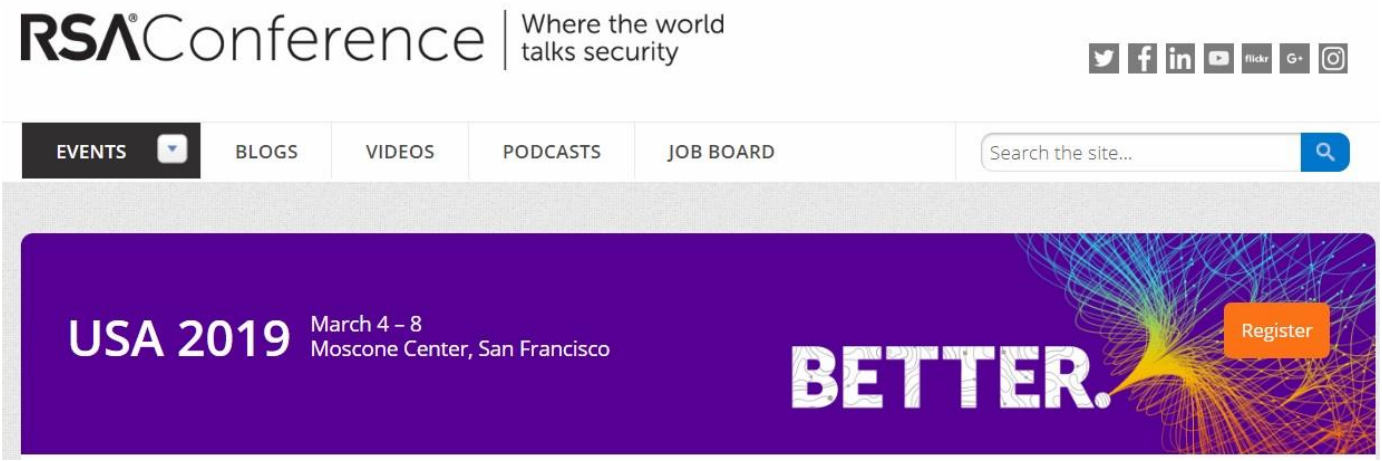
出國報告（出國類別：考察）

RSA Conference 2019 資安展
及美國關鍵基礎建設機關 SCADA 參訪



服務機關：台灣中油股份有限公司

姓名職稱：呂豐州 組長

派赴國家/地區：美國 舊金山

出國期間：中華民國 108 年 3 月 3 日至 3 月 10 日

報告日期：中華民國 108 年 4 月 2 日

摘要

本次 RSA Conference 2019 資安展是 2019 年全美最主要的資安大會，最近幾年皆能吸引 4～5 萬名與會者參加，今年即於 2019 年 3 月 4 日至 3 月 8 日在美國舊金山舉辦，前後共計 5 天。因為時差(換日線)及班機的關係，3 月 3 日由桃園機場出發、3 月 8 日深夜由舊金山搭機返回抵達桃園機場已是 3 月 10 日早上。

該大會活動地點主要座落在 Moscone Center 區域，共分為四個主場地：Moscone 南館、北館、西館及 Marriott Marquis 舉辦 Keynotes、Sessions & Events、Tutorials & Trainings、Learning Labs、Sandbox Contest 以及廠商產品攤位展示等(Booths)等各類活動主題，貫穿整個資安大會的各項活動主要與 SACADA、數據洩漏、網路威脅、雲端安全、風險管理、應用程式開發安全、可攜式裝置安全、加密和身分管理、法規遵循、社會工程(女性參與等)、立法與政策等議題有關，除邀請業界具前瞻性思想的領導者提供演說內容外，並導入產業技術與防護安全的新方法，不但是科技安全新知傳遞的園地，也是資安產業同行競合關係建立的管道。

本次研討會共分為 24 個主題、以及超過 800 位專家的演講者，多達 700 場會議及至少 700 家以上的參展廠商，在前述 4 個主要場地同時進行。

其中有一項創新的沙盒競賽，每年皆會進行投件並經過審查後，選出最優秀的 10 家新創公司，在年會活動中各進行 3 分鐘的簡報，展示其創新技術以爭取評審優勝。

本次參訪活動主要安排二項行程，行程一是參加 RSA Conference 資安大會舉辦的相關主題研討以及展點廠商所展示的資安防護技術運用。行程二則是參訪舊金山當地關鍵基礎設施機構的 SCADA，瞭解工控系統環境所採取的資安防護措施，俾汲取其經驗提升及強化自我的資安防護能量。

若各以一句話來表達前述二項參訪行程的深刻體驗，就是：

一、 對於資通安全的認知：資安攻擊是**『When』不是『If』**。

二、 對於國內工控環境(OT)的資安防護：**縱深防護、持續改善。**

目次

壹、目的

過去因為工業控制環境(OT)與企業資訊環境(IT)的實體隔離(Airgap),所以工業控制系統並不把 IT 環境中經常發生的病毒感染、駭客入侵等資安威脅放在心上，在資安防護的領域裡似乎過著與世無爭的太平盛世，但現在隨著資通科技的發展與應用，為了提升企業整體營運績效，工業控制系統已不可避免地必須透過網路介接企業資訊網路,將即時資訊傳輸至資訊系統以滿足營運資訊整合的需求,因此，傳統上工業控制系統資安防護所仰賴的實體隔離(封閉性)已不復存在，導致外界可透過網際路或企業內部網路，竊取相關工控制系統的資訊或取得工業控制系統的控制權，再加上 OT 人員長期對於資安防護的輕忽或警覺意識的薄弱，造成關鍵基礎設施曝露在高度資安風險之中。

這次個人參加 RSA Conference 2019 資安展及美國關鍵基礎設施機關 SACDA 參訪活動的目的，一則是參加美國最重要的資安大會(RSA Conference)，瞭解當前資安防護技術發展的方向與進展；二則是美國在台協會(AIT)商務組主辦安排美國基礎建設機構的參訪交流活動，實地瞭解美國工控系統環境的資安防護經驗。藉由前述瞭解資安防護技術發展與美國工控系統環境的資安防護經驗，做為本公司物聯網網路安全、資料洩漏防護、網路資安攻擊、以及關鍵基礎設施防護策略

的擬訂參考，期以強化關鍵基礎設施面臨資安威脅的防護能量，降低資安事件發生的機率與損害衝擊。

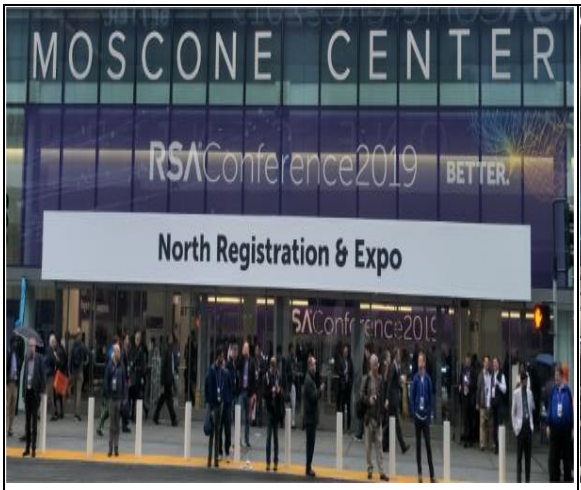
貳、過程

本次活動係美國在台協會(AIT)商務組發起，國內派員參加的機關（構）包括：國家土地安全辦公室、資通安全處、國家通訊傳播委員會、油電國營事業、資訊工業策進會以及國內資安服務與系統整合廠商。在 AIT 商務官馬奎立先生(Matthew Quigley)協助聯繫美國關鍵基礎設施(CI)機構，確定美國關鍵基礎設施機構 SCADA 參訪的 Spin off 日期後，通知相關參訪人員各自安排班機往返、當地住宿交通、以及參加 RSA 活動的行程，對於不常出國的人員而言，是難能可貴的生活體驗，也算是這次出國參訪的額外收穫。

這次 RSA Conference 參訪之行，除了參加【BETTER】主題的 RSA Confrence 資安大會之外，能與 AIT 安排的美國「國家標準技術研究所」(National Institute of Standards and Technology, NIST)、舊金山的「太平洋氣電公司」(Pacific Gas and Electric Company，PG&E)、以及資訊工業策進會安排的「加州電力調度中心」(California Independent System Operator, CAISO)，進行面對面的意見交流與參訪活動，瞭解資安防護標準或政策的擬訂過程、關鍵基礎設施機構

現行如何規劃及執行工控系統 OT 環境資安防護措施，受益良多。

下圖即為 RSA Conference 2019 Moscones Center 北館及地下室 Booths，以及本次出國參訪的的主要成員(與 NIST 交換意見後的合照)。



活動行程

（一）RSA Conference 2019 資安展活動

本次 RSA Conference 大會討論議題涵蓋廣泛，不過受限於時間的關係，僅能挑選與 IoT、雲端服務或工業控制系統等資安議題相關之 KeyNotes 或演講主題，例如軟體開發威脅、物聯網與雲端服務新興威脅、委外服務管理、法規政策參與以及關鍵基礎設施防護等有關之研討議題，以瞭解 2019 年最新資安創新之技術與觀念。

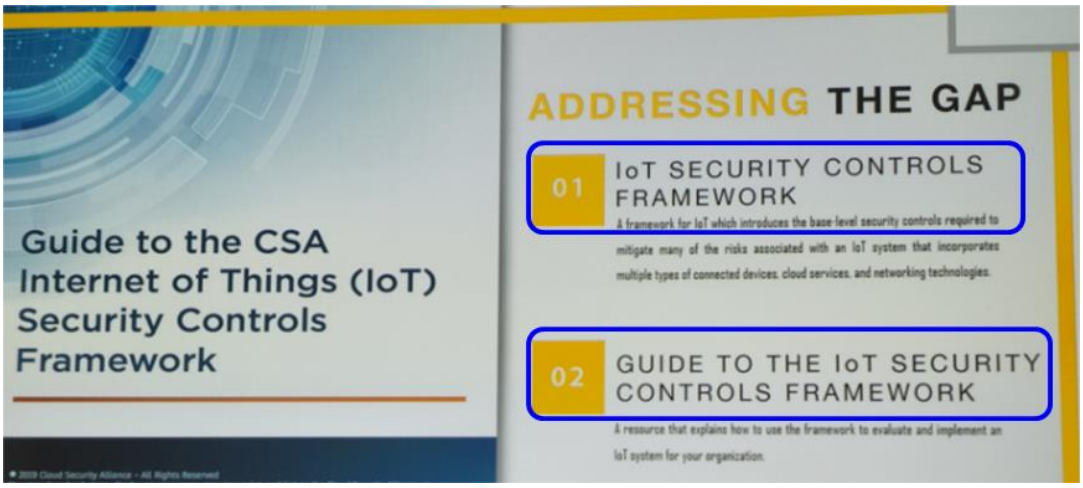
下表即是相關議題的一部分，惟某些場次因時間衝突而無法參加，難免有遺珠之憾，但個人仍覺頗有收穫不虛此行。

★ HTTPS: Is Privacy Making Us Less Secure? SPO1-T09 ★ Innovative Answers to the IoT Security Challenges SPO3-W10 ★ Internal Combustion: The Insider Threat to Industrial Control System... BC-W1ESE ★ Internet of Food: How IoT Threatens Fields, Farms and Factories SBX1-W1 ★ Lessons Learned from the IT/IoT/OT Device Explosion (formerly Breach ... BC-T8N	★ Edge Computing: New Hope against Insider Threat? (Nuix) BC-T9S ★ Engineering Trust and Security in the Cloud Era, Based on Early Lessons KEY-F03S ★ Finding the Right Answers—Facilitating Insider Threat Analysis ... GRC-T08 ★ Get Your Head Out of the Cloud. Zero-Trust Access for Hybrid IT (Pul... BC-T3S ★ Hearing Voices: The Cybersecurity Pro's View of the Profession AST2-W02

RSA Conference 相關活動主題摘述：

1. 物聯網(IoT)的安全控制框架

此項討論議題，講者探討許多**聯網裝置**、**雲端服務**以及**網路技術**的應用與風險，並闡述一個組織如何面對及降低前述三個領域串聯在一起的物聯網系統資安風險，最後並提供二份由 CSA 公布的文件供與會者參考：「物聯網設備安全控制框架」(IoT Security Controls Framework)、及「物聯網設備安全控制框架指引(Guide To The IoT Security Controls Framework)」，說明物聯網系統風險的基本控制需求，以及如何利用該框架為組織評估及實施物聯網系統。

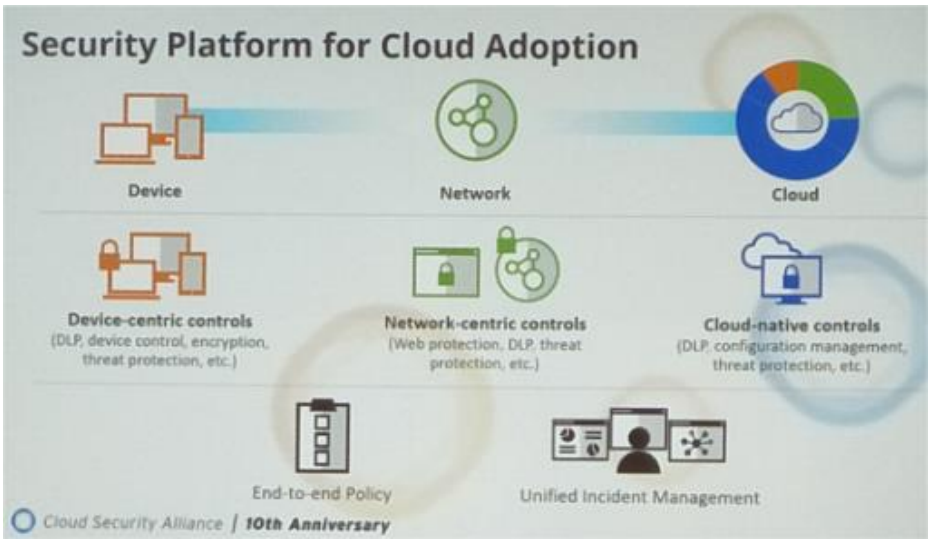


在該議題演講過程，講者提出其蒐集研究的數據，值得我們未來規劃聯網裝置、雲端服務及網路技術結合應用時，妥善考慮與採取相關資安防護控制措施，下圖即是物

聯網系統的安全平台架構設計概念。

(1)百分之 87 的企業允許員工使用非控管的裝置存取公司業務 APP。

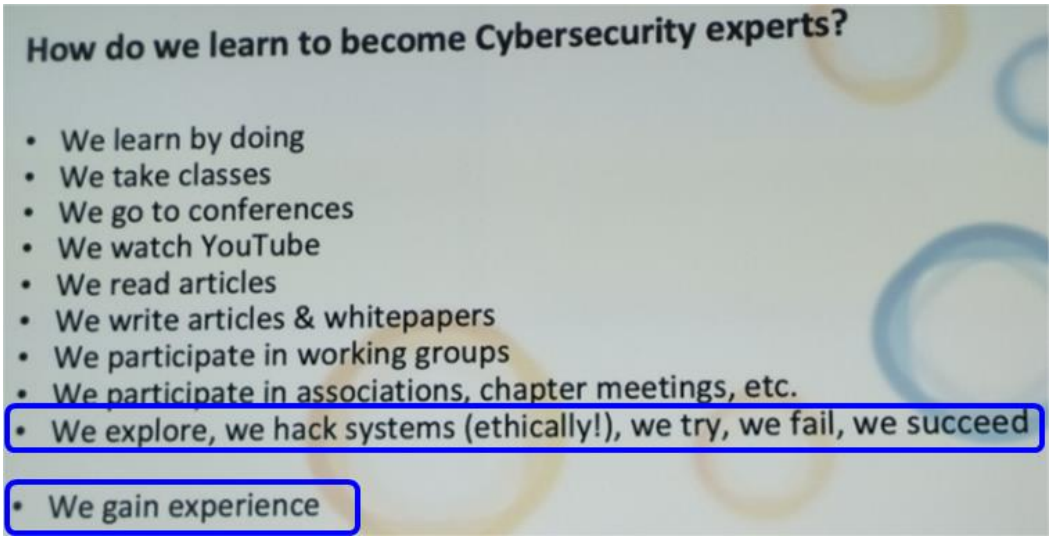
(2)存放敏感性資料的雲端服務，雖然百分之 62 受到適當的權限控管存取，但仍存在百分之 38 的資料洩漏風險-百分之 14 是透過私人的電子郵件帳號存取、百分之 12 提供網址連結提供任何人隨意取得資料檔案、另外百分之 12 則是內部人員或其他方式的資料洩漏。



2.如何成為資安攻防專家

成為一個資安專家的方法與過程，必須利用許多途徑學習與累積，例如做中學、參加研討會、閱讀相關文件、

參加工作群組等等，其中最重要的方法就是試煉場域累積實戰與經驗（參下表）。

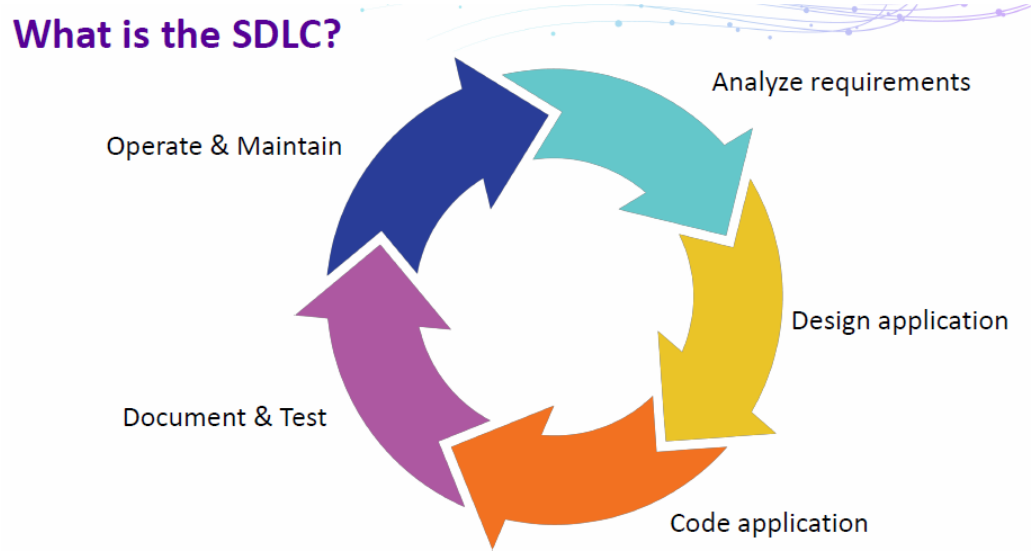


3.Dev[Sec]Ops（Developer/Security/Operations）(軟體開發者/安全/維運)

這是「軟體開發人員(Dev)」和「IT 運維技術人員(Ops)」從開發階段就將安全集成加入應用的完整生命周期的應用程式開發概念。將安全(Security)加入「DevOps 方法論」，將使開發人員和維運人員擁有更多的安全責任和活動，亦即在應用程式需求階段必須進行安全評估，讓應用系統開發人員利用工具加速開發流程的同時，也提升重視企業安全的資安意識，滿足程序化結構與自動化，並擴展 IT 的安全性。

下圖即是透過應用系統開發的正規化程序，在設計階

段即將安全風險納入考量，強化 IT 的安全性。



(二)美國 NIST 意見交流及關鍵基礎設施機構 SCADA 參訪活動

1.美國「國家標準技術研究所」(National Institute of Standards and Technology, NIST)意見交流

假美國舊金安商業服務大樓(U.S. Commercial Service San Francisco)召開 NIST 人員與我方訪人員面對面的意見交流，NIST 電腦安全部門、資訊技術實驗室的出席人員首先摘要說明該組織業務執行的方式，並回應我方參訪人員提出的諮詢意見。

框內為 NIST 與談人員

2.舊金山「太平洋氣電公司」(Pacific Gas and Electric Company，PG&E)

PG&E 公司負責舊金山地區天然氣與電力供應，是美國加州三大電力公司中規模最大的公司，其服務範圍北起 Eureka，南至貝克斯菲爾德 Bakersfield，西起太平洋岸，東至內華達山脈，在加州電業自由化過程售出大部分的發電廠，僅保留 6.8GW 的發電容量，目前的營業項目以輸配電與售電為主。

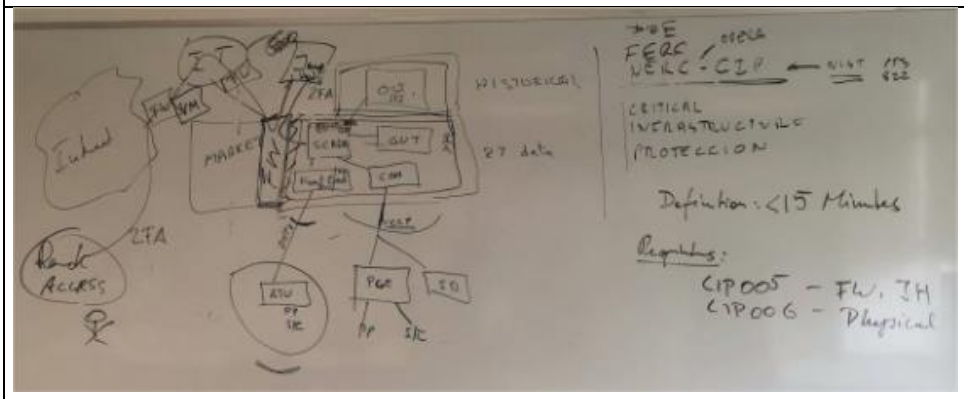
PG&E 特別由擔任 Chief of information security officer 的 Joe Sagona 參與討論，其中討論到資安標準的導入時表示他們係採用 SANS 標準，並使用 Brinqa 工具進行資安風險管理與分析(Cybersecurity Risk Management and Analytics)，當然意見交流過程中亦論及 OT 環境中對於工業控制系統的防護作為，相關心得將於具體成效章節說明。

3.「加州電力調度中心」(California Independent System Operator, CAISO)

CAISO 為北美九個獨立系統調度機構/區域輸電組織(ISO/RTO)之一，是負責營運加州約 80%(近 3000 萬人口)與部分內華達州地區的電力市場調度與電網可靠度管理之非營利公共組織，擔任發電市場、電力調度中心、排程協

調者的角色。

本次關鍵基礎設施 SCADA 參訪活動，就屬 CAISO 實地參訪的互動交流最為熱烈，CAISO 推派安全架構及品質模型管理主任(Director)、IT 基礎設施工程和網路維運主任、以及資訊安全經理、公關主任等四人與我們共同討論。



參、具體成效

一、 RSA Conference 2019 資安展活動

這次 RSA Conference 的議題探討及廠商攤位展示的內容，反應出今年大會主題「BETTER」對期許資訊安全領域不斷提升改善的願景。在會展現場亦可感受出資安廠商努力於提升現有的網路安全使用環境，不斷地研析如何防範網路攻擊以提供穩定的安全防護機制，試圖保護我們在數位時代的生產活動與生活方式的努力。在資訊軟、硬體上應用與管理上，結合了安全性、自動化的分析技術，全面覆蓋雲端服務、網路技術、行動裝置、工業控制系統等資安新興領域的應用，以防止機敏的資料洩漏與惡意的網路攻擊，有效幫助企業各項業務和營運活動的安全。而會議專家學者的研究與經驗分享中，亦可發現對於當前物聯網設備、雲端服務、工業控制系統的資安防護議題著力甚深。

此次參訪 RSA Conference 的心得，可以深刻瞭解在全球各地的資安威脅無所不在，所以資安攻擊已經不再是假設性的議題，資安防護更是刻不容緩的行動，所以願以下列二句話呈現心中的感受：

資安攻擊：是【When】不是【If】

資安防護：是【Ready】不是【Prepare】

二、 美國 NIST 意見交流及關鍵基礎設施機構 SCADA 參訪活動

(一) 美國「國家標準技術研究所」(National Institute of Standards and Technology, NIST)意見交流

1. NIST 在美國扮演的角色是偕同領域專家訂定標準，然後提供政府機關參考遵循、或是由政府機關主動提出請其研訂標準規範，且只負責標準的擬訂，並不涉及產品與標準符合度的驗證。

2. 業界或委外契約商導入的深度，則視政府管理機關的要求而定，有可能只須符合標準或規範的一部分。

3. NCC 詢及網路 BGP Hijacking 相關防護的指引或實作建議的相關資料需求，NIST 表示將攜回討論再回覆。

4. 資策會詢問有關建置試煉場域議題，NIST 則表示試煉場域的設置與維運牽涉規模的大小、且應考慮與時俱進與設施維護等問題，是很複雜的議題，並不容易。

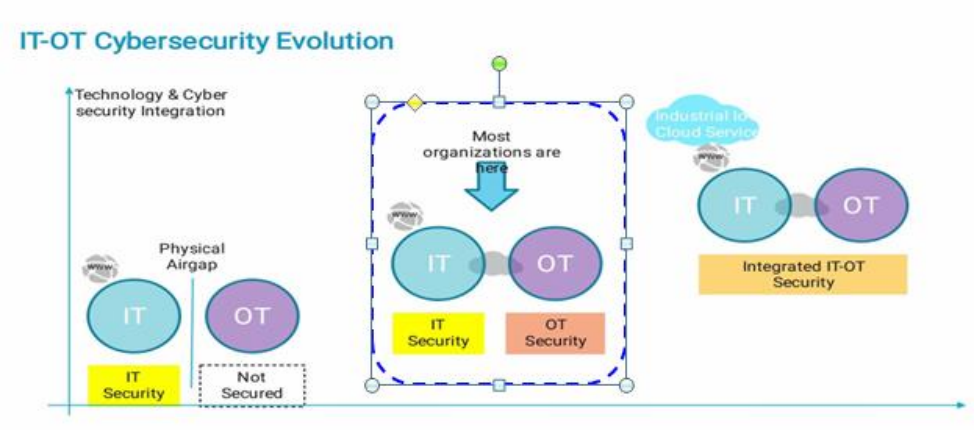
5. 最後也針對資訊系統的風險管理、安全控制以及工業控制系統(ICS)安全指引，建議可參考 NIST 編訂的 NIST 800-37、NIST 800-53、NIST 800-82 等三份標準文件。

(二) 舊金山「太平洋氣電公司」(Pacific Gas and Electric Company，PG&E)

1. PG&E 在 IT 與 OT 的資安防護營運中，係屬於分設 IT 防火牆及工控防火牆的防護模式，Data side 及 Operation side 獨立採取安全管控措施。

2. OT 環境中的 Level_2 及 Level_3 之間，評估其重要性再決定設置防火牆與否。

3. 「人」這因子是資安防護最弱的一環，且資安防護落實與否需要高級主管的支持。

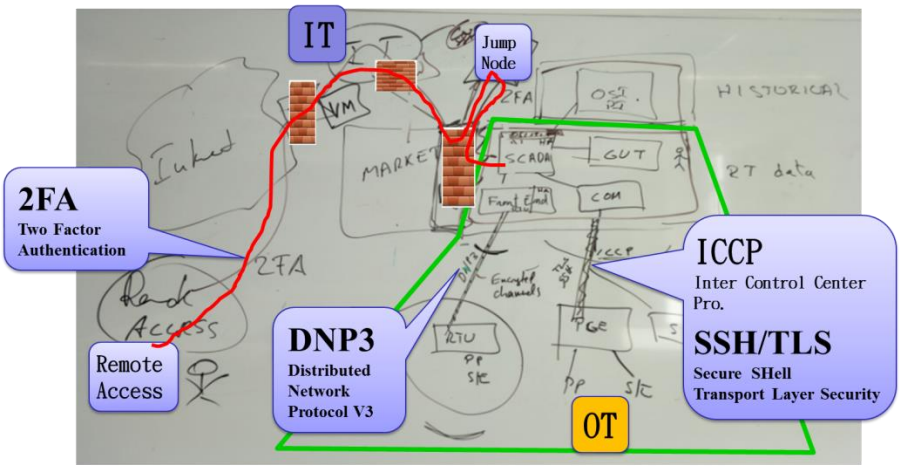


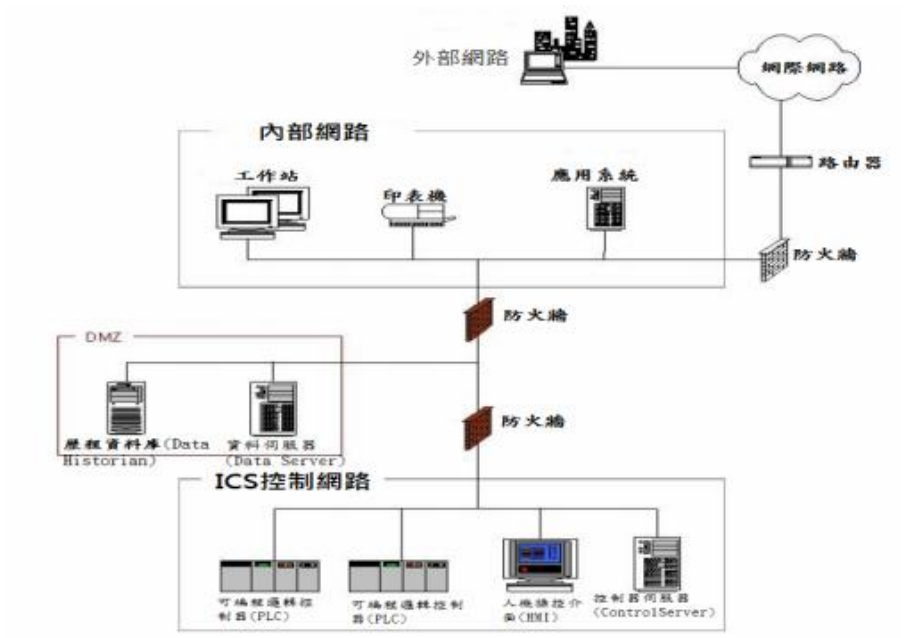
(三)「加州電力調度中心」(California Independent System Operator, CAISO)

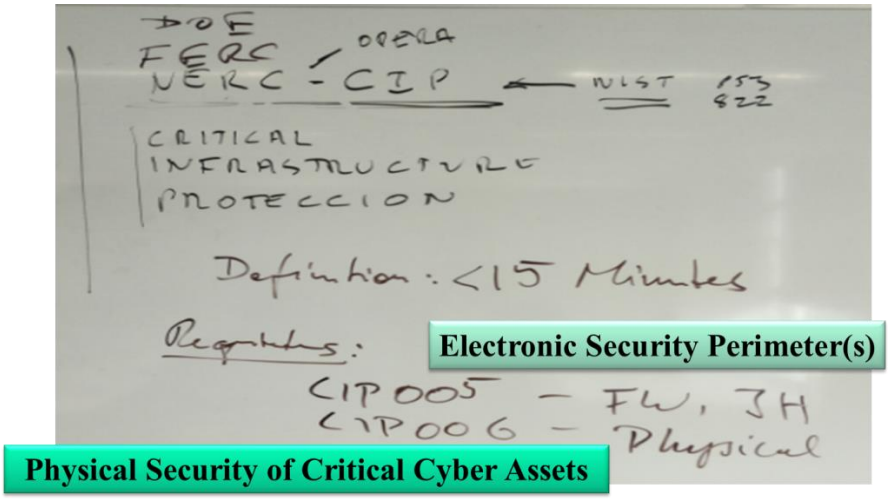
1. 企業內部 IT 與 OT 環境之維運與管理，主要由二個部門分別負責規劃與營運。亦即一個部門負責 IT/OT 資安防護技術及相關政策的研訂，另一個部門則依據其前者制定的資安防護與政策要求，統籌負責 IT 與 OT 二系統環境之執行與管理，此點與大部分將 IT 與 OT 系統交付不同部門負責的營運模式不同，或許這也是資安防護的另一種思維。

2. 參考 CIP(Critical Infrastructure Protection) 005、CIP 006、NIST SP800-153 的標準，並採用 NIST SP800-82 建議的高安全防護工業控制系統網路架構(詳下圖)，以建立防護縱深降低資安入侵風險。目前本公司對於關鍵資訊基礎設施規劃的防護要求，亦是朝此高安全防護架構設

計。


IT
Jump Node
VM
2FA
Two Factor Authentication
Remote Access
2FA
DNP3
Distributed Network Protocol V3
ICCP
Inter Control Center Pro.
SSH/TLS
Secure SHell Transport Layer Security
OT


外部網路
網際網路
內部網路
工作站
印表機
應用系統
路由器
防火牆
防火牆
DMZ
歷程資料庫(Data Historian)
資料伺服器(Data Server)
防火牆
ICS控制網路
可編程邏輯控制器(PLC)
可編程邏輯控制器(PLC)
人機接口介面(HMI)
控制器伺服器(ControlServer)


DOE
FERC / OPERA
NERC - CIP
NIST
CRITICAL
INFRASTRUCTURE
PROTECCION
Definition: <15 Minutes
Electronic Security Perimeter(s)
CIP005 - FW, IH
CIP006 - Physical
Physical Security of Critical Cyber Assets

肆、心得及建議

今年是我國資通安全管理法及其子法實施的元年，又適逢物聯網、雲端服務正蓄勢待發，國家關鍵基礎設施資安防護的概念亦如火如荼的展開，有幸奉派參加以【BETTER】為主題的 RSA Conference 資安大會，以及參訪瞭解美國關鍵基礎設施工業控制系統的資安防護實務作為，分享以下五點心得與建議：

（一）資安攻擊是『When』不是『If』、資安防護是『Ready』不是『Prepare』。

（二）國內外企業在資安防護實務上，面臨同樣的問題：『人』是資安防線上最弱的一環。

（三）國內關鍵基礎設施的資安防護規劃相較於歐美國家(以美國舊金山 CAISO 為例)，顯然起步稍微落後，但急起直追為時未晚。

（四）鼓勵同仁積極參加類似 RSA 或 ICS 的國際會議：

除可汲取各國資安專家的研究與分享、瞭解層出不窮的資安威脅，同時亦可開展資安防護的視野與觀念。

（五）資安防護縱深必須『落實管理』並『持續改善』：

資安防護技術、設備引進容易，但是落實管理才能發揮資安

縱深防護的設計能量，持續改善才能防護外界推陳出新的資安攻擊手法。