Edith Cowan University
School of Science

# CSI2450 – IoT and OT Security

**Assessment:** Report on IoT and OT threats
**Weighting:** 40% of the final mark of the unit
**Time Limit:** 10 minutes (any content exceeding 10 minutes will not be marked)

Before you proceed, make sure you have read the Video-based Assessment Common Guidelines.

**Assignment Overview:**

This assessment is aligned to the following learning outcome of this unit:

ULO 2: Examine threats to IoT and OT

In Assessment 2, you focused on the IoT aspects of a Port. In this assessment you will consider the Operational Technology (OT) aspects. The knowledge and skills you learnt through Modules 6 to 9 will be required for this assessment.

**Scenario:**

A port authority in your state is considering connecting one of their ports to their Enterprise Network to optimise its performance and operations. At this stage the port authority is only interested in connecting their conveyor belt system to their Enterprise Network.

This port is responsible to handle shipping of grains produced by farmers in the state to overseas customers. Conveyer belts are essential for the efficient operation of grain handling facilities in ports, as they allow for a continuous flow of grain from the storage areas to the loading areas and onto the ship. This reduces the need for manual labour, which can be time-consuming and costly, and improves the speed and accuracy of grain handling. Additionally, conveyer belts can help reduce the risk of damage to grain during transport, as they provide a gentle and consistent flow of grain without exposing it to excessive stress or impact. Figure 1 (Page 2) is an example of a conveyer belt loading and filling a ship's cargo hold with grains.

PLCs have been programmed to monitor and control various aspects of the conveyer belt system, including the speed, direction, and flow of the grain. They also monitor the sensors that detect the presence of grain on the conveyer belts and ensure that the grain is directed to the correct location, such as the ship's cargo hold. The PLCs and various OT components connected to the Operations Network can be found in the Figure 2 (Page 3).

The vendor that sold the OT equipment has also been contracted to maintain the OT infrastructure since 2010. The vendor's engineers typically use their own laptops to connect to the Operations Network using the WiFi access point in the Operations Department. Since their OT infrastructure has been very stable, the last time the OT components were patched and updated were in 2013.

During initial discussions with the vendor regarding the plans for the network merger, the vendor is confident that connecting the OT network directly to the existing Layer 3 switch will not cause any disruptions to the operations and would be the cheapest solution. Although this is a very appealing option, you have been hired to investigate how the vendor's suggestion would affect the cyber security posture of the port authority.

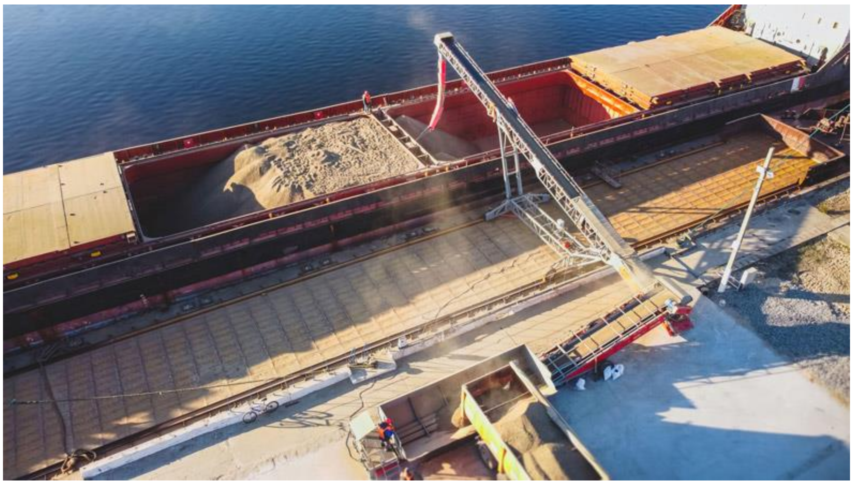

*Figure 1: An example of a conveyer belt loading grains to a ship at a Port*

**Tasks:**

At this stage of the investigation, you have only been able to gather a limited amount of information. However, the board of directors of the port authority has requested you to provide a presentation of your finding so far. The board of directors provides strategic direction and oversight of the port authority's operations. One of the key responsibilities of the board is to provide oversight of the operations, including financial performance, risk management, and compliance with regulatory requirements. The board consists of the Chief Executive Officer (CEO) and the Directors of Finance, Human Resources, Marketing, and Information Technology departments.

Since you have limited information at this stage, you may make reasonable assumptions to assist you in responding to the following tasks, provided you state them explicitly.

Your presentation should cover the following:

1. Introduce yourself and the purpose of the presentation.
2. Provide an overview of the scope of your investigation. For this task, you should provide details of the port's operations, IT and OT infrastructure that are included in your investigation. You should also list your assumptions, if any, that are relevant to fill any gaps in the information provided to respond to the rest of the tasks.
3. Identify a vulnerable device in the Operations Network that currently has a known CVE. Provide a summary of this vulnerability in your own words.
4. Perform threat modelling based on the vulnerable device that you have identified in the previous task. Put yourself in the attackers' position and create an attack tree outlining possible means to exploit the vulnerability to disrupt the ports' operations. Describe the attack tree in detail.
5. Identify two other (not including the above vulnerable device you have already identified) security concerns based on the information provided. You should also elaborate the potential consequences of these security concerns.
6. Do you agree with the vendor's suggestion? Elaborate and justify your answer. If you do not agree, suggest an alternative approach.

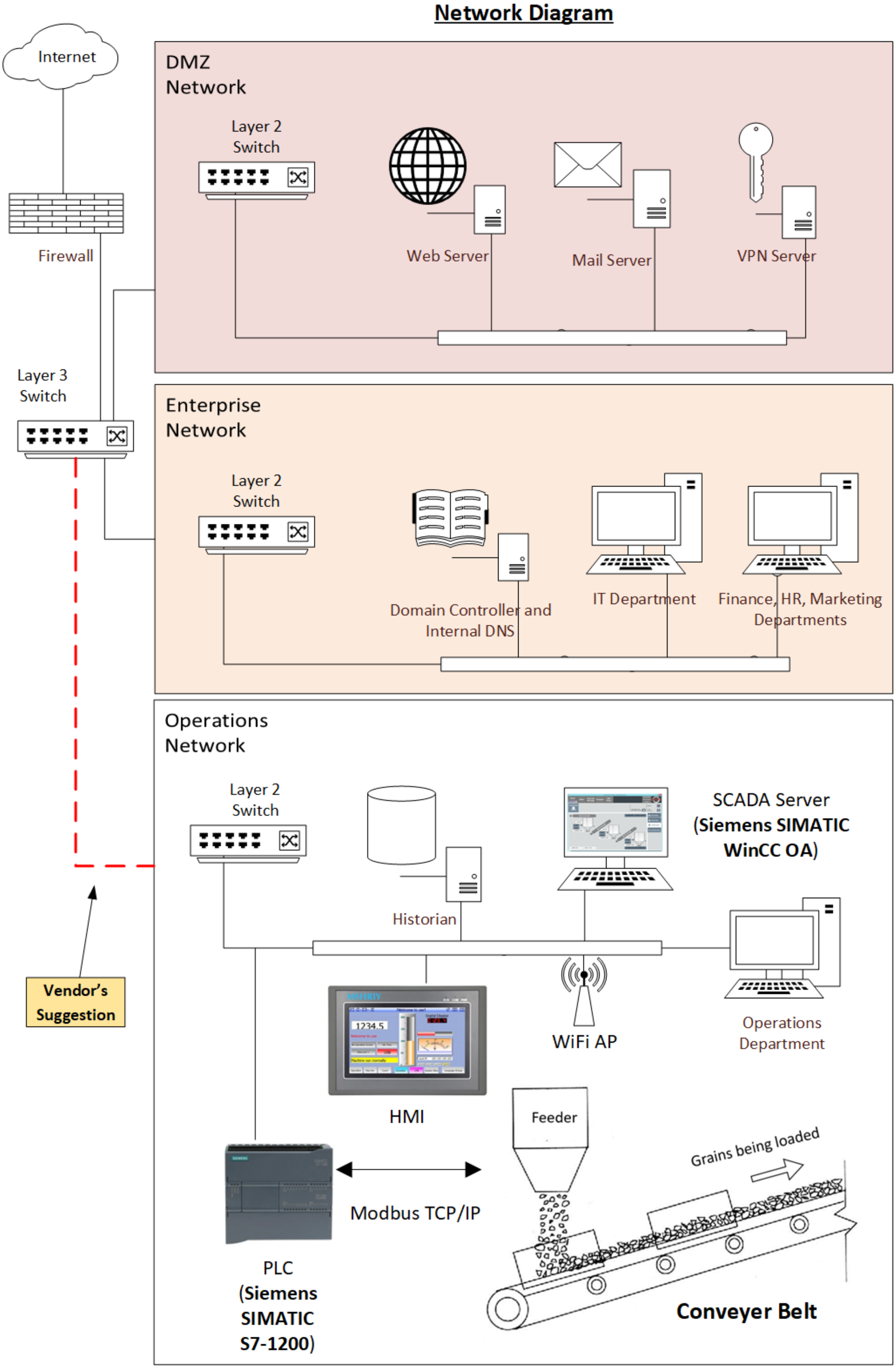

*Figure 2: Current Network Diagram*

In addition to the above tasks, you will also be marked based on:

- **Academic referencing:** follow academic integrity standards as per ECU guidelines, included both in-text and end-text referencing (APA 7), and used credible sources relevant to the subject area.
- **Presenting research:** sufficient/high level of depth and breadth of research on relevant areas required to investigate the cyber security incident and relevant recommendations.
- **Presentation quality:** sufficient/high standard of slides (graphics and text), preparation and communication of the presentation to the target audience.

**Slides and Referencing:**

- You **do not** need to submit your slides but should be used for the presentation.
- Create a PowerPoint presentation capturing the key points you are reporting. Do not fill the slides with lots of text. You are encouraged to use both graphics and text in your slides. Ensure everything on the slide is legible.
- Since the presentation has a fixed time limit, you may aim to have a maximum of 12 slides.
- Even though this is not a typical written report, your presentation should be supported by adequate research. Any information or ideas you have taken from other sources should be referenced as "in-text" in the relevant slide and a full reference should be provided as "end-text" on the last slide. A suggested approach is to use superscripts in your content slides and have a final slide with the full reference list. You must show the reference slide in the video recording and may be requested to provide the reference list separately.

**Recommended Presentation Structure:**

- Slide 1: Introduction/Title slide
- Slide 2: Outline
- Content slides addressing the rest of the tasks (include as many as required)
- Final slide: references (don't forget to include this in your video)

**Marking Criteria:**

| Criteria | Marks (40 marks) |
|---|---|
| Academic integrity, research skills and presentation quality | 4 |
| Task 1: Introduction | 2 |
| Task 2: Overview | 4 |
| Task 3: Device vulnerability | 6 |
| Task 4: Attack tree | 8 |
| Task 5: Two security concerns | 8 |
| Task 7: Vendor critique | 8 |

Refer to the marking rubric for further details.