財團法人電信技術中心出國報告

國際自動化學會(ISA)舉辦之 IEC62443 標準交流活動

單位名稱：檢測暨網通技術組
姓名職稱：董勁吾 工程師
黃俊貴 副工程師

派赴國家：美國

出國期間：108/05/05-108/05/12

報告日期：108/05/31

摘要

早在 1990 年代，隨著網路技術發展，工業自動化設備已有聯網功能。早期聯網技術著重資料互通性，期降低系統整合成本；然此舉亦衍生資安隱憂，需要發展一套管理辦法降低資安風險，ISA/IEC 62443 工業自動化資訊安全標準因應而生。

本次出國參與 ISA/IEC 62443 交流活動，主辦單位國際自動化協會(International Society of Automation, ISA) ，其所下轄的 ISA99 委員會即發展 ISA/IEC 62443 的主要組織，於工業自動化資訊安全領域，可謂權威。

本次活動，除帶回主辦方分享之資訊外，團員亦準備以再生能源資訊安全的題材與主講之專家交流討論，相關議題如下：

一、IEC 62443 簡介與發展狀況。

二、IEC 62443 應用範疇與適用章節。

三、IEC 62443 於再生能源資訊安全領域之運用。

目錄

壹、 目的……3

貳、 行程……4

參、 會議過程及內容……6

1. IEC 62443 簡介與發展近況 ……6

2. IEC 62443 應用範疇與適用章節 ……7

3. IEC 62443 於再生能源資訊安全領域之運用……10

肆、 心得及建議 ……14

伍、 附件：相關照片及資料 ……15

壹、 目的

本中心承辦標檢局「108 年度再生能源監測與資訊安全標準檢測驗證委辦計畫」中，派員參與國外 IEC 62443 標準研習活動或相關機構參訪，探討再生能源設備使用自動化工業控制系統(IACS)的可能存在資安問題與威脅，了解工業控制網路架構的參考模型，分層分析與防護機制。並研究如何對智慧變流器以 IP 網路、數據採集器(Data Logger)與監控系統(SCADA)進行資安檢測，藉以建立資安測試能量。

透過與國際專家交流，掌握先進國家於工業自動化資訊安全議題之脈動，帶回最新資訊並探討 IEC 62443 標準於再生能源資訊安全領域之應用。另一方面，考察蒐集 IEC 62443 標準發展狀與標準檢測驗證作業的運作狀況之資料，可為國內調合 CNS 標準方向之指引，亦可為國內廠商或產品未來取得 IEC 62443 合規報告或認證之參考，或有助於國內相關實驗室建立檢測能量。

同時與國際專家討論智慧變流器的資訊安全議題，含收集資安問題、發現資安弱點、資安風險評估與資安威脅等。具體希能掌握如何將 IEC 62443 中的網路安全規劃參考模型運用到本專案中，以因應智慧變流器潛存資安問題提出有效建議並開發資安需求規格，開發智慧變流器資安測試案例。

貳、 行程

本次參與之 IEC 62443 交流考察活動之出國期程為 108 年 5 月 5 日至 5 月 12 日，扣除差旅時間，實際參與活動之時間為 5 月 6 日到 5 月 10 日，活動官方名稱為「5 月休士頓資安營(Houston May Cyber Camp)」，活動地點於美國德州休士頓 AE Solution 公司之會議中心。活動的主辦單位 ISA 是一非營利性組織機構，致力於全球自動化科技領域之標準發展、專業認證，亦出版專業圖書與技術文章，並舉辦許多科技會議與展覽，並提供教育與訓練課程。其中 IEC 62443 工業自動化資訊安全標準的前身即由 ISA 下轄之 ISA99 委員會與國際電工委員會(International Electrotechnical Commission, IEC)下轄之 TC65 委員會共同發展，在 ANSI(American National Standards Institute)首次對外公開，在 ISA 發行的版本稱為 ISA-62443-x-y，IEC 發行的版本則稱為 IEC 62443-x-y。故由 ISA 舉辦之 IEC 62443 標準研討活動，具有足夠的公信力及影響力。

表 1、參訪行程

月	日	星期	訪問對象		工作內容	備註
			國家	機構或個人		
5	5	日	台灣		往程：台北-休士頓	
5	6	一	美國	國際自動化學會(ISA)/ aeSolution Inc.	參加 IEC 62443 標準交流研討活動。	
5	7	二	美國	國際自動化學會(ISA)/ aeSolution Inc.	參加 IEC 62443 標準交流研討活動。	
5	8	三	美國	國際自動化學會(ISA)/ aeSolution Inc.	參加 IEC 62443 標準交流研討活動。	
5	9	四	美國	國際自動化學會(ISA)/ aeSolution Inc.	參加 IEC 62443 標準交流研討活動。	
5	10	五	美國	國際自動化學會(ISA)/ aeSolution Inc.	參加 IEC 62443 標準交流研討活動。	
5	11	六	美國		返程：休士頓-台北	
5	12	日	台灣		返程：休士頓-台北	

活動的承辦單位 aeSolution 是一間位於休士頓的工程顧問公司，創立於 1998 年，擅長領域除工業自動化資訊安全外，還有提工業製程安全、安全儀控系統、自動化整合系統等諮詢服務。2014 年 ISA 與該公司在工業安全、工業資訊安全與警示管理等領域有簽訂授權合約，足見 aeSolution 在此類領域的專業。與會的人員有 John Cusimano、Marco Ayala 與 Krish Sridhar 先生。John Cusimano 先生是 IEC

62443 標準的投票委員之一，且是 ISA99 委員會中第四工作組(WG4)的主席，第四工作組乃發展 IEC 62443-3-2 的主要組織。Marco Ayala 與 Krish Sridhar 先生均來自 aeSolution Inc.工程顧問公司的工業資訊安全有關部門，兩位都是 ISA 認證的 IEC 62443 專家，而 Marco Ayala 更是協助 ISA 發展認部份證課程的課程規劃人之一。

表 2、與會人員

	姓名	單位	職稱
1	John Cusimano	ISA99 committee WG 4	Chairman
2	Marco Ayala	aeSolution Inc. (工程顧問公司)	ICS security Manager
3	Krish Sridhar	aeSolution Inc. (工程顧問公司)	ICS security Manager

表 3、議程

日期	時間	內容
5/6	08:00 ~ 16:00	1. 工業自動化資訊安全簡介-5 大迷思。 2. IEC/ISA 62443 標準發展概況。 3. 自動化系統之模型和安全區域劃分。 4. 討論。
5/7	08:00 ~ 16:00	1. IEC 62443 標準中資訊安全等級概念。 2. 工業型企業如何建立資訊安全管理計畫。 3. 討論。
5/8	08:00 ~ 16:00	1. 工業自動化系統面臨資訊安全問題。 2. 工業網路設備資產盤點工具介紹。 3. 已知威脅或漏洞之管理，未知威脅或漏洞的識別。技巧。 4. 討論。
5/9	08:00 ~ 16:00	1. 工業自動化系統資訊安全風險評估。 2. 工業自動化系統資安設計與安全生命週期概念。 3. 討論
5/10	08:00 ~ 12:00	1. 瞭解 IEC 62443 合規組織與 ISASecure®驗證程序。 2. 討論

參、 會議過程及內容

1. IEC 62443 簡介與發展近況

IEC 62443 工業自動化資訊安全標準是由許多子標準集合而成，其中-1-1~1-4 通論部分說明自動化工業控制系統的問題與威脅，透過風險管理的概念說明資訊安全的重要性，並提出工業控制網路架構的參考模型(Reference Model)，協助企業分層分析與提供防護機制建議。在-2-1~2-5 流程與政策部份，針對資產擁有者(Asset Owner)，也就是工廠的管理者，說明應該如何透過管理政策和流程規劃以確保生產運作的安全性。-3-1~3-3 系統部分是以系統整合商(System Integrator)的角度，說明透過需求討論、規劃設計、連線部署後的自動化運作工廠，從技術面如何確保這些整合後的自動化方案免於資安攻擊的威脅，探討內容包含執行安全評估等方式。最後-4-1~4-2 元件部分，則探討產品供應商(Product Supplier)的安全，定義與規範如何開發一個安全的產品。

由於資訊安全領域常有新的技術出現，與談專家 John Cusimano 更表示，許多標準才剛通過出版，就又進入檢討再版的程序。而 IEC 62443 標準也就難以保持穩態，除了部份子章節尚在發展當中，子章節也會變動，比如說 2019 年 2 月後，IEC 62443-2 系列從 4 個子節變成 5 個子節(IEC 62443-2-1~-2-5)。茲將迄今年 5 月為止，IEC/ISA 62443 最新的發展動態整理於圖 1 及表 4：

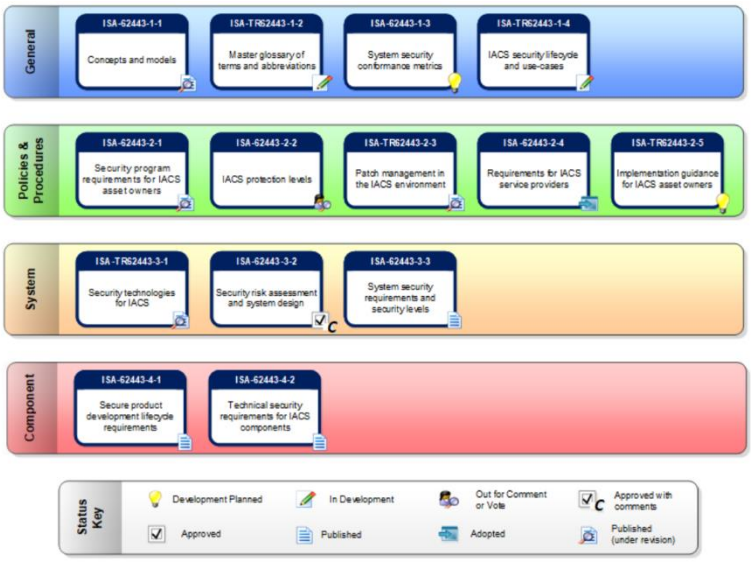

圖 1、IEC 62443 架構與發展現況
(資料來源：ISA)

表 4、IEC 62443 各子章節名稱與最新版本

章節編號	原名	譯名	最新版本
1-1	Terminology, concepts and models	術語、概念及模型	2009
1-2	Master glossary of terms and abbreviations	術語和縮寫詞彙表	草稿預審
1-3	System Security compliance metrics	系統安全合規性指標	預劃發展
1-4	IACS securing and use-cases	工業自動化控制系統保護與用例	發展中
2-1	Establishing an industrial automation and control system security program	建立工業自動化控制系統安全計劃	2010
2-2	IACS protection levels	工業自動化控制系統保護等級	草稿預審
2-3	Patch management in the IACS environment	工業自動化控制系統環境中的補丁管理	2015
2-4	Security program requirements for IACS service providers	工業自動化控制系統服務提供商的安全計劃要求	2015
2-5	Implementation guidance for an IACS security management system	工業自動化控制系統安全管理的實施指南	預劃發展
3-1	Security technologies for industrial automation and control systems	工業自動化控制系統的安全技術	2009
3-2	Security risk assessment and system design	安全風險評估和系統設計	委員會投票通過尚未正式出版
3-3	System security requirements and security levels	系統安全要求和安全級別	2013
4-1	Product development requirements	產品開發要求	2018
4-2	Technical security requirements for IACS components	工業自動化控制系統組件的技術安全要求	2019

2. IEC 62443 應用範疇與適用章節

由於 IEC 62443 標準之涵蓋範圍相當宏觀，且資訊安全的條件會因人、事、時、地、物、環境與技術等而所不同，要如何運用這些標準也成為一個難題。於交流活動時，與會專家說明應依照保護範疇的規模來對應適用的標準，保護範疇(如圖 2)分為：

(1) 資產擁有者(企業級管理面)：適用 IEC 62443-1-1、-2-1、-3-2、-3-3

(2) 系統整合者(工廠級管理面)：適用 IEC 62443-2-4、-3-2、-3-3

(3) 系統整合方案(產品面)：適用 IEC 62443-4-1、-3-3

(4)　設備(產品面)：適用 IEC 62443-4-1、-4-2

(5)　設備供應商：適用 IEC 62443-4-1

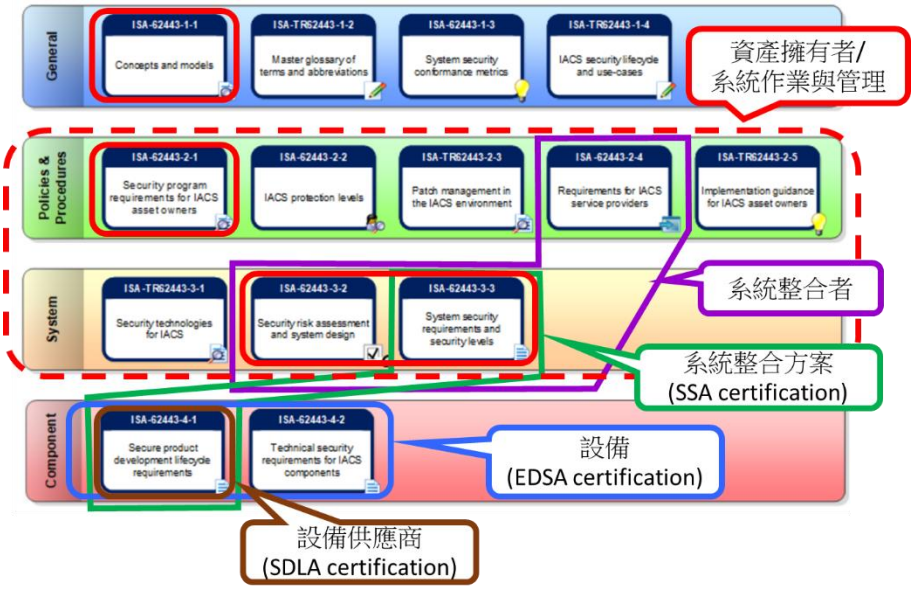

圖 2、IEC 62443 應用範疇
(資料來源：ISA、電信技術中心整理註解)

上述範疇中的第(1)、(2)項管理面，尚無核發驗證的機制，企業主及系統管理人可洽第三方工業自動化資安顧問公司，除獲得專業諮詢以提升資安等級外，可由第三方出具評估報告，證明企業為資安所做的努力。圖 3 顯示資產擁有者該如何利用 IEC 62443 來建立資安管理計畫：

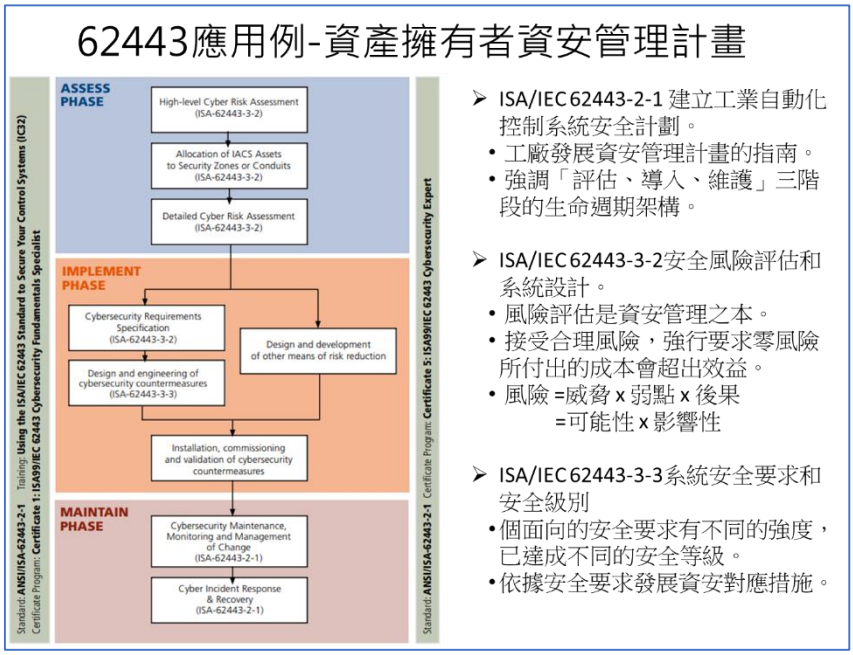

圖 3、資產擁有者該如何利用 IEC 62443 來建立資安管理計畫
(資料來源：ISA/aeSolution Inc.、電信技術中心加註解/整理)

IEC 62443 的標準屬質化的要求，較難採用制式且量化的方式執行檢測驗證，為此，ISA 設立了 ISA 安全合規機構 (ISA Security Compliance Institute, ISCI)管理一個名為 ISASecure®的認證程序，提供三個面相的認證方案與指南：嵌入式裝置安全保障(Embedded Device Security Assurance, EDSA)、系統安全保障(System Security Assurance, SSA)與開發生命周期安全保障(Security Development Lifecycle Assurance, SDLA)。其內含整理於表 5：

表 5、ISASecure®認證方案

認證方案	認證對象	內涵	主要安全規範
EDSA	設備	確認產品可抵抗網路攻擊的強健度，並確認產品未存在已知的資安漏洞。	IEC 62443-4-1 IEC 62443-4-2 Communication Robustness Test Vulnerability Identification Test
SSA	系統	確認一個工業控制系統或一子系統可抵抗網路攻擊的強健度，且未存在已知的資安漏洞。	IEC 62443-3-3 IEC 62443-4-1 IEC 62443-4-2 Communication Robustness Test Vulnerability Identification Test
SDLA	供應商	確認供應商對產品開發環境、生產程序及生命周期的安全設計。	IEC 62443-4-1

(資料來源：ISASecure®、電信技術中心整理)

Recognized CRT Test Tools

CRT Tool Supplier	Tool Name and Version *(See certificates for complete details)*	Recognition Date and Certificate Link	Recognized for EDSA 2.0.0, EDSA 2.1.0, and EDSA 3.0.0	Recognized for SSA 2.0.0, SSA 2.1.0, and SSA 3.0.0
Synopsys	Defensics *(see certificate for version numbers)*	8/31/17	Yes	Yes
Hitachi Systems	Raven ES 2.0.0.0	10/04/17	Yes	-
Beyond Security	beSTORM EDSA 6.1.1 build 6584	3/21/16	Yes	Yes
Wurldtech	Achilles Test Platform r2 3.16.1 Build 3.16.20151217193830	2/7/18	Yes	Yes
Wurldtech	Achilles Test Platform r3 3.16.1 Build 3.16.20151217193830	2/7/18	Yes	Yes
CNCERT/CC & Beijing Xinlian Kehui Technology Co., LTD	Acheron 2.2	2/22/17	Yes	Yes
Beijing Winicssec Technologies Co. Ltd.	VHunter IVM (Industrial Control Vulnerability Mining System) V3.0	1/25/19	Yes	-

Vulnerability Identification Testing Tool

Supplier Name	VIT Tool Name
Tenable	Nessus Vulnerability Scanner

圖 4、ISASecure® 認可之資安檢測工具
(資料來源：ISASecure®)

表 5 中的通訊強健測試(Communication Robustness Test, CRT) 與漏洞視別測試(Vulnerability Identification Test, VIT) 係要求產品要經過資安檢測工具的測試，而ISASecure®也公佈了合規的檢測工具清單，如圖 5 所示。目前通過 ISASecure® EDSA 驗證的產品，均公佈於 ISASecure®的網頁上。通過產品驗證的製造商如ABB、Hitachi、Honeywell、Shineider 等 10 間國際公司，驗證的產品為分散式系統控制器、場域設備控制器、管理器等 34 項。於 2011 年到 2016 年間，每年約 2~4 項產品通過認證，至 2017 年有 6 項產品通過認證，2018 年更增加到 14 項。可見IEC 62443 驗證需求，已越來越受到產業的重視。

ISASecure Certified Devices

Picture	Supplier	Type	Model	Version	Level	Certification Date
	Emerson Automation Solutions	System	DeltaV DCS and SIS	14.3	SSA 2.0.0 Level 1	3/7/2019
	Schneider Electric	Field Device Controller	Field Device Controller FDC280	S901032000 and 0901003000	EDSA 2.0.0 Level 1	12/21/2018
	Honeywell Process Solutions	Safety Manager	Safety Manager Control Processor with Quad Processor Pack QPP-0002 and Universal Safety Interface USI-0001	R162.1	EDSA 2.0.0 Level 1	12/20/2018
	Honeywell Process Solutions	Unit Operations Controller	ControlEdge UOC	R510	EDSA 2.0.0 Level 2	12/17/2018
	Schneider Electric	Safety Related Programmable Electronic System	TRICONEX Communication Module TCM	4351 A/AC/AC1, 4351 B/BC/BC1, 4352 A/AC/AC1, 4352 B/BC/BC1 - (Firmware Revision 6430 Build 344)	EDSA 2.0.0 Level 1	12/10/2018
	Honeywell Process Solutions	DCS Controller	Experion C300 with CF9	R510	EDSA 2.0.0 Level 1	11/2/2018
	Honeywell Process Solutions	Wireless Device Manager	WDMY	R320	EDSA 2.0.0 Level 1	11/2/2018
	Honeywell Process Solutions	DCS Controller	Experion C300 with CF9	R501	EDSA 2.0.0 Level 1	10/1/2018

圖 5、ISASecure® EDSA 驗證產品清單截圖
(資料來源：ISASecure®)

3. IEC 62443 於再生能源資訊安全領域之運用

除了帶回 IEC 62443 相關資訊外，我們參加交流活動的主要目的之一，即與國際專家討論如何將 IEC 62443 應用於再生能源資訊安全的議題上。實則在許多再生能源資訊安全相關的研究報告中，均有將 IEC 62443 標準納入考量，如美國Sandia National Laboratiories 實驗室的太陽能資安報告中，即把分散式能源控制系統視為工業自動化系統的一部份，如下圖 6。

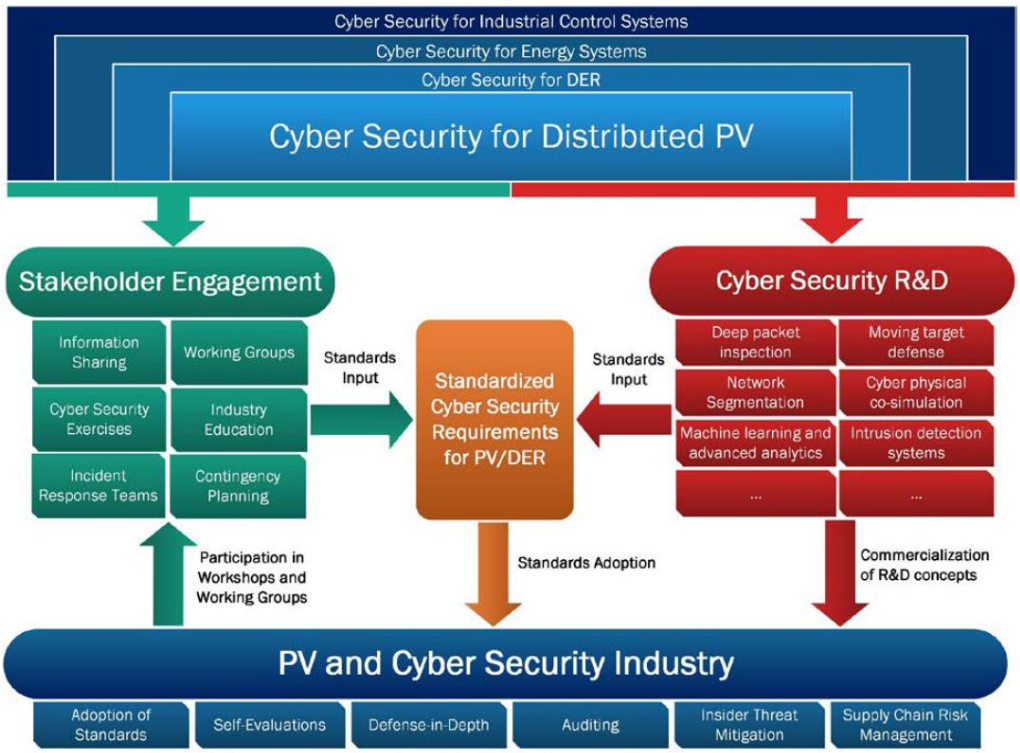

圖 6、太陽能系統資訊安全發展關係圖

(資料來源：Lai, Christine, et al. "Cyber security primer for DER vendors, aggregators, and grid operators."*Sandia National Laboratories, Albuquerque, NM*(2017).)

依 IEC 62443 的原則，要評估並規劃一個系統資訊安全計畫，起手式是盤點系統中的裝置，並繪製系統網路圖。IEC 62443 建議的系統網路圖參考模型，將網路分為 0~4 層，如圖 7 所示：

(1) 第四層：經營管理相關設備

(2) 第三層：工廠生產作業設備(排程系統)

(3) 第二層：監控流程設備(SCADA)

(4) 第一層：實際操作設備(PLC)

(5) 第零層：最前端的感知設備(感知器)

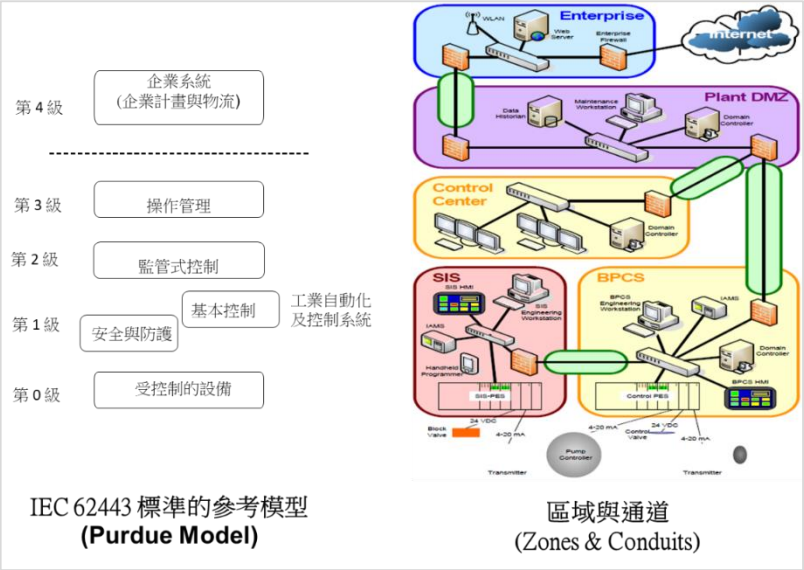

圖 7、IEC 62443 參考模型與例子
(資料來源：ISA)

系統圖繪製後將裝置劃分餘個區域，原則上同一區域要有相同的安全防護等級；區域和區域之間資料會透過「通道」傳輸；通道也要賦予安全防護等級。完成劃分後，可參考 IEC 62443-3-3，該子標準中有對各種安全等級應採取的保護手段有做定義，可為提升資安防護具體措施的參考。美國 Sandia National Laboratiories 實驗室的太陽能資安報告中，也依 IEC 62443 參考模型所繪製的再生能源監控的網路系統架構圖，如圖 8。據此和與談的專家 Krish Sridhar 先生討論。對於此系統構構圖的不同區域，得到適合的參標準建議，亦整理於圖 8。

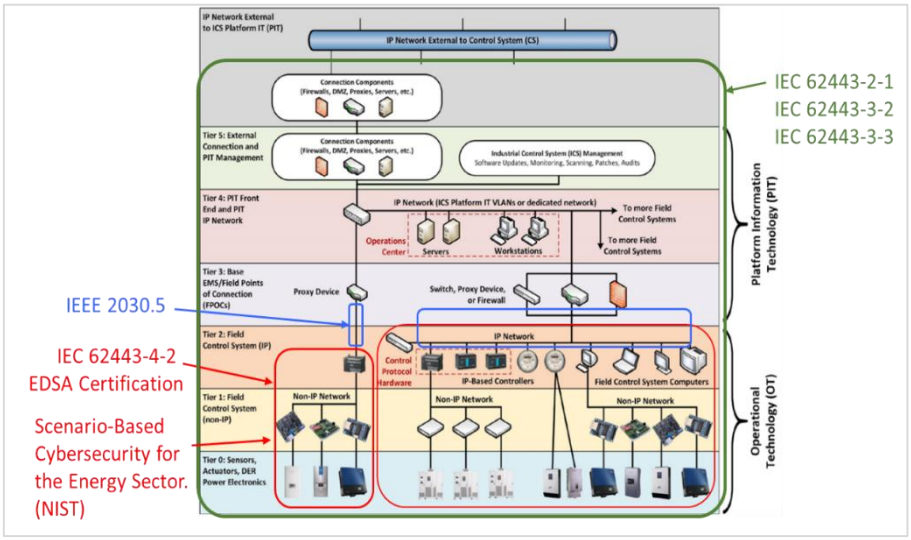

圖 8：再生能源監控系統網路架構圖及參考資安標準。
(資料來源：Lai, Christine, et al. "Cyber security primer for DER vendors, aggregators, and grid operators."*Sandia National Laboratories, Albuquerque, NM*(2017)./電信技術中心加註整理)

有關再生能源設備(智慧變流器及相關監控設備)的資安檢測，可參考ISASecure® 的 EDSA 驗證，驗證架構圖如圖 9。EDSA 當中包含了 SDA-E、FSA-E 與 ERT 三個檢查、測試主軸。SDA (Security Development Lifecycle Assessment)旨在評估設備生產時，製造商導入了哪些產品安全開發程序。面向涵蓋：安全管理、全需求識別、安全設計、安全實作、安全規格與有效性驗證、安全缺陷管理、安全升級管理與安全指南，而 FSA(Functional security assessment for components)則考量設備於系統中的安全功能需求，測試設備的安全能力。面向涵蓋：、存取控制、使用控制、資料完整性、資料機敏性、資料流限制、事件回應及資源可用性等。SDA 與 FSA 的並非透過檢測工具進行查核，多半以實品外觀功能檢查輔以文件審查為主，而 ERT(Embeddeddevice robustness test)則要求產品要經過資安檢測工具的測試，即本文表 5「主要安全規範」項目中的通訊強健測試(Communication Robustness Test, CRT) 與漏洞視別測試(Vulnerability Identification Test, VIT) ，合規的檢測工具清單則如本文圖 4 所示。

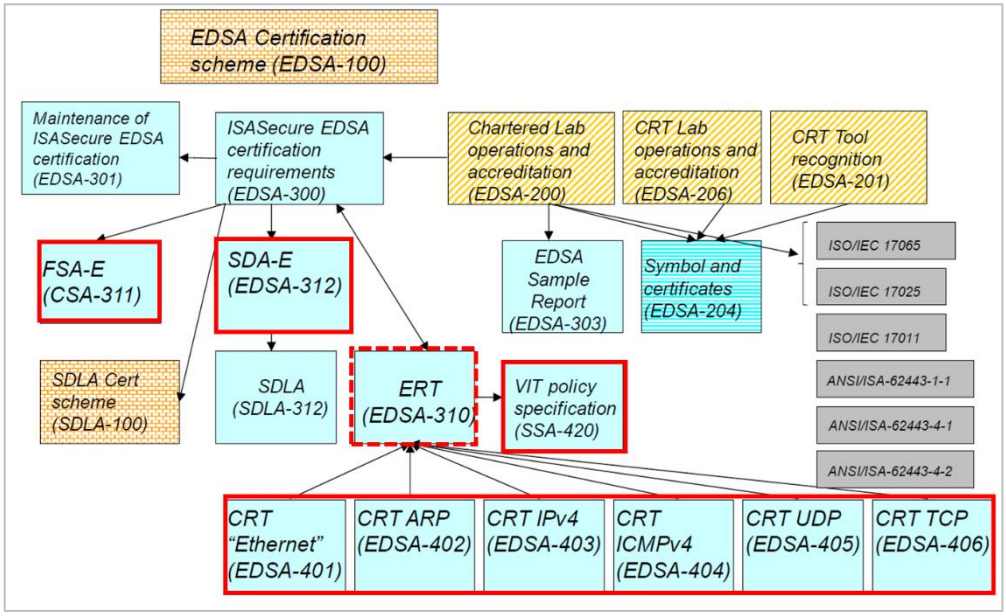

圖 9、ISASecure® EDSA 驗證架構圖
(資料來源：ISA)

在討論中，Krish Sridhar 先生也分析我們的再生能源監控架構其實所連接的網路裝置並不多，就直接將資料上傳雲端了，這類系統屬工業物聯網架構(IIoT)，ISA99 委員會 WG9 TG7 已開始對 IIoT 的議題進行討論，建議我們可持續注意 IEC 62443 於工業物聯網(IIoT)資訊安全應用方面的資訊。

肆、 心得及建議

乍聽資訊安全，給我們的第一印象，是需要瞭解一堆程式編碼與駭客技術；然則資訊安全管理其實是一套風險管理的程序。落實 IEC 62443 工業自動化資訊安全管理標準，透過標準內指導的「評估、導入、維護」資安管理程序，則不論資安環境和駭客技術如何演變，都可確保系統有一定的安全等級。

另外，通資產業的資訊安全，通常重視資料的機密性，優於資料的完整性及可用性；然而，工業自動化系統的資訊安全，首重資料的可用性。比如說，以通資產業而言，登入某網路帳戶，可能超過三次密碼錯誤就被鎖住，以保用戶資料機密；而在工業自動化場域中，若因登入失敗鎖住帳號而不能操作某一工具機，可能會造成產線停滯，帶來財損，甚至危及物安、人安。故國內雖已有 CNS 27000 系列的資訊安全國家標準，仍建議有關相局可研析 IEC 62443 標準，以調合為更適用於工業自動化領域的資訊安全標準。

經由本次參與 ISA 舉辦之 IEC 62443 交流活動，得知 IEC 62443 標準發展歷程及最新資訊，並明白標準的應用目標範籌。對於再生能源資訊安議提，目前國際間尚無明確通用之標準，和與會之專家討論後，均認為 IEC 62443 可應用於再生能源資訊安全領域。而再生能源設備的資安檢測可參考 ISA Secure® 的 EDSA 認證程序；惟目前獲得 EDSA 認證之產品多屬工業控制器，所處環境需連接複雜網路及多個工具機，且有人員頻繁操作等因素；而再生能源設備通常經過較少網路設備即連上雲端，為工業物聯網(IIOT)架構，宜依實際狀況制定檢測標準。

伍、 附件

1. 交流剪影

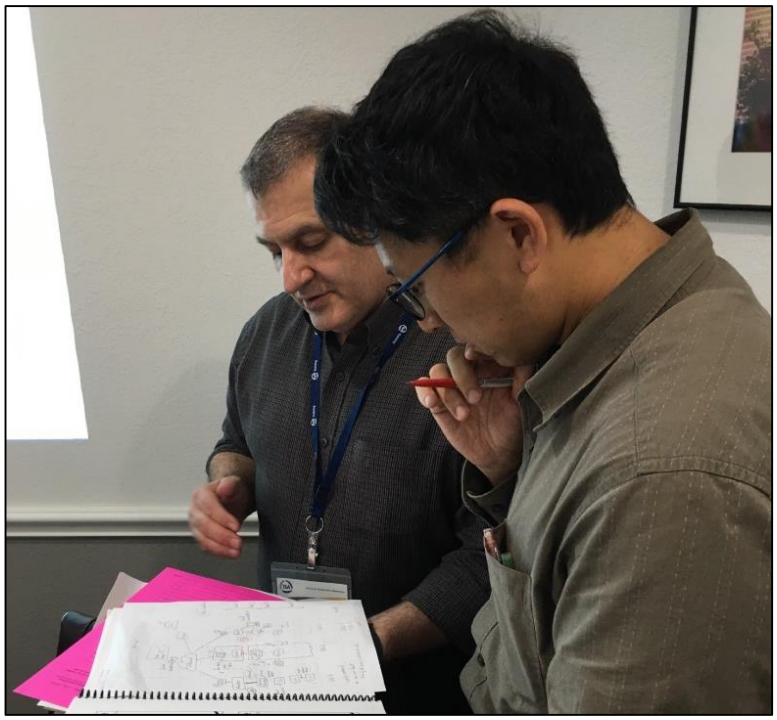

圖 10、團員董勁吾和 John Cusimano 就再生能源監控系統架構進行討論。

圖 11、團員董勁吾和與談人 Marco Ayala 及其他與會人員交流討論。

圖 12、團員黃俊貴和與談人 John Cusimano 合影

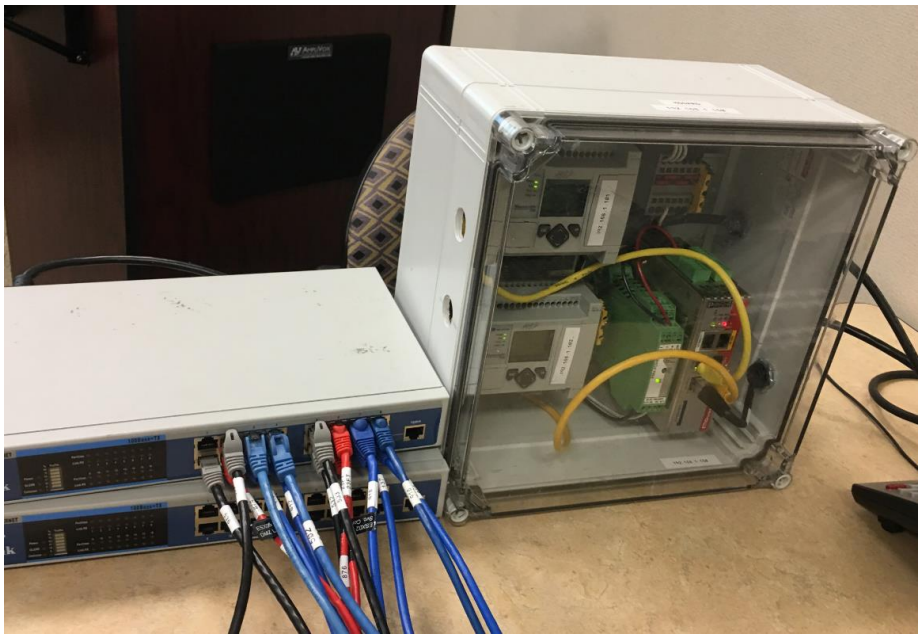

圖 13、與談人 Krish Sridhar 建構微型工業網路並以之交流資安測試技術

2. 受訪單位提供之資料

(1) IEC/ISA 62443-1-1 (紙本)

(2) IEC/ISA 62443-2-1 (紙本)

(3) IEC/ISA 62443-3-3 (紙本)