IoT-2006-3

門禁系統資安測試規範

-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 12 月

目錄

引言

門禁系統近年常見駭客癱瘓門鎖系統、門鎖鎖不住、人臉資訊外洩及使用者個資遭竊等資安威脅，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一系列門禁系統相關裝置之資安標準，協助台灣產業接軌國際，提升研發技術及保證產品質量。

「IoT-2006-3 門禁系統資安測試規範-第三部：門禁閘道控制器」(以下簡稱本測試規範)，依據「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」訂定，同時參照「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」俾利門禁系統裝置製造商、系統整合商及物聯網資安檢測實驗室等作為相關產品檢測技術的參考藍本。本測試規範中具體明列資安檢測之測試項目、測試條件、測試方法及測試標準等事項。

1. 適用範圍

本規範適用於門禁系統中的門禁閘道控制器、門禁閘道控制器整合讀取器(如圖1)。

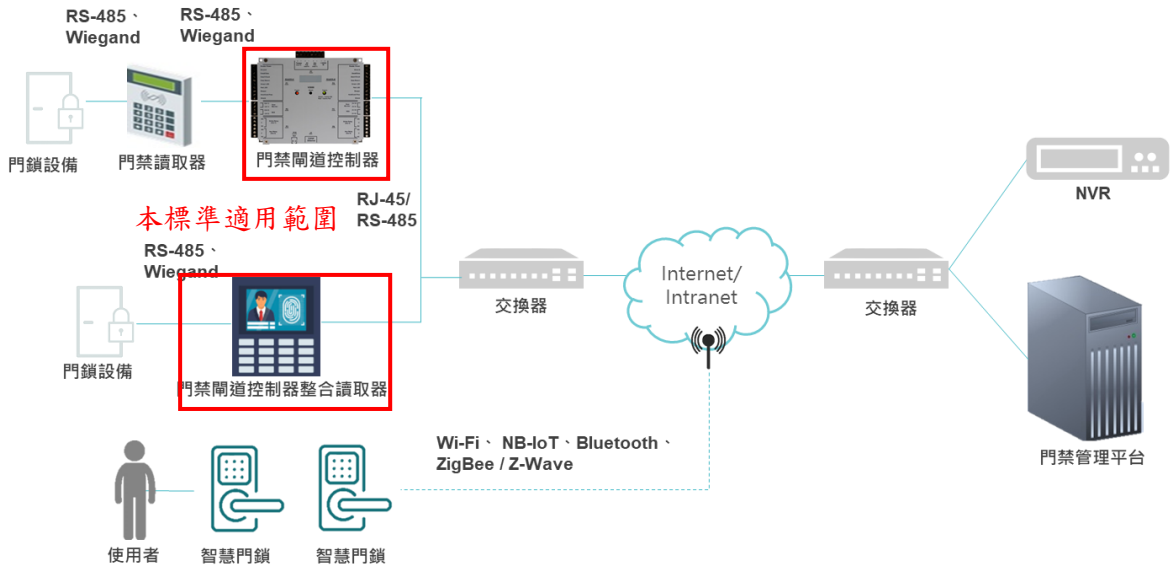

圖 1 適用範圍示意圖

2. 引用標準

下列法規、標準或文件因本規範所引用，成為本規範之一部分。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-1006-3 v1.0 門禁系統資安測試規範-第三部：門禁閘道控制器

3. 用語及定義

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」所規定之用語及定義適用於本規範。

4. 測試項目分級

本節依據「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」制定相對應之安全測試項目及測試方法。

實機測試標準等級總表，如表 1 所示，第一欄為安全測試構面，包括：身分鑑別、識別、授權機制安全、系統完整性、系統機密性、資源可用性、更新安全、警示與紀錄及實體安全；第二欄為安全測試項目，係依第一欄安全測試構面設計對應之安全測試項目；第三欄為安全等級之測試標準，按各安全測試項目所做之測試標準，評估安全等級。

安全等級依(1)相關資安風險高低、(2)安全技術實現複雜度，分為 1 級、2 級、3 級三個等級，產品應先通過較低安全等級之測試，始可進行進階等級之測試。

表 1 實機測試標準等級總表

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	-	-	-

安全構面	安全要求分項	安全等級		
		1 級	2 級	3 級
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

5. 資安測試規範

門禁閘道控制器為滿足安全功能應依不同級別依循 IoT 1006-1「門禁系統資安標準第一部：一般要求」測試規範及本節所載明之測試規範。

5.1 身分鑑別、識別、授權安全測試

檢視產品有關身分鑑別、識別、授權安全部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.1.1 鑑別機制測試

5.1.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.1.1 節。**

5.1.1.2 **身分鑑別機制測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之系統管理者帳號、通行碼。

(2) 產品應保持出廠預設環境狀態。

(3) 若產品支援使用者介面，應提供本地端管理介面。

(4) 廠商應提供產品身分鑑別機制說明文件。

(5) 廠商應提供變更設定需進行身分驗證之產品功能說明文件。

(6) 廠商應提供產品安全相關設定與產品安全相關設定功能之宣告。

(d) 測試目的：

驗證產品安全相關設定功能進行變更時，是否具備身分鑑別機制。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

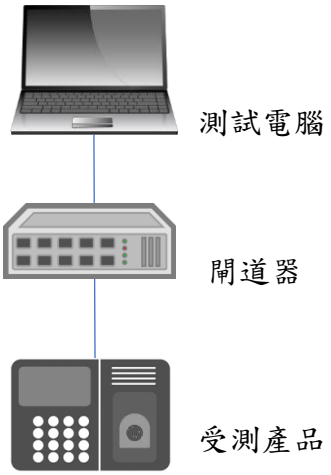

圖 2 測試示意圖

(g) 測試方法：

(1) 審閱廠商提供之說明文件。

(2) 若產品支援網頁介面、遠端指令介面或 API 介面時，將測試電腦與產品連接，並設定中間人攔截熱點，並開啟封包側錄工具進行側錄。

(3) 根據產品使用說明，開啟管理介面之使用者登入頁面。

(4) 以產品之系統管理員帳號登入，執行身分鑑別操作。

(5) 將側錄到的身分鑑別封包，再另一次身分鑑別操作時，重新發送至產品。

(6) 檢視身分驗證結果。

(7) 根據說明文件對產品安全相關功能進行設定變更，包括但不限於登入本地端管理介面、實體介面執行通行碼變更或權限角變更。

(8) 檢視產品在開啟功能設定時，是否執行身分驗證機制。

(9) 若產品支援本地端管理介面，以產品之系統管理員帳號登入，執行身分鑑別操作。

(10) 重複步驟(7)~(8)。

(h) 測試結果：

(1) 產品具備身分鑑別機制，且產品能正常執行身分鑑別機制。

(2) 身分鑑別機制具備抵抗重送攻擊的能力。

(3) 當變更安全相關設定功能時，產品應執行身分鑑別機制。

(4) 通過：(1)~(3)三項結果皆符合。

(5) 不通過：(1)~(3)三項結果不符合其一。

(6) 不適用：無。

5.1.1.3 **定期更新身分鑑別碼測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供使用手冊以說明身分鑑別碼定期(提醒)更換功能之作法。

(d) 測試目的：

驗證產品之身分鑑別碼是否具備定期(提醒)更新的功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品使用手冊。

(2) 根據使用手冊說明，驗證產品更改身分鑑別碼設定，例如:變更使用者通行碼。

(h) 測試結果：

(1) 產品應具備定期(提醒)變更身分鑑別碼之功能。

(2) 產品符合 NIST SP 800-63B 之要求。

(3) 通過：(1)~(2)項結果符合其一。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.1.2 權限控制測試

5.1.2.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.1.2 節。**

5.1.2.2 **會話鎖定功能測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.2.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之系統管理者帳號、通行碼。

(2) 產品應提供會話鎖定、解除鎖定與更改閒置時間之操作步驟。

(3) 產品應宣告人員操作之介面(例如:實體及遠端)。

(d) 測試目的：

驗證產品是否具備自動或手動會話鎖定功能，以防止非預期存取。

(e) 測試條件：

產品應支援人員操作介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 根據產品說明，登入產品操作介面。

(3) 進入產品管理介面，嘗試更改閒置時間。

(4) 將產品閒置至設定之時間，檢查產品操作介面是否已鎖定。

(5) 根據 5.1.2.3 項之方法，解除操作介面鎖定。

(6) 以手動方式啟動操作介面鎖定。

(7) 檢查產品操作介面是否已鎖定。

(h) 測試結果：

(1) 產品具閒置時間後自動鎖住功能，且可透過更改閒置時間功能更改。

(2) 產品提供手動會話鎖定功能。

(3) 通過: (1)~(2)項結果符合其一。

(4) 不通過: (1)~(2)項結果皆不符合。

(5) 不適用: 產品不支援人員操作介面。

5.1.2.3 **解除會話鎖定功能測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.2.3

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品之系統管理者帳號、通行碼。

(2) 產品應宣告人員操作之介面。

(3) 產品應提供至少 2 筆使用者及與解鎖權限紀錄之對應表，第 1 個使用者具會話鎖住及解鎖權限，第 2 個使用者不具解鎖權限，作為測試使用。

(d) 測試目的：

當會話鎖定時，驗證產品是否於相同使用者再次身分認證後，提供解除鎖定之功能。

(e) 測試條件：

產品應支援人員操作介面。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 以 5.1.2.2 之方法使用權限紀錄對應表中之第 1 個使用者，登入產品操作介面後，觸發鎖定功能

(2) 嘗試以該使用者身分，再次登入並進行存取。

(3) 再次觸發會話鎖定功能。

(4) 嘗試以使用權限紀錄對應表中之第 2 個使用者之身分，登入並進行存取。

(h) 測試結果：

(1) 會話鎖定時，可透過第 1 個使用者之身分登入解鎖並進行存取。

(2) 會話鎖定時，無法以第 2 個使用者身分登入及存取。

(3) 通過: (1)~(2)項結果皆符合。

(4) 不通過: (1)~(2)項結果不符合其一。

(5) 不適用: 產品無支援人員操作介面。

5.1.2.4 **遠端會話終止功能測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.2.4

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品之系統管理者帳號、通行碼。

(2) 其他裝置之使用者帳號、通行碼。

(3) 產品應提供可連接產品之其他裝置。

(4) 產品應提供其他裝置之操作步驟。

(5) 產品應提供終止會話之操作步驟。

(6) 產品應提供更改閒置時間之操作步驟。

(d) 測試目的：

若產品支持遠程會話(remote session)，驗證產品建立會話後，是否提供自動或手動會話終止功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

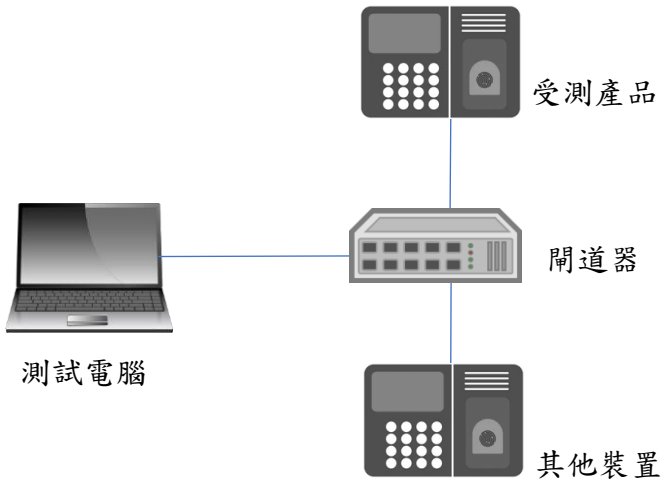

圖 3 測試示意圖

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 登入產品管理介面建立遠程會話。

(3) 嘗試更改閒置時間，並將產品閒置至設定之時間。

(4) 於會話終止時，嘗試以未授權身分之裝置，再次進行存取。

(5) 重新建立遠程會話後，嘗試手動進行會話終止。

(6) 於會話終止時，嘗試以未授權身分之裝置再次進行存取。

(7) 於會話終止時，嘗試重新建立遠程會話，並進行存取。

(8) 透過其他裝置，連上產品並建立遠程會話。

(9) 嘗試於產品更改閒置時間，並將其他裝置閒置至設定之時間。

(10) 透過其他裝置執行(4)~(7)測項。

(h) 測試結果：

(1) 產品提供閒置時間後自動終止功能，且閒置時間可進行更改。

(2) 產品提供手動會話終止功能。

(3) 會話終止後，無法於未授權狀況下存取。

(4) 會話終止後，重新建立會話時，不可再繼先前會話之操作。

(5) 通過：(1)~(2)項結果符合其一，且(3)~(4)項結果皆符合。

(6) 不通過：(1)~(2)項結果皆不符合，(3)~(4)項結果不符合其一。

(7) 不適用：產品不支援遠端會話功能，或設備間須持續連線運作。

5.1.2.5 **限制會話數量功能測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.1.2.5

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 其他裝置之使用者帳號、通行碼。

(2) 產品之系統管理者帳號、通行碼。

(3) 產品須提供可連接產品之其他裝置。

(4) 產品須提供其他裝置之操作步驟。

(5) 產品須宣告可同時存在的會話數量。

(d) 測試目的：

驗證產品是否提供限制同時存在的會話數量之功能。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 3。

(g) 測試方法：

(1) 將測試電腦連接產品。

(2) 登入其他裝置管理者介面，並連接產品。

(3) 根據產品宣告，嘗試建立多個會話，直到超過限制之數量。

(h) 測試結果：

(1) 產品具有限制同時存在會話數量的功能，產品無法同時存在超過限制數量的會話。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.2 系統完整性測試

檢視產品有關系統完整性部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.2.1 資料完整性測試

5.2.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.1 節。**

5.2.2 安全管理程序測試

5.2.2.1 測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.2 節。

5.2.2.2 匯出安全設定之機器可讀格式報告測試

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.2.2.2

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 廠商應提供產品匯出安全設定之方法。

(2) 廠商應宣告產品所匯出之安全設定，支援哪些機器可讀(machine-readable)資料格式。

(d) 測試目的：

驗證產品是否提供匯出安全設定的功能且其支援格式是否為機器可讀取的格式。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 4。

圖 4 測試示意圖

(g) 測試方法：

依據安全設定匯出之操作方法，查驗所匯出之安全設定資料是否為電腦可讀取之格式。

(h) 測試結果：

(1) 產品可匯出安全設定資料。

(2) 產品所匯出之安全設定資料格式支援逗號分隔值(CSV)、JavaScript Object Notation (JSON)或可擴展標記語言(XML)等機器可讀格式。

(3) 通過：(1)(2)項結果符合。

(4) 不通過：(1)(2)項結果不符合。

(5) 不適用：無。

5.2.3 已知漏洞測試

5.2.3.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.2.3 節。**

5.2.3.2 **產品安全監控功能測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.2.3.2

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品應提供書面資料以說明安全監控功能如何提供監控，或對接的安全監控設備符合公認資安產業慣例之證明文件作為審查依據，例如:使用手冊、安全指南。
(2) 若須倚賴其他安全監控設備，則廠商應提供支援對接的安全監控設備相關說明文件。

(d) 測試目的：

驗證產品是否使用產品安全監控的功能。

(e) 測試條件：

產品應具網路通訊或網頁介面。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品提供的書面資料。
(2) 依據 CAPEC[3]所列舉的 Inject Unexpected Items 類及 Subvert Access Control 類的資安攻擊事件，在上述二類攻擊模型中選擇「Likelihood of attack」及「Typical severity」為「High」的攻擊技術，以此對產品發動攻擊。或由廠商自行列出可防禦之資安攻擊事件及其防禦措施。
(3) 根據書面資料，驗證產品之安全監控功能，或所配置的安全監控設備及其安全監控功能是否能夠偵測、識別或回報。

(h) 測試結果：

(1) 產品所使用的產品安全監控功能，或產品所對接之安全監控設備，對於 CAPEC 所列舉的 Inject Unexpected Items 及 Subvert Access Control 類型的攻擊模型，針對其「Likelihood of attack」及「Typical severity」為「High」的資安攻擊事件能進行偵測、識別或回報。或廠商自行列出可防禦之資安攻擊事件的措施。
(2) 通過：(1)項結果符合。
(3) 不通過：(1)項結果不符合。
(4) 不適用：不支援網路通訊或網頁介面。

5.3 系統機密性測試

檢視產品有關系統機密性部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.3.1 敏感性資料儲存安全測試

5.3.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.3.1 節。**

5.3.1.2 **信任根安全測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.3.1.2

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供產品之信任根功能的操作方法。

(2) 廠商應提供如何保護信任根所用之金鑰及資料的方法。

(3) 廠商應提供信任根功能之設計文件。

(d) 測試目的：

驗證產品之信任根所保護的金鑰及資料是否具有機密性、完整性和可用性的保護。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 依據信任根功能操作方法，查驗是否可提供軟韌體完整性及真實性的保護。

(2) 查驗廠商所保護之信任根所用之金鑰及資料，是否被加密保護。

(3) 查驗廠商所保護之信任根所用之金鑰及資料，是否能防止未授權存取。

(4) 查驗廠商所保護之信任根所用之金鑰及資料，其存取修改都會被記錄。

(h) 測試結果：

(1) 產品具備信任根之功能。

(2) 產品信任根所用之金鑰及資料得到機密性、完整性及真實性的保護。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.4 資源可用性測試

檢視產品有關資源可用性部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.4.1 作業系統與網路服務測試

5.4.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.4.1 節。**

5.4.1.2 **防禦 DoS 攻擊測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.4.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 廠商應提供書面資料以說明產品因應 DoS 攻擊的方法，例如:能防禦 SYN flood、Ping of Death、ARP flood 的資源消耗型 DoS 攻擊，包括但不限於產品安全設計或透過環境面額外裝置進行的安全設置與部署。若以環境面額外裝置進行安全部署，廠商應在產品之使用說明書或資安指引中註明產品於現場佈建時額外部署的軟硬體設備，並說明建議部署的軟硬體設備類型。

(2) 廠商應提供書面資料以說明如何在降級模式下維持產品基本功能的運作，作為審查依據。

(d) 測試目的：

驗證產品遭遇 DoS 攻擊時，產品是否能在降級模式(Degrade mode)下維持基本功能運作。

(e) 測試條件：

無。

(f) 測試佈局：

如圖 2。

(g) 測試方法：

(1) 審閱產品說明文件。

(2) 使用模擬 DoS 攻擊的工具，檢視產品是否仍能維持基本功能運作。

(h) 測試結果：

(1) 產品應能在降級模式下維持產品基本運作且與說明文件相符，例如: 能防禦 SYN flood、Ping of Death、ARP flood 的資源消耗型 DoS 攻擊。

(2) 當產品以環境面額外裝置進行安全部署時，產品之使用說明書或資安指引中註明產品於布建環境額外部署之軟硬體裝置。且證明至少可防禦 SYN flood、Ping of Death、ARP flood 等資源消耗型 DoS 攻擊。

(3) 通過： (1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)二項結果皆不符合。

(5) 不適用：無。

5.4.1.3 **緩解訊息洪泛型 DoS 攻擊能力測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.4.1.3

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 廠商應提供書面資料以說明產品預防訊息洪泛 DoS 攻擊的方法，例如:能防禦 UDP flood、ICMP flood 的頻寬消耗型 DoS 攻擊，包括但不限於產品安全設計或透過環境面的安全設置與部署。若以環境面額外裝置進行安全部署，廠商應在產品之使用說明書或資安指引中註明產品於現場佈建時額外部署的軟硬體設備，並說明建議部署的軟硬體設備類型。

(2) 廠商應提供書面資料以說明產品如何減緩受到訊息洪泛 DoS 攻擊的影響，針對訊息洪泛類型 DoS 攻擊的相應測試，包括:威脅減緩測試(Threat mitigation testing)、漏洞測試(Vulnerability testing)作為審查依據。

(d) 測試目的：

驗證產品是否具備減緩受到訊息洪泛(Message flood)類型的 DoS 攻擊影響的能力。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品說明文件是否具備減緩訊息洪泛類型 DoS 攻擊的能力。

(2) 使用模擬訊息洪泛 DoS 攻擊的工具，檢視產品是否仍能減緩攻擊所造成的影響。

(h) 測試結果：

(1) 當產品遭遇訊息洪泛類型的 DoS 攻擊時，例如:UDP flood、ICMP flood，產品應能減緩訊息洪泛 DoS 攻擊對產品的影響。

(2) 產品以額外裝置進行安全部署時，產品之使用說明書或資安指引中註明產品於布建額外部署之軟硬體裝置。且證明至少可緩解 UDP flood、ICMP flood 等氾流型 DoS 攻擊。

(3) 通過：(1)~(2)二項結果符合其一。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.4.2 資源管理測試

5.4.2.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.4.2 節。**

5.5 更新安全測試

檢視產品有關更新安全部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.5.1 軟韌體更新測試

5.5.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.5.1 節。**

5.6 警示與紀錄測試

檢視產品有關警示與紀錄部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.6.1 安全事件日誌與警示測試

5.6.1.1 **測試依循「IoT-2006-1 門禁系統資安測試規範-第一部：一般要求」第 5.6.1 節。**

5.7 實體安全測試

檢視產品有關實體安全部分之送審資料是否符合 IoT-1006-3 之安全要求，並依下列各測試項目進行實機測試。

5.7.1 實體入侵防護測試

5.7.1.1 **啟動階段完整性測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.1

(b) 安全等級：

1 級。

(c) 測試資料：

(1) 產品應提供安全啟動功能之設計文件。

(2) 廠商應提供未加密韌體檔案與韌體安裝說明文件。

(d) 測試目的：

驗證產品於開機階段是否能確保韌體、軟體及組態資料之完整性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能之書面資料。

(2) 竄改韌體、軟體及組態資料後，重新啟動產品。

(h) 測試結果：

(1) 當韌體、軟體及組態資料經竄改後，產品無法被啟動。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.2 **還原預設卡號、通行碼測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.2

(b) 安全等級：

1 級。

(c) 測試資料：

產品應提供還原出廠設定操作說明。

(d) 測試目的：

驗證產品實體層的預設卡號、通行碼還原設計是否具備安全防護機制。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 檢視產品外觀(不包括設計上應鎖定於牆壁該面)，是否存在無須特殊工具即可輕易還原預設卡號及通行碼之機制，例如:使用一支筆或竹籤等非特殊工具強行破解的方式。

(2) 若存在，則測試其還原至出廠設定之功能。

(h) 測試結果：

(1) 產品外觀不存在無須特殊工具即可輕易還原回預設卡號、通行碼的機制。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

5.7.1.3 **藍牙傳輸保護測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.3

(b) 安全等級：

1 級。

(c) 測試資料：

無。

(d) 測試目的：

驗證產品藍牙是否使用安全的藍牙加密傳輸。

(e) 測試條件：

產品應支援藍牙傳輸。

(f) 測試佈局：

如圖 5。

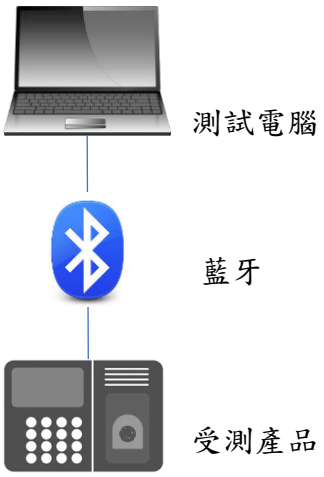

圖 5 測試示意圖

(g) 測試方法：

(1) 使用藍牙傳輸側錄工具，擷取受測物之藍牙封包，確認裝置所使用之藍牙傳輸是否加密。

(2) 藍牙傳輸是否採用符合 NIST SP 800-140Cr1 [(2)]所核可之同等或以上等級之加密演算法。

(h) 測試結果：

(1) 產品之藍牙傳輸採用符合 NIST SP 800-140Cr1 所核可之同等或以上等級之加密演算法。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品不支援藍牙。

5.7.1.4 實體介面安全管控測試

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.4

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 產品應保持出廠預設環境狀態。

(2) 產品應提供書面資料，說明進入作業系統(若有)除錯模式之方法。

(d) 測試目的：

驗證是否無法透過產品實體介面存取作業系統之除錯模式，或存取實體介面具身分鑑別。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據文件所述連接相應之實體介面。

(2) 若產品支援 USB 埠，則將測試電腦連接產品之 USB 埠，並開啟相應之管理介面連接工具。

(3) 透過 USB 埠存取作業系統之除錯模式。

(4) 若產品支援 UART 埠，則將測試電腦連接產品之 UART 埠，並開啟相應之管理介面連接工具。

(5) 透過 UART 埠存取作業系統之除錯模式。

(6) 若產品支援 JTAG 埠，則將測試電腦連接產品之 JTAG 埠，並開啟相應之管理介面連接工具。

(7) 透過 JTAG 埠存取作業系統之除錯模式。

(h) 測試結果：

(1) 若產品支援透過 USB、UART 或 JTAG 存取作業系統之除錯模式時，產品要求身分鑑別。

(2) 產品不存在可進入作業系統除錯模式之實體介面。

(3) 通過：(1)~(2)項結果符合其一。

(4) 不通過：(1)~(2)項結果皆不符合。

(5) 不適用：無。

5.7.1.5 實體保護測試

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.5

(b) 安全等級：

2 級。

(c) 測試資料：

(1) 若產品具防拆除保護機制(例:一體成型或防拆螺絲)，或具備防拆偵測設計，則應提供相關說明文件。

(2) 若產品之外殼拆除障礙，是透過現場佈建時，額外於產品外殼再裝上支架或防護罩外殼來加以保護，廠商應在產品之使用說明書或資安指引中註明產品於現場佈建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件應公告在廠商官網上。

(d) 測試目的：

驗證產品是否建立外殼拆除障礙，或具備防拆偵測設計，以防止實體入侵。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱產品提供之說明文件。

(2) 檢視產品之外殼是否一體成型。

(3) 檢視產品之外殼是否經防拆螺絲鎖住。

(4) 檢視產品是否具備防拆警示功能之防拆功能。

(h) 測試結果：

(1) 產品採用一體成形或防拆螺絲等機殼防拆除保護設計。

(2) 當產品應額外加裝支架或防護罩外殼，產品之使用說明書或資安指引中註明產品於現場布建時應額外加裝支架或防護罩外殼，並說明建議加裝的類型，且該文件公告在廠商官網上。

(3) 產品採用本身具有防拆偵測設計或加裝具有防拆偵測功能之防護，防拆警示方式包括但不限於警報聲響、簡訊或 email。

(4) 通過：(1)(3)項結果符合，或(2)(3)項結果符合。

(5) 不通過：(1)(2)項結果皆不符合，或(3)項結果不符合。

(6) 不適用：無。

5.7.1.6 **安全啟動真實性測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.6

(b) 安全等級：

2 級

(c) 測試資料：

產品須提供安全啟動功能之設計文件。

(d) 測試目的：

驗證產品於開機階段是否能確保韌體、軟體及組態資料的真實性。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 審閱具備安全啟動功能之書面資料。

(2) 確認產品在開機過程中是否驗證韌體、軟體及組態資料的簽章。

(h) 測試結果：

(1) 安全啟動功能僅能透過安全區域執行開機啟動。

(2) 書面資料證實產品在開機過程中驗證韌體、軟體及組態資料的簽章。

(3) 通過：(1)~(2)項結果皆符合。

(4) 不通過：(1)~(2)項結果不符合其一。

(5) 不適用：無。

5.7.1.7 **除錯介面偵測測試**

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.7

(b) 安全等級：

3 級。

(c) 測試資料：

產品應提供除錯介面偵測與警示之功能設計說明文件。

(d) 測試目的：

當存取產品除錯介面時，驗證產品是否有能力偵測且產生安全事件日誌。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據產品提供之說明文件，開啟相對應之管理介面連接工具。

(2) 若產品存在 USB 埠，嘗試存取作業系統除錯模式。

(3) 檢視產品狀態。

(h) 測試結果：

(1) 當產品偵測到存取除錯介面時，產品應產生安全事件日誌之紀錄。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：產品之作業系統無除錯介面。

5.7.1.8 實體介面偵測警示功能測試

(a) 測試依據：

「IoT-1006-3 門禁系統資安標準-第三部：門禁閘道控制器」之 5.7.1.8

(b) 安全等級：

3 級。

(c) 測試資料：

(1) 產品應提供實體介面偵測與警示之功能設計說明文件。

(2) 產品應提供實體介面清單。

(d) 測試目的：

當產品之實體介面有未經授權存取時，驗證產品是否有能力偵測且發出警示。

(e) 測試條件：

無。

(f) 測試佈局：

無。

(g) 測試方法：

(1) 根據產品提供之說明文件，開啟相對應之管理介面連接工具。

(2) 若產品存在 USB 埠，則插拔外接 USB 埠。

(3) 若產品存在 RJ45 埠，則插拔外接 RJ45 埠。

(4) 檢視產品狀態。

(h) 測試結果：

(1) 當產品偵測實體埠經異常插拔操作時，產品應產生安全事件日誌紀錄且向使用者和管理者發出警示。

(2) 通過：(1)項結果符合。

(3) 不通過：(1)項結果不符合。

(4) 不適用：無。

參考資料

(1) IoT-1006-1 v0.3: 門禁系統資安標準-第一部：一般要求

(2) 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

(3) CAPEC, 1000-Mechanisms of Attack, https://capec.mitre.org/data/definitions/1000.html

(4) ETSI TS 103 701 V1.1.1- Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements, https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

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 12 月 4 號	內容修訂。