115 年度
關鍵資訊基礎設施資安防護建議

中華民國 115 年 4 月

目錄

頁次

表目錄

頁次

圖目錄

頁次

第一章、 前言及目的

第一節、背景與目的

近年國際資通安全（後續全文以資安代稱）威脅日益複雜，針對國家關鍵資訊基礎設施（Critical Information Infrastructure, CII）的攻擊事件頻繁增加。其中工業控制系統（Industrial Control System, ICS）及營運技術（Operational Technology, OT）環境所面臨的網路威脅尤其顯著提升。研究指出，高達八成以上的 OT 廠商在近年內遭受資安事件，且逾七成的攻擊源自入侵資訊技術（Informational Technology, IT）系統後橫向擴散至 OT 網域，反映出 IT 與 OT 融合所衍生的跨域風險已成為重要挑戰。

有鑑於此，行政院於 2018 年發布《關鍵資訊基礎設施資安防護建議》，提供各中央目的事業主管機關擬定資安防護基準之參考依據。隨著國內關鍵基礎設施（Critical Infrastructure, CI）防護政策與制度持續演進，自 2025 年起，我國 CI 依功能屬性調整為九大領域，並更加聚焦各中央目的事業主管機關對轄內 CI 提供者的分級管理與防護落實。

本次《關鍵資訊基礎設施資安防護建議》修訂，綜整最新國際趨勢、國內制度更新與攻防態勢變化，調整政策導引內容、更新防護架構分類，並補強分層分級管理與領域應用實務，供各中央目的事業主管機關據以推動與修訂防護基準與指引。

第二節、政策依據與制度連結

本防護建議係依據《國家關鍵基礎設施安全防護指導綱領》、《資通安全管理法》及其相關授權規定辦理，為落實我國 CI 安全防護政策之重要一環。行政院已建構橫向協調與縱向治理機制，由行政院國家資通安全會報統籌國家資通安全政策，並由行政院國土安全辦公室協調各 CI 保護政策及跨部會協調任務，明確賦予各中央目的事業主管機關責任權限。

依據上述政策架構，各中央目的事業主管機關須就轄下 CI 提供者進行資安責任等級劃分，並訂定最低資通安全維護基準及其實施方式。各 CI 提

供者則應依其主管機關所訂基準，訂定並執行自有資通安全維護計畫，使整體管理與執行流程得以有效運作並持續改善。

本《關鍵資訊基礎設施資安防護建議》作為制度架構指引文件，主要提供各中央目的事業主管機關於研訂及修訂所屬領域之工控資安防護基準與落實指導作業時所依循之通則依據，並與現行資通安全責任等級分級辦法之資通系統分級與防護基準等作業程序互為補充，形成一致且可連貫之制度體系。

第三節、適用對象與範疇

本防護建議適用於經各中央目的事業主管機關指定之 CI 提供者、維運單位及其相關資通系統與 OT 環境。2025 年起，CI 領域已調整為九大類，分別為：能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區、糧食。上述各領域之中央目的事業主管機關，可將本防護建議作為制定及更新防護基準之參考依據。

在技術層面，本防護建議涵蓋 ICS、OT、資訊及通訊技術（Information and Communication Technology, ICT）等與 CI 核心業務運作相關之資訊與控制系統類型。鑒於 ICT 及 IT 系統已具備資安分級與防護基準之實務規範，各中央目的事業主管機關可持續採行現有制度推動之；惟 OT 及 ICT 中具 OT 功能的系統具有不同於傳統 IT 環境之風險樣態與管理需求，故本防護建議針對 OT 及 ICT 中具 OT 功能的系統領域提出具通用性之防護建議，供各中央目的事業主管機關依領域特性加以調整與落實於基準規範中，強化全體 CI 防護能量。

第二章、 工控環境與資安挑戰

第一節、工控環境特性

ICS 與 OT 環境在整體 CI 中，屬於高度專業且緊密貼合實際作業流程的系統。這類系統的首要目標在於維持生產與服務的穩定運作，包含電力輸配、水資源處理、天然氣輸送、交通號誌控制、環控與關鍵設備監控等。相較於一般資訊系統重視資料機密性與彈性擴充，工控環境更重視即時性、可預測性與整體系統可用性，任何延遲、短暫中斷或不在預期內的變更，都可能直接反映在實體設備狀態與公共服務品質上。

多數工控設備設計時，以長期穩定運轉為前提，硬體與韌體壽命通常跨越十年以上，系統建置完成後，往往僅進行必要的功能性維護，而不會頻繁汰換。這種長生命週期的特性，使得環境中同時存在多個世代、不同廠牌與不同通訊協定的設備，各自具有不同的設定介面與維護方式，導致整體環境高度異質。異質性不僅增加維運人員管理資產與排除故障的複雜度，也讓安全控管較難以標準化與自動化。

工控系統為了確保流程不中斷，通常以「能運作就盡量不要動」的方式管理。許多設備在設計之初並未預留定期更新機制，即使後續出現安全弱點，若更新需要停機、重新啟動或重新驗證控制邏輯，營運單位往往會對更新作業有所保留。再加上工控場域常有嚴格的停機機制，例如只能在年度或季度檢修時短暫停車或停機，導致已知弱點即使管理單位清楚掌握，也不一定能在短時間內完成修補，形成弱點暴露時間長、風險累積的情況。

此外，工控環境也對安全管理造成限制，許多設備位於廠房、變電站、抽水站、隧道機房或偏遠站點，現場作業條件與一般機房截然不同，現地維護多仰賴少數熟悉設備特性的工程人員。這些條件使得在工控環境中導入額外的安全設備、監控設備或軟體代理程式時，必須先評估對效能、穩定性與維護成本之影響，安全機制無法如同在 IT 系統中那樣快速或全面部署，這些結構性瓶頸都使工控資安防護充滿挑戰。

第二節、IT 與 OT 融合所帶來的挑戰

隨著數位轉型與智慧化應用的發展，工控環境不再是一個完全孤立的封閉網路。營運單位期望透過即時資料分析最佳化產能，利用歷程資料進行預測維護，將多個廠區整合到同一監控中心，甚至結合雲端服務進行長期趨勢分析與報表產出。這些訴求都使得工控系統與內部資訊系統之間建立更多資料交換與控制介面，原本清楚區隔的 IT 網路與 OT 網路之間，逐漸形成多條明顯與隱性的連結。

在理想情況下，這些連結會透過嚴謹的網路分區、閘道、資料交換伺服器與應用介面來管理，每一條通路都有清楚定義的方向、協定與授權規則。然而在實務上，為了滿足臨時需求或縮短建置時間，往往會出現直接將工控系統接上既有內部網路、開放共享檔案服務、使用一般遠端桌面工具直接連線控制設備、或管理帳號在多個網段共用等情形。這些做法在短期內可以解決運作需求，卻大幅擴大攻擊面，使工控環境承受來自 IT 網域的資安威脅傳播。

遠端連線是 IT 與 OT 融合後，最關鍵也是最敏感的環節之一。工控設備與系統經常需要外部原廠或系統整合廠商提供遠端支援，處理故障診斷、韌體更新、參數調整與功能擴充等工作。營運單位內部的輪班人員有時也會透過遠端方式登入監控系統或工程工作站，進行日常操作與異常處置。如果這些遠端連線缺乏集中管理，沒有明確限制來源位置與使用時段，也沒有採用強度足夠的身分鑑別與多因子驗證，攻擊者就有機會利用外洩的帳號密碼、被竊取的維運筆電或未受管控的遠端工具，直接進入控制環境的核心位置。

更進一步來看，遠端連線如果是直接連到控制伺服器或工程工作站，而非經過跳板系統與記錄機制，將使營運單位難以事後追蹤操作內容與判斷責任歸屬。一旦攻擊者以合法維運帳號登入並進行惡意操作，即使事後調閱紀錄，也不容易區分何者為正常維運、何者為惡意行為，這類風險在

實務上屢見不鮮。IT 與 OT 的融合若缺乏完善設計與治理，遠端連線就會成為繞過既有安全控制的捷徑，讓工控環境暴露於較高的入侵與誤用風險之下。

第三節、工控資安威脅態勢

近年國際間多起重大事件顯示，針對 CI 與工控環境的攻擊，已從單純癱瘓系統或造成短期中斷，演變為長期潛伏、精準操控與政治或經濟目的兼具的行動。攻擊者會花費相當時間蒐集目標資訊，分析系統架構、設備廠牌、控制邏輯與作業程序，再設計出適合此環境的攻擊路徑與工具，而不再只是隨機散布惡意程式。

在典型攻擊模式中，入侵往往始於組織 IT 網路的邊界，包括釣魚郵件、充當更新的惡意檔案、遠端服務弱點或網頁應用程式漏洞等。攻擊者一旦取得內部系統的使用權，就會利用各種方法橫向移動，尋找與工控環境相連的跳板系統、監控伺服器或資料交換節點。若這些節點與工控網路之間缺乏嚴格的分區與存取限制，攻擊者就可以逐步接近控制核心系統，進而影響工程工作站、控制伺服器或歷程資料庫。

威脅類型也變得更加多樣。勒索軟體不再只加密辦公室檔案與伺服器，而是開始嘗試干擾生產控管系統與設備監控平台，迫使營運單位因無法掌握設備狀態或失去操作能力而自動停機。部分攻擊則聚焦在竄改參數、關閉警報、調整保護機制啟動條件或修改顯示畫面，試圖在不立即引起注意的前提下，使系統長時間運作於不安全或不穩定狀態，這種「慢性」的操控行為比瞬間破壞更難察覺，也更難追溯影響。

供應鏈相關威脅同樣受到高度關注。工控環境依賴多家設備供應商、系統整合商與維運服務商，系統更新檔、韌體、設定檔與維運工具在傳遞與安裝過程中，如果未經完整驗證與保護，可能成為植入惡意程式的載體。攻擊者若能滲透某一上游廠商或配發平台，就有機會在多個場域中同時種下惡意程式或後門。這種模式使單一事件的影響範圍不再限於單一營運者，

而可能跨域、跨國擴散。

在偵測與通報面向，工控威脅具備高度隱蔽特性。傳統監控多著重在IT層面的網路流量與主機行為，對工控通訊協定與流程參數異常的敏感度有限；現場工程人員雖熟悉設備與製程，但未必能立即將異常現象與資安事件聯想在一起。若組織內缺乏結合資安專業與工控知識的分析能力，往往要在異常已經影響到實體操作或造成服務中斷時，才意識到事件與資安有關。

第四節、國際法規與產業趨勢

國際社會對CI與OT環境的資安重視程度持續提高，相關法規與產業要求亦顯著從建議性指引走向具法律拘束力的合規框架。各主要經濟體紛紛建立CI之識別機制，明確界定哪些服務、系統與技術資產屬於國家命脈，並要求各中央目的事業主管機關與營運者建立正式資安治理架構、風險管理流程與事件通報制度，搭配查核與裁罰機制，以確保整體國家安全環境之穩定。

歐盟近年推動《網路安全指令》（DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)，下稱NIS2指令）與《網路韌性法案》（Cyber Resilience Act, CRA），將資安要求延伸至重大服務營運者、OT及ICT中具OT功能的系統相關供應鏈以及具數位元素之產品，使資安責任從營運者延伸至製造者與開發者，形成完整的安全生命週期要求。美國亦透過《美國關鍵基礎設施資安事件通報法》（Cyber Incident Reporting for Critical Infrastructure Act of 2022, CIRCIA）、美國能源部資安與能源韌性辦公室（Office of Cybersecurity, Energy Security, and Emergency Response, CESER）計畫、《北美電力可靠度公司關鍵基礎設施保護標準》（North American Electric Reliability Corporation Critical Infrastructure

Protection Standards, NERC CIP）系列標準等強化其能源、交通、通訊與工控系統安全管理，要求高關鍵性領域具備通報義務、事件應變機制與供應鏈保護措施。亞太多國亦陸續採行國際工業自動化控制標準（ISA/IEC 62443）為核心結構之工控資安標準，使國際工控安全要求逐漸趨同。

這些法規與標準的強化，使工控資安從原本以工程考量為主的領域轉變為各國 CI 法制的核心要素。各國皆要求營運者在治理結構、風險評估、控制措施與事件回應中明確納入 OT 系統，而非僅針對 IT 系統進行保護。同時，供應鏈風險被普遍視為跨國重大威脅來源，各國監管機關陸續要求設備製造商、系統整合商與軟體供應商遵循安全開發流程、弱點通報、更新維護與產品安全聲明等義務，使 OT 與 ICS 供應鏈安全逐漸制度化。

在產業實務方面，設備製造商、OT 系統整合商與雲端平台提供者皆面臨來自法規與客戶的雙重壓力，紛紛調整產品設計、研發流程與支援機制，導入安全配置、韌體簽章、弱點揭露與完整性保護機制，並建立更完善的維運與遠端連線控管模式。營運者亦逐漸將工控資安納入營運風險管理與企業治理架構，從過去的專案式投入轉變為長期策略性投資，提升事件偵測能力、補強弱點管理流程，並導入更成熟的事件應變與營運持續管理。

此外，隨著人工智慧自動化（Artificial Intelligence–Assisted Automation, AI-Assisted Automation）、雲端托管控制、虛擬化 OT 平台、數位孿生、邊緣運算與大量物聯網（IoT）裝置被逐步導入工控環境，新型態攻擊也同步增加，例如 OT 逐步接入雲端監控平台、廠商遠端維運需求增加、OT 資料與數位孿生模型在雲端運算環境中處理等情況，使 OT 不再僅是封閉環境，而成為高度互聯之生態系，進一步提高資安治理與供應鏈管理的複雜度。

綜合而言，國際法規與產業趨勢顯示工控資安已從技術議題提升為國家層級的治理議題。未來各中央目的事業主管機關在訂定防護基準時，需同時考量國際合規環境、供應鏈壓力、新技術架構與工控特性，使 CII 防護制度具有前瞻性與國際一致性，並能有效因應不斷演進的攻擊模式。

第五節、面臨的主要資安挑戰

綜合上述環境特性、攻擊態勢與制度發展，可以看到工控環境在國家與產業層面面臨多重資安挑戰。系統更新與弱點修補受到技術與營運限制，即使知道存在弱點，仍難以迅速完成修補，必須透過其他補救與補償手段降低風險。IT 與 OT 的融合帶來營運效益的同時，也擴大了攻擊路徑與介面，若缺乏對工控特性的理解與跨部門治理，將使原本應受嚴格保護的控制系統暴露於一般辦公網路的威脅之中。

遠端連線則成為最需要謹慎管理的高風險環節之一。從維運角度來看，遠端連線帶來便利與成本效益，但從資安與流程安全角度來看，任何未受控的遠端通道都可能成為繞過邊界防護與內部程序的捷徑。如何在維持必要維運效率的前提下，對遠端連線實施嚴格身分鑑別、最小權限、集中跳板與完整紀錄，是工控資安治理中不可迴避的核心課題。

此外，供應鏈與外包維運範圍持續擴大，營運者不再只管理自有設備與自家員工，而必須與多家外部廠商共同維護同一套系統。這使得資安責任的界線、作業規範的一致性與弱點處理的協調難度明顯提高。如果缺乏一套清楚的供應鏈安全要求與契約控制機制，就難以確保所有參與者都遵守同一水準的安全標準。

最後，偵測能力與專業人力亦構成挑戰。即使導入新的監控工具與防護設備，若組織內欠缺同時理解工控技術與資安威脅的專業人員，相關數據與告警也未必能被正確解讀與處理。如何培養與留任具跨域知識的工控資安人才，並建立常態化的訓練與演練機制，將決定工控環境在遭遇日益複雜攻擊時能否維持足夠的韌性。

第三章、 國際標準與法規對照

第一節、國際工控資安標準概述

ICS 與 OT 環境的資安管理在國際上大致形成兩套互補的安全體系。一套是以工業自動化與控制系統（Industrial Automation and Control System, IACS）本身為核心，透過正式標準界定系統、元件與生命週期應具備的安全能力；另一套則以一般資訊系統的安全控制為基礎，透過專門指引說明如何將資安控制調整適用於工控環境。前者的代表為 ISA/IEC 62443 系列標準，後者以美國《工業控制系統資安指引》（NIST SP 800-82）最具代表性。

ISA/IEC 62443 系列標準已成為全球工控資安領域最具權威性的國際標準體系，由國際自動化協會 ISA99 委員會與國際電工委員會 IEC TC65 WG10 共同制定，其內容涵蓋政策管理、系統安全要求、元件安全要求、安全開發流程與評估方法等面向，逐步形成可支援完整生命週期管理的安全架構。該系列標準隨技術演進持續更新，近年陸續發布安全設定檔、物聯網應用、安全評估方法等新內容，使整體標準更能因應現代化 OT 與工業物聯網（IIoT）環境的安全需求。

ISA/IEC 62443 不僅應用於傳統工控場域，也逐漸成為多個產業制定資安標準時的主要參考來源。船舶與海事領域之 UR E27、軌道交通領域之 IEC 63452、醫療設備領域之 IEC 60601-4-5 與 IEC 81001-5-1，以及半導體設備領域之 SEMI E187 等標準皆大量採用 ISA/IEC 62443 所確立的區域與通道模型、安全生命週期概念與技術控制能力，形成跨產業一致的安全框架。

表 1、基於 ISA/IEC 62443 來發展資安標準的產業以及其標準

產業	標準
醫療產業	1. IEC 80001-5-1：提供指導和要求，以確保與醫療相關的 IT 系統和設備在設計、製造和維護時能夠滿足必要的安全性和效能標準。 2. IEC 60601-4-5：針對醫療設備的基本安全和基本性能要求。
智慧製造產業	IEC 63283-3：此標準專為智慧製造領域制定，主要著重於執行系統及其相關組件的安全問題。
半導體產業	SEMI E187：專注於半導體製造設備的資訊安全。
核能產業	1. IEC 62645：核能資訊安全的主要指引，為核能設施提供具體的資訊安全規範和要求。 2. IEC 62859：專注於核能資訊安全相關的人才培養與技能提升。 3. IEC 63096：針對核電廠的日常運作所制定，為了保障其資訊系統的安全運作。
電梯與手扶梯產業	ISO 8102-20：針對電梯和手扶梯的安全標準，其中包含了其控制系統的資訊安全要求
航運產業	UR E27：該標準由多國的船舶分類社所組成的國際組織所制定，主要對船舶的資訊系統及其相關設備的安全進行規範。
鐵路產業	IEC 63452：為了確保鐵路運輸系統的資訊安全，此標準特別著重於鐵路的控制和營運系統的安全性。

資料來源：本防護建議自行整理

第二節、 ISA/IEC 62443 系列標準完整架構

ISA/IEC 62443 系列標準已從早期四大類發展至六大類，截至 2025 年已發布或制定中的標準超過二十項，形成涵蓋 IACS 全生命週期的完整架構。此系列由 ISA99 與 IEC TC65 WG10 長期合作推動，已被視為全球工控資安標準的共同基礎。

第一類一般性標準包含名詞與基本架構，例如 ISA/IEC 62443-1-1（術語與模型）、1-3（系統安全合規指標）、1-4（安全生命週期與使用案例）、1-5（安全設定檔）與正在制定的 1-6（IIoT 應用）。第二類政策與流程標準則聚焦於資安管理制度與組織治理，核心為 ISA/IEC 62443-2-1（資產擁有者資安要求），另包含 2-2（實施指引）、2-3（修補管理）與 2-4（服務提供者資安要求）。第三類標準聚焦於系統層級，包含 3-1 技術報告、3-2 風險評估方法與 3-3 系統技術安全要求，能協助組織判定安全等級與系統應採行之技術措施。第四類標準針對組件層級的安全設計與開發，包含 4-1 安全開發生命週期（Secure Software Development Life Cycle, SSDLC）要求與 4-2 組件技術安全要求。第五類尚未正式發布，但 ISA 與美國能源部共同制定的電力能源營運技術安全剖析（Electric Energy OT Security Profile）為此類的代表性文件，提供電力領域以 ISA/IEC 62443 進行條文對照的應用參考。第六類則涵蓋一致性評估方法，包括 ISA/IEC 62443-6-1（對應 2-4 的評估方法）與 ISA/IEC 62443-6-2（對應 4-2 的組件評估方法），使組織與評估單位能依據一致框架進行驗證。

六大類標準形成從政策制定、系統架構、安全開發到評估驗證的完整鏈結，使營運者與各中央目的事業主管機關能依同一套語言與方法推動資安管理。本防護建議即以此架構作為基礎，將標準內容轉化為可落實於我國 CII 管理制度的政策化建議。

表 2、ISA/IEC 62443 系列標準架構

類別	標準號碼	標準名稱
一般性 (General)	62443-1-1	概念與模型
	62443-1-2	術語與縮寫詞彙表
	62443-1-3	系統安全性一致性指標
	62443-1-4	IACS 安全生命週期和使用案例
	62443-1-5	網路安全性設定檔架構
	62443-1-6	在 IIoT 中應用 ISA/IEC 62443 標準
政策與程序 (Policies & Procedures)	62443-2-1	IACS 資產擁有者的安全計畫要求
	62443-2-2	IACS 保護等級
	62443-2-3	IACS 環境中的修補管理
	62443-2-4	IACS 服務提供者的要求
	62443-2-5	IACS 資產擁有者的實施指南
系統 (System)	62443-3-1	IACS 的安全技術
	62443-3-2	安全風險評估和系統設計
	62443-3-3	系統安全要求和安全等級
組件 (Component)	62443-4-1	安全產品開發生命週期要求
	62443-4-2	IACS 組件的技術安全要求
設定檔 (Profiles)	62443-5-x	基於各產業之設定檔
評估 (Evaluation)	62443-6-1	62443-2-4 的安全評估方法
	62443-6-2	62443-4-2 的安全評估方法

資料來源：本防護建議自行整理

第三節、工控資安生命週期與責任架構

ISA/IEC 62443 將工控資安視為「全生命週期作業」，生命週期包含需求識別、系統設計、建置實施、驗證確認、營運監控、維護管理與系統除役共七個階段。此架構確保安全措施不僅在建置期生效，而能在系統長達

十年以上的生命週期中持續維運。

在需求識別階段，資產擁有者（Asset Owner, AO）需確認安全需求與目標等級，並進行初步風險評估。系統設計階段則由系統整合商（System Integrator, SI）依據需求規劃架構，包含區域與通道模型、網路分層與安全控制配置。建置階段包括硬體安裝、軟體佈署、組態設定與教育訓練，並由整合商與供應商共同進行。驗證階段則透過功能測試、整合測試、效能測試與資安測試確認安全控制成效。營運階段需建立監控、異常偵測與事件通報流程。維護階段則處理更新、修補、設備保養與政策調整。最終除役階段需確保資料清除、設備回收與文件保存不造成安全風險。

利害關係人包含 AO、SI、服務維護商（Service Maintainer, SM）與產品供應商（Product Supplier, PS）。各角色在不同階段承擔不同責任，AO 負最終責任，SI 負責架構與整合，SM 主導營運維護，PS 負責符合安全要求的產品開發與弱點修補。此架構強調資安為共同責任，需要所有利害關係人持續協作以確保整體工控系統的安全與穩定。

圖 1、工業控制生命週期

資料來源：本防護建議自行整理

第四節、《工業控制系統資安指引》NIST SP 800-82

NIST SP 800-82 則偏向實務導向的指引文件。它並不重複發明一套新的工控專用標準，而是以一般資訊系統安全控制架構為基礎，解釋這些控制在工控環境中的適用方式、限制條件與調整原則。文件從工控架構與典型拓樸出發，逐一說明網路分區、存取控制、通訊防護、營運持續與事件通報在工控情境中應如何理解；例如，該指引說明工控系統常因停機成本與相容性問題，無法依照傳統 IT 更新頻率及方式進行更新，並說明為何某些在 IT 領域被視為標準作法的安全機制，在工控領域可能需要調整佈署方式或搭配補償控制。

在管理層級，許多國家與產業會進一步將這些標準與指引整理為工控資安管理架構或控制框架，也就是常說的網路安全框架（Cybersecurity Framework, CSF）。這類框架通常以 ISA/IEC 62443 系列中對資產、區域、系統壽命週期與組織流程的要求為基礎，將其整理成較容易理解與管理的領域與控制構面，例如治理、風險管理、資產管理、技術控制與事件處理等。之後再參考 NIST SP 800-82 這類指引文件中對實作細節與場域限制的說明，將框架中抽象的控制項轉換成實務可執行的設計原則與作業程序。

從角色與關係來看，ISA/IEC 62443 屬於「正式標準」，負責回答工控系統在不同層級上應具備哪些安全要求與能力；工控資安管理框架則是基於這些標準所萃取出的「指引型框架」，用來協助各中央目的事業主管機關與營運者在治理與管理層面拆解責任與控制構面；NIST SP 800-82 則屬於「實務指引」，負責說明當組織要依循框架與標準時，在真實工控環境中可以如何調整技術配置與操作流程。標準提供要求，框架整理架構，指引說明落實方式，三者共同構成國際工控資安防護的主要支柱。

第五節、歐盟 NIS2、CRA 等監管發展

在監理法制層面，歐盟近年透過多項法規強化對關鍵服務與具有數位元素之產品的資安要求。其中，NIS2 指令是針對網路與資訊系統安全所建

立的統一法律框架，取代早期的第一版 NIS 指令。新版指令將適用範圍擴大到十八個關鍵與重要領域，涵蓋能源、運輸、醫療保健、飲用水、金融市場基礎設施、數位基礎設施以及公共行政等，要求成員國對這些領域中的營運者建立更嚴格的資安治理、風險管理與事件通報規範，並賦予監理機關更高的稽核與裁罰權限，以確保各國實質提升關鍵服務的整體資安水準。

另一方面，CRA 則專注於具有數位元素的產品本身。該法案已於 2024 年 12 月正式生效，並預計自 2027 年 12 月起全面適用，其間部分規定將分階段提前實施。法案要求所有在歐盟市場上提供且具有數位元素的產品，必須在設計與開發階段就納入資安考量，並在產品整個生命週期內持續維持弱點管理、更新與通報能力，包括在發現可利用弱點時，必須於限定時間內通報並提供修補措施，不得任由使用者長期暴露於已知風險之中。

NIS2 指令著重於確保重要與關鍵服務提供者在組織與營運層面具備足夠的資安治理與事件處理能力，而 CRA 則要求產品供應鏈的上游，包括軟硬體製造者與開發者，對其產品的安全品質與弱點處理負起責任。兩者搭配後，從服務營運者到 PS 形成完整的監理鏈條，避免出現「上游產品安全性不足、下游營運者卻需獨自承擔風險」的情況。

這些法規並非直接規定各組織必須採用特定工控標準或管理框架，但在實務上，多數歐洲國家與跨國企業會自然地以 ISA/IEC 62443 及相關管理框架作為符合 NIS2 指令與 CRA 要求的技術與管理基礎。也就是說，標準與框架在此扮演「如何滿足法規精神」的關鍵工具，而法規則提供強制性的導入動力與監督機制。

第六節、我國現行制度與國際架構關聯

我國在 CI 與 CII 防護方面，已透過行政院層級的政策與資通安全管理法建立基本架構。行政院發布的國家 CI 防護指導文件，將 CI 依功能屬性分成多個領域，並要求各領域之中央目的事業主管機關負責確認所轄 CI，

建立防護計畫與應變機制。隨著實務推動與威脅環境變化，CII 的範圍亦從早期八大領域調整為九大領域，納入更多與國家運作高度相關的新興服務與基礎設施，使制度涵蓋範圍更為完整。

資通安全管理法及其子法則從法規層面明定政府機關、特定非公務機關與 CI 提供者的資安責任，包含資安組織設置、資安維護計畫、通報義務與查核機制等。這些要求在精神上與國際上的風險管理架構與資訊安全管理制度高度相容，例如透過資產識別、風險評估、控制措施選擇與持續改善等流程，建立可稽核的管理系統。各中央目的事業主管機關在此基礎上，分別訂定所屬領域的工控資安防護基準或相關作業指引，形成「國家政策、母法授權、部會基準、CI 提供者實作」的治理階層。

在工控與 OT 環境方面，我國早期制定的 CII 資安防護建議與檢核表，主要是以國際工控指引與標準為參考來源，將工控環境中常見的控制需求整理為十一個防護類別，包括網路架構、存取控制、稽核與可歸責性、營運持續、識別與鑑別、通訊防護、系統與服務獲得、實體防護、系統與資訊完整性、組態管理與組織管理等。這種做法實際上是將國際標準與指引中的共同觀念整理為一套適合國內各領域參考的「共通底線」，提供各中央目的事業主管機關在制定防護基準時使用。

隨著歐盟 NIS2 指令、CRA 及其他國家 CI 法規的實施，全球供應鏈與跨國營運者開始面臨更高層級的合規壓力。我國各中央目的事業主管機關在研擬或修訂防護基準時，若能適度參考這些法規在治理責任、供應鏈安全、弱點揭露、通報時效與跨境合作方面的要求，將有助於確保本國 CI 不因制度差距而成為相對薄弱的一環，也能使國內 CI 提供者在面對國際合作與市場要求時，具備相容的資安管理水準。

從整體關聯來看，我國現行制度可視為在行政院政策與資安母法的架構下，逐步導入與整合國際工控標準與實務指引的過程。高層政策與法規確立責任與範圍，工控相關的防護建議與基準則將國際標準中的安全要求

轉換成適合國內情境的控制類別與實施重點，未來在面對國際法規與市場合規要求時，便能在既有制度基礎上進行調整與強化，而非重新開始建立新的體系。

第七節、國際標準於本防護建議中的運用

本防護建議在修訂時，並未單純追逐國際標準或法規名稱，而是從整體關聯與角色分工出發，將工控專用標準、管理框架與實務指引之間的關係整理為一個可供政策與實務共同使用的結構。在標準層次上，採用工控領域普遍接受的安全要求與分層分域概念作為設計基礎；在框架層次上，將這些要求拆解為各中央目的事業主管機關與 CI 提供者容易理解的防護類別與架構；在指引層次上，則透過實務說明與範例補充，使各類防護措施能在真實環境中找到具體的實施點。

換言之，本防護建議的內容並非任意羅列控制項目，而是有意識地承接國際工控標準與指引的共通精神，再結合我國 CII 的實際需求加以調整。各中央目的事業主管機關在引用本防護建議制定或修訂防護基準時，可以將其視為一套已經過國際經驗萃取與本土化整理的「中介層」，一方面維持與國際標準體系的一致性，另一方面也保有彈性，足以因應我國不同領域在技術、營運與法規上的特殊需求。

第四章、 防護架構與原則

第一節、防護架構之整體構想

本防護建議所採用的防護架構，是在既有國家 CI 政策與 CII 管理制度之上，建立一套兼顧治理、技術與實務執行的工控資安整體藍圖。這個架構的核心精神，是讓各中央目的事業主管機關與 CI 提供者在談論 ICS、OT 與 ICT 安全時，有一個共同的結構與語言，能夠對應國家政策、產業特性以及實際現場運作方式。

在系統觀點上，此架構強調分層與分域的思維。分層部分，將與 CII 運作相關的各種系統區分為企業管理層、營運管理層、控制系統層與現場設備層，使每一層的資安責任與防護重點更為清楚。企業管理層聚焦於策略、治理與資源配置，其系統多為一般企業資訊系統；營運管理層則負責排程、派工、維護管理與歷程資料分析，是連接企業決策與現場控制的橋樑；控制系統層主要包含各式控制伺服器、工程工作站、通訊閘道與資料伺服器，負責對現場設備下達命令並接收回報資訊；現場設備層則由感測器、致動器、智慧電子設備與機電設備構成，直接與物理世界互動。

在分域方面，防護架構強調將不同信任程度與不同功能性質的資產劃分在各自的安全區域內，例如企業管理區、營運管理區、控制區與現場區，並在它們之間設置非軍事區或資料中介區（DMZ）作為緩衝。區域之間的通訊必須透過具備存取控制、稽核與內容檢查能力的通訊通道連結，而非任意直接互連。這樣的設計可以避免單一區域的資安事件立即蔓延到整體系統，也便於針對不同區域配置適當的控制強度與監控機制。

在此防護架構下，國家層級的政策與法規負責設定整體方向與最低要求，例如哪些行業與系統屬於 CII 範圍、各 CII 層級應具備的基本資安能力，以及各中央目的事業主管機關與 CI 提供者各自的角色定位。各中央目的事業主管機關依據國家政策與本防護建議的架構，結合所轄領域的技術與風險特性，制定具體防護基準與配套作業指引，包括分級要求、查核機

制與輔導方式。CI 提供者則依據這些防護基準與本防護建議的內容，在自身的 ICS、OT 與 ICT 環境中，設計並建置兼具預防、偵測、應變與復原能力的防禦體系，使整體防護從政策到現場形成一致且可追溯的架構鏈結。

第二節、分層與分域原則

工控資安防護若缺乏清楚的分層與分域，容易導致責任歸屬不明、控制措施混用以及風險擴散難以阻斷等問題。因此，本防護架構將分層與分域視為最基本且最重要的設計原則。

在分層部分，企業資訊層主要承載財務、人力資源、採購、客戶管理與一般行政資訊系統，其資安需求與一般資訊系統相近，但仍需考量與 CII 營運資料交換而可能帶來的附加風險。營運管理層負責將企業策略與現場運作連結起來，例如生產排程、保養計畫、資產管理與歷程資料分析等，這一層既需與企業管理層交換資料，又必須與控制系統層保持穩定與安全的通訊關係，若設計不當，容易成為 IT 威脅入侵 OT 的中繼點。控制系統層是工控資安的核心，包含控制伺服器、工程工作站、資料伺服器與通訊閘道等，其行為會直接影響現場設備與流程安全，因此在存取控制、變更管理與監控上必須採取較企業層更為嚴謹的標準。現場設備層則由感測器、致動器、智慧電子設備、變頻器與保護裝置等構成，多數設備位於環境較為嚴苛且難以直接管理的位置，資安防護必須透過上層系統與現場實體防護共同實現。

在分域部分，系統架構設計者需要根據功能、信任等級與對安全的敏感度，將上述各層中的設備與系統劃分到不同安全區域。例如，可以為企業管理業務建立一個管理區，為營運管理與資料交換建立一個 DMZ 或營運區，為控制伺服器與工程工作站建立一個高保護的控制區，並將現場設備視為受控的現場區。在管理區與控制區之間設置 DMZ，用來放置歷程資料庫、報表伺服器與必要的資料轉換服務，使企業層與控制層之間不必直接互通，而是透過受到嚴格規範的 DMZ 間接交換資訊。各區域間的通訊

需透過具備防火牆功能、通訊協定過濾與稽核記錄能力的設備進行管理，確保每個通道只有經過核准的流量與協定可以通過，並能在事後追蹤與分析通訊行為。

透過這種分層與分域的設計，CI 提供者可以針對每一層、每一區域規劃相對應的防護深度與運作規範，使高度關鍵的控制與現場區域在防護強度與監控密度上明顯高於一般資訊區域，也能在發生資安事件時，將影響限制在特定區域內，避免全系統同步暴露於同一危害。

表 3、分層與分域原則對照表

架構維度	層級名稱	核心功能與承載系統	資安防護重點與特性	建議劃分之安全區域
分層設計	企業資訊層	財務、人力資源、採購、客戶管理、一般行政系統。	資安需求與 IT 系統相近，但需警惕與 CII 營運資料交換的風險。	管理區
	營運管理層	生產排程、保養計畫、資產管理、歷程資料分析。	核心風險點：若設計不當，極易成為 IT 威脅入侵 OT 的中繼點。	營運區
	控制系統層	控制伺服器、工程工作站、資料伺服器、通訊閘道。	直接影響流程安全，存取控制與監控標準最為嚴謹。	控制區
	現場設備層	感測器、致動器、智慧電子設備、變頻器、保護裝置。	環境嚴苛且管理困難，需依賴上層系統與實體防護。	現場區
分域設計	資料中介區	歷程資料庫、報表伺服器、資料轉換服務。	位於管理區與控制區之間，避免兩層直接互通，落實間接交換。	DMZ

資料來源：本防護建議自行整理

第三節、風險導向與安全等級

在資源有限與威脅持續演變的情況下，防護架構的設計必須以風險導向作為核心原則，而非對所有系統套用完全相同的控制強度。本防護建議強調，各中央目的事業主管機關與 CI 提供者在規劃 CII 防護措施時，應先透過風險評估掌握各類資產的重要性、脆弱性與可能事故的影響程度，再據以決定所需的安全等級與控制深度。

風險評估的過程應包括對資產類型與角色的辨識，例如哪些系統屬於維持公共安全與關鍵服務不可或缺的核心控制系統，哪些則為支援性或輔助性系統。亦需考量威脅情資與攻擊趨勢，例如近期是否有針對特定通訊協定、控制器型號或供應鏈的攻擊案例，以及自身環境中是否存在類似條件。同時，還應檢視既有防護措施的成熟度與潛在弱點，例如網路區隔是否確實執行、弱點修補流程是否運作順暢、事件通報與應變是否能在合理時間內完成。

在安全等級的設計上，可透過將風險評估結果轉換為不同層次的防護要求，使每一區域或系統在網路架構、存取控制、監控偵測、營運持續與事件通報等面向具有相對應的最低標準。安全等級較高的區域，可能需要更嚴格的身分鑑別、更精細的權限分派、更密集的稽核與監控，以及更完善的備援與復原機制；相對風險較低的區域，則可採較為簡化但仍符合基本安全的防護安排。

對各中央目的事業主管機關而言，在制定防護基準時，應結合我國資安責任等級分級機制與領域特性，建立一套清楚連結「CII 等級、風險程度與最低控制要求」的對應關係，使 CI 提供者得以依據自身環境進行細化與落實。如此一來，安全等級就不再只是抽象概念，而是與實際防護措施、查核指標與改進優先順序緊密相連的管理工具。

第四節、縱深防禦、安全原則與零信任

縱深防禦是工控資安防護中最核心且最穩定的策略之一，其目標在於

避免系統安全完全依賴單一技術、單一邊界或單一流程。工控環境的攻擊多半具有漸進式、潛伏式與跨區域移動的特性，因此防護架構必須能在不同的層次與階段形成阻力，使攻擊者即便突破某一防禦面向，也無法輕易擴散或取得系統控制權。縱深防禦的核心邏輯在於「多層、多點、獨立、互補」，每一層防護都能在其他層失效時提供替代或延緩效果，使整體系統保持安全韌性。

在網路層面，縱深防禦透過安全分區、跨區通訊限制、協定過濾與流量檢查，使攻擊行為無法自由穿越區域邊界。控制系統區域與外部網路之間必須存在可監督、可稽核且具備檢查能力的安全通道，降低以 IT 作為入口滲透 OT 的風險。在系統與主機層面，透過系統加固、最低安裝、權限最小化、程式白名單與程式完整性驗證，使攻擊者即便取得部分帳號或低階權限，也難以沿著既有功能進行濫用。在應用與資料層面，縱深防禦透過資料完整性驗證、行為監控、異常偵測與詳細的日誌記錄，提升對操作異常與惡意行為的可見度，使內部或外部的攻擊行為能夠在造成重大影響前被辨識。

上述技術防護之外，本防護建議將安全設計理念正式納入整體架構，使安全不再是系統建置完成後的補強措施，而是從生命週期起點便持續存在。Secure by design 的精神，要求系統在規劃與設計初期便將安全視為基本屬性，並確保控制邏輯、設備選型、通訊協定與資料流向能在結構上避免已知弱點。對工控設備而言，此原則尤為重要，因為許多控制器與設備在部署後難以重新調整設計，若在初期未納入安全考量，後續補救成本將極高。

Secure by default 則強調系統在交付與啟用當下即具備安全預設值。工控場域常見許多來自預設弱點的風險，例如預設密碼、未關閉的測試埠、未啟用的稽核功能與開放式通訊模式。安全預設原則要求供應商與建置團隊在產品與系統出廠或上線時即啟用必要的安全機制，使安全性不是需要

額外設定才會啟動，而是在基礎組態中即內建。

Secure by demand 則是工控環境中管理「例外維運需求」的最佳方式。在實際運作中，維運團隊常需在緊急狀況、測試階段或排除故障時開放高權限或臨時通道。若這些例外需求以長期開放方式存在，將使整體防護失去作用。Secure by demand 的精神是所有高權限或特殊操作都必須以限時授權、一次性密鑰、可追蹤的跳板系統與事後稽核來管理，使高風險操作不會在系統中長期停留。

在邏輯防護之外，實體安全是縱深防禦不可分割的一部分。工控設備多位於廠房、變電站、抽水站、隧道機房或無人值守站點，攻擊者若能直接接觸設備，便可能繞過所有邏輯層面的保護，直接插入惡意裝置、竄改組態、破壞纜線或植入有害韌體。實體安全因此必須涵蓋門禁、設備櫃安全、防拆封機制、環境監控、訪客管理與巡檢制度，確保現場設備在任何時間都不會暴露於未經授權的接觸。

此外，本防護建議亦引入零信任的核心精神，以補強傳統「可信區域」模式的限制。過往工控環境常以邊界作為信任依據，只要設備或人員位於控制網域內，便被視為可信。然而 IT 與 OT 融合、供應鏈依賴與遠端維運普及，使此假設不再安全。零信任的核心是「不預設信任任何人、任何設備、任何區域」，每一次跨區或高風險操作都需重新驗證，並依據身分、設備狀態、行為模式與當時情境來決定是否授權。

在工控場域中，零信任並非要求對所有通訊強制加密或進行頻繁身份驗證，而是要求針對高風險連線與控制指令採取更細緻的驗證與監控。例如跨控制區的管理操作必須經由跳板系統進行並要求多因素驗證，遠端維運必須使用限時授權與完整錄影記錄，對具高風險特性的設備則需強化設備身分辨識與行為基準線分析。透過零信任思維，工控環境能從「區域信任」邁向「動態信任」，使攻擊者即使突破單一區域，也無法取得持續性控制權。

綜合而言，縱深防禦為整體架構提供多層次阻擋，安全原則確保系統從起點即具備安全特質，零信任則重新定義系統授權與信任邏輯，使工控系統能在高度整合與高威脅環境中維持可控、可證明且具韌性的安全狀態。

第五節、治理與管理原則

治理與管理原則是整體防護架構能否長期有效運作的基礎，也是確保 CI 提供者在高度複雜、跨部門且與公共利益高度相關的環境中維持可持續安全能力的核心機制。工控資安的治理不能侷限於技術部門或單一維運單位，而必須建立於組織治理層級的明確責任架構之上，使資安決策、資源投入、風險評估、流程管理與事件應變都能在統一且可稽核的制度下執行。

工控資安治理的第一個要素是組織層級的權責劃分。組織內應具備能對 CII 資安負最終責任的高階管理者，負責批准資安政策、分配資源並確保資安融入整體營運策略。資安主管則需具備跨部門協調功能，協助 IT、OT、工務、維運、採購與風險管理等部門建立共同作業模式，避免因職能差異而造成政策落差。此外，工控系統相關單位需明確了解自身在控制系統維護、變更流程、遠端存取管理、設備採購與委外作業中的責任，以確保所有可能影響 ICS/OT 安全的活動均在既定程序下進行。

第二個要素是制度化的管理流程。工控資安的複雜度在於其需同時考量流程穩定性、設備可靠性與安全需求，因此治理架構必須要求營運者建立可持續運作的管理制度。此制度需涵蓋完整的資產盤點，使組織能掌握所有 CII 相關系統、控制器、現場設備、通訊線路與軟體組態。風險評估也必須定期執行，用以辨識新興威脅、弱點暴露與營運變動對系統造成的影響，並作為資安改善與資源配置的依據。

變更管理是工控資安治理的另一個核心。任何可能影響工控系統行為的變更，包括程式修改、控制邏輯更新、系統修補程式、網路調整、設備汰換或施工作業，都必須納入嚴謹的變更管理流程。此流程應包含風險評估、測試驗證、授權核准、作業監督與事後紀錄，使每一次變更可追溯、

可驗證並能確保不會影響流程安全或破壞既有控制架構。

事件通報與應變能力是治理中不可或缺的一部分。工控環境中的資安事件可能同時影響營運、公共安全與設備完整性，因此事件通報流程需同時考量資安、營運與安全等不同維度。治理架構必須要求營運者建立明確的事件識別、升級、聯繫與通報程序，並與各中央目的事業主管機關的通報要求保持一致。在重大事件發生時，組織必須能同時啟動資安應變程序與營運持續計畫（BCP），避免因延誤或資訊不一致而擴大影響。

教育訓練與能力培養亦是治理架構的重要組成。工控環境的安全需要同時理解控制系統、網路通訊、現場流程與威脅行為，因此跨領域能力不足往往會造成偵測延遲或誤判。治理架構應要求營運者為不同職務層級提供適當的訓練，例如高階管理者需理解 CII 安全對營運與法規遵循的影響，工程與維運人員需熟悉工控系統特有的安全風險，資安團隊需具備分析 OT 異常行為與指令模式的能力，而外包廠商則需遵守組織制定的安全規範。透過制度化訓練，可避免因人員調動或承攬外包造成知識斷層，使安全能力能持續累積。

治理與管理原則的另一個面向是供應鏈安全。工控系統的建置、維運與更新需要高度依賴外部供應商，因此治理架構需將供應鏈納入管理範圍，包括契約要求、安全責任、維運流程、通報義務與弱點修補時限。若供應商缺乏一致的安全要求，整體工控系統將難以維持穩定的安全能力。因此治理架構需要求營運者制定明確的供應鏈管理政策，包括廠商評估、作業規範與審查程序，使外部單位的操作與組織內部的安全流程保持一致。

最後，治理架構必須包含持續改善機制。工控資安是動態領域，威脅、設備與系統使用方式均會隨時間變動，因此治理流程需定期檢討資安政策、管理流程、防護控制、事件紀錄與查核結果，並依據過去事件或演練結果調整管理方式。透過持續改善，組織才能在面對快速變動的威脅環境時保持韌性，並確保其防護能力始終符合國家政策、法規及防護基準等要求。

透過上述治理與管理原則，防護架構可從策略層、組織層、流程層與技術層形成一致的治理體系，使 CI 提供者能在高度複雜的工控系統環境中保持透明、可管控與可持續的安全能力，並確保國家 CI 運作的穩定性與安全性。

第五章、 工控系統防護建議

第一節、工控系統網路架構

工控系統網路架構是整體資安防護的基礎核心，其功能遠不僅是傳輸資料，更是直接承載設備控制、流程調度與安全保護等高度敏感操作。工控網路與一般資訊網路最大差異，在於工控網路的傳輸及處理延遲具有高度敏感性，任何延遲、丟封包或不當流量阻斷都可能導致系統誤動作或設備失效。因此工控網路架構的設計必須充分考量即時性、可靠性、流程安全與資安防護等因素，並以最小暴露面與最小通道為原則進行部署。

5.1.1 網路分層分區規劃

- 建立明確的分層與分區，將企業管理區、營運管理區、控制區與現場區分開，確保不同類型的系統不共享同一安全邏輯。
- 透過分區隔離，避免低風險區域的威脅立即影響到高風險或高敏感的核心控制系統。
- 工控設備在可能情況下不宜直接接觸網際網路，以降低受攻擊之風險。

5.1.2 通訊通道管制

- 跨區通訊須採用白名單機制，嚴格限定來源、目的、協定、封包型態與通訊方向。
- 區域間之串接須採用受控且具稽核能力的通道，任何未經授權的通訊都必須在邊界即被拒絕。
- 嚴格執行最小通道原則，僅開放系統運作所必須之連線路徑。

5.1.3 中介區與維運管理

- 歷程資料伺服器、監控伺服器與需要跨區提供資料的應用程式，宜置放於 DMZ，避免機敏資訊系統直接接觸工控控制核心。
- 必要的更新與維運通道透過分段式與跳板式設計管理，確保外部來源無法直接接觸控制系統。

5.1.4 即時性保障與快速隔離能力

- 網路架構設計須避免不當的流量阻斷、延遲或丟封包，以防止系統錯誤動作或設備失效。
- 系統宜支援快速隔離功能，當偵測到異常流量、惡意封包或橫向擴散跡象時，能立即切斷特定區段或封鎖部分通道。
- 強化事故損害控制能力，確保 CI 在事故發生時能降低影響範圍並維持連續運作。

第二節、 存取控制

存取控制是工控環境中保護控制核心不受未授權操作的最重要措施之一，也是所有防護機制中最直接關係到人員行為與責任歸屬的環節。工控系統的存取控制必須同時滿足可追溯性、最小權限、操作分離與臨時授權等需求，使每一項操作都能被確實辨識、核准與追蹤，以避免未經管控的操作構成營運與資安風險。

5.2.1 帳號管理與權限配置

- 落實個別化帳號：所有工控系統宜要求採用個別化帳號以避免責任模糊。若因特殊場景須使用共用帳號，必須搭配排班紀錄、影像監控或工單系統，以確保操作之可追溯性。

- 明確區分職能權限：工程人員、維運人員、管理者與外部廠商均需配置不同帳號與權限，禁止以高於必要等級的權限執行日常操作，確保符合最小權限原則。

5.2.2 高風險操作與授權機制

- 多階段核准流程：針對程式下載、可程式化邏輯控制器（PLC）組態變更、保護邏輯修改、系統重啟或模式切換等高風險操作，宜採取二階段核准、獨立人員覆核或多因子鑑別。
- 限時授權管理：任何短期、例外或高敏感度操作，宜採用一次性身份識別或限時授權方式，避免高權限帳號因長期暴露而導致安全漏洞。

5.2.3 遠端存取與跳板系統管理

- 強制跳板存取：遠端存取透過跳板系統強制進入，嚴禁直接連線至控制伺服器或工程工作站，以防止攻擊者繞過現場防護措施。
- 強化事件日誌與監控：跳板系統宜具備完整記錄操作軌跡、限制執行命令及強制多因子鑑別之功能，以利事後稽核與風險控管。
- 結合工單流程：遠端存取宜與工單流程連動，確保所有授權、操作與紀錄一致，防止未經許可的協力廠商操作或不當維運行為。

第三節、事件日誌與可歸責性

事件日誌與可歸責性是確保工控操作能追蹤、能調查、能驗證的重要基礎。工控系統的操作多半直接對應到實體設備的狀態變化，因此任何未被紀錄的行為都可能在事故發生時形成調查盲點。建立完善的稽核機制，能確保事故發生後釐清事實，並支持事件調查、法規遵循與營運持續管理。

5.3.1 日誌紀錄範疇與保存

- 完整記錄操作行為：日誌紀錄宜包含身分識別、登入與登出、組態修改、控制邏輯下載、參數調整、權限變更、系統警示、設備異常及模式切換等資訊。
- 確保資料完整性：日誌資料的格式應考量現場系統可行性，並採取保護措施，確保紀錄不被未授權篡改或刪除。
- 集中管理與分析：日誌紀錄宜透過集中管理方式保存，以支援長期的事件分析與資安稽核需求。

5.3.2 異常偵測與即時告警

- 建立告警機制：當偵測到登入失敗、權限升級、非預期的程式下載或異常流量時，宜能即時產生告警並通知相關人員。
- 強化早期預警能力：透過即時告警機制，使 CI 提供者能在攻擊造成實質損害前，及早採取行動處置，降低營運風險。

5.3.3 事件調查與持續改善

- 支援事故溯源：日誌資料需與事件調查流程結合，確保在事故發生後能釐清操作責任歸屬與事實真相。
- 最佳化營運管理：透過日誌紀錄的檢視，分析事故原因以避免重複性錯誤，並作為最佳化安全防護政策之依據。

第四節、 營運持續計畫

BCP 的核心在於確保關鍵流程在面對設備故障、資安攻擊、軟體異常或外部環境變化時仍能維持最低程度的運作。工控環境中的營運持續性並非僅指「能夠運作」，而是「在不安全狀態下仍能維持核心流程不失控」。因此 BCP 需要同時結合資安事件情境與流程安全的需求，以降低對公共安全或重大營運的衝擊。

5.4.1 備援架構與相依性評估

- 明確界定運作需求：CI 提供者需定義各控制系統的最低運作需求、系統間相依性與可接受的中斷時間。
- 建立多元備援機制：依據評估結果建立備援架構，包含冗餘伺服器、同步資料庫、替代通訊路徑及自動切換機制，確保單點故障不致影響整體流程。

5.4.2 安全模式與保護機制

- 具備安全模式能力：控制系統在偵測到異常或進入不可信任狀態時，宜能進入限制性操作模式、保護性停機或僅保留基本監控能力。
- 防止事故擴大：透過系統安全模式的切換，避免設備受損、流程失控或對人員安全造成威脅。

5.4.3 定期演練與應變協作

- 實施多情境演練：定期進行包含系統故障、惡意攻擊與通訊隔離等情境的演練，以驗證技術防護與應變流程之有效性。
- 強化通報與跨部門協調：演練宜涵蓋人員判斷流程、跨部門溝通，以及與各中央目的事業主管機關的通報協作。
- 提升回應效率：透過演練確保在緊急情況下能快速回應，將事故影響範圍與損害降至最低。

第五節、 識別與鑑別

識別與鑑別控制是防止未授權使用者或設備進入工控核心的重要機制。所有使用者必須具備唯一可識別的身份，其行為需與具體個人產生關聯，以確保操作都具備可追溯性。透過合適的身分管理與設備驗證，能有效防止單一身分遭冒用或未經授權之裝置存取工控環境。

5.5.1 使用者身分識別與追蹤

- 具備唯一身分識別：所有使用者具備唯一帳號，確保其操作行為能與具體個人產生關聯，落實操作責任歸屬。
- 輔助管控機制：針對技術限制無法支援個人帳號的舊型系統或場景，宜透過門禁管控、錄影監視、工單系統或排班制度進行輔助，以維持操作的可歸屬性。

5.5.2 高風險操作之進階鑑別

- 採取多重身分鑑別：針對工程邏輯修改、保護參數變更或緊急停機程序等高風險操作，宜採取多因子鑑別或第二階段確認機制。
- 防止身分濫用：透過加強鑑別機制，防止單一身分因洩漏、被濫用或遭冒用而導致嚴重的系統性風險。

5.5.3 設備識別與連線管控

- 禁止匿名裝置連線：工控環境宜嚴禁匿名或未經註冊的裝置連線，避免不明設備成為資安破口。
- 實施設備白名單機制：宜透過裝置指紋、白名單或可驗證之硬體識別機制，確保僅有經核准且受信任的授權設備能參與系統通訊。

第六節、 系統與通訊防護

工控環境的系統與通訊防護必須兼顧低延遲、高可靠度與高完整性的需求。控制系統下達的任何指令都可能影響實體設備，通訊內容與系統組態必須受到嚴格保護，確保資料在傳輸與儲存過程中不被竄改，並維持系統組態的可信度與可恢復性。

5.6.1 通訊完整性與通道管控

- 強化通訊完整性保護：針對控制指令與傳輸資料進行完整性驗證，避免通訊內容遭到惡意竄改，確保實體設備執行之指令準確無誤。

- 跨區域通訊檢查：跨區域之資料交換須透過受控通道傳輸，並對通訊協定、控制指令及網路封包進行深度檢查，確保通訊過程安全可靠。

5.6.2 關鍵資料儲存與完整性保護

- 確保儲存資料不可竄改：關鍵資料如稽核日誌、歷史紀錄與安全參數，其儲存方式確保不被未授權刪除或竄改，必要時採取唯讀儲存或數位簽章驗證。
- 強化備份資料安全性：儲存的備份檔案進行完整性驗證，確保在系統復原時，所使用的資料是完整且未經更動的。

5.6.3 系統異動與變更管理

- 落實版本控制與驗證：針對組態檔、控制邏輯、工程程式與安全參數等核心資料，建立版本控制機制與完整性驗證程序。
- 建立詳盡變更紀錄：所有系統異動皆記錄並可供追蹤，確保任何變更都能被檢視，並在發生異常時能迅速復原至已知安全狀態。

5.6.4 異常偵測與即時應變

- 部署偵測與監控能力：系統宜具備偵測異常封包、可疑登入或未經授權操作之能力，並在發現異常時立即產生告警。
- 快速介入與調查：透過即時告警機制，使 CI 提供者能迅速介入處理，並針對資安事件進行後續調查，以防範危害擴大。

第七節、 系統與服務獲得

工控系統在導入新設備與服務時，系統與服務獲得階段是將安全要求納入規範的關鍵時機。如果在規劃與採購階段未明確納入資安要求，後續即使發現弱點，也常因原廠不支援、契約未約定或技術限制而難以補救。

因此，在導入任何控制系統、通訊設備、監控平台、雲端服務或維運服務之前，CI 提供者於規格書與合約文件中清楚列出安全設計、弱點處理、更新提供與事件通報等面向的具體要求，並將其視為採購評選與履約查核條件之一。

5.7.1 採購規格與供應商管理

- 明確資安規格要求：要求供應商說明產品在身分鑑別、存取控制、日誌紀錄、通訊保護與組態管理所具備的功能，並確認其遵循安全開發流程與測試程序。
- 建立弱點處理機制：要求供應商建立正式的弱點通報與修補流程，包含預期的修補發布時程、支援期間與通報管道，以便安排適當的導入時機。
- 控管遠端維運安全：針對具備遠端維運功能的設備與服務，供應商須說明遠端存取的安全機制與審核流程，避免未受控的通道長期存在。

5.7.2 軟體組成清單與風險評估

- 提供軟體組成清單（SBOM）：針對以軟體為核心的控制系統與平台，要求供應商提供 SBOM，並隨版本更新維持其完整性與即時性，以支撐弱點管理與風險評估。

5.7.3 外部服務與委外管理

- 查核資安管理制度：確認雲端平台、遠端監測、系統託管與維運外包服務商是否建立資安管理制度，並具備事件通報與應變能力。
- 明確責任與稽核權利：界定資料主體與資安責任歸屬，並要求供應商提供稽核報告或安全評估結果，避免責任模糊。

- 資料備援與可攜性：針對存放關鍵設定或歷程資料的外部平台，需確認資料備援機制，避免因服務終止或供應商問題導致營運風險。

5.7.4 系統文件與技術資料管理

- 建立文件管理體系：確保所有工控設備均有完整的設計文件、組態紀錄、版本資訊與維護紀錄，作為風險評估與變更管理的依據。
- 原始程式碼與技術交接：針對委外開發與客製系統，要求保存原始程式碼、建置文件與測試報告並進行交接，防止未來無法維護或安全性難以評估的情形。
- 確保維運連續性：透過完善的文件制度，防止關鍵技術資訊過度依賴特定個人或單一廠商，確保在設備故障或人員異動時，相關人員仍能依循技術文件維持系統運作，避免營運中斷風險。

第八節、 實體與環境防護

實體與環境防護是工控環境中不可或缺的一環，甚至在某些情境下，其重要性高於邏輯層面的資安控制。只要攻擊者能直接接觸控制器、通訊設備、機櫃或纜線，就可能繞過大部分網路與系統層面的防護機制。因此，CI 提供者必須將實體安全納入整體防護架構的核心，而非視為附屬議題。

5.8.1 實體進出管制與現場防護

- 強化區域進出控管：機房、控制室與通訊機櫃採用門禁管制或監視措施，並完整保留人員進出紀錄。
- 落實設備實體保護：針對現場機櫃與設備，採取加鎖、防拆封條或封閉式櫃體等實體隔離方式，降低遭觸碰或竄改之機率。
- 訪客與承包商監督：外部人員進入敏感區域須事先申請與核准，作業期間由內部權責人員全程陪同，並詳實記錄作業內容、時間與使用工具。

5.8.2 環境條件監控與電力保障

- 確保電力穩定供應：關鍵設備配備不斷電系統與備用發電設備，並制定電力異常時的自動保護策略，確保運作不因電力中斷而失控。
- 維持適當溫濕度：空調與通風系統維持在設備設計規範之環境範圍內，避免過熱或水氣凝結，並定期進行濾網與風道維護檢查。

5.8.3 環境災害評估與預防工程

- 實施環境風險評估：針對易受水災、土石流或其他自然災害影響之設施，及早採取抬高設備位置、設置防水門或導水溝等預防性工程。
- 建立環境監測機制：針對高風險區域設置水位監測或坡面穩定監控等相關監控機制，確保在災害發生前能採取應變行動。

第九節、 系統與資訊完整性

系統與資訊完整性是確保工控環境可信運行的核心要素。由於錯誤或遭竄改的指令與參數可能直接導致設備誤動作或保護機制失效，CI 提供者必須從弱點管理、惡意程式防護與系統監控等多個層面，建立完整性維護機制，確保系統狀態與資料始終處於安全可信的範圍。

5.9.1 弱點管理與補償控制

- 建立弱點追蹤流程：定期追蹤供應商與權威機構發布之弱點通報與修補資訊，並依據系統重要性評估修補的必要性與執行時機。
- 落實修補驗證：更新前需先於測試環境驗證，並在可控的維護時段執行，以避免停機或不相容之風險。
- 實施補償控制措施：對於短期內無法修補的弱點，透過加強網路區隔、限制存取來源、強化監測與縮減功能等方式，降低弱點被利用的可能性。

- 利用 SBOM：結合系統與設備之 SBOM，快速識別受特定弱點影響之元件，提高修補與防護決策之準確性。

5.9.2 惡意程式防護策略

- 部署合適防護工具：針對使用通用作業系統之工作站與監控伺服器，部署經嚴格測試之防護工具，並設定不影響即時運作的掃描策略。
- 採取多重防護機制：對於資源受限之設備，可採取白名單、檔案完整性監控或啟動檔案檢查等替代方式。
- 管控外部傳輸媒介：對可攜式媒體（如隨身碟）、維護用攜帶設備與外部檔案建立強制檢查要求，防止惡意程式透過實體媒介竄入。

5.9.3 系統監控與異常偵測

- 建立行為基準線：定期定義正常流量範圍、登入模式、控制指令頻率與設備回應特徵，並對超出基準線之行為發出警示。
- 即時調查異常行為：當偵測到未知通訊對象、頻繁登入失敗或未預期指令時，立即通知人員介入調查，降低攻擊潛伏風險。
- 強化變更管控：針對控制邏輯、組態檔與歷程資料採用版本控管與完整性驗證，確保異動皆有跡可循，並能在必要時回復至已知安全狀態。

第十節、 組態管理

組態管理是確保工控系統在長期運作中保持穩定與安全的關鍵基礎。工控環境常因應營運需求、設備汰換與系統升級而持續進行調整，若缺乏嚴謹的組態管理，容易導致設定不一致、未授權變更、版本混亂與難以復原等問題。因此，CI 提供者必須建立正式的組態變更流程，並將其視為工控資安治理的一部分，而非僅屬工程作業層面的行政程序。

5.10.1 組態變更程序

- 建立標準變更流程：變更流程包含需求提出、風險評估、測試驗證、核准、實施與回復方案等完整步驟。
- 強化重大變更審查：凡涉及控制邏輯、保護機制或系統架構之重大變更，實施前須由權責單位共同審查其對安全與資安之影響。
- 落實測試與回復演練：關鍵變更先於測試環境演練，並確保變更失敗時具備迅速復原原始組態的能力。
- 選擇適當實施時機：變更安排於影響最小的維修時段，並由專人現場監控，以便在異常發生時即時介入。

5.10.2 最小功能原則與攻擊面縮減

- 僅啟用必要服務：遵循最小功能原則，關閉所有未使用或非必要的通訊埠、服務與應用程式，以縮減潛在攻擊面。
- 實施程式執行控管：針對可執行程式與腳本，採取白名單機制，確保僅有經核准的程式能於系統上啟動，防止未知程式運作。

5.10.3 變更紀錄與版本追溯

- 詳實記錄變更軌跡：變更紀錄完整涵蓋內容、時間、執行人員、原因與核准人，確保所有異動均有跡可循。
- 落實版本歷史管理：對於工程邏輯、控制程式與設備設定保留歷史版本，以利在故障排除或事故調查時進行版本差異比較。
- 持續改善管理品質：透過分析變更紀錄與事故之關聯，定期檢討並調整變更審核標準，強化組態管理的嚴謹度。

第十一節、 組織管理

組織管理涵蓋人員、委外、政策、風險治理與跨部門協作等多個面向，是工控資安能否有效落實的根本。工控系統的安全不僅仰賴技術控制，更

依賴組織是否有能力建立並維持一套清楚、一致且可執行的管理制度。

5.11.1 政策制定與人員資安規範

- 制定明確資安政策：建立正式的工控資安政策與作業程序，定義組織目標、角色分工、人員行為規範與防護要求，並落實教育訓練。
- 實施背景審查：針對涉及 CI 相關工作的員工與承包商，依職務敏感度實施適當的背景審查與定期複核，降低內部不當行為風險。
- 落實違規處理機制：明定例外管理與違反資安規範的處理機制，確保管理制度具備執行力。

5.11.2 委外管理與廠商監督

- 合約納入資安責任：於合約中明確界定原廠、SI 與維運廠商的資安責任，包含遵守組織安全政策、保密義務、存取規範及弱點通報時限。
- 強化作業管控機制：建立廠商作業前的申請核准、作業期間的現場監督，以及作業後的檢討紀錄，確保外部活動符合既定資安流程。

5.11.3 風險治理與資源配置

- 建立定期風險評估：整合技術、營運與供應鏈風險，建立定期評估機制，並隨系統變更與威脅情勢動態調整。

5.11.4 事件應變與通報協作

- 建立跨部門應變流程：整合工務、資安、營運與管理單位，建立跨部門處理流程，確保在事件發生時能迅速協調與執行損害控制。
- 落實法規通報義務：事件通報流程銜接各中央目的事業主管機關要求，確保在法定時限內完成通報，並提供事後調查與改善報告。

- 持續最佳化應變能力：透過定期演練與事後檢討，最佳化協作流程並減少未來事故對營運與安全的衝擊。

第十二節、　責任分工

工控系統之資安防護無法由單一單位獨立完成，必須由 AO、SI、SM 及 PS 於系統全生命週期中共同協作。為確保本專章前述各項防護建議得以有效落實，各方責任分工界定如下。

AO 即 CI 提供者或營運單位，為工控系統之最終責任承擔者（Accountable）。其核心職責在於決策與治理，包括制定資安政策、核定防護基準、定義可接受風險水準，並編列預算支持資安計畫。在採購階段，AO 須向廠商提出明確資安規格，如 SBOM 與加密需求，並主導系統驗收作業。在日常營運中，AO 須負責高權限帳號的審查、主導 BCP 演練，並在發生資安事件時負責最終的通報與應變決策。

SI 負責將軟硬體組件整合、組態並建置為運作系統。SI 的主要職責在於落實安全設計，須依據 AO 之需求規劃網路分層分區架構，並實踐最小權限原則。此外，在系統交付前，SI 必須執行組態強化作業，關閉不必要之服務與連接埠，確保預設帳號密碼已變更，並於驗收時移交完整的系統文件與架構圖，確保系統以安全狀態上線。

SM 負責系統上線後之定期維護、保養、駐點或遠端支援，此角色可能由內部維運團隊或外部委外廠商擔任。SM 的職責側重於維護執行與合規作業，包括執行系統更新、弱點修補程式測試與派送，以及防毒病毒碼更新。若需進行遠端維護，SM 必須嚴格遵守遠端存取規範，使用跳板機與多因子驗證進行連線，並配合 AO 執行日誌紀錄保存與異常監控，確保維運過程不構成安全破口。

PS 為提供工控軟硬體設備（如 PLC、HMI、SCADA 軟體）之原廠或製造商。其職責在於確保產品遵循 SSDLC，使產品在出廠時即具備身份鑑別、加密與日誌記錄等原生安全功能（Security by Design）。在產品生命週

期內，PS 亦須負責弱點管理，主動發布安全公告、提供修補程式或緩解措施，並提供 SBOM 以協助識別潛在供應鏈風險。

為明確界定前述各章節防護措施之執行權責，茲制定責任分工矩陣如下表。表中 A（Accountable）代表對任務負最終成敗責任之當責者，擁有核決權；R(Responsible)為實際執行任務或操作系統之執行者；C(Consulted)為提供專業建議、技術支援或產品功能之諮詢支援者；I（Informed）則為任務完成後需被通知之對象。

表 4、工控系統資安防護責任分工表

章節	防護面向	具體工作項目範例	資產擁有者	系統整合商	服務維護商	產品供應商
第一節	工控系統網路架構	5.1.1 網路分層分區規劃	A	R	I	C
第二節	存取控制	5.2.1 帳號管理與權限配置	A	I	I	-
		5.2.3 遠端存取與跳板系統管理	A	I	R	-
第三節	事件日誌與可歸責性	5.3.1 日誌紀錄範疇與保存	A	-	C	-
		5.3.3 事件調查與持續改善	A	C	R	R
第四節	營運持續計畫	5.4.1 備援架構與相依性評估	A/R	I	C	-
		5.4.2 安全模式與保護機制	A	C	R	-
第五節	識別與鑑別	5.5.1 使用者身分識別與追蹤	A	C	R	-
		5.5.2 高風險操作之進階鑑別	A	-	-	R

章節	防護面向	具體工作項目範例	資產擁有者	系統整合商	服務維護商	產品供應商
第六節	系統與通訊防護	5.6.1 通訊完整性與通道管控	A	R	C	C
第七節	系統與服務獲得	5.7.1 採購規格與供應商管理	A/R	C	C	-
		5.7.2 軟體組成清單與風險評估	A	R	-	R
第八節	實體與環境防護	5.8.1 實體進出管制與現場防護	A/R	I	I	-
第九節	系統與資訊完整性	5.9.1 弱點管理與補償控制	A	I	I	R
		5.9.3 系統監控與異常偵測	A	C	R	C
第十節	組態管理	5.10.1 組態變更程序	A	I	I	-
		5.10.3 變更紀錄與版本追溯	A	C	R	-
第十一節	組織管理	5.11.1 政策制定與人員資安規範	A/R	I	I	-
		5.11.2 委外管理與廠商監督	A	R	R	C

資料來源：本防護建議自行整理

第十三節、 補償性控制措施彙整

在 IACS 環境中，常受限於客觀環境因素而無法落實特定的技術安全要求，例如老舊系統不支援安全性修補程式（Security patches），或組件效能不足以執行數位簽章等密碼學機制。針對此類技術缺口，IEC 62443 定義了「補償性控制措施（Compensating Countermeasures）」，即當組件本身的內建能力無法滿足目標需求時，透過外部的技術或程序手段，以替代或增強的方式來達成安全目標，本章節透過實地考察與應用情境萃取，條列出多項可供參照的補償性對策，以協助使用單位填補安全落差。

必須釐清的實務誤區：部分單位認為「封閉網路（Air-gapped network）」環境即可免除特定安全基準的適用性。事實上，封閉環境僅是降低了外部攻擊的可能性（likelihood），若因此完全放棄安全性配置，將使系統對內部攻擊（Inside attack）毫無抵抗力。根據標準，即使是 SL 1 等級也僅能防範「無意」的行為，若要抵禦具備動機的故意違反，仍需透過補償性措施（如強化實體安全控制或人事管理流程）來降低殘餘風險。任何安全性要求的排除，都必須基於風險評估提供完整的道理依據（rationale），並確保整體防禦深度（Defense in Depth）依然有效。

下表綜整本章之補償性控制措施，提供參閱。

表 5、補償性控制措施

段落與要求	要求與補償性控制措施
第一節 工控系統網路架構	
• 5.1.1 網路分層分區規劃 ○ 建立明確的分層與分區，將企業管理區、營運管理區、控制區與現場區分開，確保不同類型的系統不共享同一安全邏輯。	• 由資安與營運單位共同完成網路風險評估及分區藍圖，並制定短中長期改善計畫及完成時程。 • 以路由存取控制清單，防火牆過濾或交換器存取控制限制跨子網通訊，僅允許必要之協定來源目的與方向。 • 禁止企業網路直接接觸控制核心，必要通訊須經 DMZ 或跳板設備。 • 加強未分區網段之流量監測與紀錄以縮短事件偵測時間。
○ 透過分區隔離，避免低風險區域的威脅立即影響到高風險或高敏感的核心控制系統。	無。
○ 工控設備在可能情況下不宜直接接觸網際網路，以降低受攻擊之風險。	無。

段落與要求	要求與補償性控制措施
• 5.1.2 通訊通道管制 ○ 跨區通訊須採用白名單機制，嚴格限定來源、目的、協定、封包型態與通訊方向。	無。
○ 區域間之串接須採用受控且具稽核能力的通道，任何未經授權的通訊都必須在邊界即被拒絕。	無。
○ 嚴格執行最小通道原則，僅開放系統運作所必須之連線路徑。	無。
• 5.1.3 中介區與維運管理 ○ 歷程資料伺服器、監控伺服器與需要跨區提供資料的應用程式，宜置放於DMZ,避免機敏資訊系統直接接觸工控控制核心。	無。
○ 必要的更新與維運通道透過分段式與跳板式設計管理，確保外部來源無法直接接觸控制系統。	無。
• 5.1.4 即時性保障與快速隔離能力 ○ 網路架構設計須避免不當的流量阻斷、延遲或丟封包，以防止系統錯誤動作或設備失效。	無。
○ 系統宜支援快速隔離功能，當偵測到異常流量、惡意封包或橫向擴散跡象時，能立即切斷特定區段或封鎖部分通道。	無。
○ 強化事故損害控制能力,確保CI在事故發生時能降低影響範圍並維持連續運作。	無。
第二節 存取控制	
• 5.2.1 帳號管理與權限配置 ○ 落實個別化帳號：所有工控系統	• 所有工控系統與使用者宜要求採用個別化帳號以避免責任模糊，如無法使

段落與要求	要求與補償性控制措施
宜要求採用個別化帳號以避免責任模糊。若因特殊場景須使用共用帳號，必須搭配排班紀錄、影像監控或工單系統，以確保操作之可追溯性。	用個別化帳號，可採下列補償性控制措施： ○ 排班紀錄。 ○ 錄影監控紀錄。 ○ 門禁管制。 ○ 工單紀錄。
○ 明確區分職能權限：工程人員、維運人員、管理者與外部廠商均需配置不同帳號與權限，禁止以高於必要等級的權限執行日常操作，確保符合最小權限原則。	• 若無法落實最小化權限，可採以下補償性控制措施： ○ 強化日誌紀錄或監控。 ○ 加強補償性網路隔離。
• 5.2.2 高風險操作與授權機制 ○ 多階段核准流程：針對程式下載、可程式化邏輯控制器（PLC）組態變更、保護邏輯修改、系統重啟或模式切換等高風險操作，宜採取二階段核准、獨立人員覆核或多因子鑑別。	無。
○ 限時授權管理：任何短期、例外或高敏感度操作，宜採用一次性身份識別或限時授權方式，避免高權限帳號因長期暴露而導致安全漏洞。	• 若因工控系統技術限制無法實作者，可採下列補償性控制措施： ○ 工單紀錄。 ○ 人工多因子驗證。 ○ 事後覆核機制。
• 5.2.3 遠端存取與跳板系統管理 ○ 強制跳板存取：遠端存取透過跳板系統強制進入，嚴禁直接連線至控制伺服器或工程工作站，以防止攻擊者繞過現場防護措施。	無。
○ 強化事件日誌與監控：跳板系統宜具備完整記錄操作軌跡、限制執行命令及強制多因子鑑別之	無。

段落與要求	要求與補償性控制措施
功能，以利事後稽核與風險控管。	
○ 結合工單流程：遠端存取宜與工單流程連動，確保所有授權、操作與紀錄一致，防止未經許可的協力廠商操作或不當維運行為。	無。
第三節 事件日誌與可歸責性	
• 5.3.1 日誌紀錄範疇與保存 ○ 完整記錄操作行為：日誌紀錄宜包含身分識別、登入與登出、組態修改、控制邏輯下載、參數調整、權限變更、系統警示、設備異常及模式切換等資訊。	無。
○ 確保資料完整性：日誌資料的格式應考量現場系統可行性，並採取保護措施，確保紀錄不被未授權篡改或刪除。	無。
○ 集中管理與分析：日誌紀錄宜透過集中管理方式保存，以支援長期的事件分析與資安稽核需求。	無。
• 5.3.2 異常偵測與即時告警 ○ 建立告警機制：當偵測到登入失敗、權限升級、非預期的程式下載或異常流量時，宜能即時產生告警並通知相關人員。	無。
○ 強化早期預警能力：透過即時告警機制，使 CI 提供者能在攻擊造成實質損害前，及早採取行動處置，降低營運風險。	無。
• 5.3.3 事件調查與持續改善 ○ 支援事故溯源：日誌資料需與事	無。

段落與要求	要求與補償性控制措施
件調查流程結合，確保在事故發生後能釐清操作責任歸屬與事實真相。	
○ 最佳化營運管理：透過日誌紀錄的檢視，分析事故原因以避免重複性錯誤，並作為最佳化安全防護政策之依據。	無。
第四節 營運持續計劃	
• 5.4.1 備援架構與相依性評估 ○ 明確界定運作需求:CI 提供者需定義各控制系統的最低運作需求、系統間相依性與可接受的中斷時間。	CI 之 BCP 為確保業務不中斷，可透過人工方式（如：人工醫療行為、人工開票作業、人工備品切換機制、轉院機制…等），以達業務不中斷目的。
○ 建立多元備援機制：依據評估結果建立備援架構，包含冗餘伺服器、同步資料庫、替代通訊路徑及自動切換機制，確保單點故障不致影響整體流程。	無。
• 5.4.2 安全模式與保護機制 ○ 具備安全模式能力：控制系統在偵測到異常或進入不可信任狀態時，宜能進入限制性操作模式、保護性停機或僅保留基本監控能力。	無。
○ 防止事故擴大：透過系統安全模式的切換，避免設備受損、流程失控或對人員安全造成威脅。	無。
• 5.4.3 定期演練與應變協作 ○ 實施多情境演練：定期進行包含系統故障、惡意攻擊與通訊隔離等情境的演練，以驗證技術防護	無。

段落與要求	要求與補償性控制措施
與應變流程之有效性。	
○ 強化通報與跨部門協調：演練宜涵蓋人員判斷流程、跨部門溝通，以及與各中央目的事業主管機關的通報協作。	無。
○ 提升回應效率：透過演練確保在緊急情況下能快速回應，將事故影響範圍與損害降至最低。	無。
第五節 識別與鑑別	
• 5.5.1 使用者身分識別與追蹤 ○ 具備唯一身分識別：所有使用者具備唯一帳號，確保其操作行為能與具體個人產生關聯，落實操作責任歸屬。	• 所有工控系統與使用者採用個別化帳號以避免責任模糊，如使用共用帳號，可採下列補償性控制措施： ○ 排班紀錄。 ○ 錄影監控紀錄。 ○ 門禁管制。 ○ 工單紀錄。 • 現場操作需配合錄影監控與門禁紀錄。 • 針對控制邏輯與組態變更，由操作人簽認並由第二人員覆核。 • 將風險列入風險評估紀錄，並訂定系統更新或功能補強時程。
○ 輔助管控機制：針對技術限制無法支援個人帳號的舊型系統或場景，宜透過門禁管控、錄影監視、工單系統或排班制度進行輔助，以維持操作的可歸屬性。	無。
• 5.5.2 高風險操作之進階鑑別 ○ 採取多重身分鑑別：針對工程邏輯修改、保護參數變更或緊急停機程序等高風險操作，宜採取多	無。

段落與要求	要求與補償性控制措施
因子鑑別或第二階段確認機制。	
○ 防止身分濫用：透過加強鑑別機制，防止單一身分因洩漏、被濫用或遭冒用而導致嚴重的系統性風險。	無。
• 5.5.3 設備識別與連線管控 ○ 禁止匿名裝置連線：工控環境宜嚴禁匿名或未經註冊的裝置連線，避免不明設備成為資安破口。	無。
○ 實施設備白名單機制：宜透過裝置指紋、白名單或可驗證之硬體識別機制，確保僅有經核准且受信任的授權設備能參與系統通訊。	無。
第六節 系統與通訊防護	
• 5.6.1 通訊完整性與通道管控 ○ 強化通訊完整性保護：針對控制指令與傳輸資料進行完整性驗證，避免通訊內容遭到惡意竄改，確保實體設備執行之指令準確無誤。	• 於無法立即導入加密或強鑑別之老舊設備或協定，建議採下列措施： ○ 限定通訊僅經由專用通道，並僅允許必要來源目的及方向。 ○ 考量採用單向閘道或資料中介避免雙向控制風險。 ○ 強化協定異常與流量基準線監測。 ○ 訂定設備汰換或協定升級時程，並納入風險評估。
○ 跨區域通訊檢查：跨區域之資料交換須透過受控通道傳輸，並對通訊協定、控制指令及網路封包進行深度檢查，確保通訊過程安全可靠。	無。
• 5.6.2 關鍵資料儲存與完整性保護	無。

段落與要求	要求與補償性控制措施
○ 確保儲存資料不可竄改：關鍵資料如稽核日誌、歷史紀錄與安全參數，其儲存方式確保不被未授權刪除或竄改，必要時採取唯讀儲存或數位簽章驗證。	
○ 強化備份資料安全性：儲存的備份檔案進行完整性驗證，確保在系統復原時，所使用的資料是完整且未經更動的。	無。
• 5.6.3 系統異動與變更管理 ○ 落實版本控制與驗證：針對組態檔、控制邏輯、工程程式與安全參數等核心資料，建立版本控制機制與完整性驗證程序。	無。
○ 建立詳盡變更紀錄：所有系統異動皆記錄並可供追蹤，確保任何變更都能被檢視，並在發生異常時能迅速復原至已知安全狀態。	無。
• 5.6.4 異常偵測與即時應變 ○ 部署偵測與監控能力：系統宜具備偵測異常封包、可疑登入或未經授權操作之能力，並在發現異常時立即產生告警。	無。
○ 快速介入與調查：透過即時告警機制，使 CI 提供者能迅速介入處理，並針對資安事件進行後續調查，以防範危害擴大。	無。
第七節 系統與服務獲得	
• 5.7.1 採購規格與供應商管理 ○ 明確資安規格要求：要求供應商說明產品在身分鑑別、存取控	需求規格書（Request of Proposal，RFP）之資安規格要求，可依循國際規範設立。

段落與要求	要求與補償性控制措施
制、日誌紀錄、通訊保護與組態管理所具備的功能，並確認其遵循安全開發流程與測試程序。	
○ 建立弱點處理機制：要求供應商建立正式的弱點通報與修補流程，包含預期的修補發布時程、支援期間與通報管道，以便安排適當的導入時機。	無。
○ 控管遠端維運安全：針對具備遠端維運功能的設備與服務，供應商須說明遠端存取的安全機制與審核流程，避免未受控的通道長期存在。	無。
• 5.7.2 軟體組成清單與風險評估 ○ 提供 SBOM：針對以軟體為核心的控制系統與平台，要求供應商提供 SBOM，並隨版本更新維持其完整性與即時性，以支撐弱點管理與風險評估。	• 當系統或設備無法取得 SBOM，或 SBOM 資訊不完整時，可採行下列補償性控制措施，以支援弱點識別與風險評估，並降低弱點遭利用之風險： ○ 建立資產版本基線與可追溯清單。 ○ 要求供應商提供產品安全公告（Security Advisory）與弱點通報機制。 ○ 定期依據供應商公告或公開弱點資料庫（如 CVE、ICS advisory）進行風險評估。 ○ 建立設備韌體版本、作業系統類型、主要服務與通訊元件等基線清單，並於更新、汰換或重大變更後同步修訂，作為弱點比對與影響範圍判定之依據。 ○ 要求供應商提供等效軟體組成資訊或安全公告。

段落與要求	要求與補償性控制措施
• 5.7.3 外部服務與委外管理 ○ 查核資安管理制度：確認雲端平台、遠端監測、系統託管與維運外包服務商是否建立資安管理制度，並具備事件通報與應變能力。	無。
○ 明確責任與稽核權利：界定資料主體與資安責任歸屬，並要求供應商提供稽核報告或安全評估結果，避免責任模糊。	無。
○ 資料備援與可攜性：針對存放關鍵設定或歷程資料的外部平台，需確認資料備援機制，避免因服務終止或供應商問題導致營運風險。	無。
• 5.7.4 系統文件與技術資料管理 ○ 建立文件管理體系：確保所有工控設備均有完整的設計文件、組態紀錄、版本資訊與維護紀錄，作為風險評估與變更管理的依據。	無。
○ 原始程式碼與技術交接：針對委外開發與客製系統，要求保存原始程式碼、建置文件與測試報告並進行交接，防止未來無法維護或安全性難以評估的情形。	無。
○ 確保維運連續性：透過完善的文件制度，防止關鍵技術資訊過度依賴特定個人或單一廠商，確保在設備故障或人員異動時，相關人員仍能依循技術文件維持系	無。

段落與要求	要求與補償性控制措施
統運作，避免營運中斷風險。	
第八節 實體與環境防護	
• 5.8.1 實體進出管制與現場防護 ○ 強化區域進出控管：機房、控制室與通訊機櫃採用門禁管制或監視措施，並完整保留人員進出紀錄。	• 既有建物因結構限制短期內無法改建時，得採下列措施： ○ 使用上鎖機櫃或封閉式設備箱限制接觸。 ○ 設置監視錄影涵蓋所有設備操作區域。 ○ 設置訪客與承包商登記制度並要求全程陪同。 ○ 加強巡檢並評估可行之小型工程改善及期限。
○ 落實設備實體保護：針對現場機櫃與設備，採取加鎖、防拆封條或封閉式櫃體等實體隔離方式，降低遭觸碰或竄改之機率。	無。
○ 訪客與承包商監督：外部人員進入敏感區域須事先申請與核准，作業期間由內部權責人員全程陪同，並詳實記錄作業內容、時間與使用工具。	無。
• 5.8.2 環境條件監控與電力保障 ○ 確保電力穩定供應：關鍵設備配備不斷電系統與備用發電設備，並制定電力異常時的自動保護策略，確保運作不因電力中斷而失控。	無。
○ 維持適當溫濕度：空調與通風系統維持在設備設計規範之環境範圍內，避免過熱或水氣凝結，並定期進行濾網與風道維護檢	無。

段落與要求	要求與補償性控制措施
查。	
• 5.8.3 環境災害評估與預防工程 ○ 實施環境風險評估：針對易受水災、土石流或其他自然災害影響之設施，及早採取抬高設備位置、設置防水門或導水溝等預防性工程。	無。
○ 建立環境監測機制：針對高風險區域設置水位監測或坡面穩定監控等相關監控機制，確保在災害發生前能採取應變行動。	無。
第九節 系統與資訊完整性	
• 5.9.1 弱點管理與補償控制 ○ 建立弱點追蹤流程：定期追蹤供應商與權威機構發布之弱點通報與修補資訊，並依據系統重要性評估修補的必要性與執行時機。	• 當短期內無法修補弱點時，可透過加強網路區隔、限制存取來源、強化監測與縮減可執行功能等補償控制方式，降低弱點被利用的可能性。 • 資源受限或封閉式設備，則可採取白名單、檔案完整性監控或啟動檔案檢查等方式。
○ 落實修補驗證：更新前需先於測試環境驗證，並在可控的維護時段執行，以避免停機或不相容之風險。	無。
○ 實施補償控制措施：對於短期內無法修補的弱點，透過加強網路區隔、限制存取來源、強化監測與縮減功能等方式，降低弱點被利用的可能性。	無。
○ 利用 SBOM：結合系統與設備之 SBOM，快速識別受特定弱點影響之元件，提高修補與防護決策	• 當系統或設備無法取得 SBOM，或 SBOM 資訊不完整時，可採行下列補償性控制措施，以支援弱點識別與風

段落與要求	要求與補償性控制措施
之準確性。	險評估，並降低弱點遭利用之風險： ○ 建立資產版本基線與可追溯清單。 ○ 要求供應商提供產品安全公告（Security Advisory）與弱點通報機制。 ○ 定期依據供應商公告或公開弱點資料庫（如 CVE、ICS advisory）進行風險評估。 ○ 建立設備韌體版本、作業系統類型、主要服務與通訊元件等基線清單，並於更新、汰換或重大變更後同步修訂，作為弱點比對與影響範圍判定之依據。 ○ 要求供應商提供等效軟體組成資訊或安全公告。
• 5.9.2 惡意程式防護策略 ○ 部署合適防護工具：針對使用通用作業系統之工作站與監控伺服器，部署經嚴格測試之防護工具，並設定不影響即時運作的掃描策略。	無。
○ 採取多重防護機制：對於資源受限之設備，可採取白名單、檔案完整性監控或啟動檔案檢查等替代方式。	無。
○ 管控外部傳輸媒介：對可攜式媒體（如隨身碟）、維護用攜帶設備與外部檔案建立強制檢查要求，防止惡意程式透過實體媒介竄入。	無。
• 5.9.3 系統監控與異常偵測	無。

段落與要求	要求與補償性控制措施
○ 建立行為基準線：定期定義正常流量範圍、登入模式、控制指令頻率與設備回應特徵，並對超出基準線之行為發出警示。	
○ 即時調查異常行為：當偵測到未知通訊對象、頻繁登入失敗或未預期指令時，立即通知人員介入調查，降低攻擊潛伏風險。	無。
○ 強化變更管控：針對控制邏輯、組態檔與歷程資料採用版本控管與完整性驗證，確保異動皆有跡可循，並能在必要時回復至已知安全狀態。	無。
第十節 組態管理	
• 5.10.1 組態變更程序 ○ 建立標準變更流程：變更流程包含需求提出、風險評估、測試驗證、核准、實施與回復方案等完整步驟。	• 短期內無法建立測試環境或版本管理工具時，可採取下列措施： ○ 變更前完整備份並確認可還原。 ○ 於最小影響時段執行變更，並由人員現場監看。 ○ 以人工方式記錄變更內容、時間、執行人與核准人。 ○ 高風險變更採兩人以上交叉檢視。 ○ 補償性措施僅作為過渡安排，不得長期替代正式組態管理制度。
○ 強化重大變更審查：凡涉及控制邏輯、保護機制或系統架構之重大變更，實施前須由權責單位共同審查其對安全與資安之影響。	無。
○ 落實測試與回復演練：關鍵變更先於測試環境演練，並確保變更失敗時具備迅速復原原始組態	無。

段落與要求	要求與補償性控制措施
的能力。	
○ 選擇適當實施時機：變更安排於影響最小的維修時段，並由專人現場監控，以便在異常發生時即時介入。	無。
• 5.10.2 最小功能原則與攻擊面縮減 ○ 僅啟用必要服務：遵循最小功能原則，關閉所有未使用或非必要的通訊埠、服務與應用程式，以縮減潛在攻擊面。	無。
○ 實施程式執行控管：針對可執行程式與腳本，採取白名單機制，確保僅有經核准的程式能於系統上啟動，防止未知程式運作。	無。
• 5.10.3 變更紀錄與版本追溯 ○ 詳實記錄變更軌跡：變更紀錄完整涵蓋內容、時間、執行人員、原因與核准人，確保所有異動均有跡可循。	無。
○ 落實版本歷史管理：對於工程邏輯、控制程式與設備設定保留歷史版本，以利在故障排除或事故調查時進行版本差異比較。	無。
○ 持續改善管理品質：透過分析變更紀錄與事故之關聯，定期檢討並調整變更審核標準，強化組態管理的嚴謹度。	無。
第十一節 組織管理	
• 5.11.1 政策制定與人員資安規範 ○ 制定明確資安政策：建立正式的工控資安政策與作業程序，定義	無。

段落與要求	要求與補償性控制措施
組織目標、角色分工、人員行為規範與防護要求，並落實教育訓練。	
○ 實施背景審查：針對涉及 CI 相關工作的員工與承包商，依職務敏感度實施適當的背景審查與定期複核，降低內部不當行為風險。	無。
○ 落實違規處理機制：明定例外管理與違反資安規範的處理機制，確保管理制度具備執行力。	無。
• 5.11.2 委外管理與廠商監督 ○ 合約納入資安責任：於合約中明確界定原廠、SI 與維運廠商的資安責任，包含遵守組織安全政策、保密義務、存取規範及弱點通報時限。	無。
○ 強化作業管控機制：建立廠商作業前的申請核准、作業期間的現場監督，以及作業後的檢討紀錄，確保外部活動符合既定資安流程。	無。
• 5.11.3 風險治理與資源配置 ○ 建立定期風險評估：整合技術、營運與供應鏈風險，建立定期評估機制，並隨系統變更與威脅情勢動態調整。	無。
• 5.11.4 事件應變與通報協作 ○ 建立跨部門應變流程：整合工務、資安、營運與管理單位，建立跨部門處理流程，確保在事件	無。

段落與要求	要求與補償性控制措施
發生時能迅速協調與執行損害控制。	
○ 落實法規通報義務：事件通報流程銜接各中央目的事業主管機關要求，確保在法定時限內完成通報，並提供事後調查與改善報告。	無。
○ 持續最佳化應變能力：透過定期演練與事後檢討，最佳化協作流程並減少未來事故對營運與安全的衝擊。	無。

資料來源：本防護建議自行整理

第十四節、 情境判定決策樹

決策樹（Decision Tree）方法係參考國際標準 EN 18031 所採用之風險導向判定機制。其最大優點在於，當各領域專家對資安技術細節不熟悉時，仍可依循明確且結構化的判定流程，完成適當之資安控制措施選擇與補償性控制措施配置。本防護建議所設計之決策樹，將確保每一條分支所導向之補償性控制措施，皆為主管機關認定具同等風險緩解效力（equivalent risk mitigation effect）之方案，避免因技術限制而產生無法合規之困境。

圖 2、決策樹設計步驟

資料來源：本防護建議自行整理

一個決策樹如何設計？設計決策樹並非直接列出控制措施，而應遵循

下列步驟：

1. 風險識別：該情境欲緩解的核心風險為何(例如：未授權控制指令、資料竄改、服務中斷、時間同步失準等）？風險發生條件與影響後果為何？是否屬於高即時性／高安全性要求之場域？
2. 控制措施識別：針對該風險，識別出理想情況下的標準控制措施（例如：通訊加密、身份驗證、內聯 IPS、網路分區等），這一步的思維邏輯是「若無限制條件，最佳實務應該是什麼？」。
3. 運用情境限制識別：識別出現場可能無法直接採用主要控制措施的原因，例如：即時性與抖動限制、協定不支援加密、舊型設備效能不足、法規或供應商限制、營運不中斷要求、這一步決定決策樹的分支條件。
4. 補償性控制措施識別：當主要控制措施不可行時，識別出具等效風險緩解效果的替代方案，例如：改為白名單搭配被動監測、閘道包裹（Gateway wrapping）、改為物理分區隔離、改為強化變更管理與雙人覆核，這些措施需經主管機關確認其風險緩解效力與原控制措施相當。
5. 決策邏輯排列：最終決策樹之排列順序為風險類型、情境判定條件、是否適用主要控制、若否、等效補償措施，而非單純依「控制措施優先順序」排列。

為了讓讀者更易於使用決策樹此工具，本防護建議提供以下幾個決策樹範例供參考：

- 安全性修補程式：

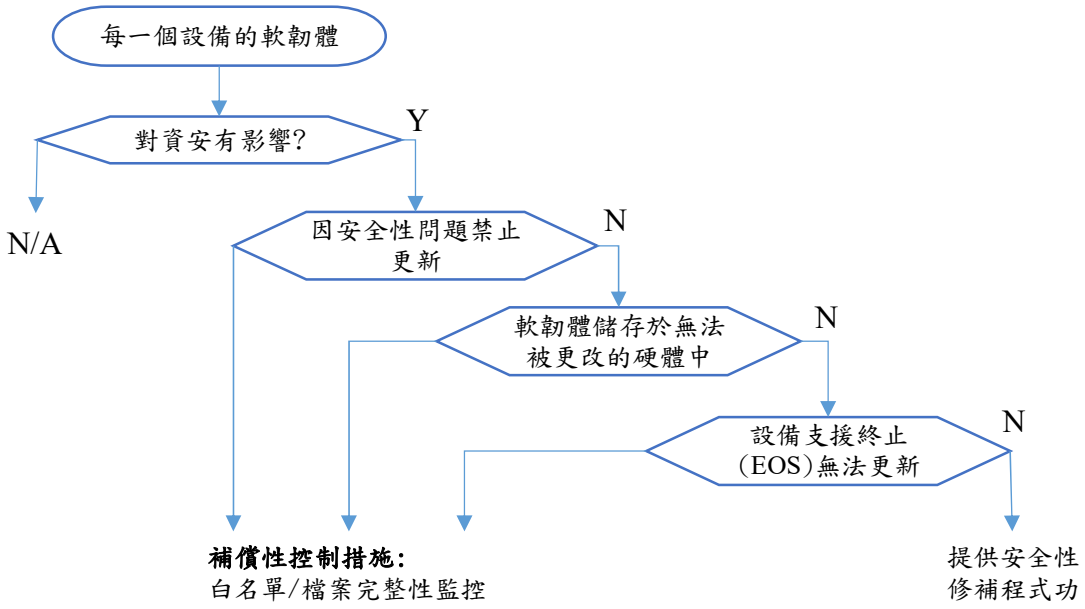

圖 3、安全性修補程式功能決策樹

資料來源：本防護建議自行整理

- 通訊加密：

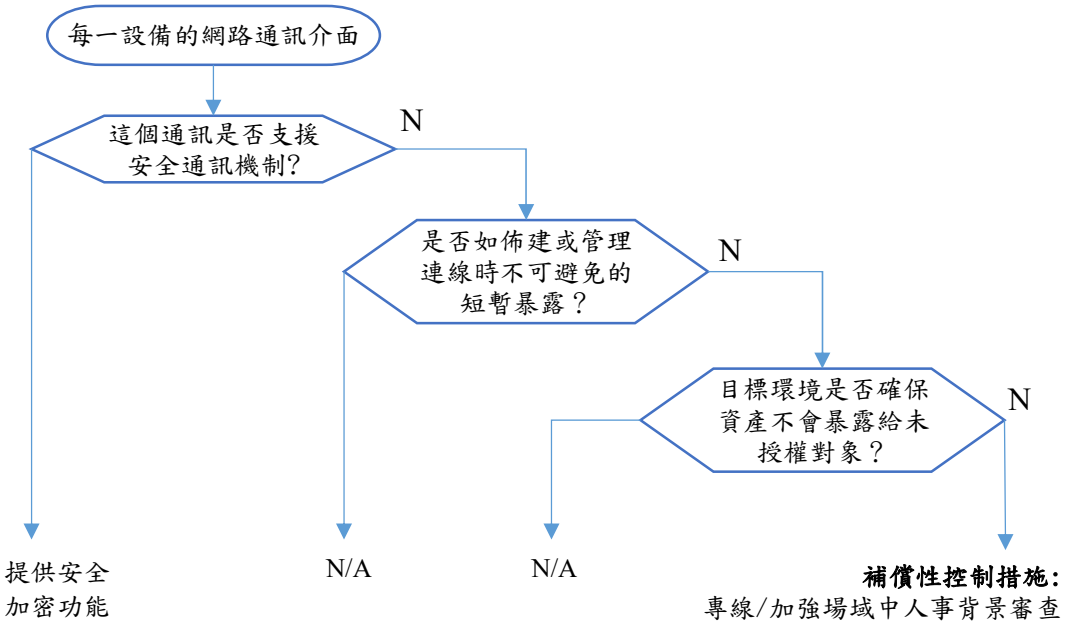

圖 4、傳輸加密功能決策樹

資料來源：本防護建議自行整理

- 漏洞管理作業：

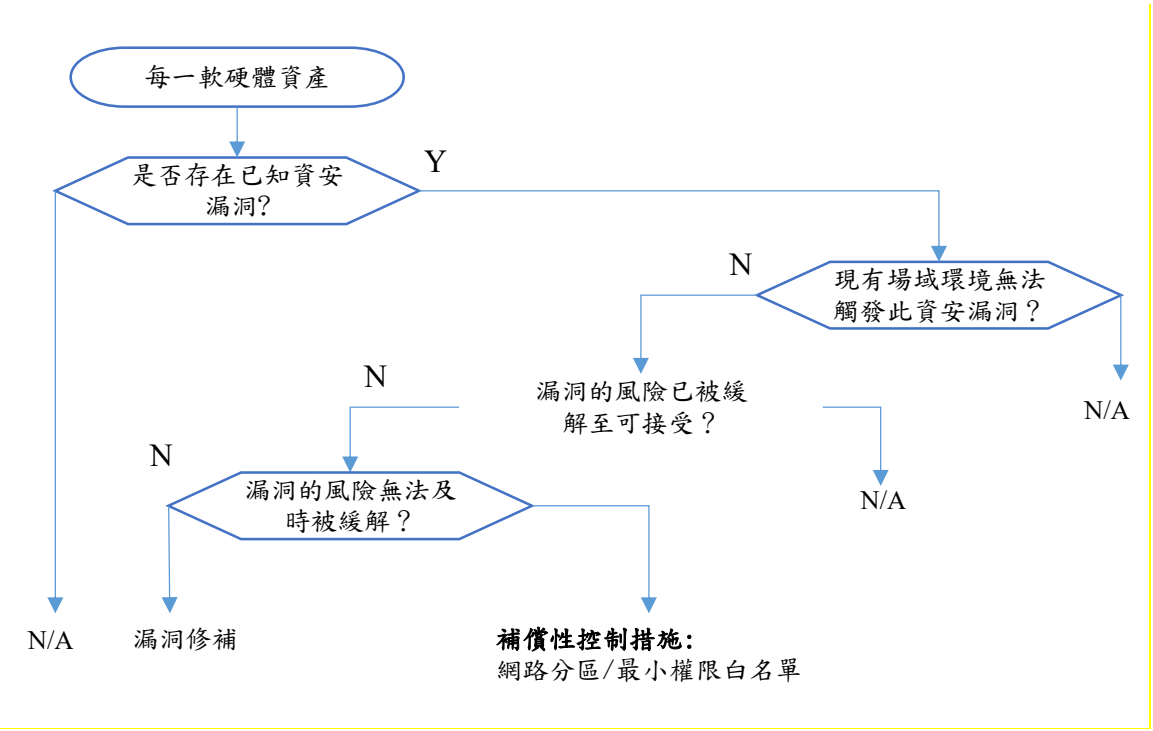

圖 5、漏洞管理作業程序決策樹

資料來源：本防護建議自行整理

由於決策樹係基於既有風險情境與控制措施所設計，在制定階段難以完全識別所有實際使用情境與技術變化，因此必然存在未涵蓋或未預期之情境。若過度僵化地依循決策樹進行判定，可能導致部分場域業者利用未涵蓋之情境作為規避基準之理由，反而削弱整體防護水準。

因此，決策樹被定位為輔助判定工具，而非限制性合規邊界。其主要功能在於協助資安成熟度較低或對技術細節掌握有限之領域，在初期導入防護基準時能有結構化判斷依循，降低誤判與錯配風險。

隨著各領域資安治理能力與實務經驗逐步成熟，防護措施之選擇回歸風險評估導向原則，而非僅依決策樹所列舉之分支進行最低限度合規。換言之，當場域已具備足夠能力辨識與評估風險時，不宜將決策樹作為限制控制措施升級或強化之依據，而應鼓勵採取高於基準之適當防護作為。

第六章、 防護建議實施參考

本章針對前述各項工控資安防護建議，在實際落實層面提出具體的實施參考，協助各中央目的事業主管機關與 CI 提供者在現有制度、技術能力與資源條件下，逐步提升 CII 在工控資安上的成熟度。整體思維與國際實務相符，一方面承接 ISA/IEC 62443 對安全計畫、流程與角色責任的要求，一方面參考 NIST SP 800-82 對工控落實步驟與優先順序的建議，將治理、技術與人員三個面向串接為具體可行的推動路徑。

第一節、 治理與責任分工

在治理層面，工控資安必須從組織最高層級獲得明確的承諾與授權，否則所有防護措施將流於零散與短期。國際經驗顯示，若缺乏明確的角色與責任界定，即使導入了許多技術工具，仍無法形成穩定的安全能力。ISA/IEC 62443 特別強調「安全計畫」與「安全管理系統」的建置，指出 AO 必須明確界定誰負責制定資安政策、誰負責營運管理、誰負責技術落實以及誰負責監督與持續改善。NIST SP 800-82 在導入策略上亦強調，高階管理階層必須將工控資安視為整體風險管理的一部分，而非單純的 IT 技術議題。

在我國 CII 環境中，AO 往往即為 CI 提供者本身，是對整體系統安全負最終責任的單位。CI 提供者在組織內正式指派負責工控資安的主管職務，使其在投資決策、人力配置、制度設計與重大變更核准等議題上具備實際決策權。不僅如此，該主管需定期聽取關於 CII 資安風險、事件狀況、弱點管理進度與供應鏈風險的報告，並將這些資訊納入內部風險委員會或管理會議，使工控資安與營運、財務、法遵與公共形象得以連動考量。

工控資安治理亦需明確界定 SI、SM 與 PS 在安全管理中的角色。SI 在規劃與建置階段負責將安全需求轉化為架構與實作方案，對分層分區設計、控制邏輯部署與安全機制整合負有實際責任。SM 在系統營運期間負責日常維護、異常排除與更新作業，必須遵守組織既定的變更管理與事件通報

流程，並避免以維運之名繞過安全控制。PS 則需提供具備安全能力的設備與軟體，並依據 ISA/IEC 62443 所要求的 SSDLC 流程提供弱點通報與更新支援，以確保系統在生命週期內持續具備可維護的安全性。

工控資安治理需要跨部門協調機制。資訊、工務、營運、採購與風險管理等單位本來各自關注不同議題，但在 ICS 與 OT 情境下，彼此的決策與行為會直接影響整體安全。例如採購若未將資安需求寫入規格，後續整合商、維護商與資安團隊將長期承受風險；現場施工與設備汰換若未依安全程序進行，將可能破壞既有架構與合規狀況。因此，AO 建立常設的工控資安治理機制或專責委員會，讓相關部門與外部利害關係人（如關鍵供應商）在政策形成與重大決策時能共同參與，避免單一部門獨自承擔或孤立決策。

各中央目的事業主管機關在治理面扮演外部監督與方向設定角色。依據 CII 分級與責任等級核定結果，各中央目的事業主管機關需制定所屬領域防護基準，明確界定各等級 CII 所需之治理結構、安全計畫與通報機制，並規劃漸進式落實時程。在實務推動上，各中央目的事業主管機關亦應考量不同利害關係人角色，例如要求 AO 就 SI、SM 與 PS 提出安全管理要求，使供應鏈各環節的責任能在制度上被具體化。對於具有跨國或多領域營運性質的組織，各中央目的事業主管機關在查核與輔導時應理解其需同時遵循之國際標準與境外法規，協助其整合多方要求，而非造成互相矛盾或重複負擔的合規壓力。此種作法與 ISA/IEC 62443 所強調的「安全計畫需考量組織環境與外部要求」相符，也呼應 NIST SP 800-82 對「管理層支援與制度整合」的重視。

第二節、 實施路徑與成熟度規劃

工控資安強化過程中，最大的風險之一是試圖在短時間內達成「全面到位」，導致治理架構尚未穩定、現場技術能力尚未成熟、供應商支援尚未跟上，便貿然導入大量控制措施，結果造成資源分散、現場負擔過重或與

既有程式邏輯出現衝突。更合適的方式是參考國際指引所倡議的分階段導入模式，將長期目標拆解為多個可達成的成熟度階段，使 AO、整合商、維護商與供應商能在各自角色下逐步提升安全能力。

在初始階段，AO 與 SI 及主要供應商合作，優先完成資產盤點與網路分區，明確標示出控制系統、營運系統與企業資訊系統的界線，並建立最基本的網路隔離、存取控制與權責分工。此階段的目標是讓組織掌握「有哪些東西、在哪裡、由誰負責」，對大多數 CI 提供者而言，只要能完成這些基礎工作，便已排除相當多顯性的結構性風險。

在中程階段，重點轉向管控變化與掌握風險。AO 建立正式的弱點管理流程與更新策略，SI 與 PS 需提供必要的版本資訊、弱點說明與修補建議，SM 則負責在不影響營運的前提下實施更新與補償控制。此階段應逐步導入事件稽核與集中日誌管理，並針對關鍵區域建立網路流量與設備行為的監測能力，讓 CI 提供者能了解系統的「正常狀態」與「異常徵兆」。同時，針對 AO、SI、SM、PS 不同角色部署相對應的訓練與演練，使技術機制與人員能力同步成長。

在長期階段，組織將風險評估、資安計畫、變更管理、設備生命週期管理與供應鏈安全管理全部納入同一治理框架，形成可持續運作的工控資安管理系統。AO 可以參考國際成熟度模型，結合自身 CII 分級與領域特性，發展適用的工控資安成熟度架構，定期評估不同廠區、系統或組織單位的成熟度狀態。SI 與維護商則需依照成熟度要求調整專案與維運作法，PS 則需依安全等級提供相應支援。成熟度評估結果可用於內部資源配置、外部審查、合作夥伴評估，並可作為各中央目的事業主管機關進行查核與輔導時的參考基礎。

各中央目的事業主管機關在設計輔導與查核機制時，可以以成熟度為導向，不僅關注 CI 提供者是否達到最低防護基準，同時評估其在治理、技術、人員與供應鏈管理上的成熟程度，鼓勵 CI 提供者不僅能「符合基準」，

更能自主提升能力。透過這種以成熟度為導向的實施路徑，AO、SI、SM 與 PS 可以在各自角色上清楚了解應前進的方向，避免只為通過查核而進行短期調整。

第三節、 供應鏈與委外安全管理

供應鏈與委外安全管理是將安全責任從組織內部延伸至整個生態系統的關鍵。ISA/IEC 62443 對服務提供者與元件供應商提出明確要求，指出僅保護系統營運者本身是不足的，必須確保提供設備、軟體與服務的外部單位也具備相對應的安全能力與流程。NIST SP 800-82 亦提示，過往許多工控事件與設備供應商的遠端維運、更新渠道或缺乏安全設計有關。

因此，AO 在規劃系統與服務獲得時，應將資安要求明確嵌入招標文件與技術規格之中，不僅要求功能符合需求，更要求供應商在安全設計、開發流程、弱點管理、更新政策與通報機制上提供透明且可驗證的說明。對於長期維運或關鍵系統，優先考量能證明符合 ISA/IEC 62443 相關部分或具備等效安全開發與服務流程之供應商，以降低供應鏈帶來的整體風險。

工程施工與維運委外契約也需明確規範外部人員在 CII 環境中所應遵守的安全規則。包括只能透過核准通道進行遠端登入、不得擅自攜入未經掃描的媒體、需遵守既定變更流程並完成作業紀錄等。所有委外作業都應與組織的工控資安政策與程序一致，避免外包單位成為規避內部控管的管道。

各中央目的事業主管機關在設計防護基準與查核項目時，宜納入供應鏈安全要求，鼓勵或要求 CI 提供者與所屬供應商共同建立安全責任矩陣，清楚列明各類資產與流程由何人負責安全，並透過文件、稽核或第三方評鑑確認其有效性。這樣的做法可將 ISA/IEC 62443 在供應鏈管理方面的精神自然融入國內制度之中。

第四節、 補償控制與技術限制因應

在工控環境中，技術限制與營運條件常使得理想中的控制措施難以完

全落實。NIST SP 800-82 明確指出，許多現場設備無法立即更新、無法安裝端點防護或無法更換通訊協定，此時若仍強行要求與 IT 相同的防護機制，反而可能增加營運風險或導致系統不穩定。ISA/IEC 62443 亦認可現場技術限制的存在，允許在符合安全條件之下採用補償控制，作為過渡期間的風險管控方式。

為使補償控制的使用具備一致、可追溯且能夠接受查核的程序，CI 提供者應建立標準化的決策流程，以清楚的原則與風險量化邏輯，非個別人員判斷，而是以決策流程決定能否採用補償控制措施。此一流程可視為「補償控制決策樹」的實務化呈現，用於逐步判斷某項控制措施是否能依建議方式落實，或需採取替代方式。

補償控制決策的第一階段，是確認該控制要求是否因技術限制、營運需求或設備相容性問題而無法在短期內實施。若經技術與營運單位共同確認其確實無法依標準要求落實，方可進入第二階段。第二階段是風險評估，需評估該控制措施的缺口對系統造成的可能影響，包括弱點可被利用的路徑、對流程安全的潛在影響、對服務可用性的風險以及是否存在可被攻擊者轉化為危害的操作模式。若風險評估結果顯示該缺口具備一定程度的安全影響，則需進入第三階段，即尋找並設計替代措施。

替代措施的目的，是在無法直接實施原始控制的情況下，透過其他機制的組合來降低風險，使其回到可接受範圍。具體措施可能包括加強網路隔離、限制可連線來源、提高監測頻度、增加存取審核與雙重確認程序、限制高風險操作時段、縮減操作授權、強化通訊解析能力或增加設備端的完整性檢查等。替代措施應以「多層互補」的方式設計，使各補償控制之間相互支持，而非單點依賴。

在補償控制決策樹的第四階段，CI 提供者需判斷替代措施是否能將殘餘風險降至可接受範圍。若替代措施不足以降低風險，則需重新評估是否可調整營運程序、暫停高風險功能或加速設備替換；若替代措施確實能達

成風險控制目標，則可正式將其納入補償控制的紀錄中。

所有補償控制均必須完整文件化，不僅記錄替代措施本身，也需清楚說明原始控制無法實施的理由、風險分析結果、替代措施能降低風險的依據以及殘餘風險的判斷。這些資訊除了供內部治理使用，也將是各中央目的事業主管機關查核時的重要佐證。補償控制不可被視為永久解決方案，而是過渡期間的風險管理手段。因此，CI 提供者應同時提出中長期改善計畫，包括設備更新、系統升級、協定替換或架構調整，以逐步移除補償控制，回到完整符合標準之安全狀態。

各中央目的事業主管機關在查核時，應了解工控現場存在之技術與營運限制，對於經過完整風險評估、具備清楚文件與已證明能有效降低風險的補償控制，予以合理認可。各中央目的事業主管機關亦應要求 CI 提供者定期重新檢視補償控制的有效性與殘餘風險，確保補償措施在環境變化後仍具備必要防護能力。此一作法既尊重工控場域的實務限制，又能維持政策方向與安全目標不被動搖，使工控防護能在現實與合規之間取得平衡。

第五節、 人員訓練與演練

ISA/IEC 62443 在安全計畫與管理要求中，多次強調人員能力與安全文化的重要性，NIST SP 800-82 亦指出許多工控事件源自人員對 OT 系統特性與資安風險認知不足。因此，建構具有工控資安意識與操作能力的人員梯隊，是本防護建議的重要實施面向。

CI 提供者依人員職務性質與接觸系統程度規劃差異性的訓練內容。對高階管理階層而言，訓練重點在於理解 CII 發生資安事件對營運、法規與社會的整體衝擊，以及董事會與經營團隊在資安治理上的責任，讓資安投資決策能建立在充分認知之上。對 OT 與 IT 技術人員的訓練，則需涵蓋工控系統特性、常見攻擊手法、事件徵兆、變更管理流程與補償控制原則，使其能在日常作業中自覺識別並避免高風險行為。對現場操作員與承包商，需強調基本資安行為，例如不任意插入外部媒體、遵守門禁與陪同規定、

依程序通報異常與配合事件調查等。

演練則是將訓練成果實際驗證與強化的過程。工控資安演練不僅限於紙上推演，而須模擬實際場景中可能發生的事件，例如控制室畫面遭竄改、遠端帳號遭濫用、勒索軟體導致歷程資料與工程程式無法使用、或供應商提供的更新包被發現存在異常。演練過程中觀察人員識別事件、啟動通報、進行初步控管與進入營運持續流程的時間與品質，並檢視跨部門協作是否順暢。

演練結束後，組織須進行系統化檢討，記錄成功之處與需要改善的環節，並更新事件應變計畫與相關程序文件。透過不斷重複的訓練與演練，組織得以從單一事件經驗累積成為制度化的應變能力，讓工控資安在面對未知威脅時，仍能維持足夠的反應速度與決策品質。

第七章、 領域應用指引

CI 各領域在應用本防護建議時，如何依照產業特性進行細化與延伸提出參考方向。工控環境在不同產業中具有截然不同的運作模式、風險承受度、流程特性與設備架構，因此建議各中央目的事業主管機關以本防護建議為「共同底線」，並進一步結合各領域實務與技術標準，使防護基準具備產業專屬性、可行性與法規一致性。各領域的應用指引亦需兼顧 ISA/IEC 62443 系列標準的通用控制原則，以及國際上對該領域主要系統安全的專業規範，使 CII 資安防護措施與國際實務能夠相互對齊。

第一節、 能源與水資源領域

本節提供各中央目的事業主管機關與能源、水資源領域之 CI 提供者，依本防護建議建置控制措施的具體方向，使各單位能以一致方式落實資安要求並形成可查核之證據。能源與水資源場域具有跨區域調度、長距離通訊、多數無人站點與高連續性運轉等特性，因此本節之控制重點著重於資產掌握、區域分明、通訊可信度、設備完整性維護與營運不中斷。

一、 分層分區與資產盤點要求

中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章，建立具體且可查核之分層分區文件，並至少達成下列事項：

- 完成企業管理層、營運管理層、控制系統層與現場設備層之架構劃分，並以控制中心、變電所、水廠、加壓站、抽蓄站及無人站為主要單位建立分區圖。
- 建立完整資產清冊，至少記載設備位置、功能、通訊方式、韌體版本、維護責任單位及是否具生命安全影響。
- 資產清冊需每年更新一次，並於新增或調整設備後十日內完成修訂。
- 對於無法更新、原廠不支援或與現行標準不相容的設備，需另行標示並提出補償控制規劃。

中央目的事業主管機關可將分層分區圖、資產清冊與補償控

制規劃列為查核必備文件。

二、 主要通訊路徑與通訊通道的安全要求

能源與水資源領域的跨區域通訊路徑眾多，涉及調度、流量控制、水質監控與現場設備回報，因此需確保通訊內容可控且可追溯。中央目的事業主管機關宜要求 CI 提供者至少落實下列事項：

- 建立正式通訊清冊，涵蓋控制中心至變電所、水廠至加壓站、無人站至監控中心等主要通訊路徑。
- 在主要通訊通道上實施協定白名單、來源白名單與通訊完整性保護，可採用具備內容檢查功能之工控防火牆或受控安全通道。
- 禁止未經授權之跨層通訊，例如現場監控設備直接連接企業管理網路。
- 維運商須透過跳板設備進行，並具備身分確認、日誌紀錄與相關作業紀錄。
- 所有主要控制通訊須具備可追溯之紀錄，紀錄保存期間至少六個月。

中央目的事業主管機關可要求 CI 提供者提交通訊清冊、通道配置文件與維運紀錄，作為查核依據。

三、 控制設備之安全性與完整性維護要求

能源與水資源領域包含保護繼電器、流量控制設備、水質分析儀、變頻器及自動化加壓設備等，因設備生命週期長，不易更新，因此需強化完整性維護。中央目的事業主管機關宜要求 CI 提供者至少建立下列措施：

- 設備之設定檔、韌體、邏輯程式及保護參數需建立版本控管，並定期比對差異。
- 高風險操作需實施雙重確認，包含保護定值變更、調度模式切

換與重大供水量調整。

- 無法安裝端點防護之設備，需以網路層補償控制加強防護，例如強制通訊白名單或外部完整性檢查。
- 所有設定變更需納入正式變更管理程序並保留批准紀錄。
- 對直接影響供電與供水之設備，需建立緊急回復流程與設定檔備援。

中央目的事業主管機關可要求 CI 提供者提交版本控管記錄、變更管理文件及設定差異比對報告，以作為查核依據。

四、 無人站管理、營運持續與補償控制要求

能源與水資源領域具有大量無人站點，中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章，建立可執行且可查核之營運持續與補償控制措施：

- 無人站需具備實體與環境監控，包括門禁、影像、環境感測與電源監控。
- 無法更新之舊型設備需建立補償控制，包括異常行為偵測、流量或電力越限監控與安全降載或停機流程。
- 建立事件通報與調度介入流程，確保資安事件或設備故障發生後即時回報至調度中心。
- 依站點重要性進行分級，調整巡檢頻率、防護要求與備援機制。
- 每年至少執行一次跨場域演練，包含通訊中斷、錯誤指令與設備失效等情境。

中央目的事業主管機關可要求提供站點分級表、補償控制清單、演練報告與事件通報紀錄，以落實查核。

第二節、 交通領域

本節目的在協助交通運輸領域之中央目的事業主管機關與 CI 提供者，依本防護建議建立具可操作性、可查核且符合業務特性的控制措施。交通

與通訊場域多為高度分散架構，包含號誌系統、聯鎖設備、場站監控、隧道控制、道路監控、航務與空管系統、電信核心網路、光纖匯聚設備及基地台等。因此本節控制重點聚焦於跨場域區隔、關鍵通訊可信度、設備完整性管理、維運商控管與連續營運能力。

一、 分層分區與跨場域資產管理要求

中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章，完成正式且可查核之分層分區及資產盤點作業，至少包含下列事項：

- 以調度中心、場站層、沿線或隧道設備層、路側節點與終端設備等邏輯範圍建立分層分區圖，並標示通訊方向與主要控制邊界。
- 建立涵蓋號誌機、PLC、聯鎖控制器、監視攝影、變頻器、路側通訊設備、電信交換設備與核心節點等之資產清冊，並記載功能、位置、設備種類、通訊協定、韌體版本與維運責任。
- 在跨縣市或跨場站系統中，需以場站為邏輯單元建立資產分類，讓中央目的事業主管機關能在查核時逐站檢視。
- 資產清冊需定期更新，並於設備汰換、功能擴增或調度流程變更後一定時間內修訂。
- 對於使用壽命長、難以升級或原廠已不支援之設備，需列入限制項目並提出補償控制機制。

中央目的事業主管機關可要求分區圖、資產清冊、限制設備清單與補償控制規劃作為定期查核項目。

二、 主要通訊路徑與通訊安全落地要求

交通領域多依賴長距離、多節點、高頻率之雙向通訊，需確保通訊可信度與指令可追溯性。中央目的事業主管機關宜要求 CI 提供者至少完成下列事項。

- 識別並建立正式通訊清冊，涵蓋調度中心至場站、場站至沿線設備、基地台至核心網、交換中心之主要通訊路徑。
- 在主要通訊通道上實施協定白名單、來源白名單及通訊完整性保護，並採用具備協定識別與內容檢查能力之工控防火牆或資安設備。
- 禁止未經授權之跨層通訊，例如行控中心的管理系統直接存取號誌設備。
- 所有遠端操作須透過跳板設備進行，並具備身分確認、相關作業紀錄與稽核能力。
- 跨場域通訊紀錄需保存至少六個月，讓中央目的事業主管機關能確認調度指令與回報內容之完整性。
- 對生命安全具有直接影響之通訊，例如列車運轉控制、隧道排風系統及緊急廣播，需強化異常訊號攔阻與錯誤指令防護能力。

中央目的事業主管機關可要求通訊清冊、通道防護配置文件與跳板設備操作紀錄作為查核依據。

三、 安全關鍵設備之完整性維護及變更控管要求

交通領域包含大量安全關鍵設備，其錯誤設定或遭到竄改可能直接導致列車延誤、交通事故或通訊中斷。中央目的事業主管機關宜要求 CI 提供者至少建立下列措施：

- 對號誌、聯鎖、場站自動化、隧道控制與空管設備建立設定檔、韌體、邏輯程式之版本控管，並定期比對差異。
- 高風險操作需實施雙重確認，包括號誌排列變更、交控模式切換、風機運轉模式調整與通訊節點重新設定。
- 無法部署端點防護之設備，需採取協定層與通訊層補償控制，例如指令白名單或跨設備行為偵測。
- 所有設定變更須納入正式變更管理流程，包含風險評估、批准

程序、回復計畫與事後紀錄。

- 對於場站控制系統與路側設備，需建立災後回復設定與設備驗證程序，以確保異常後能立即恢復運作。

中央目的事業主管機關可要求 CI 提供者提供版本控管紀錄、變更管理文件與異常比對報告，並列入檢查重點。

四、 跨場站營運持續、無人節點管理與補償控制要求

交通領域多具跨縣市、多站點與無人節點，因此需強化連續營運與補償控制。中央目的事業主管機關宜要求 CI 提供者至少達成下列事項：

- 對無人站、沿線設備、基地台與通訊節點建立實體保護與環境監控，包括門禁、攝影、設備箱防護與電力監測。
- 針對無法立即升級之舊型設備，需建立補償控制，例如異常行為偵測、跨站資料比對、訊號越限監控與安全降載或保護模式。
- 建立即時事件通報流程，使交通或通訊異常能在發生後即時回報至調度或網管中心。
- 依場站或通訊節點之重要性進行分級，並依分級調整巡檢頻率、防護要求與故障回復時間。
- 定期執行跨場站、跨網域演練，涵蓋主要通訊中斷、錯誤訊號、設備故障或惡意攻擊等情境。

中央目的事業主管機關可要求 CI 提供者提供站點分級表、補償控制清單、事件通報流程與演練報告，並納入查核項目。

第三節、 通訊傳播領域

本節目的在協助通訊傳播領域之中央目的事業主管機關與 CI 提供者依本防護建議建立具可操作性、可查核且符合網路營運環境特性的控制措施。通訊傳播領域包含核心網路、匯聚交換、基地台、光纖骨幹、網路管理系統、語音與訊號系統等，其屬性為高連續性、高維運複雜度與高外部

依賴度。因此本節的控制重點著重於網路層級區隔、核心控制面的安全、供應商維運管理、設備完整性維護與營運不中斷能力。

一、 分層分區與核心資產盤點要求

中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章，建立正式且可查核之分層分區與資產盤點成果，至少包含下列項目：

- 依核心網路、匯聚層、存取層、基地台層與管理與協定控制層建置分層分區圖，並標示通訊界線、節點位置及跨區通訊方式。
- 建立包含交換設備、核心控制器、信令設備、匯聚器、基地台、網管平台及外部對接節點之資產清冊，並記載設備功能、位置、韌體版本、通訊協定、維運責任與是否具高度關鍵性。
- 於資產清冊中標示所有可遠端維運之節點，並納入後續維運控制要求的適用範圍。
- 資產清冊需定期更新，並於節點汰換或功能擴增後一定時間內完成修訂。
- 對於生命週期長、已停產或無法更新之設備，需列為受限設備並提出補償控制計畫。

中央目的事業主管機關可將分區圖、資產清冊、受限設備清單與補償控制計畫列為定期查核項目。

二、 跨區域通訊與關鍵協定保護要求

通訊傳播領域的核心風險來自跨網域通訊、協定複雜性與高頻率維運，因此需確保協定與控制訊號的可信度與可追溯性。中央目的事業主管機關宜要求 CI 提供者至少完成下列落地措施：

- 建立正式通訊清冊，涵蓋核心網路之間、核心至匯聚、匯聚至基地台以及與外部網路之對接路徑。
- 在涉及控制與信令之通訊通道上實施來源白名單、協定白名單

與內容完整性檢查，並採用能辨識 2G 至 5G 或光纖協定的資安設備。

- 核心控制平面與管理平面須與一般業務流量進行區隔，禁止跨層直接存取。
- 所有遠端維運需透過跳板設備執行，並具身分確認、存取控管與完整操作紀錄。
- 跨節點通訊紀錄需保存至少六個月，讓中央目的事業主管機關能查核管理平面與控制平面的操作軌跡。
- 涉及國際網路或跨營運商之通訊須提供額外的協定檢查及錯誤訊號攔阻能力。

中央目的事業主管機關可要求 CI 提供者提交通訊清冊、協定保護配置文件與跳板設備操作紀錄作為查核依據。

三、 核心控制設備與基地台設備之完整性維護要求

通訊業者之核心控制器、交換設備與基地台為整體網路營運的關鍵組件，任何設定不當或未經授權之變更可能造成大範圍斷訊或訊號中斷。中央目的事業主管機關宜要求 CI 提供者至少建立下列控制措施：

- 對所有核心控制器、基地台、傳輸設備與網管平台建立設定檔、韌體與組態之版本控管，並定期比對差異。
- 涉及核心控制平面之高風險操作需進行雙重確認，包括協定參數更新、基站功率調整、交換節點切換與路由調整。
- 對無法部署端點防護之交換設備、傳輸設備或基地台，需實施網路層補償控制，包括指令白名單或行為異常偵測。
- 所有設定變更需納入正式變更管理程序，包括風險評估、批准流程、回復程序與事後紀錄。
- 對跨區域關鍵節點需建立設定備援、即時比對與快速回復機制，

使異常恢復時間控制在可接受範圍內。

中央目的事業主管機關可要求 CI 提供者提供版本控管紀錄、變更管理文件及設定差異比對報告作為查核重點。

四、 營運持續、外包維運管理與補償控制要求

通訊傳播領域需維持高可用性與高韌性，且高度依賴維運商，因此中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章建立可執行的持續營運與補償控制措施：

- 所有基地台、匯聚節點與傳輸機櫃須具備實體保護與環境監控，包括門禁、機櫃防拆、攝影、溫度與電力監測。
- 對於無法更新之舊型節點，需提供補償控制措施，例如異常流量偵測、協定越限監控、跨節點比對與必要時啟動保護模式。
- 維運商需納入集中存取管理，並以跳板設備管理所有操作。所有外包維運紀錄需保存至少六個月。
- 建立跨區域事件通報流程，使核心設備與基地台異常即時回報至網管中心。
- 依節點重要性進行分級，並依分級調整巡檢頻率、緊急應變要求與故障修復時間。
- 定期執行涵蓋多節點、多營運商之聯合演練，包括國際節點中斷、協定錯誤訊號、基地台異常與傳輸路徑故障等情境。

中央目的事業主管機關可要求 CI 提供者提供節點分級表、補償控制清單、外包維運紀錄與演練報告作為查核依據。

第四節、 緊急救援與醫院領域

本節目的在協助緊急救援與醫院領域之中央目的事業主管機關與 CI 提供者，依本防護建議建立具可操作性、可查核且符合該領域風險特性的控制措施。緊急救援系統與醫療院所資訊與控制環境通常包含急救指揮中心、救護派遣平台、醫療資訊系統、相關診斷、急救及醫療用醫療儀器期

維護醫院運作之其他支援設施。這些系統直接影響急救流程、臨床診療、病患安全與醫療服務連續性，因此控制重點在於清楚分區、保護醫療資訊、醫療設備及其他支援設施之完整性、確保關鍵通訊不中斷、強化異常偵測及掌握外包與廠商維運行為。

一、 分層分區與醫療關鍵資產盤點要求

中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章完成可查核的分層分區與資產盤點，至少包含下列項目：

- 依急救指揮與派遣層、醫療資訊層、醫療設備層、其他支援設施管理層與一般辦公層建置分層分區圖，明確界定醫療資訊系統與醫療 OT 設備控制網段不得互通之範圍。
- 建立涵蓋急救派遣平台、資料庫伺服器與外部交換節點、資安列管醫療儀器及其他支援設施之資產清冊，並記載功能、版本、位置、維護責任與是否具資安因素之影響。
- 標示所有具遠端維運需求與雲端連線能力的資安列管醫療儀器及其他支援設施，並納入後續維運控管要求。
- 資產清冊需定期更新，並於新增設備或醫療場域擴增後一定時間內完整修訂。
- 對於醫療設備生命週期長且無法更新資安列管醫療儀器及其他支援設施，需列為受限設備並提出補償控制計畫。

中央目的事業主管機關可將分區圖、資產清冊、受限設備清單與補償控制計畫列為查核必備文件。

二、 急救指揮、醫療資訊與醫療設備之通訊安全要求

緊急救援與醫院領域高度依賴醫療資訊交換、急救派遣通訊及醫療設備連線，因此通訊與資料完整性是主要風險來源。中央目的事業主管機關宜要求 CI 提供者至少完成下列落地措施：

- 建立正式通訊清冊，涵蓋急救指揮中心至救護車、急診、手術

室與生命維持設備、建築管理系統與環控設備等主要通訊路徑。

- 所有涉及臨床診療或派遣指令之通道需實施來源白名單、協定白名單與資料完整性保護，並使用具內容檢查能力的資安設備。
- 禁止資安列管醫療儀器及其他支援設施網段與一般辦公網路之直接連線，所有跨層連線需經過受控通道。
- 資安列管醫療儀器及其他支援設施之維運商與遠端支援需透過跳板設備執行，並具備身分確認、相關操作紀錄與變更稽核能力。
- 醫療影像、生命維持設備或診斷資訊之資料交換需具備傳輸加密與完整性驗證，並保留交換紀錄至少六個月。
- 急救指揮與醫療資訊系統之通訊需具備異常或錯誤訊息攔阻能力，以避免系統誤派或訊號失準。

中央目的事業主管機關可要求 CI 提供者提交通訊清冊、協定保護配置文件與跳板設備日誌紀錄作為查核依據。

三、 醫療領域資安列管醫療儀器的完整性維護要求

醫療與緊急救援系統中的診斷與治療設備若包涵資安列管醫療儀器，為避免影響急救作業，因此需建立更嚴格之設備完整性與變更控管。中央目的事業主管機關宜要求 CI 提供者至少完成下列措施：

- 對高資安風險之資安列管醫療儀器建立設定檔、韌體與軟體版本控管，並定期執行差異比對。
- 所有可能影響醫療品質、安全與治療參數之操作必須進行雙重確認，包含模式切換、參數調整或診斷軟體更新。
- 無法部署端點防護之高資安風險之資安列管醫療儀器，需以網路層補償控制保護，例如防火牆、指令白名單、外部行為監測或異常偵測機制。

- 高資安風險之資安列管醫療儀器，若設定變更需納入正式變更管理流程，包含臨床面風險評估、批准程序、回復計畫與操作紀錄。
- 高資安風險之資安列管醫療儀器需具備設定備援、診斷程式比對與災難復原機制，使意外中斷時能迅速恢復臨床運作。

中央目的事業主管機關可要求 CI 提供者提供版本控管紀錄、變更管理文件與差異比對報告，並列為查核重點。

四、 院區營運持續、其他支援設施與補償控制要求

醫院與緊急救援場域需維持高可用性，且後端支撐系統如環控、電力與建築自動化系統對醫療運作同樣具有關鍵性。中央目的事業主管機關宜要求 CI 提供者依本防護建議第五章建立下列可執行之措施：

- 對手術室、加護病房、急診室、伺服器室與重要機電設備區域建立實體與環境監控，包括門禁、影像、溫度、濕度、空調與電力監測。
- 對於無法更新或難以替換之舊型醫療設備與環控系統，需設置補償性監測，例如異常參數偵測、跨設備行為比對、診斷資料越限警示或安全降載模式。
- 建立資安事件、設備故障與醫療安全事件的整合通報流程，使各單位能在一定時間內回報至資訊或醫工管理中心。
- 依醫療作業需求建立科別與場域分級，調整巡檢頻率、防護要求與可容忍停機時間。
- 定期執行跨院區或跨部門演練，包括通信中斷、設備異常、惡意攻擊或派遣錯誤等情境。
- 後端支撐之環控與建築管理系統需納入醫療服務持續性考量，並建立獨立的緊急回復程序。

中央目的事業主管機關可要求 CI 提供者提供院區分級表、補償控制清單、演練報告與事件通報紀錄以利查核。

第八章、 推動與持續改進

工控資安防護的推動並非單一專案或短期計畫，而是一項涉及國家政策、各中央目的事業主管機關管理機制與 CI 提供者實際落地能力的長期工程。工控威脅隨科技發展與國際攻防情勢持續變動，因此整體防護作業必須具備動態調整能力，使工控資安不僅能符合法規要求，更能隨時間推進而逐步成熟。為持續推動國家層級資安政策，以及各中央目的事業主管機關與 CI 提供者持續改進之方向，本防護建議將持續滾動修訂我國 CII 防護架構，以期保持 CI 韌性並與國際一致。

在政策推動層面，行政院相關部會定期檢視國內外重大資安事件、供應鏈風險、國際法制變化與新興科技，使 CII 相關資安政策能持續與國際趨勢接軌。近年來，國際標準與法規如歐盟 NIS2 指令、CRA 以及各國對 OT 與 ICS 環境的監管要求都持續強化，這些變化可能直接影響我國產業的出口、設備採購、供應鏈合作與國際合規。因此，政策層面需持續研析這些影響，並適時更新國家 CI 資安防護政策，使制度能因應新威脅、新產業型態與跨國合作需求，同時讓各中央目的事業主管機關與 CI 提供者清楚知悉政策方向。

各中央目的事業主管機關除負責制定防護基準與定期查核外，還應建立輔導、支援與能力提升機制，使各 CI 提供者在落實過程中有明確的工具與資源可依循。各中央目的事業主管機關可提供範本防護建議、導入指引、風險評估方法、架構建議與定期教育訓練，使工控資安不再是個別單位各自摸索的工作。此外，各中央目的事業主管機關亦可推動領域內 CI 提供者進行自主評量、標竿比較與經驗分享，使防護基準不只是法規要求，而是形成跨機構、跨企業合作的產業安全文化。

在 CI 提供者層面，工控資安應視為日常營運管理的一部分，而非緊急事件發生後的補救工作。依據 ISA/IEC 62443 的工控資安生命週期思維，建議 CI 提供者將工控資安導入 PDCA （Plan Do Check Act，計畫、執行、檢查、改善）循環，使政策、流程、控制措施與監控機制能定期被檢視與調整。CI 提供者在面對資安事件、設備故障或重大變更時，啟動正式的事後檢討程序，分析事件根本原因、組織流程缺口、供應鏈問題與人員錯誤因素，並將改善措施納入制度化程序，避免相同問題再次發

生。

持續改進需要資料的支持，因此資料收集與指標管理是強化防護體系的重要手段。各中央目的事業主管機關與 CI 提供者可共同規劃一套衡量 CII 工控資安成熟度的量化與質化指標，例如弱點修補的時效、事件通報的完整性、跨部門演練的頻率與效果、查核缺失改善完成率、遠端存取申請審核時效、補償控制重新評估週期、或供應鏈風險調查覆蓋率等。透過這些指標的長期觀測，不僅能評估基準落實程度，也可作為政策調整與資源配置的基礎。

為使各領域能獲得更完整的協作環境，各中央目的事業主管機關可推動 CII 領域間的威脅情資分享、跨產業攻擊樣態分析與事件通報匿名化資料回饋，使整體工控資安生態系具備對新興威脅的早期覺察能力。此機制亦符合 NIST SP 800-82 所強調的「資訊共享與跨組織協作」，以及 ISA/IEC 62443 所強調的「組織與供應鏈安全一致性」。

總結而言，工控資安推動與持續改進並非單純提升技術能力，而是透過政策方向、標準參考、跨部門協作、成熟度管理與持續改善，使國家、各中央目的事業主管機關與 CI 提供者能在面對快速變動的威脅情勢時保持前瞻性、韌性與一致性。此一持續改進機制一旦運作成熟，將使我國 CI 更能承受跨國攻擊、重大事故與供應鏈風險，確保社會運作的穩定與安全。

第九章、 結論與展望

工控與 OT 環境已在國家整體資安布局中扮演不可替代的角色。從能源、水資源、交通運輸、電信通訊、醫療照護到金融服務，現代社會的營運已全面依賴高度自動化與遠端化的控制系統。這些系統一旦遭受資安事件或惡意操控，其影響往往不限於資訊層面的可用性，而是會直接干擾實體環境，進而影響公共安全、社會運作與國家經濟活動。國際攻擊事件的累積案例以及國際各國家對 CI 的監理強化，都清楚顯示工控資安已經從技術問題提升為國家安全策略層級的重要議題。

本次修訂之《關鍵資訊基礎設施資安防護建議》，是在既有制度與實務基礎上，回應近年工控威脅與全球監管環境所進行的全面性調整。本次修訂不僅反映 IT 與 OT 界線逐漸模糊、攻擊模式日益複雜、供應鏈風險快速擴大之現況，也回應國際監管體系的巨大變化，例如歐盟 NIS2 指令、CRA、能源與交通領域的專業安全要求，以及工控相關國際標準如 ISA/IEC 62443 系列的成熟化。隨著我國 CII 管理制度由八大領域擴充為九大領域，本防護建議亦同步調整防護架構、實施參考與領域應用指引，使各中央目的事業主管機關在制定或修訂防護基準時能有一套具備國際一致性、實務可行性與本土適用性的政策依循。

展望未來，工控環境將面臨更快速的技術演進與攻擊手法變化。人工智慧、雲端平台、虛擬化架構、邊緣運算、數位孿生與物聯網裝置的廣泛導入，將不斷改變工控系統的邊界定義與攻防模式。新技術可提升效率，也可能引入新的攻擊面；新的自動化技術可降低人力需求，也可能因決策鏈條變短而增加風險集中度。因此，未來工控資安政策需要在系統可用性、營運效率與資安防護之間取得新的平衡，以確保科技導入能真正提升產能與安全，而非形成新型態的脆弱點。

各中央目的事業主管機關與 CI 提供者需持續投入資源，強化工控資安專業人才的培育，提升跨部門與跨領域協作能力，並建立與國際標準接軌的制度環境，使國內產業得以在國際供應鏈中維持競爭力。本防護建議亦需維持動態更新，隨威脅趨勢、國際法規、產業環境與技術演進適時調整內容，使其能長期反映最新風險與可行管控措施。

透過本防護建議所提供的防護架構、治理原則、技術措施與領域應用指引，各CI若能依據自身特性落實相關措施，我國工控環境將能具備更高的整體韌性，有效降低重大資安事件對社會穩定、國家安全及民生服務的衝擊。同時，我國在國際資安體系中的可信度、合作能力與產業競爭力也將因為更穩健的工控資安全能力而持續提升，形成國家整體戰略的重要支柱。

附錄一、專有名詞中英對照表

本防護建議中所使用之英文專有名詞、縮寫和中文翻譯如下：

表 6、英文專有名詞、縮寫和中文翻譯

英文專有名詞	縮寫	中文翻譯
Artificial Intelligence–Assisted Automation	AI-Assisted Automation	人工智慧自動化
Asset Owner	AO	資產擁有者
Building Automation System	BAS	建築自動化系統
Business Continuity Plan	BCP	營運持續計畫
Critical Infrastructure	CI	關鍵基礎設施
Cyber Incident Reporting for Critical Infrastructure Act	CIRCIA	美國關鍵基礎設施資安事件通報法
Cyber Resilience Act	CRA	歐盟網路韌性法案
Cybersecurity, Energy Security and Emergency Response (U.S. DOE)	CESER	美國能源部資安與能源韌性辦公室
Cybersecurity Framework	CSF	網路安全框架
Critical Infrastructure Protection Standard	NERC CIP	北美電力可靠度公司關鍵基礎設施保護標準
Demilitarized Zone	DMZ	非軍事區或資料中介區
Industrial Automation and Control Systems	IACS	工業自動化與控制系統
Industrial Control System	ICS	工業控制系統
Industrial Internet of Things	IIoT	工業物聯網
Information and	ICT	資訊及通訊技術

英文專有名詞	縮寫	中文翻譯
Communications Technology		
Information Technology	IT	資訊技術
International Electrotechnical Commission	IEC	國際電工委員會
International Society of Automation	ISA	國際自動化協會
ISA/IEC 62443 Series	—	工控資安國際標準系列
National Institute of Standards and Technology	NIST	國家標準與技術研究院
Network and Information Security Directive 2	NIS2	歐盟網路與資訊安全指令第二版
Operational Technology	OT	營運技術
Programmable Logic Controller	PLC	可程式化邏輯控制器
Product Supplier	PS	產品供應商
Security for Power System Communications (IEC 62351 Series)	IEC 62351	能源通訊安全標準系列
Software Bill of Materials	SBOM	軟體組成清單
Supervisory Control and Data Acquisition	SCADA	監控暨資料採集系統
System Integrator	SI	系統整合商
Service Maintainer	SM	服務維護商
Secure Software Development Life Cycle	SSDLC	安全開發生命週期

資料來源：本防護建議自行整理

附錄二、國際標準與本防護建議對照

本附錄承接前述國際工控資安標準與監管發展之角色定位，說明《關鍵資訊基礎設施資安防護建議》如何在不重複制定技術標準之前提下，將其核心精神轉化為適用於我國 CII 管理制度之政策與基準。

在 ISA/IEC 62443 系列標準方面，其作為工控資安國際核心標準，本防護建議在防護類別設計、分層與分域、風險導向、安全等級概念、補償控制原則、供應鏈安全要求與安全設計理念等面向，均自然承接其核心精神。

在 NIST SP 800-82 方面，本防護建議於落實層面大量借鏡其實務觀點，將資產盤點、網路分層、邊界防護、人員訓練、事件通報、補償控制與例外處理等原則，轉化為政策導向且可稽核之管理要求，使 CI 提供者得以在我國制度下系統性落實該指引精神。

在歐盟 NIS2 指令方面，本防護建議於治理責任、風險管理、供應鏈安全與事件通報機制上與其精神保持一致，並透過制度化要求協助各中央目的事業主管機關與營運者建立可受監督之治理架構。於 CRA 部分，本防護建議對供應鏈安全、弱點管理、更新支援與安全設計原則之要求，亦反映產品生命週期安全趨勢。

綜合而言，國際標準、實務指引與監理法規分別提供技術要求、落實方式與強制動力，而本防護建議則負責將其轉譯為可直接適用於我國 CII 管理制度之政策與基準，三者在角色上相互補充，共同構成我國工控資安防護體系之完整架構。

表 7、國際標準與本防護建議對照

國際標準/法規	主要內容定位	與本防護建議對照	說明
ISA/IEC 62443-1 系列（-1-1、-1-5）	基本概念、名詞定義、安全設定檔與 profile 制度	第 1、4 章之架構原理與共通語彙	本防護建議採用其 IACS 定義、區域與通道（zones and conduits）概念、安全設定檔邏輯等作為上位語彙。

國際標準/法規	主要內容定位	與本防護建議對照	說明
ISA/IEC 62443-2 系列（2-1、2-4）	組織安全計畫、政策、程序、營運與維護要求	第 4、6、8 章之治理、持續改進、組織管理、供應鏈管理	本防護建議整體治理邏輯承接其安全計畫精神，並將其政策要求轉為各中央目的事業主管機關可用的制度框架。
ISA/IEC 62443-3-2（風險評估）	風險評估方法、安全需求的建立、決定目標安全等級（SL-T）	第 4.3、5 章跨段落（風險導向、安全等級、關鍵資產判定）	本防護建議中風險評估、安全等級概念與差異化控制深度，均來自 62443-3-2 之評估與 SL 決策邏輯。
ISA/IEC 62443-3-3（系統安全要求）	系統層級 7 大 FR(基本安全要求）與 SR（系統需求）	第 5 章 11 項防護類別之核心邏輯	FR1～FR7 與本建議的網路架構、存取控制、稽核、系統完整性與通訊保護間具高度對應性。
ISA/IEC 62443-4-1 / 4-2	程式開發安全/元件安全能力	第 5 章弱點管理、系統完整性、供應鏈要求	本防護建議於供應鏈風險、軟體更新、弱點處理等內容均承接其核心要求。
NIST SP 800-82（工控資安指引）	IACS 實務落地指引（架構、控制措施、實作建議）	第 6 章實施路徑、補償控制、事件應變、電廠/水務落地作法	本防護建議大量採用其實務實施觀點，如起始階段工作、補償控制與 OT 特性調整。
NIS2 Directive（歐盟）	關鍵與重要服務之治理責任、事件通報、供應鏈管理	第 4、6、8 章治理、事件通報、供應鏈要求	本防護建議之治理責任、通報時效、供應鏈安全與稽核思維與 NIS2 指令要求一致。
Cyber Resilience Act(歐盟 CRA)	數位產品之全生命週期安全：開發、弱點揭露、更新義務	第 5.7、5.9、6.3 章產品與供應鏈管理	本防護建議之「secure by design/ default/ demand」與弱點處理要求與 CRA 精神一致。

國際標準/法規	主要內容定位	與本防護建議對照	說明
NERC CIP（北美能源）	電力系統之資產識別、邊界保護、稽核、供應鏈與事件通報	第 5、7 章電力領域應用指引、邊界防護、營運持續	本防護建議能源領域之「變電站/調度中心」作法與 NERC CIP 核心要求一致。
IEC 62351（能源通訊安全）	電力/能源通訊協定之身分鑑別、加密、完整性保護	第 5.6、7 章能源領域之通訊保護與設備識別	本防護建議通訊安全與能源領域控制協定保護，可基於 IEC 62351 之抽象概念擴充。

資料來源：本防護建議自行整理