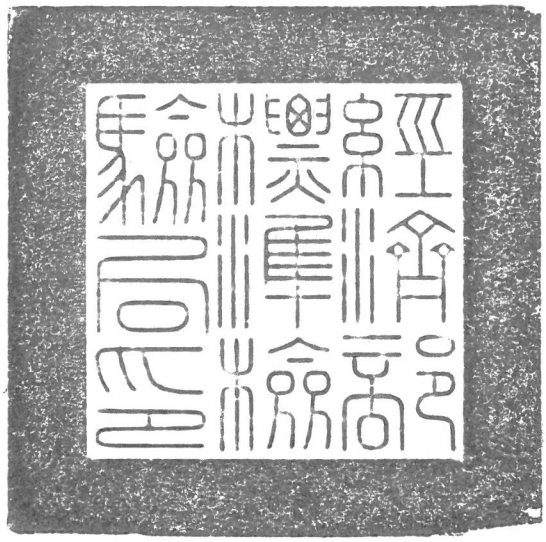
檔　　號：
保存年限：

經濟部標準檢驗局　公告

發文日期：中華民國113年6月7日
發文字號：經標檢驗字第11340005570號
附件：儲能電力轉換系統之資安檢測技術規範



主旨：公告「儲能電力轉換系統之資安檢測技術規範」。

依據：自願性產品驗證實施辦法第四條第三項。

公告事項：如附「儲能電力轉換系統之資安檢測技術規範」。

局長 陳怡鈴

裝

訂

線

儲能電力轉換系統之資安檢測技術規範
（113 年 6 月版）

目錄

圖目錄

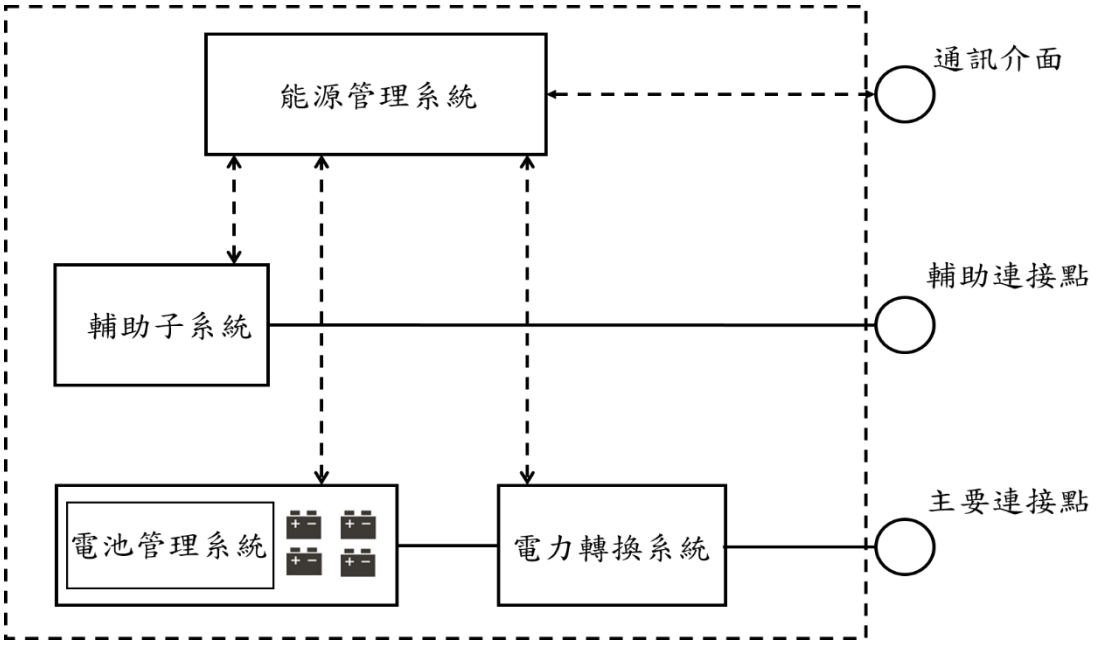
表目錄

1. 儲能系統之簡介

再生能源可減少碳排量，而達到環境保護之目的；不過，再生能源難以穩定地供給能源。舉例說明，太陽能發電須仰賴太陽的光能強度，但是太陽無法持續地保持一定的光能強度；在風力發電中也可能遭遇自然風力不足的情況。因此，產生再生能源時會發生電能的高峰期與低谷期，兩種失衡現象。儲能系統是一種可減緩上述困境之解決方案。當再生能源的產生出現高峰期時，過剩的再生能源可以保存在儲能電池中，而當再生能源的產生不足時，即可從儲能電池中提取電力。如此一來，儲能系統可有效地平衡再生能源產生的過程中所造成的失衡現象。

構成儲能系統的關鍵角色包含：儲能電池、電池管理系統、電力轉換系統，以及能源管理系統。能源管理系統具有監測、控制以及數據蒐集之功能，根據能源控制策略，可為儲能電池進行最佳化管理與分析。電力轉換系統實現交流電與直流電雙向轉換的功能，可控制與管理儲能電池的充電以及放電。電池管理系統可量測儲能電池的電壓以及監控與管理儲能電池的狀態，例如：過充電、過放電、過熱等其它異常現象。圖 1 顯示儲能系統架構之示意圖。

在儲能系統中，各個關鍵角色之間都會互相溝通，所以控制指令以及狀態資訊的來源性以及完整性應被列為較高優先考量之安全需求（通常也須伴隨資料的新鮮性 (freshness)，避免控制指令或狀態資訊被惡意重送）。來源性是為了確保控制指令以及狀態資訊來自於預期的傳送方，而完整性則是確保控制指令以及狀態資訊未被惡意地竄改。一旦缺乏上述兩項安全需求，儲能系統的裝置可能因為接受錯誤的控制指令而執行非預期的操作，亦或錯誤的狀態資訊可能導致完全相反的決策結果。



資料來源：CNS 62933-1:2021，本技術規範修改。

圖 1 儲能系統架構之示意圖

2. 適用範圍

本技術規範之適用對象為電力轉換系統。除了實現交流電與直流電的雙向轉換外，電力轉換系統還可搭配通訊模組向能源管理系統（或遠端主機）傳送或接收電力轉換資訊以及控制指令。通訊模組通常以內嵌或外掛的方式與電力轉換系統搭配，如圖 2 所示，其中虛線框劃分出本技術規範的適用範圍。

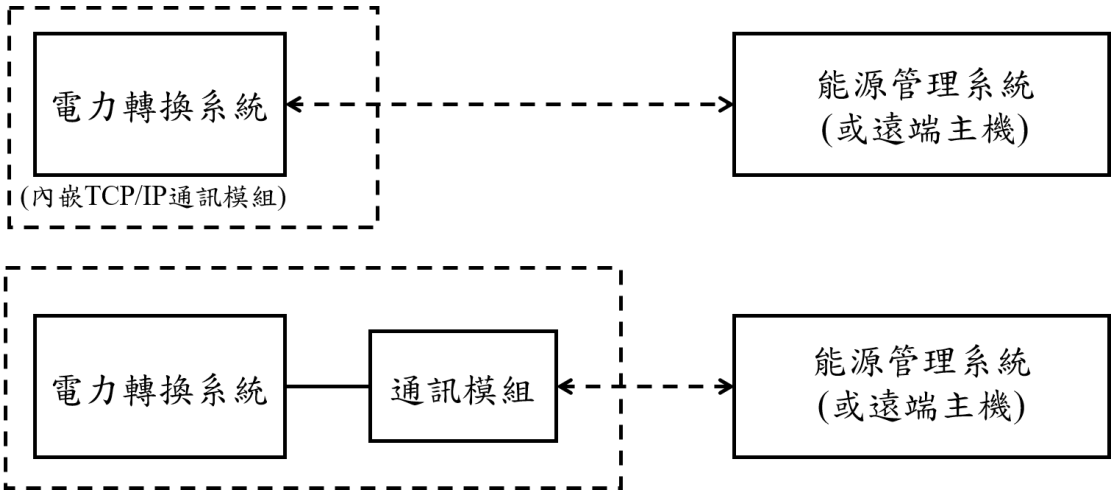


圖 2 電力轉換系統之通訊模式示意圖

3. 引用標準

下列標準之全部或部分，為本技術規範引用之相關文件，有加註年份時僅適用該版本，未加註時則適用該文件之最新版次(包含任何修訂)。

NISTIR 7628 Revision 1: 2014	Guidelines for smart grid cybersecurity － volume 1－smart grid cybersecurity strategy, architecture, and high-level requirements
NIST SP 800-82 Revision 2: 2015	Guide to industrial control systems (ICS) security － supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as programmable logic controllers (PLC)
NIST SP 800-82 Revision 3 (Draft): 2022	Guide to operational technology (OT) security
IEC 62443-4-2 Edition 1.0: 2019	Security for industrial automation and control systems － Part 4-2: technical security requirements for IACS components
CNS 62933-1:2021	電能儲存系統 (EESS)－第 1 部：詞彙

4. 用語及定義

4.1. 身分鑑別（authentication）

證實使用者所宣稱的身分。

4.2. 鑑別符（authenticator）

用以確認個體身分之方法或工具，例如：通行碼（password）、USB隨身碟保存符記（token）或感應磁卡等，作為身分授權之驗證鑑別符。

4.3. 電池管理系統（battery management system, BMS）

控制、監測以及優化儲能電池的系統，可蒐集儲能電池的電壓、電流、溫度以及其它狀態資訊，並且監測儲能電池是否發生過放電、過充電、過熱或其它異常現象。電池管理系統可將儲能電池的狀態資訊提供給能源管理系統進行管理以及儲存。

4.4. 密碼套件（cipher suite）

一系列的安全機制，包含：身分鑑別、加密與解密演算法、訊息鑑別碼（message authentication code, MAC）以及金鑰交換演算法，一般可被用來建立安全通道（例如：secure sockets layer 或 transport layer security, SSL 或 TLS）。

4.5. 共同脆弱性及曝露（common vulnerabilities and exposure, 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。

4.6. 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），現由美國資訊安全事件應變小組論壇（forum of incident response and security teams, FIRST）發展。

4.7. 通訊模組（communication module）

一種可提供網路通訊功能的裝置，此技術規範尤指建立在TCP/IP之上的網路通訊，通常以內嵌或外掛的方式與電力轉換系統結合，使電力轉換系統與外部主機或裝置之間能經由網路通訊相互傳遞資料。

4.8. 密碼系統（cryptosystem）

基於密碼學之演算法，包括加解密演算法、密碼雜湊演算法、數位簽章演算法以及金鑰協議演算法等。

4.9. 解密（decryption）

將加密資料恢復為原本的狀態。

4.10. 數位簽章（digital signature）

可為數位訊息或數位檔案產生相對應的簽章值，其可被用來驗證上述物件的完整性以及來源性。非對稱式金鑰密碼學是一種常被用來製作數位簽章的技術。NIST 186-5 納入多種數位簽章方法。

4.11. 加密（encryption）

將原文透過密碼式技術轉換成隱匿資料原始意義之密文，避免他人知悉或利用。

4.12. 能源管理系統（energy management system, EMS）

蒐集電池管理系統、電力轉換系統，以及儲能系統相關裝置之資訊與狀態。

4.13. 儲能系統（energy storage system, ESS）

由一個或數個儲能單元所構成，能夠提供電能給電網，並且由能源管理系統進行監測、控制以及保護。

4.14. 儲能單元（energy storage unit, ESU）

以鋰離子電池作為儲能載體，經由電力轉換系統儲存以及釋放電能的最小單元。儲能單元是由儲能電池、電池管理系統、電力轉換系統以及相關裝置所組成。

4.15. 金鑰管理（key management）

在密碼金鑰（cryptographic key）的生命週期中負責管理密碼金鑰以及其它安全參數的過程，包含：生成、交換、儲存、使用、以及銷毀。

4.16. 訊息鑑別碼（message authentication code, MAC）

為了驗證數位訊息或數位檔案的完整性以及來源性，對稱式金鑰密碼學可被用來計算上述物件的 MAC。傳送方以及接收方通常先協議好一把共享密鑰以及 MAC 演算法，其兩者可被用來驗證 MAC 的正確性。FIPS PUB 140-2 Annex A 以及 ISO/IEC 19772 建議多種 MAC 演算法。

4.17. 作業系統（operating system）

可被運行在計算機內的軟體或指令，負責檔案管理、分配記憶體資源、作為使用者與硬體之間的介面，以及提供特定的功能讓計算機完成必要的工作。

4.18. 通行碼（password）

允許使用者獲得存取權限或證實身分之字元串。

4.19. 個人資料（personally identifiable information）

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。

4.20. 電力轉換系統（power conversion system, PCS）

連接儲能電池的裝置，可進行交流電與直流電的雙向轉換，並且接受能源管理系統之控制指令提供能源管理、調度以及改善電力品質等功能。

4.21. 連接點（point of connection, POC）

電力系統上連接儲能系統之參考點。儲能系統可具有多個 POC 以 2 種不同類別配置：主要 POC 以及輔助 POC。為在內部儲存電能以及最終將電能放電至電力系統，不可能由輔助 POC 充入電能，但能使用主要 POC 饋電至輔助子系統以及能源管理系統。無輔助 POC 時，主要 POC 可簡稱為 POC。

4.22. 遠端網路存取（remote network access）

遠端電腦可經由網路連線操作資訊系統的功能，如同在本地端操作資訊系統的功能。

4.23. 重送攻擊（replay attack）

惡意地重複或拖延資料傳輸的一種網路攻擊。

4.24. 敏感性資料（sensitive data）

若洩漏時可能會損害使用者以及服務提供商權益之資料，包括但不限於：個人資料、通行碼、金鑰、地理位置、組態設定資訊、量測資料、監控資訊、軟韌體更新檔或其它資料。

4.25. 交談連線管理（session management）

當使用者經由網路遠端地登入 PCS 後，為了保持使用者的狀態以及與 PCS 之間的網路連線互動行為，而實現的一種交談連線管理機制，例如：採用交談識別碼（session identifier, SSID）或存取令牌（access token）來保持使用者與 PCS 之間的網路連線狀態。

5. 資訊安全構面說明與要求項目之資安分級

5.1. 資訊安全構面說明

本技術規範為電力轉換系統定義 5 類資訊安全構面，分別為：(1) 實體防護安全、(2) 識別、鑑別與授權安全、(3) 資料儲存安全、(4) 資料傳輸安全、(5) 系統安全。以下分別簡述資訊安全構面之內容。

(1) 實體防護安全：電力轉換系統的實體外觀需具備基本的防禦能力。例如，電力轉換系統應建立外殼拆除障礙以及關閉非必要之實體連接埠，降低攻擊者透過實體介面入侵作業系統或竄改資料的風險。

(2) 識別、鑑別與授權安全：對每種可存取電力轉換系統之方式均須建立識別、鑑別與授權機制，以防止攻擊者存取未經授權之資料或操作超出權限的功能。

(3) 資料儲存安全：電力轉換系統採用密碼學技術保護儲存於內部的敏感性資料，以及具備金鑰管理機制。

(4) 資料傳輸安全：電力轉換系統應採用已知最佳實踐方式建立足夠安全的網路通訊，避免攻擊者非法存取傳輸資料，確保敏感性資料的通訊安全。

(5) 系統安全：減少作業系統存在可被利用的弱點以及提供電力轉換系統整體性的安全機制，包含：網路通訊埠最小化、安全日誌功能，以及更新系統安全。

5.2. 要求項目之資安分級

本技術規範依照：(1) 資安風險之衝擊性、(2) 實現資安防護技術之複雜度，將各資訊安全要求項目分為 1 級、2 級以及 3 級之資安等級。1 級資安等級之要求項目為電力轉換系統應具備的基本防禦能力，其預期效果為抑制人員無心的操作錯誤、不成熟或無足夠資源之蓄意

攻擊行為。2 級資安等級之要求項目為進階的安全機制，預期可抑制蓄意且有足夠資源之攻擊行為，以及資安事件之衝擊恐會影響到民生關鍵基礎建設之場域。3 級資安等級之要求項目為高階的安全機制，使得電力轉換系統具備更強健的防禦能力，也能有效地降低因資安事件所致的負面衝擊。本技術規範的資訊安全構面與資訊安全要求項目彙整在表 1 中。資訊安全應基於嚴謹的風險分析與控管之上，電力轉換系統即使滿足本技術規範之所有要求項目，仍然無法保證完全不遭受惡意的攻擊。

表 1 資訊安全構面與要求項目之彙整表

資訊安全構面	資訊安全要求	項目編號	資訊安全等級		
			1 級	2 級	3 級
6.1. 實體防護安全	6.1.1. 實體介面最小化要求	6.1.1.1	V	V	V
	6.1.2. 實體存取控制	6.1.2.1	V	V	V
		6.1.2.2		V	V
6.2. 識別、鑑別與授權安全	6.2.1. 裝置識別	6.2.1.1			V
	6.2.2. 身分鑑別	6.2.2.1	V	V	V
		6.2.2.2	V	V	V
		6.2.2.3			V
	6.2.3. 通行碼管理	6.2.3.1	V	V	V
		6.2.3.2			V
		6.2.3.3	V	V	V
	6.2.4. 授權管理	6.2.4.1			V
		6.2.4.2		V	V
6.3. 資料儲存安全	6.3.1. 敏感性資料之隱私保護	6.3.1.1	V	V	V
		6.3.1.2		V	V
	6.3.2. 完整性檢查機制	6.3.2.1		V	V

資訊安全構面	資訊安全要求	項目編號	資訊安全等級		
			1 級	2 級	3 級
		6.3.2.2			V
	6.3.3. 金鑰管理	6.3.3.1			V
		6.3.3.2			V
6.4. 資料傳輸安全	6.4.1. 敏感性資料傳輸保護	6.4.1.1	V	V	V
		6.4.1.2		V	V
	6.4.2. 可信任之網路連線	6.4.2.1	V	V	V
		6.4.2.2		V	V
6.5. 系統安全	6.5.1. 安全日誌管理	6.5.1.1	V	V	V
		6.5.1.2			V
		6.5.1.3		V	V
		6.5.1.4			V
		6.5.1.5			V
	6.5.2. 系統安全性評估與強化	6.5.2.1	V	V	V
		6.5.2.2	V	V	V
	6.5.3. 敏感性資料備份	6.5.3.1			V
	6.5.4. 更新系統安全	6.5.4.1	V	V	V
		6.5.4.2	V	V	V
		6.5.4.3	V	V	V
		6.5.4.4		V	V

6. 資訊安全要求項目

6.1. 實體防護安全

6.1.1. 實體介面最小化要求

6.1.1.1. 移除或禁用 PCS 上非必要的實體介面及序列埠。(1 級、2 級、3 級)

6.1.2. 實體存取控制

6.1.2.1. 使用者以實體介面存取 PCS 前，須通過身分鑑別機制，或無實體介面可存取 PCS。(1 級、2 級、3 級)

6.1.2.2. PCS 須建立外殼拆除障礙或保有實體遭拆解之紀錄 (tamper-evident)。(2 級、3 級)

6.2. 識別、鑑別與授權安全

6.2.1. 裝置識別

6.2.1.1. 每台 PCS 都須配置唯一識別碼。(3 級)

6.2.2. 身分鑑別

6.2.2.1. 使用者以遠端網路存取 PCS 前，須通過身分鑑別機制。(1 級、2 級、3 級)

6.2.2.2. 若相同帳號在多次登入 PCS 失敗後，PCS 須暫時或永久鎖定該帳號的登入請求。(1 級、2 級、3 級)

6.2.2.3. 使用者以遠端網路存取 PCS 時，其身分鑑別機制以及交談連線管理機制應能抵禦重送攻擊。(3 級)

6.2.3. 通行碼管理

6.2.3.1. 身分鑑別所用通行碼之組合複雜度以及長度應具有足夠強度，以避免被輕易破解或遭不當利用。(1 級、2 級、3 級)

6.2.3.2. 若要修改通行碼，應先通過身分鑑別機制。(3 級)

6.2.3.3. 若 PCS 採用預設通行碼，須於首次登入後，強制使用者變更預設通行碼。(1 級、2 級、3 級)

6.2.4. 授權管理

6.2.4.1. PCS 須能唯一識別使用者身分。(3 級)

6.2.4.2. PCS 須能設置至少二階層之角色權限。(2 級、3 級)

6.3. 資料儲存安全

6.3.1. 敏感性資料之隱私保護

6.3.1.1. PCS 不應以明文方式儲存敏感性資料。(1 級、2 級、3 級)

6.3.1.2. 儲存於 PCS 內之敏感性資料須受符合 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之密碼系統所保護。(2 級、3 級)

6.3.2. 完整性檢查機制

6.3.2.1. PCS 應至少採用符合 FIPS PUB 140-2 Annex A 之密碼雜湊函式計算敏感性資料的雜湊值，並且具備完整性檢查機制。(2 級、3 級)

6.3.2.2. PCS 應採用符合 FIPS PUB 140-2 Annex A 之數位簽章方法或訊息鑑別碼實現敏感性資料之完整性檢查機制。(3 級)

6.3.3. 金鑰管理

6.3.3.1. 每台 PCS 須採用個別的金鑰保護敏感性資料，確保金鑰的唯一性。(3 級)

6.3.3.2. 金鑰須由安全的隨機亂數產生器產生。(3 級)

6.4. 資料傳輸安全

6.4.1. 敏感性資料傳輸保護

6.4.1.1. PCS 與遠端主機之間不可以明文方式互相傳輸敏感性資料。(1 級、2 級、3 級)

6.4.1.2. 敏感性資料應加密後傳輸，且密碼系統須符合 FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或 NIST SP 800-131A 規定同等或以上強度之方法。(2 級、3 級)

6.4.2. 可信任之網路連線

6.4.2.1. PCS 須能設置白名單，僅允許向特定對象傳送網路封包。(1 級、2 級、3 級)

6.4.2.2. PCS 須能設置白名單，僅允許接受特定對象之連線請求。(2 級、3 級)

6.5. 系統安全

6.5.1. 安全日誌管理

6.5.1.1. PCS 應具備安全日誌功能。(1 級、2 級、3 級)

6.5.1.2. PCS 應支援安全日誌異地備份功能。(3 級)

6.5.1.3. PCS 的安全日誌應具備紀錄滾動之功能。(2 級、3 級)

6.5.1.4. PCS 應可提供合理的日期以及時間。(3 級)

6.5.1.5. PCS 發生高敏感性的安全事件時，應具備主動告警機制。(3 級)

6.5.2. 系統安全性評估與強化

6.5.2.1. PCS 之作業系統與網路服務，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。(1 級、2 級、3 級)

6.5.2.2. PCS 僅開放必要的網路通訊埠。(1 級、2 級、3 級)

6.5.3. 敏感性資料備份

6.5.3.1. PCS 應提供敏感性資料的異地備份功能。(3 級)

6.5.4. 更新系統安全

6.5.4.1. PCS 須支援線上或手動的軟韌體更新功能。(1 級、2 級、3 級)

6.5.4.2. 當軟韌體更新作業失敗時，PCS 仍須回復正常運作。(1 級、2 級、3 級)

6.5.4.3. 若支援手動的軟韌體更新，PCS 須能驗證軟韌體的數位簽章或訊息鑑別碼，確保軟韌體之來源性與完整性。(1 級、2 級、3 級)

6.5.4.4. 若支援線上的軟韌體更新，PCS 與更新伺服器之間應建立安全通道，其須符合附錄 B 之安全通道版本以及密碼套件。(2 級、3 級)

附錄 A：資訊安全要求項目與國際標準間之對照表

安全要求項目編號	國際標準		
	NISTIR 7628	**NIST SP 800-82**	**IEC 62443-4-2**
6.1.1.1	SG.CM-7	6.2.11 (Rev. 2)	CR 7.7
6.1.2.1	-	6.2.7 (Rev. 2)	CR 1.1
6.1.2.2	6.5.1.6	-	EDR 3.11
6.2.1.1	SG.IA-2	-	CR 1.2
6.2.2.1	SG.AC-15	6.2.7 (Rev. 2)	CR 1.1
6.2.2.2	SG.AC-8	6.2.7.1 (Rev. 2)	CR 1.11
6.2.2.3	7.2.10.1	6.2.7.1 (Rev. 2)	CR 3.8
6.2.3.1	SG.AC-21	6.2.7.1 (Rev. 2)	CR 1.7
6.2.3.2	-	-	CR 1.5
6.2.3.3	SG.CM-10	-	CR 1.5
6.2.4.1	SG.IA-2	6.2.7 (Rev. 2)	CR 1.4
6.2.4.2	SG.AC-3	6.2.1.1 (Rev. 2)	-
6.3.1.1	-	6.2.16.1 (Rev. 2)	CR 4.1
6.3.1.2	4.1.2.2	6.2.16.1 (Rev. 2)	CR 4.3
6.3.2.1	6.4.2.2	6.1.6 (Rev. 2)	CR 3.4
6.3.2.2	6.4.2.2	6.1.6 (Rev. 2)	CR 3.4
6.3.3.1	4.1.2.3	-	-
6.3.3.2	SG.SC-11	6.2.16.1 (Rev. 2)	CR 4.3
6.4.1.1	-	6.2.16.1 (Rev. 2)	CR 4.1
6.4.1.2	SG.SC-12	6.2.16.1 (Rev. 2)	CR 4.3
6.4.2.1	SG.SC-10	-	NDR 1.13
6.4.2.2	SG.SC-10	-	NDR 1.13
6.5.1.1	SG.AU-3	6.2.3 (Rev. 2)	CR 2.8

安全要求 項目編號	國際標準		
	NISTIR 7628	**NIST SP 800-82**	**IEC 62443-4-2**
6.5.1.2	SG.IR-10	-	-
6.5.1.3	SG.AU-4	-	CR 2.9
6.5.1.4	SG.AU-8	6.2.12 (Rev. 3)	CR 2.11
6.5.1.5	SG.IR-7	6.2.8 (Rev. 2)	CR 6.2
6.5.2.1	SG.RA-6	-	-
6.5.2.2	SG.CM-7	-	CR 7.7
6.5.3.1	SG.IR-10	-	CR 7.3
6.5.4.1	SG.SA-7	-	NDR 3.10
6.5.4.2	SG.CP-10	-	CR 7.4
6.5.4.3	SG.SA-7	-	EDR 3.10
6.5.4.4	-	-	EDR 3.10

附錄 B：安全通道版本以及密碼套件之選用要求

採用安全通道（TLS）時應符合下列之版本號以及密碼套件：

- **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：資訊安全檢測之資料調查表

※若表格不敷使用，請自行增加

<table>
<tr><th></th><th>項次</th><th>項目</th><th>內容</th></tr>
<tr><td rowspan="15">一、電力轉換系統之基本資訊</td><td>1</td><td>送測單位名稱</td><td></td></tr>
<tr><td>2</td><td>PCS 產品型號</td><td></td></tr>
<tr><td>3</td><td>PCS 軟韌體版本號</td><td></td></tr>
<tr><td>4</td><td>PCS 軟韌體雜湊值</td><td></td></tr>
<tr><td>5</td><td colspan="2">通訊模組之基本資訊</td></tr>
<tr><td colspan="3">☐無通訊模組　☐內嵌　☐外掛
通訊模組產品型號：
通訊模組軟韌體版本號：
通訊模組軟韌體雜湊值：</td></tr>
<tr><td>6</td><td colspan="2">實體介面以及序列埠之用途</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>7</td><td colspan="2">敏感性資料之類型與用途說明</td></tr>
<tr><td colspan="3">範例：
1. 通行碼：身分鑑別時所用。
2. 加解密金鑰：為敏感性資料進行加解密所用。
3. 組態設定：設定電力能源的轉換策略參數。</td></tr>
<tr><td>8</td><td>是否具作業系統</td><td>☐是：作業系統　☐否</td></tr>
<tr><td>9</td><td>是否可被遠端存取</td><td>☐是　☐否</td></tr>
<tr><td>10</td><td>是否具實體存取介面</td><td>☐是　☐否</td></tr>
<tr><td>11</td><td>是否具帳號鎖定功能</td><td>☐否
☐是　時間長度：　閥值：</td></tr>
<tr><td>12</td><td colspan="2">請說明唯一識別碼的編碼方式以及查詢方法</td></tr>
<tr><td colspan="3"></td></tr>
</table>

	項次	項目	內容
二、資料傳輸安全機制	13	資料傳輸所選用的密碼系統	☐TDES ☐AES ☐RSA ☐其它： ☐無：請說明原因
	14	金鑰位元長度	對稱式金鑰：AES/128 位元 非對稱式金鑰：RSA/2048 位元
	15	遠端主機之 IP 白名單與連線目的	
三、資料儲存安全機制	16	請說明須儲存的敏感性資料以及儲存路徑	
	17	提供資料機密性所選用的密碼系統	☐TDES ☐AES ☐RSA ☐其他： ☐無：請說明原因
	18	金鑰位元長度	對稱式金鑰：AES/128 位元 非對稱式金鑰：RSA/2048 位元
	19	請說明資料完整性檢查機制之設計方法	
	20	金鑰產生的演算法	
四、系統安全機制	21	是否具備更新機制	☐是 ☐手動 ☐線上 ☐否：請說明原因
	22	軟韌體更新機制之操作說明	

	項次	項目	內容
	23	請說明會被記錄在安全日誌的行為以及最大的儲存空間	
	24	是否具備異地備份的事件日誌	□否：請說明原因 □是：請說明異地備份的操作方式、須被備份的資料類型、如何查看異地備份的資訊，以及其它說明文件。
	25	安全事件的告警方式	□ E-mail: □ 電話： □ 其它：
	26	請說明各個階層的角色名稱以及可存取的功能	
	27	請說明電力轉換系統必要的網路通訊埠以及用途	
	28	請說明 PCS 軟韌體檔案的數位簽章或訊息鑑別碼方法	
	29	測試用帳號	帳號： 通行碼：
備註			

填表人姓名：

送測單位地址：

送測單位之大、小章：

小章	大章

附錄 D：資訊安全要求項目以及檢測方法

本附錄提供檢測實驗室各個資訊安全要求項目之檢測方法作為參考，確保其檢測方法以及判定標準之一致性。請特別注意，本附錄的各個資訊安全要求項目之編號是依據第 6 節的內容所編排。

6.1. 實體防護安全

6.1.1. 實體介面最小化要求

6.1.1.1. 移除或禁用 PCS 上非必要的實體介面及序列埠。(1 級、2 級、3 級)

A. 測試目的

將 PCS 外觀上可被利用的實體介面最小化。

B. 測試條件

送測單位提供文件說明 PCS 外觀上必要的實體介面以及用途。

C. 測試步驟

(1) 目視 PCS 外觀上的實體介面並且記錄下來。

(2) 查看送測單位提供的文件，然後比對與實際觀察到的實體介面是否相符。

D. 預期結果

(1) 實際觀察到的實體介面與送測單位提供的文件內容相符。

(2) 若 PCS 外觀存在非必要的實體介面，須予以關閉或採實體保護。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.1.2. 實體存取控制

6.1.2.1. 使用者以實體介面存取 PCS 前，須通過身分鑑別機制，或無實體介面可存取 PCS。(1 級、2 級、3 級)

A. 測試目的

避免人員在未授權的情況下經由實體介面存取 PCS。

B. 測試條件

(1) 送測單位須提供文件說明是否可經由實體介面存取 PCS。

(2) 若存在實體介面的存取方式，送測單位須提供文件說明經由實體介面存取 PCS 以及身分鑑別的方法。

C. 測試步驟

(1) 根據送測單位的文件，經由實體介面存取 PCS。

(2) 確認是否須先通過身分鑑別機制後才可存取 PCS。

D. 預期結果

(1) 無法經由實體介面存取 PCS。

(2) 須先通過身分鑑別機制後才可存取 PCS。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.1.2.2. PCS 須建立外殼拆除障礙或保有實體遭拆解之紀錄 (tamper-evident)。(2 級、3 級)

A. 測試目的

避免或偵測人員對 PCS 進行實體攻擊。

B. 測試條件

無。

C. 測試步驟

(1) 目視 PCS 是否具備外殼拆除障礙之設計，例如：外殼為一體成形、實體鎖、防拆螺絲或其它無法輕易拆除外殼之設計。

(2) 目視 PCS 是否保有實體遭拆解之紀錄，例如：一次性貼紙、易碎貼紙、鉛封或其它可留下拆除紀錄之機制。

D. 預期結果

(1) PCS 具備外殼拆除障礙之設計。

(2) PCS 保有外殼遭拆除之紀錄。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.2. 識別、鑑別與授權安全

6.2.1. 裝置識別

6.2.1.1. 每台 PCS 都須配置唯一識別碼。(3 級)

A. 測試目的

每台 PCS 應可被唯一識別。

B. 測試條件

送測單位提供文件說明唯一識別碼的編碼方法以及查詢唯一識別碼的方式。

C. 測試步驟

(1) 審視送測單位提供的文件，確認唯一識別碼的編碼方法不容易發生重複以及耗盡。

(2) 根據送測單位的文件，實際查詢 PCS 的唯一識別碼的編碼方法是否與文件所述相符。

D. 預期結果

(1) 唯一識別碼的編碼方法足以容納 PCS 的數量並且不容易發生重複的唯一識別碼。

(2) PCS 的唯一識別碼之編碼方法與送測單位提供的說明文件相符。

E. 測試結果

「通過」：符合預期結果(1)及(2)。

「不通過」：不符合預期結果(1)或(2)。

備考：若 PCS 無查詢唯一識別碼的功能，則須滿足預期結果(1)。

6.2.2. 身分鑑別

6.2.2.1. 使用者以遠端網路存取 PCS 前，須通過身分鑑別機制。(1 級、2 級、3 級)

A. 測試目的

避免人員在非授權的情況下經由遠端網路存取 PCS 的功能。

B. 測試條件

送測單位提供文件說明 PCS 是否具備可遠端網路存取的功能以及身分鑑別的方法。

C. 測試步驟

(1) 建立遠端網路存取 PCS 的環境。

(2) 檢查遠端的使用者是否須通過身分鑑別後，才可操作 PCS 的功能。

D. 預期結果

遠端的使用者須先通過身分鑑別後，才可操作 PCS 的功能。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」：PCS 未提供使用者可遠端網路存取的功能。

6.2.2.2. 若相同帳號在多次登入 PCS 失敗後，PCS 須暫時或永久鎖定該帳號的登入請求。(1 級、2 級、3 級)

A. 測試目的

無論人員經由實體介面或遠端網路存取 PCS 的功能，其身分鑑別機制應可抵禦暴力攻擊。

B. 測試條件

(1) PCS 採用通行碼或其它所知之事（something you know）作為鑑別符。

(2) 送測單位提供文件說明 PCS 是否具備帳號鎖定的功能、登入失敗的閥值以及帳號鎖定的時間長度。

C. 測試步驟

(1) 根據送測單位的文件，設定登入失敗的閥值以及帳號鎖定的時間長度。

(2) 採用正確的帳號搭配錯誤的通行碼或其它鑑別符試圖登入 PCS。

(3) 重複執行數次測試步驟(2)，每次都採用相異的錯誤通行碼或其它鑑別符。

(4) 當登入失敗的次數抵達閥值後，採用正確的通行碼或其它鑑別符試圖登入 PCS 並且觀察登入結果。

(5) 在帳號鎖定的時間內，採用正確的通行碼或其它鑑別符試圖登入 PCS 並且觀察登入結果。

(6) 在帳號解除鎖定後，採用正確的通行碼或其它鑑別符試圖登入 PCS 並且觀察登入結果。

D. 預期結果

(1) 登入失敗的閥值最多 5 次。

(2) 當登入失敗次數抵達閥值後，PCS 禁止使用者繼續操作登入功能、提示帳號暫時（永久）鎖定之訊息，或任何不允許使用者採用相同帳號繼續登入的方式。

(3) 在帳號鎖定的有效時間內，即使採用正確的通行碼或其它鑑別符，也無法成功登入 PCS。

(4) 當帳號解除鎖定後，採用正確的帳號以及通行碼，可成功登入 PCS。

E. 測試結果

「通過」：符合預期結果(1)、(2)、(3)及(4)。

「不通過」：不符合預期結果(1)或(2)或(3)或(4)。

「不適用」:PCS 未採用通行碼或其它所知之事作為鑑別符。

備考：若 PCS 對可用性的需求較高，則可採取「當失敗登入次數抵達閥值時，PCS 能有效地即時告知具權限之管理人員」之機制作為本要求項目之補償措施。

6.2.2.3. 使用者以遠端網路存取 PCS 時，其身分鑑別機制以及交談連線管理機制應能抵禦重送攻擊。(3 級)

A. 測試目的

避免人員利用重送攻擊，在未經授權的情況下能經由遠端網路存取 PCS 的功能或資料。

B. 測試條件

送測單位提供文件說明PCS是否具備可遠端網路存取的功能以及身分鑑別的方法。

C. 測試步驟

情境一：身分鑑別機制可抵禦重送攻擊。

(1) 建立 PCS 與遠端主機之間的網路封包側錄環境。

(2) 採用正確的鑑別符操作遠端網路存取 PCS 時的身分鑑別機制，並保存相關網路封包內容。

(3) 登出 PCS 或中斷與 PCS 之間的遠端網路存取連線。

(4) 重新建立與 PCS 之間的遠端網路存取連線。當被 PCS 要求身分鑑別時，向 PCS 重送測試步驟(2)所蒐集到的網路封包內容。

情境二：交談連線管理機制可抵禦重送攻擊。

(1) 建立 PCS 與遠端主機之間的網路封包側錄環境。

(2) 採用正確的鑑別符操作遠端網路存取 PCS 時的身分鑑別機制。

(3) 當成功登入後，觀察 PCS 與遠端主機之間的交談連線管理機制，例如：交談識別碼、access token 或其它方法。

(4) 保存可以向 PCS 索取服務或資料的網路封包內容，其中須包含實現交談連線管理機制的必要參數。

(5) 登出 PCS 或中斷與 PCS 之間的遠端網路存取連線。

(6) 重新建立與 PCS 之間的遠端網路存取連線，然後向 PCS 重送測試步驟(4)所蒐集到的網路封包內容。

D. 預期結果

(1) 遠端主機或人員無法經由重送攻擊成功登入 PCS。

(2) 遠端主機或人員無法經由重送攻擊向 PCS 索取原有的回應資料或功能。

E. 測試結果

「通過」：符合預期結果(1)及(2)。

「不通過」：不符合預期結果(1)或(2)。

「不適用」:PCS 未提供使用者可遠端網路存取的功能。

6.2.3. 通行碼管理

6.2.3.1. 身分鑑別所用通行碼之組合複雜度以及長度應具有足夠強度，以避免被輕易破解或遭不當利用。(1 級、2 級、3 級)

A. 測試目的

人員應避免選用弱通行碼，增加通行碼猜測攻擊的困難度。

B. 測試條件

(1) PCS 採用通行碼作為鑑別符。

(2) 送測單位提供文件說明通行碼的設置方式，例如：註冊、重設通行碼或修改通行碼等其它功能。

C. 測試步驟

情境一：通行碼之長度具有足夠強度。

(1) 針對每種可設置通行碼的功能，將通行碼的長度設置少於 12 個字元，然後觀察設置結果。

情境二：通行碼之組合複雜度以及長度具有足夠強度。

(1) 針對每種可設置通行碼的功能，將通行碼長度設置少於 8 個字元，以及在大寫英文、小寫英文、數字以及特殊符號中任選其中 1 種以及 2 種字元型別的組合設置通行碼，然後觀察設置結果。

D. 預期結果

(1) 無法成功設置長度少於 12 個字元的通行碼。

(2) 無法成功設置長度少於 8 個字元，或僅由少於 3 種字元型別所組成的通行碼(長度為 8 至 11 個字元)。

E. 測試結果

「通過」: 符合預期結果(1)或(2)。

「不通過」: 不符合預期結果(1)及(2)。

「不適用」: PCS 未採用通行碼作為鑑別符。

6.2.3.2. 若要修改通行碼，應先通過身分鑑別機制。(3 級)

A. 測試目的

避免人員在非授權的情況下任意修改通行碼或其它所知之事（something you know）之鑑別符。

B. 測試條件

PCS 採用通行碼或其它所知之事作為鑑別符。

C. 測試步驟

(1) 在未登入 PCS 的情況下，紀錄可操作的功能。

(2) 確認可操作的功能是否包含修改通行碼或其它鑑別符的功能。

D. 預期結果

在未登入 PCS 的情況下，無法操作修改通行碼或其它鑑別符的功能。

E. 測試結果

「通過」: 符合預期結果。

「不通過」: 不符合預期結果。

「不適用」:PCS 未採用通行碼或其它所知之事作為鑑別符。

6.2.3.3. 若 PCS 採用預設通行碼，須於首次登入後，強制使用者變更預設通行碼。(1 級、2 級、3 級)

A. 測試目的

避免人員濫用預設通行碼，導致可在非授權的情況下存取 PCS。

B. 測試條件

(1) PCS 須保持出廠預設狀態。

(2) PCS 採用預設通行碼。

C. 測試步驟

(1) 在出廠預設狀態下，查看 PCS 是否採用預設通行碼。

(2) 若 PCS 採用預設通行碼，在首次登入後觀察 PCS 是否要求使用者更改預設通行碼。

(3) 以預設通行碼設置新的通行碼。

D. 在成功設置新的通行碼後，再採用預設通行碼試圖登入 PCS。

E. 預期結果

(1) PCS 要求使用者修改預設通行碼。

(2) 預設通行碼無法作為新的通行碼。

(3) 在成功設置新的通行碼後，無法再採用預設通行碼登入 PCS。

E. 測試結果

「通過」：符合預期結果(1)、(2)及(3)。

「不通過」：不符合預期結果(1)或(2)或(3)。

「不適用」：PCS 未採用通行碼作為鑑別符。

備考：在出廠預設狀態下，若 PCS 要求使用者須先設置通行碼後才可存取相關功能，則測試結果為「通過」。

6.2.4. 授權管理

6.2.4.1. PCS 須能唯一識別使用者身分。(3 級)

A. 測試目的

PCS 應禁止使用者設置已存在的帳號。

B. 測試條件

(1) PCS 提供使用者可設置登入帳號的功能。

(2) 若 PCS 無提供使用者可設置登入帳號的功能，則應提供文件說明 PCS 如何唯一識別使用者的身分。

C. 測試步驟

(1) 若 PCS 無提供使用者可設置登入帳號的功能，則審視送測單位提供的文件，確認 PCS 是否可唯一識別使用者的身分。

(2) 在 PCS 上設置第 1 組帳號。

(3) 以第 1 組帳號試圖設置第 2 組相同之帳號，然後觀察設置結果。

D. 預期結果

(1) 送測單位提供的文件足以證明 PCS 可唯一識別使用者的身分。

(2) 無法成功設置第 2 組帳號。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.2.4.2. PCS 須能設置至少二階層之角色權限。(2 級、3 級)

A. 測試目的

PCS 應落實「最小權限原則」具備合適的角色授權機制。

B. 測試條件

(1) PCS 提供使用者可設置不同階層的角色帳號。

(2) 送測單位提供文件說明各個階層的角色可操作功能。

C. 測試步驟

(1) 依照送測單位提供的文件設置每個階層的角色帳號。

(2) 分別以每個階層的角色帳號登入 PCS，然後操作各個功能。

(3) 比對各個階層的角色可操作的功能是否與送測單位提供的文件相符。

D. 預期結果

(1) PCS 提供使用者可設置不同階層的角色帳號。

(2) 各個階層的角色可操作的功能與送測單位提供的文件相符。

E. 測試結果

「通過」：符合預期結果(1)及(2)。

「不通過」：不符合預期結果(1)或(2)。

6.3. 資料儲存安全

6.3.1. 敏感性資料之隱私保護

6.3.1.1. PCS 不應以明文方式儲存敏感性資料。(1 級、2 級、3 級)

A. 測試目的

敏感性資料應先被加密後再被儲存於 PCS 中，避免敏感性資料被輕易地洩漏。

B. 測試條件

(1) 送測單位提供文件說明 PCS 須儲存的敏感性資料以及其儲存路徑，以及加密敏感性資料的方法、設計文件或其它用於佐證的資料。

(2) 送測單位提供文件說明如何瀏覽 PCS 的資料目錄。

C. 測試步驟

(1) 根據送測單位提供的文件，瀏覽儲存敏感性資料的目錄。

(2) 確認敏感性資料是否以明文的方式被儲存在 PCS 中。

D. 預期結果

(1) PCS 未儲存敏感性資料。

(2) PCS 未以明文方式儲存敏感性資料。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.3.1.2. 儲存於 PCS 內之敏感性資料須受符合 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之密碼系統所保護。(2 級、3 級)

A. 測試目的

PCS 應採用已認可的安全密碼系統保護被儲存的敏感性資料。

B. 測試條件

(1) 送測單位提供文件說明 PCS 須儲存的敏感性資料以及其儲存路徑。

(2) 送測單位提供文件說明如何瀏覽 PCS 的資料目錄。

(3) 送測單位提供文件說明採用何種密碼系統保護敏感性資料，例如：設計文件、程式碼、加解密過程的指令以及其它足以佐證的資料。

C. 測試步驟

(1) 根據送測單位提供的文件，瀏覽儲存敏感性資料的目錄。

(2) 確認敏感性資料是否以明文的方式被儲存在 PCS 中。

(3) 審視佐證文件，確認被用來保護敏感性資料的密碼系統是否為 FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或 NIST SP 800-131A 所列之方法，或者同等級以上之方法。

D. 預期結果

(1) PCS 未儲存敏感性資料。

(2) PCS 採用已認可的安全密碼系統保護敏感性資料。

E. 測試結果

「通過」：符合預期結果(1)或(2)。

「不通過」：不符合預期結果(1)及(2)。

6.3.2. 完整性檢查機制

6.3.2.1. PCS 應至少採用符合 FIPS PUB 140-2 Annex A 之密碼雜湊函式計算敏感性資料的雜湊值，並且具備完整性檢查機制。(2 級、3 級)

A. 測試目的

對於儲存在 PCS 中的敏感性資料、關鍵參數或組態設定應有合適的完整性檢查機制，可偵測出內容已被修改。

B. 測試條件

(1) 送測單位提供文件說明 PCS 所具備的資料完整性檢查機制之方法以及被保護的對象。

(2) 送測單位提供文件說明須要被保護的對象之儲存路徑。

C. 測試步驟

(1) 根據送測單位提供的文件，審閱完整性檢查機制的設計方法以及須被保護的對象。

(2) 修改敏感性資料的值或相對應的檢核碼，例如：雜湊值、簽章值、MAC 值或其它。

D. 預期結果

(1) 未具有須要完整性檢查機制的資料。

(2) 資料完整性檢查機制的設計方法至少是基於 FIPS PUB 140-2 Annex A 之密碼雜湊函式。

(3) 資料完整性檢查機制的設計方法是基於 FIPS PUB 140-2 Annex A 所列之數位簽章或訊息鑑別碼(MAC)。

(4) 資料完整性檢查機制能有效地偵測出敏感性資料或相對應的檢核碼被修改。

E. 測試結果

「通過」：符合預期結果(1)、或(2)及(4)、或(3)及(4)。

「不通過」：不符合預期結果(1)及(2)或(4)、或(1)及(3)或(4)。

備考：資料完整性檢查機制的需求對象不需包含所有的敏感性資料或關鍵參數。送測單位可自定義需要資料完整性檢查機制的對象並且詳述在說明文件中。但必要時，檢測實驗室可要求送測單位應受完整性檢查機制所保護的敏感性資料或關鍵參數。

6.3.2.2. PCS 應採用符合 FIPS PUB 140-2 Annex A 之數位簽章方法或訊息鑑別碼實現敏感性資料之完整性檢查機制。(3 級)

A. 測試目的

對於儲存在 PCS 中的敏感性資料、關鍵參數或組態設定應有合適的完整性檢查機制，可偵測內容已被修改。

B. 測試條件

(1) 送測單位提供文件說明 PCS 所具備的資料完整性檢查機制之方法以及被保護的對象。

(2) 送測單位提供文件說明須要被保護的對象之儲存路徑。

C. 測試步驟

(1) 根據送測單位提供的文件，審閱完整性檢查機制的設計方法以及須被保護的對象。

(2) 修改敏感性資料的值或相對應的檢核碼，例如：雜湊值、簽章值、MAC 值或其它。

D. 預期結果

(1) 未具有須要完整性檢查機制的資料。

(2) 資料完整性檢查機制的設計方法是基於 FIPS PUB 140-2 Annex A 所列之數位簽章或訊息鑑別碼(MAC)。

(3) 資料完整性檢查機制能有效地偵測出敏感性資料或相對應的檢核碼被修改。

E. 測試結果

「通過」：符合預期結果(1)、或(2)及(3)。

「不通過」：不符合預期結果(1)及(2)或(3)。

備考：資料完整性檢查機制的需求對象不需包含所有的敏感性資料或關鍵參數。送測單位可自定義需要資料完整性檢查機制的對象並且詳述在說明文件中。但必要時，檢測實驗室可要求送測單位應受完整性檢查機制所保護的敏感性資料或關鍵參數。

6.3.3. 金鑰管理

6.3.3.1. 每台 PCS 須採用個別的金鑰保護敏感性資料，確保金鑰的唯一性。(3 級)

A. 測試目的

避免因單獨的金鑰被洩漏後而影響其它 PCS 的安全性。

B. 測試條件

送測單位提供文件說明如何將金鑰布建至每台 PCS 中，以及產生金鑰的方法，例如：設計文件、程式碼、產生金鑰的執行過程或其它足以佐證的資料。必要時，檢測實驗室可要求送測單位進行展示。

C. 測試步驟

(1) 審視送測單位提供的文件，確認金鑰產生的方法可以使得每台 PCS 持有相異的金鑰。

D. 預期結果

每台 PCS 可持有相異的金鑰。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」:PCS 未儲存敏感性資料以及未採用密碼系統。

6.3.3.2. 金鑰須由安全的亂數產生器產生。(3 級)

A. 測試目的

金鑰產生的方法應符合不可預測性，避免因單獨的金鑰被洩漏後可推算出其它的金鑰。

B. 測試條件

送測單位提供文件說明產生金鑰的方法，例如：設計文件、程式碼、產生金鑰的執行過程或其它足以佐證的資料。必要時，檢測實驗室可要求送測單位進行展示。

C. 測試步驟

(1) 審視送測單位提供的文件，確認金鑰產生的方法是否滿足以下任一條件：

I. 金鑰產生的方法是倚靠 FIPS 140-2 Annex C 所建議之方法。

II. 金鑰產生的方法是倚靠程式語言的標準隨機亂數產生函式，而該函式未被指出資安弱點。

III. 金鑰產生的方法為業界公認或普遍實行的方法。

D. 預期結果

金鑰產生的方法滿足測試步驟(1)中所列的任一條件。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」:PCS 未儲存敏感性資料以及未採用密碼系統。

6.4. 資料傳輸安全

6.4.1. 敏感性資料傳輸保護

6.4.1.1. PCS 與遠端主機之間不可以明文方式互相傳輸敏感性資料。(1 級、2 級、3 級)

A. 測試目的

避免敏感性資料經由網路傳輸時被洩漏。

B. 測試條件

PCS 與遠端主機之間的網路連線是建立在 TCP/IP 之上，其中亦包含常見的工控協定 Modbus TCP。

C. 測試步驟

(1) 建立 PCS 與遠端主機之間的網路封包側錄環境。

(2) 操作 PCS 的各項功能。

(3) 查看網路封包內容是否含敏感性資料之明文。

D. 預期結果

(1) PCS 與遠端主機之間未經由網路連線互相傳送敏感性資料。

(2) PCS 與遠端主機之間未經由網路連線互相傳送敏感性資料之明文。

(3) PCS 與遠端主機之間若採用安全通道建立網路連線，應符合附錄 B 之版本以及密碼套件。

E. 測試結果

「通過」：符合預期結果(1)或(2)或(3)。

「不通過」：不符合預期結果(1)及(2)及(3)。

「不適用」：PCS 與遠端主機之間的網路連線非建立在 TCP/IP 之上。

6.4.1.2. 敏感性資料應加密後傳輸，且密碼系統須符合 FIPS PUB 140-2 Annex A 、NIST SP 800-140C 或 NIST SP 800-131A 規定同等或以上強度之方法。(2 級、3 級)

A. 測試目的

PCS 應採用已認可的安全密碼系統保護經由網路傳輸的敏感性資料。

B. 測試條件

(1) PCS 與遠端主機之間的網路連線是建立在 TCP/IP 之上，其中亦包含常見的工控協定 Modbus TCP。

(2) 送測單位提供文件說明採用何種密碼系統保護敏感性資料，例如：設計文件、程式碼、加解密過程的指令以及其它足以佐證的資料。

C. 測試步驟

(1) 建立 PCS 與遠端主機之間的網路封包側錄環境。

(2) 操作 PCS 的各項功能。

(3) 查看網路封包內容是否含敏感性資料之明文。

(4) 審視送測單位提供的文件，確認敏感性資料被已認可的安全密碼系統所保護。

D. 預期結果

(1) PCS 與遠端主機之間未經由網路連線互相傳送敏感性資料。

(2) PCS 採用已認可的安全密碼系統保護經由網路連線傳送的敏感性資料。

(3) PCS 與遠端主機之間若採用安全通道建立網路連線，則應符合附錄 B 之版本以及密碼套件。

E. 測試結果

「通過」：符合預期結果(1)或(2)或(3)。

「不通過」：不符合預期結果(1)及(2)及(3)。

「不適用」：PCS 與遠端主機之間的網路連線非建立在 TCP/IP 之上。

6.4.2. 可信認之網路連線

6.4.2.1. PCS 須能設置白名單，僅允許向特定對象傳送網路封包。(1 級、2 級、3 級)

A. 測試目的

避免 PCS 將資料傳送至非預期的遠端主機。

B. 測試條件

(1) 送測單位提供文件說明遠端主機的 IP 位址、MAC address 或網域名稱。

(2) PCS 的網路連線是基於 TCP/IP 之上。

C. 測試步驟

(1) 將 PCS 連結至網際網路（Internet）。

(2) 建立網路封包側錄的環境，然後蒐集至少 24 小時的網路封包。

(3) 查看與 PCS 建立網路連線的遠端主機，其 IP 位址、MAC address 或網域名稱是否與送測單位提供的文件相符。

D. 預期結果

與 PCS 建立網路連線的遠端主機，其 IP 位址、MAC address 或網域名稱與送測單位提供的文件相符。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」：PCS 與遠端主機之間的網路連線非建立在 TCP/IP 之上。

6.4.2.2. PCS 須能設置白名單，僅允許接受特定對象之連線請求。(2 級、3 級)

A. 測試目的

避免非預期的遠端主機向 PCS 請求網路連線。

B. 測試條件

(1) PCS 的網路連線是基於 TCP/IP 之上。

(2) PCS 提供使用者能設置 IP 位址白名單之功能，或者由檢測實驗室提供 IP 位址白名單給送測單位設置。

C. 測試步驟

(1) 設定 PCS 上的白名單功能。

(2) 將非白名單內的 IP 位址設定在測試電腦上。

(3) 嘗試以測試電腦與 PCS 建立網路連線。

(4) 確認 PCS 是否拒絕測試電腦的連線請求。

(5) 重複步驟(2)~(3) 3 次，每次都挑選不同的 IP 位址。

D. 預期結果

PCS 拒絕測試電腦的連線請求。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」：PCS 與遠端主機之間的網路連線非建立在 TCP/IP 之上。

6.5. 系統安全

6.5.1. 安全日誌管理

6.5.1.1. PCS 應具備安全日誌功能。(1 級、2 級、3 級)

A. 測試目的

當發生資安或非預期事件時,人員可藉由安全日誌的內容追查可能的原因。

B. 測試條件

送測單位提供文件說明安全日誌會記錄的行為,以及查詢安全日誌的方法。

C. 測試步驟

(1) 審視送測單位提供的文件，確認安全日誌應至少記錄以下行為：

I. 使用者經由遠端網路存取以及實體介面登入與登出的行為，其中包含成功以及失敗的登入嘗試。

II. PCS 之軟/韌體更新之行為。

III. 緊急或異常事件之行為。

IV. 帳號鎖定之行為。

V. 修改通行碼之行為。

(2) 根據送測單位提供的文件，操作會記錄在安全日誌的行為。

(3) 根據送測單位提供的文件，查詢安全日誌的內容是否包含應紀錄之行為，其安全日誌內容應至少包含以下欄位：

I. 被記錄的行為。

II. 發生行為的日期以及時間。

III. 產生行為的使用者帳號或設備的唯一識別碼。

D. 預期結果

安全日誌內容包含測試步驟(1)及(3)所列之資訊。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

備考：安全日誌可被記錄在 PCS 中，亦可被記錄在遠端伺服器或裝置中。

6.5.1.2. PCS 應支援安全日誌異地備份功能。(3 級)

A. 測試目的

避免因 PCS 受到損害或日誌空間不足時，無法保存完整的安全日誌。

B. 測試條件

送測單位提供文件說明安全日誌的異地備份如何被觸發，以及查詢安全日誌的方法。

C. 測試步驟

(1) 根據送測單位提供的文件，操作會記錄在安全日誌的行為。

(2) 根據送測單位提供的文件，觸發安全日誌的異地備份功能。

(3) 查詢異地備份的安全日誌，然後確認內容是否與原本的安全日誌相符。

D. 預期結果

異地備份的安全日誌，其內容與原本的安全日誌相符。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

6.5.1.3. PCS 的安全日誌應具備紀錄滾動之功能。(2 級、3 級)

A. 測試目的

當安全日誌的儲存空間已用盡，仍會持續新增記錄並且覆蓋最舊的紀錄。

B. 測試條件

送測單位提供文件說明安全日誌的儲存空間大小或者最多可儲存幾筆紀錄。

C. 測試步驟

(1) 根據送測單位提供的文件，產生會記錄在安全日誌的行為，試圖耗盡安全日誌的儲存空間。

(2) 當安全日誌的儲存空間耗盡時，持續產生會記錄在安全日誌的行為

(3) 查看安全日誌是否記錄新產生的行為並且覆蓋最舊的紀錄。

D. 預期結果

當安全日誌的儲存空間耗盡時，仍會持續記錄新的行為並且覆蓋最舊的紀錄。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」:安全日誌僅被儲存在遠端的伺服器或裝置中。

6.5.1.4. PCS 應可提供合理的日期以及時間。(3 級)

A. 測試目的

PCS 應可提供合理的日期以及時間，使得安全日誌可如實地紀錄事件發生的時間。

B. 測試條件

檢測人員具備可顯示合理的日期以及時間的裝置，例如：手機、電腦、穿戴式裝置、手錶或其它裝置。

C. 測試步驟

(1) 查看 PCS 是否具備顯示日期以及時間的功能，且日期及時間須正確。

(2) 若 PCS 顯示的日期或時間不正確，則查看是否提供可自行設定或校時的功能，然後再重複執行步驟(1)。

(3) 操作會被記錄在安全日誌的行為。

(4) 查看安全日誌，確認事件發生的日期以及時間是否與 PCS 顯示的相符。

D. 預期結果

(1) PCS 顯示的日期以及時間與檢測人員的裝置相符，其中時間的誤差可在±3 分鐘內。

(2) 安全日誌記錄事件發生的日期以及時間與 PCS 顯示的相符。

E. 測試結果

「通過」：符合預期結果(1)及(2)。

「不通過」：不符合預期結果(1)或(2)。

6.5.1.5. PCS 發生高敏感性的安全事件時，應具備主動告警機制。(3 級)

A. 測試目的

PCS 應能主動地告知人員發生高敏感性的安全事件。

B. 測試條件

(1) 送測單位提供文件說明高敏感性的安全事件。

(2) 送測單位提供文件說明如何實現 PCS 的主動告警機制，例如：發送 E-mail、警鈴、電話簡訊或其它方式。

C. 測試步驟

(1) 審視送測單位提供的文件，確認高敏感性的安全事件應至少包含以下行為：

I. PCS 之軟/韌體更新之行為。

II. 帳號鎖定之行為。

III. 修改通行碼之行為。

IV. 緊急事件之行為。

(2) 設定主動告警機制的相關組態。

(3) 觸發高敏感性的安全事件，然後查看 PCS 是否有主動告警的機制並且與送測單位提供的文件相符。

D. 預期結果

(1) 高敏感性的安全事件至少包含測試步驟(1)所列之行為。

(2) 當發生高敏感性的安全事件時，PCS 會主動告警並且與送測單位提供的文件相符。

E. 測試結果

「通過」：符合預期結果(1)及(2)。

「不通過」：不符合預期結果(1)或(2)。

6.5.2. 系統安全性評估與強化

6.5.2.1. PCS 之作業系統與網路服務，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。(1 級、2 級、3 級)

A. 測試目的

確保 PCS 的作業系統無高風險的資安弱點。

B. 測試條件

PCS 具作業系統，且網路連線功能是基於 TCP/IP 之上。

C. 測試步驟

(1) 更新資安弱點掃描工具，保持在最新狀態。

(2) 採用資安弱點掃描工具對 PCS 進行弱點掃描。

(3) 查看弱點掃描的結果，確認是否含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)以上之項目。

D. 預期結果

資安弱點掃描的結果未指出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)以上之項目。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」:PCS 未具有作業系統或網路連線功能非基於 TCP/IP 之上。

6.5.2.2. PCS 僅開放必要的網路通訊埠。(1 級、2 級、3 級)

A. 測試目的

減少可被攻擊者利用的網路服務。

B. 測試條件

(1) PCS 具作業系統，且網路連線功能是基於 TCP/IP 之上。

(2) 送測單位提供文件說明 PCS 必要的網路通訊埠以及使用目的，包含 TCP 以及 UDP。

C. 測試步驟

(1) 採用網路通訊埠掃描工具對 PCS 進行掃描，包含 TCP 以及 UDP 全部的網路通訊埠（0~65535）。

(2) 查看掃描結果，確認網路通訊埠的狀態是否與送測單位提供的文件相符。

D. 預期結果

網路通訊埠的掃描結果與送測單位提供的文件相符。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」：PCS 未具有作業系統或網路連線功能非基於 TCP/IP 之上

6.5.3. 敏感性資料備份

6.5.3.1. PCS 應提供敏感性資料的異地備份功能。(3 級)

A. 測試目的

敏感性資料應可被異地備份，確保 PCS 遭受損害時可即時地回復必要的功能。

B. 測試條件

(1) 送測單位提供文件說明哪些敏感性資料可被異地備份，包含（但不限於）：金鑰、組態設定、使用者的帳號以及通行碼，以及其它支持 PCS 正常運作的必要敏感性資料。

(2) 送測單位提供文件說明如何啟動敏感性資料的異地備份功能，以及如何載入異地備份的敏感性資料。

C. 測試步驟

(1) 根據送測單位提供的文件，操作有關敏感性資料的功能。

(2) 啟動敏感性資料的異地備份功能。

(3) 將 PCS 回復至出廠預設狀態。

(4) 載入異地備份的敏感性資料。

(5) 查看 PCS 是否可正常運作，且可回復先前備份的敏感性資料。

備考：若 PCS 未提供使用者回復至出廠預設狀態的功能，則可嘗試將組態設定回復至預設值、刪除金鑰、刪除使用者的帳號以及通行碼，或其它可更動 PCS 的敏感性資料之方法。

D. 預期結果

PCS 提供敏感性資料的異地備份功能，且與送測單位提供的文件相符。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

6.5.4. 更新系統安全

6.5.4.1. PCS 須支援線上或手動的軟韌體更新功能。(1 級、2 級、3 級)

A. 測試目的

確保 PCS 可保持最新的軟韌體狀態。

B. 測試條件

送測單位提供檢測實驗室更新版本的軟韌體檔案，並且告知版本號或功能上的差異性。

C. 測試步驟

(1) 查看當前 PCS 的軟韌體版本號或功能。

(2) 執行線上及/或手動的軟韌體更新功能。

(3) 比對更新前後的軟韌體版本號或功能，確認結果是否與送測單位所述相符。

D. 預期結果

PCS 提供手動或線上的軟韌體更新功能，且更新後的軟韌體版本號或功能上的差異性與送測單位所述相符。

E. 測試結果。

「通過」：符合預期結果。

「不通過」：不符合預期結果。

6.5.4.2. 當軟韌體更新作業失敗時，PCS 仍須回復正常運作。(1 級、2 級、3 級)

A. 測試目的

確保 PCS 的軟韌體更新功能具備失效安全（fail-safe）的機制。

B. 測試條件

送測單位提供檢測實驗室更新版本的軟韌體檔案。

C. 測試步驟

(1) 執行 PCS 的軟韌體更新功能。

(2) 在更新作業的執行過程中，試圖以各種方法中斷更新程序，例如：拔除網路線、中斷電源、關機或其它可中斷更新程序之方法。

(3) 查看 PCS 是否可回復正常運作或穩定的狀態。

D. 預期結果

PCS 可回復正常的運作狀態，未發生非預期的錯誤。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

6.5.4.3. 若支援手動的軟韌體更新，PCS 須能驗證軟韌體的數位簽章或訊息鑑別碼，確保軟韌體之來源性與完整性。(1 級、2 級、3 級)

A. 測試目的

PCS 應能驗證軟韌體檔案的數位簽章或訊息鑑別碼，確保軟韌體之來源性與完整性。

B. 測試條件

(1) 送測單位提供文件說明產生軟韌體檔案的數位簽章或訊息鑑別碼的方法以及驗證數位簽章或訊息鑑別碼的方法。

(2) 送測單位提供檢測實驗室更新版本的軟韌體檔案。

(3) PCS 提供手動的軟韌體更新功能。

C. 測試步驟

(1) 根據送測單位的文件，檢測實驗室為軟韌體檔案自行產生數位簽章值或訊息鑑別碼。

(2) 將檢測實驗室自製的數位簽章值或訊息鑑別碼附加在軟韌體檔案中或其它合適的存放位置。

(3) 執行手動的軟韌體更新功能，然後確認軟韌體更新功能是否拒絕偽造的數位簽章值或訊息鑑別碼。

D. 預期結果

因偽造的數位簽章值或訊息鑑別碼，PCS 拒絕更新軟韌體。

E. 測試結果

「通過」：符合預期結果。

「不通過」：不符合預期結果。

「不適用」: PCS 未具備手動的軟韌體更新功能。

6.5.4.4. 若支援線上的軟韌體更新，PCS 與更新伺服器之間應建立安全通道，其須符合附錄 B 之安全通道版本以及密碼套件。(2 級、3 級)

A. 測試目的

PCS 與軟韌體更新伺服器之間應建立安全通道來完成線上的軟韌體更新程序，確保軟韌體的來源性以及完整性。

B. 測試條件

PCS 提供線上的軟韌體更新功能。

C. 測試步驟

(1) 建立 PCS 與軟韌體更新伺服器之間的網路封包側錄環境。

(2) 執行 PCS 提供的線上軟韌體更新程序。

(3) 軟韌體更新程序完成後，查看 PCS 與軟韌體更新伺服器之間的網路通訊協定。

(4) 查看軟韌體更新伺服器的數位憑證之有效性。

D. 預期結果

(1) PCS 與軟韌體更新伺服器之間建立安全通道，且符合附錄 B 所列之安全通道版本以及密碼套件。

(2) 軟韌體更新伺服器採用有效的數位憑證建立安全通道，包含：正確的主體名稱與主體別名、有效期限內以及由可信任的憑證簽發單位所核發。

E. 測試結果

「通過」: 符合預期結果(1)及(2)。

「不通過」: 不符合預期結果(1)或(2)。

「不適用」: PCS 未具備線上的軟韌體更新功能。