectors and others to have SMA-F connectors. At the end of the line, before PLCs, an operator would have to physically switch a lever to switch the output to either the PL259 or SMA-F process in different parts of the factory. This function is now carried out by a PLC.

Considering security in terms of OT this is the process of production inside a facility, and if it's compromised, it can create devastating effects. As an example the process of soldering on the connectors. If the PLC that controls the functions for the soldering stations is compromised in any way, not only will the antennas be destroyed, but there could be loss of life from a fire.

6.1 Question #6: FieldBus

Which of the following are considered a fieldbus?

- RS232 connections from the PLC to the sensors and actuators carrying 4 – 20 mA signals?
- A non-time-critical communications system, such as Ethernet
- A deterministic Ethernet like network such as TSN
- None of the above

7 OT Security Audit

8 Exercise 2# Audit Worksheet

Consider the devices from this topic and those identified in Exercise #1. Use the audit worksheet on the next page to identify how these systems, and related devices, play a role in the airport you passed through.

Industrial Automation & Control Systems and Devices

OT/Device	User(s)	Use	Connection	Application	Vulnerabilities

This page is intentionally blank