IoT-1006-3

門禁系統資安標準

-第三部：門禁閘道控制器

V2.0

行動應用資安聯盟

中華民國 112 年 11 月

目錄

目錄 **1**

引言 **2**

1. 適用範圍 **3**

2. 引用標準 **4**

3. 用語及定義 **5**

4. 安全等級 **6**

4.1 安全等級概述 6

5. 一般要求 **8**

5.1 身分鑑別、識別、授權安全 8

5.2 系統完整性 9

5.3 系統機密性 10

5.4 資源可用性 10

5.5 更新安全 11

5.6 警示與紀錄 11

5.7 實體安全 11

附錄 A (參考) 技術要求事項與各標準規範對照表 **12**

參考資料 **14**

版本修改紀錄 **15**

引言

根據 Marketsandmarkets 市調報告中指出，門禁系統的全球市場規模將從 2018 年的 75 億美元，每年以 8.24% CAGR (複合成長率)速度上升，預測到 2024 年達到 121 億美元。與 Mordor Intelligence 研究顯示，預估 2019-2024 年北美為全球門禁系統需求最大市場，與亞太地區皆為成長率最高的區域。然而門禁系統遭受各式各樣的資安威脅，主要可分為 4 大類: (1)駭客癱瘓門鎖系統、(2)門鎖鎖不住、(3)人臉資訊外洩、(4)用戶個資遭竊，這些威脅將使原本讓群眾安全安心的門禁服務不再被信任。

有鑑於此，於經濟部工業局(數位發展部數位產業署承接)支持下制定本系列標準，本系列標準基於國際工控資安標準 IEC 62443 及歐盟資安標準 ETSI EN 303 645，針對智慧門禁系統上相關應用的裝置制定資安標準，包括門禁系統上的門禁管理平台、門禁閘道控制器、門禁讀取器與智慧門鎖，以緩解門禁系統遭遇之資安威脅。

1. 適用範圍

本系列標準規定門禁系統產品之資安要求，本標準適用範圍包括門禁閘道控制器、門禁閘道控制器整合讀取器，其作為門禁讀取器與門禁管理平台資料傳輸之出入口，其應用包括但不限於將門禁讀取器接收之卡片、通行碼等資料傳送至門禁管理平台，及接收門禁管理平台發送之控制指令予以令管制出入門開啟或關閉。

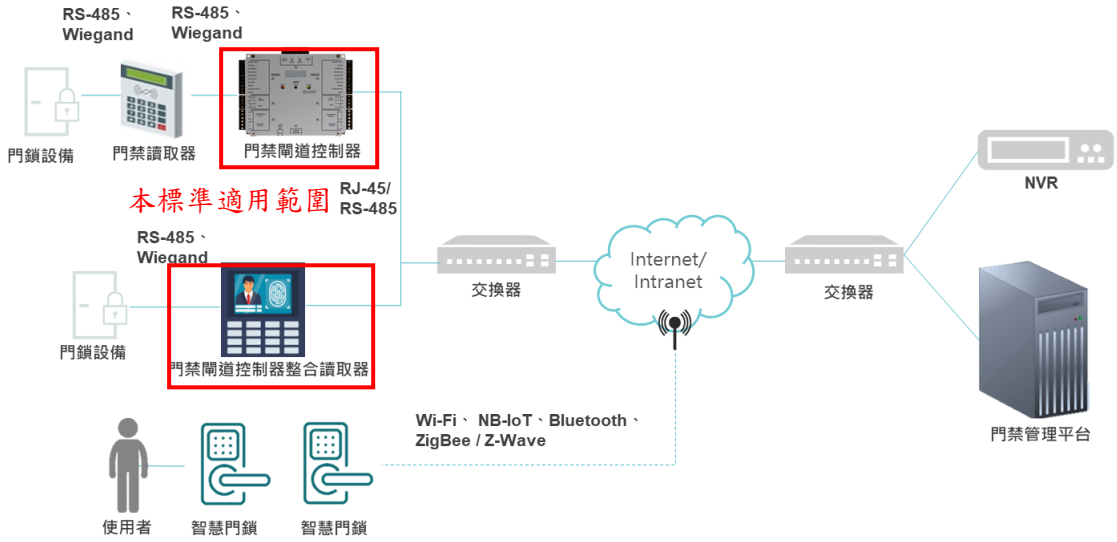

圖 1 門禁系統架構示意圖

按產品功能設計，產品適用標準說明：

- 產品為門禁閘道控制器，須依循 IoT-1006-1「門禁系統資安標準-第一部：一般要求」標準規範及本標準所載明之標準規範。
- 若產品具有管理門禁系統使用者功能，並整合門禁讀取器時，則須依循 IoT 1006-1「門禁系統資安標準 第一部：一般要求」、IoT 1006-2「門禁系統資安標準 第二部：門禁管理平台」、IoT 1006-4「門禁系統資安標準 第四部：門禁讀取器」及本標準之標準規範。

2. 引用標準

以下引用標準係本標準必要參考文件。如所列標準標示年版者，則僅該年版標準予以引用。未標示年版者，則依其最新版本(含補充增修)適用之。

[1] IEC 62443-4-2-2019	**Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components**
[2] ETSI EN 303 645 V2.1.1(2020-06)	**Cyber Security for Consumer Internet of Things: Baseline Requirements**
[3] IoT-1006-1 v1.0	**門禁系統資安標準-第一部：一般要求**

3. 用語及定義

「IoT-1006-1 門禁系統資安標準-第一部：一般要求」所述及下列用語及定義適用於本標準。

3.1 降級模式(Degrade mode)

係產品發生故障時，產品為繼續提供必要功能運作而設計的操作模式。

4. 安全等級

安全等級係為降低或消弭產品之資訊安全威脅，透過最適之安全組合，確保產品達到安全之要求。

4.1 安全等級概述

安全等級總表，如表 1 所示，第一欄為安全構面，包括：(1)身分鑑別、識別、授權安全、(2)系統完整性、(3)系統機密性、(4)資源可用性、(5)更新安全、(6)警示與紀錄及(7)實體安全；第二欄為安全要求分項，係依各安全構面設計對應之安全要求分項；第三欄為安全等級，按各安全要求分項之驗證結果，作為安全等級評估標準。本安全等級總表各欄的關連性，須依循本節 5.1 至 5.7 之技術規範內容。

安全等級依(1)引用國際標準之安全要求等級、(2)相關資安風險高低，分為 1 級、2 級與 3 級三個等級。產品應先通過較低安全等級之測試，始可進級高階等級之測試。

表 1 安全要求等級總表

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
身分鑑別、識別、授權安全	5.1.1 鑑別機制	5.1.1.2 5.1.1.3	-	-
	5.1.2 權限控管	5.1.2.2 5.1.2.3	5.1.2.4	5.1.2.5
系統完整性	5.2.1 資料完整性	-	-	-
	5.2.2 安全管理程序	-	-	5.2.2.2
	5.2.3 已知漏洞安全	-	5.2.3.2	-
系統機密性	5.3.1 敏感性資料保護	-	5.3.1.2	-
資源可用性	5.4.1 作業系統與網路服務	5.4.1.2	5.4.1.3	-
	5.4.2 資源管理	-	-	-
更新安全	5.5.1 軟韌體更新	-	-	-
警示與紀錄	5.6.1 安全事件日誌檔與警示	-	-	-
實體安全	5.7.1 實體入侵防護	5.7.1.1 5.7.1.2 5.7.1.3	5.7.1.4 5.7.1.5 5.7.1.6	5.7.1.7 5.7.1.8

4.1.1 安全構面：

(a) 身分鑑別與授權機制安全：溝通介面，包括遠端指令管理介面、網頁管理介面、操控程式等，應確保鑑別與授權相關機制。

(b) 系統完整性：產品的資料保護，監控與修補產品已知漏洞及預防與處置機制的資訊安全管理。

(c) 系統機密性：敏感性資料之儲存與通訊安全，通訊服務存在未知之資安漏洞與否。

(d) 資源可用性：產品須確保服務可維持正常運作的能力。

(e) 更新安全：產品之作業系統及韌體版本更新服務及韌體程式設計等，須具備足夠安全防護。

(f) 警示與紀錄：產品日誌紀錄須有管理機制，且於發生安全事件須具有警示能力。

(g) 實體安全：產品輕易被拆解與否，或產品資料存儲與測試用連接埠的處置，應視為實體安全要求的標的。

4.1.2 安全要求分項：

IoT-1006-1 之第 4.1.2 節之規定適用於本標準。

4.1.3 安全等級：

IoT-1006-1 之第 4.1.3 節之規定適用於本標準。

5. 一般要求

門禁閘道控制器為滿足安全功能，所有門禁系統之門禁閘道控制器產品應依不同級別依循 IoT 1006-1「門禁系統資安標準 第一部：一般要求」標準規範及本節所載明之標準規範。

5.1 身分鑑別、識別、授權安全

5.1.1 鑑別機制

5.1.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.1.1 節之要求。

5.1.1.2 產品應具備身分鑑別機制，變更產品安全相關設定之功能應執行身分認證，例如:設定時間、門禁權限、解除警示功能等，包括但不限於本地端管理介面、實體介面執行通行碼變更或權限角色變更。(1 級)

5.1.1.3 產品應具備定期更新身分鑑別碼的功能或符合 NIST SP 800-63B，例如:變更使用者通行碼。(1 級)

5.1.2 權限控管

5.1.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.1.3 節之要求。

5.1.2.2 使用者與產品建立會話(Session)後，應提供鎖定功能，阻止其他使用者提出相同會話請求。(1 級)

5.1.2.3 當使用者與產品建立之會話鎖定(Session)，應提供解除鎖定機制。(1 級)

5.1.2.4 當產品遠端指令介面網路連線閒置時，應具備遠端會話終止(Remote session termination)功能。(2 級)

5.1.2.5 產品的所有介面應提供限制建立會話(Session)數量的功能。(3 級)

5.2 系統完整性

5.2.1 資料完整性

5.2.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.1 節之要求。

5.2.2 安全管理程序

5.2.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.2 節之要求。

5.2.2.2 產品應提供匯出安全設定的功能且其支援格式應為機器可讀取的格式。(3 級)

5.2.3 已知漏洞安全

5.2.3.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.2.3 節之要求。

5.2.3.2 產品應使用公認資安產業慣例之產品安全監控之功能，包括但不限於 ISO/IEC 國際標準、歐盟國際標準或美國國家標準等普遍業界所接受的作法。(2 級)

5.3 系統機密性

5.3.1 敏感性資料保護

5.3.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.3.1 節之要求。

5.3.1.2 產品應確保自身信任根所使用到的金鑰及資料都要確保其機敏性、完整性及可用性。(2 級)

5.4 資源可用性

5.4.1 作業系統與網路服務

5.4.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.4.1 節之要求。

5.4.1.2 當產品遭遇 DoS 攻擊時，產品應能在降級模式(Degrade mode)下維持基本功能運作。(1 級)

5.4.1.3 產品應具備減緩受到訊息洪泛(Message flood)類型之 DoS 攻擊影響的能力。(2 級)

5.4.2 資源管理

5.4.2.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.4.2 節之要求。

5.5 更新安全

5.5.1 軟韌體更新

5.5.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.5.1 節之要求。

5.6 警示與紀錄

5.6.1 安全事件日誌檔與警示

5.6.1.1 產品須依循 IoT-1006-1 門禁系統資安標準-第一部：一般要求第 5.6.1 節之要求。

5.7 實體安全

5.7.1 實體入侵防護

5.7.1.1 產品於啟動階段應確保韌體、軟體及組態資料的完整性。(1 級)

5.7.1.2 產品外部不應有徒手(不須特殊工具)即可還原預設卡號及通行碼預設值的功能。(1 級)

5.7.1.3 藍牙應加密傳輸且符合第一部 5.3.1.1 項(1)之要求。(1 級)

5.7.1.4 產品預設不應透過實體介面存取產品作業系統之除錯模式。 若需經實體介面存取，則應通過身分鑑別作業始得執行。(2 級)

5.7.1.5 產品應採用一體成形或防拆螺絲等機殼防拆除保護，及具備防拆偵測設計。(2 級)

5.7.1.6 產品於啟動階段應確保韌體、軟體及組態資料的真實性。(2 級)

5.7.1.7 產品當偵測到除錯介面之存取行為時，應產生安全事件日誌。(3 級)

5.7.1.8 產品偵測到實體遭未經授權存取時，應向使用者及管理者發出警示且應產生安全事件日誌。(3 級)

附錄 A
(參考)
技術要求事項與各標準規範對照表

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.1.1.2		5.5-5 - Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.
5.1.1.3	CR 1.5C - Authenticator management - change/refresh all authenticators periodically	5.1-4 - Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.
5.1.2.2	CR2.5A - Session lock - initiation	-
5.1.2.3	CR2.5B - Session lock - removal	-
5.1.2.4	CR2.6 - Remote session termination	-
5.1.2.5	CR2.7 - Concurrent session control	-
5.2.2.2	CR7.6RE(1) - Machine-readable reporting of current security settings	-
5.2.3.2	CR6.2 - Continuous monitoring	-
5.3.1.2	NDR3.12 - Provisioning product supplier roots of trust	5.4-1(partial) - Sensitive security parameters in persistent storage shall be stored securely by the device.
	NDR3.13A - Provisioning asset owner roots of trust	
	NDR3.13B - Provisioning asset owner roots of trust	
5.4.1.2	CR 7.1 - Denial of service protection	-
5.4.1.3	CR7.1 RE(1) - Denial of service protection - Manage communication load from component	5.12-2(partial) - The manufacturer should provide users with guidance on how to securely set up their device.
		5.12-3(partial) - The manufacturer should provide users with guidance on how to check whether their device is securely set up.
5.7.1.1	NDR3.14 - Integrity of the boot process	-
5.7.1.2	-	-
5.7.1.3	-	-

本標準要求事項	對應標準規範	
	IEC 62443-4-2[1]	ETSI EN 303 645[2]
5.7.1.4	NDR 2.13 - Use of physical diagnostic and test interfaces	5.6-4 - Where a debug interface is physically accessible, it shall be disabled in software.
5.7.1.5	NDR3.11 - Physical tamper resistance and detection	-
5.7.1.6	NDR3.14 RE(1) - Authenticity of the boot process	5.7-1 - The consumer IoT device should verify its software using secure boot mechanisms.
5.7.1.7	NDR2.13RE(1) - Use of physical diagnostic and test interfaces -Active monitoring	-
5.7.1.8	NDR3.11RE(1) - Communication authentication	-

參考資料

(1) SP 800-140C Rev. 1:2022 CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759, https://csrc.nist.gov/publications/detail/sp/800-140c/rev-1/final

版本修改紀錄

版本	時間	摘要
V1.0	111 年 7 月 22 日	版本維持不變，修改內容為編規錯誤及測試一致性問題，如勘誤與修正對照表。
V2.0	112 年 11 月 27 日	修訂內容。