關鍵資訊基礎設施資安防護建議

中華民國107年11月

目　次

圖 目 次

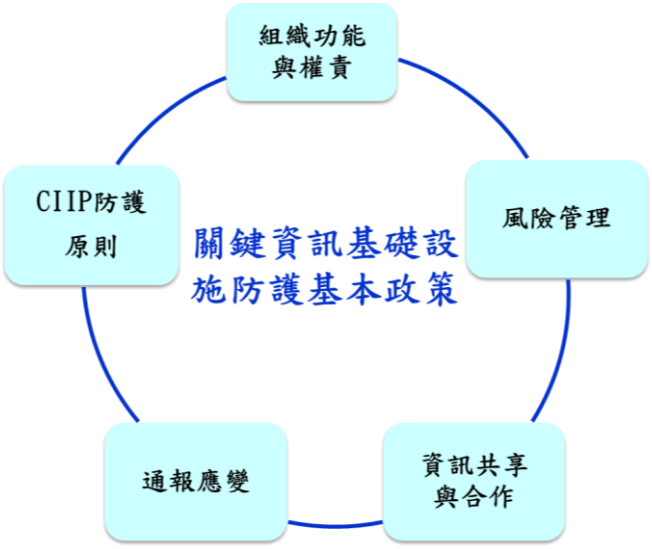
表 目 次

1. 前言

為落實「關鍵資訊基礎設施防護基本政策」，特制定「關鍵資訊基礎設施資安防護建議」(以下簡稱本防護建議)，以提供關鍵基礎設施領域層級作為制定資安防護基準之參考。

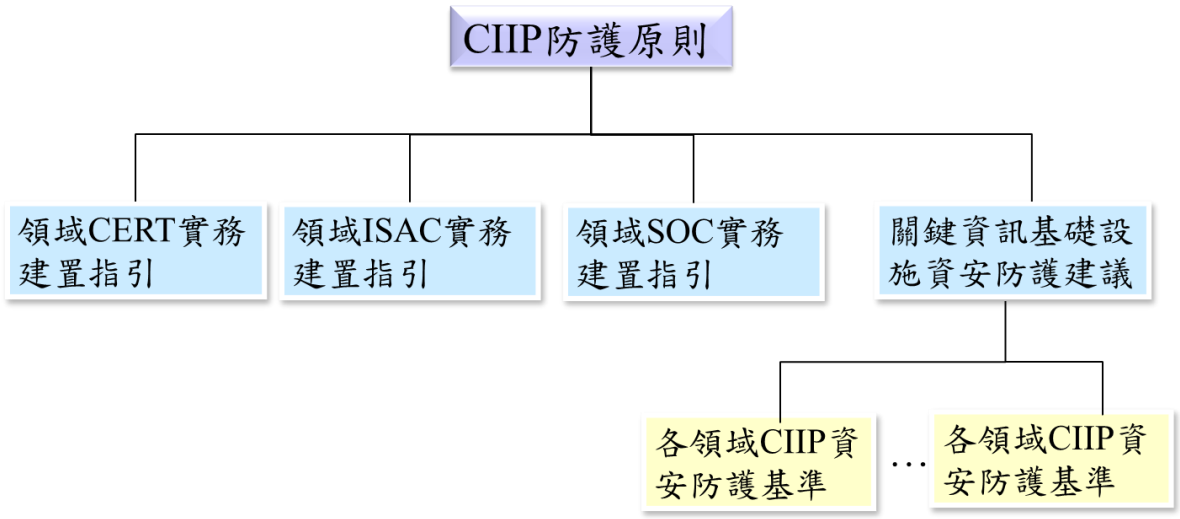
1.1 目的

依循「關鍵資訊基礎設施防護基本政策」架構(詳見圖 1)，為強化關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)能量，各關鍵基礎設施領域須落實 CIIP 防護原則，故由國家層級制定本防護建議(詳見圖 2)，提供各關鍵基礎設施領域層級參考，再由各關鍵基礎設施領域層級依領域特性，訂定資安防護基準相關文件，以提升關鍵資訊基礎設施資安防護能力。



資料來源：本計畫整理

圖1　我國 CIIP 基本政策架構



資料來源：本計畫整理

圖2　CIIP 防護原則架構

1.2 使用建議

依「關鍵基礎設施防護基本政策」定義，關鍵資訊基礎設施是架構於關鍵基礎設施(Critical Infrastructure, CI)之八大領域基礎上，包含能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關及高科技園區。關鍵資訊基礎設施(Critical Information Infrastructure, CII)係指涉及核心業務運作，為支持關鍵基礎設施持續營運所需之重要資訊系統或調度、監控與數據擷取系統(Supervisory Control and Data Acquisition, SCADA)，亦屬關鍵基礎設施之重要元件。

依 CII 所涵蓋多樣性系統類型，如資通系統(Information and Communication Technology, ICT)、工業控制系統(Industrial Control Systems, ICS)及資訊系統(Informational Technology, IT)等。針對 ICT 與 IT 因系統性質較相近，相關防護建議請參考「資訊系統分級與資安防護基準作業規定」[2]。

本防護建議針對 ICS 提出通用性防護建議，各關鍵基礎設施領域層級參考本防護建議，依領域特性調修防護建議內容，進而制定資安防護基準。

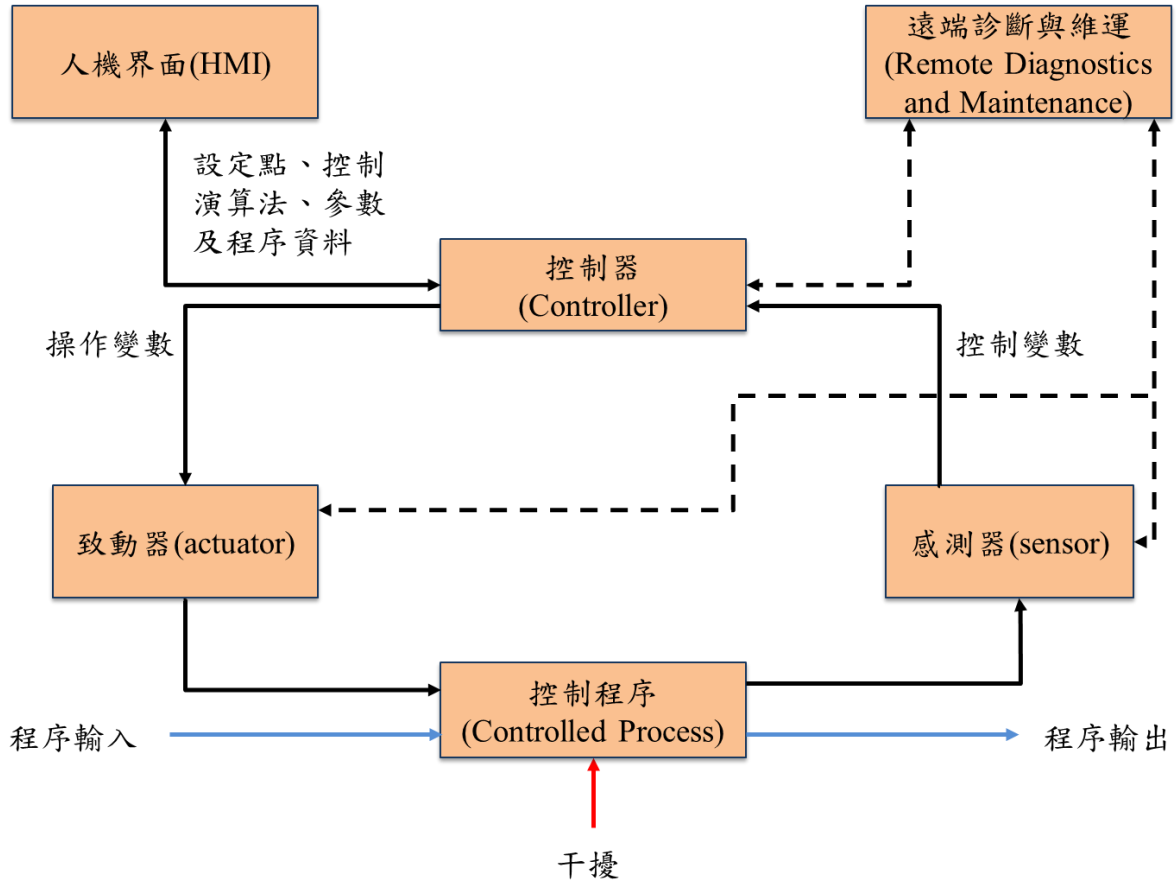
2. 工業控制系統簡介

ICS 是所有控制系統類型的總稱，由各種自動化控制元件與透過感知、監測等之流程監控系統，所涵蓋領域非常廣泛，如電力、水、油、天然氣、通訊、食物、交通及製造業等相關領域，其中常見控制系統包含 SCADA、分散式控制系統(Distributed Control Systems, DCS)及可程式邏輯控制器(Programmable Logic Controller, PLC)等[3]。

2.1 ICS 運作

典型 ICS 使用網路串接控制迴路、人機介面(Human Machine Interface, HMI)、遠端診斷及維修工具等。而控制迴路藉由感測器(sensor)、致動器(actuator)及控制器(如 PLC 等)調整欲控制之流程，詳見圖 3。

感測器將所量測到的實體狀態由類比訊號轉換成數位資料，傳送至控制器做為控制變數。控制器解析控制變數計算出對應的操作變數，並送至致動器(如控制閥、斷路器、開關及馬達等)，致動器接收到控制器命令後，進行流程調整。HMI 可以顯示流程現狀與程序資訊，維運人員與工程人員可透過 HMI 監控與規劃設備設定值、控制邏輯及建立控制器內之參數。遠端診斷與維修工具主要在於預防、辨別及回復操作流程中的異常或故障[3]。



資料來源：本計畫整理

圖3　ICS 運作

2.2 SCADA 簡介

SCADA 系統主要用於控制分散設備(如電力傳送與分配系統、軌道及公共運輸系統等)[3]，以集中式進行控制數據蒐集，其組成包含數據蒐集系統、數據傳輸系統及 HMI 軟體。SCADA 系統透過 HMI 彙整流程資料及傳輸流程訊息，進行集中式監視與控制。維運人員可從集中控制室即時監控整個系統，並根據系統的複雜性與相關設置，調整系統之控制與運作，任務可自動執行或由維運人員下指令執行。

典型硬體設備包含控制中心的控制伺服器、通訊設備，以及一個或多個分散在不同廠區之遠程終端單元(Remote Terminal Unit, RTU)或 PLC 等，控制

伺服器儲存與處理 RTU 傳送來之輸出輸入訊息。

常見 SCADA 系統詳見圖 4，控制中心設置控制伺服器、通訊路由器、HMI、工程工作站及歷程資料伺服器(Data Historian Server)。HMI 顯示現場與紀錄資訊，控制中心負責警報、趨勢分析、報表集中管理，以及依據所偵測到的事件採取行動。維運人員可於現場執行致動器控制與感測器之監視，以及透過現場遠端設備執行遠端偵測與修復。控制中心與現場透過網路通訊(如電話線、電纜、光纖、無線電、廣播、微波及衛星等)傳送資訊，其所包含子系統說明如下：

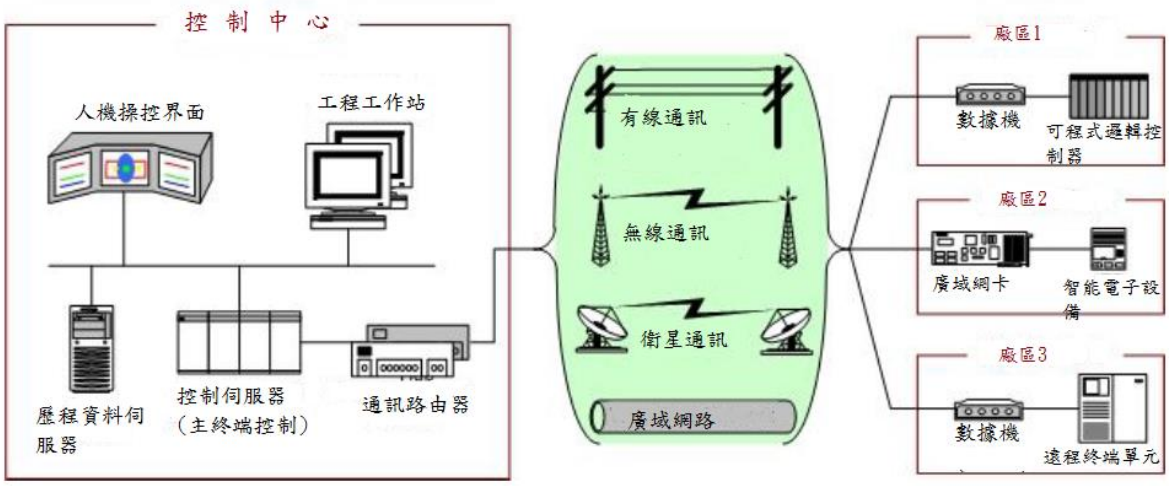
- PLC 是在傳統的順序控制器的基礎上，引入微電子技術、計算機技術、自動控制技術及通訊技術而形成的工業控制裝置，目的是用來取代繼電器、執行邏輯、計時及計數等順序控制功能。國際電工委員會（International Electrotechnical Commission, IEC）頒布 IEC 61131-3，針對 PLC 提出共通性程式語言。PLC 是一種數字運算操作的電子系統，專為在工業環境下應用而設計，它採用可編程式的儲存器，用來在其內部儲存執行邏輯運算、順序控制、定時、計數及算術運算等操作的指令，並通過數字的、模擬的輸入與輸出，控制各種類型的機械或生產流程。PLC 及其相關設備，都應易於與工業控制系統形成一個整體，易於擴充其功能的原則設計。在工業自動化與控制系統的網路體系結構中，PLC 為重要的控制元件，通常用於實現工業設備的具體操作與功能控制，通過迴路控制提供集中式流程管理。

- HMI 是一個可以顯示流程狀態的裝置，作業人員可以依此裝置監視與控制程式，可以採集資料，也可以送出監控指令。HMI 會連結到 SCADA 系統的資料庫與軟體，讀取相關資訊，以顯示趨勢、診斷資料及相關管理用的資訊，如定期維護程式、物流資訊、特定感測器或機器的細部線路圖或連線至可協助故障排除的專家系統。

●RTU 連接許多實體感測器，並將類比信號資料採集後，轉換成數位訊號，將數位的資料傳送給監控系統。

●智能電子設備(Intelligent Electronic Device, IED)係指應用在水、電及天然氣等關鍵基礎設施電子感測(如智慧電表)等設備。

●歷程資料庫伺服器用來存放 SCADA 設備所蒐集的歷程資料。



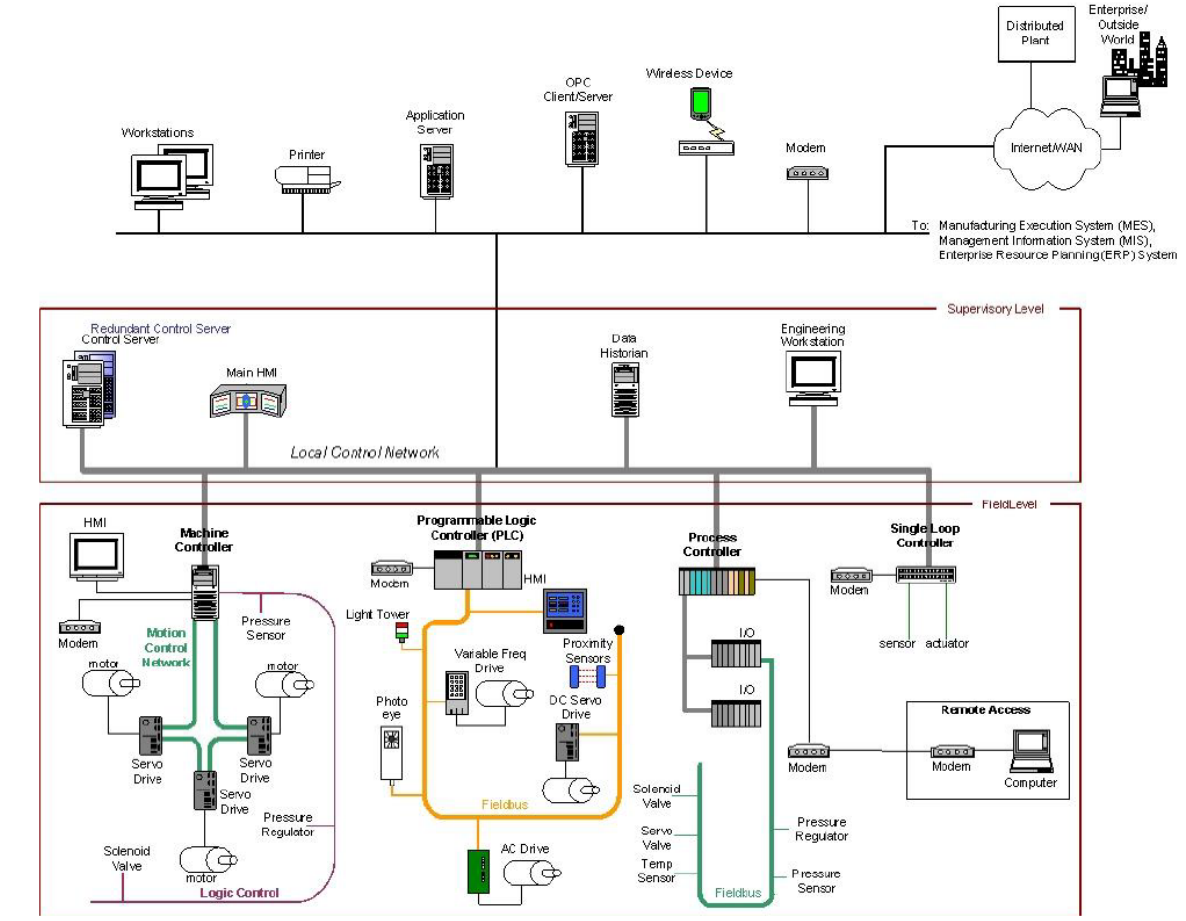
資料來源：本計畫整理

圖4　常見 SCADA 系統架構

2.3 DCS 簡介

DCS 主要用於在同一廠區內控制生產流程的系統[3]，如煉油廠、水處理廠、發電廠、化工廠、汽車廠、製藥廠等工業流程。DCS 是整合式控制架構，控制監督多種整合的子系統，並採用集中監控的方式協調系統內之控制器以執行整個生產流程。透過模組化生產系統，DCS 降低單點故障對整個系統的影響，並使用在須具有高可靠性與安全性的大型連續生產流程工廠，在許多現代化系統中，DCS 系統與企業網路串接，以便提供企業運作所需之生產資訊。

DCS 涵蓋從底層生產流程到企業層的整套設備(詳見圖 5)，一個監控伺服器經由控制網路連接其下所屬設備，控制器依據控制伺服器命令與感測器的測量值，控制流程上的致動器，廠區控制裝置使用標準工業通訊協定(如 Modbus 等)。



資料來源：[3]

圖5　常見 DCS 系統架構

2.4 其他類型控制系統

其他類型控制系統也具有相似的功能特徵，許多建築、交通、醫療及物流系統使用不同的通訊協定，但它們與傳統 ICS 具有相似的特性，都需要考量其安全性[3]，例如：

- 能源管理系統。
- 照明控制系統。
- 火警系統。
- 滅火系統。
- 入侵偵測系統。
- 實體存取系統。
- 垂直運輸系統(如電梯與電扶梯)。
- 實驗室儀器控制系統。

3. 文獻探討

為對工業控制系統提出通用性防護建議，本防護建議參考國際安全標準與主要國家防護文件，包含 NIST SP800-82[3]、IEC 62443-3-3[5]、北美電力可靠度協會(North American Electric Reliability Corporation, NERC)提出之 CIP V5[6]、美國核子管理委員會(Nuclear Regulatory Commission, NRC)提出之 RG5.71[7]，以及中國大陸「工業控制系統信息安全防護指南」[9]與 GB/T 33009.1「工業自動化和控制系統信息安全 集散控制系統(DCS)第 1 部分：防護要求」[10]等。

3.1 NIST SP800-82

美國 NIST SP800-82[3]定義 ICS 包含 SCADA、DCS 及其他支援工業流程相關系統，同時提出 18 類安全領域，共 221 項安全防護建議(請參考表 1)，其中註記顯示之數據表示控制措施數。

表1　NIST SP800-82 安全防護

ID	安全領域	ID	安全領域
AC (22)	Access Control 存取控制	MP (7)	Media Protection 媒體防護
AT (4)	Awareness and Training 認知與訓練	PS (8)	Personnel Security 人員安全
AU (12)	Audit and Accountability 稽核與可歸責性	PL (8)	Planning 規劃
CA (9)	Security Assessment and Authorization 安全評鑑與授權	PE (18)	Physical and Environmental Protection 實體與環境防護
CM (11)	Configuration Management 組態管理	RA (5)	Risk Assessment 風險評鑑

ID	安全領域	ID	安全領域
CP (12)	Contingency Planning 營運持續計畫	SA (9)	System and Services Acquisition 系統與服務獲得
IA (8)	Identification and Authentication 識別與鑑別	SC (41)	System and Communications Protection 系統與通訊防護
IR (8)	Incident Response 事件通報應變	SI (17)	System and Information Integrity 系統與資訊完整性
MA (6)	Maintenance 維護	PM (16)	Program Management 計畫管理

資料來源：本計畫整理

3.2 IEC 62443-3-3

由 ISA99 委員會與 IEC 技術委員會第 65 工作組(TC65WG10)，共同開發 62443 系列標準，以符合網路安全要求與工業自動化控制系統(Industrial Automation Control Systems, IACS)復原力要求。若文件編號為「ISA-62443-x-y」，表示由 ISA 所發布；文件編號為「IEC 62443-x-y」則表示由 IEC 所發布[4]。

62443 系列以資訊技術系統(如 ISO/IEC 27000 系列等)的安全標準為基礎，依 IACS 環境特性制定相關安全標準。62443 系列可分為 4 大群組(詳見圖 6)，以下將對群組與組成元素進行說明：

- 共同(General)：此群組針對整個系列共同元素進行說明。
  - 62443-1-1 於 2007 年發行初版，內容介紹 62433 系列概念與模組。
  - 62443-1-2 說明 62443 系列所使用的專有名詞與名詞縮寫之技術報告。

– 62443-1-3 描述 62443 系列基礎與系統之相關量化方法標準。

– 62443-1-4 使用範例說明 IACS 元件層的生命週期安全技術報告。

●政策與程序(Policies and Procedures)：說明 IACS 安全相關政策與程序。

– 62443-2-1 此標準於 2009 年發行初版，內容要求與定義 IASC 網路安全管理系統，包含使用者與設備擁有者等相關權責。

– 62443-2-2 提供 IASC 網路安全管理系統營運要求指引標準。

– 62443-2-3 於 2015 年由 ISA 與 IEC 共同發表 IACS 之更新管理指引報告。

– 62443-2-4 對其他控制系統供應商的要求準則之標準。

●系統要求(System Requirements)：強調在系統層的安全要求。

– 62443-3-1 描述在 IACS 環境所使用的安全技術報告。

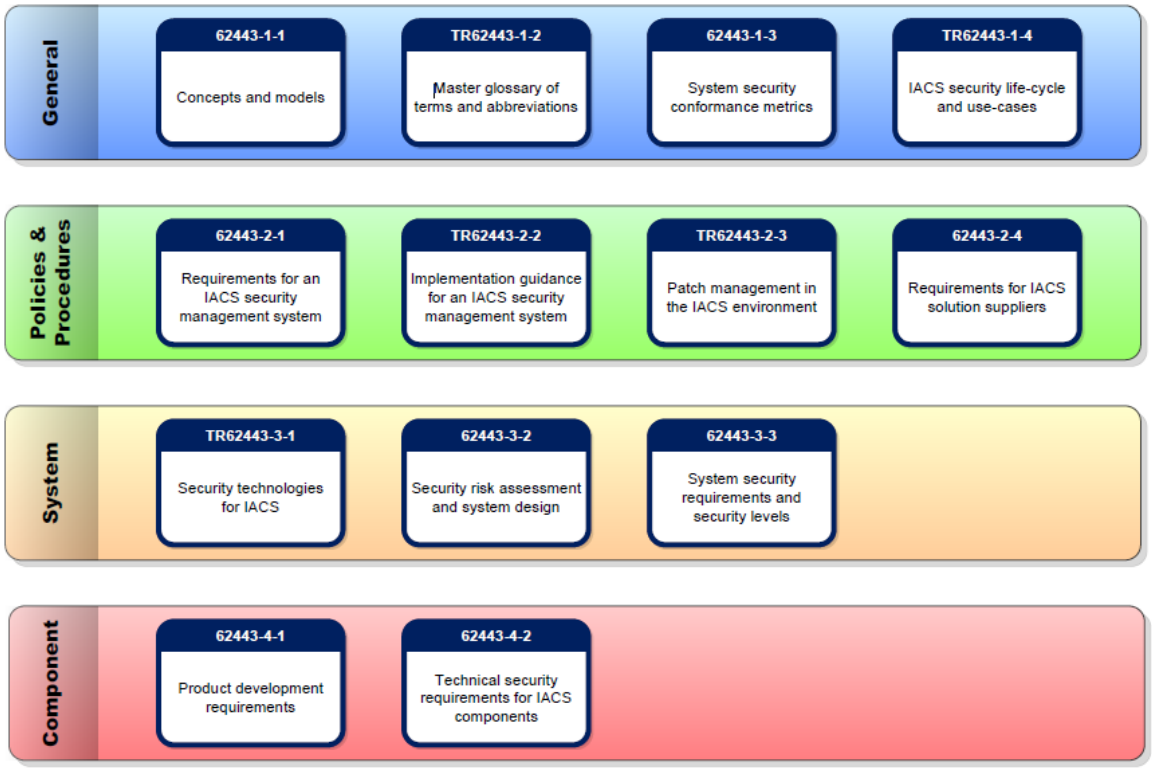
– 62443-3-2 強調 IACS 系統安全設計與風險評估標準。

– 62443-3-3 於 2013 年發行，針對系統安全與安全層級要求之標準。

●元件要求(Component Requirements)：強調與 IACS 相關產品開發的安全要求規格。

– 62443-4-1 適用開發產品之要求標準。

– 62443-4-2 對子系統、系統組成元件及其他控制系統供應商等列入系統規範要求之標準。



資料來源：[4]

圖6　IEC 62443 系列

62443-3-3 安全標準內容[5]，依循 62443-1-1 所定義的 7 大類基本要求架構，針對系統安全與安全層級提出安全標準要求。

- 識別與鑑別控制(Identification and authentication control, IAC)。
- 使用控制(Use control, UC)。
- 系統完整性(System integrity, SI)。
- 資料機敏性(Data confidentiality, DC)。
- 資料流限制(Restricted data flow, RDF)。
- 事件回應(Timely response to events, TRE)。
- 資源可用性(Resource availability, RA)。

IEC 62443-3-3 提出 7 類基本要求，共 100 項安全防護建議(請參考表 2)，其中註記顯示之數據表示控制措施數。

表2　IEC 62443-3-3 控制措施

ID	安全領域	ID	安全領域
IAC (24)	Identification and authentication control 識別與鑑別控制	RDF (11)	Restricted data flow 資料流限制
UC (24)	Use control 使用控制	TRE (3)	Timely response to events 事件回應
SI (19)	System integrity 系統完整性	RA (13)	Resource availability 資源可用性
DC (6)	Data Confidentiality 資料機敏性		

資料來源：本計畫整理

3.3 NERC CIP V5

NERC 屬於非營利公司，其使命為確保北美大眾電力系統之可靠性，監督緊鄰美國的國家包含加拿大與墨西哥部分互聯電力系統。NERC 主要職責包含與所有利害相關者合作，制定電力系統運行標準，監測與執行遵守標準，評估資源充足性，以及提供教育與培訓。

CIP V1 為 NERC 2008 年制定專論電力關鍵基礎設施的網路安全標準[8]，每年透過聯邦能源監管委員會制定安全防護標準，至今已發展至 CIP V5。

CIP V5 提出 14 類安全領域[6]，共 257 項安全防護要求(請參考表 3)，其中註記顯示之數據表示控制措施數。在 CIP V5 中，CIP-002~CIP-012 為專論網路安全標準(CIP-012 安全防護要求目前為草案階段)。

表3　NERC V5 安全防護要求

ID	安全領域	ID	安全領域
CIP-001 (12)	Sabotage Reporting 設備破壞報告	CIP-008 (11)	Cyber Security — Incident Reporting and Response Planning 資通安全-事件通報應變與回應計畫
CIP-002 (17)	Cyber Security — Critical Cyber Asset Identification 資通安全-識別關鍵資通資產	CIP-009 (26)	Cyber Security — Recovery Plans for Critical Cyber Assets 資通安全-關鍵資通資產復原計畫
CIP-003 (39)	Cyber Security — Security Management Controls 資通安全-安全管理控制	CIP-010 (7)	Cyber Security — Configuration Change Management and Vulnerability 資通安全-組態變更管理與弱點
CIP-004 (26)	Cyber Security — Personnel & Training 資通安全-人員與訓練	CIP-011 (6)	Cyber Security — Information Protection 資通安全-資訊防護
CIP-005 (20)	Cyber Security — Electronic Security Perimeter(s) 資通安全-電子安全場域	CIP-012 (2)	Cyber Security – Control Center Communication Networks 資通安全-控制中心通訊網路
CIP-006 (36)	Cyber Security — Physical Security of Critical Cyber Assets 資通安全-關鍵資通資產實體安全	CIP-013 (3)	supply chain 供應鏈

ID	安全領域	ID	安全領域
CIP-007 (46)	Cyber Security — Systems Security Management 資通安全-系統安全管理	CIP-014 (6)	Physical Security 實體安全

資料來源：本計畫整理

3.4 NRC RG5.71

美國核子管理委員會認知核電廠數位技術的使用日益增加，導致潛在的資通安全相關問題，故整合電機工程師協會(IEEE)、NIST 及美國國土安全部(Department of Homeland Security, DHS)發展 RG5.71[7]。

RG5.71 參考 NIST SP800-53[1]與 SP800-82[3]，依據核設施獨特環境制定包含技術、營運及管理組成安全管控的防禦策略。

RG5.71 提出 14 類安全領域，共 152 項安全防護要求(請參考表 4)，其中註記顯示之數據表示控制措施數。

表4　RG5.71 安全防護要求

ID	安全領域	ID	安全領域
A.2 (2)	Cyber Security Plan 資通安全計畫	C.3 (11)	System and Information Integrity 系統與資訊完整性
A.3 (3)	Cyber Security Program Implementaion 資通安全程序實施	C.4 (3)	Maintenance 維護

ID	安全領域	ID	安全領域
A.4 (3)	Maintaining the Cyber Security program 維護資通安全計畫	C.5 (6)	Physical and Environmental Protection 實體與環境防護
A.5 (1)	Document Control and Records Retention and Handling 文件控制、紀錄保留及處理	C.6 (1)	Defensive Strategy 防禦策略
B.1 (23)	Access Control 存取控制	C.7 (1)	Defense-in-Depth 深度防禦
B.2 (12)	Audit and Accountability 稽核與可歸責性	C.8 (8)	Incident Response 事件回應
B.3 (22)	Critical Digital Asset and Communications Protection 關鍵數位資產與通訊防護	C.9 (6)	Contingency Planning/Continuity of Safety、Security and Emergency Preparedness Funtions 持續計畫
B.4 (9)	Identification and Authentication 識別與鑑別	C.10 (10)	Awareness and Training 認知與訓練
B.5 (5)	System Hardening 系統強化	C.11 (9)	Configuration Management 組態管理
C.1 (6)	Media Protection 媒體防護	C.12 (6)	System and Services Acquisition 系統與服務獲得
C.2 (2)	Personnel Security 人員安全	C.13 (3)	Security Assessment and Risk Management 安全評估與風險管理

資料來源：本計畫整理

3.5 GB/T 33009.1

本節論述中國大陸對工業控制系統的資安防護相關措施，以下說明保留中國大陸原用語。

2016 年中國大陸工業和信息化部發布「工業控制系統信息安全防護指南」[9]，並發布 GB/T 33009.1「工業自動化和控制系統信息安全集散控制系統(DCS)第 1 部分：防護要求」[10]。

工業控制系統信息安全防護指南提出 11 項工業控制系統安全防護，摘要內容如下：

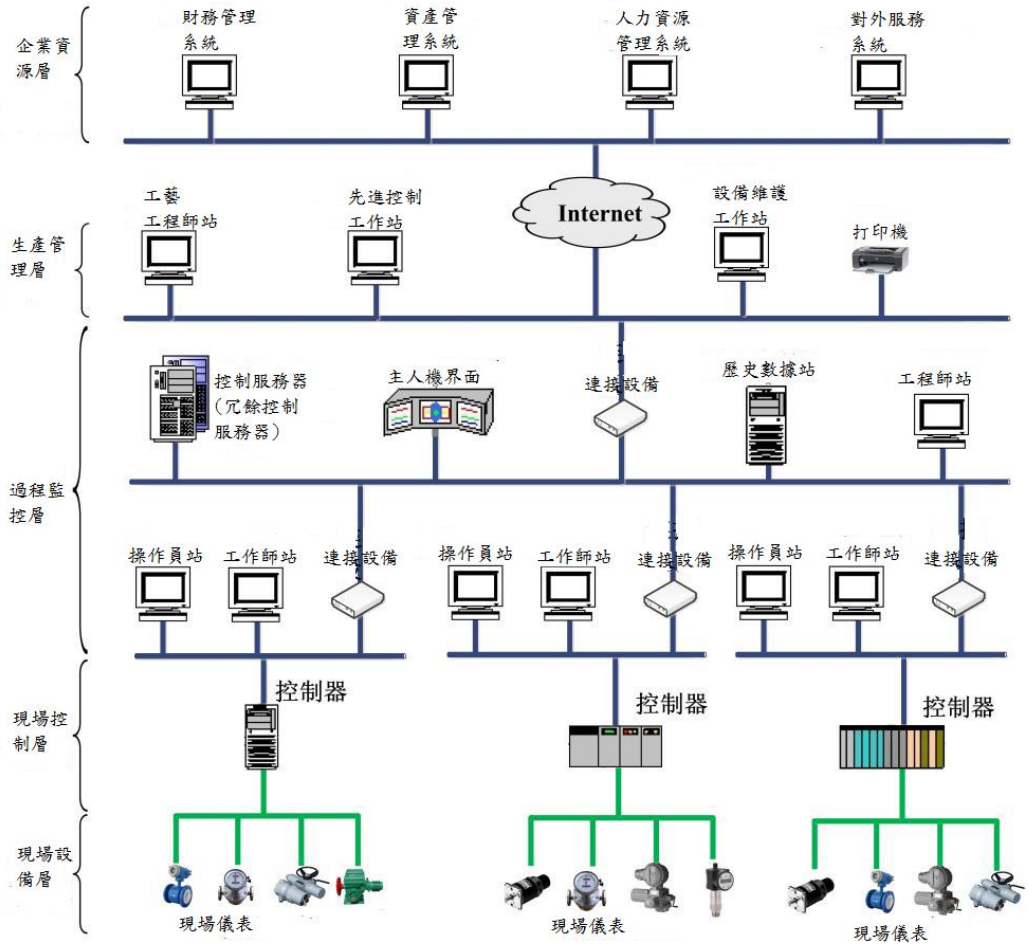
- 安全軟件選擇與管理：提出工業系統使用防毒軟體或軟體白名單，並建立入侵防護管理機制。
- 配置與補釘管理：建立安全漏洞與更新管理機制，包含定期稽核與更新測試等。
- 邊界安全防護：依據工業控制系統性質區分生產、測試及開發環境，並建立防火牆等防護設備進行安全防護。
- 物理含環境安全防護：對重要的控制軟硬體所在區採取物理安全防護措施，並針對不必要的傳輸媒介(如 USB 等)進行拆除與嚴格控制。
- 身分認證：對於主機登錄、服務資源使用採用雙重認證，並以最小特權原則建立帳號權限。
- 遠程訪問安全：禁止工業系統使用 FTP、HTTP 及 Telnet 等網路服務，系統須留存日誌檔案，並定期進行稽核。
- 安全監測與應急預案演練：應部署網路安全監測設備，建立應急預案計畫相關標準作業程序與相關演練。
- 資產安全：建設工業控制系統資產清單與相關負責人，以及相關資產使用規則。

●數據安全：針對工業系統傳輸數據進行保護，並定期備份。

●供應鏈管理：對於系統服務商應以合同方式明確說明信息安全責任與義務，並要求服務商做好保密工作。

●落實責任：建立工控安全管理機制、成立信息安全協調小組，落實工控安全責任制，部署工控安全防護措施。

工業自動化和控制系統信息安全集散控制系統(DCS)第 1 部分：防護要求，依據典型 DCS 系統網路結構(詳見圖 7)進行安全防護要求規劃，GB/T 33009.1 由 5 個部分組成，詳見表 5。並依要求項目提出基本要求、常規要求(含加強要求、深度加強要求)提出共 97 項防護標準。



資料來源：[10]

圖7　典型 DCS 系統的網路結構示意

表5　GB/T 33009.1

安全領域	要求項目
安全防護概述 (5)	▪通用 DCS 系統網路結構 ▪DCS 防護總體要求和原則
物理訪問控制要求 (4)	提出包含機房與進出人員等相關4點基本要求
過程監控層信息安全 (47)	▪區域劃分　▪安全審計 ▪訪問與使用控制　▪資源控制 ▪入侵防禦　▪數據安全 ▪身分鑑別與認證
現場控制層信息安全 (28)	▪區域劃分　▪安全審計 ▪訪問與使用控制　▪資源控制 ▪入侵防禦　▪數據安全 ▪身分鑑別與認證
現場設備層信息安全 (13)	▪區域劃分　▪安全審計 ▪訪問與使用控制　▪數據安全 ▪入侵防禦 ▪身分鑑別與認證

資料來源：本計畫整理

3.6 文獻分析

依上述 NIST SP800-82、IEC 62443-3-3、NERC CIP V5、NRC RG5.71 及 GB/T 33009.1，針對於適用範圍、ICS 網路架構、存取控制、稽核管理、營運持續及實體防護等 18 項安全防護建議分析(詳見表 6)。

綜合分析結果，以 NIST SP800-82 所涵蓋的防護面向範圍最為廣泛，包含事前管理如風險評鑑、安全控制措施等；事中應變如事件通報應變等；事

後改善如營運持續計畫等；以及組織內計畫管理建議。另外，NIST SP800-82 所提列 ICS 安全防護的控制措施項目最為周全，因此本防護建議參考 NIST SP800-82 架構，並依據我國國情提出針對 ICS 相關系統與資料之防護要求建議。各關鍵基礎設施領域層級可參酌本防護建議，依領域特性調修防護建議內容，進而制定資安防護基準。

表6　文獻分析比較

國際安全標準與主要國家防護文件 / 安全防護建議	NIST SP800-82	IEC 62443-3-3	NERC CIP V5	NRC RG5.71	GB/T 33009.1	補充說明
1.適用範圍	適用所有 ICS	適用所有 ICS	適用電力產業	適用核電廠	適用所有 ICS	
2.工業控制系統網路架構	✓	✓			✓	▪ NIST、IEC 及 GB/T：提出防火牆與網段防護要求 ▪ NERC 與 NRC：未詳細說明與要求，所以不列入
3.存取控制	✓	✓	✓	✓	✓	5 份文件均有針對帳號管理、遠端存取及存取權限等均有安全防護要求
4.稽核與可歸責性	✓	✓	✓	✓	✓	5 份文件均有對稽核所需的內容、稽核資訊防護、時戳及日誌檔等提出控制要求

國際安全標準與主要國家防護文件 安全防護建議	NIST SP800-82	IEC 62443-3-3	NERC CIP V5	NRC RG5.71	GB/T 33009.1	補充說明
5.安全評鑑與授權	✓	✓	✓	✓	✓	▪ NIST、NRC：對於安全評鑑、安全程序、管理授權，以及對滲透測試等提出要求 ▪ IEC、NERC 及 GB/T：提出安全評鑑、安全程序等提出要求，但未對 ICS 滲透測試提出要求
6.組態管理	✓	✓	✓	✓	✓	5 份文件均有對組態變更、組態制定程序等提出安全要求
7.營運持續計畫	✓			✓		▪ NIST 與 NRC：提出制定營運持續計畫要求 ▪ IEC、NERC 及 GB/T：著重在 ICS 安全防護控制措施實作，因此並未提出營運持續管理面要求

國際安全標準與主要國家防護文件 安全防護建議	NIST SP800-82	IEC 62443-3-3	NERC CIP V5	NRC RG5.71	GB/T 33009.1	補充說明
8.識別與鑑別	✓	✓	✓	✓	✓	5 份文件對識別與鑑別控制措施要求內容相似
9.事件通報應變	✓		✓	✓		▪ NIST、NERC 及 NRC：對事件通報處理、監控及通報均有提出要求 ▪ IEC 及 GB/T 未提出事件通報應變相關要求
10.維護	✓		✓	✓	✓	▪ NIST、NERC、NRC 及 GB/T：提出系統、組織管理及人員等維護控制要求 ▪ IEC：未特別提出相關要求
11.媒體防護	✓	✓	✓	✓	✓	5 份文件均有對媒體存取、傳輸等提出防護要求
12.實體與環境防護	✓	✓	✓	✓	✓	5 份文件均對 ICS 實體存取、訪客存取及相關備援等提出防護要求

國際安全標準與主要國家防護文件 安全防護建議	NIST SP800-82	IEC 62443-3-3	NERC CIP V5	NRC RG5.71	GB/T 33009.1	補充說明
13.安全計畫	✓		✓	✓		▪NIST、NERC 及 NRC：提出安全計畫管理的相關要求 ▪IEC 與 GB/T：未對組織安全管理面提出相關要求
14.人員安全	✓		✓	✓		▪NIST、NERC 及 NRC：均有對人員篩選、離職等相關安全管理提出要求 ▪IEC 與 GB/T：未對人員安全管理面提出相關要求
15.風險評鑑	✓			✓		▪NIST 與 NRC：有提出風險評鑑方法 ▪IEC、NERC 及 GB/T：未提出風險評鑑相關方法與要求
16.系統與服務獲得	✓	✓	✓	✓	✓	5 份文件對外部系統服務、系統文件及系統開發等提出相關要求

國際安全標準與主要國家防護文件 安全防護建議	NIST SP800-82	IEC 62443-3-3	NERC CIP V5	NRC RG5.71	GB/T 33009.1	補充說明
17.系統與通訊防護	✓	✓	✓	✓	✓	5 份文件對資料傳輸、儲存安全及系統服務等提出相關防護要求
18.系統與資訊完整性	✓	✓	✓	✓	✓	5 份文件對漏洞修補、惡意程式防護及系統監控等提出相關防護要求

資料來源：本計畫整理

4. 工業控制系統防護建議

依 3.6 文獻分析結果，以 NIST SP800-82 所提列 ICS 安全防護的控制措施項目最為周全，因此本防護建議主要參考 NIST SP800-82 架構，並依據我國資通系統資安防護基準之類別為基礎，增加網路架構、實體與環境防護及組織管理等防護類別，提出針對 ICS 相關系統與資料之防護要求。

本防護建議使用 ICS，做為一個描述用於工業產物之類比與數位控制系統的總稱。ICS 包含 SCADA、DCS、PLC、程式自動控制器(Programmable Automation Control, PAC)、HMI、儀控(Instrumentation and Control, I&C)及營運技術(Operations Technology, OT)。

參考 NIST SP800-82 架構與美國工業控制系統網路緊急應變小組(Industrial Control Systems Cyber Emergency Response Team, ICS-CERT) 2016 年報告[11]，彙整「工業控制系統網路架構」、「存取控制」、「稽核與可歸責性」、「營運持續計畫」、「識別與鑑別」、「系統與通訊防護」、「系統與服務獲得」、「實體防護」、「系統與資訊完整性」、「組態管理」及「組織管理」等 11 大類別納入本防護建議，並強調 ICS 相關系統與資料之完整性與可用性。

4.1 工業控制系統網路架構(ICS Network Architecture)

工業控制系統網路存在 ICS 網路與內部 IT 網路串接邊界脆弱性，基於工業控制系統與企業網路之差異性，工業控制系統應依據其特性，規劃網路架構與邊界防護，強化其資通安全防護強度。

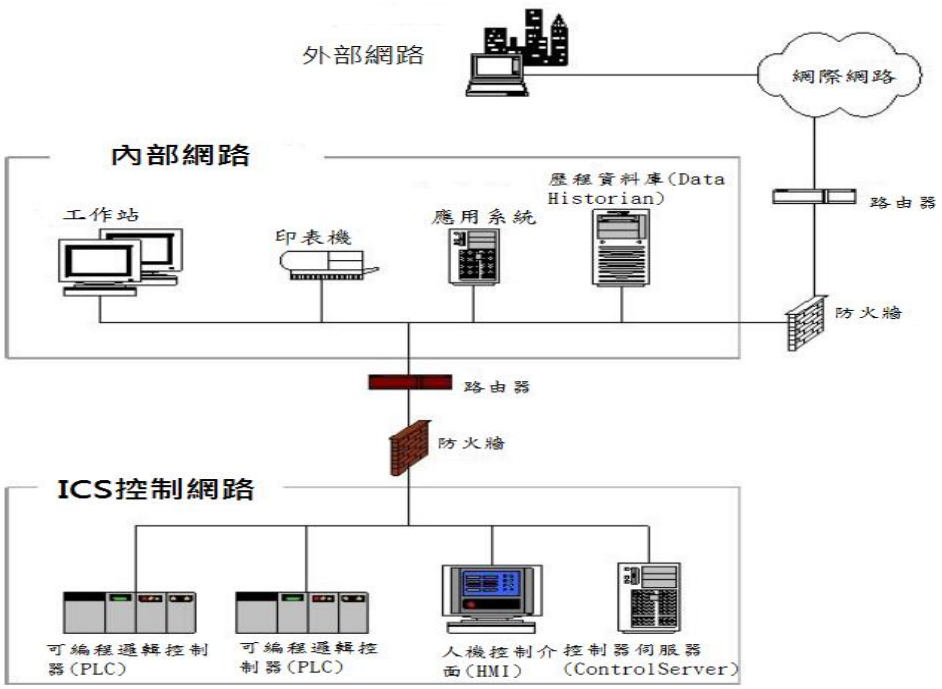
4.1.1 網段規劃(Network Segregation)

因業務需求，ICS 資料須透過網路進行資料存取與監控，此 2 個異質系統經由網路進行相連後，若無適當安全防護機制，將因彼此連結，增加彼此資安威脅與隱憂。

基於上述原因，建議組織應依據系統功能與服務特性等，進行網段規劃，並於不同網段間架設防火牆，過濾彼此資料傳輸封包，強化安全防護，以下將針對不同安全強度的網段規劃進行說明，可做為組織網段規劃之建議。

●低安全防護

基於異質的裝置與網路封包，應在 ICS 控制網路前，架設可過濾內部網路與 ICS 控制網路之不同異質網路封包(如 HTTP 與 Modbus 等)之防火牆，並在內部網路對外連線架設處理網際網路封包防火牆，網路架構詳見圖 8。此網路架構可降低防火牆負載，並加強縱深防禦能量。依循此網路架構，內部網路的系統經由 ICS 控制網路前防火牆，存取架設於 ICS 控制網路之系統資料。



資料來源：本計畫整理

圖8　低安全防護網路架構

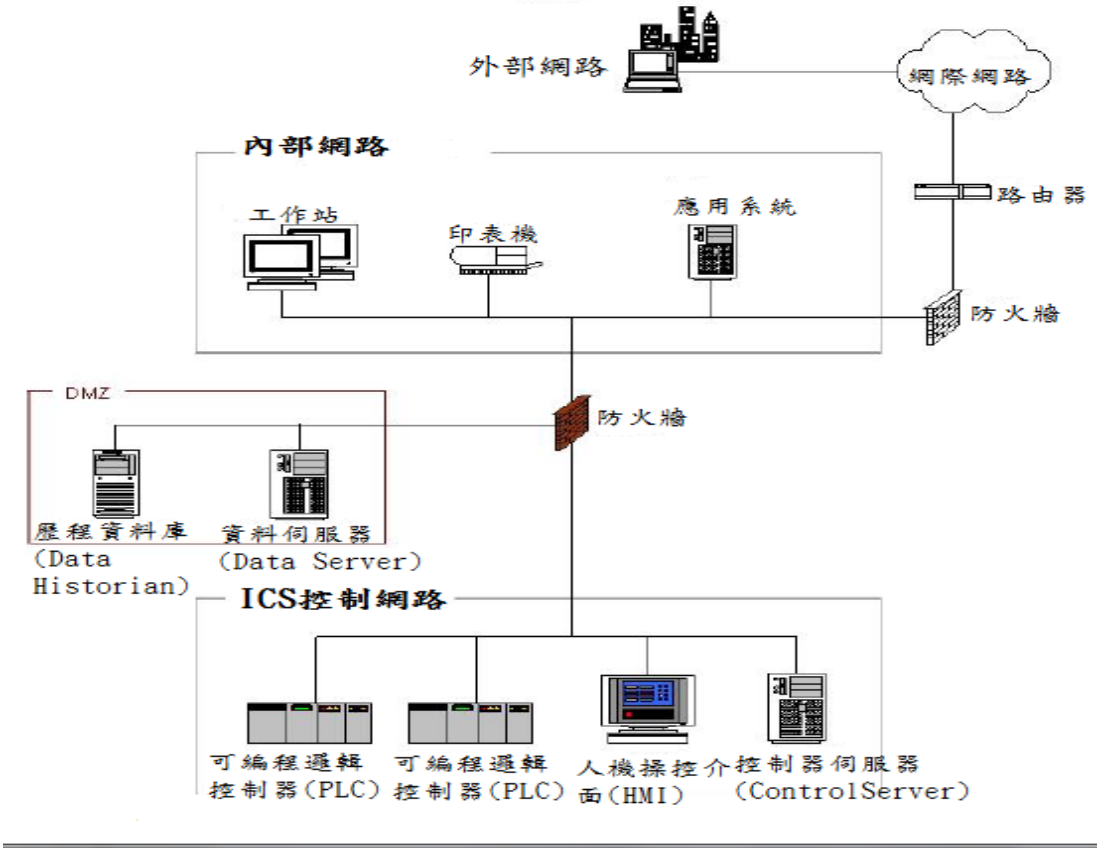
●中安全防護

– 架設非軍事區(Demilitarized Zone, DMZ)

在內部網路與 ICS 控制網路間架設 DMZ，此區放置 2 個網路須共同存取資料之系統，如歷程資料庫或資料伺服器等，讓內部網路系統或使用者不會直接存取到工業控制網路內的設備或機器，降低工業控制系統被攻擊風險。

– 防火牆要求

防火牆須具有 2 種或以上(如 HTTP 與 Modbus 等)之網路封包過濾功能，且防火牆須具備對 ICS 控制網路設備、DMZ 間及內部網路進行網路連線過濾功能，網路架構範例詳見圖 9。



資料來源：本計畫整理

圖9　中安全防護網路架構

●高安全防護

– 架設 DMZ

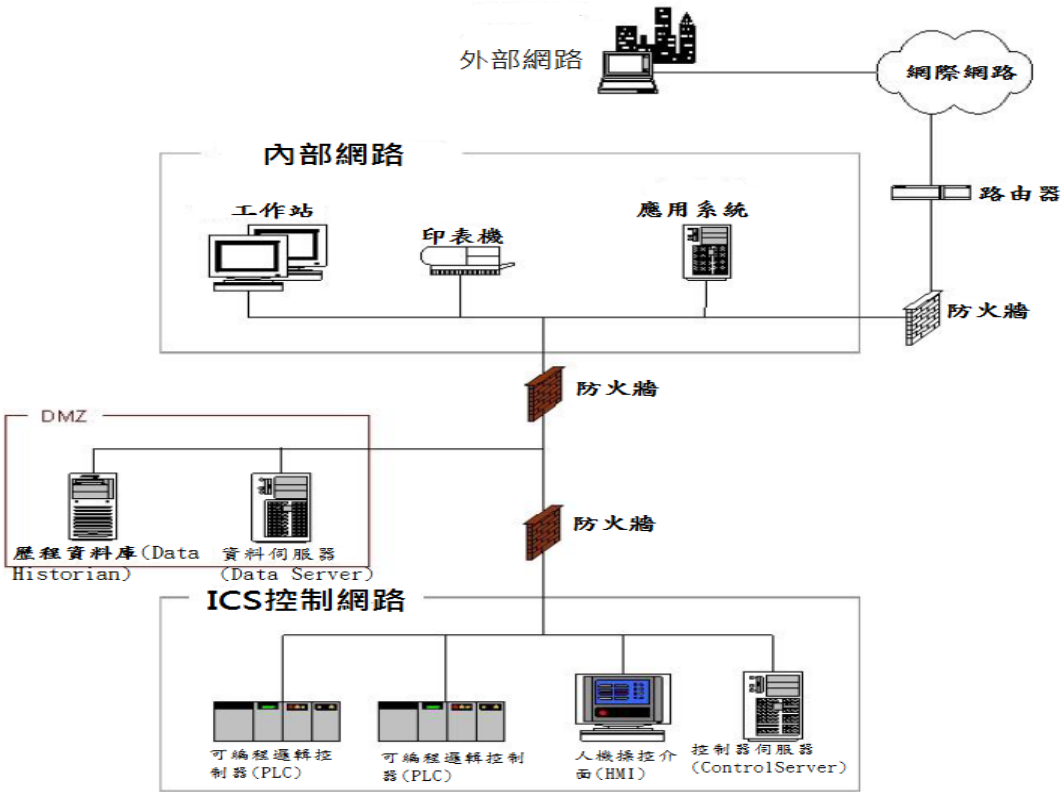
DMZ 要求同中安全防護。

– 防火牆要求

考量當組織遭受到大量攻擊或資料交換頻繁時，單一防火牆可能面臨功能喪失或效能降低等情況，為強化安全防護能量，在 DMZ 對外網路架設一對防火牆，分別對內部網路與 ICS 控制網路進行網路封包過濾，詳見圖 10。對於防火牆防護功能規劃須依組織特性與需求進行調整，提供防護規劃說明如下：

如第 1 個防火牆針對內部網路與 DMZ 進行封包過濾與阻擋，第 2 個防火牆則對 DMZ 與 ICS 控制網路的網路流量進行過濾。

高安全防護網路架構，可有多道防火牆進行封包過濾，強化 ICS 控制網路防禦能力，但也增加防護成本，以及網路安全管理複雜度。本防護建議以高安全防護網路架構，做為組織防護規劃首要考量。



資料來源：本計畫整理

圖10 高安全防護網路架構

4.1.2 邊界防護(Boundary Protection)

- 監視與控制系統外部邊界，以及系統內關鍵內部邊界之通訊。
- 透過邊界防護設備，區隔出連接到外部的網路或非 ICS 之系統。
  - 邊界防護設備包含閘道器、路由器、防火牆、防護裝置、惡意程式碼分析裝置、虛擬化系統或在安全架構防護內實作之加密通道。

●ICS 除以防火牆進行低中高等級防護外，組織亦需考量系統之重要性，以實體隔離或資料單向傳輸等方式實施最高等級之邊界防護。

●建議定期審查防火牆規則。

4.2 存取控制(Access Control)

在 ICS 領域常見密碼複雜度低、人員透過遠端連線至系統端進行維運或控制管理及系統授權過大等資訊安全脆弱點。因此，將對使用者帳號管理、限制遠端存取及無線網路設施之存取進行限制，並防止未經授權之存取。

4.2.1 帳號管理(Account Management)

●建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。

●系統已逾期之臨時或緊急帳號需刪除或禁用。

●禁用系統閒置帳號。

●定期審核系統帳號之建立、修改、啟用、禁用及刪除動作。

●當超過組織所規定之預期閒置時間或可使用期限時，系統需自動將使用者登出。

– 對於設定閒置時間或可使用期限對於某些流程控制應用並非適切，如 HMI 與操作人員用於持續流程監視設備，建議考量並實作因應對策(如門禁系統等)與責任歸屬。

●依照組織所規定之情況及條件(如上班時間或指定 IP 來源等)使用系統。

●監控系統帳號於發現異常使用，並於發現帳號異常使用時回報管理者。

4.2.2 遠端存取(Remote Access)

透過外部網路(如網際網路等)對 ICS 進行管控與存取資料，視為遠端存取。

●對於每一種允許之遠端存取類型，都需先取得授權，建立使用限制、組態需求、連線需求及文件化。

●監控系統遠端連線。

●採用加密機制來防護遠端存取連線的機密性。

●系統遠端存取之來源應為組織已預先定義與管理之存取控制點。

●依維運需求，授權透過遠端執行特定之功能與存取相關資訊。

●採用伺服端的集中過濾機制檢查系統使用者授權。

4.2.3 最小權限(Least Privilege)

採用最小權限原則，只允許使用者(或代表使用者行為的程序)依據任務與業務功能，完成指派任務所需之授權存取。

4.2.4 無線網路管理(Wireless Management)

●建立無線存取使用限制、組態/連線需求及實作指引。

●使用無線存取系統需先取得授權。

4.3 稽核與可歸責性(Audit and Accountability)

當工業控制系統發生資安事件時，常因缺少完整的系統資料，無法進行資安事件處理，可能導致相似的資安事件重複發生。基於此脆弱點，將對稽核資料蒐集提出相關建議。

在多數工業控制系統未支援具有稽核資訊與使用稽核工具之功能，但對於能進行稽核與可歸責性之系統，需包含稽核事件、稽核紀錄內容、稽核儲存容量、稽核處理失效之回應、時戳及稽核資訊之防護等，以符合稽核的需求。

4.3.1 稽核事件(Audit Events)

- 依律定之時間週期與紀錄留存政策，保留稽核紀錄，並滿足法規要求。
- 確保系統有稽核特定事件(如更改密碼、登錄失敗、系統存取失敗、操作參數變改、操作模式切換、製造流程警報發生、機械設備被開停、系統軟硬體異常或通訊流量異常等)之能力，並決定有哪些特定事件在系統中應該被稽核。
- 定期審查稽核事件。

4.3.2 稽核紀錄內容(Content of Audit Records)

- 稽核類別需包含存取控制、要求錯誤、作業系統事件、控制系統事件、備份與儲存事件、組態變更及稽核日誌事件等。
- 稽核紀錄至少需包含事件類型、何時發生、何處發生及任何與事件相關之使用者之身分識別等資訊，並採用日誌記錄機制。

4.3.3 稽核儲存容量(Audit Storage Capacity)

- 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量(ICS 稽核儲存容量需求可能大於資通系統)。
- 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。配置足夠的稽核儲存容量可減少因容量不足，所造成的潛在損失或降低無法稽核之發生率。

4.3.4 稽核處理失效之回應(Response to Audit Processing Failures)

- 系統應在稽核處理失效(如儲存容量不足等)情況下，採取適當行動，如關閉系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。
- 當組織規定需要即時通報的稽核失效事件發生時，系統應在組織規定之時效內，對組織特定之人員、角色提出告警。

4.3.5 時戳(Time Stamps)

- 使用系統內部時鐘產生稽核紀錄所需時戳，並可對映到世界協調時間(UTC)或格林威治標準時間(GMT)。
- 系統內部時鐘應具備定期同步機制。

4.3.6 稽核資訊之防護(Protection of Audit Information)

- 應對稽核資訊與稽核工具進行防護，以防止未授權的存取、修改及刪除。
- 對稽核紀錄之存取管理，僅限於有權限之使用者。
- 定期備份稽核紀錄到與原稽核系統不同之實體系統(如 Log 伺服器等)。
- 應防護稽核資訊之完整性。

4.4 營運持續計畫(Contingency Planning)

工業控制系統常有固定位置的實體元件，當這些元件突然發生無法運轉的情況，若組織內無元件備料，無法立即進行元件替換，將影響工業控制系統所能提供的基本服務。此時組織應啟動緊急應變計畫，維持組織營運持續運作，工業控制系統應將其特殊性列入營運持續計畫，確保基本服務持續運作。

4.4.1 營運持續計畫(Contingency Plan)

- 確認必要任務、維運功能及相關營運持續需求。
- 計畫內容需包含電力、燃料、淨水及汙水等相關支援系統，並以恢復必要功能或業務為首要目標。
- 提供復原目標、復原優先事項及度量標準。
- 定期審查 ICS 營運持續計畫。

4.4.2 安全模式(Safe Mode)

- 當危及安全的條件被偵測時，系統需限制只能進入安全模式操作。
- 安全模式操作可以自動或手動啟動，如在有限的電力或減少通訊頻寬下，只允許某些功能進行。

4.4.3 控制系統備援(Control system backup)

- 重要的控制系統應具有備援系統。
- 備援系統應與時俱進。
- 評估備援系統時，應將事件鑑識(如稽核日誌)與加密功能，列入系統備援考量。

4.5 識別與鑑別(Identification and Authentication)

工業控制系統常有使用者未授權存取、多人共用一組系統帳號等資安脆弱點，因此提出此防護建議。

在建立識別與鑑別相關防護措施時,須考量工業系統在執行此防護措施時，是否會影響系統效能，並依其環境進行防護措施調整。識別與鑑別措施範圍包含使用者、裝置及鑑別資訊回饋。

4.5.1 內部使用者之識別與鑑別(Organizational Users Identification and Authentication)

- 系統應具備唯一識別與鑑別組織使用者(或代表組織使用者行為之程序)，不應有共用帳號之行為。
  - 若不可能使用個人之使用者帳號時，為確保存取安全性與可追蹤性之充分等級，宜連同補充措施(如使用廠區排班資訊、影像紀錄等)，定義有關例外情況之精確規則。

- 系統應採用實體安全措施進行識別。

4.5.2 裝置之識別與鑑別(Device Identification and Authentication)

- 應識別與鑑別連接至工業控制系統裝置，以及其限制連線數量與類型。
  - 若因技術限制、個別資通系統之設計、結構或性質等因素，建議考量實作因應對策。
- 應識別組織所屬裝置與非個人裝置(如委外廠商所屬裝置與行動裝置等)。

4.5.3 身分鑑別管理(Authenticator Management)

- 使用預設密碼登入系統時，應於登入後要求立即變更。
- 基於密碼之鑑別系統應強制最低密碼複雜度；強制新的密碼最少變更之字元數；強制密碼最短及最長之效期限制。
- 使用者更換密碼時，組織內應訂定異於使用過密碼相同之次數(如不可以與前 3 次使用過密碼相同等)。
- 具備帳戶鎖定機制，組織應訂定帳號登入進行身分鑑別失敗次數(如登入失敗 5 次等)，以及不允許該帳號繼續嘗試登入之時間(如至少 15 分鐘等)。
  - 帳戶鎖定機制對於某些流程控制應用並非適切，如 HMI 與操作人員用於持續流程監視設備，建議考量實作因應對策與責任歸屬。
- 身分鑑別相關資訊不以明文傳輸。
- 身分驗證機制需防範自動化程式之登入或密碼更換嘗試。

4.5.4 鑑別資訊回饋(Authenticator Feedback)

系統應遮蔽在鑑別過程中之資訊(如密碼等)，以防止未授權之使用者可能之窺探或使用。

4.6 系統與通訊防護(System and Communications Protection)

ICS 網路傳輸常出現資訊安全脆弱點包含使用明文傳輸,缺乏傳輸資料完整性確認，以及重要組態資料無儲存與備援。

透過資料傳輸之機密性與完整性，以及資料儲存安全之防護要求，以達到系統通訊資訊之防護，須考慮系統效能與可用性，並依其環境進行防護措施調整。

4.6.1 傳輸之機密性與完整性(Transmission Confidentiality and Integrity)

ICS 需盡其可能使用加密機制(如數位簽章或加密雜湊函數等)，以防止資訊揭露。

4.6.2 資料儲存之安全(Protection of Information at Rest)

- 靜置資訊指資訊位於系統特定元件，如儲存設備上之狀態。與系統相關需要防護的資訊，如系統組態設定等資訊應予以防護。
- 機密資訊應加密儲存。

4.7 系統與服務獲得(System and Services Acquisition)

ICS 可能因為外部服務供應商提供服務時,監管不完善,形成資通安全威脅，防護建議範圍包含外部系統服務與系統文件。

4.7.1 外部系統服務(External System Services)

外部系統屬於組織系統授權範圍外實作的服務，但不是組織系統的一部分(如供應商維修系統等)，應要求外部服務供應商遵守與符合組織的安全要求。

4.7.2 系統文件(System Documentation)

- 組織應建立 ICS 系統、系統元件及系統服務相關安全措施的實作與運作，

相關之管理文件。

●組織應定期確認管理文件內容的品質與完整性。

4.8 實體與環境防護(Physical and Environmental Protection)

ICS 在實體環境常見的安全威脅包含缺少備援電力、溫溼度控制及人員實體存取等，因此應針對實體存取授權、實體存取控制、實體存取監控、緊急電源、溫溼度控制、水損防護及第三方/陪同者的存取等提出防護建議。

4.8.1 實體存取授權(Physical Access Authorizations)

●應建立系統所在的設施實體存取授權之使用者清單，並定期審查存取清單。

●當使用者不再需要存取時，應由設施存取清單移除該使用者。

4.8.2 實體存取控制(Physical Access Control)

●ICS 應考量實體安全之相依性，並考量電子與機械設備室的進出管制。

●緊急事件發生時，工業控制設備應進行限制授權管制。

4.8.3 實體存取監控(Monitoring Physical Access)

●組織應監控系統設施的實體存取，並監控、偵測及警示實體安全事件。

●監控範圍應包含備援系統與遠距離終端設備等。

4.8.4 緊急電源(Emergency Power)

●應建立能供應最小業務負載量之長時間電力備援。

●建議可採用替代電力供應，做為緊急備源電源。

4.8.5 溫溼度控制(Temperature and Humidity Control)

系統環境的溫溼度控制系統(如冷暖氣系統、照明系統等)，也屬於工業控制

系統重要一環，須定期維護溫溼度控制系統。

4.8.6 水損防護(Water Damage Protection)

在關鍵基礎設領域類別所使用的工業控制系統運作時，水的供應狀況會影響系統運作。應確保工業控制系統周邊設備，如火災防護、緊急照明及備援系統等，建議具有水偵測防護管理，避免漏水造成系統損害。

4.8.7 第三方/陪同者的存取(Third Party/Escorted Access)

- 篩選、執行及文件化第三方人員的安全控制，並監控服務提供者的行為與承諾。
- 在相關合約與協議文件中明確包含人員安全控制。

4.9 系統與資訊完整性(System and Information Integrity)

ICS 系統特性缺乏惡意程式防護、漏洞修補與更新及系統監控等資通安全要求，因此當系統使用網際網路串接時，將造成資安威脅。因此提出漏洞修補、惡意程式防護、系統監控，以及可預測之故障預防之防護建議，以提升系統與資訊之完整性。

4.9.1 漏洞修補(Flaw Remediation)

- 多數工業控制系統與相關軟體，常需藉由供應商進行軟體更新，需定期追蹤與驗證漏洞修復。若因技術限制、個別資通系統之設計、結構或性質等因素，致系統漏洞無法修復時，應實作降低弱點暴露因應對策。
- 工業控制系統進行漏洞修補後，應進行測試。

4.9.2 惡意程式防護(Malicious Code Protection)

- 系統應具有偵測惡意程式防護機制。

  – 若因技術限制、個別資通系統之設計、結構或性質等因素(如缺乏廠商

支援或不可能安裝即時更新等)無法部署惡意程式防護工具，宜採取其他型式對策(如加強 USB 惡意程式掃描、ICS 防火牆防護功能等)。

- 防護工具應具有針對工業控制系統防護，如流量監控與稽核等。

4.9.3 系統監控(System Monitoring)

- 使用監控工具等相關技術，須確認不會影響工業控制系統操作。
- 當既有之工業控制系統不能監控出入流量時，應單獨對相關資通系統進行監控。

4.9.4 可預測之故障預防(Predictable Failure Prevention)

- 參考工業控制系統之平均故障時間(Mean Time To Failures, MTTF)，做為系統可靠度與潛在故障考量基準。
- 依據平均故障時間、維修與運作紀錄及產品生命週期等資訊，定義系統使用期限，以降低元件故障可能造成潛在危害。

4.9.5 故障容許度(Fault Tolerance)

定義系統裝置故障容許度標準，並進行相關防護措施。

4.10 組態管理(Configuration Management)

常見安全弱點包含組態變更控制與使用者擁有過大的系統管理權限，依此安全顧慮，對組態變更控制與基本功能提出防護措施。

4.10.1 組態變更控制(Configuration Change Control)

- 系統相關組態變更應予以文件化，並保留系統組態控制變更紀錄。
- 依規定的時間週期，保留系統組態控制變更紀錄。
- 稽核與審查系統組態控制變更紀錄。

4.10.2 最基本功能(Least Functionality)

- 設定系統僅提供業務必要的功能。
- 系統僅提供必要的功能，關閉不須使用之功能、埠、協定及服務。
- 系統應將獲得授權執行的軟體程式列入白名單。
- 應定期審查必要的功能內容與白名單。

4.11 組織管理(Organization Management)

在 ICS 領域常見組織管理弱點包含缺乏安全意識相關訓練、管理程序完整度不足及安全程序不足。

本控制類別將針對組織管理層面的委外管理、人員管理、風險政策及事件應變內容，提出相關建議。

4.11.1 委外管理(Outsourcing Management)

委外管理對於供應商與承包商的資通安全要求，相關詳細管理可參考「政府資訊作業委外安全參考指引」。

4.11.2 人員管理(Personal Management)

- 應建立人員資安政策之目的、範圍、角色、責任、管理承諾及組織間之協調。
- 對系統使用者(包含管理人員、高階管理者等)提供基本的資安認知教育訓練，進行教育訓練時間應包含當系統有新使用者、系統功能變更及定期實施等。
- 人員離職時，應於規定時間禁止存取資通系統。

4.11.3 風險政策(Risk Policy)

- 應對資訊與系統分級，且建立相關安全分級政策。
- 應訂定期審查風險評鑑結果。

4.11.4 事件應變(Incident Response)

- 應建立事件應變政策與計畫。
- 應定期進行事件應變演練與訓練。
- 應定期檢視事件處理程序。

5. 結論

國際間近年頻傳工業控制系統遭受到惡意攻擊事件，所導致的財物損失、系統損害甚至人員傷亡，此衝擊影響程度與範圍均超乎預期。因此，世界各國開始重視會嚴重影響人民生活、國家經濟及健康等關鍵基礎設施所屬之工業控制系統之資通安全。

工業控制系統高度強調可用性，而一般資通系統較重視機密性，2 者在功能設計理念具有相當大的差異，因此工業控制系統無法完全套用已建立的資通系統資安防護相關標準或建議。且工業控制系統廣泛使用於能源、交通、醫療及製造等領域，各領域的工業控制系統會因領域不同而有其特殊性，其資安防護須依領域進行調整。

本防護建議為蒐集世界主要國家與國際工業控制系統資安標準，以及相關防護建議與防護標準等文件，並依我國國情涵蓋關鍵基礎設施之工業控制系統，提出通用性防護建議。

基於保障國家安全與永續生存發展，各關鍵基礎設施領域層級可參考本防護建議，檢視 CI 領域特性，調整成各領域所須遵行之資安防護目標、防護基準及作法等。

6. 參考文獻

[1]Security and Privacy Controls for Federal Information Systems and Organizations , NIST SP800-53rev4, 2013.

[2]行政院國家資通安全會報(104 年)。「資訊系統分級與資安防護基準作業規定」。

[3]Guide to Industrial Control Systems(ICS) Security, NIST SP800-82 Revision2, 2015.

[4]The 62443 series of standards-Industrial Automation and Control Systems Security, ISA, 2016

[5]Industrial communication networks-Network and system security-Part 3-3: System security requirements and security levels, IEC 62443-3-3.

[6]Critical Infrastructure Protection Reliability Standards Version 5, NERC ,2017.

[7]Cyber Security Programs For Nuclear Facilities, Regulatory Guide 5.71,2010.

[8]NERC CIP Standard Mapping to the Critical Security Controls-Draft, 2013.

[9]工業控制系統信息安全防護指南，中國大陸，2016 年。

[10]工業自動化和控制系統信息安全 集散控制系統(DCS)第 1 部分：防護要求，GB/T 33009.1，中國大陸，2016 年。

[11]ICS-CERT Annual Assessment Report FY 2016, 2017, United State ICS-CERT.

7. 附件

附件 1　專有名詞英中對照表

附件 2　工業控制系統檢核表

附件1 專有名詞英中對照表

本防護建議之專有名詞中英對照，以 CNS 27001、CNS 27002 及 CNS 27005 優先考量，若有不足，則乃依據標準檢驗局所制定之名詞為範本，若無對應到 CNS 27001 與 CNS 27002、標準檢驗局等資料者，則由撰述小組進行中英對照之彙編謹供參考。

附表 1-1　專有名詞英中對照表

英文	中文
A	
Access Agreements	存取協議
Access Control Decisions	存取控制決策
Access Control List	存取控制清單
Access Control for Mobile Devices	行動裝置存取控制
Access Control for Output Devices	輸出設備存取控制
Access Control for Transmission Medium	傳輸線路存取控制
Access Control Policy And Procedures	存取控制政策和程序
Access Enforcement	強制存取控制
Access Restrictions for Change	變更存取限制
Account Management	帳號管理
Acquisition Process	獲得程序
Adaptive Identification and Authentication	調適識別與鑑別
Allocation of Resources	資源分配
Alternate Audit Capability	備用稽核能力
Alternate Communications Protocols	備用通訊協定

英文	中文
Alternate Processing Site	備用處理網站
Alternate Storage Site	備用儲存網站
Alternate Work Site	備用工作場所
Alternative Security Mechanisms	備用安全機制
Application Partitioning	應用程式分隔
Asset Monitoring and Tracking	資產監控和追踪
Audit and Accountability Policy and Procedures	稽核和可歸責性的政策和程序
Audit Events	稽核事件
Audit Generation	稽核的產生
Audit Record Retention	稽核紀錄之保存
Audit Reduction and Report Generation	稽核紀錄精簡與報告產製
Audit Review, Analysis, and Reporting	稽核審查、分析與報告
Audit Storage Capacity	稽核儲存容量
Authenticator Feedback	鑑別資訊回饋
Authenticator Management	鑑別資訊管理
B	
Baseline Configuration	基準組態
Boundary Protection	邊界防護
Business Continuity Plan	業務持續計畫
C	
Central Management	集中管理
Collaborative Computing Devices	協同運算元件

英文	中文
Component Authenticity	元件鑑別
Concurrent Session Control	連線數控制
Configuration Change Control	組態變更控制
Configuration Management Plan	組態管理計畫
Configuration Management Policy and Procedures	組態管理政策和程序
Configuration Settings	組態設定
Content of Audit Records	稽核紀錄內容
Continuous Monitoring	持續監控
Continuous Process	連續流程
Control Loop	控制迴路
Controlled Maintenance	維護管制
Control Network	控制網路
Controller	控制器
Control Server	控制伺服器
Communications Routers	通訊路由器
Critical Infrastructure	關鍵基礎設施
Critical Infrastructure Protection	關鍵基礎設施防護
Critical Information Infrastructure	關鍵資訊基礎設施
Criticality Analysis	關鍵程度分析
Cross-Organizational Auditing	跨組織稽核
Cryptographic Key Establishment and Management	加密金鑰建立與管理

英文	中文
Cryptographic Module Authentication	加密模組鑑別
Cryptographic Protection	密碼防護
Cycle Time	週期時間
D	
Data Mining Protection	資料探勘防護
Data Historian	歷程資料
Delivery and Removal	交付和移除
Denial of Service Protection	阻絕服務攻擊之防護
Detonation Chambers	惡意程式引爆作業區
Developer Configuration Management	開發者組態管理
Developer Security Architecture and Design	開發者安全架構與設計
Developer Security Testing and Evaluation	開發者安全測試與評估
Developer-Provided Training	開發者訓練
Development Process, Standards, and Tools	發展程序、標準與工具
Device Identification and Authentication	裝置之識別與鑑別
Distributed Control Systems	分散式控制系統
Distributed Processing and Storage	分散式處理與儲存
Demilitarized Zone	非軍事區
E	
Emergency Lighting	緊急照明
Emergency Power	緊急電源
Emergency Shutoff	緊急切斷功能
Error Handling	錯誤處理

英文	中文
Escorted Access	陪同者的存取
External System Services	外部系統服務
F	
Fail in Known State	失敗之已知狀態
Fail-Safe Procedures	故障防護程序
Fire Protection	消防
Flaw Remediation	漏洞修復
Fault Tolerance	故障容許度
H	
Heterogeneity	異質性
Honeyclients	誘捕系統終端
Honeypots	誘捕系統
Human-Machine Interface	人機界面
I	
Identification and Authentication (Non-Organizational Users)	識別與鑑別(非內部使用者)
Identification and Authentication (Organizational Users)	內部使用者之識別與鑑別
Identification and Authentication Policy and Procedures	識別與鑑別政策和程序
Identifier Management	識別符管理
Incident Response	事件應變
Industrial Control Systems	工業控制系統
Information and Communication Technology	資通系統

英文	中文
Informational Technology	資訊系統
Information Input Validation	資訊輸入驗證
Information Leakage	資訊洩露
Information Output Filtering	資訊輸出過濾
System Backup	系統備份
System Component Inventory	系統元件清單
System Documentation	系統文件
System Inventory	系統清冊
System Monitoring	系統監控
Information System Partitioning	資訊系統分隔
Industrial Control System	工業控制系統
Intrusion Detection System	入侵偵測系統
Intelligent Electronic Device	智能電子設備
Internal System Connections	內部系統連接
L	
Local Area Network	區域網路
Least Functionality	最基本功能
Least Privilege	最小權限
Location of Information System Components	資訊系統元件的位置
M	
Maintenance Personnel	維護人員
Maintenance Tools	維護工具
Malicious Code Protection	惡意程式碼防護

英文	中文
Media Access	媒體存取
Media Marking	媒體標記
Media Protection Policy and Procedures	媒體防護政策和程序
Media Storage	媒體儲存
Media Transport	媒體傳輸
Media Use	媒體使用
Mean Time To Failures	平均故障時間
Memory Protection	記憶體防護
Mobile Code	行動碼
Modem	數據機
Monitoring for Information Disclosure	資訊揭露之監控
Monitoring Physical Access	實體存取監控
N	
Network Disconnect	網路斷線
Nonlocal Maintenance	非本地端維護
Non-Modifiable Executable Programs	不可變更之執行程式
Non-repudiation	不可否認性
O	
Operations Security	作業安全
Out-of-Band Channels	不同之傳輸通道
Outsourcing Management	委外管理
P	
Personal Management	人員管理

英文	中文
Physical Access Authorizations	實體存取授權
Physical Access Control	實體存取控制
Physical and Environmental Protection Policy and Procedures	實體和環境防護之政策和程序
Platform-Independent Applications	跨平台應用程式
Port and I/O Device Access	連接埠與輸出入裝置存取
Power Equipment and Cabling	電力設備和佈纜
Predictable Failure Prevention	可預測故障之預防
Previous Logon (Access) Notification	前次登錄(存取)通知
Process Isolation	流程隔離
Programmable Logic Controller	可程式邏輯控制器
Protection of Audit Information	稽核資訊之防護
Protection of Information at Rest	資料儲存之安全
Publicly Accessible Content	可公開存取的內容
R	
Re-authentication	重新鑑別
Reference Monitor	參考監視
Remote Access	遠端存取
Remote Terminal Unit	遠程終端單元
Resource Availability	資源可用性
Response to Audit Processing Failures	稽核處理失效之回應
Risk Policy	風險政策
S	

英文	中文
Safe Mode	安全模式
Security Alerts, Advisories, and Directives	安全警示、諮詢與指導
Security Assessment and Authorization Policies and Procedures	安全評鑑與授權政策與程序
Security Assessments	安全評鑑
Security Attributes	安全屬性
Security Authorization	安全授權
Security Authorization Process	安全授權之流程
Security Concept of Operations	安全運作概念
Security Function Isolation	安全功能隔離
Security Function Verification	安全功能驗證
Security Impact Analysis	安全衝擊分析
Security Planning Policy and Procedures	安全計畫之政策和程序
Sensor Capability and Data	檢測器之能力與資料
Separation of Duties	權責分離
Service Identification and Authentication	服務識別與鑑別
Session Authenticity	連線之鑑別
Session Lock	連線鎖定
Session Termination	連線終止
Software Usage Restrictions	軟體使用限制
Software, Firmware, and Information Integrity	軟體、韌體及資訊完整性
Spam Protection	垃圾郵件防護
Supply Chain Protection	供應鏈防護

英文	中文
Supervisory Control And Data Acquisition	監控與數據擷取系統
System and Communications Protection Policy and Procedures	系統與通訊防護政策與程序
System and Information Integrity Policy and Procedures	系統與資訊完整性政策與程序
System and Services Acquisition Policy and Procedures	系統與服務獲得政策與程序
System Development Life Cycle	系統發展生命週期
System Interconnections	系統互連
System Maintenance Policy and Procedures	系統維護政策和程序
System Security Plan	系統安全計畫
System Use Notification	系統使用通知
T	
Tamper Resistance and Detection	文件竄改防範與偵測
Technical Surveillance Countermeasures Survey	技術監控對策調查
Telecommunications Services	電信服務
Temperature and Humidity Controls	溫濕度控制
Testing, Training, and Monitoring	測試、訓練與監控
Thin Nodes	精簡節點
Third-Party Personnel Security	第三方人員安全
Third Party Access	第三方存取
Time Stamps	時戳
Timely Maintenance	及時維護

英文	中文
Transmission Confidentiality and Integrity	傳輸之機密性與完整性
Transmission of Security Attributes	安全參數傳輸
Trusted Path	信任路徑
Trustworthiness	可信賴度
U	
Unsuccessful Logon Attempts	嘗試登錄失敗
Unsupported System Components	不支援之系統元件
Usage Restrictions	限制方法
Use of External Systems	使用外部系統
User-Installed Software	使用者安裝軟體
V	
Visitor Access Records	訪客存取紀錄
Virus	病毒
Vulnerability Scanning	弱點掃描
W	
Water Damage Protection	水損防護
WAN Card	廣域網路卡
Whitelist	白名單
Wireless Access	無線存取
Wide Area Network	廣域網路
Worm	蠕蟲

資料來源：本計畫整理

附件2 工業控制系統檢核表

工業控制系統網路架構(ICS Network Architecture)			
項次	項目	是否納入防護基準	說明
1	網段規劃(Network Segregation)	□是 □否	
2	邊界防護(Boundary Protection)	□是 □否	

存取控制(Access Control)			
項次	項目	是否納入防護基準	說明
1	帳號管理(Account Management)	□是 □否	
2	遠端存取(Remote Access)	□是 □否	
3	最小權限(Least Privilege)	□是 □否	
4	無線網路管理(Wireless Management)	□是 □否	

稽核與可歸責性(Audit and Accountability)			
項次	項目	執行確認	說明
1	稽核事件(Audit Events)	□是 □否	
2	稽核紀錄內容(Content of Audit Records)	□是 □否	
3	稽核儲存容量(Audit Storage Capacity)	□是 □否	
4	稽核處理失效之回應(Response to Audit Processing Failures)	□是 □否	
5	時戳(Time Stamps)	□是 □否	
6	稽核資訊之防護(Protection of Audit Information)	□是 □否	

營運持續計畫(Contingency Planning)			
項次	項目	是否納入防護基準	說明
1	營運持續計畫(Contingency Plan)	□是 □否	
2	安全模式(Safe Mode)	□是 □否	
3	控制系統備援(Control system backup)	□是 □否	
識別與鑑別(Identification and Authentication)			
項次	項目	是否納入防護基準	說明
1	內部使用者之識別與鑑別(Identification and Authentication(Organizational Users))	□是 □否	
2	裝置之識別與鑑別(Device Identification and Authentication)	□是 □否	
3	身分鑑別管理(Authenticator Management)	□是 □否	
4	鑑別資訊回饋(Authenticator Feedback)	□是 □否	
系統與通訊防護(System and Communications Protection)			
項次	項目	執行確認	說明
1	傳輸之機密性與完整性(Transmission Confidentiality and Integrity)	□是 □否	
2	資料儲存之安全(Protection of Information at Rest)	□是 □否	
系統與服務獲得(System and Services Acquisition)			

項次	項目	是否納入防護基準	說明
1	外部系統服務(External System Services)	□是 □否	
2	系統文件(System Documentation)	□是 □否	
實體與環境防護(Physical and Environmental Protection)			
項次	項目	執行確認	說明
1	實體存取授權(Physical Access Authorizations)	□是 □否	
2	實體存取控制(Physical Access Control)	□是 □否	
3	實體存取監控(Monitoring Physical Access)	□是 □否	
4	緊急電源(Emergency Power)	□是 □否	
5	溫溼度控制(Temperature and Humidity Control)	□是 □否	
6	水損防護(Water Damage Protection)	□是 □否	
7	第三方/陪同者的存取(Third Party/Escorted Access)	□是 □否	
系統與資訊完整性(System and Information Integrity)			
項次	項目	是否納入防護基準	說明
1	漏洞修補(Flaw Remediation)	□是 □否	
2	惡意程式碼防護(Malicious Code Protection)	□是 □否	
3	系統監控(System Monitoring)	□是 □否	

4	可預測之故障預防(Predictable Failure Prevention)	□是 □否	
5	故障容許度(Fault Tolerance)	□是 □否	
組態管理(Configuration Management)			
項次	項目	是否納入防護基準	說明
1	組態變更控制(Configuration Change Control)	□是 □否	
2	最基本功能(Least Functionality)	□是 □否	
組織管理(Organization Management)			
項次	項目	是否納入防護基準	說明
1	委外管理(Outsouring Management)	□是 □否	
2	人員管理(Personal Management)	□是 □否	
3	風險政策(Risk Policy)	□是 □否	
4	事件應變(Incident Response)	□是 □否	

資料來源：本計畫整理