出國報告（出國類別：進修）

112 年「提升職業訓練師專業職能駐點計畫」
(ISA/IEC 62443 工業自動化與控制系統安全認證課程)

服務機關：勞動部勞動力發展署北基宜花金馬分署、桃竹苗分署及中彰投分署
姓名職稱：林嘉琪副研究員、蔡宏松副訓練師、簡勝輝副訓練師等 3 位訓練師
派赴國家：美國
出國期間：112 年 9 月 9 日至 112 年 9 月 29 日
報告日期：112 年 12 月 13 日

摘要

我國積極推動製造業實現數位轉型，為避免製造業成為駭客主要攻擊和勒索的目標，政府以強化工業控制系統資安的防範措施，確保國內關鍵基礎設施在資訊系統方面的安全性。

美國在工業控制系統資安發展方面擁有豐富經驗，隨著技術的發展和資安威脅的演變，採取提高工業控制系統（ICS）的安全性之措施。國際自動化學會（ISA）是發布工業自動化和控制系統領域相關標準之非營利專業協會，其標準有助於企業降低資安風險。

鑒此，勞動部勞動力發展署 112 年度計畫薦派訓練師赴美接受 ISA 工業控制系統資安認證課程的培訓，學習如何在發展工業物聯網（IIOT）過程中實現工業自動化控制系統上的網路資訊安全，從而將這些知識納入職業訓練課程，並提供更專業的培訓。

ISA 網址：https://www.isa.org/

RICE 網址：https://www.rice.edu/

NASA 網址：https://www.nasa.gov/

目次

壹、基本資料

一、原屬單位(代表人)：勞動部勞動力發展署北基宜花金馬分署。

二、派訓單位：勞動部勞動力發展署。

三、級職姓名(代表人)：副研究員 林嘉琪。

四、出國時間：112 年 9 月 9 日。

五、返國時間：112 年 9 月 29 日。

六、受訓地點及單位（中英文）：德州休士頓，美國國際自動化協會（Houston in Texas, International Society of Automation）。

七、受訓班次名稱（中英文）：工業自動化與控制系統安全認證課程（ISA/IEC 62443 Certificates: IC32, IC33, IC34, IC37）。

貳、進修目的：

一、參加美國國際自動化協會工控資安研習課程：

因應行政院推動「5+2」產業創新，未來國家產業政策將朝向加速產業升級轉型發展，本部勞動力發展署各分署肩負培訓國家技術建設人力重任，各分署訓練師實有必要深入瞭解全球產業發展趨勢及關鍵職能技術，以提升專業技能及教學知能，始有助於我國勞動力培植及促進產業發展。

在製造業智慧化轉型時代，工業控制與營運科技(Operation Technology, OT)資訊安全人才為製造業要轉型非常重要及關鍵專業人才。美國為資訊技術重鎮，美國國際自動化協會(International Society of Automation, ISA)提出 ISA/IEC 62443 標準(如圖 1)，並由美國國家標準學會(ANSI)公開頒布，該標準提供了 OT 良好的工程管理指南，針對工業環境下的風險管理提出完整的 SOP，給出完整的防護與資安指標規範，並依從事 IT 和控制系統安全角色的專業人士設計開發認證課程。藉由訓練師至美國實際參加專業課程訓練，提升工業自動化及控制系統的專業技能及教學知能，以利我國勞動力培植及促進產業發展。

二、參訪美國德州美國國家航空暨太空總署(NASA) 休士頓太空中心、萊斯大學(Rice University)等績優單位，藉由實際觀摩與進行國際交流，觀察並瞭解美國產業發展及工廠實務，有助於訓練師爾後辦理職業訓練時，跳脫傳統思維，以新技術及教學模式為規劃精進方向。

參、進修內容摘要：

一、工控資安課程：

(一) 使用 ISA/IEC 62443 標準來保護控制系統：

1.控制系統的安全性介紹

2.安全意識

3.法規與標準

4.ISA/IEC 62443 系列

5.ISA/IEC 62443 模型

6.IACS(Industrial Automation and Control System)生命週期介紹

7.建立 CSMS(Cyber Security Management System)

(二) 評估新的或既存的 IACS 系統之網路安全：

1. IACS 網路安全生命週期介紹

2.風險評估之準備

3.風險元素

4.網路安全風險評估

5.文件及報告

(三) IACS 網路安全設計及實施：

1. ICS(Industrial Control System)網路安全的生命週期

2.設計概念

3.詳細設計

4.OSI 參考模型

5.網路分層

6.防火牆

7.入侵偵測系統

8.系統強化

9.存取控制

10.遠端存取

11.網路安全接收測試

12.系統整合商的角色

(四) IACS 網路安全操作與維護：

1.ICS 網路安全的生命週期之評估階段

2.ICS 網路安全的生命週期之設計階段

3.IACS 環境中的不同角色

4.安全管理及維護

5.事件回應與回復

6.故障排除

二、參訪績優單位：

(一) 美國國家航空暨太空總署(NASA) 休士頓太空中心：

1. NASA 太空中心(NASA SAPCE CENTER)

2. 電車遊覽(Tram Tour)

(1) 太空任務中心(Mission Control Center)

(2) 太空載具原型場(Space Vehicle Mockup Facility)

(3) 火箭廣場(Rocket Park)

(二) 萊斯大學(Rice University)：

1. Duncan Hall(Department of Computer Science)

(1) 拜訪計算機科學系賈乃輝助理教授(臺籍教授)

(2) 參觀學校的環境與先進的研究設備

2. Rice University Boot Camp (萊斯大學訓練營課程)

Rice University Cybersecurity Boot Camp (萊斯大學網路安全訓練營課程)

肆、進修過程說明：

一、第一週：(112 年 9 月 9 日至 9 月 16 日)

(一)日期：112 年 9 月 11 日- IC32 使用 ISA/IEC 62443 標準來保護控制系統

IC32 課程目標:

1. 描述控制系統安全的需求和重要性
2. 描述安全意識作為有效對策的需求和重要性
3. 描述 ISA/IEC 62443 系列文件的結構和內容
4. 定義如何創建有效的長期安全計劃之原則
5. 討論風險分析、工業網路和網路安全的基本概念
6. 討論構成 ISA/IEC 62443 標準基礎的基本概念（例如，縱深防禦和區域與通道）
7. 描述如何通過安全的軟體開發策略使系統本質上更加安全
8. 描述用於有效性或正確性驗證系統安全的措施

(1) 控制系統安全簡介:

- 定義控制系統網路安全
- 控制系統網路安全的趨勢
- 潛在後果
- 惡意軟體事件和趨勢
- 關於工業自動化與控制系統（IACS）安全的迷思
- IT 和 IACS 之間的區別
- 縱深防禦及網路風險的概念

階段性目標:

- 了解對控制系統安全的需求和重要性
- 討論當前控制系統安全的趨勢以及它們如何影響控制系統
- 分析 IT 和 IACS 之間的差異
- 認知到在 IACS 環境中仍然存在有關網路安全的誤解(迷思)。

(2) 安全意識

- 定義安全意識
- 安全意識的有效性
- 安全意識作為一種對策

階段性目標:

- 了解安全意識如何在工業自動化與控制系統（IACS）環境中成為降低風險的有效對策。

(3) 法規與標準

- 法規
- 標準

階段性目標:

- 解釋法規與標準的區別
- 解釋法規和標準如何影響工業自動化與控制系統（IACS）環境

(4) ISA/IEC 62443 系列

- ISA/IEC 62443 系列概述
- IC32 課程主要資料來源(624443-1-1, 624443-2-1, 624443-3-3)
- ICS vs IACS
- ISA 99 委員會和 ISA/IEC 62443 系列

階段性目標:

- 定義 ISA/IEC 62443 系列
- 總結 ISA 99 委員會如何為 ISA/IEC 62443 系列文件的創建做出貢獻

(5) ISE/IEC 62443 模型和安全級別

- ISE/IEC 62443 模型
- ISA 99 模型關系
- 參考模型級別
- 資產模型
- 參考體系結構
- 區域和導管模型
- 安全級別

階段性目標:

- 識別 ISA/IEC 62443 系列中的模型
- 解釋這些模型在 IACS 環境中如何使用
- 定義安全級別

(6) IACS 網路安全生命周期簡介

- IACS 網路安全生命周期簡介
- 評估階段
- 開發和實施
- 維護
- 持續流程
- IACS 自動化解決方案安全生命周期

階段性目標:

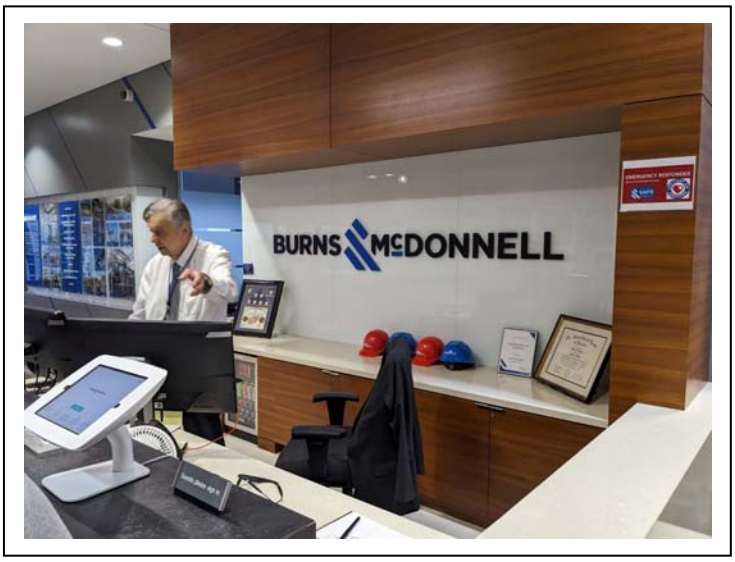
- 定義 IACS 網路安全生命周期並確定每個階段的子活動
- 識別 ISA 提供的課程，以更好地理解每個階段
- 總結來自 ISAGCA 的 IACS 自動化解決方案安全生命周期

(7) 建立工業自動化和控制系統安全計劃

- ISA/IEC 62443-2-1 CSMS 和 ISO/IEC 27001 ISMS
- 網路安全管理系統(CSMS)
- 開發 CSMS 的過程
- CSMS 的 6 個頂層活動

階段性目標:

- 討論 ISA/IEC 62443-2-1 和 ISO/IEC 27001 之間的互補性質
- 指出 ISA/IEC 62443-2-1 CSMS 中包含哪些元素
- 總結基於 ISA/IEC 62443-2-1 的 CSMS 是如何開發的



德州休士頓，美國國際自動化協會（Houston in Texas, International Society of Automation）報到處

正式上課前的 ISA 簡介及相關規則與逃生相關動線

工業自動化與控制系統安全認證課程（ISA/IEC 62443 Certificates: IC32, IC33, IC34, IC37）之上課教室

(二)日期：112 年 9 月 12 日

1. 演進的安全標準和實踐
2. 網路基礎知識 OSI 參考模型
3. 網路安全基礎知識
4. 工業協議
5. Wireshark/ PCAP（網路封包分析工具）
6. 工業自動化和控制系統（IACS）環境中的補丁管理介紹
7. 系統設計的安全風險評估介紹
8. 工業自動化和控制系統服務提供商的安全計畫要求

9. 開發安全產品和系統

(1) 不斷發展的安全標準和實踐

- 公私合作
- NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) 框架
- 監測和評估適用的法律法規
- 全球框架
- 標準開發組織(SDOs)

階段性目標:

- 確定如何實現公私合作
- 分析 NIST-CSF 框架及其與 ISA/IEC 62443 的關係
- 確定全球框架及其創建中涉及的標準開發組織 SDOs

(2) 網路基礎知識

- 網路類型
- ISO/OSI 參考模型
- 1-7 層

階段性目標:

- 識別基本的網路類型
- 識別 ISO/OSI 參考模型
- 討論 ISO/OSI 模型的七個層次以及它們之間的互動關係

(3) 網路安全基礎知識

- 為什麼我們需要關注安全
- 網路攻擊方法
- 網路安全技術
- 入侵偵測與預防
- 虛擬私人網路
- 網路分割

階段性目標:

- 解釋基本的網路安全以及為什麼需要在 IACS 環境中處理它

(4) 工業協議

- 工業協議
- Modbus
- OPC

階段性目標:

- 描述工業協議
- 討論 Modbus 和 OPC 的基礎知識

(5) IACS 環境中的補丁管理簡介

- 惡意代碼保護
- IACS 補丁管理
- 資產擁有者的要求
- 產品供應商和服務供應商的要求

階段性目標:

- 解釋 IACS 補丁管理如何構成一種強大的對抗措施，以保護 IACS 免受惡意軟體的侵害
- 確定關於 IACS 補丁管理的資產所有者、產品供應商和服務供應商的要求

(6) 系統設計的安全風險評估簡介

- 安全級別(SL)
- 基本要求(FR)
- FR 和 SL 向量
- 風險公式
- 簡單的示例
- 解決系統設計的風險問題

階段性目標:

- 描述安全級別及其與基本要求的關係
- 確定風險公式
- 討論 ISA/IEC 624443-3-2 和 ISA/IEC 624443-3-3 如何處理系統設計的風險問題

(7) IACS 服務供應商的安全計劃要求

- IACS 服務供應商的要求
- 供應商:
  - 集成
  - 維護
  - 產品

階段性目標:

- 總結 ISA/IEC 624443 如何處理服務供應商的安全要求

(8) 開發安全的產品和系統

- 產品安全開發生命周期的要求
- IACS 組件的技術安全要求
- ISA 安全合規

階段性目標:

- 討論 ISA/IEC 624443 如何處理產品安全開發生命周期的要求

和組件的技術安全要求

- 描述 ISA 安全合規

IC32 講師合照

(三)日期：112 年 9 月 13 日評估新舊 IACS 系統的網路安全

IC33 課程目標:

1. 識別並記錄評估範圍內的 IACS
2. 指定、收集或生成執行評估所需的網路安全資訊
3. 識別或發現 IACS 產品或系統設計中原有的網路安全漏洞
4. 解釋過程危害分析的結果
5. 組織和促進 IACS 的網路安全風險評估
6. 識別並評估現實的威脅情景
7. 識別並評估現有對抗措施的效果
8. 識別現有政策、程序和標準中的差距
8. 評估新對抗措施的成本、複雜性和效益，以提出有意義的建議
9. 建立並記錄安全區域和導管
10. 制定網路安全要求規範

(1) IACS 網路安全生命周期介紹

- 細談 IACS 網路安全生命周期(評估->開發和實施->維護)
- 評估階段 - 每個區域都被指派了目標安全級別(SL-T)
- 開發和實施階段 -
  - 實施對策措施以達到目標安全級別(SL-T)
  - 實現的安全級別(SL-A)取決於各種因素
- 維護階段 -

- 確保實現的安全級別(SL-A)優於或等於目標安全級別(SL-T)
- 如有必要，進行對策措施審核和/或測試，以達到並保持實現的安全級別

- 持續過程

(2) 為風險評估做準備:了解正在考慮的系統(SUC)-無論是未來還是現有的

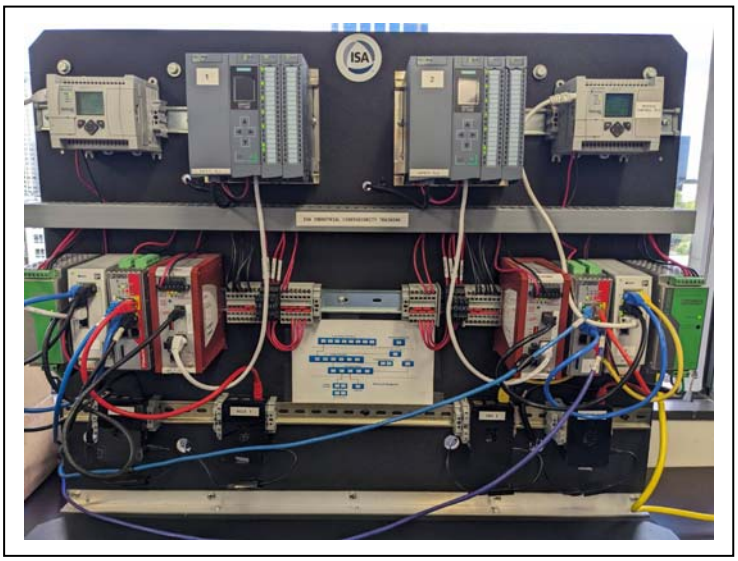
- 評估的定義
  - 在進行評估之前，必須制定一個實踐計劃
  - 識別項目的步驟以執行評估
  - 識別正在評估的系統
- 主要目標(無論是在工程階段的未來系統還是已經安裝並運行的現有系統)
  - 深入了解評估範圍內的系統，以可視化後果、評估風險，並做出減輕不可接受風險的明智決策
    - 了解當前相關的做法和程序
    - 了解正在考慮的系統
    - 了解正在控制的工業製造過程
- 關鍵組件
  - 系統架構圖
  - 網路圖
  - 資產清單
  - 關鍵性評估
  - 流程圖
  - 資料流
  - 業務流程
- ISA 95 企業功能層中的功能層級
  - Level 4-企業物流系統
  - Level 3-製造運營系統
  - Level 2-控制系統
  - Level 1-智能設備
  - Level 0-物理過程
- Exercise:
  - Exercise 1: Asset Inventory
    - 目標：使用軟體資產管理（SAM）工具來查詢環境中

的工作站以及運行在該設備上的軟體和服務的資訊。

- ◆ 電腦需求: Windows 10 Virtual Machine

■ Exercise 2: Perform a High-Level Cybersecurity Risk Assessment(高層次網路安全風險評估)

- ◆ 目標：分成一個小組，討論一個程序控制的應用程式，並對該程序執行高層次的網路安全風險評估。



IC33 模擬工控系統 / IC33 網路相關實作 / IC33 ISA62443 整體規劃

(四)日期：112 年 9 月 14 日

(1) 風險元素-工業網路安全風險計算的基本要素

- 風險方程式-威脅利用漏洞產生後果
- 威脅來源
  - 威脅源是可以表現出威脅的實體
  - 它可能是一個人或一組人，也可能是硬體或軟體等物件
  - 它甚至可能是環境事件，如火災或洪水
  - 在識別威脅源時，一些有助於識別威脅源的特徵，例如其位置、能力和動機
- 滲透測試
- 漏洞評估與滲透測試的比較
- 進行工業自動化和控制系統（IACS）高層漏洞評估
- IACS 網路安全評估工具
- CSET 的好處

(2) 網路風險評估-分析工業網路安全風險以做出明智決策

- 了解風險是確定如何最好地保護系統的首要步驟
  - 了解風險
    - 確定現實威脅
    - 辨識現有的漏洞
    - 識別關鍵資產
    - 了解被破解的後果
    - 評估當前防護措施的效力
  - 制定應對不可接受風險的計劃
    - 評估現有的對抗措施
    - 建議額外的對抗措施
    - 建議更改現行政策和程序
    - 優先考慮建議事項(基於相對風險)
    - 評估成本、複雜性與效力的平衡
- ISA62443-2-1 風險評估要求
  - 4.2.3.1 選擇風險評估方法
  - 4.2.3.2 提供風險評估背景資訊
  - 4.2.3.3 進行高層風險評估
  - 4.2.3.4 識別工業自動化和控制系統
  - 4.2.3.5 開發簡單的網路圖
  - 4.2.3.6 優先考慮系統
  - 4.2.3.7 執行詳細的漏洞評估
  - 4.2.3.8 識別詳細的風險評估方法
  - 4.2.3.9 進行詳細的風險評估
  - 4.2.3.10 確定再評估的頻率和觸發標準
  - 4.2.3.11 整合物理、HSE 和網路安全風險評估結果
  - 4.2.3.12 在工業自動化和控制系統的生命周期內進行風險評估
  - 4.2.3.13 記錄風險評估
- 來自 ISA/IEC 62443-3-2 的網路風險評估流程
  - ZCR 1 ： 辨識審查的系統
  - ZCR 2：初始風險評估
  - ZCR 3.1：建立區域和導管
  - ZCR3.2：分隔業務和工業自動化和控制系統
  - ZCR3.3：分隔與安全相關的資產
  - ZCR3.4：分隔暫時連接的設備

- ZCR3.5：分隔無線設備
- ZCR3.6：分隔通過外部網路連接的設備
- ZCR4：將初始風險與可容忍的風險進行比較
- ZCR5：執行詳細的網路安全風險評估
- ZCR5.1：識別威脅
- ZCR5.2：識別漏洞
- ZCR5.3：確定後果和影響
- ZCR5.4：確定未緩解的可能性
- ZCR5.5：確定未緩解的網路安全風險
- ZCR5.6：確定 SL-T
- ZCR5.7：比較未緩解風險和可容忍的風險
- ZCR5.8：識別和評估現有的對抗措施
- ZCR5.9：重新評估可能性和影響
- ZCR5.10：確定剩餘風險
- ZCR5.11：比較剩餘風險和可容忍的風險
- ZCR5.12：識別額外的網路安全對抗措施
- ZCR5.13：記錄和傳達結果

- Exercise:
  - Exercise 3: High Level Risk Assessment Using CSET(使用 CSET 進行高層次風險評估)
    - 目標：介紹一個高層次評估工具，以作為討論評估工作流程的起點。
    - 軟體：使用運行於主機電腦（筆記本電腦或 Shuttle）的 DHS CSET 工具。
    - 學習成效:
      - 使用 DHS CSET 工具創建架構圖：學生應該學會如何使用 DHS CSET 工具來建立工廠的工業自動控制系統（IACS）的架構圖。
      - 比較合規性：使用 ISA/ANSI 62443 標準，比較 IACS 的合規性，以確保它是否符合這些標準中的安全要求。
      - 生成報告（例如差距評估）：使用 CSET 工具生成報告，例如差距評估報告。這些報告將提供有關 IACS 中可能存在的差距和風險的重要資訊。
  - Exercise 4: Vulnerability Scanning(弱點掃描)

- ◆ 目標：旨在使用弱點掃描工具，以了解資產由於缺乏更新和強化而可能變得易受攻擊。
- ◆ 軟體：VMWare Workstation、Kali Linux 虛擬機器、Windows XP 虛擬機器和 Nessus Essentials。

■ Exercise 5: Pentest Windows XP Using Kali Linux(使用 Kali Linux 測試 Windows XP)

- ◆ 目標：在這個實驗中，將向介紹 Metasploit，以便使用弱點來滲透 XP 系統。
- ◆ 軟體：Windows XP Service Pack 2（操作系統）, Kali Linux

(五)日期：112 年 9 月 15 日

1. 文件和報告

(1) 如果未記錄步驟，將無法進行驗證、查核或證明

(2) 文件必須經過修訂、修改、審查、批准並處於一個控制計劃之下。

(3) 漏洞評估報告

(4) 網路安全風險評估報告

(5) 網路安全要求規範

■ ZCR6：網路安全要求規範

(6) SUC 描述

(7) 區域和管道特性

(8) 威脅環境

(9) Exercise:

■ Exercise 6: Creating a Zone & Conduit Diagram (創建區域和通道圖)

- ◆ 目標：瞭解如何根據 ISA/IEC 62443-3-2 的要求創建區域和通道。

■ Exercise 7: Detailed Risk Assessment

- ◆ 目標：介紹詳細風險評估的流程。

二、第二週：(112 年 9 月 17 日至 9 月 23 日)

(一)日期：112 年 9 月 18 日 – NASA 參訪

1. NASA 太空中心(NASA Johnson Space Center)

(1) Starship Gallery

- 展覽真實的太空船，包括 Apollo 17 Command Module，Mercury 9 “Faith 7"，Gemini V 等等。
- 展示太空人任務訓練空間的生活區
- 38 億年歷史的月球岩石

(2) Astronaut Gallery

- 展覽許多太空服和各種太空人服裝，
  - Sally K. Ride 飛行中的工作服
  - Kathryn Sullivan 的穿梭艙外移動裝置
  - Ed White 的艙外活動訓練服等等。

(3) Mission Mars

- 觸摸來自紅色星球(火星)的真實隕石
- 展示有關火星的所有資訊，包括它的天氣模式，太空人在探索地形時穿什麼，以及火星地面上的樣子。

(4) International Space Station Gallery

- 國際太空站以每小時 17,000 英里的速度繞地球軌道運行，這個龐大的實驗室為太空人提供寶貴的研究空間，以增進我們對宇宙的理解。
- 在展覽中，通過交互式機器人展覽和現場表演“生活在太空”，可了解國際空間站的所有資訊。

(5) 電影和現場演示

- Mission Briefing Center 設有一名官員，負責轉發當前外層空間即時更新的任務
- Destiny Theatre 連續播放電影《Human Destiny》，敘述 NASA 的歷史及其創立以來執行的計畫項目。

2. 太空任務中心(Mission Control Center)

(1) 主要任務是確保太空任務的成功運行，包括載人和無人太空飛行，如載人太空梭、國際太空站（ISS）和其他太空探測器的任務。

(2) 追蹤太空飛行器的位置、狀態和運行，並為太空人和太空飛行器提供支援和指導。

(3) 推進太空探索，瞭解宇宙，並開發新的技術和解決方案，以支持未來太空探索的需求。

3. 太空人訓練設施(Astronaut Training Facility)

(1) 專門用於培訓和訓練太空人，以確保他們具備在太空任務中執行各種任務所需的技能和知識。

訓練太空人應對太空任務中可能遇到的各種情況和挑戰。這些訓練活動涵蓋了多個方面，包括：

- 太空行走訓練：太空人需要在太空中執行太空行走（EVA）任務，例如修復太空站或執行科學實驗。Astronaut Training Facility 提供水下太空行走訓練，模擬太空行走的重力和環境，以幫助太空人熟練這項技能。
- 模擬飛行訓練：太空人需要了解和操縱太空飛行器，包括太空梭、太空艙和載人太空艙。設施提供飛行模擬器，允許太空人在地球上練習飛行。
- 科學實驗訓練：太空人將在太空中執行各種科學實驗，包括實驗室工作和地質採樣。他們在這個設施中接受科學實驗的相關培訓。
- 國際太空站模擬：太空人需要在太空站上工作，Astronaut Training Facility 提供太空站模擬訓練，幫助他們熟悉太空站的運作和生活環境。

4. 火箭廣場(The Lyndon B. Johnson Space Center Rocket Park)

(1) Rocket Park 的主要任務是通過展示歷史上的火箭和太空飛行器，展示 NASA 的太空探索歷史，以及太空人的勇氣和成就。

(2) 展示一系列具歷史意義的火箭和太空飛行器。

(3) 介紹登陸月球太空探索的人員及歷史

(4) 363 英尺(110.6 公尺)高的農神 5 號(Saturn V)火箭的主場: 又名土星 5 號，是美國國家航空暨太空總署（NASA）在阿波羅計畫和太空實驗室兩項太空計劃中使用的運載火箭，為可載人的多級可拋式液態燃料火箭。

5. 獨立號廣場 (Independence Plaza)

(1) 探索原始的 NASA 905 太空梭運輸機，在 42 年的職業生涯中進行了 200 多次穿梭

(2) NASA-905

- 展示 NASA 905 的內部配備，介紹太空梭計劃的歷史。
- 由波音 747 改造而來
- 負責將各種退役的太空梭運送至各地

(3) 獨立號

- 駕駛艙和太空人狹窄的生活區域

NASA 大門口

獨立號廣場（Independence Plaza）上方為獨立號，下方為 NASA-905

(二)日期：112 年 9 月 19 日 – 萊斯大學參訪

1. Duncan Hall

(1) 萊斯大學校園參觀

(2) Computer Science 系館參觀

(3) 拜訪計算機科學系台籍助理教授賈乃輝教授(Nai-Hui Chia)

- 簡介量子電腦
  - 是一種使用量子位元（qubit）而不是傳統二進制位元（bit）進行運算的計算機。它倚賴量子力學的原理，這些原理允許位元同時處於多種狀態，而不僅僅是 0 或 1。這種特性賦予量子電腦強大的計算能力，使其在處理某些特定問題時能夠比傳統計算機更有效率。
- 量子電腦對資安的衝擊
  - 量子電腦在破解傳統加密方法和加密系統方面的強大能力
  - 量子通信技術被視為一種解決量子計算對通信安全的挑戰的方法。
  - 量子計算未來可能用於加強國家之間的資訊戰。如同 AI 的發展，需要有後續的配套措施，故需在量子計算規範和安全性方面的有所限制。
- 探討量子力學在資安上面的應用
  - 量子密鑰分發（Quantum Key Distribution，QKD）
  - 量子加密協議
  - 量子隨機數生成

- 量子認證

2. Rice University Boot Camp

(1) 線上教育課程，其初衷為學習不間斷

(2) 各式的線上課程

- Rice University Cybersecurity Boot Camp (萊斯大學網路安全訓練營課程)
- Coding Boot Camp(web 開發)
  - HTML, CSS, jQuery, Bootstrap, Node.js, MySQL, MongoDB, Express.js, React.js
- Digital Marketing Boot Camp(數位行銷)
  - 營銷策略、活動開發、數位廣告以及現代網站分析和報告的專業知識。
- FinTech Boot Camp(金融科技)
  - Python 編程、金融庫、機器學習算法、以太坊和區塊鏈
- Data Analytics Boot Camp(數據分析與視覺化)
  - 中級 Excel、Python、JavaScript、SQL、Tableau、機器學習、Git/GitHub 等
- UX/UI Boot Camp(使用者體驗/使用者介面)
  - 以用戶為中心的設計研究(用戶需求, 用戶體驗訪談等)
  - 視覺原型和線框圖(Adobe XD, Figma, Google Slides 等)
  - 用戶界面開發(UI 網格和組成, 色彩理論, 排版等)
  - 網頁原型(HTML, CSS, jQuery, Bootstrap, JavaScript, GitHub 等)

IC33 模擬工控系統

賈乃輝教授辦公室

(三)日期：112 年 9 月 20 日 IACS（工業自動化與控制系統）網路安全的設計、實施和測試

IC34 課程目標:

1. 定義安全開發生命周期過程和交付物: 制定網路安全開發生命周期過程，並明確定義和提供相應的交付物，以確保網路安全標準得以遵循。
2. 解釋獨立的安全需求規範: 了解和解釋獨立的安全需求規範（CRS），以確保網路安全的設計和實施符合規範要求。
3. 基於 CRS 資訊開發概念設計: 利用 CRS 中的資訊，開發概念性的網路安全設計，確保網路架構滿足安全需求。
4. 執行基本的防火牆配置和啟動: 配置和啟動基本的防火牆設備，以確保網路邊界的安全性。
5. 設計安全的遠程訪問解決方案: 開發安全的遠程訪問解決方案，以允許遠程用戶安全地訪問 IACS 系統。
6. 制定系統強化設計規範: 制定系統強化設計規範，以確保系統已經實施了網路安全的最佳實踐，包括安全配置和訪問控制。
7. 實施基本的網路入侵偵測系統: 部署和配置基本的網路入侵偵測系統，以監視網路流量並識別潛在的威脅。
8. 制定網路安全驗收測試計劃: 制定網路安全驗收測試計劃，以確保系統滿足網路安全標準和規範。
9. 執行基本的 CFAT 或 CSAT: 進行基本的網路安全驗收測試，以驗證系統的安全性能和合規性。
10. 這些任務和步驟有助於確保 IACS 系統在設計、實施和測試過程中符合網路安全標準和最佳實踐，以降低網路威脅和風險。

1. IACS 網路安全生命周期

(1) 是一個網路安全生命周期模型，它包括以下四個主要階段：

- 評估（Assess）: 在這個階段，組織會評估其當前的網路安全狀態，包括現有的漏洞、威脅、風險和資產。這包括進行安全風險評估、漏洞掃描、威脅情報分析和資產管理，以了解組織的網路安全需求。
- 開發和實施（Develop and Implement）: 在這個階段，組織將根據評估的結果制定和實施網路安全策略、政策和控制措施。這包括制定安全政策、規程、安全控制、安全培訓和應急響應計劃，以提高網路安全性。
- 維護（Maintain）: 維護階段涉及持續監視和維護網路安全控制措施，以確保其有效性。這包括定期更新漏洞掃

描、監控安全事件、進行安全審計和合規性檢查，以保持網路的安全性。

- 持續過程（Continuous Process）： 安全生命周期是一個持續的過程，不斷評估、改進和適應新的威脅和技術。這個階段強調了不斷學習和改進的重要性，以適應不斷變化的網路安全環境。

- 這一生命周期模型旨在幫助組織建立並維護強大的網路安全體系，以應對不斷演變的網路威脅。通過定期評估、規劃、實施和維護網路安全措施，組織可以提高其網路的安全性並減少潛在的風險。

2. 概念設計

(1) 概念設計是網路安全中的一個重要步驟，旨在制定網路安全策略和計劃，以滿足特定的網路安全需求。以下是概念設計的一些主要元素：

- 解釋網路安全需求規範： 首先，需要詳細閱讀和理解網路安全需求規範（CRS），以確定網路安全的關鍵要求和標準。
- 定義 5 個安全級別(SL)： 根據 CRS 中的資訊，定義五個安全級別，以根據系統或網路中的重要性和敏感性對不同區域和組件進行分類。這些級別可以包括從高度敏感到非敏感的範圍。
- 定義 3 個 SL 類型定義： 根據定義的安全級別，為每個級別制定相應的安全類型定義，包括適用的安全控制、訪問控制規則和安全策略。
- 定義 4 個 Ts 來管理風險：采用 4 個 Ts 方法來管理風險，其中 4 個 Ts 代表"Threat"（威脅）、"Transfer"（轉移）、"Treat"（處理）和"Terminate"（終結）。這些方法有助於確定風險並採取適當的措施來管理它們。
- 解釋 5 個 Ds 來處理風險：使用 5 個 Ds 方法來處理風險，其中 5 個 Ds 代表"Detect"（檢測）、"Deter"（威懾）、"Delay"（延遲）、"Deny"（拒絕）和"Defeat"（擊敗）。這些方法有助於確定如何處理風險，包括通過檢測威脅、威懾攻擊、延遲攻擊、拒絕攻擊或擊敗攻擊的發生。
- 為每個區域和通道制定安全策略： 根據定義的安全級別和類型定義，為每個區域和通道開發網路安全策略，包括安全控制、訪問控制、監控、審查和事件回應計劃。

- 概念設計的目標是確保系統或網路的整體安全性，並根據不同的需求和風險來制定適當的安全策略。

3. 詳細設計

(1) 詳細設計是系統或軟體開發生命周期模型中的一個關鍵階段，它建立在概念設計之後，旨在更詳細地規劃系統或軟體的實現。以下是有關詳細設計的一些關鍵方面：

- 系統/軟體開發生命周期模型： 系統/軟體開發生命周期模型是一種用於規劃和管理系統或軟體開發過程的框架。常見的模型包括瀑布模型、敏捷開發、疊代和增量模型等。這些模型指導開發人員在不同階段執行各種任務，包括需求分析、概念設計、詳細設計、編碼、測試和維護。
- ISA/IEC 62443-3-3 的七個基本要求： ISA/IEC 62443-3-3 是工業自動化與控制系統（IACS）網路安全的標準。七個基本要求包括：
  - 資產管理
  - 訪問控制
  - 認證和身份驗證
  - 安全通信
  - 安全配置管理
  - 安全事件管理
  - 安全升級和維護
- 組件分類和 ISA/IEC 62443-4-2： ISA/IEC 62443-4-2 是關於 IACS 組件的安全標準。它定義了不同的組件分類，包括控制器、網路設備、人機界面、工程站、外部設備和通信組件等。這些分類有助於組織根據其重要性和風險來選擇適當的安全措施。
- 設計規範的六個部分： 詳細設計規範通常包括以下六個部分：
  - 系統或軟體的總體架構
  - 資料結構和資料庫設計
  - 界面設計
  - 安全性和訪問控制設計
  - 算法和業務邏輯設計
  - 測試策略和計劃
- 這些部分有助於指導開發人員更詳細地規劃系統或軟體

的實現，包括安全性、性能、用戶界面和數據管理等方面。

- 詳細設計階段在系統/軟體開發生命周期中定義了系統或軟體的具體實現細節，為後續的編碼和測試提供了指導。

(2) OPC

4. TCP/IP 網路和 OSI 參考模型

- TCP/IP 網路和 OSI 參考模型是計算機網路領域的兩個重要概念，它們為網路通信提供了基礎和標準。
- ISO OSI/Reference Model（ISO OSI/參考模型）: OSI 是"Open Systems Interconnection"的縮寫，是一個國際標準化組織（ISO）定義的網路通信模型。它將網路通信分解為七個不同的層級，每個層級負責特定的功能，包括物理層、數據鏈路層、網路層、傳輸層、會話層、表示層和應用層。這個模型有助於不同廠商的設備和協議能夠互操作，因為它提供了一個通用的參考框架。
- TCP/IP Networking（TCP/IP 網路）: TCP/IP 是"Transmission Control Protocol/Internet Protocol"的縮寫，是互聯網上最常用的協定套件。它實際上是基於 OSI 模型的，但將其分為四個主要層級：網路接取層（與 OSI 的物理層和資料連結層相當）、網路層、傳輸層和應用層。TCP/IP 協定套件包括 TCP、UDP、IP 等協議，用於實現互聯網通信。
- Switches and VLANs（交換機和虛擬區域網路）: 交換機是網路設備，用於在區域網路（LAN）上交換封包。它們工作在資料連結層，通常用於內部網路中的設備連接。虛擬區域網路（VLANs）是一種將網路設備分組的方法，使其看起來像它們在不同的物理網路上。這有助於改善網路性能和安全性。
- Routers and IP Routing（路由器和 IP 路由）: 路由器是網路設備，用於在不同網路之間轉發封包。它們工作在網路層，負責在不同的子網和網路之間進行封包路由。IP 路由是確定封包如何在網路中傳遞的過程。
- TCP and UDP Port Numbers（TCP 和 UDP 埠號）: TCP 和 UDP 是兩種常用的傳輸層協議，它們使用埠號來標識不同的應用程序或服務。埠號用於將封包正確介接到目標應用程序。
- Gateways（閘道器）: 閘道器是連接兩個不同網路的設備，通常用於在不同網路協定或架構之間進行數據轉換。它們能夠將數據從一個網路傳輸到另一個網路，充當封包的入口或出口。閘道器可以用於連接不同類型的網路，例如將區域網路連接到網際網路。

5. 網路分割

- 網路分割（Network Segmentation）是一種網路設計策略，旨在將一個大型網路劃分為多個更小的子網或段，以提高網路安全、性能和管理。在工業自動化和控制系統（IACS）的網路安全領域，網路分割通常是一項關鍵的措施。
- 一些與網路分割相關的要求和概念來自於以下標準：
  - ISA/IEC 62443-2-1 要求：這是與 IACS 網路安全相關的國際標準，其中包括了對網路分割的要求和指南。這個標準強調了需要根據系統的重要性和風險，劃分不同的網路區域，並採取相應的安全措施來保護這些區域。這包括控制數據流、訪問控制和監控。
  - ISA/IEC 62443-3-2 要求：這是與 IACS 網路安全相關的另一個國際標準，它提供了有關網路安全的詳細要求和指南。在標準中，對網路分割的要求涉及到定義網路區域和通道、訪問控制、安全隔離和審計。
  - Demilitarized Zones (DMZ) and Architectures（非軍事區域和架構）： DMZ 是一種網路架構，通常用於將互聯網與內部網路分隔開。這個概念與網路分割相關，因為它涉及到將不同的網路區域劃分為內部、DMZ 和外部。內部網路通常包括受信任的系統，DMZ 用於托管公共服務，而外部網路與互聯網相連。這種架構有助於隔離不同安全級別的網路，同時提供必要的服務。

6. 防火牆（Firewalls）

- 防火牆（Firewalls） 是網路安全中的關鍵組件，用於監視和控制網路流量，以確保只有授權的封包能夠通過。
- 兩種類型的防火牆：
  - 軟體防火牆： 這種防火牆通常是在操作系統或應用程序級別運行的軟體，用於過濾和控制封包的流動。它們通常用於保護單個計算機或服務器。
  - 硬體防火牆： 這種防火牆是獨立設備，通常部署在網路邊界或數據中心中，用於監控和篩選流經網路的所有封包。硬體防火牆通常能夠處理更大的數據流量，並提供更強大的安全功能。
- 三類防火牆：
  - Packet Filtering Firewalls（封包過濾防火牆）： 這些防火牆基於封包的來源、目標、介面和協定等資訊，簡單

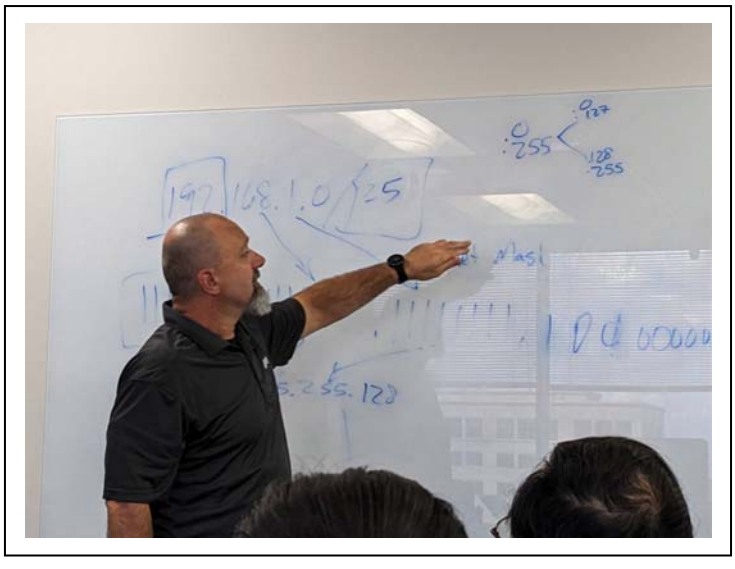
地決定是否允許封包通過。它們通常用於基本的網路訪問控制。

- Stateful Inspection Firewalls（有狀態檢查防火牆）：這些防火牆在分組過濾基礎上增加了狀態資訊的追蹤，允許它們檢查封包的狀態和連接。這使它們能夠更深入地理解網路流量，提供更精確的安全控制。
- Proxy Firewalls（代理防火牆）： 代理防火牆充當客戶端和服務器之間的中間人，它們接收、檢查和轉發請求。代理防火牆可以對傳輸的數據進行深入檢查和修改，提供高級的安全性和隱私保護。

- 深度封包檢查（Deep Packet Inspection，DPI）： DPI 是一種網路流量分析技術，能夠更深入地檢查封包的內容，包括應用層資料。它可以識別特定的應用程序、協議和內容，以幫助防火牆更精確地監視和控制流經網路的數據。
- 防火牆規劃和實施的關鍵步驟：
  - 需求分析： 確定網路的安全需求，包括保護的資產、威脅模型和安全策略。
  - 選擇合適的防火牆類型： 基於需求和預算，選擇軟體防火牆或硬體防火牆。
  - 設計網路拓撲： 定義防火牆的位置和配置，以確定如何集中或分散部署防火牆。
  - 規則和策略定義： 制定規則和策略，以確定哪些封包被允許通過，哪些被拒絕。
  - 實施和配置： 安裝和配置防火牆設備，包括規則的設置和性能優化。
  - 監視和維護： 定期監視防火牆活動，進行日誌分析和定期更新規則，以適應新的威脅。
- 防火牆配置的最佳實踐：
  - 最小權限原則：只允許必要的流量通過防火牆。
  - 規則審查：定期審查和更新防火牆規則，刪除不再需要的規則。
  - 日誌和監視：啟用日誌記錄和監視，以跟蹤網路活動並檢測異常情況。
  - 更新和維護：定期更新防火牆軟體和簽名資料庫，以確保對最新威脅的保護。

- 備份和災難恢復：定期備份防火牆配置，並建立災難恢復計劃。

- 防火牆是網路安全的基礎組成部分之一，它有助於防範網路威脅和保護關鍵資產。通過合理的規劃、配置和維護，防火牆可以成為網路安全的有效防線。
- 在網路安全實踐中，重要的是不斷更新和適應新的威脅和安全挑戰，以確保防火牆繼續發揮有效作用。此外，保持對最佳實踐的遵循是確保防火牆安全性的關鍵，因為網路攻擊者不斷演化，網路防禦也必須不斷進步。
- Exercise:
  - Exercise 1: Network and Packet Analysis(網路和封包分析)
    - 目標：使用多個軟體套裝工具可以識別您的資產並檢查您的網路。在本實驗環境中使用兩個開源程序來進行網路和封包分析。
    - 軟體和設備：使用 Paint Factory 的培訓板。該練習將使用 IC333437 虛擬機器和 Nmap 以及 Wireshark 應用程序進行。在操作前應先確認 Paint Factory 的 HMI 軟體應該在運行。



IC34 課堂討論

(四)日期：112 年 9 月 21 日

1. 入侵偵測系統

(1) 入侵偵測系統是一種用於檢測嘗試入侵或濫用計算機系統的的工具。

(2) 類似於物理安全入侵的安全警衛和視頻監控

(3) 它允許系統管理員在次要安全問題升級為關鍵的安全事件之前進行響應。

(4) 有兩種主要類型：

- 網路入侵偵測系統(NID)
- 主機入侵偵測系統(HID)

(5) 有兩種檢測方法：

- 預定義規則（基於特徵碼的）
- 異常檢測（行為模型）

(6) 網路入侵偵測系統(NIDS)

- 監視網路流量以尋找可疑活動
- 通常放置在網路的邊界和其他戰略位置,以檢測入站和出站流量。

(7) IDS 傳感器和數據收集器都連接到管理控制台。這些網路不應產生任何顯著的額外網路流量，也不應干擾運營。或者可以使用一種帶外型連接(數據傳輸通道獨立於正常的網路傳輸,被管理設備即使在關機狀態甚至故障的狀態下,都可以進行修復重開機或是日誌監控等管理作業)。

(8) 常見的網路入侵偵測系統包括 Snort、OSSIM、McAfee 網路安全平台、Industrial Defender 和 Suricata。

(9) 主機入侵偵測系統(HIDS)

- 一種監視和分析單個主機的內部和網路接口的入侵偵測系統
- 通常需要在本地主機上安裝代理程序
- HIDS 代理程序監視系統完整性、應用程序活動、文件更改、主機網路流量和系統日誌
- 如果檢測到未經授權的更改或活動,它將通過彈出窗口通知用戶並向中央管理服務器發出警報
- 一些常見的主機入侵偵測系統(HIDS)的功能包括日誌分析、事件關聯、完整性檢查、策略執行、路由工具檢測和警報。
- 常見的主機入侵偵測系統包括 OSSEC、Samhain、Tripwire、AIDE、Prelude Hybrid IDS、IBM Proventia

Desktop、Cisco CSA、Checkpoint Integrity、Symantec Endpoint Protection、McAfee Host Intrusion Prevention、HIDS、Carbon Black 和 FireEye HX 系列。

- 入侵偵測系統（IDS）最佳實踐
  - 分布式部署 - 在區域入口點安裝 NIDS
  - 使用工業自動化控制系統（IACS）IDS 特徵碼來增強 IT IDS 特徵碼
  - 實施入侵防止系統時應極度謹慎，以避免無意中阻止必要的流量

(10) 工控系統（ICS）架構的安全要求

- 太常見的情況是，安全對策被實施時安全性不足。例如：
  - 使用沒有或預設管理帳號的 IP 監控攝影頭
  - 具有 Telnet 管理功能的防火牆
  - 具有弱訪問控制和未強化的安全相關服務器（例如：網域控制器、門禁讀卡器、網路管理、遠程訪問、應用程序白名單）
- 對於安全對策，需要記錄安全要求。

2. 系統強化

(1) 系統強化是通過減少受攻擊面來保護系統的過程。

(2) 減少攻擊的可能途徑，通常包括以下措施：

- 移除不必要的軟體
- 移除不必要的用戶帳戶
- 禁用或移除不必要的服務
- 強化訪問控制（例如，多因素身份驗證）
- 安裝安全補丁

(3) 通過這些措施，系統的強化可以減少潛在的攻擊面，提高系統的安全性。

(4) 任何組件均可以進行強化，以增強其安全性，包括但不限於：

- 操作系統：操作系統的安全性可以通過配置、更新、禁用不必要的服務和應用程序，以及實施訪問控制來進行強化。
- 資料庫：資料庫安全性可以通過訪問控制、加密、審計和應用程序安全來進行強化。
- 應用程序：應用程序的安全性可以通過代碼審查、漏洞修復、訪問控制和輸入驗證來進行強化。

- 管理交換機：網路交換機可以通過配置安全策略、訪問控制列表和端口安全來進行強化。
- 路由器和防火牆：路由器和防火牆的安全性可以通過配置防火牆規則、更新韌體、實施虛擬專用網路（VPN）和訪問控制來進行強化。
- 通信閘道器：通信閘道器的安全性可以通過身份驗證、訪問控制、加密和審查來進行強化。
- 數據機（Modems）：數據機的安全性可以通過訪問控制和加密來進行強化，以防止未經授權的訪問。
- PLCs（可編程邏輯控制器）、RTUs（遠程終端單元）：工控系統的設備可以通過限制物理訪問、更新韌體、實施網路隔離和訪問控制來進行強化。
- IEDs（智能電子設備）：IEDs 的安全性可以通過配置、韌體更新和訪問控制來進行強化，以保護關鍵基礎設施。
- VFDs（變頻驅動器）：變頻驅動器的安全性可以通過配置、限制訪問和更新韌體來進行強化，以確保工業控制系統的穩定運行。
- 在每種情況下，強化的目標是降低潛在攻擊面，提高系統的安全性，以防範潛在的威脅和風險。

(5) Exercise:

- Exercise 2: Firewalls and DMZ(防火牆和 DMZ)
  - 目標： 學習配置 mGuard 和 Tofino 防火牆以限制數據流量。所有通過 mGuard 的通信必須過濾。對 Siemens S7-1500 的通信必須設置為唯讀。
  - 軟體：IC333437 Vertual machine, VTScada HMI, Tofino Configurator, HTTPS Web Interface
- Exercise 3: Network Device Hardening(網路設備強化)
  - 目標： 保護網路設備，僅允許特定機器登入，禁用未使用的介面，並在 FL2000 交換機上配置安全服務。
  - 軟體：網頁瀏覽器
- Exercise 4: Assigning Policies with Active Directory(使用 Active Directory 分配策略)
  - 目標：將設置一個具有自己帳戶的 Active Directory。設置完成後，必須更改 Applocker 虛擬機器以將 PC 添加到他們的網域。完成後，將使用群

組策略來控制用戶權限。

- 軟體：AppLocker-VM-Active Directory 快照, Active Directory-Controller VM-Windows Server 2016
- 參考資料：
  - ISA/IEC-62443-3-3 FR 1
  - 5.1 識別和驗證所有使用者（人類、軟體流程和設備），然後才允許它們訪問控制系統。

■ Exercise 4 Part 2: Assigning Policies with Active Directory(使用 Active Directory 分配策略)

- 目標： 在設置 Active Directory 後，需要為操作員帳戶分配策略。將使用基於帳戶的策略來禁用對命令提示字元的訪問。
- 軟體：AppLocker-VM, Active Directory-Controller VM
- 參考資料：
  - ISA/IEC-62443-3-3 FR 2
  - 6.1 執行已分配給已驗證使用者（人、軟體流程或設備）的特權，以執行所請求的 IACS 上的動作，並監控這些特權的使用。

IC33 模擬工控系統實作

(五)日期：112 年 9 月 22 日

1．網路安全驗收測試

- 定義:
  - 網路安全驗收測試：這是一種測試過程，用於確認一個系統、應用程序或設備在網路安全方面是否符合預期的標準和要求。
  - 網路安全工廠驗收測試：這是在設備、系統或應用程序生產過程中進行的驗收測試，旨在確保它們在工廠出廠之前已經經過網路安全測試，以滿足相關標準和要求。
  - 網路安全現場驗收測試：這是在設備、系統或應用程序在實際現場部署之前進行的驗收測試，以驗證它們在特定環境下的網路安全性能。
  - 測試工具：網路安全驗收測試通常需要使用各種測試工具，包括漏洞掃描工具、入侵偵測系統、封包分析器等，以評估系統的安全性能。
  - 測試最佳實踐：在進行網路安全驗收測試時，應遵循一些最佳實踐，包括詳細的測試計劃、清晰的測試目標、合適的測試工具和方法、記錄測試結果、修復發現的安全漏洞以及定期重覆測試，以確保系統在整個生命周期中保持安全性。
- 在交付和啟動之前，系統的網路安全應該由運營公司進行測試和驗收。
- 網路安全工廠驗收測試(CFAT)
  - 在工廠驗收測試（FAT）現場（例如供應商或系統集成商）執行。
  - 在系統的功能測試完成後執行。
- 網路安全現場驗收測試(CSAT)
  - 在系統將要運行的地點進行現場驗收測試。
  - 在運行測試完成後執行。
  - 但在將系統交付給運營之前。
- 注意：對於經過驗證的項目和類似的應用（例如核能、制藥等）具有嚴格的變更管理控制措施，建議將網路安全驗收測試納入功能測試的一部分，包括在工廠驗收測試（FAT）和現場驗收測試（SAT）中進行。這有助於確保系統在整個生命周期中保持網路安全性。
- 網路安全驗收測試的兩個主要目標
  - 驗證是否具備網路安全規範：這個目標旨在核實系統、應用程序或設備是否滿足網路安全規範和標準。這包括確保

系統已按照規範要求進行配置，採取了必要的安全措施，並符合行業標準，以滿足網路安全的基本要求。

- ◆ 驗證安全設置是否正確配置：確保操作系統、應用程序/資料庫、網路設備、工業自動化控制系統（IACS）設備和防病毒軟體等的安全設置已正確配置。
- ◆ 驗證安全組件的安裝和配置：確認安全組件（例如防火牆）已正確安裝和配置。
- ◆ 檢測系統是否正常運行並能夠識別和報告事件：驗證入侵偵測系統和其他檢測系統是否正常運行，並能夠識別和報告潛在的安全事件。
- ◆ 驗證額外的控制措施（本地和遠程）是否正確建立：確保所有額外的訪問控制和安全措施（包括本地和遠程訪問控制）都已正確建立並按照規範進行配置。
- ◆ 這些驗證步驟有助於確保系統在網路安全方面符合規範和要求，並已正確配置和運行，以提供最佳的網路安全保護。

■ 網路安全健壯性測試：這個目標旨在測試系統的網路安全強壯性，以確保其能夠抵禦各種潛在的網路攻擊和威脅。這種測試包括模擬各種攻擊場景，例如漏洞掃描、惡意代碼攻擊、拒絕服務攻擊(DoS)等，以評估系統的反應和恢復能力。這有助於確保系統在遭受網路威脅時能夠維持正常運行並保持數據的完整性和保密性。

- ◆ 抗擊網路攻擊（例如，惡劣氣象條件或模糊測試）。
- ◆ 入侵測試，以驗證防火牆配置是否有效。
- ◆ 搜索已知漏洞，以確保系統沒有受到已公開的安全漏洞的威脅。
- ◆ 網路安全健壯性測試有助於評估系統的能力，抵禦各種潛在的網路威脅和攻擊，從而增加系統的網路安全性。這些測試幫助識別和糾正系統中可能存在的漏洞，以確保其在受到威脅時能夠有效應對並維護正常運行。

2．整合服務提供商的角色

- ● 整合服務提供商的角色在網路安全中扮演著關鍵的作用。以下是關於整合服務提供商在網路安全中的角色、基本要求和成熟級別的一些資訊：

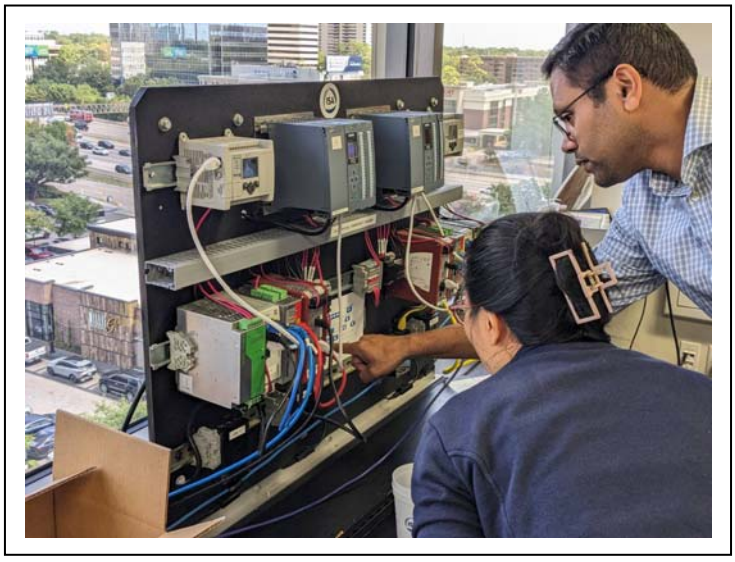
- 角色：
  - 系統集成： 整合服務提供商負責將不同的網路安全解決方案整合到客戶的環境中，確保這些解決方案協同工作以提供綜合的網路安全保護。
  - 咨詢和設計： 他們為客戶提供網路安全戰略、規劃和設計方案，以滿足客戶的安全需求。
  - 部署和維護： 整合服務提供商負責將安全解決方案部署到客戶的系統中，並確保它們的有效運行。他們還提供維護和升級服務，以確保系統的長期可用性和安全性。
  - 培訓和支持： 他們提供培訓和支持，以確保客戶的員工了解如何使用和管理網路安全解決方案。
- 網路安全中的角色：在網路安全中，整合服務~~提~~供應商需要擔任以下角色：
  - 系統集成者： 負責將各種安全解決方案整合到客戶環境中，確保其協同工作。
  - 網路安全顧問： 提供策略性建議，幫助客戶制定網路安全策略和計劃。
  - 安全分析師： 分析客戶的網路和系統，識別潛在的威脅和漏洞，並提出解決方案。
  - 安全工程師： 負責設計、部署和維護網路安全解決方案。
- 基本要求：
  - 了解網路安全領域的最新趨勢和威脅。
  - 熟悉不同的網路安全解決方案和技術。
  - 具有相關認證和資質，例如 CISSP、CEH、CCNA 等。
  - 能夠與客戶建立良好的合作關系和溝通能力。
  - 為客戶提供高質量的服務和支持。
- 成熟級別：整合服務提供商的成熟級別可以根據其在網路安全領域的經驗、專業知識和客戶滿意度來評估。一些成熟級別包括：
  - 初級水平： 提供基本的集成和支持服務，但缺乏深入的網路安全知識。
  - 中級水平： 具備一定的網路安全專業知識，能夠提供更高級的解決方案。
  - 高級水平： 擁有豐富的網路安全經驗和專業知識，能夠為客戶提供高度定制化的解決方案，保護其免受複雜的網路威脅。
- Exercise:
  - Exercise 5: Remote Access(遠程訪問)

- 目標：將在防火牆配置中應用正確的設置，以建立對遠程站點的安全連接。
- 設備/軟體：Windows 10 虛擬機, Phoenix Contact 防火牆/路由器, Chrome 瀏覽器

■ Exercise 6: Radius Server(Radius 伺服器)
- 目標：將設置 Radius 以登入到 mGuard。他們將以一種方式配置 mGuard，以便可以從一個中央管理系統中添加和刪除用戶，該系統將用於驗證 mGuard。
- 軟體：學生虛擬機, ISA-L3-Server（在背景運行），網頁瀏覽器
- 參考資料：ISA/IEC-62443-3-3 FR 1

■ Exercise 7: Define Policies and Procedures(定義 USB 政策和程序)
- 目標：了解政策和程序之間的區別，以及在組織中擁有政策和程序的好處。介紹如何編寫政策和程序。

■ Exercise 8: Using Part 62443-3-3 to validate SL-A(使用 Part 62443-3-3 來驗證 SL-A)
- 目標：使用 Part 3-3 來理解安全要求（SR）與需求增強（RE）之間的關係，以及它們與 SL-T、SL-C 和 SL-A 之間的關係。
- 軟體：Security Requirements Mappings.xlsx



來自西門子工程師的同學解說

三、第三週：(112 年 9 月 24 日至 9 月 29 日)

(一)日期：112 年 9 月 25 日工業自動化與控制系統（IACS）網路安全的操作和維護

IC37 課程目標:

1. 執行基本的網路診斷和故障排除
2. 解釋 IACS 設備診斷告警和事件日誌的結果
3. 實施 IACS 備份和恢復程序
4. 定義 IACS 補丁管理生命周期
5. 實施 IACS 補丁管理程序
6. 實施防病毒管理程序
7. 描述應用程序控制和允許列表工具的基礎知識
8. 描述網路和主機入侵偵測的基礎知識
9. 描述安全事件和事件監測工具的基礎知識
10. 實施事故響應計劃
11. 實施 IACS 變更程序管理

(1) 細談 IACS（工業安全操作與維護）安全生命周期

- 評估階段是 ISES（工業安全操作與維護）安全生命周期的首要步驟，其學習目標是了解以下內容：
  - ISES 安全生命周期及其最重要的步驟： 評估階段是 ISES 安全生命周期的第一步，目的是全面了解工業自動化與控制系統（IACS）的當前狀態和安全風險。了解 ISES 安全生命周期的整體框架，以及各個階段的目標和活動。
  - ISA/IEC 62443 風險評估過程： ISA/IEC 62443 是與 IACS 網路安全相關的國際標準，它提供了關於如何進行風險評估的指南。在評估階段，了解 ISA/IEC 62443 標準中規定的風險評估流程，包括資產識別、威脅和漏洞分析，以及風險分級。
  - 風險評估結果的文件化： 在評估階段，了解如何記錄和文件化風險評估的結果，包括已識別的威脅、漏洞、資產價值、風險級別等資訊。文件化是為了在後續步驟中制定適當的安全策略和控制措施提供基礎。
- 開發和實施階段是 ISES（工業安全操作與維護）安全生命周期的關鍵步驟，其學習目標包括：
  - 四種降低風險的方式（4 Ts）： 在“評估”階段已經識別了風險，學習如何在開發和實施階段採取措施來降低這些風險。了解四種降低風險的方法，即"避免"（Avoid）、"轉移"(Transfer)、"減輕"(Mitigate)和"接受"(Accept)。

- 回顧“評估”階段中識別的四種降低風險的方式(4 TS):進一步加深對在“評估”階段確定的四種降低風險的方法的理解。這包括重新審視如何避免風險、轉移風險、減輕風險和接受風險。
- 五種風險處理方式（5 Ds）的理解： 了解如何處理已識別的風險，包括"避免"（Avoid）、"減輕"（Mitigate）、"轉移"（Transfer）、"接受"（Accept）和"分享"（Share）。了解每種處理方式的含義和應用場景。
- 審視一些重要的技術控制來降低風險水平： 學習一些技術控制措施，這些措施可以在實施階段用於減輕風險。這些措施可能包括訪問控制、加密、入侵偵測系統、漏洞修復等技術安全控制。

- 在工業自動化與控制系統（IACS）環境中，不同的角色扮演著關鍵的作用，以確保系統的安全性和可靠性。學習目標包括：
  - 不同角色是什麼: 了解在 IACS 環境中扮演關鍵角色的人員，如系統管理員、網路管理員、安全管理員、工程師、監控員等。每個角色都有特定的職責和任務。
  - ISA/IEC 62443 IACS 網路安全生命周期是什麼： 了解 ISA/IEC 62443 標準，特別是其關於 IACS 網路安全的生命周期。這一生命周期包括評估、開發與實施、維護和持續過程等不同階段。
  - 產品和自動化解決方案安全生命周期的差異： 學習產品（如工業控制設備）的安全生命周期與自動化解決方案（如整個工業自動化系統）的安全生命周期之間的區別。理解在不同情況下，安全策略和措施可能有所不同。
  - 每個角色的職責包括什麼： 深入了解不同角色在 IACS 環境中的職責和任務。例如，系統管理員可能負責系統配置和日常維護，而安全管理員可能負責監測和強化安全性。
  - 如何根據公司的角色最佳使用 ISA/IEC 62443 標準： 了解不同公司、組織和角色如何根據其特定需求和職責最佳地使用 ISA/IEC 62443 標準來加強 IACS 網路安全。這可能包括標準的實施和符合性要求。
  - 通過深入了解不同角色、標準和最佳實踐，可以更好地理解在 IACS 環境中如何協同工作，以確保系統的安全性和可用性。這有助於建立更強大的工業自動化與控制系統，並保護其免受潛在的網路威脅。
- 安全管理和維護是工業自動化與控制系統（IACS）網路安全生

命周期的重要組成部分。學習目標包括：

- 回顧 IACS 網路安全生命周期中維護階段的目標：了解維護階段的主要目標，即確保系統的長期安全性和可靠性。在此階段，關注的是持續的安全性維護和改進。
- 回顧一些促進維護階段的重要控制措施： 了解在維護階段使用的一些重要控制措施，如安全更新、日誌分析、入侵偵測、漏洞管理等。這些措施有助於維護系統的安全性。
- 定義在維護階段必須執行的活動： 確定在維護階段需要執行的具體活動，如安全補丁管理、風險評估的定期審查、日誌和事件監控、網路入侵偵測系統的維護等。
- 解釋數字安全和物理安全之間的平衡：了解數字安全（網路和系統安全）與物理安全（設備和設施的物理安全）之間的關系，以及如何在兩者之間取得平衡，以全面保護 IACS。
- 維護階段是確保 IACS 網路安全持續有效的關鍵時期。在此階段，系統需要定期更新、監測和維護，以適應不斷變化的威脅和風險。學習這些目標和控制措施將有助於確保系統在長期內保持高水平的安全性和可用性。

(2) IACS 資產清單

- IACS 資產清單是工業自動化與控制系統（IACS）網路安全的關鍵組成部分。其要點包括：
  - 設施應至少維護 IACS 和 SCADA 硬體（物理和虛擬）和軟體的資料庫： 這意味著工業設施應當記錄和管理所有涉及 IACS 和 SCADA 的硬體和軟體，無論是物理設備還是虛擬實體。
  - 通過文件和現場調查編制： 資產清單的構建需要依靠詳細的文件記錄和實地調查。這包括檢查硬體設備、操作系統、應用程序、網路設備和其他與 IACS 相關的組件。
  - 可以使用自動化工具來收集這些數據： 為了更高效地維護資產清單，可以使用專門的自動化工具來自動收集硬體和軟體資訊。這些工具可以掃描網路和系統，自動檢測和記錄相關資訊。
  - 自動化工具應小心測試以確保不影響系統可用性和完整性，也不引入安全漏洞： 在部署自動化工具之前，應當對其進行嚴格的測試和評估，以確保它們不會對 IACS 系統的可用性、完整性和安全性產生負面影響。這包括檢查工具是否會導致系統中斷、數據損壞或安全漏洞。
- 通過維護詳細的資產清單，工業設施可以更好地了解其 IACS 和 SCADA 系統的組成部分，有助於有效的風險管理、安全策略

的制定以及系統的維護和升級。這也有助於提高對潛在風險的可見性，以便更好地應對潛在的威脅和漏洞。

(3) 細談系統強化

- 系統強化是通過減少系統的攻擊面來提高系統安全性的過程。這通常包括以下措施：
  - 移除不必要的軟體： 卸載或停用不需要的軟體和服務。減少系統上運行的軟體數量有助於降低潛在的漏洞和攻擊面。
  - 禁用過時的加密算法，如 TLS 1.0： 加密算法和協議的安全性會隨著時間的推移而降低，因此應禁用不安全的加密算法，並使用更安全的替代方案。
  - 移除不必要的用戶帳戶： 禁用或刪除不再需要的用戶帳戶。過多的用戶帳戶可能增加系統的脆弱性。
  - 強化訪問控制： 強化系統的訪問控制，例如使用多因素身份驗證（MFA）。這有助於確保只有授權用戶能夠訪問系統。
  - 禁用或刪除不必要的服務： 停用或刪除系統中不需要的服務和功能。不必要的服務可能存在安全漏洞，應當予以禁用。
  - 安裝安全補丁： 及時安裝操作系統和應用程序的安全補丁和更新，以修復已知漏洞和強化系統的安全性。
- OPC

(4) 訪問控制

- 涉及制定政策、程序和技術控制措施，以管理系統資源的使用。其目標是確保只有授權的用戶、程序、進程或其他系統可以訪問系統。訪問控制包括以下方面：
  - 建立和激活帳戶： 創建用戶帳戶並激活它們以允許授權的用戶訪問系統。這包括分配用戶名和密碼或其他身份驗證方式。
  - 修改帳戶： 對現有帳戶進行更改，例如增加或降低權限，更改密碼或更新用戶資訊。
  - 審查帳戶： 定期審查帳戶以確保它們仍然需要，以及權限設置是否合適。這有助於減少潛在的風險。
  - 禁用和移除帳戶： 禁用或刪除不再需要的帳戶。這確保了失去授權的用戶無法訪問系統資源。
- 訪問控制還包括實施與執行問題有關的措施，如：
  - 職責分離（Separation of Duties）： 確保敏感操作需要

多個人的授權，以減少濫用風險。

- 最小權限（Least Privilege）： 用戶和進程應僅分配執行其工作所需的最低權限級別，以減少潛在威脅。
- 成功登入嘗試（Successful Logon Attempts）： 記錄成功的登入嘗試，以監視系統的使用情況。
- 系統使用通知（System Use Notification）： 向用戶發出通知，提醒他們系統的使用規則和責任。
- 先前登入通知（Previous Logon Notification）： 通知用戶上次登入時間和位置，以幫助檢測潛在的惡意活動。
- 並發會話控制（Concurrent Session Control）： 確保用戶不能同時擁有多個活動會話，從而減少濫用風險。
- 會話鎖定（Session Lock）： 在用戶離開工作站時自動鎖定會話，以防止未經授權的訪問。
- 會話終止（Session Termination）： 自動終止不活動的會話，以確保未經授權的訪問。

- Exercise:
  - Exercise 1: Build the Board(搭建實驗板)
    - 目標：將有線連接和配置實驗環境，以更好地了解實驗設置。
    - 軟體：IC333437 虛擬機, HTTPS Web 界面

課程規劃設計師解說

(二)日期：112 年 9 月 26 日安全監控與檢測

1.安全監控與檢測是工業自動化與控制系統（IACS）網路安全的重要組成部分。其目標不僅包括預防安全事件，還包括及時檢測異常活動，以便

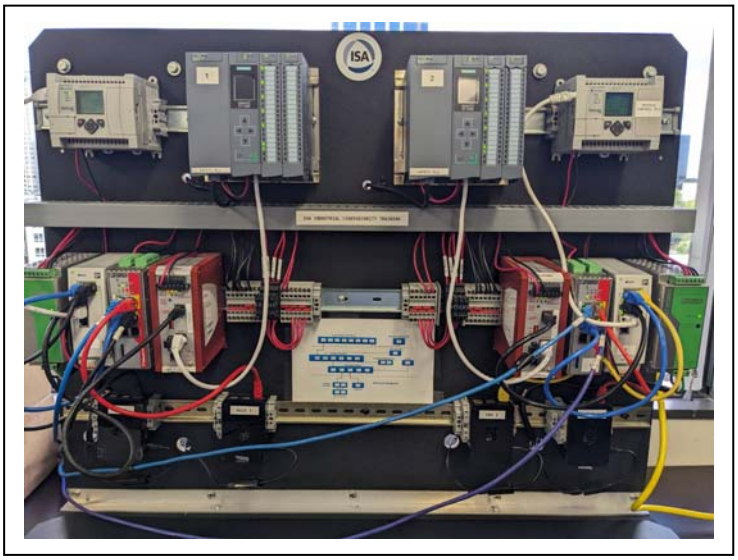
快速採取措施。學習目標包括：

- 檢測異常活動： 了解如何監視系統以檢測可能的異常活動，這些活動可能表明系統受到攻擊或存在問題。異常活動的檢測是安全事件的早期警告系統。
- 網路入侵偵測（Network Intrusion Detection）： 學習如何使用網路入侵偵系統（NIDS）來監視網路流量，以便識別潛在的攻擊和入侵嘗試。NIDS 可以檢測與已知攻擊模式不符的流量。
- 主機入侵偵測（Host Intrusion Detection）： 了解主機入侵偵系統（HIDS）的原理，它用於監視單個計算機或主機以檢測異常行為，如文件變更或未經授權的訪問。
- 監視日誌（Monitoring Logs）： 學習如何監視系統和應用程序生成的日誌，以識別異常事件或異常行為。日誌監視有助於了解系統的活動並及時採取行動。
- 定期測試和審核（Periodic Testing/Auditing）： 理解定期進行安全測試和審核的重要性，以確保系統的安全性。這包括漏洞掃描、滲透測試和安全審計。
- Exercise:
  - Exercise 2: Allowlisting
    - 目標：介紹應用程式的允許清單管理，以及如何使用 Windows Applocker 和群組策略編輯器阻止應用程式。
    - 軟體：gpedit.msc (Applocker), Applocker 虛擬機, 命令提示符
  - Exercise 3: Patch Management(補丁管理)
    - 目標： 此實驗將介紹 Microsoft Windows 軟體更新服務的功能。
    - 所需電腦：學生筆記本電腦
    - 所需設備：教室網路
    - VM/主機：Windows 10 Education 或 Enterprise
    - 所需軟體：WSUS Agent
  - Exercise 4: Snort Intrusion Detection System(Snort 入侵偵測系統)
    - 目標：創建關於 ICMP 流量、Modbus 流量和任何黑名單 IP 地址的警報。將 Snort 發出的警報發送到遠程主機上的 Syslog 程序。
    - 所需設備：
      - 配有 Snort IDS 映像的樹莓派和電源供應。
      - 短型 Cat 5 乙太網電纜。

- 運行 Kiwi Syslog Server 或類似的 Syslog 伺服器程序以及 Putty 終端模擬器的獨立筆記型電腦或計算機。
- 可選設備可能包括連接到樹莓派的 HDMI 顯示器、鍵盤和滑鼠。

■ Exercise 5: Monitoring(監控)

- 目標：學習生成 Syslog 消息並將它們記錄到一個單一伺服器（服務）。
- 軟體:網頁瀏覽器, IC333437 虛擬機器, Kiwi Syslog 伺服器



IC33 模擬工控系統/ IC33 模擬工控系統

(三)日期：112 年 9 月 27 日事件響應與恢復

1. 事件響應與恢復是工業自動化與控制系統（IACS）網路安全的重要組成部分。事先準備對於在發生安全事件時可有效地作出適當反應。

學習目標包括：

- 越來越多的法規要求關鍵服務運營商報告事件： 了解在許多司法管轄區中，法規要求關鍵基礎設施和服務提供商報告網路安全事件。有助於提高網路安全的透明度和合規性。
- Mitre ATT&CK 框架對防禦者的作用： 了解 Mitre ATT&CK 框架如何幫助網路防禦者理解和應對威脅行為，從而改進安全策略和增強網路防禦。
- 事件響應生命周期： 學習事件響應生命周期的不同階段，包括事件的檢測、通報、評估、緩解、恢復和改進。了解在每個階段應採取的措施。

- 網路安全事件響應計劃： 理解制定網路安全事件響應計劃的重要性，以確保組織在發生安全事件時有明確的應對策略和流程。
- 事件預防： 學習如何採取措施來預防網路安全事件，包括強化系統安全性、培訓員工、監控威脅情報等。
- 事件管理： 了解如何有效管理事件，包括對事件進行分類、分級、通報、追蹤和記錄。
- 事件後分析和取證： 學習如何進行事件後的分析和取證，以確定事件的原因、影響和後續行動。
- 通過充分了解事件響應和恢復的原則和最佳實踐，組織能夠更好地準備、應對和從網路安全事件中恢復。這有助於減少潛在損害，並改進網路安全策略，以提高系統的可用性和安全性。

2. 報告責任 - 歐洲 NIS 指令
   - 隨著時間的推移，向監管機構報告網路安全事件變得日益成為義務，特別是對於那些運營關鍵基礎設施和服務的組織。
   - 一個例子是歐洲的 NIS 指令（Network and Information Systems Directive），該指令旨在加強歐盟範圍內的網路安全。以下是相關內容：
     - NIS 指令： NIS 指令是歐洲聯盟於 2016 年頒布的法規，涉及網路和資訊系統的安全。
     - 其主要目標是提高整個歐盟的網路安全水平。
     - 各成員國的實施：每個歐盟成員國都在 2018 年以國家法規的形式采用了 NIS 指令，並建立了國家監管機構，負責指定和監督關鍵基礎設施和服務的運營商。
   - 關鍵基礎設施和服務的運營商（OESs）： NIS 指令確定了關鍵基礎設施和服務的運營商，這些運營商包括能源、水資源、交通、醫療等領域的實體。這些運營商有責任確保網路安全，並在發生對其提供的關鍵服務連續性產生顯著影響的網路安全事件時向相關監管機構報告。
   - 類似的要求： 類似的報告責任要求也適用於歐盟以外的地區。全球範圍內，越來越多的地區要求運營商向監管機構報告網路安全事件。
   - 為了履行這些報告責任，組織需要建立詳細的網路安全事件響應流程，並確保其記錄和流程是清晰、透明的。這有助於確保網路安全事件得到適當的處理，減少潛在的影響，同時遵守法規要求。

3. MITRE ATT&CK 框架

- MITRE ATT&CK 框架，是由 MITRE（麻省理工學院林肯實驗室的非營利組織）於 2013 年啟動，旨在記錄高級持續性威脅（APT）在 Windows 企業網路中使用的常見戰術、技術和程序（TTPs）。該框架的目標是解決以下問題：
  - 對手行為： 不僅關注典型的指示標示，如域名、IP 地址或文件雜湊值，還關注對手的行為。
  - 適用於真實環境： 要確保該框架適用於真實的網路和網路防禦環境，而不僅僅是理論概念。
  - TTPs 的可比性： TTPs 需要使用相同的術語，以便能夠比較不同類型的對手組織之間的行為。
- MITRE ATT&CK 框架是一個基於實際觀察的對手行為知識庫，包括實際攻擊中觀察到的攻擊者行為。它是免費的、開放的、全球可訪問的，由社區驅動的資源。該框架旨在幫助網路安全專業人員更好地了解對手行為，從而提高網路安全的水平，採取更有效的防禦措施。

4. 事後分析和取證（Post Incident Analysis and Forensics）
- 取證過程的目標是通過查找和分析與感興趣的事件相關的事實，以更好地理解該事件。事後分析和取證通常涉及到追查和分析計算機系統、網路或數據的活動，以確定事件的原因、威脅行為和影響。這有助於收集證據，幫助組織採取適當的行動，包括改進安全性和法律訴訟。
- 通常，進行事後分析和取證需要遵循以下四個階段的過程：
  - 準備： 在這個階段，確定需要進行取證分析的事件或情況，制定調查計劃，確保數據採集工具和資源的準備就緒。
  - 數據採集： 這是收集與事件相關的數據和資訊的階段。數據可以來自各種來源，包括計算機系統、網路日誌、資料庫、存儲設備等。數據採集需要確保數據的完整性和保密性。
  - 分析和解釋： 在這個階段，對收集到的數據進行分析和解釋，以確定事件的發生原因、威脅行為和可能的影響。分析通常包括數據挖掘、恢復刪除的資訊、重建事件時間線等。
  - 報告和記錄： 最後，生成詳細的報告，其中包括對事件的描述、分析結果、所發現的證據、可能的推斷和建議措施。這些報告可能用於法律訴訟、安全改進和未來的預防措施。
- 通過詳細的調查和分析，組織可以更好地理解事件的性質，並採取措施以減少未來事件的發生，並提高網路安全水平。
- Exercise:

- Exercise 6A: Troubleshooting(故障排除)
  - 目標:這個實驗將通過要求學生診斷故意引入的問題來測試學生在課堂上所學概念和技巧的知識。
  - 軟體：全部
- Exercise 7: Incident Recovery(事故恢復)
  - 目標：Modbus 是一種序列通訊協議，由施耐德電氣於 1979 年發明，現在也廣泛用於工業應用的 TCP 通信。它並未考慮安全性，以明文傳輸數據並且不提供身份驗證。在這個實驗中，將使用 Metasploit Framework 中包含的 Modbus 客戶端來導致西門子安全系統出現誤報。
  - 準備：使用 IC333437 虛擬機器, Kali Linux 虛擬機器, VT Scada HMI 軟體。
- Exercise 8: SIEM(安全資訊和事件管理)
  - 目標:提供對 SIEM（Security Information and Event Management）的介紹，並配置 SIEM 以檢測遠程登入嘗試，執行文件完整性監控，監控入侵偵測系統和防火牆日誌。
  - 軟體:學生虛擬機器（IC333437）, Snort IDS, MGuard - firewall web-interface, SecurityOperationCenter-VM。
  - 參考資料：ISA/IEC-62443-3-3 FR 1（識別和身份驗證控制），FR2（使用控制），FR3（系統完整性），FR6（對事件的及時響應）。

伍、受訓心得：

一、學習心得：

(一)工控資安課程：

工業控制自動化技術是一項高度綜合性的技術，它結合了控制理論、儀器儀錶、計算機科學以及其他資訊科技，旨在實現對工業生產過程的監測、控制、最佳化、排程、管理和決策。其主要目標是提高產量、提高質量、降低消耗以及確保生產過程的安全。

自 20 世紀 90 年代以來，隨著工業計算機（工業 PC）的蓬勃發展，基於 PC 的自動化系統迅速普及，由工業 PC、I/O 裝置、監控裝置和控制網路組成的系統已成為實現低成本工業自動化的關鍵途徑。

工業控制系統（工控系統）掌控著眾多關鍵基礎設施，包括發電廠、水力發電站、能源供應系統、交通控制系統和通信網路等。然而，工業控制系統的不足可能導致工業生產中斷、設備損壞以及數據洩露等問題，這將對經濟造成嚴重損失。因此，工業控制系統安全性（ICS 安全）對政府機構和製造業者都至關重要且迫切需要。

工業控制系統網路安全已成為現代工業和基礎設施運營中的一個關鍵問題，它對於維護生產運營的穩定性、環境保護、資產保全、供應鏈穩定性、數據和隱私保護、生命安全風險的避免以及法規合規性具有重要意義。

目前，工業控制系統網路（OT）與資訊技術系統網路（IT）共同管理，然而，IT（Information Technology）和 OT（Operational Technology）是兩個在用途、功能和特點上存在重要差異的技術領域。

1、 用途：IT 主要關注數據處理、資訊管理、計算機軟硬體和網路通信等領域，通常應用於企業的日常管理、通信、數據分析和應用軟體等。OT 主要應用於實體工業控制系統，包括工業自動化、生產過程控制、監控、儀器儀表、機械設備等，用於控制和監視物理設施和工業製造過程。
2、 數據性質：IT 處理的數據通常是企業的事務數據，例如客戶資訊、財務數據、市場銷售數據等，這些數據通常是非即時的，用於企業的日常管理和決策。OT 處理的數據通常是即時的，用於控制和監視物理過程，例如即時溫度、壓力、流量等數據。
3、 技術特點：IT 技術更多關注數據的處理和存儲，使用通用的計算機硬體和軟體，通常注重數據的機密性和完整性。OT 技術專注於實體控制系統，使用特定的硬體和軟體，注重即時性、可靠性和穩定性，以確保

工業製造過程的運行安全和效率。

4、 安全需求：IT 系統通常需要保護數據的機密性、防止未經授權的訪問、防止數據洩露和網路攻擊。OT 系統的安全需求更強調可用性和完整性，因為工業製造過程的中斷可能導致重大事故或損失，因此保護控制系統免受攻擊和故障是勢在必行。

ISA/IEC 62443 是一套國際標準，旨在提供工業自動化和控制系統（IACS）的網路和資訊安全指南。這些標準是由國際電工委員會（IEC）和國際安全自動化聯盟（ISA）共同開發和維護，並具有以下主要特點和組成部分：

1. **結構與分類**：ISA/IEC 62443 標準是一系列文件，每個文件處理工業控制系統安全的不同方面。它們根據主題和內容進行分類，包括網路安全、系統安全、組織和政策、產品安全等。
2. **風險評估和管理**：ISA/IEC 62443 強調風險評估和管理的重要性。組織應該評估其控制系統面臨的威脅，並採取適當的措施來降低風險，以確保其正常運營和安全性。
3. **網路安全**：這一系列標準強調保護工業控制系統中的網路和通信設施的必要性，包括設備、協定和網路架構。
4. **系統安全**：ISA/IEC 62443 提供了關於如何設計、實施和維護安全的工業控制系統的指南。這包括控制系統的體系結構、安全功能和漏洞管理。
5. **組織和政策**：此系列標準強調組織層面的安全管理和政策制定，包括安全文化、培訓、風險管理和安全績效指標。
6. **產品安全**：ISA/IEC 62443 標準還包括有關工業控制系統產品（如 PLC、SCADA 系統等）安全性的指南，包括設計、開發和測試方面的建議。
7. **認證和合規性**：標準提供了關於如何進行安全認證以及確保系統符合標準要求的資訊。

ISA/IEC 62443 標準的目標是幫助組織確保其工業控制系統不受惡意攻擊和網路威脅的影響，以確保生產運營的穩定性和安全性。這對於關鍵基礎設施和工業自動化行業尤其重要，因為這些領域的安全漏洞可能對社會和經濟造成重大影響。為了應對不斷變化的威脅和技術環境，實施 ISA/IEC 62443 標準需要不斷演進和改進。

將 ISA/IEC 62443 標準實施在自動化工業控制系統中需要一個系統性的過程，包括以下步驟和指南，以實現這一目標：

1. **了解標準**：在開始實施之前，深入了解 ISA/IEC 62443 標準。該標準包括一系列文件，每個文件都涵蓋了工業控制系統安全的不同方面。確保對這些文件需有基本的理解。
2. **進行風險評估**：通過進行風險評估，確定工業控制系統面臨的潛在威脅

和弱點。評估可能的資安風險，包括未經授權的訪問、惡意軟體攻擊和物理訪問等。

3. **確定資安需求**：根據風險評估的結果，確定資安需求。這可能包括訪問控制、身份驗證、事件監測、物理安全等資安措施。
4. **設計安全措施**：基於資安需求，設計工業控制系統的安全措施，包括網路架構設計、訪問控制策略、身份驗證方法等。
5. **實施安全措施**：根據設計，開始實施資安措施。這可能包括設置防火牆、設定訪問控制列表、部署入侵偵測系統等。
6. **執行測試和驗證**：在正式運行之前，對工業控制系統的資安措施進行測試和驗證。這有助於確保這些措施能夠正確地工作並達到預期的安全效果。
7. **執行培訓**：培訓工作人員，使他們了解新的資安政策和程序。操作員應該知道如何處理警報、報告事件以及遵循安全最佳實踐。
8. **定期審查和更新**：資安是一個不斷演進的過程，定期審查和更新工業控制系統的資安措施是維持系統安全的一種手段。如追踪最新的資安威脅，並相應地調整策略。
9. **合規性和認證**：如果適用，確保工業控制系統符合 ISA/IEC 62443 標準的相關合規性要求，並考慮進行資安認證。
10. **建立資安文化**：建立一個資安文化，使所有工作人員都參與到資安保護中。這包括強調資安意識和負責任的資安行為。

除解說 62443 標準外，課程中透過設計一系列的實作練習來加深並落實實際可能面臨的問題及如何實施 62443 標準。

IC33 課程實作:

Exercisel: Asset Inventory

要正確評估工業自動控制系統（IACS）的網路安全，需要了解在操作環境中設備上運行的服務和軟體。

Exercise2: Perform a High-Lever Cybersecurity Risk Assessment (高層次網路安全風險評估)

高層次的網路安全風險評估的目的是確定與工業自動控制系統（IACS）相關的最壞情況風險。該評估並非旨在討論具體的威脅情境，而是假定系統受到最壞情況的侵害，並評估如果發生該情況的後果。

Exercise 3: High Level Risk Assessment Using CSET(使用 CSET 進行高層次風險評估)

Paint Factory 已經建立了一支風險評估團隊。作為風險評估團隊的一部分，須強制性的執行高層次風險評估（例如差距評估）。DHS 的 CSET 工具是美

國國土安全部提供的工具，是作為風險評估的一個很好的起點。

Exercise4: Vulnerabilities Scanning(弱點掃描)

使用弱點掃描工具 Nessus Essentials 進行弱點掃描，以發現可能的安全弱點。評估弱點掃描的結果，確定哪些弱點存在，以及它們對系統的潛在威脅。針對發現的弱點做處理，包括更新系統、應用安全措施和硬化系統。最後學習撰寫報告，詳細說明弱點掃描的結果以及應對措施。

Exercise 5: Pentest Windows XP Using Kali Linux(使用 Kali Linux 測試 Windows XP)

通過掃描系統來測試 Windows XP Service Pack 2 的穩健性。透過之前學到的弱點掃描知識，掃描 Windows XP 系統，確定可能的弱點。使用一個用於漏洞測試的框架 Metasploit 來測試弱點。並試圖利用發現的弱點來滲透 Windows XP 系統。最後評估滲透測試的結果，確定系統的弱點以及可能的風險。

Exercise 6: Creating a Zone & Conduit Diagram(創建區域和通道圖)

將工業自動控制系統（IACS）劃分為區域和通道是進行詳細風險評估的重要步驟。這也對於制定多層防禦策略和將策略傳達給運營和維護人員至關重要。從瞭解區域和通道的概念開始，確定 IACS 中的邊界，以確定不同區域的範圍。根據 IACS 的功能和風險特性，定義不同的區域。這可能包括控制區域、監視區域、儀表盤區域等。接著劃分通道，以確保區域之間的通信和數據傳輸是受控的。其中通道可以是物理通道或虛擬通道。若能使用繪圖工具或軟體來創建區域和通道圖，便能清晰地顯示 IACS 的組織和通信結構。然後評估不同區域的風險，以確保每個區域都有適當的安全措施。最後討論如何制定區域和通道之間的通信策略，以確保數據的安全性和完整性。

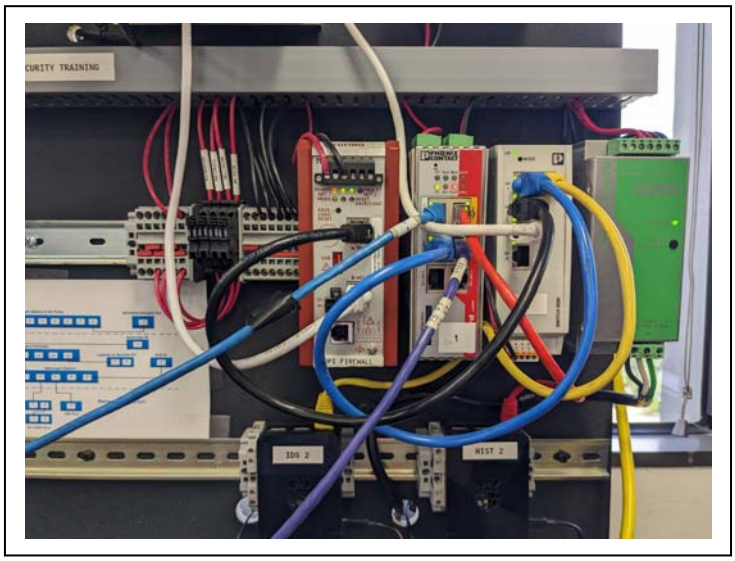
Exercise 7: Detailed Risk Assessment(詳細風險評估)

在 ISA 62443 定義的評估過程中，執行詳細的網路安全風險評估是一個至關重要且強制性的步驟。其目的是瞭解如何進行詳細的風險評估，以確保工業自動控制系統（IACS）的安全性。根據其實際情況，包括 IT 代表、自動化代表、運營代表、HSE 代表等將參與評估過程。按照 ISA 62443 中定義的流程進行詳細風險評估。這可能涉及評估 IACS 的架構、通信、身份驗證、訪問控制等各個方面。學習如何有效地識別和評估 IACS 的安全風險，以制定相應的安全措施。

總之，實施 ISA/IEC 62443 標準需要計劃、設計、實施和維護一個綜合的資安策略，以確保工業控制系統的安全運行。這需要結合技術措施、培訓和文化改進，以應對不斷變化的資安威脅。

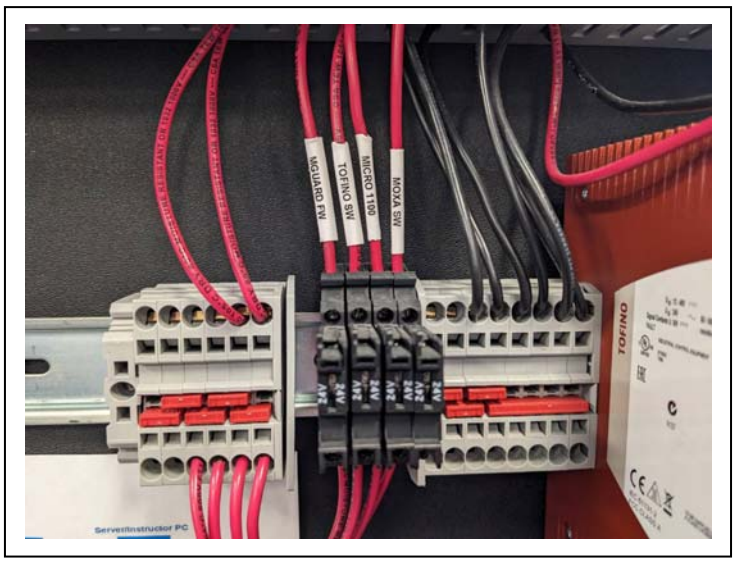
工控系統

工控系統架構說明圖



工控系統

History & IDS



工控系統配線

網路設備(左起:防火牆、防火牆 DMZ、switch、power supplier)

(二)參訪績優單位：

(1)萊斯大學(Rice University)

萊斯大學（Rice University）是美國德克薩斯州休斯頓市的一所知名私立研究型大學，成立於 1912 年。它享有出色的學術聲譽，不僅在美國，也在全球範圍內備受推崇。該校在多個學科領域，特別是工程、科學、人文和社會科學方面，取得卓越的學術成就。萊斯大學擁有多個學院和學術部門，包括工程學院、文學和藝術學院、社會科學學院、自然科學學院等。

萊斯大學積極參與工業控制系統（Industrial Control Systems, ICS）資安領域的研究和教育工作。工業控制系統資安是一個關鍵領域，關注的範疇包括工廠、能源設施、水力發電廠、交通系統等關鍵基礎設施的安全性。這些系統通常由計算機化的控制系統來管理。以下是萊斯大學在工業控制系統資安領域的研究方向：

1. ICS 漏洞分析和測試：分析工業控制系統的漏洞和弱點，以確保它們能夠抵禦潛在的攻擊。這包括對現有控制系統的測試和評估，以確保其安全性。
2. 威脅情報和分析：監視和分析與工業控制系統資安相關的威脅情報，以及開發相應的安全解決方案。
3. 安全協議和標準：參與制定和改進工業控制系統的資安標準和協議，以確保它們能夠應對不斷變化的威脅。

4. 教育和培訓：提供與工業控制系統資安相關的教育和培訓課程，以培養未來的資安專業人才。

Nai-Hui Chia 是萊斯大學計算機科學系的助理教授。他曾在印第安納大學布盧明頓分校 Luddy 資訊學、計算和工程學院擔任助理教授，還曾在馬里蘭大學聯合量子資訊和計算科學中心（QuICS）擔任哈特里博士後研究員。

賈教授的研究領域包括量子算法、量子複雜性理論和量子密碼學。他致力於理解量子計算的能力、限制以及它如何改變計算機科學。

近年來，量子電腦因其強大的運算速度和潛在能力而引起了全球科學界和產業界（如 Google、IBM、Microsoft、Intel 等）的關注。在訪談過程中，參與討論了量子電腦與資訊安全之間的關聯性，並提出了以下觀點：

1. 什麼是量子電腦?

   量子位元（qubit）是量子電腦最基本的運算單元，為了使量子位元能夠被運用，量子必須有量子疊加（quantum superposition）和量子糾纏狀態（quantum entanglement）的特性，由於量子位元的疊加和糾纏特性，使得量子位元可以不像傳統電腦位元只能為 0 或 1，而是能夠同時為 0 和 1，此特性使量子位元的運算能力增加，量子電腦得以進行大量資料的平行運算。目前主流的五種量子運算方式有矽自旋量子、離子阱、超導迴路、鑽石空位和拓樸量子。

2. 量子電腦強大之處: 量子電腦不像傳統電腦，運算步驟被位元數限制；傳統電腦在解決這類問題時，嘗試的次數和所欲搜尋的數字可能組數呈線性關係。而量子運算由於其特殊的量子特性，運算次數只需可能情形總數的平方根，滿足指數型的複雜運算需求。

3. 量子電腦之於現在技術的衝擊

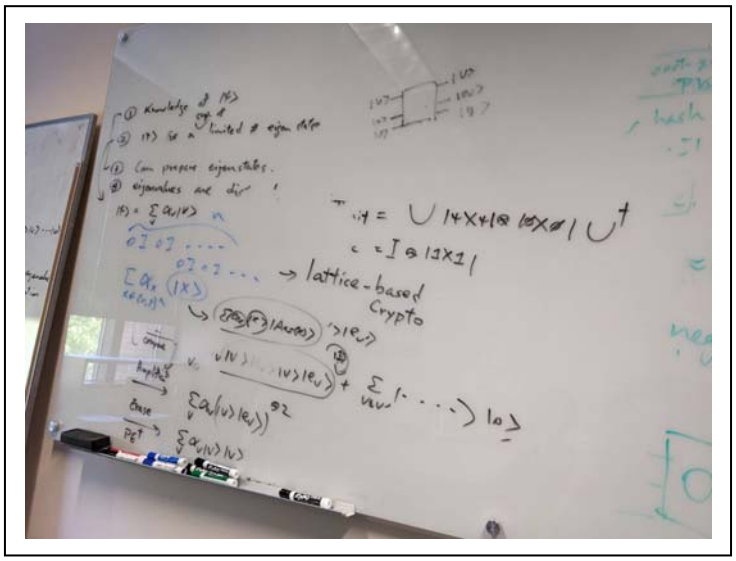
   - 量子電腦和人工智慧的結合: 量子電腦的強項在於亂數產生、尋找未排序數列的最小值、解決圖論中的節點連結問題、特徵吻合等，科學家已經設計出多種量子演算法，來解決傳統電腦不易解決的問題。而機器學習正好大量倚重這類型的大量線性代數運算，因此開始試圖將量子演算法和機器學習結合，機器學習是少數在量子電腦發展早期就有機會找到利基的領域。
   - 量子電腦在化學和製藥的應用: 量子電腦足以真正模擬

和創造複雜的電子和分子互動模型，因為量子位元的疊加特性使量子電腦能夠輕鬆完成這類運算，對新藥和新材料研發做出極大的貢獻，新藥的研發前期將可透過量子電腦模擬化合物結構和生物體內酵素或受器的交互作用，對療效和副作用做較佳的預測，減少研發時間和成本。

- 量子電腦對比特幣市場和區塊鏈安全的威脅：橢圓曲線數位簽章(elliptic curve signature)可能在量子運算下暴露出弱點，研究人員估計在 2027 年這項安全協定就可能會被破解，故量子運算技術對區塊鏈的威脅和未來金融市場的衝擊不可小覷。

4. 量子運算的技術挑戰

- 穩定量子態的維持：量子態十分容易受到振動或電磁場，甚至一般熱擾動的干擾，所以現在的量子電腦需要在接近絕對零度的超低溫度操作。使量子維持在某個量子態時間夠長，足以完成運算工作並增加運算正確率。
- 量子位元的可擴充性：現行主流量子運算技術之一的矽自旋量子，由於可利用已經十分成熟的半導體技術，具有和現行電腦相容性，且被認為未來容易向上擴充。
- 量子軟體研發：除硬體上的技術開發外，為了使量子電腦真正發揮效能，應該同步開發因應量子運算的量子軟體。而量子電腦由於運算硬體設計尚未統一，將具有不同性質的細微差別，軟體需要一定程度的客製化。運算的高複雜度也將帶動新的演算法和開發工具的需求，量子電腦軟體設計人員需具備深厚的物理、數學和軟體工程知識，跨領域、對各領域有深度知識的人才培育將會是軟體研發的關鍵。



量子演算法基本說明

Rice University Boot Camp

(2)美國國家航空暨太空總署(NASA)

美國國家航空暨太空總署（英語：National Aeronautics and Space Administration，縮寫作 NASA）是美國聯邦政府的獨立機構，其使命在於推動並領導國家的太空探索和航空研究。NASA 成立於 1958 年，是全球最重要的太空機構之一，其工作領域包括以下幾個面向：

- 太空探索 ：NASA 負責規劃和執行各種太空任務，其中包括載人和無人任務，以深入研究地球、太陽系和宇宙的奧秘。其中最著名的是阿波羅登月計劃，使人類首次登上月球，並取得了重大的科學成就。此外，NASA 還積極參與其他行星探測任務，如火星探測和木星探測等。

- 科學研究：NASA 支持並進行各種科學研究項目，跨足領域廣泛，包括天文學、地球科學、行星科學、生命科學等。NASA 的太空望遠鏡，如哈勃太空望遠鏡，已經提供了令人驚嘆的宇宙圖像和數據，幫助科學家更深入地了解宇宙的演化和構成。
- 航空研究：除了太空探索，NASA 還致力於推動航空技術的發展。該機構進行各類飛行試驗，致力於開發新的飛行器和航空技術，以提高飛行的安全性、效率和環境友好性。這項工作有助於改進航空產業，使飛行變得更加安全和可持續。
- 國際合作：NASA 與其他國家以及國際太空機構合作緊密，共同開展各類太空任務和研究項目。最著名的國際合作項目之一就是國際空間站（International Space Station），這個空間站是多個國家合作建設和運營的，為科學研究和國際合作提供了獨特的平台。

綜上所述，NASA 在太空探索、科學研究和航空技術領域發揮著重要的領導作用。不僅幫助我們更深刻地理解宇宙的奧秘，還推動著科技的不斷進步，為人類未來的太空探索和科學研究創造了更多機會和可能性。

此外，NASA 也高度重視資訊安全，採取了多種措施來確保其太空任務、科學研究和技術開發的機密性、完整性和可用性。以下是 NASA 在資訊安全方面採取的一些防護措施和做法：

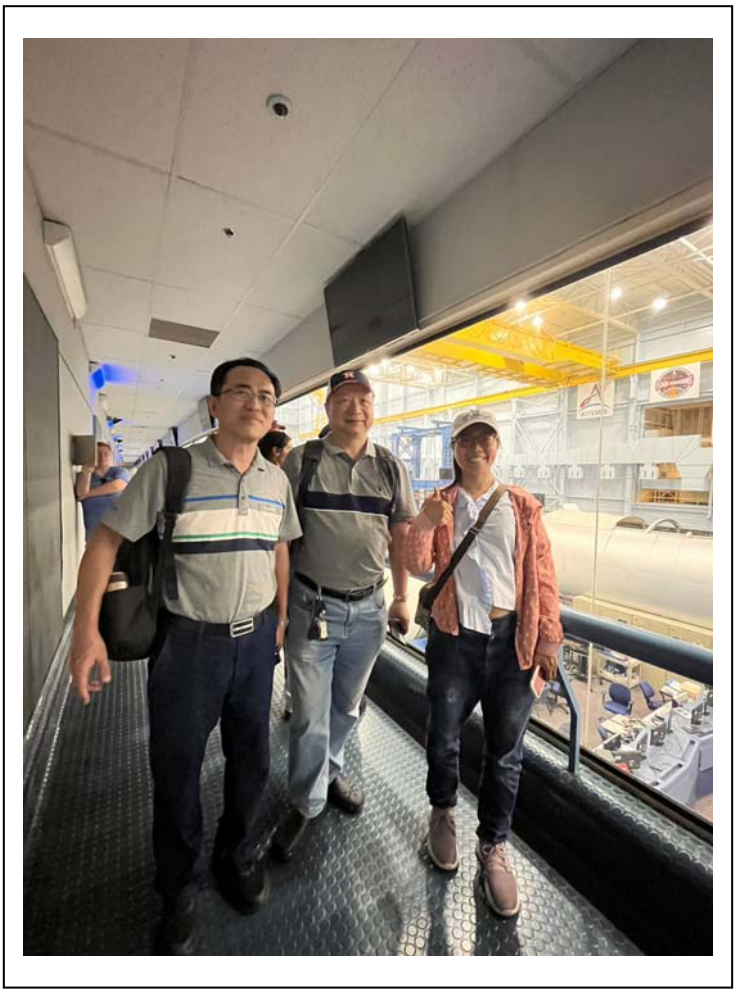
- 網路安全：NASA 維護著一個高度安全的計算和通信網路，以保護其系統免受網路攻擊和惡意軟體的威脅。這包括使用防火牆、入侵偵測系統（IDS）、入侵防禦系統（IPS）和加密技術來保障網路的安全。
- 數據加密：敏感數據在傳輸和存儲時通常會進行加密，以確保只有授權人員能夠存取和理解這些數據。NASA 採用強加密算法來保護其數據。
- 身份驗證和訪問控制：NASA 實施了嚴格的身份驗證和訪問控制措施，以確保只有經過授權的人員才能訪問其系統和敏感資訊。這包括使用多因素身份驗證和訪問權限管理系統。
- 安全培訓：NASA 為其員工提供資訊安全培訓，教育他們如何識別和應對潛在的網路威脅和社會工程攻擊。員工的安全意識培訓在對保護機構的資訊資產上是很重要的一個環節。
- 威脅監測和應對：NASA 擁有一支專門的安全團隊，負責監測網路活動，及時識別並應對潛在的威脅和攻擊。這些團隊積極

響應安全事件，以減輕潛在風險。

- 安全政策和合規性：NASA 遵循聯邦政府的安全政策和法規，確保其資訊安全實踐符合標準。此外，NASA 也與其他政府機構和合作夥伴共享資訊安全。
- 災備和業務連續性：NASA 制定了應對網路攻擊、自然災害和其他緊急情況的應急計劃，以確保其關鍵業務的連續性。

這些措施不僅有助於保護太空任務和科學研究的機密性，還確保了國家的太空探索和技術發展在資訊安全方面的高度可信度。 NASA 在太空探索和資訊安全方面的工作都是對人類的貢獻，為我們的未來探索之路提供了堅實的基礎。

Tram Tour



太空模擬艙設備區(Space Vehicle Mockup Facility)

二、個人參訓心得：

(一) 林嘉琪參訓心得：

參加 ISA/IEC 62443 標準認證課程，使我有機會深入了解工業控制系統（ICS）的資訊安全挑戰和解決方案。這讓我更加了解為這些系統提供資訊安全保護的重要性，並理解到工業控制系統的獨特特點，特別是其即時操作、高度互聯性和長時間運行等特性，這些特點使工業控制系統（ICS）不同於傳統的資訊技術（IT）環境。

將 ISA/IEC 62443 標準應用到自動化工業控制系統是一個系統性的過程，遵循 ISA/IEC 62443 的生命週期，形成一個不斷演進且循環的流程。首先，我們深入瞭解 ISA/IEC 62443 標準的概述，課程中詳細介紹了 ISA/IEC 62443 資訊安全標準，包括其各個部分和細節。隨後，討論了風險評估的重要性，並介紹了如何根據工業生產環境、公司文化和國家法規來進行風險評估，以確定工業控制系統所面臨的威脅和弱點。我們學習了如何建立風險評估框

架，以協助制定相應的資訊安全策略，作為後續管理的基礎。接著，我們探討了在人事、地點和物理方面的資訊安全措施，這些措施是在確定資訊安全需求後，為實施工業控制系統的資訊安全措施而展開的。在正式運行之前，我們需要對工業控制系統的資訊安全措施進行測試和驗證，以確保這些措施能夠正確運作並達到預期的安全效果。

課程還覆蓋了網路安全和硬體安全方面的基本原則和實踐，包括網路分段、身份驗證、訪問控制和物理安全等。我們強調了資訊安全需要全體員工的參與，包括資訊安全意識的強化和負責任的資訊安全行為，以確保組織成員都知道如何保護資訊並應對安全事件。建立組織內對資訊安全的一致理解，並制定資訊安全政策，以明確規定組織在資訊安全方面的立場、目標、原則和指導方針。我們還學習了資訊安全程序，這些程序是描述具體操作的文件，提供了實現資訊安全政策要求的具體步驟和指南，以確保工業控制系統的運行符合資訊安全要求。這些程序包括培訓、監控和事件應對等方面的標準操作程序（SOP）。

此外，為確保資訊安全的完整性，我們討論了資訊安全認證方式，用於驗證個人或組織在資訊安全領域的達成度。課程中不僅介紹了 ISA/IEC 62443 標準，還提供了實際案例和實踐經驗的分享，這使我更好地理解資訊安全概念的實際應用，並學到如何應對現實中可能的資訊安全挑戰和執行困難。這個課程將對我未來在工業控制系統資訊安全領域的工作和貢獻提供堅實的基礎。

參訪萊斯大學的經驗非常有價值，我們拜訪了賈乃輝教授，他的研究專注於量子電腦的演算法證明。這是非常令人振奮的領域，因為隨著人工智慧的發展，我們可以解決某些特定應用場景中的問題，但量子電腦具有顯著的計算優勢，源於量子力學原理，這些原理允許位元同時處於多種狀態，而不僅僅是 0 或 1。這將為我們帶來前所未有的計算能力，尤其在因子分解、優化問題、材料模擬等領域具有巨大的應用潛力。同時，我們討論了量子電腦對當前安全系統的挑戰，因為量子計算理論的推導表明，傳統的 RSA 和 ECC 等加密方法取決於大整數的因數分解問題的難解性，而量子電腦有可能縮短這一過程的時間，進而破解現有的加密系統。電子簽名和身份驗證系統也會受到量子計算攻擊的影響，一旦私鑰被破解，將威脅到電子文件的完整性和真實性。因此，我們需要思考如何應對這些潛在的安全挑戰，特別是在加密學、藥物設計、人工智慧和科學研究等領域。

參訪 NASA Space Center Houston（休士頓太空中心）也是一個令人難以忘懷的經驗。這個中心提供了許多互動式和教育性展示，類似於台灣的科博館。我們參觀了各種不同的區域，包括展示太空飛行器和太空探測器的星際

大廳，太空探索展覽，實時科學實驗，模擬太空飛行和太空行走體驗，以及火箭公園和使命控制中心。這次參訪讓我更深入地了解太空探索的歷史和未來計劃，並體驗到 NASA 的運作方式。

對於未來課程的規劃，我建議參考萊斯大學的網路安全訓練營課程。這門課程涵蓋了網路、系統、網頁技術、資料庫和防禦和攻擊性網路安全等多個領域的相關知識和實踐培訓。這將有助於學生深入了解網路安全的基本原則，包括網路分析、系統管理、網路安全設計和架構、風險管理、加密學、漏洞評估、身份和訪問管理，以及雲安全等領域。同時，學生將學習關於道德黑客和滲透測試，以及編程和腳本編寫等技能。這些知識和技能對於應對網路安全和數據保護方面的挑戰是缺一不可。

至於工業控制系統（IACS）相關資訊安全防護，我建議引進一系列技術、設備和工具，包括防火牆、網路安全設備、網路分段和隔離技術、漏洞管理和掃描工具、安全協議和加密、威脅情報和情報共享、安全監控和事件管理、身份和訪問管理、物理安全設施、安全培訓和教育，以及安全策略和政策等。這些設施和措施將有助於確保 IACS 的安全性。

最後，在 ISA/IEC 62443 標準認證課程完成後，我期許能夠將所學應用於工業控制系統（ICS）安全的實踐和執行中。這包括實施相應的標準和最佳實踐，進行風險評估和漏洞分析，制定安全策略和政策，實施安全監控和事件管理，進行定期演練和測試，持續改進，確保合規性和審查，以確保工業控制系統的安全性。這是一個具有挑戰性但也極具價值的使命，我期許能為確保這些關鍵系統的安全性做出貢獻。

(二)蔡宏松參訓心得：

工業自動化及控制系統(Industrial Automation and Control Systems，IACS，簡稱「**工控系統**」)運作於複雜的工業環境之中。現今由於工業 4.0 的發展，組織日益頻繁地在企業與工控系統間分享資訊。然而，由於工控系統設備與製程直接連結，所以資安如果受損，後果不單只是商業機密的遺失與資訊流中斷，甚至還可能造成人員喪失生命或產品損失、破壞環境、違反法規及危害操作安全。上述情況所產生的影響可能不只波及受害的組織本身，還可能會嚴重損害組織所在國家/地區的基礎設施。

除了外部威脅之外，意圖不軌的內部知情人員，或是無心、無惡意的行為，都有可能會造成嚴重的資安風險。此外，工控系統通常會與其他商業資訊系統整合，因此，修改或測試系統都有可能會對系統操作造成意外的電子性影響。由於當前有越來越多外部人員會進入工控系統的區域內部，形同不

斷地對系統進行安全測試，所以上述影響發生的次數以及造成的後果也都隨之加劇。綜合以上因素，未經授權或採取破壞性手段存取工業製程機密的情況顯然非同小可。科技進展與合夥關係可能有益商業活動，卻也增加了潛在的資安風險。企業面臨的威脅增多時，資安需求也會隨之提升。

製造業所用的系統(特別是管理和監控生產設備的工控系統)，生產設備一般置於與外部網路實體隔離的「生產內網」，不容易遭受網路資安的威脅。然而，隨著工業 4.0 網路智慧化的生產管理、設備有即時監測管理的需求，製造業者會將生產系統連上公司的網路以增加效率。此舉雖然提升了效率，但是同時也增加了生產內網被攻擊的機會。以往的舊系統保護機制也可能在連網後，無法防禦層出不窮的新興攻擊方式。通常未受到保護的舊系統，暴露在網際網路(Internet)之下，約半個小時就會中毒。

IEC 62443 是「工業自動化及控制系統」的安全標準，由 ISA 提出並由 ANSI 公開頒布，而後被 IEC 組織採納。IEC 62443 的評估測量包含申請人用正在開發的安全系統功能做評估、整合及維持特定產品的功能或解決辦法。IEC 62443 的安全性標準，是為了解決一系列工控系統應用上所遇到的資訊安全問題。工控系統包括用於製造和加工廠的設施、建築環境控制系統、地理位置分散的業務(例如公用事業：電力、天然氣和水)、石油生產管道和分配設施，以及其他行業和應用(例如作為運輸網路，使用自動化或遠端控制的資產設備)。

IEC 62443 規範標準主要基於四大方面：

1.一般(General)：所有與標準理念及其基礎概念、條款和方法有關的所有資料文件。

2.政策與程序(Policies & Procedures)：概述了工業自動化和控制系統資訊技術安全管理體系及必要要求。

3.系統(System)：提出了技術規範，作為 IACS 的設計指導方針，其中 IACS 是一種由資料採集與監控系統(Supervisory Control and Data Acquisition, SCADA)的應用、可程式邏輯控制系統(Programmable Logic Controller , PLC)、現場總線(Fieldbus)、智慧電子裝置(Intelligent Electronic Device, IED)、致動器和感測器等不同元件組成的一種資訊技術系統。

4.元件(Component)：控制系統元件的設計與開發要求。

IEC 62443 是一系列文件的集合，目前共有 14 份的文件：其中國際標準(International Standard, IS)有 10 份，技術報告(Technical Report, TR)

有 4 份。

IEC 62443 標準中的適用對象(Role)共有 4 大類:

1.資產所有者(Asset Owner)。負責營運和操作。工控系統的負責人。

2.維護服務提供者(Maintenance Service Provider)。負責維護。支援工控系統。

3.系統整合商(System Integrator)。負責調適和確認，設計和部署。涵蓋設計和建置系統的流程和系統需求，把工控系統移交給資產所有者。

4.產品供應商(Product Supplier)。負責產品開發與支援。涵蓋產品開發生命週期和要求。

由於工控系統的規模通常非常龐大，這 4 大類的適用對象必須依照 IEC 62443 建議的框架，建立具有生命週期(Life Cycle)運作的安全系統，讓安全走入制度化，融入工作環境而非僅是紙上評鑑作業。

整個 IEC 62443 的資訊安全的保護是基於縱深防禦 (Defense in Depth)的方式，防禦層由外而內包括：1.實體的安全、2.政策及程序、3.區域分隔及安全通道 (Zone and Conduit)、4.惡意軟體的避免、5.存取的控制、6.監控及偵測、7.補丁的安裝程序等。縱深防禦是資訊安全界的一個眾所周知的概念，它並不是指多種對抗技術共同使用的簡單措施。重點是根據安全性的先後次序，將防禦措施由外而內分層執行。除了技術之外，人力資源、組織、流程的措施也是需要分層落實。重要的是要在各個領域落實網路安全。在技術方面，工控系統的網路環境，劃分為區域(Zone)和連接區域的管道(Conduit)，然後將資產分成具有共同安全等級(Security Level)的群組來管理。

實體安全(Physical Security)的保護對象為:人員、硬體、程式、網路、資料等。可能造成危害的事件有火災、天然災害、竊盜、竄改、恐攻、不滿的員工等。重要資產需要設置安全機制予以保護。強化實體安全的項目有:識別證、讀卡機、USB 鎖、網路機房管制等。工作站、鍵盤、滑鼠須附鎖保護。

在政策及程序方面，IEC62443-2-1 要建立 IACS 安全計畫，規定了資產所有者的管理和營運架構。維護/管理這種安全性的機制稱為 CSMS(Cyber Security Management System)。它是一個 PDCA 的循環：計畫（Plan）、執行（Do）、查核（Check）、行動（Act）。它從分析更高等級的風險開始。然後，需要重複進行具體案例的風險分析、政策設計、組織重組、培訓、管理措施實施、審計和審查。

IEC62443-2-1 與 CSMS 認證的關係，與資訊安全中 ISO27001 標準與 ISMS(Information System Management System)認證的關係相同。由於 CSMS 是在 ISMS 的基礎上發展起來的，因此兩者之間有很多共同點，系統地延續 PDCA 循環的框架是相同的。另一方面，不同的一點是他們的目標。ISMS 的目標是所有資訊資產，但對於 CSMS 來說，其目標不僅包括資訊，還包括 IACS。其次，ISMS 認為重要的是資訊的機密性(Confidentiality)、完整性(Integrity)和可用性(Availability)，簡稱 CIA；而 CSMS 的觀點認為 CIA 的 A 尤其重要。此外，CSMS 也預設了對健康、安全和環境 (HSE) 的影響。

IEC62443-3-2 涉及工控系統的安全設計。如何將資產劃分為區域的一個要點是確定安全需求，並將其定義為通用需求。為每個基礎要求定義一個層級，然後根據通用要求和層級將資產分組。 然後，從物理和邏輯上分離資產，並明確區域之間的邊界。在現場，不僅根據邏輯要求分離資產，而且設置物理邊界也可能很困難。然而，如果不同需求或等級的資產共存於同一組中，所使用的安全技術和操作不固定，從而造成低效率。普渡大學企業參考架構(PERA)模型中定義的等級 0 至 4 可能會成為大區域，但實際的做法是根據需要，在每個層級設定子區域。

IACS 資產和區域的基本安全要求稱為基本要求 (FR, Foundational Requirements) 共有 7 項基本要求：
FR1.識別和認證控制(IAC, Identification and Authentication Control)
FR2.使用控制(UC, Use Control)
FR3.系統完整性(SI, System Integrity)
FR4.資料機密性(DC, Data Confidentiality)
FR5.限制資料流(RDF, Restrict Data Flow)
FR6.及時回應事件(TRE, Timely Response to Event)
FR7.資源可用性(RA, Resource Availability)

其次，對這 7 個項目中的每一個要求，分配一個安全級別(SL, Security Level)，來設定對資產和區域的安全要求(例如:某個區域中的 FR1 被分配為 2 級，FR2 為 1 級，FR 3 為 2 級，依此類推)。安全級別是一個具有五個級別的評分系統。每個級別的概念如下：SL0 是沒有需求定義和保護的級別，SL1 是有防止意外違規的基本保護的級別。SL4 是有保護的級別，有一個複雜的保護措施可以防止故意攻擊。為了衡量安全級別，系統需求(SR) 是針對每個基

礎需求(FR)專門定義的。此外，對於每個系統要求，指定了要求執行(RE)以滿足每個安全等級(SL)。

成熟等級(Maturity Level)主要是用來衡量整個資訊安全系統是否成熟，此處的資訊安全系統指的是人員、資安政策、流程及表單。成熟等級分成一至四級，用來描述資訊安全標準作業流程落實的程度。

惡意軟體(Malware)是造成資安損失的頭號敵人，也會造成工控系統的混亂。現今的主要的 DCS 和 PLC 如果使用 Windows 作業系統，都支援防毒軟體的安裝。

現今的工控系統中使用到為數眾多的資訊產品，例如伺服器、工作站和作業系統、HMI、資料庫、防火牆、交換器、路由器、PLC、VFD 等。在存取的控制上要確保這些裝置只能夠被經過授權的使用者或程式所存取。強化的措施如：職責分離、最小權限、嘗試登入失敗管制、系統使用通知、限制並行使用、強制離線等。在身分證明上，使用 2 種以上的憑證來驗證身分。

工控系統比較容易受駭，新的弱點幾乎每天都在通告。為了修補弱點必須安裝補丁(Patch)。安裝補丁的建議如下：

1. IACS 的裝置必須可以進行補丁的安裝
2. 補丁的安裝可以周期性進行(例如每季)
3. 補丁的安裝適用於生產環境
4. 定期檢討 IACS 的弱點

以上是一份簡明版的 ISA/IEC 62443 CSMS 心得介紹，內容可以快速融入相關資訊安全或工業控制訓練的部分課程內容，收到短時間高成就的效果。IEC 62443 是目前全球唯一採取共識 (投票) 決定出來的一個工控資安的標準，它不是單一個組織所制定出來的。此外，中華民國國家標準 CNS 也已經採納了 IEC 62443，轉成 CNS 62443 的國家標準。由目前的發展情況來看，IEC 62443 很有可能將成為工控環境的資訊安全標準，就像是 ISO 27000 系列在 IT 環境 的資訊安全標準一樣。

此次進修收穫豐富，對未來課程的規劃，建議參考萊斯大學(Rice University)的資安訓練營課程。這門課涵蓋了：資安概論、系統管理、網路、防禦和攻擊安全等，跨領域的相關知識和實習培訓。這將有助於學員把課堂上學到的網路知識，實際應用在安全的維護上面。成為名符其實的資安戰士

(Cyber Warrior)。這些是就業市場上的熱門知識與技能。

關於工控系統（IACS）相關資訊安全防護實務，建議參考 ISA 協會課程中使用的軟硬體配置，引進系列技術，包括：工控防火牆、PLC、虛擬系統、IDS、網路分段和隔離技術、弱點掃描工具、安全協議和加密、威脅情報和情報共享、安全監控和事件管理等。ISA 協會的講師都有 10 年以上的實務經驗，傳授的知識經驗相當到位。

此行在 ISA/IEC 62443 標準認證課程完成後，我希望能夠將所學心得由厚達 10 公分的英文講義中萃取出來，方便日後中文化的教學訓練和知識移轉；也希望仿製 ISA 協會的工控資安的實驗模組，方便日後的技術移轉。這些資安的訓練心得具有高度價值，值得建立與持續改進，並且需要與時俱進。「道高一尺，魔高一丈」，正好就是形容工控資安領域永無休止的一場攻防戰。

(三)簡勝輝參訓心得:

工業控制系統應用在許多不同領域，如石油、製藥、水力及電力輸配控制等，隨著科技發展如工業 4.0、智慧製造、工業物聯網 IIoT 及大數據應用等，為了即時取得數據進行管理，許多工控營運網路 OT 介接至 IT 網路，工控系統的網通安全(Cybersecurity)遂成為產業轉型成功及國家安全之重點之一。近年來在國內外發生多起重大的工控資安事件，因而工控系統的資安議題受到相當大的矚目。工控系統安全現最重要的參考標準為國際自動化協會所訂定 ISA/IEC 62443，透過風險評鑑、網路分段區隔、修補程式管理、入侵偵測、事件回應及回復等流程，以加強人員資安防護意識（Awareness），能強化工控系統安全。以下簡述本次駐點期間參加的四個課程可以參考運用的內容。

IC32 課程-探討以 ISA/IEC 62443 標準防護工控系統安全

本課程主要為工控資安概念的建立，介紹當前的工業安全環境及網路攻擊是如何發生及入侵攻擊案例探討。和 IT 資安思維強調私密性、完整性及可用性之順序不同，在工控環境下通常最重視的是可用性，接著才是完整性及私密性，即在工控環境下主要需維持設備的順利運作及指令配方的正確。依其運用場合的不同，工控資安事件可能影響產品品質、民生用水用電的維持，甚至可能發生長期的危害如爆炸、影響人身安全及對環境造成破壞等，故根據 ISA/IEC 62443 網通安全(Cybersecurity)和安全(Safety)及作業完整性同等重要。

整個工控網路，將具有共同資安需求之設備組成安全區域(Security zone)；另連結不同區域且具相同安全需求的通訊通道，組成管道(Conduit)，並依其能不受弱點影響且維持正常運作的能力指定安全等級(Security level)。建立深度防禦的概念,即由多個不同資安措施如防火牆、入侵偵測系統、防毒系統、存取

控制等不同機制共同來防堵資安事件的發生，並敍述如何應用降低風險的主要技術防毒、修補及接取控制的運作管理來降低風險。課程中也討論整個 IEC/ISA 62443 標準和實作，各種在 IACS 環境運作的工控網路協定，簡介 IACS 環境下如何進風險評估等工控安全知識及管理概念。

IC33 課程-評估現存或新建工業自動化控制系統之網通安全

工業自動化控制系統 IACS 網路安全生命週期主要有 3 個階段，分別為評估(Assess)、發展及建置(Develop& Implement)、和維護(Maintain)，IC33 課程專注於 IACS 網路安全生命周期的第一階段，根據 ISA/IEC 62443-1-1 標準的定義。學習如何識別和記錄 IACS 資產，執行網路安全漏洞和風險評估，以識別和理解需要減輕的高風險漏洞。根據 ISA/IEC 62443-2-1，這些評估需要對新的和現有的應用程序進行。

IEC 62443-3-2 包括區域、管道和風險評估的要求內容，幫助組織系統地進行風險評估，這些要求稱為區域和管道要求（Zones& Conduits Requirement, ZCR）。ZCR 包括：決定被考慮的系統（System under Consideration, SuC），與利用現有文件所進行初始風險評估。SuC 分成相關的區域和管道，根據每個區域／管道定義的目標安全級別，必須確定區域／管道是否應進行詳細風險評估，區域和管道不需要有相同的目標安全能力等級（Security Level - Target, SL-T）。詳細的風險評估由幾個步驟組成，從識別威脅、漏洞與其後果與影響開始，進一步詳細風險評估，並確定三類風險：未減輕的風險、可容忍的風險和剩餘風險。

IC34 課程-網路安全之設計及建置

ISA-62443-3 定義如何建置工控系統網通安全，涵蓋建構安全網路、資安技術導入等，在 IACS 網路安全生命週期之評估階段的主要產出為資通安全需求規格(Cybersecurity Requirement Specification, CRS)，本課程探討網通安全生命週期之發展及建置階段，依 CRS 內每個區域的目標安全等級 SL-T，就可以使用提供必要安全能力的元件及防制措施來實現達成安全等級(SL-A)，且希望每個區域達成安全等級 SL-A 要大或等於目標安全等級 SL-T。

發展及建置階段主要步驟有概念設計、細部設計及網通安全接受測試。概念設計重新檢視判讀風險評估產出的網通需求規格 CRS，為每一個安全區域建立目標安全等級，並識別出可連入區域的接取點(Access point)，運用整體及深度防禦的 5D(Deter、Detect、Delay、Deny 及 Defeat)安全能力來處理風險，並以 4T(Tolerate、Transfer、Terminate 及 Treat)來管理風險，得到概念性的系統架構以進行細部設計。

在細部設計中，每個區域的安全可以其安全基礎需求(Foundational Requirement)並以數字向量的形式表示(FR1,FR2.., FR7)，這 7 個安全基礎需求有識別和驗證控制(IAC)、使用控制(UC)、系統完整性(SI)、資料私密性(DC)、受限資料流 (RDF)、事件即時回應(TRE)及資源可用性(RA);每一基礎需求又可分為多個系統需求(SR)及可提升其安全等級之多個需求提升措施(RE)，這些安全措

施即可依其強度將區域提升至不同安全等級。

細部設計另需考量導入資安技術及措施來設計系統，有一共通控制系統安全限制，即在任何情況下要維持受控系統之健康、安全、環境和可用性。主要引入的資安技術有網路分段、防火牆、入侵偵測系統、強化作業系統、網路及設備、存取控制及遠端接取等。利用防火牆阻隔重要 IACS 系統的接取，並建構出工控隔離區，以達成深度防禦的部署。工控防火牆可識別出工控環境特有之工控協定如 Modbus 等，可對工控應用進行有效管制。工控環境下之入侵偵測系統，建置偵測工控攻擊之特徵碼，可偵測出已知之攻擊。

IC37 課程-工業自動化控制系統網通安全之維運

課程探討 IACS 資通安全生命週期之維護階段，主要工作有安全管理和維護、安全監控及偵測、事件回應及復原。和 IT 環境不同，在 IT 的安全和管理維護若發現弱點，通常會適時的加以修補，在工控系統環境下，修補若執行不正確，會對整個系統的安全性及可操作性產生負面影響。資產擁有者對每個所有的資產及修補程式，必需詳細收集、分析修補程式等相關資訊，在測試系統上進行測試驗證，確定可行之後才部署到設備上，最後在設備上對修補程式進行驗證，以確保設備可以正常運行。但應用修補程式是一風險管理決策，若進行修補的成本過高如設備停關機的生產損失，可能會推遲修補。

本次 ISA/IEC 62443 的認證課程是在休士頓 Burns and McDonnell 工程顧問公司辦理，該公司主要業務為規劃如風力、煉油、電力、水力輸配等大型工控場域，觀察到該公司友善的工作環境，有數位熟齡員工包括保安人員，只要有能力仍可在工作崗位作出貢獻，台灣已逐漸步入高齡化社會，國內如何運用熟齡勞動力，及個人自我人生規劃均可以作為借鏡。另有員工運用電腦升降桌坐著或站著工作，避免久坐以提升工作效率;至於在訓練課程的學習上，參訓學員多是工控資安、工控維運管理或 IT 資安規劃人員，很願意主動分享工作經驗及看法，也讓我們能獲得較為缺乏的實務知識。整個課程內容相當充實，需要有更多的學習才能完全融會貫通，往下將會多關注資安事件案例，以了解如何對工控環境有最佳的防護，也希能多參加資安/工控資安相關研討會，以持續提升資安技能並掌握業界新知。經工控資安認證課程學習後，除了擴展對工控資安領域的認識外，也學習到 IT 及 OT 各項資安管理面的考量，對整個資安能有較全面的認識。未來在介紹資安概論時可以附加工控資安領域，培養具 IT 及 OT 資安概念之網路技術人力，其在工作崗位上，可因具有資安意識而減少資安事件，協助提升產業的資安防護能量。

實作課程學習方面，ISA 運用虛實整合來模擬一油漆工廠的工控場域，使用虛擬系統模擬各區域的工作站，另搭配有小型模擬工控環境的網路架構;虛擬系統具一致性軟體環境，節省學員建置環境、除錯及摸索的時間，另整個教學系統可支援工控資安各階段的實習，如如練習資產盤點、執行高階風險評估、弱點掃描、詳細風險評估、工控防火牆管理、系統強化及入侵攻擊等實習，對工控資安

/資安的人才培訓有相當助益。

駐點學習期間至休士頓太空中心參訪，參觀了阿波羅十一號登月計畫控制室及登月當時監控影片重播，讓人相當振奮，登月控制室為早期的遠程監控系統，若以現在可以是一超大監控螢幕，由監控與資料獲取 SCADA 系統，將資料匯集輸出至螢幕。我國近年也將太空科技列為發展重點之一，國內也能自製人造衛星及小型火箭，期許太空科技未來也能成為國人的驕傲。策斯大學參訪，感謝賈乃輝教授於百忙中抽空接待，得知量子電腦的運算能力有機會破解較弱加密及完整性演算法，重要監控設施應提高其加密演算法強度。1962 年美國約翰・甘迺迪總統在策斯大學宣布登月計畫，演講中提出”We must be bold.”，在策斯大學看到了許多這個標語，有趣的是和前日至太空中心登月計畫控制中心參觀剛好互為呼印。

駐點學習另二位為團長林老師及蔡老師，林老師為人主動敏捷，學習相當積極很值得效法。蔡老師思慮週到，凡事均能事先設想並預為規劃，讓我們的生活學習相當順利，很是感謝二位老師。

陸、建議事項：

本案係考量除已具備工控背景者外，具資安背景學習工控亦有其優勢；因而本署建議薦派具 1 至 3 年網絡安全領域之經驗，同時須具有一定的工業環境經驗之訓練師，以其跳脫傳統思維進行學習。為促進參加研習訓練師之訓練成效，酌提建議如下：

一、 專業領域之先備條件：

以本案為例，先備條件為工業控制與資訊科技等專業基礎，為能提昇研習效果，除篩選具備相關專業人員參訓外，另建議參訓人員提前半年至 1 年於國內參加相關領域之研習。

二、 須具備足夠的語文程度：

(一) 全美語之短期訓練，教學內容相當緊湊，講師授課時，學員需要有直覺吸收及即刻理解之能力，方能跟上教學進度，若語文程度不足，需要時間轉譯，再分析講師教受內容，除降低訓練成效外，亦增加個人課後學習負擔。

(二) 另為強化參訓人員全外語之能力，建議針對專業基礎知識提供外語課程或交流，以利提前熟悉授課情境及強化語言能力。

柒、紀實照片：

萊斯大學校門口

萊斯大學 Duncan Hall 系館內部