# 使用 Microchip 安全晶片於工業安全標準 IEC62443

作者: 顏睿余 主任應用工程師



隨著 5G、物聯網等持續發展,資訊及網絡安全對於工業自動化及控制系統 (IACS) 有著至關重要的考慮。下文將會簡介 IEC62443 工業安全標準,以及 Microchip 如何助您設計出符合此安全規範的產品。

### 關於 ISA/IEC 62443

ISA/IEC 62443 是一份長達 800 頁關於工業安全的統合文件,包含各種標準,技術規格與技術報告。這些文件於 2007 年由國際自動化學會 (ISA) 發布,其目的為提供安全標準以應用於工業自動化及控制系統,後來該標準亦被國際電工委員會 (IEC) 所採納,故有 ISA 62443 和 IEC 62443 兩種版本。

# ISA/IEC 62443 的內容架構

在整個工業自動化的架構中,ISA/IEC 62443 定義了 3 種角色,分別為資產擁有者 (Asset Owner)、系統整合者 (System Integrator) 和產品供應者 (Product Supplier)。ISA/IEC 62443 的 14 份標準文件被歸屬為 4 個章節,分別為:一般 (General)、政策與程序 (Policies and Procedures)、系統 (System) 和元件 (Component)。當中不同的角色應該參照不同的章節進行運作。

3 / 11					
General	IEC 62443-1-1	IEC TR-62443-1-2	IEC 62443-1-3	IEC 62443-1-4	
	Terminology, Concepts and Models	Master Glossary of Teams and Abbreviations	System Security Conformance Metrics	IACS Security Lifecycle and use-cases	
Policies and Procedures	IEC 62443-2-1	IEC TR-62443-2-2	IEC TR-62443-2-3	IEC TR-62443-2-4	IEC 62443-2-5
	Establishing an Industrial Automation and Control System Security Program	Master Glossary of Teams and Abbreviations	System Security Conformance Metrics	IACS Security Lifecycle and use-cases	Implementation Guidance for IACS Asset Owners
System	IEC TR-62443-3-1	IEC 62443-3-2	IEC 62443-3-3		
	Terminology, Concepts and Models	Master Glossary of Teams and Abbreviations	System Security Conformance Metrics		
Component	IEC 62443-4-1	IEC 62443-4-2			
	Product Development Requirements	Technical Security Requirements for IACS Components			

## 產品供應者如何遵從 IEC62443

對產品供應者 (Product Supplier) 而言,ISA/IEC 62443 的第 4 章節所規範的元件標準 (Component) 最為相關,元件標準的章節中包含了 2 份標準文件,分別為:IEC62443-4-1 和 IEC62443-4-2。

- IEC62443-4-1: 安全產品開發週期需求 (Secure Product Development Lifecycle Requirements) 該標準依據不同的安全成熟等級 (Maturity Levels) 在產品開發中定義了一系列需要實踐的項目 (Practices)
- IEC62443-4-2: 工業自動化控制系統的技術安全需求 (Technical Security Requirements for IACS Components) 該標準依據不同的安全等級 (Security Levels) 為其所開發的產品定義一系列的基礎需求 (Foundational Requirements)

# 如何設計產品以符合 ISA/IEC 62443-4-2 的規範

本文希望為各位讀者簡化 200 頁的 IEC62443-4-2,並讓大家了解如何搭配 Microchip 的 IC 去設計符合該規範的產品。

前文所述 ISA/IEC 62443 定義了 3 種角色,而 IEC62443-4-2 主要是想滿足資產擁有者在安全等級上的需求。所謂的安全等級,IEC62443-4-2 將其分成 5 級 (0-4),同時條列了具體的描述做為定義:



而且為了讓產品供應者在設計產品時有具體的設計條件去符合所謂的安全等級,IEC 62443-4-2 定義了7 種基礎需求,而每個基礎需求皆有條列具體的細項進行說明,該些細項分為一代需求 (CRs) 和進階需求 (REs),能夠對應到不同的安全等級,工程師在產品設計前必須先帶視這些基礎需求及其細項。

FR1	Identification and Authentication Control (IAC)
FR2	Use Control (UC)
FR3	System Integrity (SI)
FR4	Data Confidentiality (DC)
FR5	Restricted Data Flow (RDF)
FR6	Timely Response to Events (TRE)
FR7	Resource Availability (RA)

依據上表定義,基礎需求 1 (FR1) 主要是在定義裝置的身分識別與認證 (IAC),為了具體描述這種類別的安全需求, IEC 62443-4-2 定義了若干個元件需求 (CR1,x) 與進階需求 (RE1,x,x) 來闡述細項。

以下表為例作說明,在基礎需求 1 的第 7 項元件需求 (CR1.7) 中定義了透過密碼作裝置身分認 證的強度需求,另外再搭配 2 個進階需求 (RE1.7.1 和 RE1.7.2) 分別定義密碼的產生與其使用時限在人類使用者和全部使用者上的規範。產品供應者在設計產品時參考該表即可瞭解對於不同的 5 種安全等級的需求,這 3 項需求項目 (CR1.7、RE1.7.1 和 RE1.7.2) 是否需要列入產品設計當中。

RE1.7.2 - Password Lifetime Restrictions for Human Users

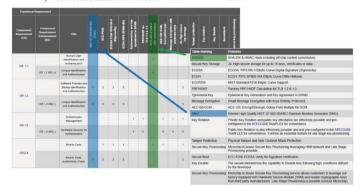
RE1.7.2 - Password Lifetime Restrictions for Human Users

RE1.7.3 - Password Lifetime Restrictions for All Users

- 如果設計的規格無法滿足 CR1.7 , 則代表該設計的安全等級只有 0
- 如果設計的規格只滿足 CR1.7 但不滿足 RE1.7.1 和 RE1.7.2,則代表該設計之安全等級為 2
- 如果設計的規格能滿足 CR1.7 與 RF1.7.1 但不滿足 RF1.7.2,則代表該設計之安全等級為 3

# 搭配使用 Microchip 的安全元件以符合 ISA/IEC 62443-4-2

以下列出了 Microchip 的 ATECC608B/CEC1712/CEC1736 能提供的密碼學硬體引擎規格,這 些規格將能對應到上述元件需求 (CR) 與進階需求 (RE) 的規範,也就是說產品供應者能搭配 Microchip 的元件進行產品設計以期符合 IEC62443-4-2 上的規範。



以下列出 4 點做進一步説明如何選用 Microchip 的產品幫助取得 IEC62443-4-2 認證:

#### ・密碼學的應用

在 IEC62443-4-2 裡定義得很清楚,所有的安全規範都是以應用的形式作條列,而非密碼學演算法本身,也就是說,產品設計必須搭配各項密碼學演算法去符合各個需要的元件需求與進階需求。的確現今坊間已存在各種高速運算品片,對於密碼學演算法的計算應該不成問題,但若是能搭配 ATECC608B 進行各項密碼學演算法,其高速的硬體加速引擎和超低睡眠功耗(30 nA)對產品而言可提供更長的裝置運作時間與密碼保護時間(如上述 RE1.7.1 與 RE1.7.2)。關於 Microchip 安全元件的相關資料請參考以下連結:

https://www.microchip.com/en-us/products/security/security-ics/cryptoauthentication-family

# ・信任根 (Root of Trust, RoT)

基於 IEC62443-4-2 元件需求 (CR3.12),其明列產品供應者需要針對發行的裝置程式碼提供證書簽章並且透過信任根對該程式碼的內容不變性 (Integrity) 進行認證。Microchip 提供CEC1712/CEC1736 晶片可扮演獨立的信任根,搭配運作於設備當中即可對現有的程式碼在開機前進行驗證把關,並在程式碼有問題時將程式碼回復為安全版本。CEC1736 可更進一步地在程式運作當下扮演監督的職責。關於 Microchip 信任根模組的相關資料,請參考下方連結:

https://www.microchip.com/en-us/products/security/prot

# ・IIL High 等級之密鑰保護

基於第 1 點說明,密碼學演算法在 IEC62443-4-2 的規範下是必要的,但所有的演算法都是基於密鑰,也就是說就算現有的設備對於各種密碼學算法的運算都不成問題,但如果沒有辦法妥善的保護密鑰,所有的密碼學演算法都相當於沒有任何保護作用,完全沒有安全性可言。 Microchip 提供的一系列安全元件能對存放於內的密鑰提供如同金庫般強而有力的保護。針對密鑰保護能力的驗證,ATECC608 已通過安全共通準則的密鑰儲存保護測試,並取得最高等級評分 (JIL High)。以擁有相同密鑰保護能力的晶片來說,選擇 ATECC608 擁有相當高的性價比。更多關於 ATECC608 JIL High 的說明請參考:

https://www.microchip.com/en-us/products/security/trust-platform/trustflex/trustflex-aws-iot-authentication/aws-iot-greengrass-atecc608b

# ・密鑰燒錄保護

密鑰的保護既然很重要,則密鑰的燒錄一定也是一個需要被重視的環節。如果燒錄密鑰時沒有特定的保護方式防止外洩,則燒錄完成後,保密 IC 再怎麼有銅牆鐵壁的保護都沒有用,漏洞在一開始就已經存在。這是在 IEC62443-4-1 當中即有規範到的部分。針對一系列ATEC608/CEC1712/CEC1736 等安全晶片,Microchip 皆能提供無人工廠 (HSM) 的保密燒錄服務,大家可在此了解 Microchip Trust Platform 相關運作:

https://www.microchip.com/en-us/products/security/trust-platform

聯繫信息 > Microchip 台灣分公司

電郵: rtc.taipei@microchip.com 聯絡電話: • 新竹 (03) 577-8366 技術支援專線: 0800-717-718

・ 高雄 (07) 213-7830 ・ 台北 (02) 2508-8600



