

建築物昇降設備(電梯)資安檢測技術規範

1. 適用範圍及電梯網路通訊系統架構

1.1 適用範圍

本技術規範之適用範圍如圖 1 中的電梯控制板及其相關介面之網路安全要求，相關搭配使用之行動應用 App 與後端管理系統則非屬適用範圍。

本技術規範所規定的資訊安全要求，目的在確認電梯控制板具有基礎資訊安全防護能力，包含：(1)實體安全、(2)系統安全、(3)軟/韌體更新、(4)通訊安全、(5)身分鑑別與授權機制安全，以確保電梯控制板之資訊安全。

1.2 電梯網路通訊系統架構

近年物聯網蓬勃發展，電梯也朝著智慧化與雲端化邁進，透過電梯廂體內部或周邊擺置相關感測器蒐集數據，將保養參數透過網路傳送回電梯大樓管理室或電梯供應商之伺服器，搭配大數據運算來評估與預測電梯是否該進行維修；亦或結合行動應用 App 操作即可控制電梯開啟、關閉、或預訂電梯樓層等應用，於此同時相關資安風險亦伴隨而來。

本技術規範參照國際相關資安標準/規範並針對電梯網路通訊系統中資安關鍵設備「電梯控制板」訂定相關資訊安全要求。電梯系統之電梯控制板可能透過感測器收集數據並將資料透過網路通訊方式回傳至電梯大樓管理室或連上網際網路回傳資料至電梯供應商或電梯系統整合商的伺服器。圖 1 為電梯網路通訊系統架構示意圖，其中電梯控制板接受來自外部相關控制指令，並連接馬達或警報器等裝置來輸出控制馬達轉動方向或產生警報等功能。

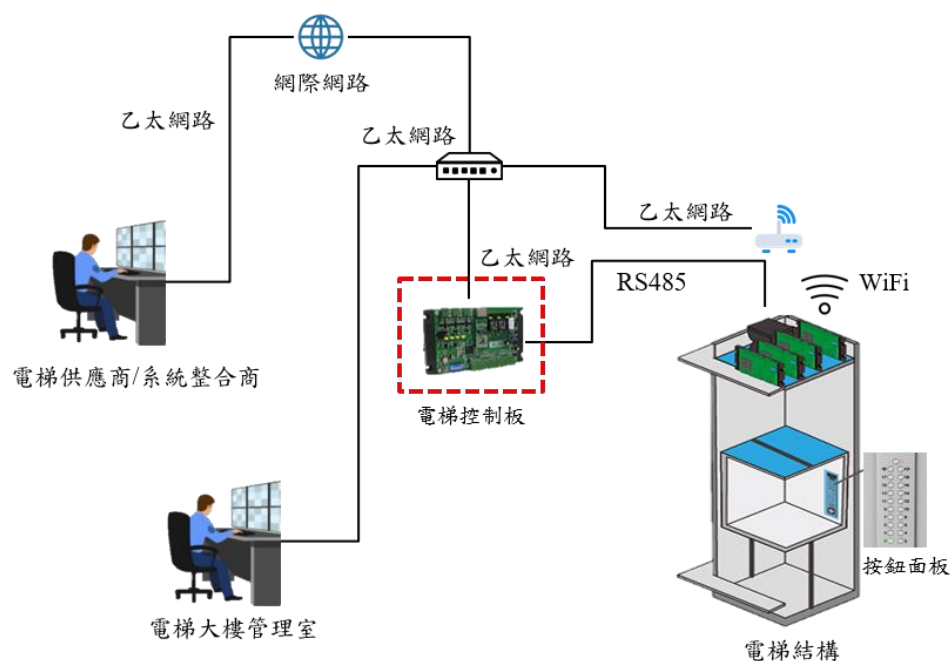


圖 1 電梯網路通訊系統架構示意圖

2. 引用標準

下列標準因本技術規範所引用，成為本技術規範之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)，無加註年分者，適用該最新版(包括補充增修)。

ISO 8102-20 : 2022	Electrical Requirements for Lifts, Escalators and Moving Walks - Part 20 : Cybersecurity
IEC 62351-5 : 2013	Power Systems Management and Associated Information Exchange – Data and Communications Security – Part 5: Security for IEC 60870-5 and Derivatives
IEC 62443-3-3 : 2013	Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels
CNS 62443-4-1	工業自動化及控制系統之安全性 – 第 4-1 部：產品開發生命週期之安全要求事項

IEC 62443-4-2 : 2019	Security for Industrial Automation and Control Systems – Part 4-2: Technical Security Requirements for IACS Components
FIPS PUB 140-2 Annex A : 2021	Security Requirements for Cryptographic Modules
NIST SP 800-52 Revision 2 : 2019	Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
NIST 800-140C : 2021	CMVP Approved Security Functions
NIST 800-131A : 2019	Transitioning the Use of Cryptographic Algorithms and Key Lengths
UL 2900-1 : 2017	Software Cybersecurity for Network Connectable Products, Part 1 : General Requirements

3. 用語及定義

3.1 鑑別符(authenticator)

用以確認個體身分之方法，如通行碼(password)、USB 隨身碟保存符記(token)或感應磁卡等當作電梯產品的授權身分驗證鑑別符。

3.2 密碼套件(cipher suite)

係指使用於安全通道(Secure Sockets Layer / Transport Layer Security, SSL/TLS)上用以協商安全設定之一系列安全機制，包括：身分，驗證、加密、訊息鑑別碼(Message Authentication Code, MAC)及金鑰交換演算法。

3.3 共同脆弱性及曝露(common vulnerabilities and exposures, CVE)

由美國非營利組織 MITRE Corporation 所屬之 National Cybersecurity FFRDC 所營運維護脆弱性管理計畫，針對每一資訊安全脆弱性項目給予全球認可之唯一共通編號。

3.4 共同脆弱性評分系統(common vulnerability scoring system, CVSS)

依資訊安全脆弱性之特點與影響進行評分之系統。由美國國家基礎建設諮詢委員會負責研究(National Infrastructure Advisory Council, NIAC)發起，現由美國資訊安全事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)提供的脆弱性評分系統，以衡量軟體脆弱性的特徵及嚴重性進行評分。

3.5 昇降設備(電梯)控制板(lifting equipment (elevator) control panel)

電梯控制板可接受來自外部相關操作指令，並連接馬達或警報器等裝置來輸出控制馬達的轉動方向或產生警報等功能。目前電梯控制板的主要樣態可分為兩大類：(1) 採用微控制器或微處理器為主計算

單元的控制板；(2) 基於可程式化邏輯控制器（PLC）的控制板。電梯控制板可經由工業控制 I/O 介面（例如：RS232 或 RS485）與其它硬體元件相互溝通，也可經由網路介面（例如：乙太網路或 WiFi）連接至建築物的內部網路或外部網際網路。

3.6 通行碼(password)

指一組能讓使用者使用系統或用以識別使用者身分之字元串，例包括：本機儲存資料加密檔案通行碼密碼、自身帳號及通行碼密碼、遠端網路服務帳號及通行碼密碼。

3.7 個人資料(personal information)

依「個人資料保護法」第 2 條第 1 款定義為自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

3.8 重送攻擊(replay attack)

指一種網路攻擊手法，透過惡意重複或拖延正常的資料傳輸而實施。

3.9 遠端登入(remote login)

指操作者以遠端操作控制板前應先鑑別身分的一種機制。

3.10 遠端操作(remote operation)

指操作者可以不受限於地理因素而達到操作控制板之目的。操作者與控制板通常未同時位於相同的地理區域中，例如：相異的樓層、相異的建築物或相異的實體空間中。操作者以直接或間接方式經由網路介面對控制板遠端地進行資料讀取、參數更新、命令與資料傳遞，以及其它操作行為。

3.11 敏感性資料(sensitive data)

指洩漏時可能對使用者或電梯供應商之權益造成損害之資料，包括

但不限於個人資料、通行碼、關鍵控制指令、保養參數、金鑰或地理位置等。此等資料依使用者行為於電梯控制板及其附屬儲存媒體之建立、儲存或傳輸。

4.安全構面與資訊安全要求

4.1 安全構面

本技術規範包含電梯控制板之實體安全、系統安全、軟/韌體更新、通訊安全，以及身分鑑別與授權機制安全等構面，說明如下：

- (a) 實體安全：電梯控制板的實體介面需有一定防禦能力，如外加箱體保護並有鎖扣等機制設計。電梯控制板應建立拆除障礙並應關閉非必要之實體埠，以降低駭客透過實體介面入侵或竄改資料的風險。
- (b) 系統安全：確保系統的防禦能力，包含已知脆弱性掃描、軟/韌體原始碼之資安防護、事件日誌功能等。
- (c) 軟/韌體更新：電梯控制板之軟/韌體版本更新服務等，須具備足夠安全防護。電梯控制板之系統或軟/韌體等，亦應具備足夠之資訊安全防護。
- (d) 通訊安全：電梯控制板與傳輸之資料應具有足夠安全之防護，避免遭受蓄意人士入侵。電梯控制板之通訊應採已知最佳實踐方式架構，對敏感性資料之傳輸，亦應加密保護，以確保通訊安全。
- (e) 身分鑑別與授權機制安全：對每個可遠端操作電梯控制板須建立識別、鑑別與授權機制，以及權限控管相關機制，包括遠端指令管理介面、通訊協定、重送攻擊等，應具備一定防護能力，以防止人員存取未經授權之資料或進行權限外之操作。

4.2 資訊安全等級

本技術規範將各項資訊安全要求等級依(1)相關資安風險高低、(2)技

術實現複雜度綜合考量，分為 1 級、2 級，1 級之預期效果為防止無心之操作誤會、不成熟之攻擊行為或無足夠資源之蓄意攻擊行為；2 級則預期能防止蓄意且有資源之攻擊行為。對於資訊安全等級之說明，整理於表 1。

表 1 電梯之資訊安全等級說明

資訊安全等級	說明	備考
1 級	防止無心之操作誤會、不成熟之攻擊行為或攻擊者無足夠資源之蓄意攻擊行為。	電梯之基礎資訊安全要求。
2 級	防止蓄意且有資源之攻擊行為。	電梯之進階資訊安全要求。

4.3 安全構面與要求概述

安全構面與要求如表 2 所示，第 1 欄為安全構面，包含：(1)實體安全、(2)系統安全、(3)軟/韌體更新、(4)通訊安全、(5)身分鑑別與授權機制安全；第 2 欄為資訊安全要求，係依第 1 欄安全構面設計之對應安全要求；第 3 欄為安全要求項目，須依循第 5 節所規定內容。各資訊安全要求相應之標準規範要求事項對照表，彙整於附錄 A。

4.4 資安要求檢測方式

屬適用範圍之電梯控制板於測試前，需填具自我檢查表，並提供各測試項目之自我檢查、相關說明及相應之佐證資料，自我檢查表格式如附錄 C。針對電梯控制板之資安要求與檢測方式，如附錄 D 所示。

表 2 安全構面與資訊安全要求總表

安全構面	資訊安全要求	安全要求項目	資訊安全等級	
			1 級	2 級
5.1 實體安全	5.1.1 實體介面最小化要求	5.1.1.1	V	V
	5.1.2 防止未經授權實體操作	5.1.2.1	V	V
		5.1.2.2		V
5.2 系統安全	5.2.1 最小權限	5.2.1.1	V	V
	5.2.2 事件日誌	5.2.2.1		V
		5.2.2.2		V
	5.2.3 軟/韌體安全性評估	5.2.3.1	V	V
		5.2.3.2	V	V
	5.2.4 敏感性資料儲存	5.2.4.1	V	V
		5.2.4.2		V
5.3 軟/韌體更新	5.3.1 更新安全	5.3.1.1	V	V
		5.3.1.2		V
	5.3.2 安全版本	5.3.2.1	V	V
		5.3.2.2		V
5.4 通訊安全	5.4.1 傳輸資料保護	5.4.1.1		V
		5.4.1.2	V	V
5.5 身分鑑別與授權機制安全	5.5.1 身分鑑別	5.5.1.1	V	V
		5.5.1.2	V	V
		5.5.1.3		V
		5.5.1.4		V
		5.5.1.5		V
	5.5.2 帳戶管理	5.5.2.1	V	V
	5.5.3 存取控制	5.5.3.1	V	V

5. 資訊安全要求

本節詳盡載明電梯控制板為滿足安全功能應採取的方法，電梯控制板應符合本節中所有資訊安全基本要求。

5.1 實體安全

5.1.1 實體介面最小化要求

5.1.1.1 電梯控制板應移除不需使用的介面及序列埠。

5.1.2 防止未經授權實體操作

5.1.2.1 電梯控制板本體應建立外殼拆除障礙或保有實體遭拆解之紀錄。

5.1.2.2 電梯控制板之保護外殼若有被未經授權打開應有告警機制。

5.2 系統安全

5.2.1 最小權限

5.2.1.1 電梯控制板僅使用最少必要的通訊埠。

5.2.2 事件日誌

5.2.2.1 電梯控制板應具安全日誌功能並紀錄事件。

5.2.2.2 電梯控制板發生異常安全事件時，應具備主動告警機制，包括回報管理者或推播警示、告警等訊息。

5.2.3 軟/韌體安全性評估

5.2.3.1 電梯控制板不應存在美國國家弱點資料庫所公開的常見弱點與脆弱性資料 CVE，且共同脆弱性評分系統 CVSS 最新版本之分數評比 7 分以上或嚴重性等級評比為高(High)以上者。

5.2.3.2 電梯控制板之軟/韌體程式碼應進行靜態分析確認無存在嚴重性資安弱點。

5.2.4 敏感性資料儲存

5.2.4.1 電梯控制板所儲存之敏感性資料應加密儲存。

5.2.4.2 電梯控制板所儲存之敏感性資料其加密方式應採用符合 FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或 NIST SP 800-131A 規定之同等或以上強度的加密演算法。

5.3 軟/韌體更新

5.3.1 更新安全

5.3.1.1 電梯控制板若有進行軟/韌體更新時，即使發生更新失敗，系統應仍能回復正常運作。

5.3.1.2 電梯控制板之軟/韌體更新，其軟/韌體應具保護機制，使軟/韌體之程式碼無法被解析；若採安全通道進行更新，則安全通道版本及密碼套件應符合附錄 B 之要求。

5.3.2 安全版本

5.3.2.1 電梯控制板的軟/韌體版本應受管制。

5.3.2.2 電梯控制板供應商應能提供每個軟/韌體的加密雜湊值作為軟/韌體版本之追溯管控。

5.4 通訊安全

5.4.1 傳輸資料保護

5.4.1.1 敏感性資料應加密傳輸，若採安全通道進行傳輸，其版本及密碼套件應符合附錄 B 的要求。

5.4.1.2 電梯控制板連接網路時，不應對未宣告的 IP 進行封包傳輸。

5.5 身分鑑別與授權機制安全

5.5.1 身分鑑別

5.5.1.1 遠端操作電梯控制板之功能時應先通過身分鑑別機制。

5.5.1.2 使用者之初次鑑別若採公開取得之預設通行碼，則各產品之預設通行碼應相異，或於首次遠端登入後，應有強制使用者變更預設通行碼之機制。

5.5.1.3 對於遠端登入之身分鑑別所使用之通行碼強度應有一定規則之要求，以避免被輕易破解並遭不當利用。

5.5.1.4 進行遠端操作電梯控制板之功能時，應具防止重送攻擊之機制。

5.5.1.5 若使用者在多次嘗試遠端登入電梯控制板失敗後，電梯控制板將暫時或永久拒絕該使用者的請求，登入次數與鎖定時間應可設定。

5.5.2 帳戶管理

5.5.2.1 遠端操作電梯控制板之功能時，若以帳戶與通行碼作為身分鑑別機制，則不可包含常見預設帳戶。

5.5.3 存取控制

5.5.3.1 遠端操作電梯控制板之功能時應能設置白名單，僅允許特定主機可存取控制。

附錄 A (參考)

標準規範要求事項對照表

安全要求 項目	IEC 62443 系列	其他相關資訊安全規範
5.1.1.1	CNS 62443-4-1 SD-4	
5.1.2.1	IEC 62443-4-2 CR 3.11 、 IEC 62443-4-2 EDR3.11	
5.1.2.2	IEC 62443-4-2 EDR 2.13	
5.2.1.1	IEC 62443-3-3 SR 7.7	
5.2.2.1	IEC 62443-4-2 CR 1.12	
5.2.2.2	IEC 62443-3-3 SR 3.3	
5.2.3.1	CNS 62443-4-1 SVV-3 、 CNS 62443-4-1 DM-3	
5.2.3.2	CNS 62443-4-1 SI-1	
5.2.4.1	IEC 62443-4-2 CR 4.1	
5.2.4.2	IEC 62443-4-2 CR 1.7	FIPS PUB 140-2 Annex A 、 NIST SP 800-140C 、 NIST SP 800-131A
5.3.1.1	IEC 62443-3-3 SR 7.4	
5.3.1.2	CNS 62443-4-1 SUM-4	IEC 62351-5 5.4.10 、 NIST SP 800-52
5.3.2.1	IEC 62443-4-2 CR 1.2	
5.3.2.2	CNS 62443-4-1 SUM-4	
5.4.1.1	IEC 62443-3-3 SR 4.1 、 IEC 62443-3-3 SR 4.3	IEC 62351-5 5.4.10 、 NIST SP 800-52
5.4.1.2	IEC 62443-4-2 FR 5	
5.5.1.1	IEC 62443-4-2 EDR 2.13 、	

安全要求 項目	IEC 62443 系列	其他相關資訊安全規範
	IEC 62443-4-2 NDR 1.13	
5.5.1.2	IEC 62443-4-2 CR 1.5	
5.5.1.3	IEC 62443-3-3 SR 1.7 、 IEC 62443-4-2 CR 1.7	UL 2900-1 8.3(b) 、 8.3(c)
5.5.1.4	IEC 62443-3-3 SR 3.8 、 IEC 62443-4-2 CR 3.8	
5.5.1.5	IEC 62443-3-3 SR 1.11 、 IEC 62443-4-2 CR 1.11	
5.5.2.1	CNS 62443-4-1 SG-6	
5.5.3.1	IEC 62443-3-3 SR 5.2 RE 1	

附錄 B (規定) 安全通道版本及密碼套件使用要求

指超文件傳輸協定(HTTP)結合安全接套層協定(SSL)或傳輸層安全性協定(TLS)，建立安全通道以保護傳輸中資料不被竊取之技術；然而安全接套層協定在 2014 年 10 月由 Google 指出其資訊安全脆弱性，宣布將全面禁用，所以已經完全由傳輸層安全性協定取代安全接套層協定。但傳輸層安全性協定 v1.0 同樣不被信任，因此目前本技術規範應使用的版本為：傳輸層安全性協定 v1.2 同等或以上之版本。

以下為各版本安全通道(TLS)可選用之密碼套件：

- TLSv1.2
 - TLS_ECDHE_ECDSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
 - TLS_ECDHE_ECDSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES256_SHA384
 - TLS_ECDHE_RSA_WITH_AES256_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES128_SHA256
 - TLS_ECDHE_RSA_WITH_AES128_SHA256
- TLSv1.3
 - TLS_AES_128_GCM_SHA256
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_CCM_SHA256
 - TLS_AES_128_CCM_8_SHA256

附錄 C

建築物昇降設備(電梯)控制板自我檢查表

基本資訊			
申請單位：		填表日期：	
廠牌：		型號及板號：	
是否具備網路通訊傳輸實體介面？	<input type="checkbox"/> 具有網路通訊傳輸介面 <input type="checkbox"/> 未具有網路通訊傳輸介面	軟/韌體版本：	
網路通訊介面類型	<input type="checkbox"/> 不適用(未具有網路通訊傳輸介面) <input type="checkbox"/> 具內網通訊/介面類型： _____ <input type="checkbox"/> 具網際網路之外網通訊/介面類型： _____		
是否可被遠端操作	<input type="checkbox"/> 是，其功能為何？ _____ <input type="checkbox"/> 否 (請提供佐證資料)		

產品名稱	安全要求	安全要求項目	資安等級	自我檢查	附加說明或佐證
電梯控制板	5.1.1 實體介面最小化要求	5.1.1.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
	5.1.2 防止未經授權實體操作	5.1.2.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.1.2.2	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
	5.2.1 最小權限	5.2.1.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.2.2 事件日誌	5.2.2.1	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.2.2.2	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

產品名稱	安全要求	安全要求項目	資安等級	自我檢查	附加說明或佐證
	5.2.3 軟/硬體 安全性評估	5.2.3.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		5.2.3.2	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
	5.2.4 敏感性資料儲存	5.2.4.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.2.4.2	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.3.1 更新安全	5.3.1.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.3.1.2	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
	5.3.2 安全版本	5.3.2.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.3.2.2	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.4.1 傳輸資料 保護	5.4.1.1	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		5.4.1.2	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	

產品名稱	安全要求	安全要求項目	資安等級	自我檢查	附加說明或佐證
	5.5.1 身分鑑別	5.5.1.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.5.1.2	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.5.1.3	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
		5.5.1.4	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
		5.5.1.5	2	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	5.5.2 帳戶管理	5.5.2.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合	
	5.5.3 存取控制	5.5.3.1	1	<input type="checkbox"/> 符合 <input type="checkbox"/> 不符合 <input type="checkbox"/> 不適用	
	※佐證資料：				
※若說明欄格位不足時，可以附註方式將必要資訊呈現於此欄位，本欄位不限格式、可自行延伸。					

附錄 D

建築物昇降設備(電梯)控制器之資安要求與檢測方式

資安要求	說明	檢測方式	結果	等級
5.1.1 實體介面 最小化要求	5.1.1.1 電梯控制板應 移除不需使用的 介面及序列埠。	1.廠商應提供文件說明實體介面之目的及相關保護措施。 2.檢視待測物外觀並清點實體介面，其結果應與廠商之說明文件相符，否則本項不符合。 3.如存有非必要之實體介面未移除，則應預設關閉或採實體保護，否則本項不符合。	1.符合 2.不符合	1
5.1.2 防止未經 授權實體 操作	5.1.2.1 電梯控制板本 體應建立外殼 拆除障礙或保有 實體遭拆解之紀錄。	1.檢視待測物之外殼，應一體成形、或具實體鎖、或設計於可上鎖之箱體內、或採防拆螺絲、或使用一次性貼紙，以建立拆除障礙。 ※備考： 若待測物無箱體或外殼，則廠商應提供說明文件敘述產品之實體保護機制(如廠商可於使用手冊內宣告將電梯控制板置放在有防拆機櫃並上鎖)。	1.符合 2.不符合	1
	5.1.2.2 電梯控制板之 保護外殼若有 被未經授權打 開應有告警機 制。	1.嘗試以未經授權的方式開啟控制板之外殼，觀察是否有告警機制。	1.符合 2.不符合	2

資安要求	說明	檢測方式	結果	等級
5.2.1 最小權限	5.2.1.1 電梯控制面板僅使用最少必要的通訊埠。	1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。 2.廠商應於自我宣告表中說明待測物開通之通訊埠與開通原因。 3.啟用之通訊埠應符合最少權限原則，若存在非必要之通訊埠或未能提供說明者，則本項不符合。 4.將待測物與測試電腦連接，啟用具網路埠掃描功能之工具，對待測物執行 TCP 埠、UDP 埠及埠 0 之掃描。 5.比對掃描結果應與廠商說明一致，否則本項不符合。	1.符合 2.不符合 3.不適用	1

資安要求	說明	檢測方式	結果	等級
5.2.2 事件日誌	5.2.2.1 電梯控制板應具安全日誌功能並紀錄事件。	<p>1.安全日誌可存在於待測物(本地端)或遠端內。</p> <p>2.安全日誌應至少包含：</p> <p>(1) 軟/韌體更新紀錄</p> <p>(2)緊急/異常事件</p> <p>(3)重大影響之控制命令(如有遠端操作功能)。</p> <p>且每一事件應可由紀錄中辨識事件時間、事件種類與誘發事件之來源身份(可能為人員或設備)。</p> <p>3.安全日誌之存取應設有權限管理。廠商應說明存取安全日誌之操作方式，並提供具存取權限之帳號與鑑別符。</p> <p>4.檢視安全日誌，其內容應符合第 2 點之要求，否則本項不符合。</p>	<p>1.符合</p> <p>2.不符合</p>	2

資安要求	說明	檢測方式	結果	等級
	<p>5.2.2.2</p> <p>電梯控制板發生異常安全事件時，應具備主動告警機制，包括回報管理者或推播警示、告警等訊息。</p>	<p>1.若電梯控制板不具有遠端操作功能，則本項可申明為不適用。</p> <p>2.廠商應提供自定義異常安全事件之說明。異常安全事件包含但不限於：</p> <p>(1)輸入通行碼超過頻次限制。</p> <p>(2)非白名單上之主機嘗試進行遠端登入。</p> <p>3.廠商應說明待測物發生異常安全事件時的告警機制。</p> <p>4.觸發異常登入安全事件，並檢視待測物之告警機制，其結果應與廠商說明一致，否則本項不符合。</p>	<p>1.符合</p> <p>2.不符合</p> <p>3.不適用</p>	2
<p>5.2.3</p> <p>軟 / 韌 體</p> <p>安全性評估</p>	<p>5.2.3.1</p> <p>電梯控制板不應存在美國國家弱點資料庫所公開的常見弱點與脆弱性資料 CVE，且共同脆弱性評分系統 CVSS 最新版本之分數評比 7 分以上或嚴重性等級評比為高(High)以上者。</p>	<p>1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。</p> <p>2.使用弱點識別工具對待測物進行弱點掃描，脆弱性識別應依共同脆弱性評分系統(CVSS)進行判定。</p> <p>3.若測得共同脆弱性及暴露(CVE)編號之漏洞，且其 CVSS 最新版本之分數大於等於 7 (或嚴重等級為 High 或 Critical 者)則本項不符合。</p> <p>4.若帶有中等級之脆弱性，廠商應能提供合理管控措施，否則本項不符合。</p>	<p>1.符合</p> <p>2.不符合</p> <p>3.不適用</p>	1

資安要求	說明	檢測方式	結果	等級
	5.2.3.2 電梯控制板之軟/韌體程式碼應進行靜態分析確認無存在嚴重性資安弱點。	<p>1.應由檢測方評估後採以下其中一種方式取得電梯控制板軟/韌體程式源碼靜態分析資訊：</p> <p>(1)廠商能提供電梯控制板軟/韌體程式源碼經靜態程式碼分析之證明與相關檢測報告，由檢測方確認廠商使用之工具種類、工具比對資料庫與相關設定之合理性。</p> <p>(2)廠商提供電梯控制板之軟/韌體程式源碼(source code)由檢測方進行靜態程式碼分析。</p> <p>2.對標的檔案進行靜態程式碼弱點分析。分析工具應可識別共同弱點(CWE)或共同脆弱性(CVE)並比對弱點或脆弱性評分系統(CWSS/CVSS)以進行等級判定。</p> <p>3.若測得具共同弱點/脆弱性(CWE/CVE)編號之漏洞，且其CWSS/CVSS分數大於等於7(或嚴重等級為High或Critical者)，廠商應能提供合理管控措施並說明之，否則本項不符合。</p>	<p>1.符合</p> <p>2.不符合</p>	1

資安要求	說明	檢測方式	結果	等級
5.2.4 敏感性資料儲存	5.2.4.1 電梯控制板所儲存之敏感性資料應加密儲存。	1. 敏感性資料包括但不限於金鑰、憑證、關鍵數據、身分鑑別資訊(如使用者帳號、通行碼)及含有使用者隱私之資料，廠商應提供自定義敏感性資料之說明。 2. 敏感性資料儲存於待測物時，應先進行加密。廠商應提供說明佐證待測物具備該保護機制，並提供存取敏感性資料之方式及路徑。 3. 嘗試存取敏感性資料，其內容應為密文之形式，否則本項不符合。	1. 符合 2. 不符合	1
	5.2.4.2 電梯控制板所儲存之敏感性資料其加密方式應採用符合 FIPS PUB 140-2 Annex A、NIST SP 800-140C 或 NIST SP 800-131A 規定之同等或以上強度的加密演算法。	1. 若電梯控制板未儲存敏感性資料，則本項可申明為不適用。 2. 廠商應提供待測物所儲存之敏感性資料加密保護演算法作為審查依據。 3. 依廠商提供之演算法及密鑰對敏感性資料進行加密，所得結果應與儲存於待測物中之敏感性資料密文一致；廠商若無法提供密鑰，則應提供資料佐證之。	1. 符合 2. 不符合 3. 不適用	2

資安要求	說明	檢測方式	結果	等級
5.3.1 更新安全	5.3.1.1 電梯控制板若有進行軟/韌體更新時，即使發生更新失敗，系統應仍能回復正常運作。	1.對廠商提供之軟/韌體檔案進行修改，或以其他來源之軟/韌體對待測物進行更新，更新程序中應有查覺軟/韌體錯誤之機制，能拒絕更新或有立即警示之設計，否則本項不符合。 2.遇有更新中斷之情形(如斷開電源或通訊連線)，待測物應能回復更新前之狀態或進入待機狀態。待測物重新完成更新後應能正常運作。	1.符合 2.不符合	1
	5.3.1.2 電梯控制板之軟/韌體更新，其軟/韌體應具保護機制，使軟/韌體之程式碼無法被解析；若採安全通道進行更新，則安全通道版本及密碼套件應符合附錄 B 之要求。	1.若待測物之軟/韌體採安全通道進行更新，則安全通道版本及密碼套件應合於附錄 B 之要求，否則本項不符合。 2.若待測物非採安全通道進行軟/韌體更新，則軟/韌體應加密保護，或無法經由反組譯解出軟/韌體之明文程式碼。	1.符合 2.不符合	2

資安要求	說明	檢測方式	結果	等級
5.3.2 安全版本	5.3.2.1 電梯控制板的軟/韌體版本應受管制。	1.廠商應提供資料佐證軟/韌體版本之序號受管制(如：序號編碼方式、序號清單管制文件)。 2.廠商應提供查詢待測物軟/韌體版本資訊之操作說明，而操作後所查得之版本應與廠商所提供之資料相符。	1.符合 2.不符合	1
	5.3.2.2 電梯控制板供應商應能提供每個軟/韌體的加密雜湊值作為軟/韌體版本之追溯管控。	1.軟/韌體若採安全通道方式進行更新，則本項可申明為不適用。 2.廠商應提供軟/韌體版本與其加密雜湊值對照表，並置於網站上或使用者可取得之處。 3.依廠商所述之方式加密軟/韌體後，所得加密雜湊值應與對照表一致，否則本項不符合。 ※備考： 廠商亦可提供詳細資料，說明內部自訂的軟/韌體版本管控機制。廠商自訂的管控機制須能有效地察覺軟/韌體內容已受到變更。	1.符合 2.不符合 3.不適用	2

資安要求	說明	檢測方式	結果	等級
5.4.1 傳輸資料 保護	5.4.1.1 敏感性資料應加密傳輸，若採安全通道進行傳輸，其版本及密碼套件應符合附錄 B 的要求。	1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。 2.建立待測物之網路通道，並進行相關操作以觸發待測物之網路行為。 3.廠商應提供針對敏感性資料傳輸加密之機制。 4.查看傳輸具敏感性資料之網路封包，其應受加密保護；若採用安全通道進行傳輸，則安全通道版本及密碼套件應符合附錄 B 之要求。	1.符合 2.不符合 3.不適用	2
	5.4.1.2 電梯控制板連接網路時，不應對未宣告的 IP 進行封包傳輸。	1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。 2.廠商應宣告待測物預期會連結之伺服器 IP 位址或網域名稱及其他可能位置。 3.將待測物連接至網際網路並與測試電腦處於同一網域，持續以測試電腦監聽側錄往來待測物之封包至少 24 小時。 4.檢查側錄之封包，其目的地位址應與廠商所宣告之內容相符，否則本項不符合。	1.符合 2.不符合 3.不適用	1

資安要求	說明	檢測方式	結果	等級
5.5.1 身分鑑別	5.5.1.1 遠端操作電梯 控制板之功能 時應先通過身 分鑑別機制。	1.待測物之存取(遠端登入)及進入除錯模式(若具備除錯模式)應具備身分鑑別機制，且其鑑別符不可公開取得(預設通行碼除外)。 2.廠商應提供存取待測物及進入除錯模式之操作方式。 3.待測物於進入除錯模式或接受控制命令(與人員生命財產安全相關之緊急命令則不在此限)時，應能要求身分鑑別，並於通過鑑別後得觸發相應之行為。	1.符合 2.不符合	1
	5.5.1.2 使用者之初次 鑑別若採公開 取得之預設通 行碼，則各產 品之預設通行 碼應相異，或 於首次遠端登 入後，應有強 制使用者變更 預設通行碼之 機制	1.審閱產品之預設通行碼設計文件，檢視產品是否存在相同之預設通行碼，若相異則本項符合。 2.若存有相同之產品預設通行碼，則首次登入成功後，系統應要求更改預設通行碼，否則本項不符合。 3.首次登入成功而被要求更改通行碼時，仍採預設通行碼做設定，若可成功設定，則本項為不符合。	1.符合 2.不符合	1

資安要求	說明	檢測方式	結果	等級
	<p>5.5.1.3</p> <p>對於遠端登入之身分鑑別所使用之通行碼強度應有一定規則之要求，以避免被輕易破解並遭不當利用。</p>	<p>1.若通行碼為人員使用者自行定義，則通行碼之複雜性要求應符合下列最小需求：(A)不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元；(B)長度至少為 8 個字元；(C)包含下列 4 種字元中的 3 種：</p> <p>(1)英文大寫字元 (A 到 Z)</p> <p>(2)英文小寫字元 (a 到 z)</p> <p>(3)十進位數字 (0 到 9)</p> <p>(4)非英文字母字元(例如：!、\$、#、%)</p> <p>2.檢視廠商說明並進行相應帳號登入操作，若通行碼要求與廠商說明相符，則本項符合。</p>	<p>1.符合</p> <p>2.不符合</p>	2
	<p>5.5.1.4</p> <p>進行遠端操作電梯控制板之功能時，應具防止重送攻擊之機制。</p>	<p>1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。</p> <p>2.以廠商提供之測試用帳號與鑑別碼登入待測物，側錄待測物與遠端主機間之通訊封包，並擷取其交談識別碼。</p> <p>3.登出帳號。</p> <p>4.將前步驟中之交談識別碼，透過測試工具執行重送攻擊，待測物應能拒絕之。</p>	<p>1.符合</p> <p>2.不符合</p> <p>3.不適用</p>	2

資安要求	說明	檢測方式	結果	等級
	<p>5.5.1.5</p> <p>若使用者在多次嘗試遠端登入電梯控制面板失敗後，電梯控制面板將暫時或永久拒絕該使用者的請求，登入次數與鎖定時間應可設定。</p>	<p>1.若待測物不以通行碼作為其身份鑑別之方式，則本項可申明為不適用。</p> <p>2.除廠商特意申明之「最低權限使用者」(如僅具閱覽展示資訊之權限)，其餘使用者之通行碼輸入錯誤容許次數應為 5 次(含)以下，超過容許之登入次數時，介面應有重置或時間間隔鎖定機制。</p> <p>3.依廠商提供之測試帳號及通行碼登入待測物，應能成功登入。後以錯誤之通行碼再登入，應登入失敗，且超過通行碼輸入錯誤容許次數後，應有重置或時間間隔鎖定機制，否則本項不符合。</p>	<p>1.符合</p> <p>2.不符合</p> <p>3.不適用</p>	2
5.5.2 帳戶管理	<p>5.5.2.1</p> <p>遠端操作電梯控制面板之功能時，若以帳戶與通行碼作為身分鑑別機制，則不可包含常見預設帳戶。</p>	<p>輸入常見預設帳號 (root、admin、administrator、user、guest)於登入介面中，待測物應無法識別之。</p>	<p>1.符合</p> <p>2.不符合</p>	1

資安要求	說明	檢測方式	結果	等級
5.5.3 存取控制	5.5.3.1 遠端操作電梯控制板之功能時應能設置白名單，僅允許特定主機可存取控制。	1.若待測物不具有網路通訊相關介面，則本項可申明為不適用。 2.廠商應提供相關文件，說明待測物設置白名單之操作方式。設定幾組主機之 IP 或 MAC address 於控制板之白名單。 3.嘗試以非白名單內之 IP 或 MAC address 存取待測物，待測物應拒絕存取。	1.符合 2.不符合 3.不適用	1