出國報告（出國類別：實習）

排煙脫硫(FGD)控制系統安裝、運轉及維護技術研習

服務機關：台灣電力公司 台中發電廠
姓名職稱：林珈丞 儀電工程師
派赴國家/地區：美國
出國期間：112 年 09 月 18 日至 112 日 09 月 26 日
報告日期：112 年 10 月 31 日

行政院及所屬各機關出國報告提要

出國報告名稱：排煙脫硫(FGD)控制系統安裝、運轉及維護技術研習

頁數 25 含附件：□是■否

出國計畫主辦機關/聯絡人/電話：

台灣電力公司 / 翁玉靜 /（02）2366-7685

出國人員姓名/服務機關/單位/職稱/電話：

姓　名	服務機關	單　位	職　稱	電話
林珈丞	台灣電力公司	台中發電廠	儀資維護專員	(04)2630-2123

出國類別：□1 考察□2 進修□3 研究■4 實習□5 其他(開會)

出國期間：112/09/18-112/09/26

出國地區：美國

報告日期：112/10/31

分類號/目

關鍵詞：Ovation、控制系統、Cybersecurity

內容摘要：（二百至三百字）

本次赴美國艾默生電氣公司(Emerson Electric Company)參加「排煙脫硫(FGD)控制系統安裝、運轉及維護技術研習」，其研習目的是學習 EMERSON OVATION 控制系統之系統架構及控制器、模組增設和 OVATION 資安防護(Cybersecurity)等相關知識，俾使爾後機組運轉維護、更新改善帶來助益。

配合台中發電廠 5~10 號機 AQCS 空污改善工程，5-8 機原控制系統須增設控制器，並擴充及更新現有系統的控制功能，設備運轉之好壞，不僅會影響公司形象，甚至會造成超環保而產生罰鍰或機組因環保限制而降載，本組負責對 EMERSON OVATION 控制系統的運作、維護保養及修改控制邏輯等工作，赴原廠實習可以掌握相關知識，有利於日後之運轉及維護工作。

於本實習報告中，介紹 EMERSON OVATION 控制系統之系統架構、最新控制器 OCR 3000 和 OVATION 資通安全(Cybersecurity)防護。

目錄

頁次

壹、 出國目的

目標:研習台中發電廠5~10號機AQCS空污改善工程之EMERSON OVATION控制系統，包含系統架構、網路及通訊運作維護、故障排除及控制器、模組增設維護等相關知識，俾使在試運轉過程能協助解決相關問題並對爾後機組運轉維護、更新改善帶來助益。

緣由：配合台中發電廠 5~10 號機 AQCS 空污改善工程，5-8 機原控制系統須增設控制器，並擴充及更新現有系統的控制功能，設備運轉之好壞，不僅會影響公司形象，甚至會造成超環保而產生罰鍰或機組因環保限制而降載，本組負責對 EMERSON OVATION 控制系統的運作、維護保養及修改控制邏輯等工作，赴原廠實習可以掌握到相關之操作運維知識，有利於日後之運轉及維護工作，確有必要前往原廠研習。

貳、 過程

前往國家：美國

出國期間：112 年 09 月 18 日至 112 年 09 月 26 日

起始日	迄止日	行程	工作內容
112.09.18	112.09.18	台北→洛杉磯	往程：(台北－洛杉磯機場－洛杉磯)
112.09.19	112.09.23	洛杉磯	研習 Emerson 公司 OVATION 控制系統之控制器、模組建置、系統架構、組成等安裝、測試技術。
112.09.24	112.09.24	洛杉磯→西雅圖	赴 Emerson 公司旗下之西雅圖機構，研習 OVATION 控制系統軟、硬體設計維護技術與相關問題研討。
112.09.25	112.09.26	西雅圖→台北	返程：(西雅圖機場－台北)

參、 實習內容

一、 OVATION 控制系統之系統架構介紹

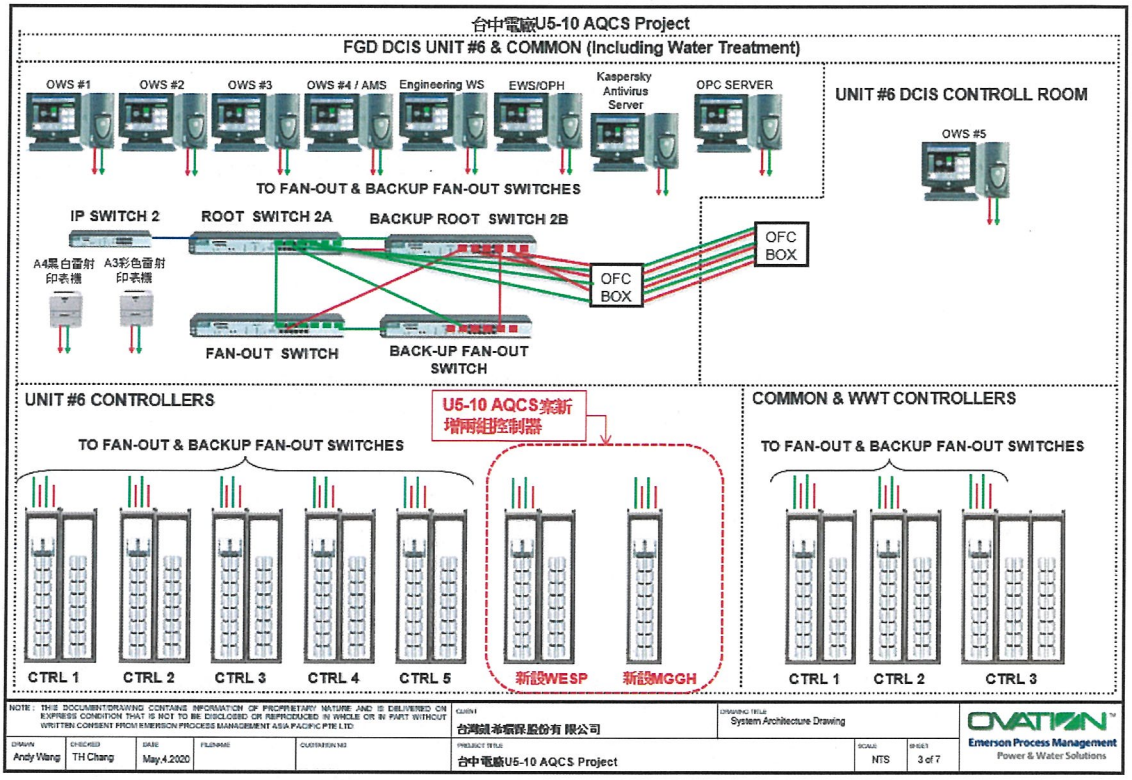
OVATION 控制系統廣泛應用於燃煤電廠，如圖一所示，汽機、鍋爐、煤處理、環境等機組均適用，並結合附屬設備如發電機等，可遠端監視其狀況。對於複循環、太陽能與水處理機組等工業自動控制需求，亦可實現與滿足。

圖一 OVATION 控制系統應用於燃煤電廠

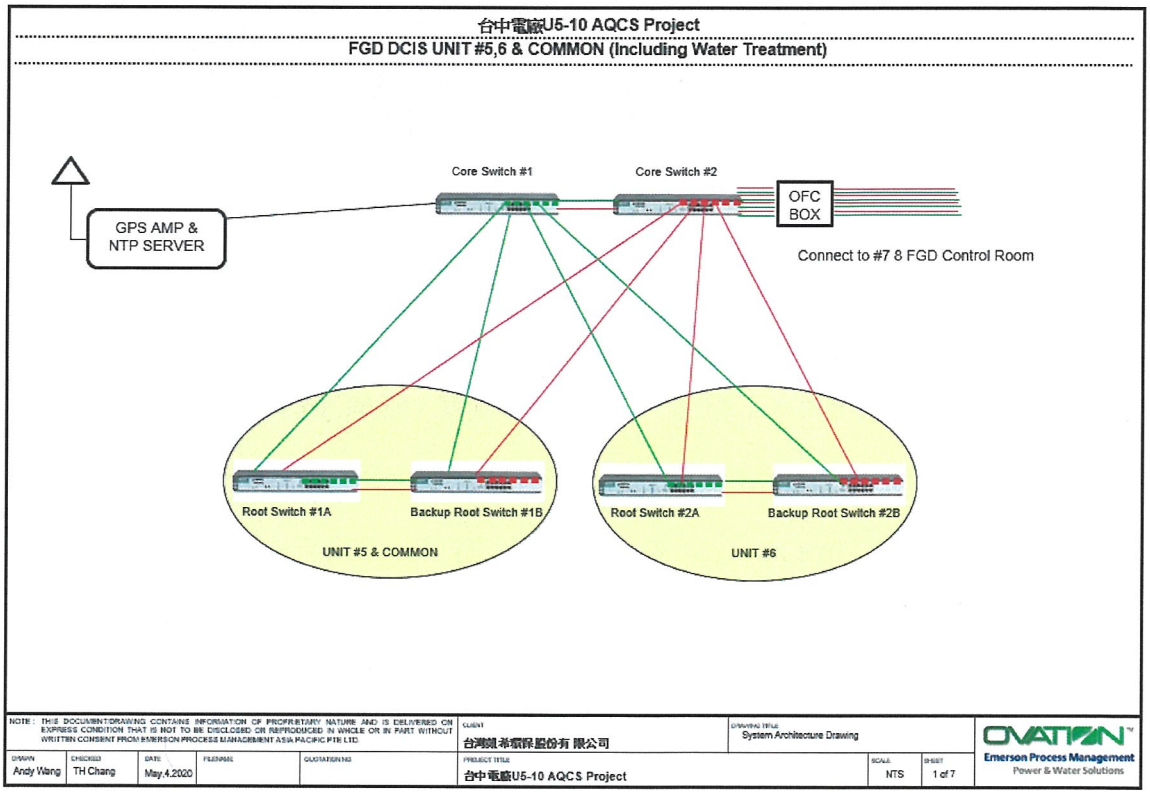
以台中電廠#5~#10 AQCS 更新改善案系統架構圖(#6 與共同設備)為例，如圖二，#6 內部 OVATION 分散式控制系統之架構，包含各式工作站(操作員、工程師、OPC、防毒軟體、資料庫伺服器、歷史報表及其他功能)，還有許多控制器，各節點利用三層式的網路架構連接，三層交換機(Core Switch、Root Switch 與 Fan-Out Switch)皆有備援，Core Switch 為架構中的最上層(第三層)，使用 Cisco 公司 Switch，為不同機組間提供通訊網路，並可查詢、使用不同機組資訊及點位(跨網域通訊)，如圖三所示。

其中 ROOT SWITCH 另外接出至 IP SWITCH，提供網路給印表機使用。

本次 AQCS 更新改善案新增兩組系統，濕式靜電集塵(WESP)與熱煤管氣對氣加熱器(MGGH)。



圖二 台中電廠#5~#10 AQCS 更新改善案系統架構圖(#6 與共同設備)



圖三 台中電廠#5~#10 AQCS 更新改善案系統架構圖(跨網域通訊)

OVATION 控制系統 SWITCH 的設置方式說明如下：

(1)Root Switch(第二層)：除第 1 埠外，所有埠組態成 100 MBPS，全雙工通訊，不可自動協商(調節速度到最高的公共水平)。

A. Port 1：定義為自動協商，阻止 OVATION 系統多路傳輸，可與 IP 設備連接，一般連接 IP SWITCH。

B. Port 2 & 3：使用於連接 Root Switch 的備援(Redundant)。

C. Port 4~24：連接下層 SWITCH (Fan-Out Switch)，或作為 Local Port。

(2)Fan-Out Switch(第一層)：除第 1 埠外，所有埠組態成 100 MBPS，全雙工通訊，不可自動協商。

A. Port 1：定義為自動協商，阻止 OVATION 系統多路傳輸，可與 IP 設備連接，一般連接 IP SWITCH。

B. Port 2：使用於連接 Fan-Out Switch 的備援(Redundant)。

C. Port 3~4：連接上層 SWITCH (Root Switch)。

D. Port 5~24：作為 Local Port 連接 OVATION 站。

二、 控制器 OCR 3000 介紹

台中電廠 FGD5~8 舊有控制器為 OCR 400，AQCS 更新後控制器升級為 OCR 1100，外觀尺寸皆相同，功能上有提升。而 OVATION 最新推出的控制器為 OCR 3000，採用基於 Zynq UltraScale+ 的處理器，使用網路介面與 OVATION 網路通訊，處理器、網路介面與 I/O 卡片連接處整合為單一模組的背板如圖四，相比前代控制器可少 2 張卡，MAC ADDRESS 也不用修改，等於少了 2 個故障點，維護上更方便，其他主要差異如下：容納軟硬體點數增加 1 倍(64,000 點)；處理器升級為四核心 ARM® Cortex™ A53 (1.2GHz)；5 個控制區同時執行時，每個控制區掃描速度可調整 (10 ms - 300s)。

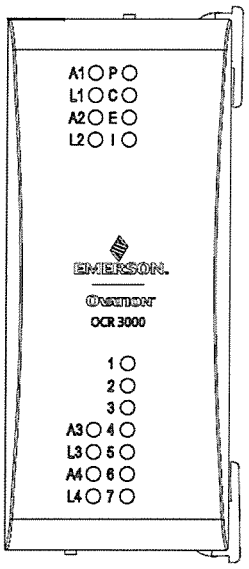
Figure 3. OCR3000 Controller module (5X00918) - 2 Copper and 2 SFP Variant

圖四 OCR 3000 控制器及整合式背板

觀察控制器上的 LED 燈號顯示，可得知控制器與 OVATION 網路、I/O 裝置之通訊狀況，如圖五，P 為電源狀態，一般為綠燈閃爍，代表電源供應電壓正常。C 為通訊狀態，一般閃爍綠燈，顯示控制器內部通訊正常運作。E 為錯誤狀態，閃爍紅燈時，則控制器內部通訊異常。I 為內部錯誤狀態，紅燈閃爍時代表控制器內部發生各種錯誤，可能原因包括控制器正在初始化、內部硬體錯誤、控制器重置及 OCR 3000 已察覺到內部錯誤。

1~7(紅燈)說明：當應用程序執行且無內部錯誤時，代表控制器的控制模式，控制模式時 7 個燈滾動式亮起熄滅，備份模式時 1 個燈滾動，若有內部錯誤時工作站會顯示錯誤代碼。A1~A4(綠燈)顯示 Ethernet ports 1~4 的網路活動狀態，閃爍則有網路活動，資料傳輸中，無燈號則沒有網路活動。L1~L4(綠燈) 顯示 Ethernet ports 1~4 的網路連接狀態，綠燈恆亮代表網路建立連接，無燈號則失去網路連接。透過狀態燈號指示，可短時間內判斷控制器異常可能原因。

Figure 6. Status LEDs for OCR3000



圖五 OCR 3000 狀態燈號

因採用備援式架構，控制器可達成自動故障轉移(FAIL OVER)控制，若控制模式下，看門狗(watchdog)檢測電路在增加計數值時，因處理器發生故障，無法即時重置計數值，會檢測到計數值溢出，而後採取恢復措施，關閉主處理器的 I/O 介面，通過 OVATION 網路發送故障訊息；備援處理器收到後即接手 I/O BUS 的控制，執行製程控制應用程式，並廣播資訊。

涵蓋極廣範圍的事件，都能觸發自動轉移，包括：

(1)控制器故障

(2)網路控制器故障

(3)I/O 介面故障

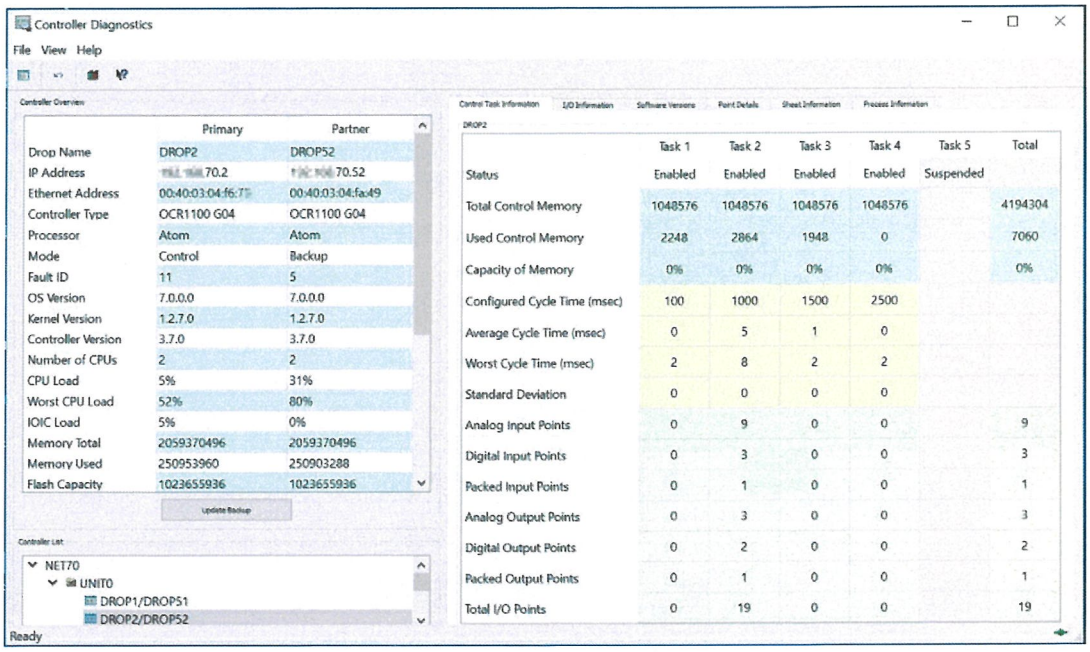
(4)控制中的處理器電源被移除

(5)控制中的處理器被重置

一旦控制權交給備援處理器，就可將故障處理器斷電、修理，當復電時對執行控制策略不會影響或產生傷害。重新啟動後，修復的處理器偵測到備援處理器控制中，就會轉為備援角色；而控制中的處理器偵測到備援處理器出現，便會調整備援操作。此自動故障轉移控制，可達到無擾動程度，確保其可靠性。

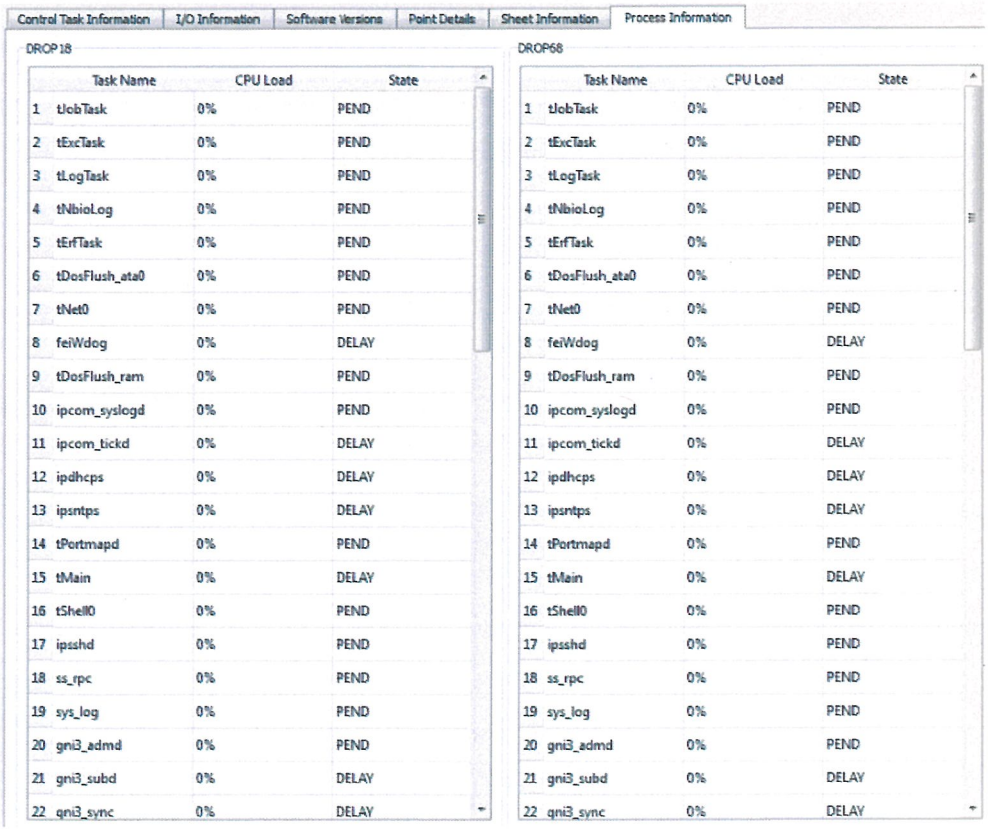
檢測網路中的所有控制器，可使用控制器檢測工具，診斷介面視窗如圖六，功能設計如下，向備援控制器更新資料，與主要控制器相符合，顯示控制器之控制任務資訊，可得知所有任務狀態、使用的記憶體量…相關資訊，顯示控制器連接之 I/O 模組資訊，為控制器連接之 I/O 模組下載韌體。

Figure 83. Controller Diagnostics window



圖六 控制器診斷介面視窗

診斷介面視窗中製程資訊頁籤，提供目前執行中任務的資訊，如圖七，可了解各任務的狀態，及使用的 CPU 負載。

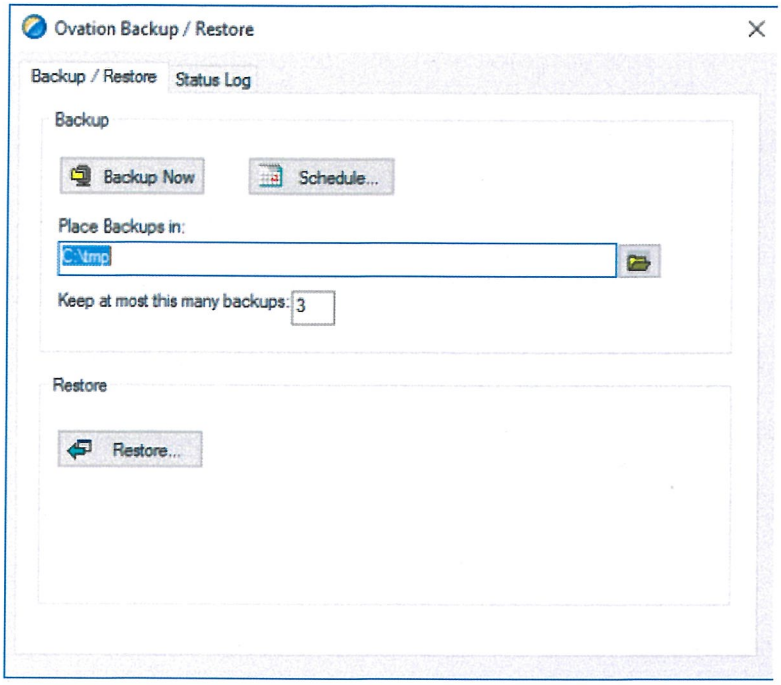


圖七 製程資訊頁籤

Ovation Developer Studio 備份及還原功能，找到「系統」資料夾，選擇 Backup/Restore，會跳出功能視窗，如圖八，設定好備份路徑後，按下 Backup Now，即可執行備份動作，在 Status Log 頁籤可檢視備份狀態及進度；按下還原按鈕，資料庫會還原到最近一次的備份。

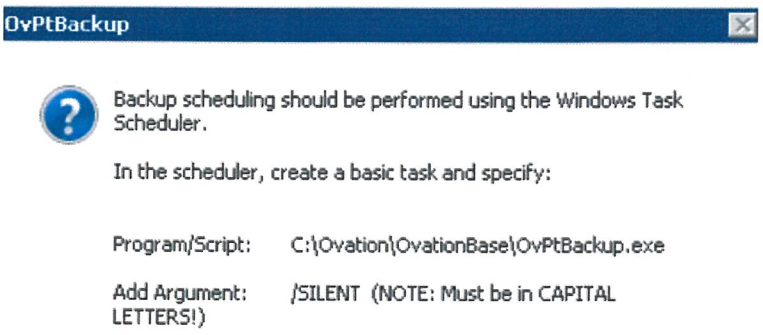
此功能用來備份及還原 OVATION 資料庫(包含控制邏輯圖、圖控設定參數及伺服器系統網路檔案)，方式是匯出資料庫並存成檔案，此檔案也可匯入資料庫，並還原至原本狀態。

Figure 62. Ovation Backup/Restore window



圖八 備份及還原功能視窗

在保留最多多少備份欄位中(預設是 3)，一旦備份數量超過，最舊的檔案將會被刪除。若要設定自動執行備份，按下 Schedule，跳至 WINDOWS 的任務排程器，輸入欲開啟程式及 Argument 如下圖九，再設定觸發週期。



圖九 輸入欲開啟程式及 Argument

三、 資通安全(Cybersecurity) 介紹

近年來國際間駭客攻擊事件頻傳，許多國家關鍵基礎設施遭受各種不同的駭客攻擊，導致設施癱瘓；甚至竊取後毀損資料或外洩個資，使得資安防護議題開始被重視，我國台灣今年也將進行《資通安全管理法》修法，以利推動國家資通安全政策，強化資安防護。

何謂資安防護？它是一門專業技術，關於保護電腦網路、裝置及資料，不被未授權的存取或犯罪使用，也是確保資訊機密性、完整性與可用性的專業性工作。前述機密性、完整性與可用性，是資安安全架構的基石(CIA Triad)，機密性：旨在對資料採用適當安全機制保護進行保密，限制未經授權的資料之訪問與修改權，除了確保隱密性，也降低機密資料陷入威脅的機率；完整性：確保維持資料原來的狀態，只允許有權限的使用者可以修改資料內容；可用性：已授權實體可即時地訪問存取與使用之特性，以確保資訊與系統能夠持續營運、正常使用，為企業產生最大化的價值。資安團隊可鑑於此三原則制定相關策略或評估潛在的威脅與漏洞。

工業控制系統領域的資安防護又是如何發展的?因為有下列三種工業規章：(1)北美電力可靠性委員會：NERC CIP(關鍵基礎設施保護)標準(2)國際電工委員會：IEC 62443(3)美國國家標準暨技術研究院：SP800-82。

一個系統的安全程度只取決於最弱的資產，削弱安全性是因為有漏洞，而常見的漏洞如下：

(1)供應商遠端存取點：產生外部接入點，可能使漏洞病毒進入。

(2)複雜度不足的密碼與過期的作業系統修補程式：易被破解。

(3)過期的防毒特徵資料庫：無法識別新的病毒。

(4)曝光的防火牆規則與失去功能的主機型防火牆：使得外部網際

網路可輕易通過直到內網，不需透過主機發送封包。

(5)共享帳戶：讓隱私洩露或遭到駭客攻擊的風險增加。

(6)不發達的資安程式：未即時更新、缺乏資源，造成防護力不足。

常見的網路安全(Cybersecurity)威脅如下：

(1)VIRUS/MALWARE (病毒/惡意軟件)：用於竊取數據、中斷運營或要求付款。

(2)RANSOMWARE(勒索軟件)：威脅發布受害者數據或阻止訪問（通過加密）的惡意軟件，除非支付贖金。

(3)DENIAL-OF-SERVICE ATTACK(拒絕服務攻擊)：用過多的請求淹沒機器/網路以破壞合法數據流（包括控制）。

(4)SPEAR PHISHING(魚叉式網絡釣魚)：假裝是受信任組織的某個人，通過電子郵件發送受惡意軟件感染的鏈接或文件，70% 的網路犯罪集團仍在使用它！

(5)CREDENTIAL REUSE (憑證重用)：使用來自不太安全的站點的駭客憑證，或在多個平台重複使用相同的密碼，又或者繼續使用“默認帳戶”。

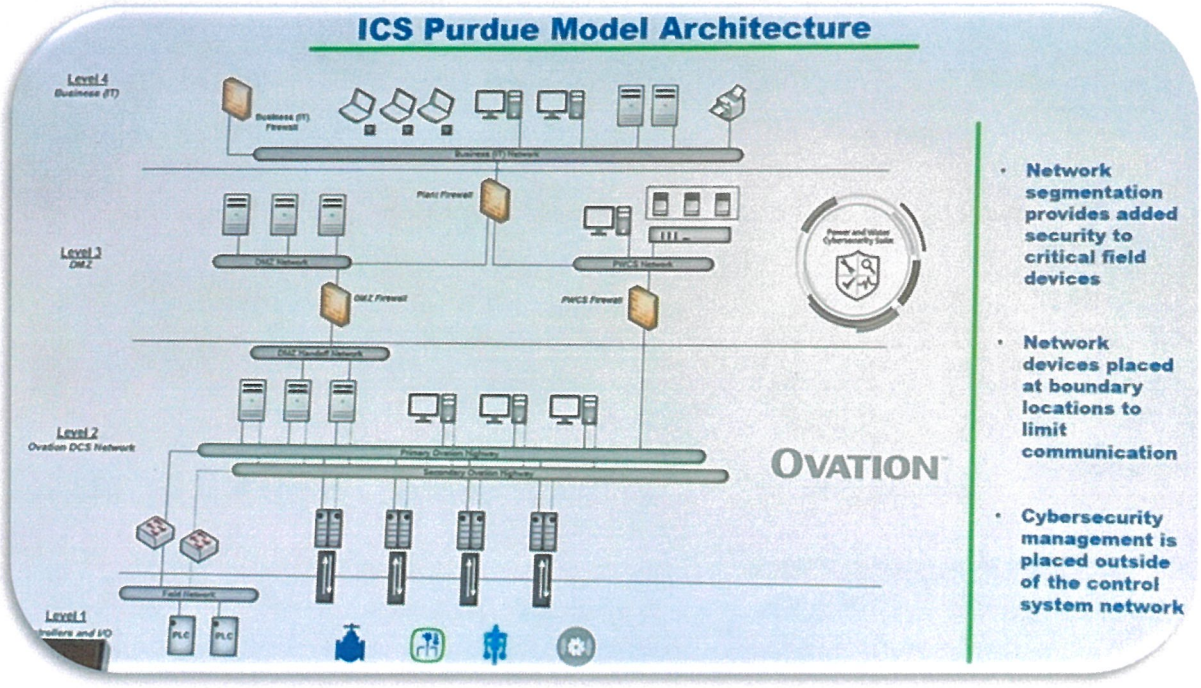
以發電廠來看，常見網路安全(Cybersecurity)威脅的來源有三，如圖十，若先針對可能的威脅建立防禦措施，便可降低資安風險。

圖十 常見網路安全(Cybersecurity)威脅的來源

四、 普渡模型與 OVATION 工業控制系統網路架構

普渡模型(Purdue Model)被國際工控自動化標準協會 ISA99(現為 ISA/IEC 62443)所採納，用來描述大型工業控制物聯網環境中重要元件的關聯、 依存關係及資料／控制流向，亦可作為風險識別標示及安全解決方案部署，是組織和管理工業通信和控制系統的分層框架，它在工業環境中實現可靠性、安全性和效率方面發揮著關鍵作用。它顯示典型工業控制系統(ICS)的所有主要組件的互連和相互依賴關係，將 ICS 架構分為兩個區域－資訊技術(IT)和運轉技術(OT) 。

普渡模型的基礎是 OT，用於關鍵基礎設施和製造，以監控和控制物理設備和操作流程。與模型頂部的 IT 區域是分開的。兩者之間設計非軍事區(Demilitarized zone，DMZ) 來分隔和控制 IT 和 OT 區域之間的訪問。 EMERSON 專家參考普渡模型建構出 OVATION 工業控制系統網路架構，如圖十一所示，由四個層級組成，每個層級都有特定的功能：製程控制、區域監控、非軍事區(DMZ)和工廠管理。



圖十一 OVATION 工業控制系統網路架構

第 1 層為現場製程控制層，包含一切與安全無關對受控設備進行控制的系統或裝置，其中的受控設備屬基礎設施，即製程中運作的實體設備或元件，也包含了各式各樣安裝在現場的感應器、驅動器、PUMP、閥門…等構成製程的元件，有些系統透過可程式化邏輯控制器（Programming Logic Control, PLC）來控制，大部分系統實體製程，是由人直接於現場或遠端操作，主要執行：

(1)依照編寫好的邏輯控制製程，優化工廠操作以達穩定運轉及生產，並兼顧環保空汙及水汙的各項管制標準。將所有製程變量保持在安全限制內(保護邏輯自動觸發或操作員手動調整)。

(2)通過人機介面使操作維護人員能作監視及控制。

(3)提供警報及事件記錄。

第 2 層為機組操作監控層，屬於監控中心，監控整個機組區域製程控制場域，包括監控和資料蒐集系統（Supervisory Control And Data Acquisition，SCADA)與分散式控制系統(distributed control system，DCS)，功能為監視畫面及存取控制。透過這些系統的監控、警報與事件回應，可使操作維護人員即時監控製程狀況，同時降低所需的人力成本，讓現場製程的可用率、安全維持穩定。

第 1 層及第 2 層為運轉技術(OT)，使用各種軟硬體結合來控制及維護工業設備，實現自動化控制。第 4 層為資訊技術(IT)，包括：資料蒐集、使用、傳輸以及儲存，重點在管理、開發、安裝又或是規劃、研發資訊的電腦主機、網路通訊裝置等硬體設備或軟體，也負責對於老舊的設備進行更新或汰換。

第 3 層非軍事區層，是在不信任的外部網路(IT)和可信任的內部 DCS 網路(OT)外，建立一個面向外部網路的物理子網路，透過不同防火牆區隔出一層，有獨立網段，讓 IT 層使用者可以存取企業及工廠的公

開資訊，但無法存取內部敏感資訊。此非軍事區層的設置，限制了通訊，讓 OT 與 IT 並非可直接互相存取，增加安全性，提升關鍵區域的資安強度。

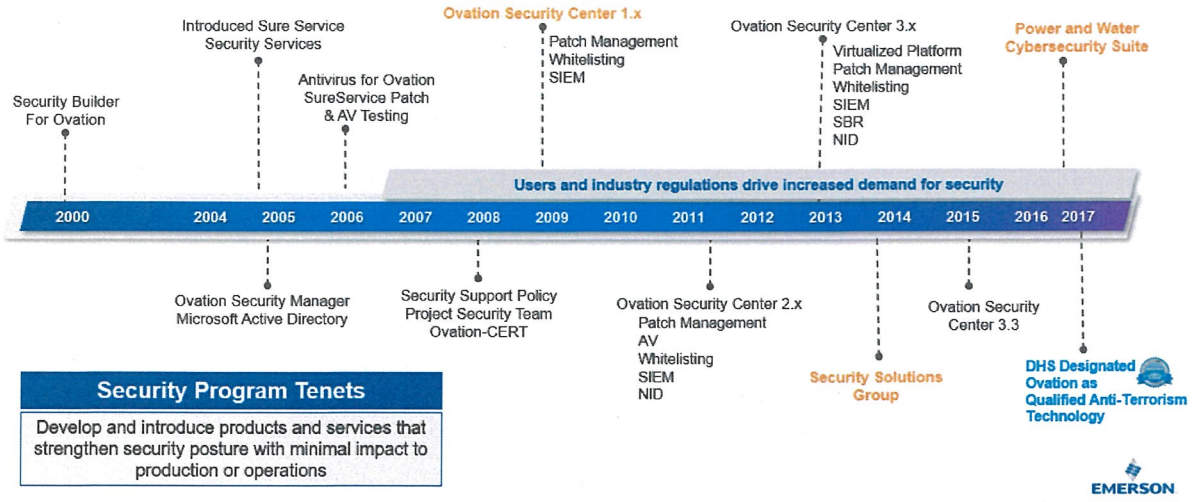
第 4 層為企業及工廠營運層，包含了業務、研發、運轉管理及人力資源發展…等，會直接連到外部網路。

五、 EMERSON 安全解決方案

EMERSON 安全解決方案團隊成員，包含全球工業 Cybersecurity 專業人士、CCNA 認證工程師及認證道德黑客(如圖十二認證標章)，都是有 Cybersecurity 和網路專業知識的專家，他們專門開發並提供 Cybersecurity、先進的網路服務和解決方案。

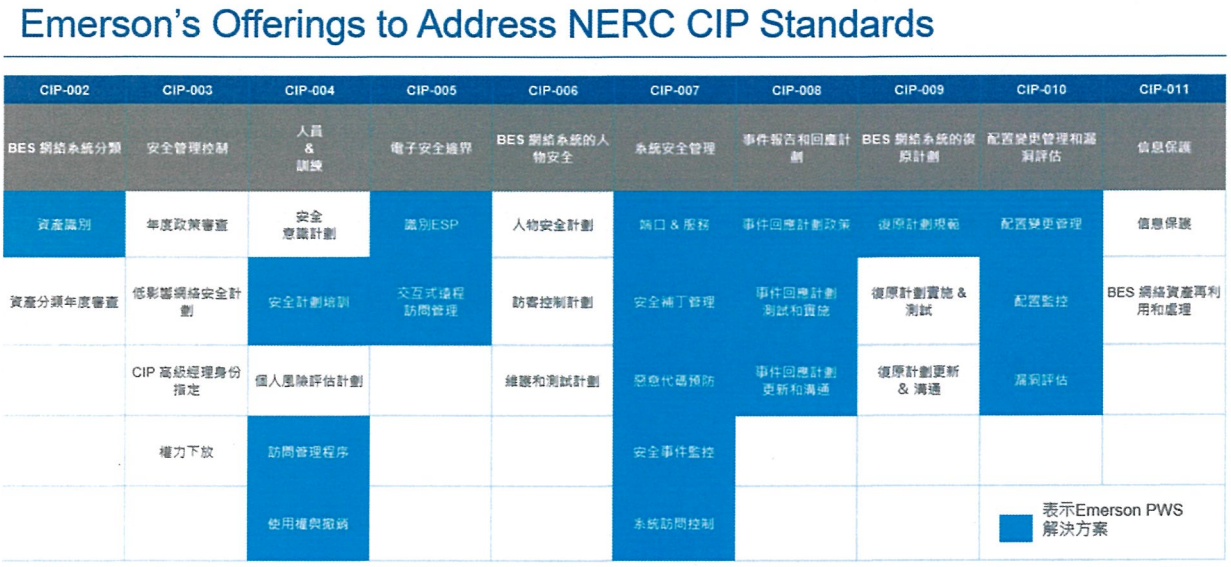
圖十二 認證標章

EMERSON 的資安計劃與解決方案建立歷史如圖十三所示，早在西元 2000 年就成立了建造 OVATION 系統安全的團隊，而後不斷推出安全功能及服務。2007 年起，使用者與工業界的規章使得安全需求增加，便成立了 OVATION 安全中心，開發更多安全功能，提供專家即時諮詢與到現場執行安全任務。2016 年末，EMERSON 集多年之大成，推出了電力和供水資安套件 (Power and Water Cybersecurity Suite，PWCS)。



圖十三 EMERSON 的資安計劃與解決方案建立歷史

針對美國 NERC CIP 標準，EMERSON 提供了相應的電力與供水解決方案(PWS)，如圖十四。



圖十四 EMERSON PWS 解決方案

美國國土安全部（DHS）根據美國安全法案進行徹底的申請、審查和測試後，艾默生過程管理電力與水解決方案公司（Emerson）Ovation 控制解決方案已被國土安全部指定為合格的反恐怖主義技術(如圖十五)。該名稱涵蓋 Ovation 控制系統及電力和供水資安套件，以及

Emerson 的 Cybersecurity 服務。

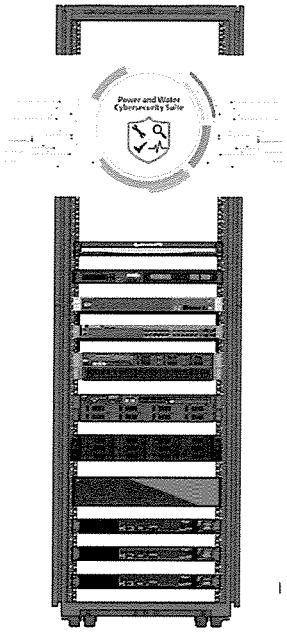
圖十五 國土安全部指定為合格的反恐怖主義技術

此指定為 EMERSON 客戶提供重要的法律責任保護，《安全法》(SAFETY Act)內容寫到：「凡經過聯邦認證提供維安服務和產品的民營業者，如果無法避免恐怖攻擊也不需要負責。」以應對因《安全法》定義的恐怖主義行為而引起的索賠，意即若事件肇因於「恐怖主義行為」，導致各種事故或業務中斷而遭第三方索賠，將由國土安全部保護而免責。

六、 電力和供水資安套件(PWCS)

此套件包括軟體與專門用於抵御威脅和保護系統網路完整性的模塊，如圖十六，協助發電客戶符合 NERC CIP 標準，以實現大容量電力系統的可靠運行，提供增強的控制系統保護，而不會中斷。能主動監控威脅並實施補救措施，防止工作站和服務器遭受病毒和恶意軟件入侵。設備控制可保護並集中管理與 Windows 工作站和服務器相關聯的儲存

設備。解決方案可確定工作站和服務器的補丁需求，並提供用於備份和恢復的工具。



圖十六 電力和供水資安套件

PWCS 模塊組成如圖十七所示，硬體由下而上依序介紹：

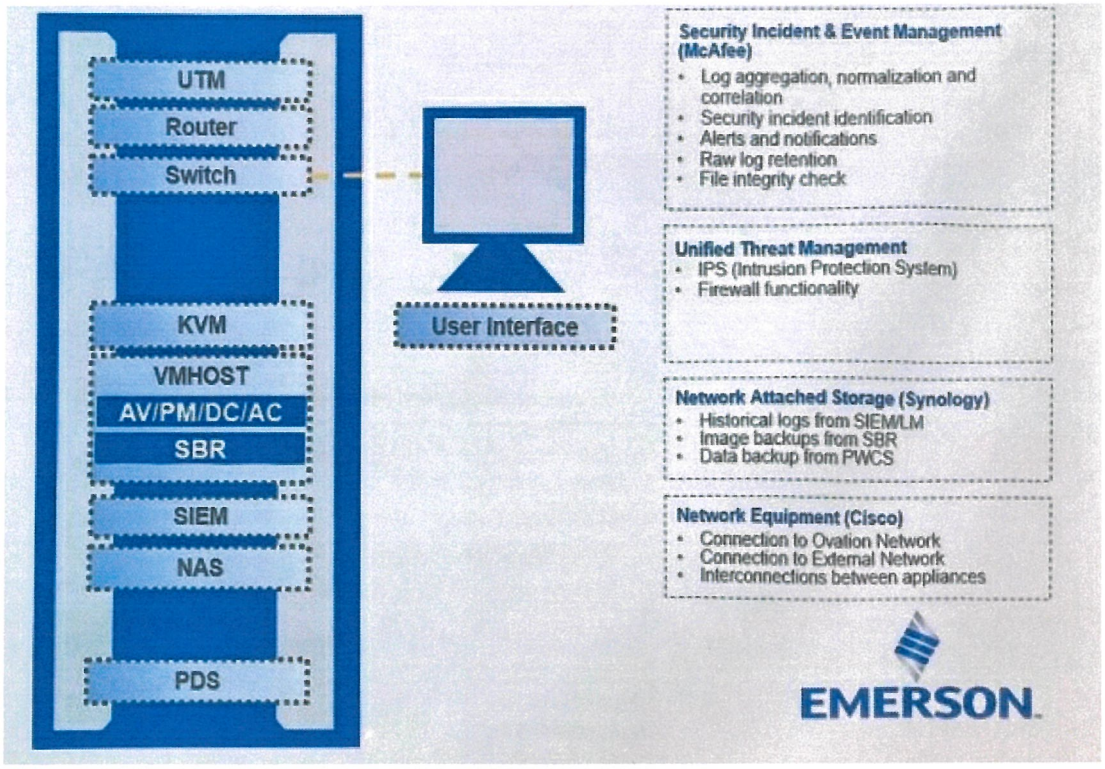
(1)PDS：分散式電源系統，確保電源供應無虞。

(2)NAS：存放 Ovation 網路中電腦系統備份，能透過網路存取檔案。

(3)SIEM(Security Incident & Event Management)：提供集中儲存和管理安全事件 (logs)功能，包括補丁管理、應用程序控制、防病毒，VMHost 也將其事件發送到 SIEM。

(4)PWCS VMHOST：使用 VMWare 建立兩台虛擬機，功能分別為 e Policy Orchestrator 及 SBR(system Backup & Recovery)。

(5)UTM(unified threat management)：提供防火牆與入侵偵測防禦系統(IPS)等功能，能有效阻擋來自網路上的威脅，確保使用者不致遭受來自外部的攻擊，例如分散式阻斷服務（DDoS）攻擊。



圖十七 PWCS 模塊組成

PWCS 資安防護功能實踐由分析開始，啟動各種防禦機制，正常運作時全面監督檢測，最後回應進行處理如圖十八，相關功能介紹如下：

圖十八 PWCS 資安防護功能實踐

(1)Antivirus Protection (防病毒保護)：為工作站和服務器提供即時病毒和惡意軟件保護，防範已知惡意軟件感染。

(2)Application Control (應用程式控制)：使用白名單技術減少未知應用程式執行。

(3)Configuration Management (電腦系統配置管理)：有效管理系統配置，重點關注基於 Windows 的工作站和服務器、網路設備和 Windows 的 Active Directory，減少系統收集資料時的負擔。

(4)Device Control (移動設備控制管制)：防止使用未經授權的可移動媒體來幫助阻止惡意軟件的傳播。例如嵌入式 CD/DVD 驅動器和串行/並行端口，以及各種可移動設備。

(5)Network Intrusion Detection (網路入侵檢測)：通過電子安全邊界上的路由器監控數據流量，並使用深度數據包檢測監控和檢測可疑流量，偵查出透過網路的攻擊。

(6)Patch Management (補丁管理)：識別漏洞並安裝可用的補丁管理包，包含 OVATION 系統、WINDOWS 系統及第三方軟件補丁，修複已知漏洞。

(7)Rogue System Detection (離群系統偵測)：提供未知網絡連接設備的通知。即時監控以檢測未受保護和不受管理的系統，並將離群系統轉換為託管客戶端。

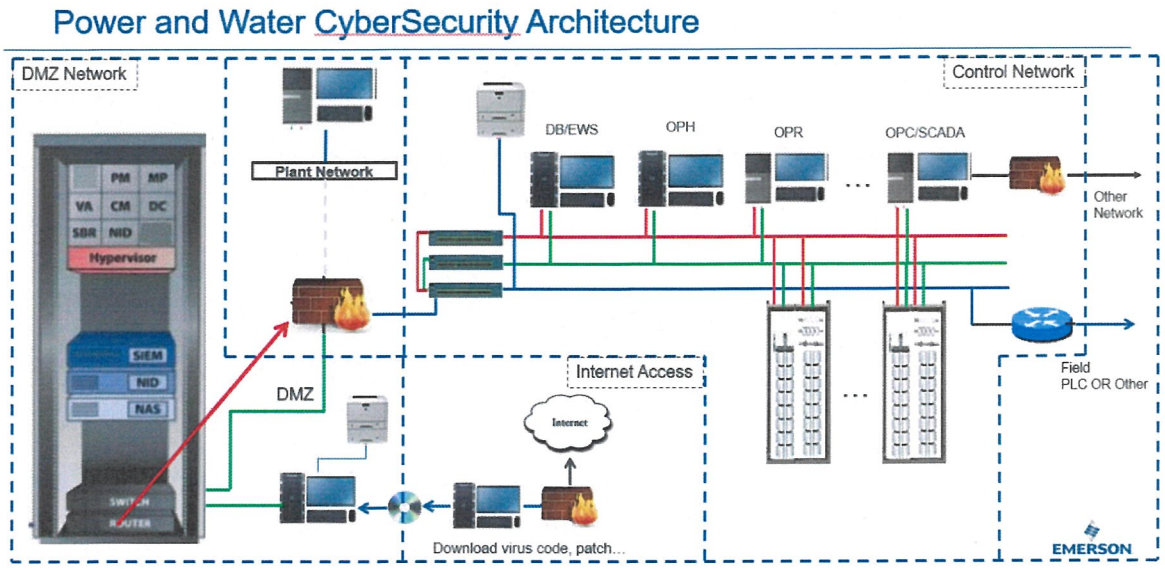
(8)Security Incident & Event Management (安全事件和事件管理)：從包括 Windows、Linux 和 Solaris 在內的各種操作系統收集安全事件及儲存系統事件日誌；也包含交換機、防火牆和路由器。該模塊還通過簡單網路管理協議 (SNMP) 或系統日誌消息 (Syslog) 從其他數據源收集事件。

(9)System Backup & Recovery (系統備份和復原)：執行與每個工作

站硬盤相關的磁盤或文件級數據備份和恢復。由嵌入在 PWCS 中的管理服務器軟件和加載在工作站和服務器上的代理組成。

(10) Vulnerability Assessment (弱點評估)：通過提供可靠、靈活和主動的工具來掃描系統環境中的弱點並提供降低風險的指導，意即提供 DCS 系統安裝已知而未安裝的安全議題，從而縮小漏洞和風險。

將電力和供水資安套件(PWCS)整合進控制系統架構後(如圖十九)，在外網與內網間形成一個非軍事區(DMZ)，如此一來控制系統網路可受 PWCS 保護與監控，大幅強化資安。



圖十九 PWCS 整合控制系統之架構

七、 問題與回覆

問題一：廠內曾發生過三部機組陸續停止通氣，當時發現是 SWITCH 功能有問題導致，請進一步說明及如何解決？

答覆：

Ovation DCS 系統的跨網域通訊(Multi-Network function)是透過 Cisco 公司的 Core Switch 3560 在不同網域上以廣播(broadcast)發送。然而當時確認狀況是 Core Switch 發生 TCAM(ACL and forwarding table information)損壞時，並不會因為發生異常而停止工作，而是將其自身的 Layer 3 功能降階為 Layer 2 功能而持續發送資料。但因 Ovation 的資料係以 SID(System ID)之流水編號組成，即使是不同網域，仍有可能有部分資料的 SID 是重疊的，因而造成 Ovation 的跨網域資料部分混亂，進而導致系統異常。

解決方式是修改 Switch 參數規劃，將 Root Switch 連至 Core Switch 的 port function 由 broadcast 改為 IP，使得即使 Core Switch 僅剩 Layer 2 功能，也會因為相關跨網域資訊已有指向固定 IP 位置，而不會有混亂的情形發生。

問題二：I/O 卡片發生 INTERNAL FAULT，因串聯架構導致可能的故障點繁多，大卡、小卡、FUSE、終端電阻、ROP 板、通訊線(電源)或背板？如何快速判斷確切故障點?

答覆:OVATION 韌體升級到 3.8 以上版本後，便可使用新增程式「SYSTEM VIEWER」，開啟後查看 FAULT CODE 說明，再點選 HELP 按鈕，獲取硬體位址解碼及 I/O 狀態值等進一步資訊，可幫助判斷問題點。

肆、 心得與建議

建議一：資安防護實踐重視系統備份，甚至使用 NAS 另外儲存一份備份檔，故建議增加另外一份定時備份。作法說明：由於工作站已作 RAID(容錯式磁碟陣列)，無法再增加內接式硬碟，在不改動原架構前提下，建議使用外接式硬碟，搭配 Ovation Developer Studio 的定期備份功能，比如每月備份一次，將來進行還原後的資料庫能更符合所需。

建議二：廠內控制系統之廠牌繁多(Siemens、Foxboro、Emerson)，如能朝向單一廠牌規劃，相同控制系統可減少人員之訓練時間、備品之儲備數量、降低維護成本，建議於機組新建或更新改善時能考慮控制系統廠牌單一化。(本次#5~#10 AQCS 更新改善案，所幸沿用原有控制系統之廠牌，不致增加太多維護負擔。)

心得：

這次出國實習參觀了 EMERSON 在美國不同的分公司，認識最新控制器 OCR 3000，及獲取資安資訊及訓練，原廠大力推薦升級至 OCR 3000，惟基於預算、備品、國內實蹟與成熟度考量，全面性綜合評估後才能決定。聽了 EMERSON 介紹他們資安團隊的歷史，才知道他們做了這麼多的努力，不只是 OVATION 控制系統獲得全球性的獎項，受發電領域客戶喜愛，還設計了 PWCS 資安套件，並且由認證專家組成的資安團隊能提供即時諮詢，若發生計劃外的停機也可到現場執行安全任務。上述 PWCS 資安套件加上 Ovation 控制系統及 Cybersecurity 服務，被美國國土安全部指定為合格的反恐技術，深受肯定。本著追求創新科技的企業精神，持續提出符合業界需求的解決方案，所以 EMERSON 才會備受工業界

領導者們信賴，通過與他們合作來解決一個又一個巨大的挑戰。

隨著國內日益重視資安問題，即便是封閉式網路也需強化資安，既有的 OVATION 控制系統，再結合 EMERSON 設計的 PWCS 資安套件，防止駭客及病毒入侵、攻擊，就能全面性、有效的保護機組網路，確保國家關鍵基礎設施的安全。

實習期間需長時間全神貫注，一邊以最快速度聽英文、同步翻譯，一邊配合課程進度順勢提出想問的問題，有些吃不消。即便出國前已把握時間沉浸在英文環境加強英聽，仍有 10%遺漏。語速比想像中更快，一句話還特別長，有時會不小心分神，還好講師並不趕進度，能配合我需求先停下來，換個方式講解，或針對問題進一步解答再繼續課程，讓我收獲更多。往後將持續學習，再提升專業能力，同時也精進英文能力，期許能為公司有更多的貢獻。

特別感謝總處長官翁組長勝欣、台中發電廠許廠長家豪、吳副廠長重仁、江經理瑞益等長官之栽培，才能有本次前往美國 EMERSON 公司實習的機會，不但增進專業技術，也拓展個人視野，留下職涯中重要的里程碑。最後還要感謝本課所有同仁，在出國期間分擔我的工作，讓我無後顧之憂，不勝感激。

伍、 參考資料

1. Ovation Controller (OCR3000) User Guide
2. Ovation Developer Studio User Guide
3. Power and Water Cybersecurity Suite(PWCS) Student Handout
4. Cybersecurity Best Practices
5. Security Solutions Overview