從 IEC 62443 看儀器應具備的資訊安全功能

The Cybersecurity Functions that an Instrument Should Possess from the Perspective of IEC 62443

李維楨
Wei-Chen Lee

製造業目前已是受到最多資安攻擊的產業的首位，在製造業中，各式的儀器、不同的老舊通訊協定及欠缺的資安人才導致許多資安漏洞的生成，如何客觀地評估儀器應該具有的資訊安全特性成為一重要議題。本論文目的即為使用國際認可並適用於工控環境中的資安標準 IEC 62443-4-2 來探討儀器應具有的資訊安全特性，論文中我們將 IEC 62443-4-2 的 7 項基本要求應用在儀器上以分別來探討在這 7 項基本要求下的細部規範。

Manufacturing is currently the most attacked industry. In the manufacturing industry, various instruments, different legacy communication protocols, and a lack of OT cybersecurity expert have generated many vulnerabilities. How to objectively assess the cybersecurity attributes that instruments should have became an essential issue. This paper aims to use the internationally recognized OT cybersecurity standard IEC 62443-4-2 to discuss the cybersecurity attributes that instruments should have. Requirements are applied to instruments to discuss the detailed specifications under these seven fundamental requirements in IEC 62443-4-2.

一、IEC 62443 簡介

近年來，工業自動化及控制系統 (industrial automation and control system, IACS, 以下簡稱工控) 環境中的資安事件日益增加，例如在 2021 年 5 月，美國最大的油管公司 Colonial Pipeline 遭受到勒索軟體的攻擊導致其系統關閉了 5 天，造成美國東岸部份區域燃料的缺乏，對民生產生了很大的衝擊，最終並支付給駭客贖金才得以將系統重啟[(1)]。在國內也有類似情形，已知的包括了一些大型的製造業者也都遭受過惡意的攻擊，導致了巨大的損失。過去在資安攻擊的目標上，製造業並非是太受青睞的的目標，根據 IBM 的報告[(2)] 顯示，製造業在 2021 年已成為受到最多資安攻擊排行榜的第一名，超過了金融和保險業。如果回溯去

看，在 2019 年製造業只能排在受到最多資安攻擊排行榜的第八名，其上升速度之快令人訝異。然而，為什麼駭客喜歡攻擊製造業呢？其原因很多，其中包括了生產線上的各子系統複雜且部份子系統老舊、機臺間使用許多通訊格式、部份通訊格式無安全機制 (如可程式邏輯控制器 PLC 常使用的 Modbus 通訊) 及缺乏工控領域的資訊安全人才等，這樣的情況給工廠的資訊安全帶來了很大的風險。而這些資安的威脅並不全然來自外部，也有來自內部的資安威脅[3]，使得基本的資安防護設備如防火牆等也無法防範這些來自內部的功擊。因此，在工業物聯網 (industrial internet of things, IIoT) 的趨勢下，現今製造業中使用的儀器，自身也要具備適當的資訊安全防護功能，以抵抗來自外部及內部的攻擊。由於儀器經常使用於工控環境當中，我們可將視為工控系統的一種。而目前已有的資安標準中，僅有 IEC 62443 可用來評估工控系統的元件和系統中的潛在資安弱點[4]。故對於儀器的資安特性，可根據 IEC 62443 資安標準來建構。Shaaban 等學者[5] 便根據 IEC 62443 規範了使用在智慧農業上的物聯網裝置的資安特性。而本論文的目的即為基於 IEC 62443 的國際標準來看儀器應具備的資訊安全特性。

在談 IEC 62443 之前，我們首先要介紹二個組織，第一個是國際自動化學會 (International Society of Automation, ISA)，另一個是國際電工委員會 (International Electrotechnical Commission, IEC)。國際自動化協會所屬的委員會 ISA99 自 2002 年起開始發展工控環境下的資安標準，也就是 ISA 62443。之後在 IEC 下屬的委員會 TC 65 也基於 ISA 62443 發展出 IEC 62443，因此我們可以說 IEC 62443 是由 ISA 和 IEC 共同發展出來的。在發展 ISA 62443 時，ISA99 也和 ISO 很緊密的合作以確保 62443 標準和 ISO 27000 系列的資安標準是一致的。ISO 27000 系列的標準也就是用在一般 IT (information technology) 環境中的資訊安全的標準。換言之，IEC 62443 和 ISO 27000系列的標準在很多地方有共通之處。差別在於 IEC 62443 是針對工控環境的資訊安全標準。IEC 62443 是一系列文件的集合，目前規劃的共有 14 份的文件，已出版的有 9 份。這些文件包含了國際標準 (international standard, IS)、技術報告 (technical report, TR) 以及技術規格 (technical specification, TS)。

為什麼我們要採用 IEC 62443 呢？ 一個原因是 IEC 62443 是目前全球唯一採取共識 (投票) 決定出來的一個工控領域資訊安全的標準，它不是一家公司或一個組織所制定出來的。另一原因是中華民國國家標準 CNS 也已經採納了 IEC 62443，轉化成為 CNS 62443 的國家標準。目前 CNS 62443 總共發行了 CNS 62443-1-1、CNS 62443-3-1、CNS 62443-4-1 及 CNS 62443-4-2 這 4 份文件，而 CNS 62443-2-4 和 CNS 62443-3-3 正準備發行中，初步預計要發行 6 份的 CNS 62443 的國家標準。故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。

IEC 62443 的文件總共分成 4 個大類，分別是 IEC 62443-1 到 IEC 62443-4。IEC 62443-1 系列的文件主要概述了工業資訊安全流程並介紹了資安基本概念，目前已發行的只有 IEC 62443-1-1 這份技術規範。IEC 62443-2 系列為有關資安政策和程序的文件，目前已發行了 IEC 62443-2-1、IEC 62443-2-3 和 IEC 62443-2-4 這 3 份文件。第三大類為 IEC 62443-3 系列的文件，這類主要是有關系統的文件，提供了設計和實施資訊安全系統的重要指導，目前這一系列的文件已全部出版，包括了 IEC 62443-3-1、IEC 62443-3-2 及 IEC 62443-3-3。第四大類為 IEC 62443-4 系列的文件，主要是有關元件 (component) 或產品 (product) 的文件，描述了元件在開發時及開發後必須滿足的資訊安全要求，目前也已全部發行完畢，包含了 IEC 62443-4-1 及 IEC 62443-4-2 這兩份文件。

IEC 62443 的主要的適用對象為資產的擁有者 (asset owner)、服務提供者 (service provider)、系統整合商 (system integrator) 以及產品供應商 (product supplier)。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，包括實體的安全、政策及程序、區域分隔及安全通道 (zone and conduit)、惡意軟體的避免、存取的控制監控及偵測以及補丁的安裝程序等。

IEC 62443 內有二個比較容易使人困惑的名詞：成熟等級 (maturity level) 和安全等級 (security level)。成熟等級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地的程度。而安全等級則會和本文所探討的儀器所具備的資訊安全性能相關。根據 IEC 62443-4-2 的規範，針對元件的資訊安全等級亦可分為四級。安全等級一代表著元件能防止偶然的攻擊行為，安全等級二代表著元件能防止使用低資源及簡單的方法的故意攻擊行為。安全等級越高，在 IEC 62443-4-2 中的要求也越多，但也代表著元件能防止更複雜的攻擊行為。一般元件設定的安全等級大約在安全等級二 (security level 2) 或安全等級三 (security level 3)。要達到安全等級二，根據 IEC 62443-4-2，元件需滿足的項目大約有 60 項。如果要元件要達到安全等級三，則要滿足的項目會更多。

二、IEC 62443-4-2 簡介

由以上討論，我們可以知道，針對一臺需要連網的儀器，我們可根據 IEC 62443-4-2[6] 來評估該儀器是否能防止惡意的攻擊。在 IEC 62443-4-2 當中有 7 個基本的要求 (fundamental requirement, FR)，FR1 是識別和鑑別控制、FR2 是使用控制、FR3 是系統完整性、FR4 是資料的保密性、FR5 是限制資料流、FR6 是對於事件的即時反應、FR7 是資源的可用性。這 7 個基本要求以及其相關的流程列於表 1 當中。

表 1. IEC 62443-4-2 元件資訊安全的 7 項基本要求[6] 及相關流程

基本要求	相關流程
FR1 –識別和鑑別控制 (Identification and Authentication Control)	使用者鑑別和授權
FR2 –使用控制 (Use Control)	角色和責任的執行
FR3 –系統完整性 (System Integrity)	檔案變更的管理
FR4 –資料保密性 (Data Confidentiality)	使用加密技術
FR5 –限制資料流 (Restricted Data Flow)	網路分隔
FR6 –即時回應事件 (Timely Response to Event)	稽核日誌
FR7 –資源可用性 (Resource Availability)	系統備份與還原

對於儀器開發者而言，若要能取得具公信力的證書以證明儀器的確滿足 IEC 62443-4-2 中的要求時，則通常要進行 IEC 62443-4-2 的認證 (certification)。認證的主要步驟如下：首先進行差距分析，比對產品本身的資安性能與 IEC 62443-4-2 的要求之間的差異。然後可進行產品改善以設法減少這些差異，使得產品能夠盡量符合 IEC 62443-4-2 的標準。接下來就是由合格的實驗室測試產品，測試完畢之後認證單位會根據測試的結果頒發相關的證書。目前國內已有廠商針對其資通產品進行並通過 IEC 62443-4-2 的認證。

三、儀器應有的資訊安全功能

儀器應有的資訊安全功能可基於 IEC 62443-4-2 的 7 項基本要求下的細部規範，以下我們將針對此 7 項要求的細部規範逐一檢視。

第一項為識別和鑑別控制。從 IEC 62443-4-2 對識別和鑑別技術的要求，我們應該要能夠區別儀器的每一位使用者。在傳統非連網的儀器上，通常只要能接觸到儀器即可操作，但由資安的角度上現在我們必須要知道是誰在操作這臺儀器。因此，儀器上必須要能夠設定帳號及密碼，也要有管理者來管理所有的帳號密碼，包括新增、啟用、修改、禁用和刪除這些帳號及其密碼。而管理者也能基於密碼的長度及資源種類設定密碼的強度要求。並且在指定時間內登入錯誤超過一定次數時，可以限制使用者登入系統，例如連續 3 次登入錯誤時即無法在 30 分鐘內登入等，在使用者登入前也應顯示警告訊息 (例如連續 3 次登入錯誤時即無法在 30 分鐘內登入) 以嚇阻攻擊者。如果儀器容許以無線方式登入的方式操作的話，儀器應該要能夠鑑別這些經由無線通訊連線的使用者，此處使用者包括人、設備或軟體程序 (API or library)。如果儀器也容許經由不可信賴的網路 (例如 Internet 公網) 存取的話，儀器也應該具備監控這樣的存取方式的能力。

第二大項的基本要求是使用控制，我們要確保儀器的使用者具有最小的權限，也就是儀器使用者僅能操作儀器，並不具有能修改不必要的系統參數的權限。儀器並能夠以自動或手動方式中斷遠端的連線或限制遠端連線的數量。若儀器可容許以無線方式連線的話，儀器也應該具有能夠授權、監控和限制以無線方式的連線通訊。而儀器在經過一段靜止時間後應該夠能自動地將操作的螢幕畫面鎖定，以避免未授權者操作儀器。此外，在儀器上能生成適當的日誌檔 (log)，將存取控制、錯誤的請求、作業系統事件、控制系統事件、備份和還原事件及配置更改等重要的行為記錄並儲存下來。當日誌儲存空間不足時系統也能夠自動提醒管理者，以避免空間不足導致日誌無法儲存。這些儲存下來的日誌都必須要有正確的時間戳記 (可經由網路標準協定 NTP 來取得正確時間)，以追溯事件發生的時間點。

在第三大類的基本要求也就是系統完整性上，儀器本身應能保護傳遞訊息的完整性，並具有保護機制 (例如防毒軟體) 來預防、偵測、通報及減輕惡意程式的影響，並能定期更新保護機制 (例如更新病毒碼資料庫或是作業系統補丁)。儀器也應該能夠偵測和防止在未經授權的情況下對儀器上所安裝的軟體和靜態資訊進行更改。此外儀器也應該能夠驗證輸入儀器的指令的語法和內容是否是正確的 (預防 command injection 之類的攻擊)。當儀器因遭受攻擊而無法正常運作時，應有機制可以將儀器的輸出重新設定為預設狀態。

在第四項的基本需求即資料保密性上，儀器本身應具有明確的存取授權機制， 使未授權的使用者無法存取儀器本身所儲存的資料，以保護儲存資料的機密性。儀器本身也應該有明確的存取授權機制以便能清除所有的資訊，不論這些資訊是儲存在正在使用的儀器或已淘汰不用的儀器上時。當儀器傳輸的資料如需加密的話，應使用業界普遍接受的方式及加密演算法以建立和管理密鑰。

在第五項的限制資料流部分，儀器本身所在的網路應和一般 IT 的網路進行邏輯分割 (例如在網路交換器上設定 VLAN)，以預防於一般網路上的攻擊可輕易延伸至儀器上。儀器本身亦能禁止來自外部的一般訊息，例如可阻絕使用儀器來接收個人的電子郵件訊息等。

而在第六項即時回應事件的部分，儀器應能讓授權人員或軟體 (例如 SIEM 軟體) 讀取其日誌以進行分析，儀器本身也能夠使用業界普遍接受的方式持續監控所有資訊安全機制，以便即時偵測、描述和通報資安的攻擊。

而在第七項資源的可用性上，儀器應能在阻斷服務 (denial of service, DoS) 攻擊時以降級模式運行，並能透過安全功能限制儀器內部資源的使用以防止資源耗盡。另一方面，儀器也能備份關鍵檔案，並在故障或中斷後能還原到已知的安全狀態。儀器上未使用的通訊埠或服務等也應該要關閉，並能顯示目前已安裝的元件及相關屬性。

四、結論

過去在開發儀器時，著重的是儀器的基本功能。然而隨著工業物聯網的快速發展，許多儀器都必須能夠上網。一旦儀器上網，許多資訊可以快速的流通，也可享有遠端操控的便利性，但隨之而來的是資訊安全上的風險。如何確保儀器的資訊安全，IEC 62443 是很好的參考依據。在 IEC 的文件當中主要可參考 IEC 62443-4-2。此文件中，針對使用者的鑑別、帳號密碼的設定、存取的監控、使用者的權限、操作的紀錄、惡意程式的防護、資料的存取、資料流的監控、通訊埠的開啟與關等，均有相關的規範。當我們在開發儀器時，我們便可以根據這些規範加以考慮，以強化所開發儀器的資訊安全防護能力，並確保該儀器能在工控環境的資安風險下正常運作。

參考文獻

1. R. Bold, H. Al-Khateeb, and N. Ersotelos, *Appl. Sci*., **12**, 24, (2022).
2. *X-Force Threat Intelligence Index 2022*, IBM, (2022).
3. L. Huang and Q. Zhu, *IEEE Trans. Inf. Forensics Secur*., **16**, (2021).
4. M. Lezzi, M. Lazoi, and A. *Corallo, Comput. Ind*., **103**, (2018).
5. A. M. Shaaban, S. Chlup, N. El-Araby, and C. Schmittner, *Appl. Sci*., **12**, 11 (2022).
6. *IEC 62443; Security for Industrial Automation and Control Systems-Part 4-2: Technical Security Requirements for IACS Components*. IEC International Standard: Geneva, Switzerland, (2019).

作者簡介

李維楨先生為美國加州大學柏克萊分校機械工程博士，現為國立臺灣科技大學機械工程系教授，國科會「發展智慧製造及半導體先進製程資安實測場域專案計畫」主持人。李教授已取得由國際自動化學會所頒發的 ISA/IEC 62443 資訊安全專家的證書。

Wei-Chen Lee received his Ph.D. in Mechanical Engineering from University of California at Berkeley. He is a Professor in the Department of Mechanical Engineering at National Taiwan University of Science and Technology and the Principal Investigator of the “Development of a Cybersecurity Test Site for Smart Manufacturing and Advanced Semiconductor Process” project supported by the National Science and Technology Council. Prof. Lee received the ISA/IEC 62443 cybersecurity expert certificate from International Society of Automation (ISA).