經濟部

工控物聯網共通性資安指南

中華民國108年12月10日

第 1 章 前言

1.1 目的

因應雲端、大數據等新興 IT 科技，於近年來開始導入原有工控（IACS、DCS、SCADA)等元件構成的 OT（Operation Technology）環境，興起了工業 4.0、智慧製造及關鍵基礎設施的智慧連網，在此統稱為工控物聯網。2018 年某半導體製造公司全台各廠因 WannaCry 病毒弱點未修補，造成生產線大當機超過數十小時，損失高達數十億台幣，震撼國際製造業及資安產業，燃起製造業長期漠視的資安意識，管理階層及利害關係人紛紛關切資安對工控物聯網議題。

然而工控物聯網的資產擁有者雖然都知道資安的重要性，但卻不知如何進行對工控物聯網的風險分析及如何發展一個可持續改善資安防護水準的資安計畫，更談上與利害關係人如何進行風險溝通，另一方面 IT 的資服業者、工控元件的供應商，亦無法提出全面完整的工控物聯網安全解決方案。

為使資產擁有者能針對現有或是即將規劃的工控物聯網整體架構、軟硬體建置、維運組織及第三方供應商的安全風險的識別、分析、處理及持續改善，本指引將參考國際物聯網、資通信安管理標準、操作實務，以資產擁有者的視角，撰擬本指南，以作為針對工控物聯網全面風險管理、提出安全需求之參考，並由資安顧問及服務提供商、資訊系統產品及服務提供者、工控系統產品及服務提供者及物聯網安全實驗室依本指南提出符合資產擁有者的工控物聯網資安解決方案或服務，以利進行雙方共同參考的文件。

本指南預期實施效益如下：

- 提供製慧製造或基礎設施服務製程中產線智慧化過程可靠的架構。
- 保障工業投資在資訊安全無虞情況下順利運作。
- 對於有生產製造企業或基礎設施提供者，提供製造過程資訊安全的保障的實作指南
- 針對安全要求（法令或客戶）給予第三方服務供應商明確的指導
- 對於資產擁有者及客戶，提供工控物聯網系統、元件建置及製造過程資訊安全的保障

1.2 適用對象

1.2.1 資產擁有者

提供導入工控物聯網作為智慧製造基礎的資安風險與控制需求的指示，用以提列安全需求、選擇資安服團隊（資安顧問、資服 SI、工控 SI、物聯網安全實驗室）協助導入工控物聯網安全機制生命週期所需最佳實務參考。

1.2.2 資安顧問及服務提供商

本指南提供工控物聯網安全管理框架，用以協助客戶由風險管理角度，整合 IT/OT 整合產生資安風險，進行安全計畫、專案管理、評估工控物聯網建置後持續安全管理、緊急應變處理及標準(CSCIS/IIC/ISO27001/IEC62443)、法規遵遁等工作指導書。

1.2.3 資訊系統產品及服務提供者

由本指引導出安全需求，在工業物聯網普渡(Purdue)模型上層 Level3~5 提供 IT 資安產品及服務解決方案，以對接需求端在本指引的安全需求，提供建決方案建置及後續維護。

1.2.4 工控系統產品及服務提供者

由本指引導出安全需求，在工業物聯網普渡(Purdue)模型上層 Level0~3 提供 OT 資安產品及服務解決方案，以對接需求端在本指引的安全需求，提供建決方案建置及後續維護。

1.2.5 物聯網資安實驗室

可依國際工控安全標準（IEC62443)及國際物聯網安全實務（CSCIS/IIC)提供針對工控物聯網的元件，如終端控制裝置、匣道器、邊緣運算、雲端運算安全評估，針對安全等級需求高的工控物聯網裝置，本指引將建議需取得 IEC62443 4-1、4-2 安全認證。

1.3 章節架構

本指南共區分 8 個章節，整體架構如圖 1：

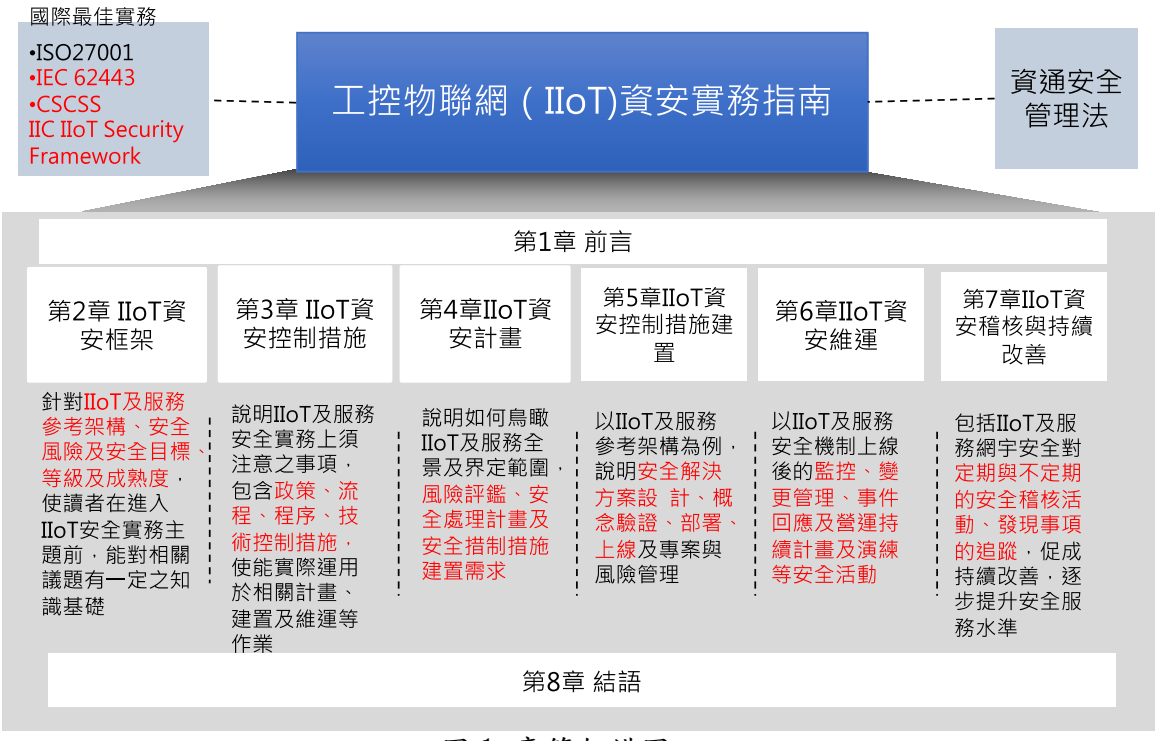


圖 1 章節架構圖

1.4.1 第 1 章說明目的、名詞解釋、章節架構及使用說明

1.4.2 第 2 章針對工控物聯網（IIoT）安全參考架構、安全風險及安全目標、等級及成熟度，使讀者在進入 IIoT 安全實務主題前，能對相關議題有一定之知識基礎。

1.4.3 第 3 章 說明 IIoT 安全安全實務上須注意之事項，包含政策、流程、程序、技術控制措施，使能實際運用於相關計畫、建置及維運等作業

1.4.4 第 4 章 說明如何鳥瞰 IIoT 安全全景及界定範圍，風險評鑑、安全處理計畫及安全措制措施建置需求。

1.4.5 第 5 章 以 IIoT 安全參考架構為例，說明安全解決方案設 計、概念驗證、部署、上線及專案與風險管理。

1.4.6 第 6 章 以 IIoT 安全安全機制上線後的監控、變更管理、事件回應及營運持續計畫及演練等安全活動。

1.4.7 包括 IIoT 安全定期與不定期的安全稽核活動、發現事項的追蹤，促成持續改善，逐步提升安全服務水準

1.4.8 第 8 章 結論：總結本指南概要

1.4 使用說明

本指南主要以資產擁有者的需求為出發點，第 1 章為本指南的導讀，使得資產擁有者與提供工控物聯網資安防護軟硬體、專案服務的各方（資安顧問、資服／工控系統產品及服務提供者與資安實驗室）可以有共同對本指南有總體認知及共通的語彙。

第 2 章是以企業著名企業的普渡(Purdue)企業參考架構模型（PERA）對企業的 IT/OT 一般架構進行垂直剖析，並以現今國際著遍接受的的資訊安全管理實務整理為本指南建議工控物聯網（IIoT）資安框架、資安等級及資安成熟度。以便利資產擁有者及資安顧問能以高階的風險評鑑方式，對企業 IIoT 進行水平分割成不同資安需求的區域及連接的傳輸管道，以鑑別出中、高風險的區域及傳輸管道，以利實施資安對策。

第 3 章是針對整體組織工控物聯網環境，以組織廣度、系統及元件三種比例的管理與技術性安全控制措施的，各控制措施都有安全能量等級（SL-C）並以組織自訂目標安全等級(SL-T)，組織可以持續衡量安全等級的達成(SL-A)，來評估組織的 IIoT 的資安成熟度。，

第 4～7 章是組織執行 IIoT 安全計畫（Security Program）的 PDCA 管理循環，讓組織可以由混亂無序的 IT/OT 現況逐步走向資安受管理的 IIoT（Managed Cybersecuirty of IIoT）。實務的導入需要結合目標場域，以建置實驗場域來驗證符合安全控制措施的解決方案有效性，流程概如圖 2 所示，惟實驗場域的建置指南不在本指南的範圍。

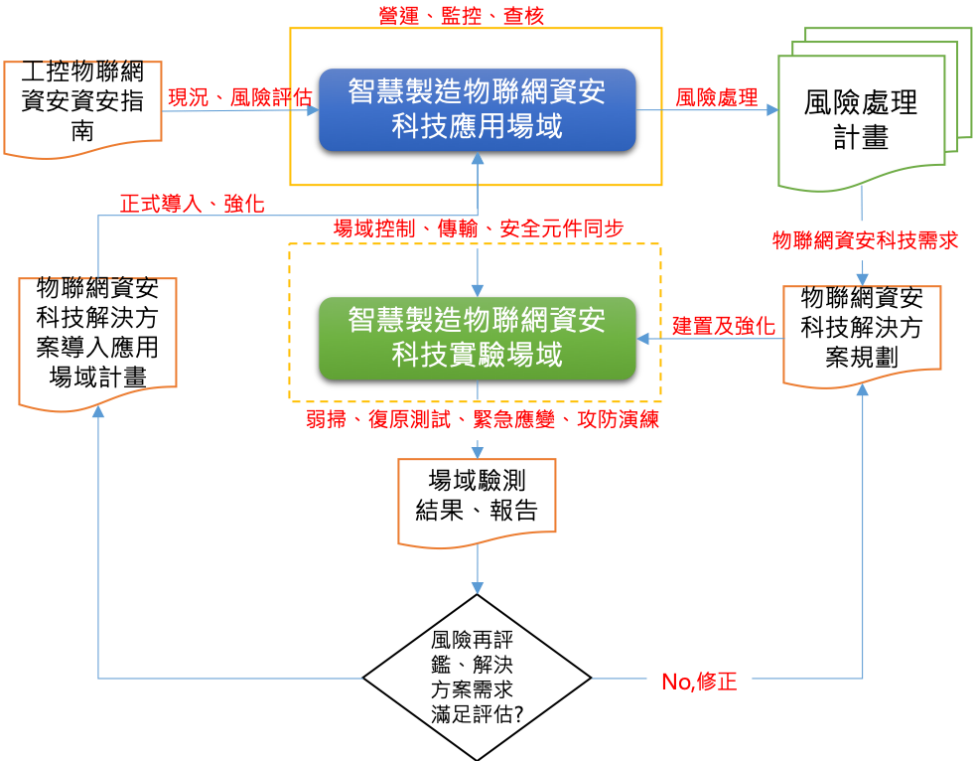


圖 2 本指南實務導入示意圖

第 8 章 是本指南總結及未來本指南延伸的發展，並說明與個別產業指引的界接關係。

對於本指南各方對本指南研讀的章節建議如下表：

章節	資產擁有者	資安顧問	資服供應商	工控供應商	資安實驗室
第 1 章	V	V	V	V	V
第 2 章	V	V	V	V	
2.1	V	V	V	V	
2.2	V	V			
2.3	V	V	V	V	
2.4	V	V			
2.5	V	V	V	V	V
2.6	V	V			
第 3 章	V	V	V	V	V
3.1	V	V	V	V	
3.2	V	V	V	V	
3.3	V	V	V	V	
3.3.1	V	V	V	V	
3.3.2	V	V	V	V	
3.3.3	V	V		V	V
第 4 章	V	V			
第 5 章	V	V			
第 6 章	V	V	V	V	
第 7 章	V	V			
第 8 章	V	V	V	V	V

第 2 章 工控物聯網資安概論

2.1 工控物聯網參考架構

2.1.1 普渡(Purdue)企業（概念）參考架構

在工控物聯網領域中，為了要檢視企業在工控自動化 IACS（OT）環境及運用資訊科技（IT）達成工控、生產製造設備連網，製程智慧化，而構成的資產、資料流及安全風險的全貌，有各式各樣的呈現方式不勝凡數，如最普遍被接受的參考架構是「普渡(Purdue)企業參考架構」（Purdue Enterprise Reference Architecture, PERA）模型，簡稱「普渡(Purdue)模型」（如圖 3），該參考架構被國際工控自動化標準協會 ISA99(現為 ISA/IEC 62443)所採納，用來描述大型工控物聯網環境中重要元件的關聯、依存關係及資料／控制流向，亦可作為風險識別標示及安全解決方案部署，每個組織因產業及生產標的與流程流程均大不相同，但普渡(Purdue)模型可以用單一抽象的架構表達複雜且不易統一的系統架構，以下為各層的說明

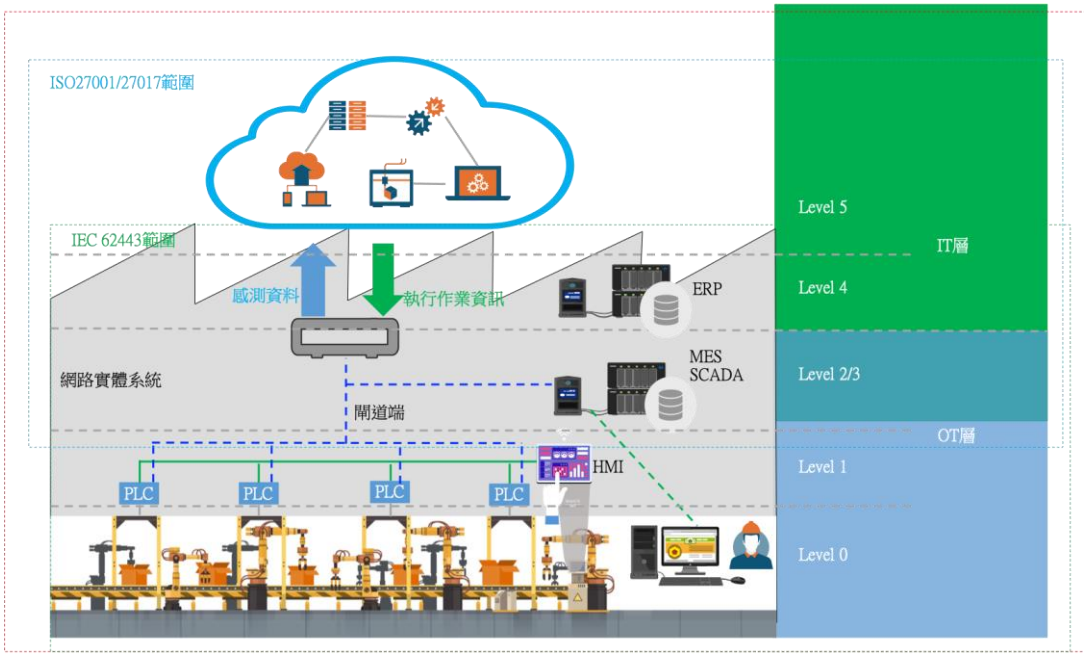


圖 3 普渡(Purdue)企業參考架構(PERA)模型與國際標準對應關係

2.1.1.1 第 5 層 企業智慧層

運用雲端、大數據(big data)、機器學習、人工智慧等智慧科技分析由製程現場（第 0 層）、控制層（第 1 層）、區域監控層（第 2 層）、現場製造和操作控制傳回資料及由第 4 層，進而產生企業決策所需或能回饋到生產製造活動、資源最佳化的智慧。

2.1.1.2 第 4 層 企業營運層

是企業日常營運中樞，包含了業務、研發、供應鏈管理及人力資源發展等活動，主要是作為企業營運的核心 IT 系統，常見重要業務系統如下：

- 企業資源規劃系統（Enterprise Resource Planning, ERP）
- 產品生命週期管理（Product Lifecycle Management, PLM）系統
- 供應鏈管理（Supply Chain Management, SCM）系統
- 客戶關係管理（Customer Relation Management, CRM）系統。

以上這些主要的核心資訊系統及週邊支援的應用系統及 IT 基礎設施，構成企業營運的資訊流系統。

2.1.1.3 第 3 層 廣域現場製造和操作控制層

從第 3 層至第 0 層是屬於工控自動化(Industrial Automation Control System, IACS)或稱為工控場域（Industrial Controls Zone）俗稱為操作科技（Operation Technology, OT）。
第 3 層主要為了大範圍（不同實體地理位置或場域）或是分散式工控系統的操作人員設計的監控及操作，主要的元件包含但不限於以下

- SCADA 的監控中心
- DCS 的監視畫面及存取控制
- 生產現場的視訊監視系統
- 環境安全衛生監視系統
- 生產環境資通信安全可視化監控系統

透過這些系統的監控、警報與事件回應的功能，可使操作人員的監控時間涵蓋提昇至 7x24x365，同時所需的人力負荷也可降低，讓生產現場的可用率、安全維持在可接受水準。

2.1.1.4 第 2 層 區域現場製造和操作控制層

第 2 層與第 3 層的功能大同小異，第 2 層是靠近生產場域或是基礎設施的監控、操作及事件回應機制，通常與生產場域或是基礎設施在同一地理位置或是同一場域的實體環境。對第 0 層的生產機具或是基礎設施的製程元件，有直接的實體連接，包含但不限於以下：

- 可程式化邏輯控制器（Programming Logic Control, PLC）
- 變頻驅動器 VFD
- 人機操作介面 HMI

在這層中操作人員可通過 HMI 即時與生產機具或是基礎設施的製程元件進行人機互動，或透過 PLC 或 VFD 來進行自動控制。

2.1.1.5 第 1 層 控制層

第 1 層包含了對第 0 層的受控設備的本地控制與保護裝置

- 基本製程控制系統（Basic Process Control System, BPCS）

BPCS 系統泛指一切與安全無關對受控設備進行控制的系統或裝置，主要執行功能是：

- 在預先設定的操作條件下控制過程，優化工廠操作以生產高品質的產品，並嘗試將所有過程變量保持在其安全限制內。
- 通過操作員控制台提供操作員界面以進行監視和控制（人機界面）
- 提供警報/事件記錄和趨勢設施
- 產出生產資料報告

- 安全儀表系統（Safety instrumented system , SIS）
  SIS 是保障生產安全的重要措施，它應在危險事件發生之前正確地執行其安全功能，避免或減少事故的發生。然而有些時候，由於安全儀表系統發生失效，在需要它執行安全功能時無法正確執行預定的功能，從而導致災難事故的發生。

2.1.1.6 第 0 層 受控設備層

這一層為受控設備（Equipment Under Control, EUC）層，是放置第 1 層所控制的實體設備位置。這些 EUC 包括在基礎設施或工業製造流程 （Process）中運作的實體設備或元件，也包含了各式各樣安裝在生產環境的感應器（Sensor）及執行器(Actuators)，如生產設備、工業機器人、驅動器、電機、閥門等構成製程的元件，這些實體製程有些是實體性，有些是化學性，是由人直接於現場或遠端操作或透過普渡(Purdue)模型上層的指令及控制機制來作動，將原材料輸入，經這事先定義或設定一連串製程工序及生產條件，最終如期產出預期品質的產出物。

2.1.1.7 工控區域的非軍事區(Industrial Demilitarized zone, IDMZ)

在一般非製造業企業或基礎設施服務供應者的網際網路或稱外網（Internet）及內網（Intranet），為使外部使用者可以存取企業的公開資訊或提供服務，又不希望外部使用者或是惡意人士可以直接連線到內部網路，會存取企業的機密或是不公開資訊，在這樣的便利與安全的考量下會利用防火牆建立一個內外網都可連線的 DMZ。
在前述的 PERA 模型，我們知道 0～3 層是屬於OT，4～5 層是屬於 IT，在尚未進行智慧連網前，OT 與 IT 甚至是完全實體隔離，維運管理也是分屬不同部門的人員，但在工業 4.0 或是智慧製造的需求興起後，原來兩個相互隔離的網路環境開始如 Internet/Intranet 般的連接起來，所以就需要在 OT 與 IT 的銜接處，在 PERA 模型的第 3／4 層間設置 DMZ 區的需要。所以 DMZ 區的架構示意如下圖

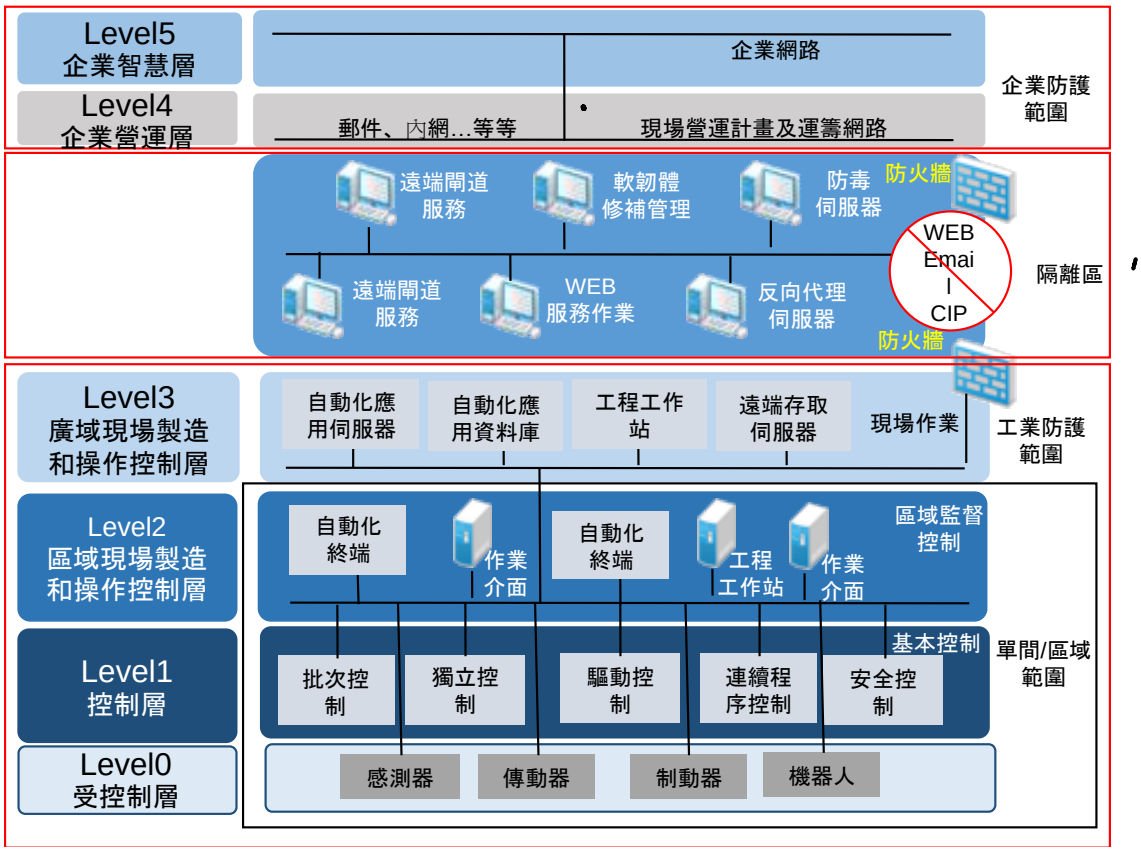


圖 4 Industrial DMZ 區示意圖

2.1.2 資產型式(Asset Model)

雖然在 PERA 是以水準方式的區分系統及元件的抽象連接，但是實體的單一或是不同地理位置的生產或基礎設施場域是多條製程，且均有不同水準或是垂直的相依性存在，而組成不同的資產模式（Asset Model）

現代控制系統是透過複雜的資通信網路連接，具有許多互連元件，執行各種任務以安全有效地運作化工廠、汽車零部件製造廠、管道、發電設施、輸配電網路以及許多其他類型的工業設施、運輸系統和實用製程。

過去這些在 OT 環境系統與企業 IT 環境中的其他資通信系統是相互隔離，並使用專有硬體、軟體和網路協議。由於其成本優勢，IACS 系統供應商已經採用商用現成產品（Commercial Off-The-Shelf, COTS）資訊技術，並且業務需求推動了控制系統與業務資訊系統的整合，因此不再是 IT 與 OT 實體隔離情況。

從安全角度來看，關注的是控制設備本身、該設備的使用者，控制系統元件之間的連接以及與業務系統和其他網路的互連的風險及控制措施。

本指南適用於多個產業領域中使用的各種工控物聯網。因此，資產模型必須從較高階層開始，並且足夠一般以適應部署控制系統的許多情況可以參考圖 5

圖 5 一般製程資產模型範例

由於網路在安全性方面發揮著重要作用，因此資產模型明確包含網路元素通常出現在層次結構的每個層級。 在每個層級設備（或設施）是通過適當類型的網路連接在一起。 雖然網路本身可能是相互關聯的在一起，這個模型沒有描述這種聯繫，這種表達方式容易識別被網路區隔與連接的資產的風險。

與參考模型的情況一樣，SCADA 應用程式的視圖略有不同。 一個典型的 SCADA 資產模型如圖 6 所示。

圖 6 SCADA 的資產模型

資產模型描繪了可能存在於個別層面的輔助資訊系統層次結構。 這些系統不直接控制生產製程，而是通過控制設備進行互動從中收集資料，或是反向發送配方和生產指指令。 線路、區域和站點資訊系統還充當資料庫，為整個企業的使用者提供生產資訊，可以與在企業資料中心中運作的企業資源規劃（ERP）應用程式進行互動。

可以根據需要收摺或擴展模型，以反映所檢視的實體，前提是它與其他模型和視圖比例一致。 例如，只有一個區域的工廠可以省略區域分類，前提是參考架構和後續區域反映了收摺資產模型。以下為從大範圍至單點不同比例的視圖：

2.1.2.1 企業(Enterprise)

企業是生產和運輸產品或營運和維護基礎設施服務的商業實體。 企業通常連接到網際網路以與其他企業進行通信或向員工提供資訊和服務（如電子郵件、入口網頁、客戶服務系統）。 企業通常營運一個或多個資料中心或

是使用雲端服務以支援其資訊處理要求。 這些 IT 資產支援的業務流程的安全性超出了本指南的範圍。本指南僅限於討論與 OT 環境有實體連線或是資料流相關的內外部系統及服務。

2.1.2.2 地理位置站點（Geographic Sites）

站點是企業的實體、地理或邏輯資產群組的子集合。 它可能包含區域、生產線、製程單元、製程單位、控制中心和自動運送車輛。 站點可以通過廣域網路（WAN）連接到其他站點。 站點可以包括資訊系統，例如協調站點的生產活動的製造執行系統(MES)。

2.1.2.3 控制中心（Control Center）

控制中心是一種特殊的站點。 基礎設提供商通常使用一個或多個控制中心來監督或協調其運作情形。 如果企業具有多個控制中心（例如：位於單獨站點的備份中心），則它們通常通過 WAN 連接在一起。 控制中心包含 SCADA 主機和相關的操作員顯示設備以及諸如歷史記錄的輔助資訊系統。

2.1.2.4 遠端站點（Remote Site）

遠端站點包含可程式邏輯控制器（PLC）、遠端終端單元（RTU）或智慧電子設備（IED）形式的設備，負責監視和控制站點本地的操作。 遠端站點通過通信網路（有時稱為遙測網路）連接到控制中心。 遠端站點也可以彼此連接（以便促進如各電力傳輸網格中的變電站之間的保護中繼的功能）。

2.1.2.5 區域(Area)

區域是站點的實體環境、地理位置或邏輯資產群組的子集合。 它可能包含生產線、生產細胞和生產單元。 區域可以通過站點 LAN 彼此連接，並且可以包含與在該區域中執行的操作相關的資訊系統。

2.1.2.6 生產線、單元、細胞及車輛（Lines, Units, Cells, Vehicles）

區域內由執行製造，基礎設施控制或自動運送車輛功能的較低層級元素組成。 該層級的實體設備可以通過有無線區域控制網路連接在一起，並且可以包含與在該實體中執行的操作相關的資訊系統。

2.1.2.7 監控設備（Supervisory Control Equipment）

監控設備包括 IT 伺服器、HMI、區域網路和通信設備，允許操作員遠端監控和控制分佈在廣泛地理區域的設施。

2.1.2.8 控制設備（Control Equipment）

控制設備包括 DCS、PLC、動作控制器、智慧驅動器以及用於管理和控制製程的相關操作員界面控制台。 它還包括現場總線網路，其中控制邏輯和演算法在協調其動作的智慧功能在現場設備上執行。

2.1.2.9 現場 I / O 網路

現場輸入/輸出（Input/ Output, I/O）網路是將這些元件連接到控制設備的通信鏈路（有線或無線）。

2.1.2.10 感應器和執行器（Sensors and Actuators）

感應器和執行器是連接到製程設備的終端元件。

2.1.2.11 受控制設備(Equipment under Control, EUC)

控制系統的資產以下是構成受控設備的資產，如生產機台、化學反應爐、工業機器人等。 該層級也稱為實體或製造或作業過程。

2.1.3 實體參考架構

實體參考架構是根據資產模型中定義的以元件層級視圖的個別實體構建的。參考架構是針對每種情況進行檢視，具體針對資產間的關聯性以直觀方式對資產間的相對位置及關連進行描繪與標示。 每個組織建立一個或更多參考體系結構取決於所執行的業務功能所需的系統、元件及相連的管道的總和。 組織通常具有單一的參考架構已被概括為涵蓋所有營運設施的公司。 每個設施或設施類型可以還有一個更詳細的參考網路架構圖，擴展了企業模型。
圖 7 中示出了用於製造功能的簡化參考架構的圖例

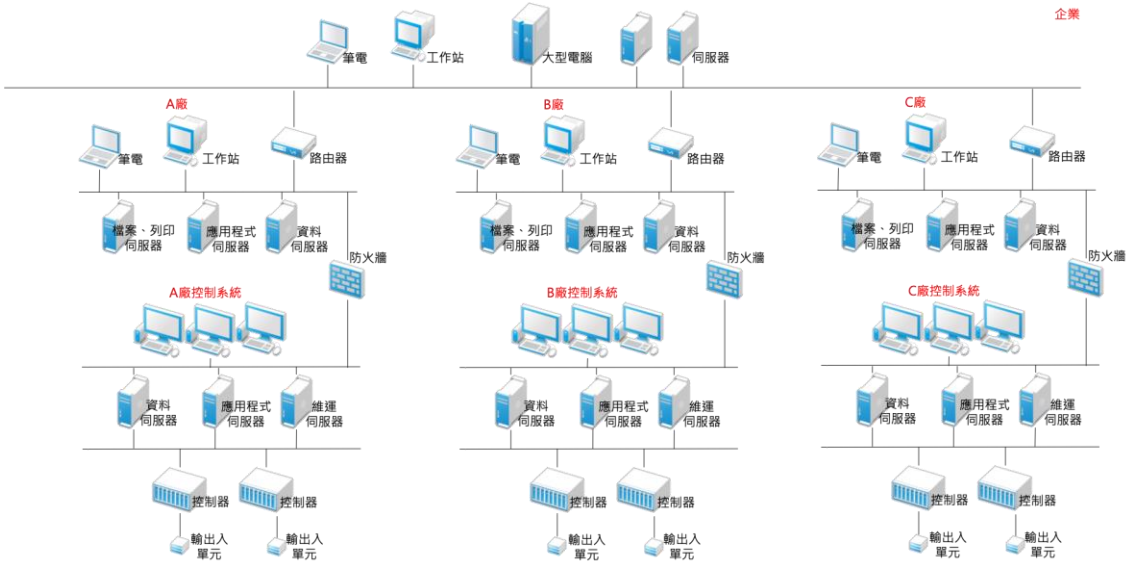


圖 7 實體參考架構示意圖

2.1.4 安全區域與管道模型(Zone and Conduit Model)

從參考架構可以更進一步發展為「安全區域和管道模型」。 它用於描述邏輯企業內部資產的群組或企業的子集合。 資產群組為實體（例如，業務、設施、站點或 IACS）然後可以針對安全政策進行分析要求。 該模型有助於評估常見威脅，弱點和對應的威脅達到保護安全目標所需的安全水準（SL-T）所需的對策分組資產。 通過以這種方式對資產進行分組，可以為所有資產定義安全政策該區域的成員。 然後可以使用該分析來確定所需的適當保護基於在區中執行的活動。

2.1.4.1 界定安全區域

在構建安全計劃時，定義安全區域是安全計畫成功的最重要步驟與要素之一，也是正確定義生產製程的最重要或關鍵區域的工作。 當定義安全區域時，組織必須確保使用參考架構和資產模型來開發適當的安全區域和安全層級，以滿足工控物聯網系統安全政策中建立的安全目標。
當在同一個實體設備（裝置）中執行不同層級的活動時，組織可以將實體設備（裝置）對應到更嚴格的安全要求，或者建置具有獨立的區域安全政策的獨立區域，該政策是兩個區域之間的混合政策。 這種情況的典型實例發生在製程歷史記錄伺服器中。 為了有效，伺服器需要存取作為要收集的資料源的

關鍵控制設備。 但是，為了滿足向主管和流程優化團隊提供資料的業務需求，需要比典型的控制系統安全要求允許更自由地存取設備。

如果涉及不同層級活動的多個應用程式在單一實體設備上運作，則還可以建立邏輯區域邊界。 在這種情況下，對特定應用程式的存取僅限於具有該應用程式等級權限的人員。 一個例子是運作伺服器和基於客戶端的分析工具的單台機器。 只有具有更高等級權限的人員才能存取伺服器，而所有員工都可以使用客戶端插件存取電子表格。

2.1.4.2 區域識別

區域可以是一組獨立資產，一組子區域，也可以是獨立資產和資產的組合，這些資產和資產也分組為主區域中包含的子區域。 區域具有繼承的特徵，這意味著子區域必須滿足父區域的所有要求。 簡化的多重樹狀區域模型如圖 8 所示。這裡企業區域是父級，每個工廠是子區域或子子區域，控制子區域包含在工廠子區域。

將安全區域與設施中的實體區域或區域對齊具有明顯的優點 – 例如，將控制中心與控制安全區域對齊，可以看出其父子階層的繼承關係。

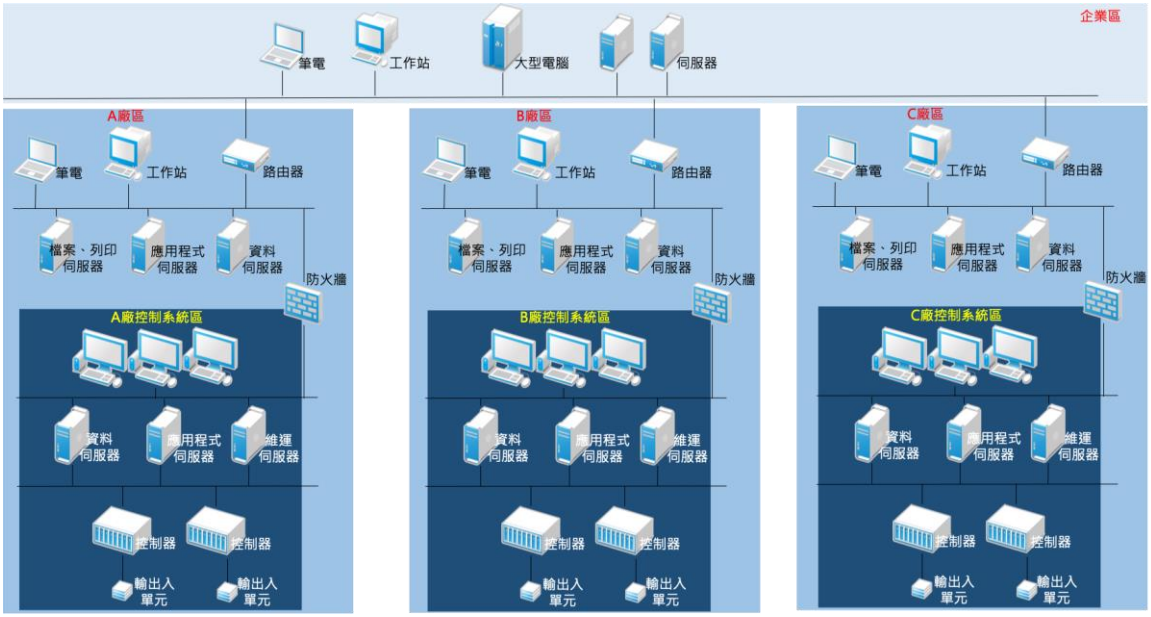


圖 8 多重區域系統架構圖

可以將相同的企業體系結構分組到單獨的區域中，如圖 9 所示。在此模型中，區域政策是獨立的，每個區域可能具有完全不同的安全政策。

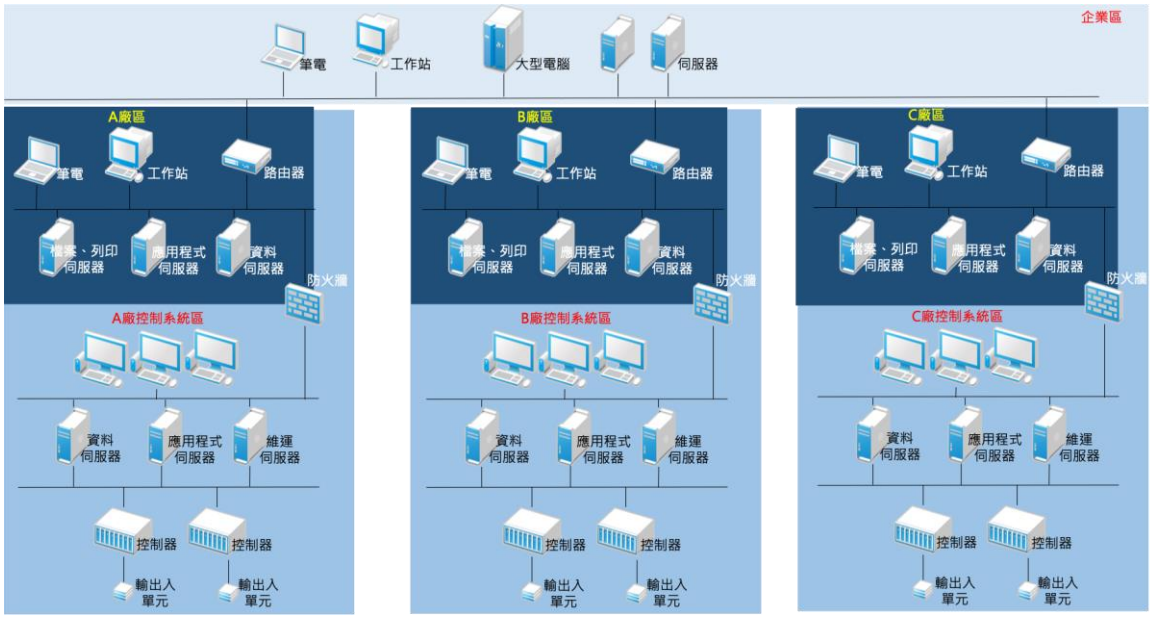


圖 9 各自獨立區域範例

以同一個 SCADA 架構可以前述範例描繪如圖 10 及圖 11：

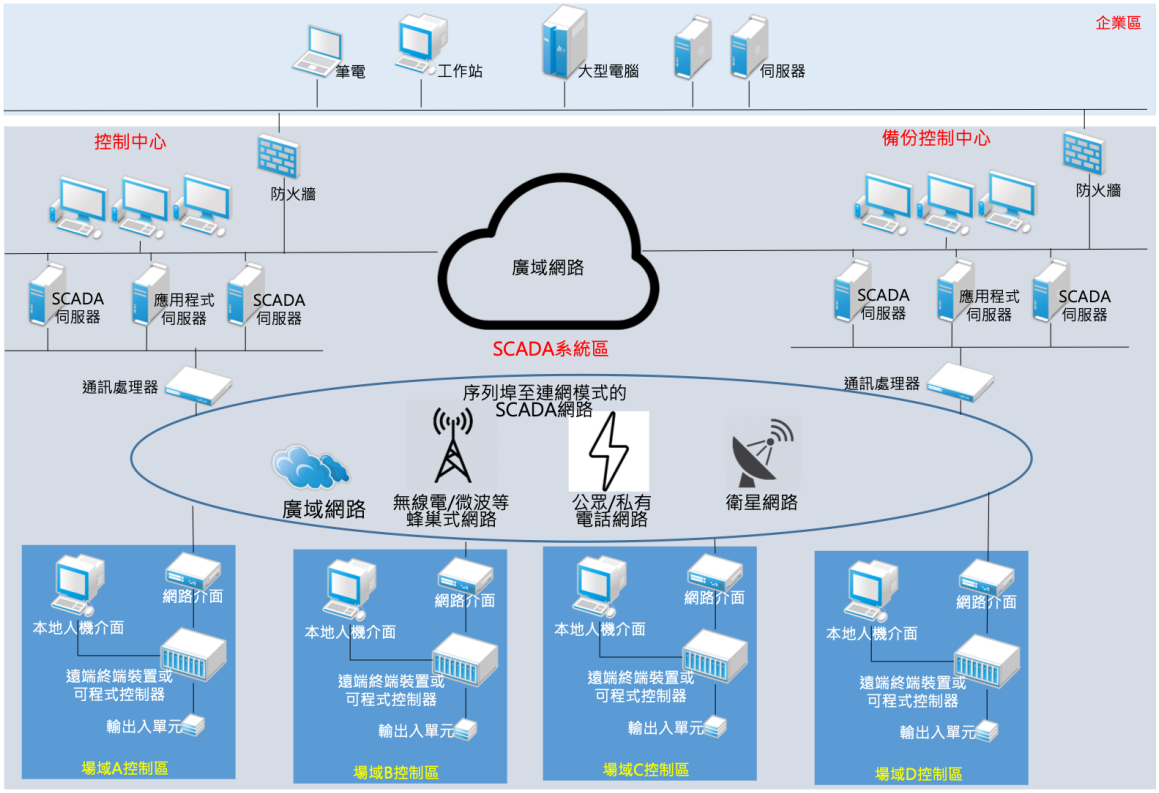


圖 10 SCADA 安全區域繼承政策實例

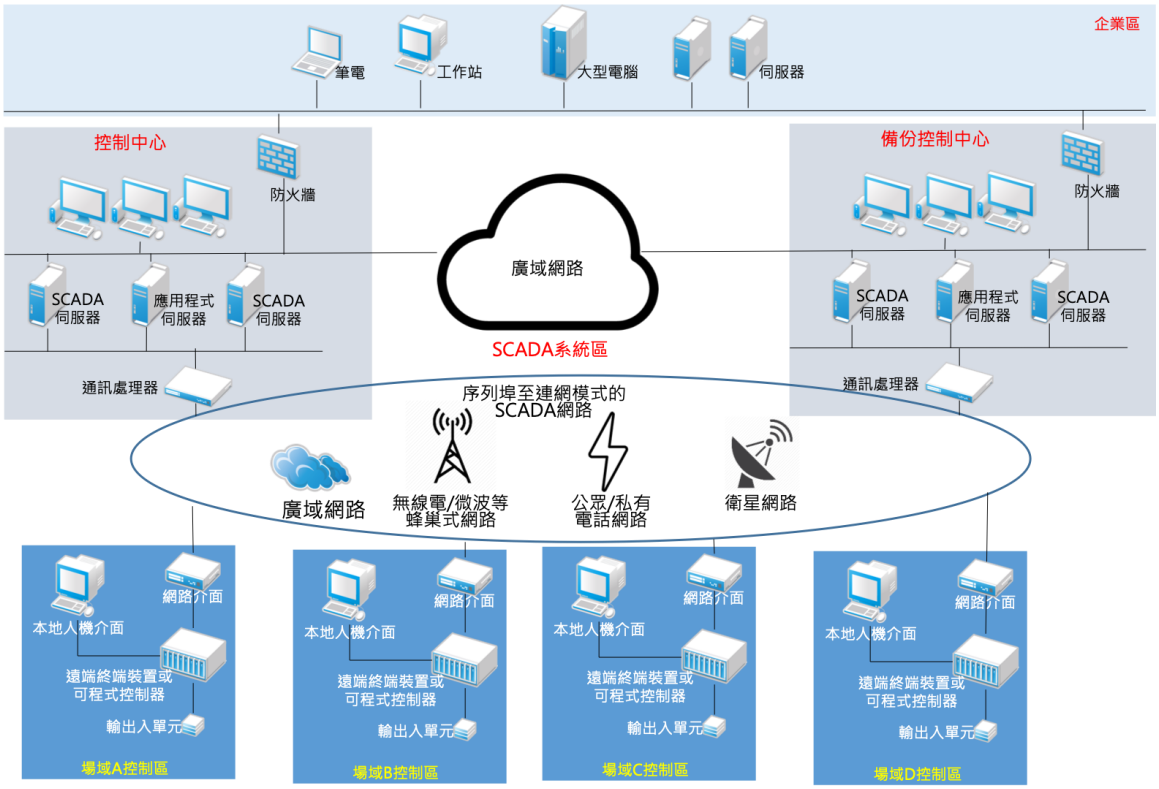


圖 11 SCADA 安全區域獨立政策實例

2.1.4.3 區域特性(Zone Characteristic)

每個區域都有一組特性和安全要求，這些特性是其屬性， 表達採取下到形式：

a）安全政策

b）資產盤點

c）存取要求和控制

d）威脅和弱點

e）安全弱點的後果

f）授權可應用技術

g）變更管理流程。

以下段落中更詳細地描述了這些屬性。

2.1.4.3.1 安全政策

每個區域都有一個控制文件，用於描述總體安全目標以及如何確保滿足目標安全等級。 這包括：

a）區域範圍

b）區域安全等級

c）執行安全政策的組織結構和職責

d）與該區域相關的風險

e）達成所需目標的安全政策

f）要執行的安全措施

g）區域內允許的活動類型

h）允許存取該區域的通信類型

i）區域屬性的文件。

所有上述內容都記錄在案並組合到區域安全政策中，該政策用於指導和測量區域內包含的資產的建構和維護。

2.1.4.3.2 資產盤點

為了維護區域內的安全性，組織必須維護所有資產（實體和邏輯）的列表。此列表用於評估風險和弱點，並確定和維護達成安全政策目標所需的適當安全措施。盤點準確性是達成安全政策中規定的安全目標的關鍵因素。 當區域內的資產發生異動或連接管道、通信方式發生改變時，以及將新資產添加到區域以確保滿足該區域安全目標時，必須更新列表。
實體資產和元件是區域中包含的實體設備。 舉例包括如下：
a）電腦硬體（例如，工作站，伺服器，儀器，控制器，電源，磁盤驅動器或磁帶備份）
b）網路設備（例如，路由器、交換機、集線器、防火牆或實體電纜）
c）通信鏈路（例如，總線、鏈路、調製解調器（Modem）和其他網路介面、天線）
d）存取認證和授權設備（例如，網域控制器、網路存取控制伺服器、資料讀取器和影像掃描器等）
e）開發系統硬體
f）模擬和訓練系統硬體
g）外部系統硬體
h）備品盤點
i）監視和控制設備（例如，感應器、開關和控制器）
j）參考手冊和資訊。
邏輯資產包括區域中使用的所有軟體和資料。 舉例如下：
a）電腦系統軟體（例如，應用程式、作業系統、通信介面、配置表、開發工具、分析工具和實用程序）
b）作業系統和應用程式工具集的修補和升級
c）資料庫
d）資料檔案
e）設備配置文件
f）為備份和復原目的而維護的軟體和資料的副本
g）設計基礎文件檔案（例如，功能要求包括資訊和資產、安全分類和保護等級，實體和軟體設計、弱點評估、安全邊界、基準測試、裝配和安裝文件檔案）
h）供應商資源（例如，產品更新、修補、服務包、實用程序和驗證測試）。
2.1.4.3.3 存取需求及控制
就其性質而言，區域意味著存取僅限於可以存取的所有可能實體的一小部分。然後，區域的安全政策必須闡明區域滿足其業務目標所需的存取權限，以及如何控制此存取。

2.1.4.3.4 威脅和弱點評估

特定區域記憶體在威脅和對應的弱點。 組織必須識別和評估這些威脅和弱點，以確定導致區域內資產無法滿足其業務目標的風險。 記錄威脅和弱點發生的過程在作為區域安全政策一部分的威脅和弱點評估作業中。
存在許多可能的對策以降低威脅利用區域內的特定弱點的風險。 安全政策應概述在成本與風險權衡之間哪些類型的對策適合於滿足區域的目標安全等級。

2.1.4.3.5 授權可應用技術

隨著工控物聯網不斷發展以滿足不斷變化的業務需求，需要控制用於實施變更的技術。 這些系統中使用的每種技術都帶來了一系列弱點和對應的風險。為了最大限度地降低特定區域的風險，區域安全政策需要具有區域中允許的動態技術列表以及不允許的技術。如允許或不允許在生產線上使用無線區域網路傳輸資料及生產指令。

2.1.4.3.6 變更管理流程

需要一個正式且準確的流程來維護特定區域資產清單的準確性以及區域安全政策的更改方式。 正式流程可確保對區域的更改和添加元件不會危及安全目標。 此外，還需要一種適應不斷變化的安全威脅和目標的方法。 威脅和弱點及其相關風險將隨著時間的推移而發生變化。

2.1.4.4 界定管道

管道是適用於安全區域間特定通信過程。作為安全區域資產的邏輯分組（在這種情況下為通信資產）。安全管道保護它所包含通道的傳輸內容安全，以相同方式與實體管道保護電纜不受實體損傷。管道可以被認為是在一個區域內連接區域或用於通信的「通道」。內部（區域內）和外部（區域外）管道封閉或保護提供資產之間鏈接的通信「通道」（概念電纜）。最常見的是IACS 環境管道與網路相同。也就是說，管道是佈線、路由器、交換機與構成通信的網路管理設備所組成。管道可以是不同網路技術的分組，以及可以的通信通道發生在一台電腦中。管道用於分析通信威脅和區域內和區域之間的通信中可能存在的弱點。
管道可以被視為包含資料或提供實體連接的管道區域之間的溝通。管道可以具有子管道以提供一對一或一對多區域溝通。為管道提供安全通信可以通過以下方式達成實施適當的區域安全政策。

2.1.4.5 管道屬性

實體上，管道可以是連接區域以用於通信目的的電纜。
管道是一種不像有子區域的區域; 也就是說，管道不是由子管道組成的。管道由共享特定通信通道的所有區域的列表定義。 兩個實體設備間使用管道中包含的通道的設備和應用程式定義管道端點。該企業管道在圖 12 中突出顯示。

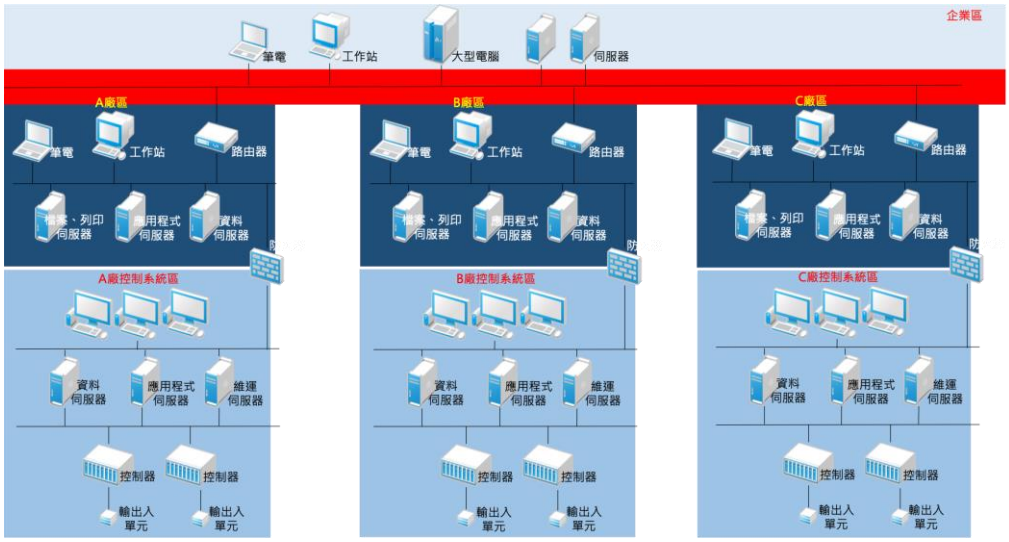


圖 12 企業連接管道

與區域一樣，可以構建類似的視圖以用於 SCADA 應用程式。 一個例子是如圖 13 所示。

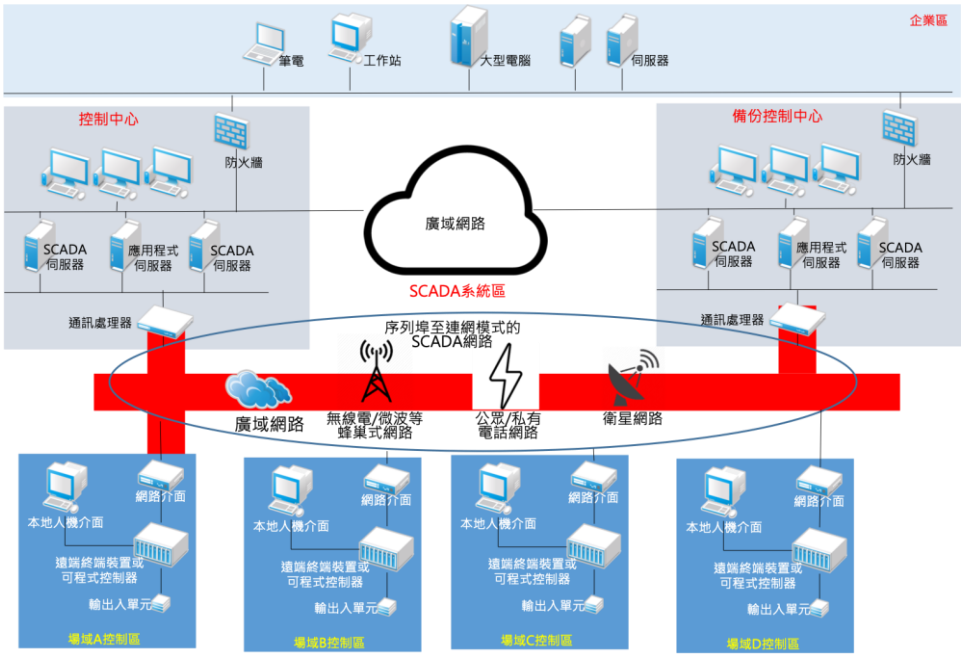


圖 13 SCADA 的管道案例

與區域一樣，每個管道都有一組特性和安全要求，這些特性是其屬性。採取以下形式：

a）安全政策
b）資產盤點
c）存取要求和控制
d）威脅和弱點
e）安全弱點的後果
f）授權可應用技術

g）變更管理流程
h）連接區域。

2.1.4.5.1 安全政策

每個管道都有一個控制文件，描述總體安全目標以及如何確保滿足目標安全等級。 本文件包括：
a）管道範圍
b）管道安全等級
c）實施管道安全政策的組織結構和責任
d）與管道相關的風險
e）達成所需目標的安全政策
f）要執行的安全措施
g）管道內允許的通道類型
h）管道屬性的文件。

所有上述內容都記錄在案並彙總到管道安全政策中，該政策用於指導和衡量管道內所含資產的建置和維護。

2.1.4.5.2 資產盤點

與區域盤點一樣，需要準確的通信資產列表。

2.1.4.5.3 存取要求與控制

就其性質而言，管道意味著存取僅限於可以存取的所有可能實體（Entity）的有限集合。 然後，管道的安全政策必須闡明管道所需的存取以達成其業務目標，以及如何控制該存取。

2.1.4.5.4 威脅和弱點評估

特定管道存在威脅和對應的弱點。 組織必須識別和評估這些威脅和弱點，以確定導致管道內資產無法滿足其業務目標的風險。 記錄威脅和弱點的過程發生在作為管道安全政策一部分的威脅和弱點評估中。

存在許多可能的對策以降低威脅利用管道內的特定弱點的風險。 安全政策應概述在成本與風險權衡中哪些類型的對策是適當的。

2.1.4.5.5 授權可應用技術

隨著工控物聯網不斷發展以滿足不斷變化的業務需求，需要控管未經風險評估用於實施變更原有管道運行中技術。 這些系統中使用的每種技術都帶來了一系列弱點和對應的風險。 為了最大限度地降低特定管道的風險，管道安全政策需要具有管道中允許的動態技術列表。

2.1.4.5.6 變更管理流程

需要一個正式而準確的流程來維持特定管道政策的準確性以及如何進行變更。正式流程可確保管道的更改和添加不會危及安全目標。 此外，還需要一種適應不斷變化的安全威脅和目標的方法。 威脅和弱點及其相關風險將隨著時間的推移而發生變化，需要持續更新對既有管道的衝擊及對策。

2.1.4.5.7 連接區域

根據與其連接的區域來描述管道。

2.1.5 模型間關聯

前幾節描述的模型彼此相關，並與政策、程序和構成安全計劃的指南。 這些關係如下圖 14 所示，形成一個生命週期的循環，彼此互相校準，使得將複雜的工控物聯網環境，透過 Top-down 的政策與程序與 bottom up 聚集為區域的資產，能簡化管理，並能快速定位出工控物聯網的脆弱點，而以各項控制措施，降低弱點被利用的風險。

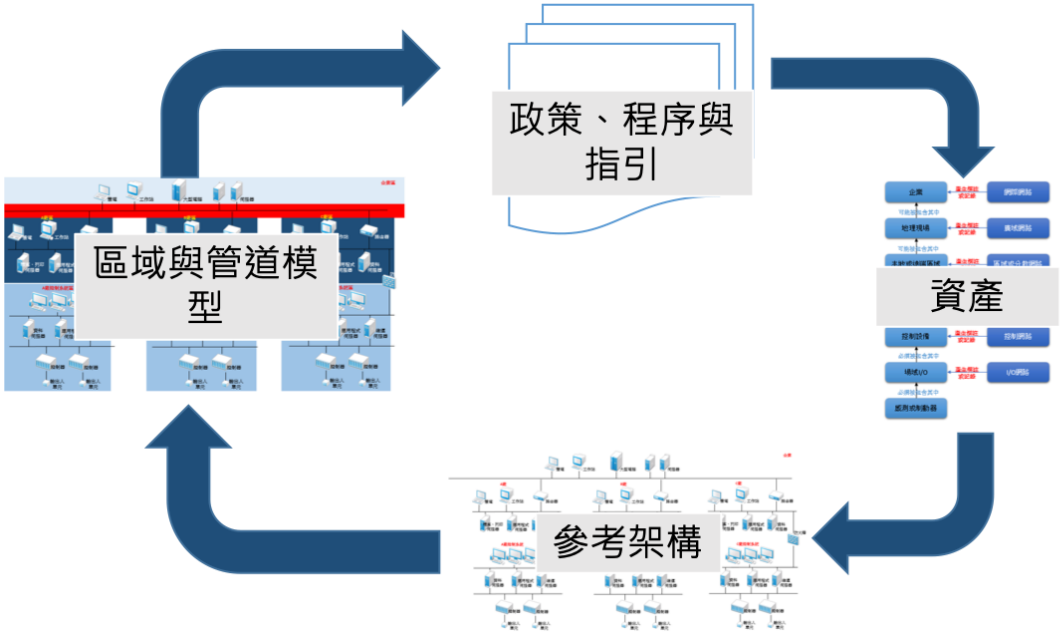


圖 14 參考架構模型間關聯示意圖

2.2 工控物聯網資安風險

2.2.1 工控物聯網系統的資安案例

2.2.1.1 Stuxnet 蠕蟲事件

資訊安全廠商趨勢科技 2010 年 10 月 6 日針對一隻已經危害全球各地許多電腦、名為 Stuxnet 的蠕蟲惡意程式提出嚴重警訊。該惡意程式的特徵是會自動自我複製，其主要攻擊目標是例如發電廠、煉油廠中的自動化生產與控制（SCADA）系統，同時 SCADA 系統的主要製造商西門子公司亦已警告客戶該隻惡意程式會藉由 USB 設備和網路共享進行蔓延。

Stuxnet 的蠕蟲是世界上首隻攻擊西門子 SIMATIC WinCC 與 PCS 7 系統的病毒，目的在取得 WinCC SQL Server 登入 SQL 資料庫的權限。其利用了微軟所公告一可允許遠端執行程式碼的 MS10-046 Windows 系統弱點進行散佈。

Stuxnet 是一個蠕蟲型的惡意程式，可透過已感染的 USB 等可卸除式裝置進入電腦，專門攻擊 Windows Shell 當中的一個弱點（請參考 Microsoft 資訊安

全公告 MS10-046)。此弱點會讓惡意程式入侵一些所謂的「監控與資料擷取」(SCADA) 系統，如電力公司或能源煉解廠用來控制生產和營運的系統。
Stuxnet 的最主要目標是電力公司的 SCADA 系統，因此，SCADA 系統的主要製造商西門子 (Siemens) 已經對使用者發出此病毒的警告通知，因為它也會攻擊西門子的 WinCC 系統。
2010 年 11 月 Stuxnet 蠕蟲攻擊伊朗核電廠，鎖定水庫、油井、電廠等重要基礎設施。大多數 Stuxnet 的攻擊目標出現在伊朗，引發意圖破壞核子設施的陰謀論說。毫無疑問的是，Stuxnet 是一款高度精良的惡意軟體，其資源，不管是在時間，金錢或人力上其皆十分充裕地被運用來發展。
我們依據國際著名資安研究機構 SANS 於 2015 年 10 月由 Michael J. Assante and Robert M. Lee 發佈的有關 Stuxnet 蠕蟲的的 IACS 擊殺鏈 (Kill Chain) 分析報告，將 Kill Chain 描繪在 PERA 模型上，依圖 15 所示。

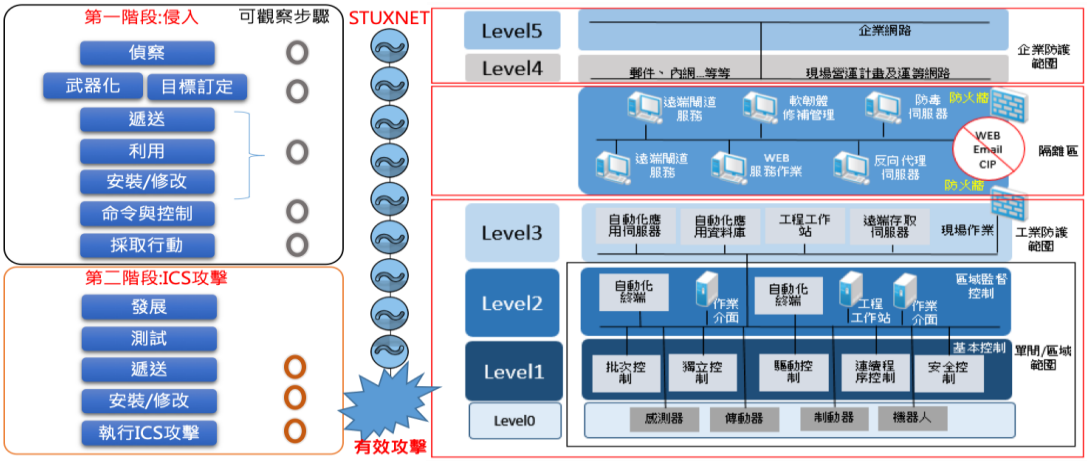


圖 15 Stuxnet 蠕蟲的 Kill Chain

由上圖可見，主要攻擊過程經過 2 個階段，第一階段是在 IT 環境進行滲透，主要目的是建立可供後續攻擊的命令與控制 (Command and Control, C&C) 中繼站。第 1 階段的攻擊參考模型，如圖 16

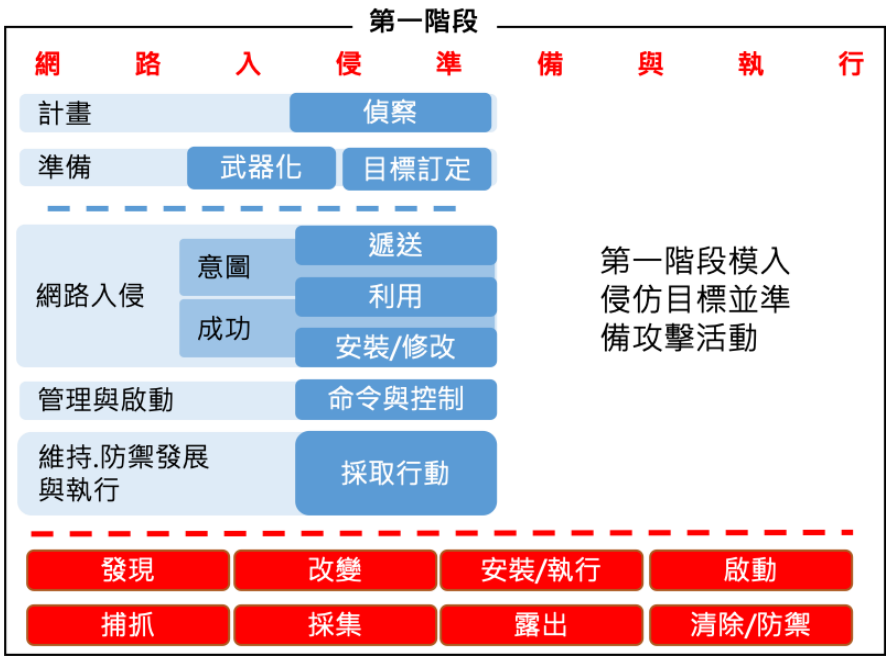


圖 16 Kill Chain 第 1 階段 Cyber Attack 攻擊準備與執行模型

第 1 階段步驟 1：規劃

在第 1 階段的攻擊中，規劃是第一階段的第一步驟，包括進行偵察。偵察是通過觀察或其他檢測方法獲取有關某事物的資訊的活動。網路攻擊計劃和偵察通常包括對目標進行研究，通常使用 Google 和 Shodan 等開源資訊收集工具，以及搜索公開資料，如公告和社交媒體資料。

規劃階段的目標是揭示弱點並識別支授攻擊者努力瞄準的標的，交付和利用系統元素的資訊。可能對攻擊者有用的資訊類型可以包括人員、網路、主機、帳戶和通信協定資訊，以及有關政策，過程和過程的資訊。

IACS 的規劃和偵察還可以包括諸如研究 IACS 技術弱點和功能或了解製程和操作模型如何易受剖析等活動。被動偵察技術（通常稱為足跡踩點）可以利用網際網路上可用的大量資訊來開發有關目標的資訊而不被觀察到。偵察通常包括主動對應目標的公共或私人可存取的攻擊面，模式化活動以及通過例行查詢確定作業系統軟體的版本。

攻擊者還可以嘗試隱藏在預期的網際網路流量和活動的雜訊中。有關組織的公開資訊有助於確定攻擊者可用的目標選項，而防禦者無法選擇的一件事是他們的組織是否值得成為被攻擊的目標。

第 1 階段步驟 2：準備

準備是第 1 階段的第 2 步駭，可以包括武器化或目標定位。武器化包括修改其他無害的文件，例如電腦檔案，以便作為攻擊者的下一步。很多時候，武器化表現為文件，例如 PDF，其中包含弱點利用。但是，武器化電腦檔案可能只是以惡意方式利用可用功能，例如，作為 Word 電腦檔案中的巨集。

定位目標也可以在第二階段進行，並且當攻擊者或其代理（例如腳本或工具）識別潛在的受害者時進行標定方向。以現代軍事用語來說，目標是分析目標並確定目標的優先次序，並將適當的致死和非致命行動與這些目標相匹配，以創造特定的預期效果。網路攻擊者根據在一段時間內所需的努力，技術成功的可能性和風險之間的權衡來決定他們將對目標使用什麼攻擊工具或方法檢測。例

如，在偵察之後，攻擊者可以確定進入環境的虛擬專用網路（VPN）是防禦者網路的正確部分，因為它可能是以最少的資源支出來達成其目標的最佳方法。武器化和定位都可以發生，但兩者都不是必需的。在 VPN 攻擊案例中，攻擊者可以識別直接登錄網路的憑據並繞過武器化的需要。同樣，攻擊者可以將功能武器化到多個目標，而無需專門針對任何特定目標，只有在獲得初始存取權限後才能選擇所需目標。

第 1 階步驟 3：入侵

要獲得初始存取權限，需要第 1 階段的第 3 步驟，稱為網路入侵。入侵是攻擊者成功或不成功的任何嘗試，以獲得對防禦者網路或系統的存取權。這包括投射武器步驟，其中攻擊者使用一種方法與防禦者的網路進行互動。例如，網路釣魚電子郵件將成為攻擊者的武器化 PDF 的傳遞機制，或者 VPN 會將攻擊者直接傳遞給網路。下一步，即弱點利用步驟，是攻擊者用來執行惡意操作的手段。當 PDF 或其他文件打開時，該手段可能是對弱點的利用，或者可能是利用對網路的現有存取，例如使用 VPN 的憑證。當攻擊成功時，攻擊者將安裝諸如遠端存取特洛伊木馬之類的功能。攻擊者還可以修改現有功能。例如，在較新的 Windows 環境中，PowerShell 工具為攻擊者提供了足夠的功能，使他們無需依賴惡意軟體來執行入侵。防禦者應該專注於發現和理解威脅，並且不應該總是假設威脅僅是基於惡意軟體的。

第 1 階段步驟 4：維持權限及運用

隨著網路入侵的成功，攻擊者將進入下一階段，維持權限及運用取得特權。這裡攻擊者將使用這樣的方法建立命令和控制（Command & Control, C2）作為與先前安裝的功能的連接或濫用可信任通信（例如 VPN）。有能力且持久的攻擊者經常建立多個 C2 路徑，以確保在檢測到或移除連接時不會中斷連接。值得注意的是，C2 方法並不總是需要支援高頻率雙向通信的直接連接。例如，某些對受保護網路的存取可能依賴在單向通信路徑上，需要更多時間將資訊移出並傳送命令或程式碼。攻擊者通常通過隱藏正常的出站和入站流量來建立 C2，從而劫持現有通信。在某些情況下，攻擊者通過植入設備建立自己私密的通信管道來建立 C2。通過維持權限及運用存取環境，攻擊者現在可以開始達成其目標。維持、隱藏、開發和執行階段記錄了許多攻擊者可能擁有的最終目標。在這個階段，攻擊者行動起來將完整製作目標清單，作為下一步的攻擊目標。

每個攻擊者的行為都很難偵測並處理;然而，常見的活動包括發現新系統或資料，在網路周圍進行橫向移動、安裝和執行其他功能，啟動這些功能，捕獲傳輸通信（如使用者憑證），收集所需資料，從中挖掘出來的資料。攻擊者善於利用環境和反數位鑑識技術，如清除攻擊活動的痕跡或在遇到事件應變人員等防禦者時捍衛自己的立足點，以避免被發現遭清除，造成擊殺鏈的中斷。

這可能是規劃和執行 IACS Cyber 擊殺鏈第 2 階段的關鍵階段。有關 IACS 以及工業製程、工程和營運的大量資訊存在於面向 Internet 的網路（如企業網站或企業辦公網路）中。是非常重要的是，維護者應評估受保護較少的網路中存在哪些資訊和工具，以幫助防止攻擊者試圖破壞 IACS。同樣重要的是要注意，攻擊者可以針對供應商或合作夥伴網路執行第 1 階段以獲取必要的資訊，例如 IACS 項目文件傳遞路徑或系統整合商或供應商到 IACS 的遠端存取鏈接。當攻擊者成功破壞了 IACS 的安全性並且能夠繼續進入第 2 階段時，第 1 階段的攻擊活動可以告一段落。

重要的是要強調，如果防禦者擁有網際網路，這個階段可以被繞過 ，從成功受到攻擊的第三方面臨 IACS 元件或有關 IACS 和流程的資訊。
很大一部分惡意軟體和網路入侵發生在第 1 階段，因為這是最有可能發生國家級情報和間諜活動的地方。
在許多情況下，根據攻擊者目前的目標，進行間諜活動的價值明顯高於實施包括破壞或操弄系統在內的實際攻擊的價值。如果持久存取符合國家安全或軍事目標或犯罪目標，攻擊者可以在以後啟動後續行動。因此，即使沒有直接的危險或業務影響，識別和糾正攻擊者情報工作也很重要。
使 IACS 網路攻擊與傳統 IT 網路攻擊截然不同的原因在於 IACS 元件由底層工程和製程構成，並以獨特的方式和配置進行設計，攻擊者需對設計方式擁有廣泛的知識，以便在有意義的情況下對其產生影響。此外，在正確構建的 IACS 中，有許多層系統和檢測感應器，攻擊者必須在第 1 階段中廣泛地偵察以獲得對 IACS 元件的存取權限。不幸的是，不正確設計或貪圖便利防禦者直接將 IACS 連接到網際網路顯著破壞了正確構建的 IACS 在安全性方面的固有優勢。
為了繼續利用這些固有的防禦性架構，防守者必須在連網設計以及選擇如何整合系統時要謹慎。例如，將安全系統整合到與營運相同的網路中可以顯著減少攻擊者為完全破壞系統而花費的精力。它還使防禦者更難以識別和修復攻擊。這種失敗的防禦架構加上同時增加的攻擊機會導致 IACS 安全性大幅下降。通過正確構建的 IACS，即使傳統上沒有設計安全性的環境（這可能是一個重大問題）也不容易以有意義和可預測的方式產生影響。這個問題在 IACS 攻擊的第 2 階段可視化可獲解決。
在第 2 階段，攻擊者必須使用在第 1 階段獲得的知識來專門開發和測試能夠有意義地攻擊 IACS 的能力。 不幸的是，因為對於敏感設備，第 1 階段攻擊者操作可能會導致意外攻擊。 這對於國家級的網路行動來說是一個重大風險，因為這種攻擊可能被認為是有意的並且具有不可預見的後果，而提早暴露在防禦者的雷達之下。 例如，嘗試主動發現 IACS 網路上的主機可能會中斷必要的通信或導致通信卡板失敗。 與 IACS 應用程式和基礎架構元素的簡單互動可能會導致無意的結果。 此活動仍將包含在第 1 階段內，並且在執行步驟中會產生意外影響。 蓄意攻擊發生在第 2 階段，如圖 2 所示。

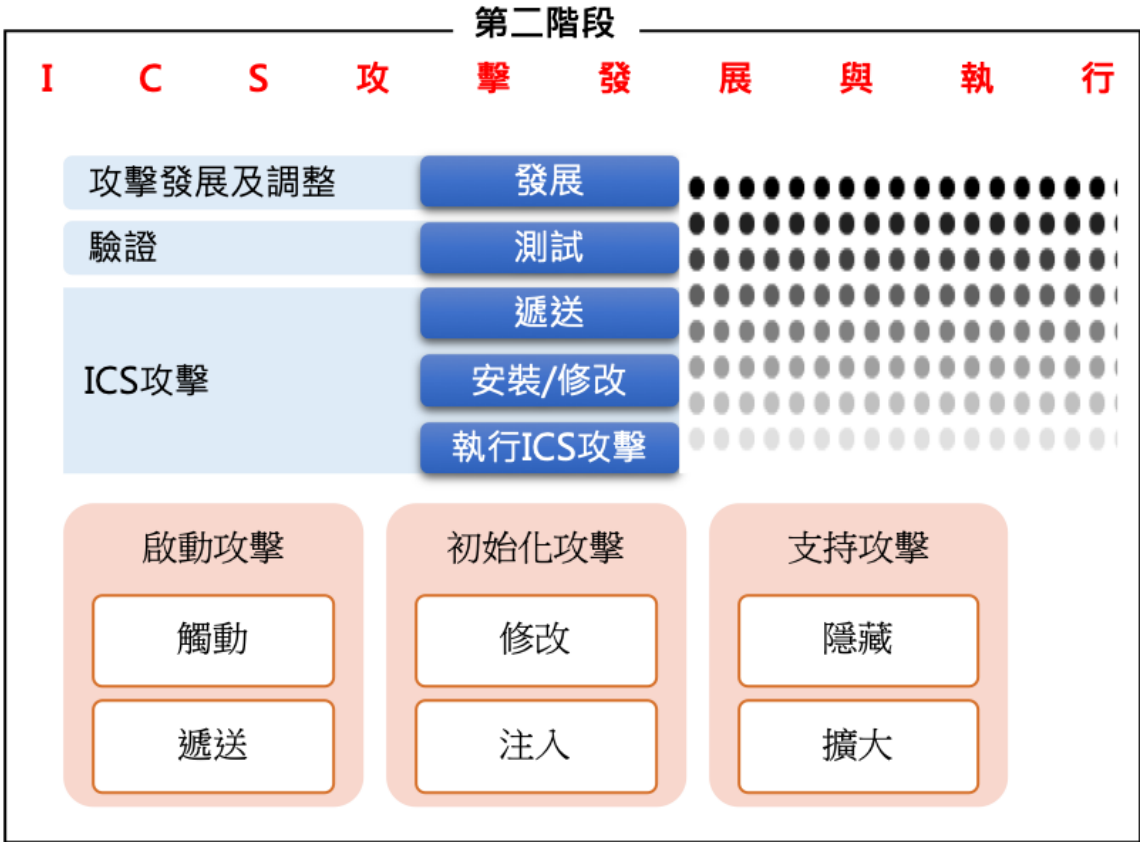


圖 17 第 2 階段 IACS 攻擊發展與執行

第 2 階段步驟 1：攻擊開發和調校

第 2 階段從攻擊開發和調校步驟開始，其中攻擊者開發了一種新的功能，以適應特定的 IACS 實施和所需的影響。 這種發展很可能是通過滲透的資料進行的。只有對系統所有者和操作員能夠觀察其行為能力的低評價的無恥攻擊者才會通過即時生產環境測試來試驗和發展他們的攻擊。 因此，在正常情況下，攻擊者的開發和調整尤其難以檢測。 由於需要延長開發和測試時間，第 1 階段和第 2 階段攻擊之間可能還存在長時間的潛伏期。

第 2 階段步驟 2：驗證

一旦攻擊者開發了一種可行攻擊手法，下一階段就是驗證階段。 在這裡，如果具有能力實施任何有意義且可靠的影響，則攻擊者必須在類似或相同配置的系統上測試其實施攻擊能力。 即使是簡單的攻擊，例如增加對系統阻斷服務的網路掃描，也需要進行一定程度的測試，以確認掃描可以阻斷對系統的服務。 但是，對於更重要的影響，可能需要更大規模測試，其中攻擊者可能獲得實體 IACS 設備和軟體元件。 雖然大多數維護者很難洞察 IACS 供應商社群，但各種政府組織可以利用他們的來源和方法來識別此類設備的異常收購，這可能表明已經建立的第 1 階段成果來實施的第 2 階段攻擊。

第 2 階段步驟 3：IACS 攻擊

最終，最後階段是 IACS 攻擊，攻擊者將在其中提供非預設功能，安裝或修改現有系統功能，然後執行攻擊。攻擊可能有許多方面（預備或併發攻擊）屬於啟用，啟動或支援以達成其最終效果的攻擊類別。這些可能是必要的，以觸發操

弄製程的特定元素所需的條件，啟動製程設定點和變量的變化，或通過諸如欺騙狀態資訊等欺騙工廠操作員認為一切正常的政策來支援攻擊。
發起攻擊的複雜性取決於系統的安全性、監控和控制的製程，安全設計和控制以及預期的影響。例如，破壞 IACS 的簡單阻斷服務比以設計方式操作流程或能夠攻擊系統並且可以選擇重新攻擊（如圖 18 所示）更容易達成。攻擊者最終需要操弄製程造成重大傷害，包括可靠或可預測的實體破壞，破壞受控制的設備或製程元件，或修改，包括操弄配方、配方和混合物。

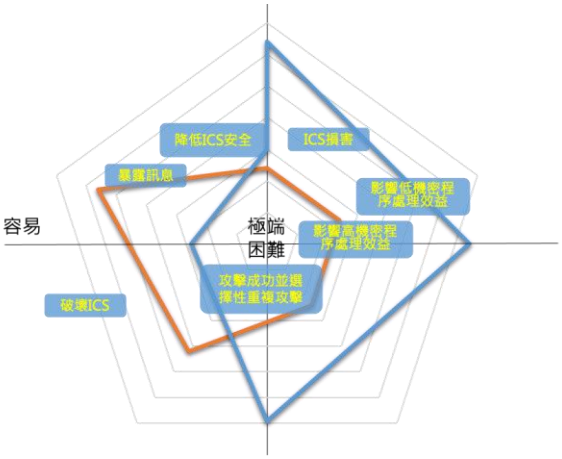


圖 18　IACS 系統攻擊困難度比較

雖然有各種方法來攻擊 IACS 環境，但達成功能影響的最常用方法分為三類：造成失能、阻斷和操弄。 它們包括：

- 失去檢視畫面、阻斷檢視畫面、操弄檢視畫面
- 阻斷控制、失去控制、操弄控制
- 啟動安全感應器和儀器、阻斷安全感應器和儀器，操弄安全和操弄感應器和儀器。

2.2.1.2 WannaCry 病毒事件

2018 年 8 月，台灣某半導體製造發生台灣廠區晶圓廠生產線嚴重當機事件，造成全臺主要晶圓廠都傳出產線當機事件。

依台灣著名 IT 媒體 ithome 媒體報導，該半導體製造公司過去向來是資安模範生，層層管制、嚴格把關的種種資安措施，甚至視為業界最高標準之一，任何一支 USB 都不能入廠，就連全球科技大廠執行長來臺參觀某半導體製造公司廠房時，都得在門口櫃臺繳出手機，筆電貼上封條，沒有例外。如此嚴密防護的某半導體製造公司，竟然也發生產線中毒事件，甚至災情擴散全臺廠房。這個訊息震驚了各界。病毒如何進入感染，也成了各界熱議的話題，USB 感染或外部駭客攻擊是外界推測出事的兩種可能原因。
後來該半導體製造公司首度出面回應，證實了機臺中毒的訊息，證實部分機臺遭受病毒感染。
這次病毒事件也造成公司出貨延遲，以及相關成本的增加，損失超過了新台幣 70 億元。

造成機台控制電腦中毒的病毒是在 2017 年造成全球災情的 WannaCry 病毒，WannaCry 被認為利用了美國國家安全局被駭客盜取的工具的「永恆之藍」（Eternal Blue）工具以攻擊執行 Microsoft Windows 作業系統的電腦。「永恆之藍」傳播的勒索病毒以 ONION 和 WNCRY 兩個家族為主。其利用了某些版本的微軟伺服器訊息區塊（SMB）協定中的數個弱點，而當中最嚴重的弱點是允許遠端電腦執行程式碼。修復該弱點的安全修補程式已經於此前的 2017 年 3 月 14 日發布，但很多電腦並沒有更新。前述半導體製造公司也坦承因人員的疏失，新機並沒有照標準作業程序在安裝在產線前進行更新，再加上新機臺連上公司內部電腦網路而導致病毒擴散。

2.2.1.3 自動挖幣惡意程式攻擊

一家日本的光學設備製造商在 2019 年 2 月底遭到自動化挖幣惡意程式攻擊，在遭受第一波攻擊時第前幾天即造成產量暴跌，造成這家在全球有 30 多個國家有業務的光學設備製造商的重要業務及生產用伺服器資源被大量用來進行加密貨幣的挖掘，造成無法接受訂單、無法進行生產排程，也無法開立發票，雖然惡意程式在第二波攻擊時被擊退，但是該公司在泰國的生產線版迫關閉 3 天，兩座工廠的產能降低至原來的 40%，據日本當地報導該公司到 3 月底也未能恢復正常的產能運作。
據國際知名的趨勢科技的調查，該自動化病毒是由 internet 先感染辦公室區域（OA Zone）再透過工廠區（Factory Zone）間的連線，感染到生產場域，攻擊路徑的示意圖，如圖 19

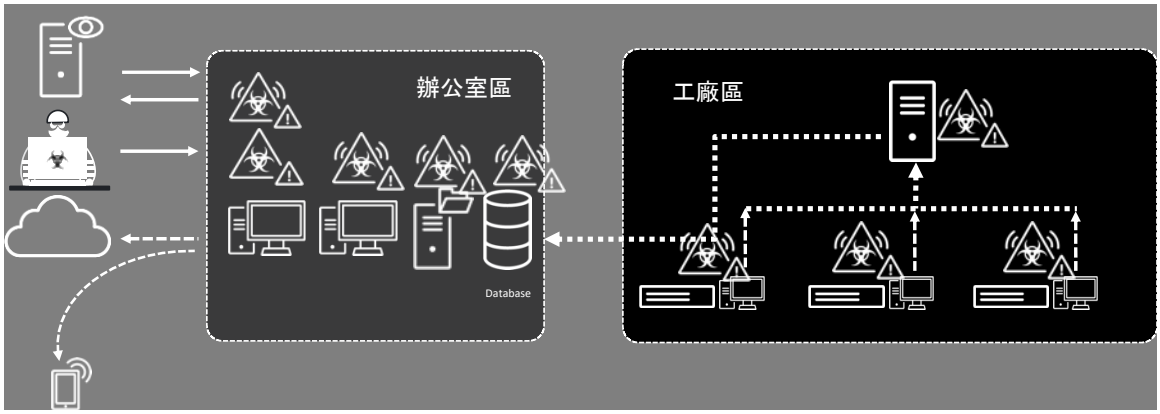


圖 19 Automatic Coin Mining malware 感染途徑（資料來源：趨勢科技）

第一波約有 100 多部 Windows PC 感染，此階段主要是為了竊取身分認證與存取權限，惡意程式不斷在內部進行破解、自行複製、水平移動及取得權限並用來挖掘加密貨幣，如圖 20

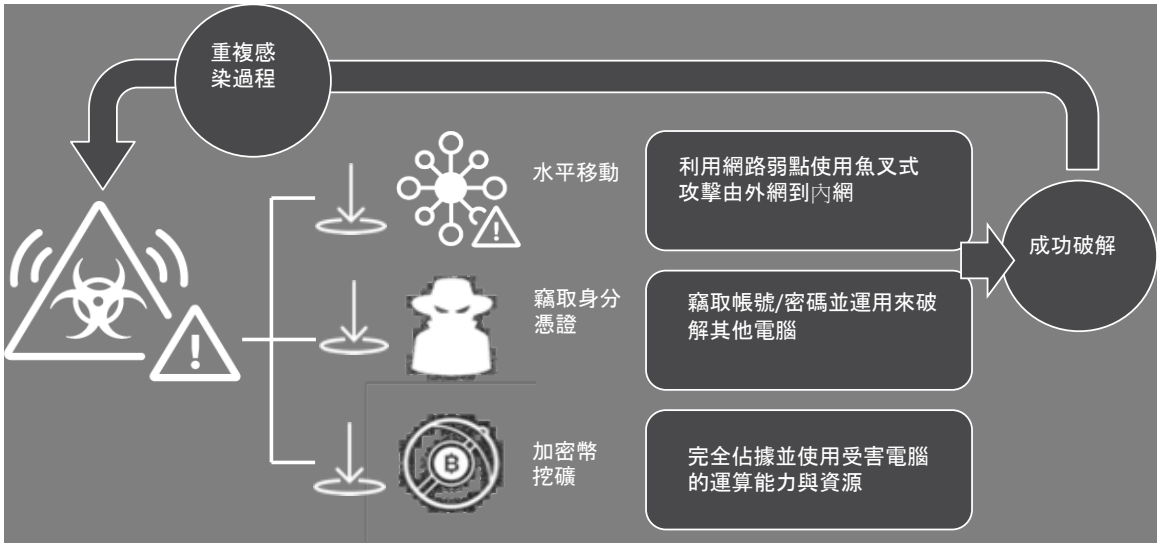


圖 20 自動挖幣攻擊原理示意圖 （資料來源：趨勢科技）

因惡意程式不斷重複自我複製、竊取帳號密碼、破解及非法佔用電腦系統資源，最後造成整個辦公室區及工廠區的運作緩慢，示意圖，如圖 21

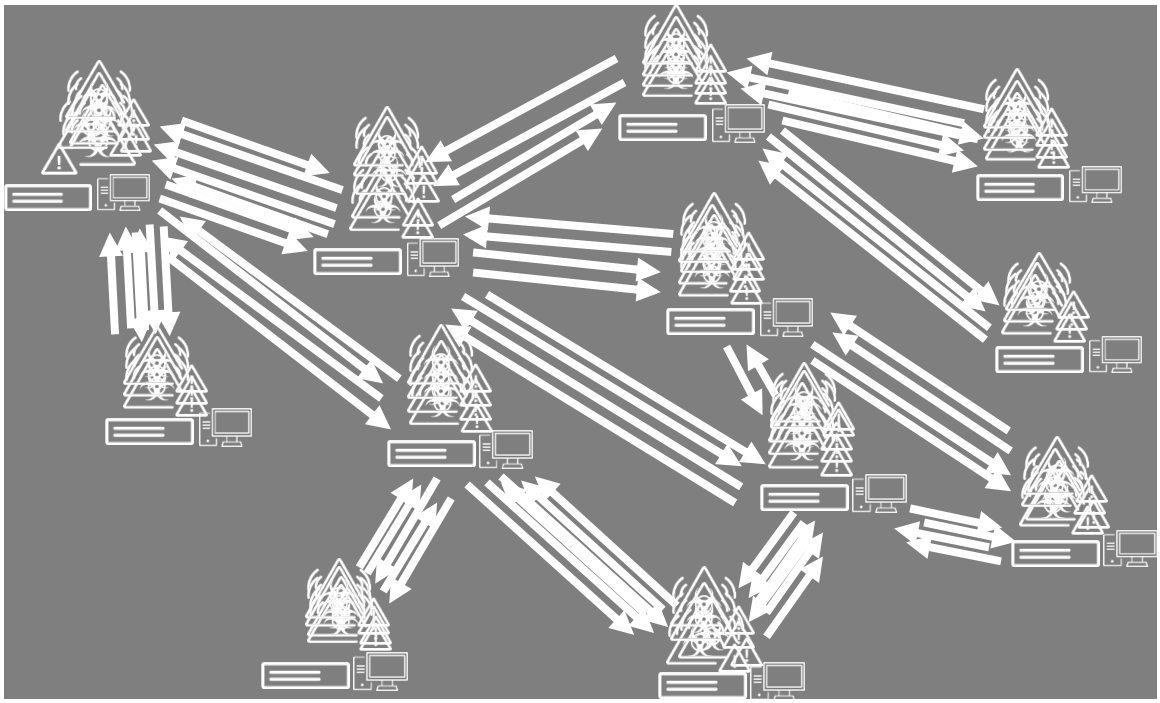


圖 21 自動挖幣惡意程式耗用企業資源示意圖（資料來源：趨勢科技）

最終造成企業的系統、網路異常緩慢，只能將網路設備暫時關閉才能中止被大量「自動挖幣」惡意程式，將整個系統資源耗盡，但若未完全清楚，一旦網路恢復，又立即重複前述自動複製、竊取帳密、佔用並耗用資源進行加密貨幣，並最終將整個企業的系統與網路可用性災難性降低至不可接受的服務水準。

2.2.2 工控物聯網資安事件影響

由上節的案例中，我們可以發現工控物聯網的資訊安全涉及預防通過電腦設備和通信網路惡意行為與入侵系統相關的風險外，也包括了內部 IT 與 OT 環境的安全管理及對供應商的安全要求。入侵的影響可能包括：

- 系統可用性和生產能力的損失
- 劣質的產品品質
- 向未經授權的目的地發布敏感資訊
- 設備損壞
- 人身傷害
- 危害公眾健康和信心
- 違反法律和監管要求
- 妥協的形象等

以上的影響，對人身安全、生產品質、效率、法規要求及企業形象等影響，對企業或基礎設施提供者，都會帶來有形的生命及財產損失及無形的商譽的衝擊。

2.2.3 工控物聯網發生資安風險逐年增高主要原因

依工研院產業科技國際政策發展所研究，過去製造業所用的系統（特別是管理和監控生產設備的工業控制系統 IACS），生產設備一般置於與外部網路實體隔離的「生產內網」，不容易遭受網路資安威脅。然而，隨著網路智慧化生產管理、設備即時監測管理需求，製造業者也將生產系統連上公司網路以增加效率，同時也增加了被攻擊的機會，而且，以往的舊系統保護機制也可能在連網後，無法防禦層出不窮的新興攻擊方式。

進而引發以下 4 項影響工控物聯網安全防護的關鍵議題：

1.工控物聯網系統企業掌握度低：企業引入新的生產設備時，往往是軟體、硬體、作業系統整套購買，為避免影響功能，供應商不會開放最高層級的作業系統權限，並禁止企業資安／資訊人員安裝任何軟體或工具，除非供應商自行釋出更新，否則資安及資訊管理部門很難對這類機台的資安弱點，進行修補、檢查。此外，上游供應鏈廠商負責的新機台，是否能在安裝前保證不會夾帶病毒？在廠安裝的客製化預載軟體以及安裝程序是否會引入惡意程式？上述都是需留意的重點。

2.工業控制系統缺乏資安考量：由於許多工業生產設備原本在獨立的系統與隔離的環境操作，在初期設計缺乏身份驗證和基本加密等防護功能。

這意味著，若內部網路遭入侵，常缺乏有效阻擋的機制，攻擊者在一點突破之後，可以輕易地進入生產製造系統的不同部分，如監視和管理生產程序的控制器，進而可能導致作業停擺、設備損害、財務損失、智慧產權被竊，以及大量影響人員健康和安全的風險。

3.製造生產系統更新速度緩慢：工廠生產設備端採用的作業系統，因為常有特殊的硬體驅動需求或客製化的應用程式要求，而非市面上的標準作業系統，必須由上游廠商提供客製化版本，也因此，作業系統版本的弱點修補及更新，會與標準版作業系統有極大的時間落差。如此一來，容易造成早已公佈的系統弱

點及修補程式在這些生產機台主機上無法即時更新，增加暴露在遭受入侵感染的危險期。

4.製造業或關鍵基礎設施提供商以生產維持穩定為原則：製造業主要目標是保持生產設備穩定運作，任何環境的改變（如加入增強的安全解決方案）都可能會影響製程，製造業管理者偏好只進行微小的改變，期望在加入新的安全解決方案時，保持正常運作以及可靠性，在可能需要進行生產環境設備檢修和測試時，需要更多的時間進行評估與實驗。

迄今為止，企業資訊安全防護主要仍以 IT 為中心。這樣的觀點帶有一些關於如何管理風險的隱含假設，即各端點得到充分保護，並且機器之間的通信受到保護。 IT 通常採用客戶端 - 伺服器模型，其中客戶端和伺服器運作多個應用程式的程序（Process）以眾所周知的網路協議（如 IP，TCP 或 HTTP）進行通信。由於這種同質性，安全控制和監控承擔了一系列眾所周知的攻擊和攻擊模型。IT 系統中的風險評估取決於成功攻擊的可能性和可能造成的損害，但這種損害通常涉及金錢或聲譽，很少考慮其他結果，如安全威脅。因此，從業務決策到實施，OT 安全性被忽視。 OT 中常見的攻擊類型（例如實體攻擊）不在 IT 安全風險評估範圍，網路元素不考慮工控網路協議。
但現在製造業或基礎設施提供者，正在 IT 網路上使用來自工業系統的通信協議添加新設備，例如智慧路燈或電視機上盒，這些協議已被重新用於控制家用電器或工業設備。這些「物聯網」系統側重於可用性而非安全性，因此雖然技術驅動因素與工控物聯網相同，但業務驅動因素和關鍵系統特性要求不同。
與此同時，OT 系統增加了更多 IT 元件，特別是運作設備管理軟體的控制台。即使未連接到網路的控制系統也會受到 IT 攻擊，例如可攜式媒體上的軟體病毒，可以跨越網路。
參考 ISA Automation Conference 2012 ISA 法國主席 Jean-Pierre 的簡報，造成工控物聯網資安風險逐步上昇，主要 3 大主要原因如下：
• 網路互連
- 控制網路和企業網路之間的整合
- 遠端連接（除錯，維護等）
- «運動鞋網路»：以 USB 碟，CD 片，筆記本電腦，智慧手機等可攜式媒體或裝置或非固定連線的等不受控管方式來傳輸資料
• 使用商用現成元件（COTS）
- 不安全的通信協議
- 商業作業系統（操作員工作站，工程工作站）
- 不定期打修補的應用程式
• 缺乏安全政策和程序
- 兩種作業差異文化的共存：商業(IT)和工控自動化（OT）
- 缺乏安全作業程序（網路安全和防病毒管理等）
- 缺乏安全管理程序（存取控制、修補管理、訪客及分包商管理等）
- 缺乏安全意識，專業訓練，主動負責.....

2.3 工控物聯網資安目標

2.3.1 資訊安全

在資訊安全領域被用來設定為目標的是資訊安全三要素「機密性（Confidentiality）」、「完整性(Integrity)」及「可用性（Availability）」，在一般的 IT 領域的資安目標順序通常為 C->I->A，會保護資訊，如營業秘密、個人資料的「機密性」為優先、其次是資訊的正確性或不被非授權篡改的「完整性」及關鍵核心系統的「可靠度」(Reliability)或「可用性」，但參考 IEC624432 的 1－1 之 5.2 安全目標，在 IACS（OT）的領域，其順序則通常為 A ->I-> C，此外由於 Level 0 的生產場域或基礎設施都是實體的實體或化學製程，都必需靠機械、引擎、馬達、高溫或高壓鍋爐、化學等具破壞原物料原有形狀或是特性的製造過程，此一過程若有不慎，超出安全容許範圍，輕則能造成生產機器損壞，重則可能產生火災、爆炸，危及人命安全。當然這些資安目標有可能因企業對 IT/OT 的身特殊需求，而在重要順序排序上不一定會以圖 22 的 IT/OT 目標的優先次序相同，但多數會是以下圖的安全目標的順序為主。

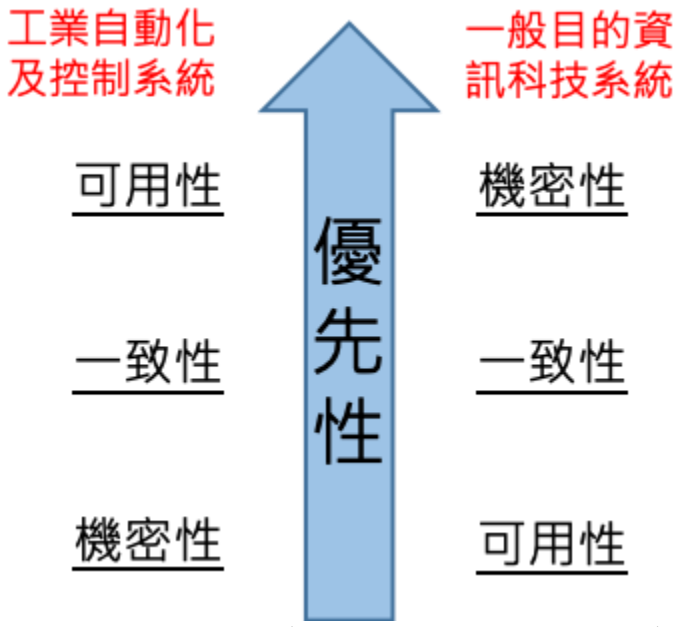


圖 22 安全目標順序（資料來源 IEC 62443 1-1）

從上節工控物聯網的 PERA 模型參考架構中，我們可以得知是上層的 IT 環境與底層的 OT 環境的整合，需要就 IT 與 OT 環境的需求分別去界定安全目標，但綜合來說我整們整理如下：

2.3.2 安全(Safety)：

安全是系統運作的條件，不會由於財產損失或環境而直接或間接地造成不可接受的人身傷害風險或人身健康損害。

2.3.3 高可靠度：

可靠度是指系統或元件在規定的條件下在指定的時間段內執行其所需功能的能力。在工控物聯網的應用產業可靠度的要求通常是高的。
可靠度和可用性是相關的。 可靠性是實際可用性與計劃可用性之間的一小部分，受計劃維護、更新、修復和備份的影響。 這些會降低可用性，但如果安排得當，它們不會降低可靠性。 可靠性反映了企業在計劃和預期工作時可以依賴系統工作的程度。

2.3.4 高可用性

高可用性（high availability, HA），指系統無中斷地執行其功能的能力，代表系統的可用性程度。是進行系統設計時的準則之一。高可用性系統與構成該系統的各個元件件相比可以更長時間運作。通常在運用工控物聯網的產業對可用性的要求通常比機密性來得高
高可用性通常是透過提高系統的容錯能力來達成。定義一個系統怎樣才算具有高可用性往往需要根據每一個案例的具體情況來具體分析。

2.3.5 持續營運

在生產製造公司或是關鍵基礎設施的提供者，其關鍵製程一旦因天然災害、人為破壞或是網路攻擊，導致生產進度中斷，都可能造成企業、國家社會、甚至國際供應鏈服務衝擊，工控物聯網需在發生事件後，能在緊急回應並處理事件，之後有能力在目標可容忍中斷時間內回復最小可運作服務水準，是工控物聯網安全的目標之一。

2.3.6 資料保護

融合 IT 和 OT 涉及其關鍵系統特徵的複雜合併。 雖然許多工業系統將 IT 和 OT 結合起來通過軟體控制設備，但這些系統通常在 OT 側被隔離。 將這些系統結合在一起，會修改 IT 和 OT 既有已實施安全控制措施。 例如，保留儲存在雲端中的資訊完整性可能會影響 OT 系統的可靠性，因此成為安全問題。
如果由於不正確的安全建置而未經授權修改儲存在 IT 系統中的控制資訊，則依賴於這些資料的 OT 系統可能會失敗。

2.4 工控物聯網資安框架

工控物聯網的發展可能是由小型企業的生產管理部門（Level 4）與生產現場(Level 0,1)，隨著業務擴大及工控自動化科技與智慧製造技術發展，大量開始運用非 IACS 的 IT 系統及元件，使得企業得以工控物聯網來管理多條生產製程、跨地境、跨國的產線或基礎設施的複雜的 OT 環境。
在過去屬製造業的企業或基礎設施提供者環境中，IT 與 OT 環境多數是實體隔離或是低度互相連結，且系統建置、維運的組織及人員也是分開的，常見的現象負責企業 IT 層人員不瞭解 OT 的運作，反之亦同。為利以企業資安治理角度，可將資訊安全管理制度適用範圍延伸到 OT 環境，以使 IT 與 OT 環境在同一個資安管理框架下。

在 IT 領域全球最普遍認可的資訊安全管理實務國際標準 ISO／IEC 27001 系統，亦是我國國家資訊安全管理標準 CNS 27001，依這個標準可建置並維持一個持續以 PDCA 改善資安有效性的管理制度，ISO/IEC 27001 的管理框架，包含了如圖 23

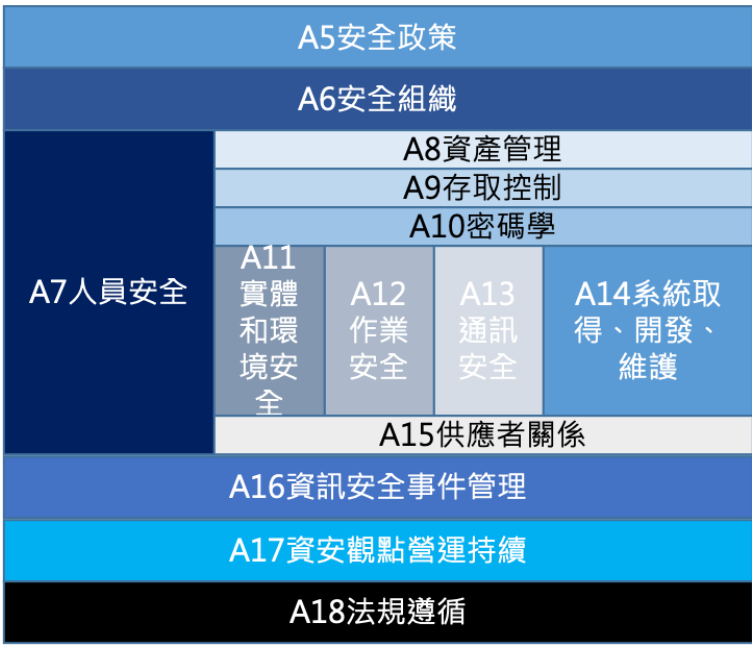


圖 23 ISO 27001 控制領域

ISO／IEC 27001 系列資訊安全系統最新版本為 ISO/IEC 27001:2013，已經採用了新的 ISO 的 Annex SL 高階管理架構，如圖 24，易於與應用普遍於製造業且也於新版採用 Annex SL 高階的 ISO9001/14000 等管理制度進行整合，也都在規劃時均需進行不同管理標的風險評鑑，所以 ISO／IEC 270001 適合作為企業資訊安全管理的框架。

圖 24 ISO Annex SL 架構

在 OT 環境工控自動化資訊安全標準，由國際自動化學會(The International Society of Automation, ISA)所發展的 IEC 62443 ，IEC 62443 由 ANSI(AMERICAN NATIONAL STANDARDS INSTITUTE 美國國家標準學會)/ISA （USA International Standards Authority, Inc.美國國際標準管理局）提出，被 ISO/IEC 採納，所以該標準會以不同的名字出現，包括：ANSI/ISA-99，ISA-99，ISA 62443，ISO/IEC 62443，ISO 62443，IEC 62443。 IEC62443 並不是單一文件，是由 13 份文件組成，架構如圖 25

圖 25 IEC62443 文件架構

從上面的文件架構，可以看出從 IACS 的「管理」總綱(General)層級定義概念及模式、專用術語定義，政策與程序（Policies & Procedure）層級由

IACS 的「安全需求」、「建置指引」、「修補管理」到供應商的「安裝維護」的流程，到系統（System）層級以安全等級(Security Level)來區分不同功能區域（Zone）的系統安全需求與安全科技（Security Technology），在元件(Component)層及則以安全設計(Secure by Design)及規範「元件安全需求」。

在上述兩個 IT 與 OT 的主流資訊安全標準 ISO27001 與 IEC 62443，雖在控制領域的劃分的思維方向不同，就整體企業資訊安全管理的 Top-down 下，以 ISO 27001（ISMS）的框架為涵蓋企業的整體範圍，再以安全區域及管道以 IEC62443 的 7 項安全需求作為考量，發展出圖 26 安全框架。

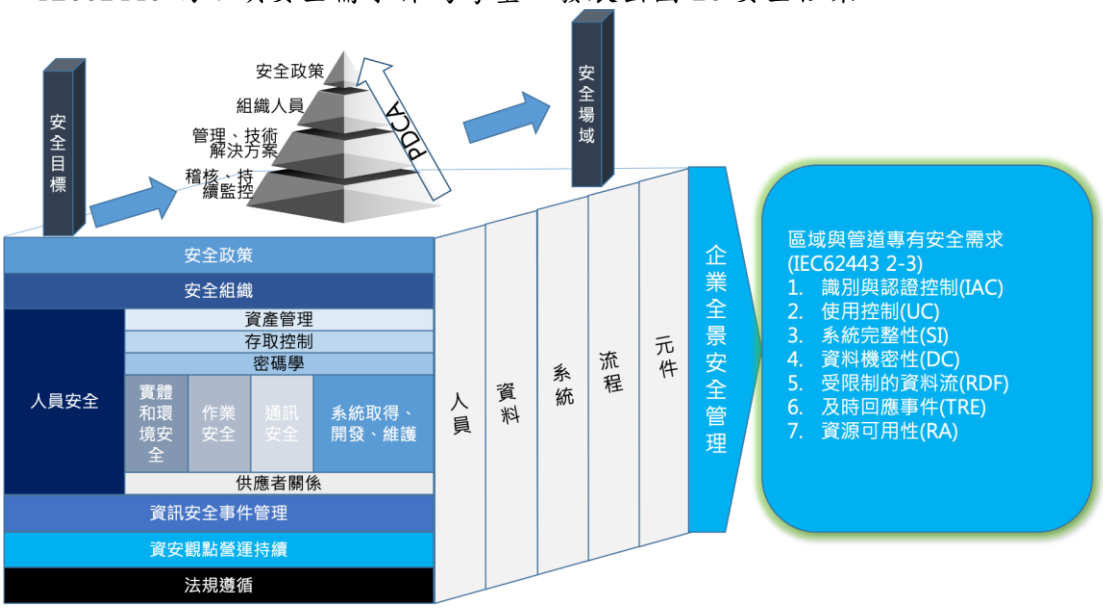


圖 26 工控物聯網安全框架建議架構

在此框架中，可以由可與其他管理系統如品質管理系統(QMS)、環境管理系統（EMS）等整合的 ISMS 作為高階管理系統，作為企業或基礎設施提供者的共通性控制領域框架，主要的體系架構為：

- 安全政策
- 安全組織
- 資產管理
- 身分識別與存取控制
- 密碼學
- 人員安全
- 實體和環境安全
- 作業安全
- 網路安全
- 系統獲取、開發和維護
- 供應鏈安全
- 安全事件管理
- 系統即時性及高可用性
- 法規遵循

在本指南的適用範圍並不包含在企業的營運層與 IACS 資料傳輸、監控或直接及間接控制無關的應用系統，如人資、財會或是官方網站等應用系統，但會包含所有與生產製造流程或基礎設施的製程有關的 IT 及 IACS 系統是本指南所涵蓋的範疇。

2.5 安全等級

2.5.1 共通性安全等級

建立安全等級概念的目的是集中考慮區域安全性，而不是基於單個設備或系統。通常，IACS 由來自多個供應商的設備和系統組成，它們共同起作用以為工業操作提供整合的自動化功能。正如個別設備的功能能力有助於 IACS 的能力一樣，個別設備的安全能力和實施的對策必須相互協作以達成區域的期望安全等級。安全等級為組織決策運用具有不同程度之安全有效性的對策和設備提供了參考框架。

安全等級提供了解決區域安全性的定性方法。作為定性方法，安全等級定義適用於比較和管理組織內區域的安全性。隨著可獲更多可用的資料，以及可用簡易數學公式表達風險、威脅和安全事件的形成，這一概念將轉向用於選擇和驗證安全等級（SL）的定量方法。它適用於資產擁有者組織以及工控和安全產品的供應商。它將用於選擇要在區域內使用的 IACS 設備和對策，以及識別和比較跨產業的不同組織中的細分區域的安全性差異性。

使用安全等級方法的每個組織應該建立每個等級代表達成何種程度資安目標的定義以及如何衡量區域的安全等級。應在整個組織內始終如一地使用此定義或特徵。安全等級可用於識別區域的綜合分層縱深防禦政策，該政策包括基於硬體和軟體的技術對策以及管理型對策。

安全等級對應於對策的必要有效性以及區域或管道的設備和系統的固有安全屬性，其基於對區域或管道的風險的評估。安全等級方法提供了對區域或管道的風險進行分類的功能。例如它還有助於確定用於防止未經授權的電子干擾的對策所需的有效性，這些干擾可以讀取或影響區域或管道內設備和系統的正常運作。安全等級是區域和管道的屬性，而不是設備，系統或系統的任何部分的屬性。

建議至少使用 3 個安全等級。本指南會以 4 個等級來舉例，可以定性地描述 4 個水準，如下表 1 中所示。組織可以自行依需要，選擇對此進行擴展，並定義其他安全等級來描述其獨特的安全要求。

表 1 – 安全等級表

安全等級	定性描述	需求理由
1	低	未經控制或部份控制，對抗偶發性意外或低技能內外部攻擊 A:容許 8 小時以上製程中斷 I:容許資料不同步、24 小時校正後正確。 C:無需保護機敏資料
2	中	對抗一般外部攻擊技術或內部人員破壞的工控環境。 A:容許造成 8 小時以下暫製程中斷

		I:容件資料於 1 小時內同步後正確無誤。 C:內外部被授權人員外不可存取機敏資料。
3	高	一般基礎設施或對抗中高階外部攻擊技術的工控環境。 A:容許 1 小時以內暫製程中斷。 I:不容許資料錯誤及篡改。 C:僅內部被授權人員外不可存取機敏資料
4	特高	關鍵基礎設施、對抗國家級或高階技術攻擊活動。 A:容許 1 分鐘以內中斷時間。 I:不容許資料錯誤及被篡改。 C:僅極少數被授權人員外不可存取機敏資料。

2.5.2 安全等級類別

2.5.2.1 分類

可以定義三種不同類型的安全等級：

a）目標安全等級（Target Security Level, SL-T） - 區域或管道的目標安全等級。

b）達成安全等級(Achieved Security Level, SL- A) - 已達成區域或管道安全等級。

c）控制措施安全等級(Control Security Level, SL-C) - 安全等級與區域或管道相關對策的能力或固有的安全等級區域或管道內的設備或系統的能力。

2.5.2.2 目標安全等級(SL-T)－期望達成安全等級目標

應將目標安全等級分配給區域。可以將目標安全等級分配給管道。在風險評估期間確定區域和管道的目標安全等級。只要在使用所考慮的管道的區域的風險評估期間考慮與管道相關聯的安全屬性，就不需要將管理目標安全等級分配給管道。風險評估應考慮到區域或管道安全受損的可能性和後果。風險評估可以是定性的、半定量的或定量的。 目標安全等級確定必須採取的控制措施，設備和系統所需的有效性，以防止區域或管道的安全受到損害。

控制措施可以是：

a）技術控制措施（防火牆、防毒軟體等）

b）管理控制措施（政策和程序）

c）實體控制措施（鎖門、安全警衛等）

影響區域和管道目標安全等級確定的因素是：

a）具有定義的區域邊界和管道的網路架構

b）所考慮的區域及將與之通信的區域的目標安全等級

c）管道的目標安全等級，如果指定，適用於區域的通信安全目標設定。

d）實體存取區域內的設備和系統。

在區域內，計算目標安全等級應基於安全層及其對整體的影響。

2.5.2.3 達成安全等級（SL-A） －已經滿足目標安全等級的程度

區域或管道的達成安全等級取決於區域或管道內的設備和系統的固有安全屬性或控制措施的屬性，以防止區域或管道的安全受到損害。 達成安全等級是時間的函數，由於對策的降級，新的弱點，調整的威脅或攻擊方法，安全層中的弱點以及設備和系統的固有安全屬性，直到它們被檢視，更新或升級，因此隨著時間而減少。

目的是確保在任何特定時間區域或管道的達成安全等級大於或等於區域或管道的目標安全等級。

2.5.2.4 能力安全等級 （SL-C）- 對策、設備或系統的安全等級能力

控制措施安全等級定義為區域或管道內的設備和系統的對策和固有安全屬性，其有助於區域或管道的安全性。它衡量了對策、設備或系統對其所處理的安全屬性的有效性。

以下是可以通過控制措施、設備或系統解決的安全屬性的部份實例：

a）證明對等實體的真實性
b）保持訊息的真實性和完整性
c）保持訊息/資訊/通信的機密性
d）確保可歸責制（不可否認性）
e）實施存取控制政策
f）防止服務阻斷攻擊
g）保持平台可信度
h）檢測篡改
i）監控安全狀態。

區域或管道內的對策，設備或系統的控制措施安全等級基於由該區域或管道的對策，設備或系統所解決的相關安全屬性而對達成安全等級做出貢獻。

2.5.3 安全等級運用

在設計新系統（綠色區域）或修改現有系統（棕色區域）的安全性時，第一步是將系統分成不同的區域，並在必要時定義連接這些區域的管道。 一旦建立了系統的區域模型，則基於後果分析為每個區域和管道分配安全等級目標，該後果分析描述了對應區域或管道的期望安全性。 在初始區域和管道分析期間，沒有必要完成詳細的系統設計。 描述區域中的資產應該提供的功能以及區域之間的連接以滿足安全目標就足夠了。

圖 27 顯示了氯卡車裝載站的控制系統分解為由管道連接的區域的系統的高階層範例。它顯示了五個區域：基本製程控制系統（BPCS）、安全儀表系統（SIS）、控制中心、工廠 DMZ 和企業。 BPCS 和 SIS 都使用 PLC 通過 SIS 使用特殊功能安全 PLC（FS-PLC）操作裝載站的不同方面，該安全 PLC 適用於安全系統。兩個 PLC 通過使用邊界保護設備的不可路由的串接或以太網連接進行連接。每個 PLC 都連接到本地交換機，帶有用於可程式的工程工作站和用於操作的 HMI。BPCS 和 SIS 區域還包含儀器資產管理系統（IAMS），用於測量和測試儀器。包含多個工作站和 BPCS 的控制中心都連接到工業非軍事區（IDMZ）。IDMZ 可以容納各種元件和系統，例如圖中所示的資料歷史記錄和維護工作站。工廠 DMZ 顯示連接到企業系統，企業系統包含企業無線區域網路（WLAN）和 Web 伺服器。

圖中顯示了多個域控制器和邊界保護設備，以指示可用於提高安全性的一些控制措施。

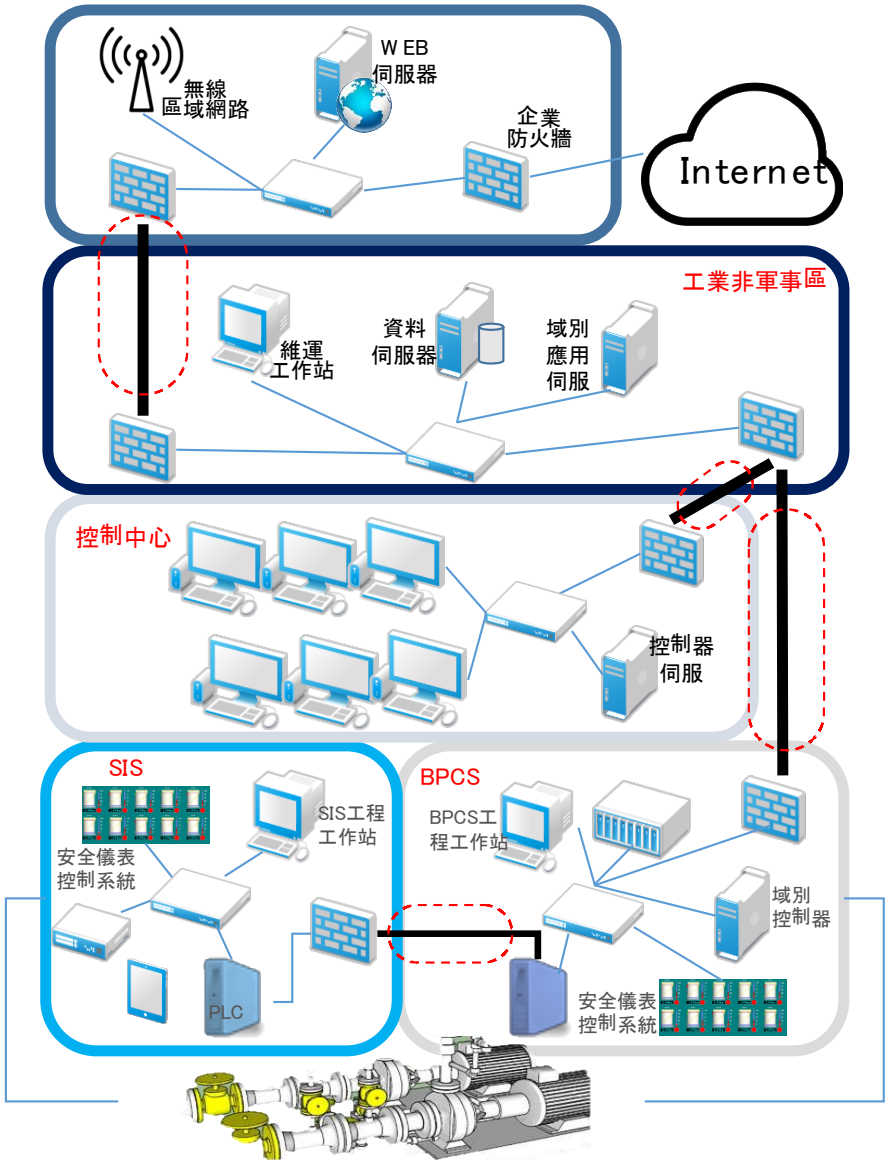


圖 27 製程高階視圖－表達區域及管道

在這個特定的例子中，每個工控網路通過自己的 PLC，現場設備和 HMI 相互獨立地運作。確定目標安全等級(SL-T)後，系統可以設計（綠色區域）或重新設計（棕色區域）以試圖滿足那些 SL-T。設計過程通常是一種迭代方法，在整個過程中多次針對目標檢查系統設計。

在系統的設計過程中，有必要評估不同元件和子系統的安全功能。產品供應商必須通過比較功能和組織中針對不同功能安全等級定義的要求，為其元件或系統提供這些功能能力安全等級（SL-C）。這些功能的 SL-C 可用於確定特定元件或系統是否能夠滿足系統的目標安全等級（SL－T）。產品供應商或系統整合商還必須提供有關如何配置元件或系統以滿足所聲明的安全等級的指導。

在特定設計中可能會有一些元件或系統無法完全滿足 SL－T。在部件或系統的安全能力安全等級（SL-C）低於 SL－T 的情況下，需要考慮補償控制措施以滿足期望的 SL－T。補償控制措施可以包括改變元件或系統的設計以增加其能力，選擇另一個元件或系統以滿足安全等級目標或添加額外的元件或系統以滿足安全等級目標。在設計過程中的反覆比較安全等級差異之後，應重新評估系統設計達成的安全等級（SL-A），以查看它們與系統的安全等級目標的比較。

一旦系統設計得到核可和付諸實施，就需要對系統進行評估，以防止或減輕系統安全等級的惡化。應在系統修改期間或之後以及定期計劃進行評估。在確定所達成的安全等級之後，將需要評估系統是否仍然滿足原始安全等級目標。如果系統不滿足這些要求，可能有多種原因，包括缺乏程序維護或需要重新設計系統的部分。

本質上，控制系統安全效能是獨立於特定的使用情境確定的，但是在特定的情境中使用，以便達成對應系統體系結構，區域或管道的安全等級目標（見圖 28）。

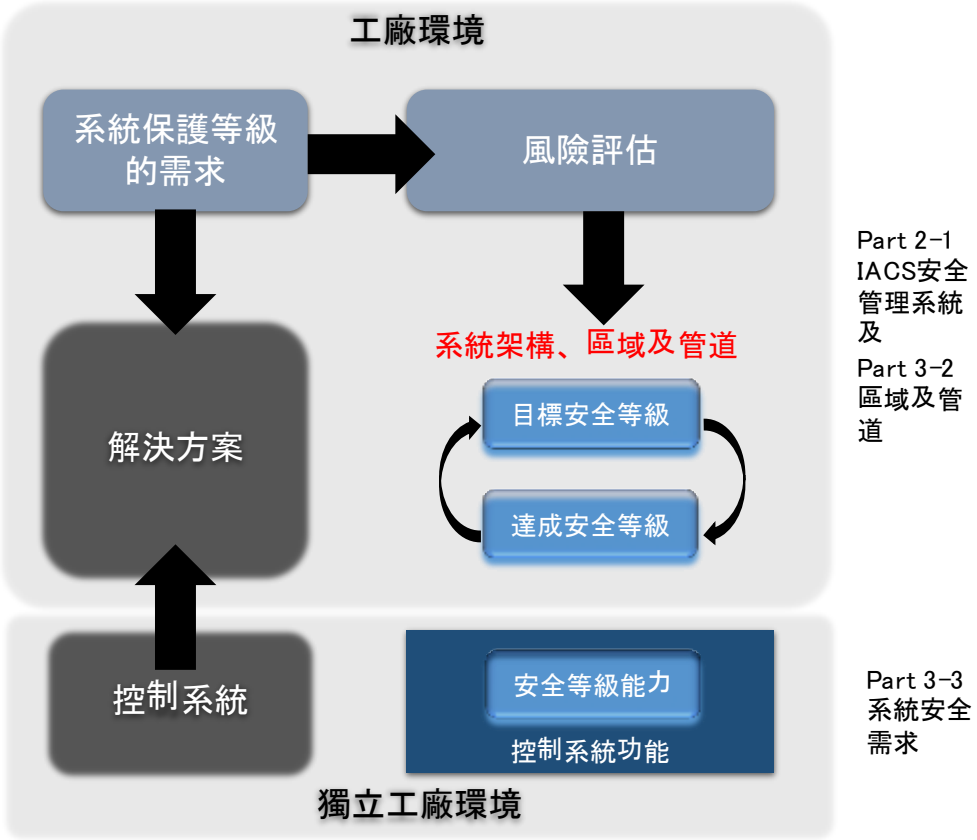


圖 28 不同安全等級類型對應關係關聯圖

第 3 章 工控物聯網資安控制措施

3.1 資安政策

3.1.1 組織層級資訊安全管理政策與作業程序

在台灣，一個有國際客戶的製造企業可能已經有以 ISO 9001 建置的品質管理系統(Quality Management System, QMS)或是以 ISO14001 建立的環境管理系統(Environment Management System, EMS)，但是在台灣的製造業，除了少數被客戶要求或是較有資訊安全管理意識會導入國際資安管理標準 ISO 27001 的資訊安全管理系統（Information Security Management System, ISMS）或是 ISO 22301 營運持續管理系統(Business Continuity Management System ,BCMS)，顯示資訊安全管理思維尚未廣泛成為製造業或關鍵基礎設施提供者的組織核心價值之一。

本指南建議組織以 ISMS 作為 IT 與 OT 一致性的資訊安全管理框架，合併 IT/OT 環境後本指南將 ISMS（Information Security Management System） 一辭，建議改為 CSMS(Cybersecurity Management System)，本指南作為組織工控物聯為政策、程序與控制措施選擇的指導方針，將 CSMS 的管理範圍由企業區域(PERA 的第 4／5 層)，延伸至工控區域（PERA 的第 0～3 層）。在管理系統中政策通常被視為最高指導原則。我們在第 2 章有描述以 CSMS 作為企業或基礎設施服務提供者資訊安全系統管理框架。

資安政策使組織能夠遵循一致的程序來維持可接受的安全等級。政策在組織的不同等級定義，從在企業等級建立的治理或管理政策到定義安全管理細節的操作政策。最具體的政策是組織的標準，是必須達成的最低水準或是最低安全要求，是共通的準則或規範，透過安全審核可以衡量合規性，為達成組織最低的安全要求，組織需要制定安全需求，並強制落實執行。

資安政策是指定或規範組織如何保護敏感和關鍵系統資源的規則。政策明確規定了什麼是強制性的。由於政策是強制性且明確的，因此可以進行審核。組織的安全政策還考慮到法律、監管和合約義務。它們是評估測試組織實際操作的衡量標準。

補充政策是程序。安全程序詳細定義了提供某種安全措施所必需的步驟順序。由於其詳細程度，程序適用於特定問題。它們可能與特定技術有關。政策參考程序並強制使用它們。

與政策和作業程序相對應的是工作指導書（或稱為實作指引）。工作指導書不是強制性的。它們用以描述一種做某種可行但非強制性的方法。由於指南不是強制性的且較為籠統目的是為了適應各種可能的情境，而刻意模糊不清，因此無法根據工作指導書對實務工作進行審核。工作指導書有時由沒有權力要求遵循的小組編寫。工作指導書不適用於描述強制性的做法。

由於組織在不同部門的政策和程序往往不同，因此必須充分協調。具體而言，工控物聯網的資安政策必須與用於一般 IT 安全的類似政策協調。如果各方之間有良好的工作關係，安全計劃將更加成功，一套協調良好的政策可以支援良好的關係。

各種政策和程序結構的一致性增加了整套政策和程序的一致性。每份政策或作業程序文件都有一個簡短但準確的目的陳述。它還有一個範圍聲明，用於定義文件的適用的所在站點、組織部門、區域、系統或是實體位置。它描述了用以在減少的風險以及文件的關鍵原則。這些常見項目通過提供有關政策或程序意圖的更多資訊來指導讀者。他們還描述了文件提供指導的意圖，這在需要修改文件時很有用。圖 29，是 CSMS 的文件架構的

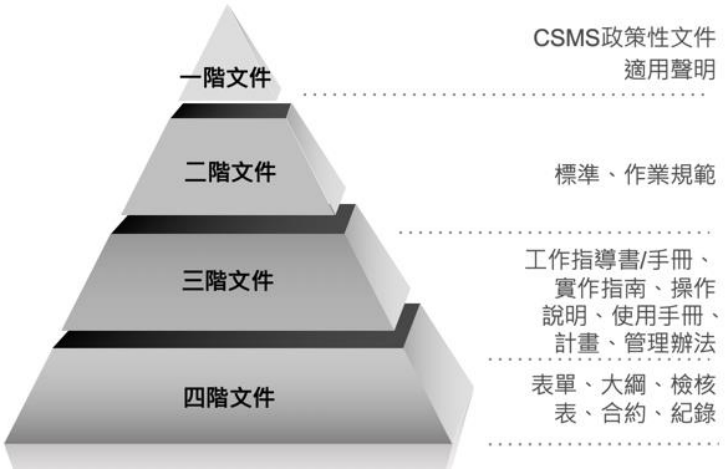


圖 29 管理文件架構

系統生命週期中的不同階段具有不同的安全問題。資安政策和程序可能只涉及某些生命週期階段。某些政策和程序可能會指定它們僅適用於某些階段。所有個別階段的所有安全問題都在資安政策和作業程序的應用在 PERA 中各層及 OT 環境中依高階風險評鑑切分出的安全區域及管道，達成適當的安全等級及成管理成熟度。

資安政策和過程包含有關組織如何衡量合規性和更新政策的說明。在有基礎設施的企業組織，會以一、二階文件作為組織資訊安全的標準，在三階的作業規範、管理辦法，則可依企業區域、IDMZ 及工控區域的控管需求，分別訂定。四階文件則可將流程表單、執行紀錄、區域及管道安全控制說明文件等。

組織通常認知到在執行或評估稽核時需要更新政策。稽核可以識別政策和程序中的含糊之處，以及未使所需過程或結果明確的政策和程序部分。稽核可以識別應添加到政策和程序中的問題。稽核還可以確定應重新評估和調整或可能收回授權的要求。

政策和程序應該允許不可預見的情況，使其無法遵循它們。政策還應說明如何記錄和核決政策和程序的例外情況。記錄核決的例外情況會導致更明確的安全狀態，而不是在政策和程序中留下不精確和模棱兩可的情況。

此外，組織應明確要求什麼是要求而不是政策中的可選建議。準確使用「必須」，「應」、「需」，「得」、「宜」和「可」之類的詞語可以消除歧義。政策聲明可以在其引言部分中更準確地定義這些單詞。 「必須」、」「應」、「需」和用於要求。 「得」、「宜」或「可」用於可選的建議，因此不用於強制要求的政策和程序。提供滿足要求的選項可能是適當的。像「在可能的情況下」或「除非必要」之類的用語引入歧義，除非該陳述還描述瞭如何確定案件是否可能或必要。

3.1.2 管理組織、角色與權責

政策和程序確定誰負責什麼。製程控制人員是否負責控制網路？它是否負責「非軍事區」（DMZ）之間的存取管理政策及執行？這是在管理現場常見的問句。

政策與程序及製程現場的設備是需要由人或是由人來設定設備自動化來落實執行，故人的因素在工控物聯網安全中是極為重要的一環，在工業 4.0 或智慧製造風潮興起後，組織開始意識到運用 IT 在長期發展的網路傳輸、雲端資料處理、企業商業智慧應用系統來強化企業或基礎設施提供者的製造現場的品質、效率、可預測維修及彈性調整產線生產。但許多企業卻因過去 IT 與 OT 環境是隔離，僅依靠少量或是批次的資料交換，長期以來 IT 與 OT 的管理組織與人力發展是各自獨立的，甚至在多廠區及多產品線的 OT 環境下，更可能在 OT 網路內劃分更多的部門是各自發展其政策、程序及安控措施。
在工控物聯網發展下，組織需要思考，現行 IT 與 OT 管理權責各自獨立狀況下，又有需要整合串接 IT 與 OT 的環境，是否能有效運作？資訊安全要求是否能完全由上至下落實到組織的生產現場？是當前推動工業 4.0 或智慧製造或基礎設施智慧化及安全的一大挑戰。

3.1.2.1 管理組織

在 IIoT 的整合環境下，IT 與 OT 的資料流、甚至自動化控制設備的交互作用頻率增加不少，人員也需要更頻繁地交流與分工互動。權責分工與授權管理對於 IIoT 來說是跨部門組織議題的重中之重。依第 2 章我們所討論資訊安全的管理框架，跨組織不同的職能部門，無法一開始就大破大立設置一個單一部門去解決所有問題，在實務上也不可行。在組織的政策程序上也不容易直接對每個人的職務去定義使用權限及應負責任。比較好的實務作法是建立一個 IIoT 的矩陣式（或稱虛擬）管理組織，以角色或部門在政策與程序內去進行分工與授權。
IIoT 的管理組織建議納入的角色至少包含：

- 管理階層：需要對 IIoT 環境內的利害關係人有溝通及影響力，可能是企業的副總經理層級以上人員、工廠廠長、製造部門主管
- 產品／專案經理：需要對單一產線或是產品有來自客戶或是來自上下游供應鏈有安全要求的主要對內及對外溝通管道。
- 製程環境主管或作業代表：熟悉對影響製程現場的生產環境（OT）的環境人身及設備安全議題，包含對生產品質、效率、可用性及危安因素等問題能進行溝通，並能落實安全控管機制。
- IT 主管：負責企業區域的 IT 建置、維運，維持組織業務系統、電子通信系統正常運作，並負責 IT 區域的資訊安全管理，有些組織也常把 OT 連網的作業也交由 IT 負責。。
- 實體環境管理主管：負責組織、廠區的環安衛系統的安全。
- 資訊安全人員
  這個組織除了協調有關 IT/OT 整合功能需求與協調事項，同也需討論安全議題，如 IIoT 環境下的風險、對策及持續改善議題，再透過協調及溝通，運用各原功能部門主管的管理權力，要求相關人員遵守組織所訂的資訊安全政策。

3.2 流程與程序（管理控制措施）

政策和程序可以涵蓋幾個主題。因不分產業，每個組織文化與 IIoT 現況都不同，應透過風險管理活動確定適用於其工控物聯網的適當政策和程序。可能的主題包括：

- 風險管理 – 風險管理對於開發具有成本效益的安全計劃是非常重要，該計劃提供了統一的足夠安全保障，但這並不需要設備或程序過於昂貴且嚴重超出適當安全範圍。但是，風險管理很複雜，需要根據組織進行調整。風險管理政策定義如何確定可接受的風險水準等級以及如何控制風險的過程與結果。該等級取決於特定組織的目標和環境。應定期重複確定風險等級的過程，以適應環境的變化。
- 存取管理 – 通過限制僅存取需要並受信任存取權限的使用者來改進系統中的資產的安全性。存取管理政策識別使用者的不同角色以及每個角色對每類資產（實體或邏輯）所需的存取權限。它規定了員工保護資產的責任，以及管理員維護存取管理程序的責任。對這些存取權限的授權應由管理層進行充分記錄，並定期進行審核。隨著保護資料機密性及實體設施使用控制的需要，存取管理對於系統完整性和可用性可能同樣重要甚至更重要。
- 高可用性和持續性規劃 – 此主題中的政策為備份和復原以及業務持續性和災難復原計劃提供必要的框架和要求期望。它們還定義了歸檔特徵（例如，必須保留多長時間的資料）。
- 實體安全 – 控制系統的安全性取決於包含控制系統的空間的實體安全性。在為控制系統編寫資安政策之前，工廠站點可能已經具有實體資安政策。但是，與系統實體存取相關的政策可能與涉及非系統資產的政策不同。例如，所有煉油廠工作人員可以對工廠圍欄內的大多數設施進行一般存取，但 IT 基礎設施室可能只僅限於 IT 相關人員需要存取。控制系統資安政策應包括對實體資安政策的引用並聲明其依賴性。控制系統的資安政策必須包含足夠的實體安全性細節，以便將站點實體資安政策的應用於任何特定控制系統。例如，某些設備必須位於鎖定的機櫃中，並且鑰匙必須保存在受限制的位置。
- 架構 – 政策和程序描述控制系統的安全配置，包括但不限於以下問題：
  a）推薦的網路架構設計
  b）推薦防火牆配置
  c）使用者授權和認證
  d）互連不同的製程控制網路
  e）使用無線通信
  f）域名和信任關係
  g）修補管理
  h）防毒管理
  i）在關閉軟體介面，禁用或避免未使用或危險的服務的系統強化以及禁用可移動儲存設備及媒體
  j）存取外部網路（即網際網路）
  k）適當使用電子郵件。
- 可攜式設備 – 可攜式設備會帶來固定設備的所有安全風險，但其移動性使得從安裝到稽核的正常安全程序不太可能覆蓋它們。它們的可移動性在外部實體安全區域或連接到安全區域時攔截資訊時提供了額外的破壞機會。因此，通常需要特殊政策來涵蓋可攜式設備。該政策應該被要求與固定設備相同的安全保護政策，但提供此保護的技術和管理機制可能不同。
- 無線設備和感應器 – 使用無線電頻譜傳輸代替電線的控制設備已經在某些控制系統應用中廣泛使用多年。隨著成本的降低和新標準的出現，2020 可

能出現 5G 應用於生產現場，自動化和控制系統的潛在應用不斷擴大，部分原因是安裝成本降低。有線和無線設備之間的關鍵區別在於在後一種情況下，信號不限於實體安全邊界，使它們更容易被攔截和損壞。因此，特定於無線設備的資安政策適用於當前使用或可能在其操作中部署無線設備或感應器的組織。該政策可以指定哪些應用程式

在組織的全面性的資訊安全管理，可參考 ISO 27001：2013 來實作 CSMS，相關的控制要求的檢核表，如附錄 B「資訊安全管理制度檢核表」

3.3 技術性控制措施（技術控制措施）

3.3.1 工控自動化系統安全（IACS Security）概觀

擁有工業自動化和控制系統（IACS）的組織越來越多地使用廉價、高效和高度自動化的商用現貨（COTS）網路設備。出於快速及有效等商業原因，控制系統也越來越多地與非 IACS 網路互連 ，為了區別傳統以各種工業通訊協定互連但未與企業網路相連的 IACS，與企業 IT 網路相連，甚至運用到網際網路及雲端服務的現代 IACS，本指南會以工控物聯網(IIoT)來稱呼。這些設備在開放式網路技術和增強的連接性為控制系統硬體和軟體的網路攻擊提供了更多機會。這種弱點可能導致部署的控制系統中的健康、安全和環境（HSE）遭到破壞，財務損失或影響聲譽後果。

部署現行適用企業辦公區域 IT 網路安全解決方案以解決 IACS 安全問題的組織可能無法完全理解此決策的結果。雖然許多企業辦公區域 IT 應用程式和安全解決方案可以應用於 IACS，但需要以適當的方式應用它們以消除造成意外副作用的後果。因此，用於定義系統要求的安全對策或控制措施需要基於功能要求和風險評估的綜合分析、判斷，通常還包括對 IACS 運作影響程度的認知。

用於 IACS 安全對策或控制措施不應該導致基本服務和功能的喪失，其中包括緊急程序在內。經常部署的 IT 安全措施確實具有這種上述可能性。IACS 安全目標側重於控制系統可用性、工廠資產保護、工廠營運和時間關鍵的系統回應速度。 IT 安全目標通常不會強調這些因素;他們可能更關心保護資訊而不是實物資產。無論基礎設施提供者或工廠整合程度如何，都需要明確說明這些不同的目標作為安全目標。風險評估的關鍵步驟應該是確定哪些服務和功能對於 IACS 營運是非常重要。例如，在某些 IACS 運作環境中，工程支援服務可能被確定為非必要的服務或功能。在某些情況下，安全措施可能導致暫時喪失非必要服務或功能，這樣並不會使主要基本服務或關鍵功能受到不利影響的。

在我們深入討論任何安全性討論之前，我們將先詳細討論 IACS 是什麼以及它的作用為何？ 我們將研究構成工業控制系統的不同部分。 從架構的角度來看整體 IIoT 中的各個部分，並了解它們如何協同工作以完成一項共同任務。 我們將通過檢查用於連接 IACS 中所有元件、系統和連接設備的各種工業通信協議來帶出安全控制措施需求。

下圖顯示了正確設計的現代 IACS 的架構。 本章的目的是介紹架構設計中的方法和安全注意事項，如圖 32 所示：

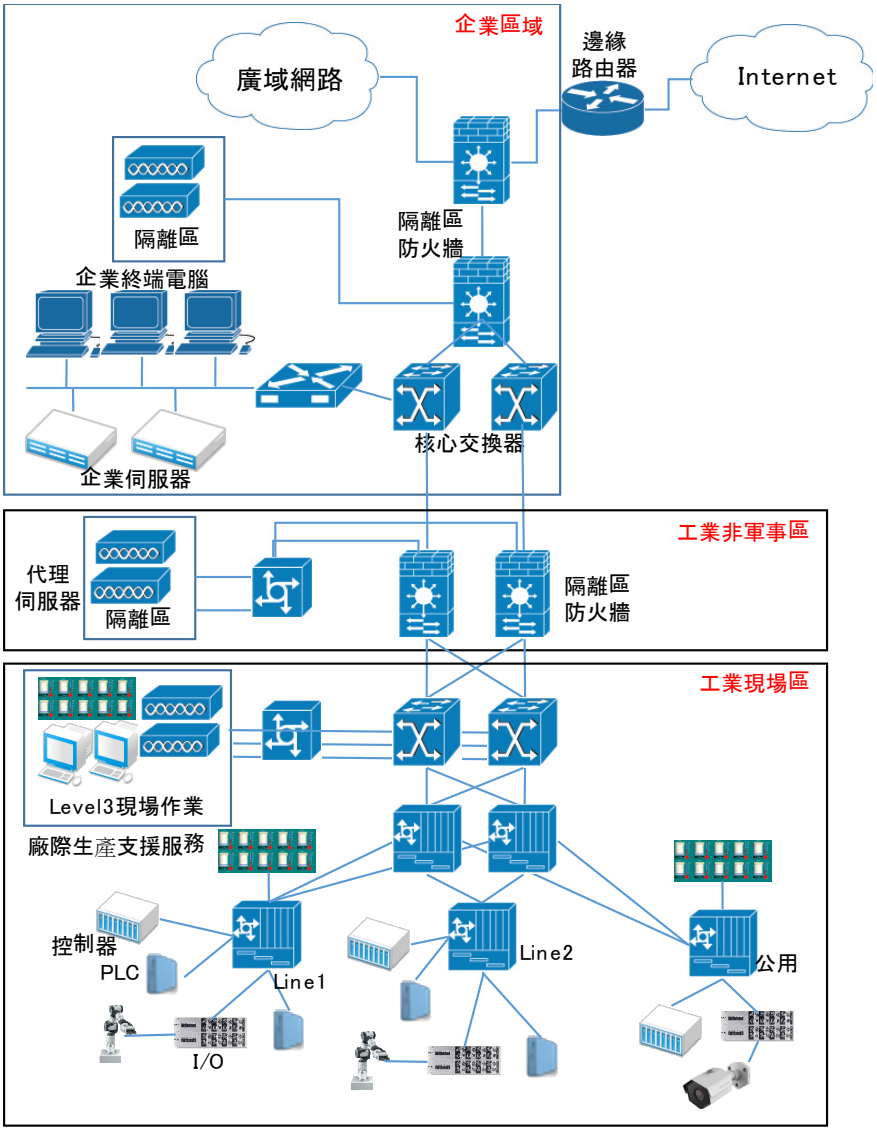


圖 30 IACS 參考示意架構

在圖中標示了 3 個區域，企業區域（Level 4/5）、工業非軍事區（Industrial Demilitarized Zone，IDMZ）及工業現場區或稱工控區域（Level 0~3）3 部份。另外，IACS 是工業生產技術中使用的各種控制系統和相關儀器，透過製程以達成共同的目標，例如製造產品或提供服務。 從高層次的角度來看，IACS 可以按其功能進行分類。 它們可以具有以下部分中討論的一個或多個功能:

- 視圖（View）功能：視圖功能包括即時監視自動化系統當前狀態的功能。 維運服務商、主管、維護工程師或其他人員可以使用此數據做出業務決策或執行糾正措施。 例如，當操作員看到炊具 1 的溫度變低時，他們可能決定增加炊具的蒸汽供應進行補償，使溫度上升至正常溫度值。 視圖過程本質上是被動的，僅僅為人類提供資訊或視圖以作出反應：

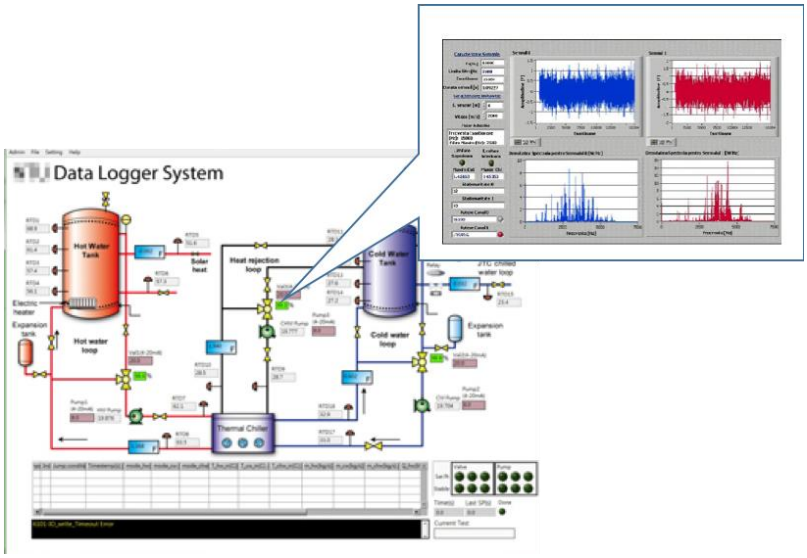


圖 31 視圖實例

從安全角度來看，如果攻擊者可以操弄操作員對控制系統狀態的看法，或者換句話說，可以更改操作員決策所依據的值，則攻擊者可以有效地控制製程中的物理或化學反應，從而完成整個製程。 例如，通過操弄炊具 1 的溫度的顯示值，攻擊者可以使操作者誤認為溫度太低或太高並且讓操作員對操弄的數據採取行動，造成製程產出的產物品質不佳，甚至發生工業災害。

- 監控(Monitor)功能：通常是控制迴路的一部分，例如在油箱中保持穩定水平的自動化。監視功能將密切關注臨界值，例如壓力、溫度及水位等，並將當前值與事先定義閾值進行比較，並根據監視功能的設置進行警報或互動操作。視圖功能和監視功能之間的關鍵區別在於確定偏差。對於監視功能，該確認及反應動作是自動化，而對於視圖功能，該確認及反應動作是由觀察值的人做出的。監視功能的反應範圍從彈出警報顯示器到全自動系統關閉程序。
  從安全角度來看，如果攻擊者可以控制監視器功能正在查看的值，則可以觸發或阻止該功能的反應;例如，監視系統正在查看炊具 1 的溫度，防止溫度超過 500 華氏度的情況。如果攻擊者向系統提供低於 500°F 的值，那麼該系統將被誘騙，誤判一切都很好，而實際上，系統可能會崩潰，甚至發生災害

- 控制（Control）功能:圖 32 說明控制功能的運作機制。

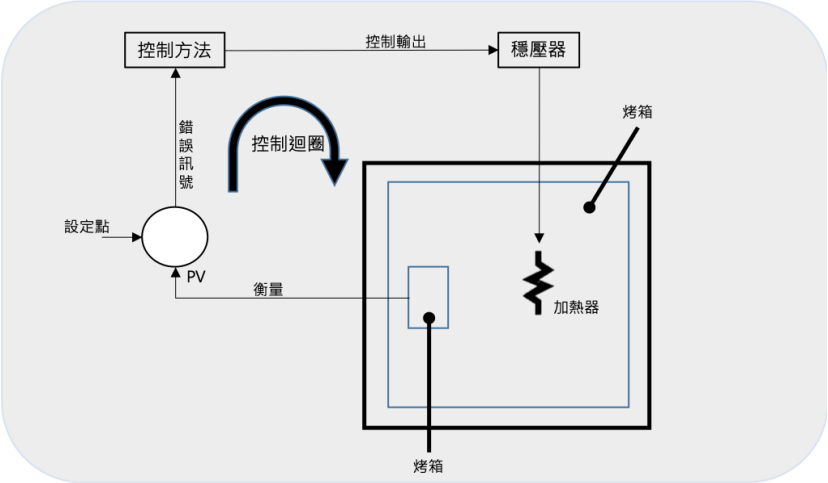


圖 32 控制功能運作機制

控制功能是控制、移動、觸發和啟動實體物件的機制。控制系統是使執行器接合、閥門打開和電機運作的原因。控制動作可以由操作員按下按鈕或改變 HMI 顯示器上的設定點來啟動，也可以是作為製程控制的一部分的自動回應。從安全角度來看，如果攻擊者可以操弄值（輸入），控制系統會對攻擊者做出反應，或者如果攻擊者可以設計用於或打算用於更改或操弄控制功能本身（控制程序），則可以欺騙系統進行操作。多數人都認為操弄這樣攻擊的手法是卓越且高難度，但是現在應該是無法通過現代交換網路和加密網路協議來完成。不幸的是，在大多數 IACS 網路中，CIA 安全分類的機密性和完整性部分的重要性不如可用性。更糟糕的是，對於大多數工業控制系統而言，可用性最終是構建系統時唯一的設計考慮因素。再加上在這些網路上運作的 IACS 通信協議從未考慮到安全性的事實，人們可以開始看到所提到場景的被攻擊的可行性。

基於上一節對 IACS 可能遭受內外部針對系統、元件及網路的攻擊，導致生產製造系統或是輔助的健康、安全及環境（health, safety and environmental，HSE）系統的攻擊，對系統可用性造成衝擊，甚至越權調整基礎設施服務設定或感應器的異常容許範圍，造成生產過程的偏差，導致品質下降甚至是發生災害。

3.3.1.1 設計及實作 IACS 控制措施限制因素

在 IT 環境中可用性大部份組織的考量是機密性優先於完整性及可用性，故 IT 環境會透過多重存取控制，如多重防火牆，或是加密、去識別化等資安控制措施，但往往會為了機密性而犧牲了完整性與可用性。但是如果運用在 IACS 或俗稱 OT 環境的控制措施設計就是要考量不會衝擊到可用性與完整性，並能維持基本控制功能的可用性。基本功能就是「維護健康、安全、環境（HSE）和受控設備(UCE)可用性所需的功能或能力」。 除非得到風險評估的支援權責人員作出決策，否則安全措施不得對高可用性 IACS 的基本功能產生不利影響。規劃和實施本章中描述的安全需求時，其安全控制措施的實施不應導致失去保護、失去控制、失去視圖或喪失其他基本功能。在進行風險分析後，某些設施可能會確定某些類型的安全措施可能會停止持續營運，但安全措施

不應導致喪失可能導致健康，安全和環境（HSE）後果的保護措施。一些具體的限制包括：

- 存取控制不得阻止基本功能的操作，具體而言：
  - 用於基本功能的帳戶不應被鎖定，即使是臨時的。
  - 驗證和記錄操作員操作以強制執行不可否認性不應增加系統回應時間的造成顯著延遲。
  - 對於高可用性控制系統，CA 憑證頒發機制的故障不得中斷基本功能。
  - 身分識別和認證不應阻止安全儀器功能（Safety Instrumented function , SIF）的發起。同樣，對於授權實施亦相同。
- 產生錯誤時間戳記的稽核記錄，不得對基本功能產生不利影響。
- 如果區域邊界保護機制進入失效關閉或孤島模式，則應保持 IACS 的基本功能。
- 控制系統或安全儀表系統（SIS）網路上的拒絕服務（DoS）事件不得阻止 SIF 發揮作用。

實際運用在構成工控物聯網（連網的生產環境 IACS）的控制系統及元件相當多元，在本指南主要以「控制系統」與「元件」兩部份來描述 IIoT 的功能需求（Functional Requirement, FR）及安全需求 （Security Requirement, SR）。

3.3.2 控制系統(Control System, CS)安全控制技術要求

控制系統區分功能需求如下：

功能需求編號	功能需求分類
FR 1	識別和認證控制(Identification and authentication control, IAC)
FR2	使用控制(Use control, UC)
FR 3	系統完整性(System integrity, SI)
FR 4	資料機密性 (Data confidentiality, DC)
FR 5	受限制的資料流 (Restricted data flow, RDF)
FR 6	及時回應事件 (Timely response to events, TRE)
FR 7	資源可用性 (Resource availability, RA)

3.3.2.1 FR 1 識別和認證控制（IAC）

區分	內容
目的	在允許所有使用者存取控制系統之前，識別並驗證所有使用者（人員、軟體程序和設備）。

安全等級區分	·SL1 – 通過防止未經身份驗證的實體偶然或偶然存取的機制來識別和驗證所有使用者（人員、軟體程序和設備）。 ·SL2 – 通過機制識別和驗證所有使用者（人員、軟體程序和設備），這些機制使用簡單的資源，一般技能和低動機來防止實體有意未經身份驗證的存取。 ·SL3 – 通過機制識別和驗證所有使用者（人員、軟體程序和設備），這些機制使用具有適度資源，IACS 特定技能和適度動機的複雜手段防止有意未經身份驗證的存取。 ·SL4 – 通過機制識別和驗證所有使用者（人員、軟體程序和設備），防止實體使用具有擴展資源，IACS 特定技能和高動力的複雜手段進行有意的未經身份驗證的存取。
功能要求說明	資產擁有者必須製作所有使用者（人員、軟體程序和設備）的列表，並為每個控制系統元件確定所需的 IAC 保護等級。 IAC 的目標是通過在啟動通信之前驗證請求存取控制系統的任何使用者的身份來保護控制系統。 建議和指引應包括將以混合模式運作的機制。 例如，某些控制系統元件需要強大的 IAC，例如強認證機制，而其他元件則不需要。

3.2.2.1.1 FR 1 識別和認證控制（IAC）的安全要求清單

安全要求編號	安全要求名稱
SR 1.1	人類使用者識別和認證
SR 1.2	軟體程序和裝置識別和認證
SR 1.3	帳戶管理
SR 14	身份識別管理
SR 1.5	驗證器管理
SR 1.6	無線網路存取管理
SR 1.7	基於密碼的身份驗證的強度
SR 1.8	公鑰基礎結構（PKI）憑證
SR 1.9	公鑰認證的強度
SR 1.10	驗證器反饋
SR 1.11	登錄嘗試失敗
SR 1.12	系統使用通知
SR 1.13	通過不受信任的網路存取

有關系統安全控制要求檢核表，請參考附錄 C「系統安全技術要求檢核表」

3.2.2.1.2 SR 1.1 人類使用者識別和認證

編號	區分	內容
SR 1.1	基本要求	控制系統應提供識別和驗證所有人類使用者的能力。 此功能應在所有介面上強制執行此類身份識別和認證，這些介面為人類使用者提供對控制系統的存取，以根據適用的安全政策和程序支援職責分離和最小特權。
SR 1.1	說明	需要識別和驗證所有人類使用者以存取控制系統。應該通過使用諸如密碼、令牌、生物辨識等方法來完成對人類使用者

		的身份的認證，或者在多因素認證的情況下，使用它們的某種組合來完成對這些使用者的身份的認證。 人類使用者的地理位置也可以用作身份驗證過程的一部分。此要求應適用於對控制系統的本地和遠端存取。除了在控制系統等級識別和驗證所有人類使用者（例如，在系統登錄時），通常在應用程式等級使用識別和認證機制。 在人類使用者作為單一群組（例如控制室操作員）運作的情況下，使用者識別和認證可以是基於角色的或基於群組的。對於某些控制系統，提供操作員直接互動的能力是非常重要。當地的緊急行動以及控制系統的基本功能不得因識別或認證要求而受到阻礙。可以通過適當的實體安全機制來限制對這些系統的存取。這種情況的一個例子是關鍵操作室，其中存在嚴格的實體存取控制和監視，以及輪班計劃將責任分配給一組使用者。然後，這些使用者可能正在使用相同的使用者身份。此外，應對指定的操作員工作站客戶端進行身份驗證（SR 1.2 – 軟體程序和設備身分識別和身份驗證），或者此共享帳戶的使用應限於控制室的保護環境。 為了支援 IAC 政策，控制系統作為第一步驗證所有人類使用者的身份。在第二步中，強制分配給已識別的人類使用者的權限（參見 SR 2.1 – 授權實施）。
SR 1.1 RE(1)	增項要求	（1）唯一的識別和認證 控制系統應提供唯一識別和驗證所有人類使用者的能力。
SR 1.1 RE(2)	增項要求	（2）不可信任網路的多因素認證 控制系統應提供使用多因素身份驗證的能力，以便人類使用者通過不受信任的網路遠端存取控制系統（SR 1.13 – 通過不受信任的網路存取）。
SR 1.1 RE(3)	增項要求	（3）所有網路的多因素認證 控制系統應提供對所有人類使用者存取控制系統採用多因素認證的能力。
SR 1.1 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.1 ·SL-C（IAC，控制系統）2：SR 1.1（1） ·SL-C（IAC，控制系統）3：SR 1.1（1）（2） ·SL-C（IAC，控制系統）4：SR 1.1（1）（2）（3）

3.2.2.1.3 SR 1.2 軟體程序和裝置識別和認證

編　　號	區　　分	內　　容
SR 1.2	基本要求	控制系統應提供識別和驗證所有軟體程序和裝置的能力。 此功能應在所有介面上強制執行此類身分識別和身份驗證，這些介面提供對控制系統的存取，以根據適用的安全政策和程序支援最小權限。
SR 1.2	說明	識別和認證的功能是將 ID 對應到未知的軟體程序或裝置（以下稱為本控制措施中的元件），以便

		在允許任何資料交換之前使其知曉。允許惡意元件發送和接收控制系統特定資料可能導致合法控制系統遭受有害行為。 需要識別和驗證所有元件，以便對控制系統進行所有存取控制。應通過使用諸如密碼，令牌或位置（實體或邏輯）之類的方法來完成對這些元件的身份的認證。此要求應適用於對控制系統的本地和遠端存取。但是，在使用單個元件連接到不同目標系統的某些情況下（例如，遠端供應商服務支援），元件具有多個身份識別在技術上可能是不可行的。在這些情況下，必須採用補償措施。 需要針對所有元件的身分識別和認證機制來防止諸如中間人或訊息欺騙之類的攻擊。在某些情況下，這些機制可能涉及在同一實體伺服器上運作的多個軟體程序，每個軟體程序都有自己的身份。在其他情況下，身份認證可以綁定到實體裝置，例如在特定 PLC 上運作的所有軟體程序。 在識別和驗證可攜式和行動裝置時，需要特別注意。這些類型的裝置是將不希望的網路流量、惡意軟體或資訊外洩引入控制系統（包括其他隔離網路）的已知方法。 在元件作為單一群組運作的情況下，身分識別和認證可以是基於角色的、基於群組的或基於元件的。是非常重要的是，當地的緊急行動以及控制系統的基本功能不得因識別或認證要求而受到阻礙。例如，在一般的保護和控制方案中，一組裝置聯合執行保護功能，並與群組內的裝置之間的多播訊息通信。在這些情況下，通常使用基於共享帳戶或共享對稱密鑰的群組認證機制。 為了支援識別和認證控制政策，控制系統作為第一步驗證所有實體的身份。在第二步中，強制分配給所有身分識別個體元件的權限（參見 SR 2.1 – 授權實施）。
SR 1.2 RE(1)	增項要求	（1）唯一的識別和認證 控制系統應提供唯一識別和驗證所有軟體程序和裝置的能力。
SR 1.2 SL-C	安全等級	·SL-C（IAC，控制系統）1：未選用 ·SL-C（IAC，控制系統）2：SR 1.2 ·SL-C（IAC，控制系統）3：SR 1.2（1） ·SL-C（IAC，控制系統）4：SR 1.2（1）

3.2.2.1.4 SR 1.3 帳戶管理

編號	區分	內容
SR 1.3	基本要求	控制系統應提供授權使用者管理所有帳戶的能力，包括新增、啟用、修改、禁用和刪除帳戶。
SR 1.3	說明	帳戶管理可以包括建立帳戶群組（例如，個人、基於角色、基於裝置和控制系統），組成員資格條件的建立和相關授權的分配。在某些 IACS 實例中，如果從風險分析或監管方面確定個人帳戶是不必要的，只要有適當的補償對策（例如有限的實體存取或組織的核准措施），就可以接受共享帳戶及記錄。 用於軟體程序間處理通信的非人類使用者帳戶（有時稱為服務帳戶）（例如，控制伺服器到歷史記錄器和 PLC 用於控制伺服器）通常需要來自人類使用者帳戶的不同安全政策和程序。為了增強安全性，帳戶管理應根據統一的政策進行，並在本地部署在控制系統的相關元件中。用於首次安裝系統的未使用的預設系統帳戶應該是可移除的。安全性增強在於帳戶管理的簡化和一致應用。
SR 1.3 RE(1)	增項要求	（1）統一帳戶管理 控制系統應提供支援統一帳戶管理的能力。
SR 1.3 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.3 ·SL-C（IAC，控制系統）2：SR 1.3 ·SL-C（IAC，控制系統）3：SR 1.3（1） ·SL-C（IAC，控制系統）4：SR 1.3（1）

3.2.2.1.5 SR 1.4 身份識別管理

編號	區分	內容
SR 1.4	基本要求	控制系統應提供支援使用者、群組、角色或控制系統介面管理身份識別的能力。
SR 1.4	說明	身份識別區別於它們允許實體在特定控制系統控制領域（control domain）或區域內執行的權限（參見 SR 2.1 – 授權實施）。人類使用者作為單一群組運作的地方（如控制室操作員），使用者識別可以是基於角色的、基於群組的或基於裝置的。對於某些控制系統，直接操作員與互動的能力是是非常重要的。控制系統的本地緊急行動不應受到身分識別要求的阻礙。系統可能受到適當的補償對策的控管。控制系統的部分可能需要身份識別，但不一定是整個控制系統。例如，無線裝置通常需要身份識別，而有線裝置可能不需要。

SR 1.4	增項要求	無
SR 1.4	安全等級	·SL-C（IAC，控制系統）1：SR 1.4 ·SL-C（IAC，控制系統）2：SR 1.4 ·SL-C（IAC，控制系統）3：SR 1.4 ·SL-C（IAC，控制系統）4：SR 1.4

3.2.2.1.6 SR 1.5 驗證器管理

編　　號	區　　分	內　　容
SR 1.5	基本要求	控制系統應提供以下能力： a）初始化驗證器內容; b）在控制系統安裝時更改所有預設驗證器; c）更改/刷新所有驗證器; 和 d）保護所有驗證器在儲存和傳輸時不被未經授權的洩露和修改。
SR 1.5	說明	除了身份識別（SR 1.4 – 身份識別管理）之外，還需要驗證器來證明身份。控制系統驗證器包括但不限於令牌、對稱密鑰、私鑰（公鑰/私鑰的一部分）生物辨識、密碼、實體密鑰和密鑰卡。人類使用者應採取合理措施保護身份驗證器，包括保持其個人身份驗證器的所有權，不得借用他人或共享身份驗證器，並立即報告遺失或受損的身份驗證器。身份驗證器有一個生命週期。自動建立帳戶時，需要建立新的身份驗證器，以便帳戶所有者能夠進行身份驗證。例如，在基於密碼的系統中，該帳戶具有與其關聯的密碼。初始驗證器內容的定義可以解釋為管理員定義帳戶管理系統為所有新帳戶設置的初始密碼。能夠設定這些初始值使攻擊者更難以猜測帳戶建立和第一次帳戶使用之間的密碼（這應該涉及帳戶所有者設置新密碼）。某些控制系統安裝有無人監看的安裝程序，這些安裝程序使用預設密碼建立所有必需的帳戶，而某些嵌入式裝置隨附預設密碼。隨著產品上市時間的拉長，這些密碼通常成為公開的秘密，並可以 Internet 上搜尋到。能夠更改預設密碼可以保護系統免受未經授權的使用者使用預設密碼進行存取。在網路身份驗證中使用時，可以從儲存或傳輸中獲取密碼。這種複雜性可以通過諸如加密或雜湊之類的加密保護或者根本不需要傳輸密碼的交握協議來增加。但是，密碼可能會受到攻擊，例如，暴力破解或破壞傳輸或儲存中密碼的加密保護。可以通過定期更改/刷新密碼來減少機會之窗。類似的考慮適用於基於加密密鑰的認證系統。通過使用硬體機制，如可信任平台模組（TPM）、硬體密碼模組（Hardware Security Module, HSM）等硬體安全模組，可以建立增強的保護。 應在適用的安全政策和過程中指定驗證器的管理，例如，更改預設驗證器的約束、刷新周期、驗證器保護規範或緊急存取控制系統程序（類似在火警時

		會跳脫平時的實體門禁的存取控管以利人員逃生）。 由於安全措施而導致的鎖定或失控是不可接受的。如果要求控制系統具有高水準的可用性，則應採取措施來保持這種高水準的可用性（例如補償實體對策、複製密鑰和監督覆蓋）。 除了此要求中指定的身份驗證器管理功能外，身份驗證機制的強度還取決於所選身份驗證器的強度（例如密碼複雜性或公鑰身份驗證中的密鑰長度）以及在身份驗證過程中驗證身份驗證器的政策（例如，密碼有效期多長或在公鑰憑證驗證中執行哪些檢查）。對於最常見的身份驗證機制，基於密碼和公鑰的身份驗證 SR 1.7 – 基於密碼的身份驗證的強度，SR 1.8 – 公鑰基礎結構（PKI）憑證和 SR 1.9 – 公鑰身份驗證的強度進一步提供要求。
SR 1.5 RE(1)	增項要求	（1）軟體程序身份憑證的硬體安全性 對於軟體程序和裝置使用者，控制系統應提供通過硬體機制保護相關驗證器的能力。
SR 1.5 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.5 ·SL-C（IAC，控制系統）2：SR 1.5 ·SL-C（IAC，控制系統）3：SR 1.5（1） ·SL-C（IAC，控制系統）4：SR 1.5（1）

3.2.2.1.7 SR 1.6 無線網路存取管理

編　　號	區　　分	內　　容
SR 1.6	基本要求	控制系統應提供識別和驗證從事無線通信的所有使用者（人、軟體程序或裝置）的能力。
SR 1.6	說明	任何無線技術都可以，並且在大多數情況下應該被視為另一種通信協議選項，因此與 IACS 使用的任何其他通信類型具有相同的 IACS 安全要求。 但是，從安全的角度來看，存在有線和無線通信之間至少有一個顯著差異：實體安全對策在使用無線時效率通常較低。出於這個原因和可能的其他原因（例如監管差異），風險分析可能合法地導致更高的 SL-T（IAC，控制系統）用於無線通信而不是在相同的使用情境中使用的有線協議。 無線技術包括但不限於微波、衛星、封包無線電、電氣和電子工程師協會（IEEE）802.11x，IEEE 802.15.4（ZigBee，IEC 62591-WirelessHART®，ISA-100.11a），IEEE 802.15 .1（藍牙），無線區

		域網路行動路由器，帶有網路共享的行動電話(4G/5G)和各種红外線技術等。
SR 1.6 RE(1)	增項要求	（1）唯一的識別和認證 控制系統應提供唯一識別和認證從事無線通信的所有使用者（人、軟體程序或裝置）的能力。
SR 1.6 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.6 ·SL-C（IAC，控制系統）2：SR 1.6（1） ·SL-C（IAC，控制系統）3：SR 1.6（1） ·SL-C（IAC，控制系統）4：SR 1.6（1）

3.2.2.1.8 SR 1.7 基於密碼的身份驗證的強度

編　　號	區　　分	內　　容
SR 1.7	基本要求	對於使用基於密碼的認證的控制系統，控制系統應提供基於最小長度和各種字元類型強制可設定密碼強度的能力。
SR 1.7	說明	基於使用者名和密碼的使用者身份驗證是一種最簡易且常用的機制。對此類機制的許多攻擊都集中在猜測密碼（例如，字典攻擊或有針對性的社交工程攻擊）或破壞儲存密碼表示的加密保護（例如，使用彩虹表或暴力破壞雜湊函數衝突）。 通過增加允許字元數來增加有效密碼集的大小會使這種攻擊更加複雜，但只有在實際使用增加的集合大小時（通常使用者在密碼中不會包含特殊字元，因為它們被視為更難記住）。限制密碼的生命週期會降低攻擊者違反特定密碼保密的機會。 為了防止使用者通過將密碼更改為新密碼然後立即更改回其原始密碼來繞過此控制，通常也會強制執行密碼的最短生命週期。在到期之前更改密碼的通知允許使用者根據過程操作條件在方便的時間更改密碼。 通過限制密碼的重用（防止僅在少數常用密碼更換使用）可以進一步增強這種保護，這進一步降低了曾經破壞的密碼的有用性。使用多因素身份驗證可以建立超出基於密碼的機制的擴展保護（參見 SR 1.1 – 人類使用者識別和身份驗證以及 SR 1.2 – 軟體程序和裝置識別和身份驗證）。
SR 1.07 RE(1)	增項要求	（1）人類使用者的密碼產生和生命週期限制 控制系統應提供防止任何特定的人類使用者帳戶在可設定的代數中重複使用密碼的能力。 此外，控制系統應提供對人類使用者實施密碼最短和最長有效週期限制的能力。 這些功能應符合普遍接受的安全產業實務常見

		做法。 注意：這是一種普遍接受的良好實行，控制系統提供了在到期前的可設定時間內提示使用者更改其密碼的功能。
SR 1.7 RE(2)	增項要求	（2）所有使用者的密碼生存期限制 控制系統應提供對所有（不限人類）使用者實施密碼最短和最長有效週期限制限制的能力。
SR 1.7 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.7 ·SL-C（IAC，控制系統）2：SR 1.7 ·SL-C（IAC，控制系統）3：SR 1.7（1） ·SL-C（IAC，控制系統）4：SR 1.7（1）（2）

3.2.2.1.9 SR 1.8 公鑰基礎結構（PKI）憑證

編　　號	區　　分	內　　容
SR 1.8	基本要求	公鑰基礎結構（PKI）憑證 在使用 PKI 的情況下，控制系統應提供根據普遍接受的最佳實務操作 PKI 的能力或從現有 PKI 獲得公鑰憑證。
SR 1.8	說明	接收公鑰憑證的註冊需要包括主管或權責人員的授權，並且需要使用安全流程來完成，該流程驗證憑證持有者的身份並確保憑證頒發給正確的目標使用者。任何延遲使用公鑰憑證引起的不應降低控制系統的運作效能。 選擇適當的 PKI 應考慮組織的憑證政策，該政策應基於違反受保護資訊機密性的風險。關於政策定義的指導可以在普遍接受的標準和指南中找到，例如基於 X.509 的 PKI 的網際網路工程任務組（IETF）評論請求（RFC）3647。例如，憑證頒發機構（CA）的適當位置，無論是在控制系統內還是在 Internet 上，以及可信 CA 的列表都應該在政策中考慮，並且取決於網路架構。
SR 1.8 RE	增項要求	無
SR 1.8 SL-C	安全等級	· SL-C(IAC, 控制系統) 1: 未選用 · SL-C(IAC, 控制系統) 2: SR 1.8 · SL-C(IAC, 控制系統) 3: SR 1.8 · SL-C(IAC, 控制系統) 4: SR 1.8

3.2.2.1.10　SR 1.9 公鑰認證的強度

編　　號	區　　分	內　　容

SR 1.9	基本要求	公鑰認證的優勢 對於使用公鑰認證的控制系統，控制系統應提供以下能力： a）通過檢查特定憑證的簽名的有效性來驗證憑證; b）通過構建到接受的 CA 的憑證路徑來驗證憑證，或者在自簽名（self signed）憑證的情況下，通過將葉子憑證部署到與頒發憑證的主體進行通信的所有主機來驗證憑證; c）通過檢查特定憑證的撤銷狀態來驗證憑證; d）建立對應私鑰的使用者（人、軟體程序或裝置）控制; 和 e）將經過身份驗證的身份對應到使用者（人員，軟體程序或裝置）。
SR 1.9	說明	公鑰/私鑰加密機制很大程度上取決於特定主體的私鑰的保密性以及對信任關係的正確處理。在基於公鑰認證驗證兩個實體之間的信任時，必須將公鑰憑證追溯到可信實體。憑證驗證中的常見建立錯誤是僅檢查憑證籤名的有效性，但不檢查簽名者中的信任。在 PKI 設置中，如果簽名者是受信任的 CA 或具有由受信任 CA 頒發的憑證，則受信任者是受信任的，因此所有驗證器都需要將呈現給他們的憑證追溯回受信任的 CA.如果無法建立這樣的可信任 CA 鏈，則不應信任所呈現的憑證。 如果使用自簽名憑證而不是 PKI，則憑證主體本身會對其憑證進行簽名，因此永遠不會存在受信任的第三方或 CA 作為上層驗證驗證本地簽名為有效機制，這應該通過將自簽名公鑰憑證部署到需要通過其他安全機制驗證它們的所有相對方（例如，受信任環境中所有相對方的設定）來進行補償。需要通過安全通道將可信憑證分發給相對方。在驗證過程中，只有在自簽名憑證已存在於驗證相對方的可信憑證列表中時，才應信任該自簽名憑證。應將受信任憑證集設定為最小必需集。 在這兩種情況下，驗證還需要考慮撤銷憑證的可能性。在 PKI 設置中，這通常通過維護憑證撤銷列表（CRL）或運作線上憑證狀態協議（OCSP）伺服器來完成。 當由於控制系統約束而無法進行撤銷檢查時，諸如憑證壽命短的機制可以補償缺少及時的撤銷資訊。請注意，短壽命憑證有時會在控制系統環境中產生重大的操作問題。
SR 1.9 RE(1)	增項要求	（1）公鑰認證的硬體安全性 控制系統應根據普遍接受的安全產業實務常見做法和建議，通過硬體機制提供保護相關私鑰的能力。

SR 1.9 SL-C	安全等級	·SL-C（IAC，控制系統）1：未選用 ·SL-C（IAC，控制系統）2：SR 1.9 ·SL-C（IAC，控制系統）3：SR 1.9（1） ·SL-C（IAC，控制系統）4：SR 1.9（1）

3.2.2.1.11 SR 1.10 驗證器反饋

編號	區分	內容
SR 1.10	基本要求	控制系統應提供在認證程序中遮蔽認證資訊反饋的能力。
SR 1.10	說明	遮蔽反饋保護資訊免受未經授權的個人的可能利用，例如，當人類使用者輸入密碼時顯示星號或其他隨機字元掩蓋了認證資訊的反饋。 其他例子包括無線網路常用加密演算法 WEP 密鑰，SSH 令牌輸入和 RSA 一次性密碼的輸入。 身份驗證實體不應提供有關身份驗證失敗原因的任何提示，例如未知使用者名稱。
SR 1.10 RE	增項要求	無
SR 1.10 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.10 ·SL-C（IAC，控制系統）2：SR 1.10 ·SL-C（IAC，控制系統）3：SR 1.10 ·SL-C（IAC，控制系統）4：SR 1.10

3.2.2.1.12 SR 1.11 登錄嘗試失敗

編號	區分	內容
SR 1.11	基本要求	登錄嘗試失敗 控制系統應提供在可設定的時間區段內強制限制任何使用者（人、軟體程序或裝置）的有限次數的連續無效存取嘗試的能力。 控制系統應提供在指定的時間區段內拒絕存取的能力，或者在超過此限制時由管理員解鎖的能力。 對於代表運作關鍵服務或伺服器的系統帳戶，控制系統應提供禁止互動式登錄的能力。
SR 1.11	說明	由於可能產生拒絕服務攻擊，可能會限制連續無效存取嘗試的次數。 如果啟用，則控制系統可以在由適用的安全政策和過程建立的預定時間區段之後自動重置為零存取嘗試次數。 將存取嘗試重置為零將

		允許使用者（人員、軟體程序或裝置）獲得存取權限，如果他們具有正確的登錄身份識別。 在緊急情況下需要立即操作員回應時，不應使用控制系統操作員工作站或節點的自動拒絕存取。 所有鎖定機制應考慮連續操作的功能要求，以減輕可能導致系統完全失效或人員受傷的不利拒絕服務操作條件。 允許對用於關鍵服務的帳戶進行互動式登錄可能會導致拒絕服務或其他濫用行為。
SR 1.11RE	增項要求	無
SR 1.11 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.11 ·SL-C（IAC，控制系統）2：SR 1.11 ·SL-C（IAC，控制系統）3：SR 1.11 ·SL-C（IAC，控制系統）4：SR 1.11

3.2.2.1.13 SR 1.12 系統使用通知

編號	區分	內容
SR 1.12	基本要求	控制系統應提供在驗證之前顯示系統使用通知訊息（顯示警語）的能力。 系統使用通知訊息內容應由授權人員設定。
SR 1.12	說明	隱私和安全政策和程序需要與適用的法律、指令、政策、法規、標準和指南保持一致。通常，這一要求的主要、特別是對違法者進行法律起訴並證明有意違反。因此，此功能必須支援政策要求，並且不會提高IACS安全性。系統使用通知訊息可以以個人登錄控制系統時顯示的警告橫幅的形式建立。在控制系統工具中作為發布的實體通知實施的警告橫幅不能防止遠端登錄問題。 包含在系統使用通知訊息中的元素例子如下： a）個人正在存取特定的控制系統; b）可以監控、記錄系統使用情況並進行審核; c）禁止未經授權使用該系統，並受到刑事或民事處罰;和 d）使用該系統表示同意監測和記錄。
SR 1.12 RE	增項要求	無

SR 1.12 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.12 ·SL-C（IAC，控制系統）2：SR 1.12 ·SL-C（IAC，控制系統）3：SR 1.12 ·SL-C（IAC，控制系統）4：SR 1.12

3.2.2.1.14 SR 1.13 通過不受信任的網路存取

編號	區分	內容
SR 1.13	基本要求	控制系統應提供監視和控制通過不可信任網路存取控制系統的所有方法的能力。
SR 1.13	說明	通過不可信任網路存取控制系統的例子，通常包括遠端存取方法（例如撥接、寬頻和無線網路）以及來自公司辦公室（非控制系統）網路的連接。 控制系統應限制通過撥接連接建立的存取（例如，根據請求源限制撥號存取）或防止未授權連接或覆蓋授權連接（例如，使用虛擬專用網路（VPN））技術。 只有在必要和認證時，才能通過不受信任的網路存取地理位置遠端控制系統元件位置（例如，控制中心和現場位置）。 安全政策和過程可能需要多因素身份驗證，以便遠端使用者存取控制系統。
SR 1.13 RE(1)	增項要求	（1）明確的存取請求核准 除非得到權責人員的核准，否則控制系統應拒絕提供通過不受信任網路的存取請求的能力。
SR 1.13 SL-C	安全等級	·SL-C（IAC，控制系統）1：SR 1.13 ·SL-C（IAC，控制系統）2：SR 1.13（1） ·SL-C（IAC，控制系統）3：SR 1.13（1） ·SL-C（IAC，控制系統）4：SR 1.13（1）

3.2.2.2 FR 2 使用控制

編號	區分	內容
FR2	目的	實施經過身份驗證的使用者（人員、軟體程序或裝置）的分配權限，以在 IACS 上執行請求的操作並監視這些權限的使用。
FR2	安全等級區分	·SL1 – 根據指定的特權限制使用 IACS，以防止偶然或巧合的濫用。 ·SL2 – 根據指定的特權限制使用 IACS，以防止實體使用資源較少，一般技能和動機較低的簡單手段進行規

		避。 ·SL3 – 根據指定的特權限制使用 IACS，以防止實體使用具有適度資源，IACS 特定技能和適度動機的複雜手段進行規避。 ·SL4 – 根據指定的權限限制 IACS 的使用，以防止實體使用具有擴展資源，IACS 特定技能和高動力的複雜手段進行規避。
FR2	功能要求說明	一旦識別並驗證了使用者，控制系統就必須將允許的動作限制為控制系統的授權使用。資產擁有者和系統整合商必須為每個使用者（人員、軟體程序或裝置）、群組、角色等（SR 1.4 – 身份識別管理）分配定義 IACS 授權使用的特權。使用控制的目標是通過在允許使用者執行操作之前驗證已經授予必要的特權來防止對控制系統資源的未授權操作。動作的例子是讀取或寫入資料、下載程序和設置設定。建議和指南應包括將以混合模式運作的機制。例如，某些控制系統資源需要強大的使用控制保護，例如限制性特權，而其他控制系統資源則不需要。通過擴展，需要將使用控制要求擴展到靜態資料。使用者權限可能會根據時間/日期，位置和存取方式而有所不同。

3.2.2.2.1FR 2 使用控制的安全要求清單

安全要求編號	安全要求名稱
SR 2.1	授權執行
SR 2.2	無線網路使用控制
SR 2.3	無線網路使用控制
SR 2.04	行動程式碼
SR 2.05	會話鎖定
SR 2.06	遠端會話終止
SR 2.07	會話總量控制
SR 2.08	可稽核的事件
SR 2.09	稽核儲存容量
SR 2.10	對稽核處理失敗的回應
SR 2.11	時間戳記
SR 2.12	不可否認

3.2.2.2.2 SR 2.1 授權執行

編　　號	區　　分	內　　容
SR 2.1	基本要求	在所有介面上，控制系統應提供執行分配給所有人類使用者的授權的能力，以控制 IACS 系統的使用，以支援職責分離和最小特權。
SR 2.1	說明	使用控制政策（例如，基於身份的政策、基於角色的政策和基於規則的政策）和相關的讀/寫存取強制機制（例如，存取控制列表、存取控制矩陣和加密）來控制兩者之間的使用使用者（人員、軟體程序和裝置）和資產（例如：裝置、文件、記錄、軟體程序、程式和安全領域）。 在控制系統驗證了使用者（人員、軟體程序或裝置）的身份後（參見 SR 1.1 – 人類使用者識別和認證以及 SR 1.2 – 軟體程序和裝置識別和認證），它還必須根據定義的安全政策和過程驗證是否實際允許所請求的操作。例如，在基於角色的存取控制政策中，控制系統將檢查分配給已驗證使用者或資產的角色以及分配給這些角色的權限，如果請求的操作由權限覆蓋，則執行，否則拒絕。這允許執行職責分離和最小特權。不應允許使用執行機制對控制系統的運作效能產生不利影響。 對控制系統元件的計劃內或計劃外更改可能對控制系統的整體安全性產生重大影響。因此，只有合格和授權的個人才能獲得控制系統元件的使用，以便啟動變更，包括升級和修改。
SR 2.1 RE(1)	增項要求	（1）所有使用者的授權執行 在所有介面上，控制系統應提供執行分配給所有使用者（人員、軟體程序或裝置）的授權的能力，以控制 IACS 的使用，以支援職責分離和最小特權。
SR 2.1 RE(2)	增項要求	（2）權限對應到角色 控制系統應為授權使用者或角色提供定義和修改所有人類使用者角色權限對應的能力。 註 1：將角色限制為固定嵌套層次結構是一種普遍接受的良好做法，其中較高等級的角色是較低權限角色的超集。 例如，系統管理員通常不一定包含操作員權限。 註 2：該增項要求也適用於軟體程序和裝置。
SR 2.1 RE(3)	增項要求	（3）主管覆蓋 控制系統應支援主管手動覆蓋當前人類使用者授權的可設定時間或事件序列。 註：通常需要在發生緊急情況或其他嚴重事件時實施受控，稽核和手動覆蓋自動化機制。 這允許管理員使操作員能夠快速回應異常情況，而無需關閉當前會話並建立新會話作為更高權限的人類使用者。

SR 2.1 RE(4)	增項要求	（4）雙重核准 控制系統應支援雙重核准（Dual control），其中一項行動可能對工業程序產生嚴重影響。 註：將雙重核准限制為需要非常高度可靠且可靠且正確執行的操作，這是一種普遍接受的良好做法。 要求雙重核准強調了由於未採取正確行動而導致的嚴重後果。需要雙重核准的情況的一個例子是改變關鍵工業程序的設定點。 當需要立即回應以保護 HSE 後果（例如，緊急關閉工業製程）時，不採用雙重審批機制是一種普遍接受的良好做法。
SR 2.1 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.1 ·SL-C（UC，控制系統）2：SR 2.1（1）（2） ·SL-C（UC，控制系統）3：SR 2.1（1）（2）（3） ·SL-C（UC，控制系統）4：SR 2.1（1）（2）（3）（4）

3.2.2.2.3 SR 2.2 無線網路使用控制

編　　號	區　　分	內　　容
SR 2.2	基本要求	根據普遍接受的安全產業實務常見做法，控制系統應提供授權、監控和實施無線連接控制系統的使用限制的能力。
SR 2.2	說明	任何無線技術都可以並且在大多數情況下應該被視為另一種通信協議選項，因此受 IACS 安全性要求與 IACS 使用的任何其他通信類型相同。 然而，風險分析可能導致要求無線 IACS 元件支援此相同使用情境和 SL-T 的有線系統通常所需的更高的使用控制能力。 監管差異還可能導致有線和無線通信之間所需的不同能力。 如 SR 1.6 – 無線網路存取管理，無線技術包括但不限於微波，衛星，群組無線電，IEEE 802.11x，IEEE 802.15.4（ZigBee，IEC 62591 – WirelessHART®，ISA-100.11a） ），IEEE 802.15.1（藍牙），無線區域網路行動路由器，帶有網路共享的行動電話和各種红外線傳輸技術。
SR 2.2 RE(1)	增項要求	（1）識別並報告未經授權的無線裝置 控制系統應提供識別和報告在控制系統實體環境中傳輸的未授權無線裝置的能力。
SR 2.2 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.2 ·SL-C（UC，控制系統）2：SR 2.2 ·SL-C（UC，控制系統）3：SR 2.2（1） ·SL-C（UC，控制系統）4：SR 2.2（1）

3.2.2.2.4 SR 2.3 對可攜式和行動裝置使用控制

編　　號	區　　分	內　　容
SR 23	基本要求	控制系統應提供自動執行可設定使用限制的功能，包括： a）防止使用可攜式媒體和行動裝置; b）要求具體情況的授權; 和 c）限制與可攜式和行動裝置之間的程式碼和資料傳輸。
SR 2.3	說明	可攜式媒體和行動裝置可能會引入不需要的網路流量、惡意軟體或資訊外洩，因此在典型的控制系統環境中應該有與其使用相關的特定控制。安全政策和程序可能不允許通過可攜式媒體和行動裝置的某些功能或活動。 保護可攜式媒體和行動裝置上的資訊（例如，在儲存期間以及在受控區域之外的傳輸過程中使用加密機制來提供機密性和完整性保護）在其他地方有所涉及（參見 FR 4 - 資料機密性）。
SR 2.3 RE(1)	增項要求	（1）執行可攜式媒體和行動裝置的安全狀態 控制系統應提供驗證試圖連接到區域的可攜式或行動裝置是否符合該區域的安全要求的能力。
SR 2.3 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.3 ·SL-C（UC，控制系統）2：SR 2.3 ·SL-C（UC，控制系統）3：SR 2.3（1） ·SL-C（UC，控制系統）4：SR 2.3（1）

3.2.2.2.5 SR 2.4 行動程式碼

編　　號	區　　分	內　　容
SR 2.4	基本要求	控制系統應根據可能對控制系統造成損害的可能性，提供對行動程式碼技術實施使用限制的能力，包括： a）阻止行動程式碼的執行; b）要求對程式碼的來源進行適當的認證和授權; c）限制移入/移出控制系統的行動程式碼; 和 d）監控行動程式碼的使用。
SR 2.4	說明	行動程式碼技術包括但不限於 Java，JavaScript，ActiveX，可攜式文件格式（PDF），Postscript，Shockwave 電影，Flash 動畫和 VBScript。 使用限制適用於選擇和使用安裝在伺服器上的行動程式碼以及在各個工作站上下載和執行的行動程式碼。 控制程序應防止在正式運作製程之控制系統內開發、獲取或引入不可接

		受的行動程式碼。 例如，行動程式碼交換可以直接與控制系統不允許，但可以在由 IACS 人員維護的受控相鄰環境中被允許。
SR 2.4 RE(1)	增項要求	（1）行動程式碼完整性檢查 在允許程式碼執行之前，控制系統應提供驗證行動程式碼完整性的能力。
SR 2.4 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.4 ·SL-C（UC，控制系統）2：SR 2.4 ·SL-C（UC，控制系統）3：SR 2.4（1） ·SL-C（UC，控制系統）4：SR 2.4（1）

3.2.2.2.6 SR 2.5 會話鎖定

編　　號	區　　分	內　　容
SR 2.5	基本要求	控制系統應提供通過在可設定的不活動時間區段或手動啟動後啟動會話鎖定來防止進一步存取的能力。 會話鎖定應保持有效，直到擁有該會話的人類使用者或其他授權的人類使用者使用適當的身份識別和認證程序重新建立存取權限。
SR 2.5	說明	負責控制系統的實體應使用會話鎖定來阻止對指定工作站或節點的存取。 在指定工作站或節點的可設定時間區段之後，控制系統應自動啟動會話鎖定機制。 在某些情況下，不建議控制系統操作員工作站或節點的會話鎖定（例如，在緊急情況下立即操作員回應所需的會話）。 會話鎖定不能代替退出控制系統。 在控制系統不能支援會話鎖定的情況下，負責管理人員應採用適當的補償對策（例如，提供增強的實體安全性、人員安全性和稽核措施）。
SR 2.5 RE	增項要求	無
SR 2.5 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.5 ·SL-C（UC，控制系統）2：SR 2.5 ·SL-C（UC，控制系統）3：SR 2.5 ·SL-C（UC，控制系統）4：SR 2.5

3.2.2.2.7 SR 2.6 遠端會話終止

編　　號	區　　分	內　　容

SR 2.6	基本要求	控制系統應提供在可設定的不活動時間區段後自動終止遠端會話的能力，或由發起會話的使用者手動終止遠端會話的能力。
SR 2.6	說明	只要在資產擁有者根據風險評估定義的區域邊界存取控制系統，就會啟動遠端會話。 此要求可能僅限於用於控制系統監控和維護活動（非關鍵操作）的會話，這些會話基於控制系統的業務需求、風險評估以及安全政策和過程。 在同樣經風險評估及業務、生產實際狀況在某些特殊的情境控制系統或元件可能不允許終止會話。
SR 2.6 RE	增項要求	無
SR 2.6 SL-C	安全等級	·SL-C（UC，控制系統）1：未選用 ·SL-C（UC，控制系統）2：SR 2.6 ·SL-C（UC，控制系統）3：SR 2.6 ·SL-C（UC，控制系統）4：SR 2.6

3.2.2.2.8 CS 2.7 會話總量控制

編　　號	區　　分	內　　容
SR 2.7	基本要求	控制系統應提供將任何特定使用者（人、軟體程序或裝置）的每個介面的同時執行中會話數限制為可設定數量的會話的能力。
SR 2.7	說明	如果沒有對同時執行的會話數施加限制，可能會對控制系統或網路設備等運算、記憶體或儲存空間，發生資源耗盡阻斷服務（denial-of-service ,DoS）。 由於控制系統資源有限，可能會鎖定特定使用者與鎖定所有使用者和服務之間存在進行權衡調控。 元件產品供應商或系統整合商可能需要提供有關如何分配會話數量值的充分資訊以利進行限制。
SR 2.7 RE	增項要求	無
SR 2.7 SL-C	安全等級	·SL-C（UC，控制系統）1：未選用 ·SL-C（UC，控制系統）2：未選用 ·SL-C（UC，控制系統）3：SR 2.7 ·SL-C（UC，控制系統）4：SR 2.7

3.2.2.2.9 SR 2.8 可稽核的事件

編　　號	區　　分	內　　容

SR 2.8	基本要求	控制系統應提供產生與以下類別的安全性相關的稽核記錄的能力：存取控制、請求錯誤、作業系統事件、控制系統事件、備份和恢復事件、設定更改、潛在偵察活動和稽核日誌事件。 個人稽核記錄應包括時間戳記、來源（發起裝置、軟體程序或人類使用者帳戶）、類別、類型、事件 ID 和事件結果。
SR 2.8	說明	此要求的目的是記錄與控制系統的安全性相關重要事件的發生，這些事件需要經過稽核，以追蹤事件發生原因。 開啟稽核活動會影響控制系統的效能。安全稽核功能通常需與系統及網路運作健康程度進行調校。在編製可稽核事件列表時，應考慮一般公認和可接受的清單和設定指南。組織安全政策和程序可預先定義足以支援事故後鑑識或調查的可稽核事件的依據。此外，稽核記錄應足以用於監測滿足本指南要求的安全機制的有效性和正常運作。 應該注意的是，事件記錄的要求適用於特定的系統功能，特別是特定等級的系統安全要求。例如，根據 FR 6 的要求，在 SL 1 系統上記錄身分認證事件（在存取控制類別中）的要求僅適用於 SL 1 所需的認證功能等級。事件可能發生在任何控制系統中元件（例如登錄嘗試事件）或可由專用監視器觀察。例如，網路連接埠掃描可能由入侵偵測系統（IDS）或入侵防禦系統（IPS）才能偵測到。
SR 2.8 RE(1)	增項要求	（1）集中管理的全系統稽核追溯能力 控制系統應提供集中管理稽核事件的能力，並能將整個控制系統中多個元件的稽核記錄編譯成可用系統範圍（邏輯或實體）、時間相關的稽核追溯。 控制系統應提供以產業標準格式導出這些稽核記錄的能力，以便通過標準商業日誌分析工具進行分析，例如安全資訊和事件管理（SIEM）系統。
SR 2.8 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.8 ·SL-C（UC，控制系統）2：SR 2.8 ·SL-C（UC，控制系統）3：SR 2.8（1） ·SL-C（UC，控制系統）4：SR 2.8（1）

3.2.2.2.10 SR 2.9 稽核儲存容量

編　　號	區　　分	內　　容
SR 2.9	基本要求	控制系統應根據組織事件管理需求規劃日誌管理和系統設定以分配足夠的稽核記錄儲存容量。 控制系統應提供

		稽核機制，以減少超出此類容量的可能性。
SR 2.9	說明	控制系統應提供足夠的稽核儲存容量，同時考慮保留政策，要執行的稽核和線上稽核處理要求。 需要考慮的指南可依據組織的資安事件回應或處理規範。 審核儲存容量應足以在適用的政策和法規、業務要求或事故調查回溯所需的一段時間內保留日誌。
SR 2.9 RE(1)	增項要求	（1）達到稽核記錄儲存容量閾值時發出警告 當分配的稽核記錄儲存量達到最大稽核記錄儲存容量的可設定百分比時，控制系統應提供發出警告的能力。
SR 2.9 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.9 ·SL-C（UC，控制系統）2：SR 2.9 ·SL-C（UC，控制系統）3：SR 2.9（1） ·SL-C（UC，控制系統）4：SR 2.9（1）

3.2.2.2.11 SR 2.10 對稽核處理失敗的回應

編　　號	區　　分	內　　容
SR 2.10	基本要求	控制系統應提供警報的能力，並防止在稽核處理失敗時，喪失基本服務和功能。 根據普遍接受的產業實務常見做法和建議，控制系統應提供支援稽核處理失敗的適當行動的能力。
SR 2.10	說明	稽核記錄產生通常發生在事件來源。 稽核處理涉及傳輸、可能的擴充（例如新增時間戳記）和持久儲存稽核記錄。 稽核處理失敗包括例如軟體或硬體錯誤，稽核捕獲機制中的故障以及達到或超過稽核儲存容量。 在設計適當的回應措施時要考慮的準則應依據組織的資安事件回應或處理規範。 應該注意的是，執行覆蓋最早的稽核記錄或停止稽核日誌的產生，可能會超出稽核儲存容量的回應，但意味著可能會遺失必要的取證資訊。
SR 2.10 RE	增項要求	無
SR 2.10 SL-C	安全等級	·SL-C（UC，控制系統）1：SR 2.10 ·SL-C（UC，控制系統）2：SR 2.10 ·SL-C（UC，控制系統）3：SR 2.10 ·SL-C（UC，控制系統）4：SR 2.10

3.2.2.2.12 SR 2.11 時間戳記

編　　號	區　　分	內　　容

SR 2.11	基本要求	應使用內部系統時鐘產生稽核記錄的時間戳記。並與公認的外部時間校時來源同步且應保護時間校時來源免受未經授權的更改。
SR 2.11	說明	應使用內部系統時鐘產生稽核記錄的時間戳記（包括日期和時間）。 如果不存在系統範圍的時間同步（這在許多安裝中是典型的），則需要已知的偏移來支援對一系列事件的分析。 此外，內部產生的稽核記錄與外部事件的同步可能需要與公認的外部時間校時來源（例如國家時間與頻率標準實驗室 NTP、全球定位系統（GPS）、全球導航衛星系統（GLONASS）和伽利略）同步。 應保護時間校時來源免受未經授權的更改。
SR 2.11 RE(1)	增項要求	（1）內部時間同步 控制系統應提供以可設定的頻率同步內部系統時鐘的能力。
SR 2.11 RE(2)	增項要求	（2）保護時間校時來源的完整性 應保護時間校時來源免受未經授權的更改，並在更改時引起審核事件。
SR 2.11 SL-C	安全等級	·SL-C（UC，控制系統）1：未選用 ·SL-C（UC，控制系統）2：SR 2.11 ·SL-C（UC，控制系統）3：SR 2.11（1） ·SL-C（UC，控制系統）4：SR 2.11（1）（2）

3.2.2.2.13 SR 2.12 不可否認服務

編號	區分	內容
SR 2.12	基本要求	控制系統應提供驗證特定人類使用者是否採取特定行動的能力。
SR 2.12	說明	使用者採取的特定動作的例子包括執行操作員動作、改變控制系統設定、建立資訊、發送訊息、核准資訊（例如指示同時）和接收訊息。 不可否認性防止使用者否認曾執行特定活動之虛假聲明，例如，未由特定文件撰寫的作者、未發送訊息的發送者、未接收訊息的接收者或簽署人未簽署文件。 如果使用者採取特定操作（例如，發送電子郵件和核准作業工單）或接收到特定資訊，則可以使用不可否認服務來確定資訊是否源自使用者。 通過採用各種技術或機制（例如，數位簽章、數位訊息接收和時間戳記）獲得不可否認服務。
SR 2.12 RE(1)	增項要求	（1）所有使用者的不可否認性 控制系統應提供確定特定使用者（人、軟體程序或裝置）是否採取特定行動的能力。

SR 2.12 SL-C	安全等級	·SL-C（UC，控制系統）1：未選用 ·SL-C（UC，控制系統）2：未選用 ·SL-C（UC，控制系統）3：SR 2.12 ·SL-C（UC，控制系統）4：SR 2.12（1）

3.2.2.3 FR 3 系統完整性(System integrity, SI)

區　　分	內　　容
目的	確保 IACS 的完整性，以防止未經授權的操作
安全等級區分	·SL1 – 保護 IACS 的完整性，防止偶然或巧合操弄。 ·SL2 – 保護 IACS 的完整性，防止某人使用資源少，一般技能和動機低的簡單手段操弄。 ·SL3 – 保護 IACS 的完整性，防止某人使用具有適度資源，IACS 特定技能和適度動機的複雜手段進行操弄。 ·SL4 – 保護 IACS 的完整性，避免使用具有擴展資源，IACS 特定技能和高動力的複雜手段操弄的 IACS。
功能要求說明	IACS 經常經歷多個測試週期（單元測試、工廠驗收測試（FAT）、現場驗收測試（SAT），認證，除錯等），以確定系統在開始生產之前將按預期執行。 一旦投入營運，資產擁有者有責任維護 IACS 的完整性。 資產擁有者可以使用他們的風險評估方法，為不同的系統、通信管道和 IACS 中的資訊分配不同等級的完整性保護。 實體資產的完整性應保持在營運和非營運狀態，例如生產期間，儲存期間或維護停機期間。 邏輯資產的完整性應在傳輸和靜止時保持，例如通過網路傳輸或駐留在資料儲存庫中。

3.2.2.3.1 FR 3 系統完整性的安全要求清單

安全要求編號	安　　全　　要　　求　　名　　稱
SR 2.3	通信完整性
SR 3.2	惡意程式碼保護
SR 3.3	安全功能驗證
SR 3.4	軟體和資訊完整性
SR 3.5	輸入驗證
SR 3.6	確定性輸出
SR 3.7	錯誤處理
SR 3.8	會話完整性
SR 3.9	保護稽核資訊

3.2.2.3.2 SR 3.1 通信完整性

編　　號	區　　分	內　　容
SR 3.1	基本要求	控制系統應提供保護傳輸資訊完整性的能力。
SR 3.1	說明	許多常見的網路攻擊基於傳輸中的資料操弄，例如網路資料封包的操弄。交換或路由網路為攻擊者提供了更大的機會來操弄封包，因為對這些未偵測到的網路存取通常更容易，並且還可以操弄交換和路由機制本身以便獲得對傳輸資訊的更多存取機會。在控制系統的使用情境中的操弄可以包括從感應器傳遞到接收器的測量值的改變或者從控制應用發送到執行器的命令參數的改變。 取決於使用情境（例如，本地網路段內的傳輸與通過不可信任網路的傳輸）和傳輸中使用的網路類型（例如傳輸控制協議（TCP）/網際協議（IP）與本地串接設備的序列鏈路），可行且適當的機制會有所不同在具有直接鏈路（點對點）的小型網路上，如果端點的完整性也受到保護，則對較低 SL 的所有節點的實體存取保護可能就足夠了（參見 SR 3.4 – 軟體和資訊完整性），同時在分佈在員工經常性實際存取的區域（LAN）或廣域(WAN)網路上，實體存取很可能是不可執行的。 如果商業服務用於提供作為商品項目的通信服務而不是完全專用的服務（例如租用專線與 T1 鏈路），則可能更難以獲得有關通信完整性實施所需安全控制的必要保證（例如由於法律限制）。如果滿足必要保證的安全要求是不可行或不切實際的，那麼實施適當的補償對策或明確接受額外風險可能是適當的。 工控自動化裝置經常受到可能導致完整性問題或誤報事件的環境條件的影響。以下是幾個維持通信完整性的舉例： ● 很多時候，環境中含有微粒、液體、振動、氣體、輻射和電磁干擾（EMI），這些干擾會導致影響通信線路和信號完整性的條件。網路基礎設施的設計應盡量減少對通信完整性的實體/環境影響。例如，當微粒、液體或氣體成為問題時，可能需要使用密封的 RJ-45 或 M12 連接器代替電線上的商用級 RJ-45 連接器。電纜本身可能需要使用不同的護套來代替處理微粒、液體或氣體。 ● 如果出現振動問題，可能需要使用 M12 連接器，以防止 RJ-45 連接器上的彈簧銷在使用過程中斷開。 ● 在輻射或 EMI 成為問題的情況下，可能需要使用屏蔽雙絞線或光纖電纜來防止對通信信號的任何影響。 ● 如果計劃無線網路驗證它是可行的解決方案，則可能還需要在這些區域中執行無線頻譜分析。

SR 3.1 RE(1)	增項要求	（1）密碼完整性保護控制系統應提供使用加密機制識別通信期間資訊變化的能力。 註：在仔細考慮安全需求以及對系統效能和系統故障恢復能力的潛在後果之後，確定加密機制對訊息身份驗證和完整性的適當使用是一種普遍接受的良好做法。
SR 3.1 SL-C	安全等級	·SL-C（SI，控制系統）1：SR 3.1 ·SL-C（SI，控制系統）2：SR 3.1 ·SL-C（SI，控制系統）3：SR 3.1（1） ·SL-C（SI，控制系統）4：SR 3.1（1）

3.2.2.3.3 SR 3.2 惡意程式碼保護

編　　號	區　　分	內　　容
SR 3.2	基本要求	控制系統應提供使用保護機制來預防、檢測、報告和減輕惡意程式碼或未授權軟體的影響的能力。 控制系統應提供更新保護機制的能力。
SR 3.2	說明	控制系統應使用保護機制來防止、檢測、緩解和報告通過電子郵件、電子郵件附件，Internet 存取，可攜式媒體傳輸的檢測到的惡意程式碼（例如，病毒、蠕蟲、特洛伊木馬和間諜軟體）的實例（例如，一般 USB 裝置、軟碟或光碟）、PDF 文件、Web 服務，網路連接和受感染的筆記型電腦或其他常用手段。 檢測機制應該能夠檢測應用程式二進位文件和資料文件的完整性違規。技術可以包括但不限於二進位完整性和屬性監視、雜湊和簽章技術。緩解技術可以包括但不限於文件清理、隔離、文件刪除、主機通信限制和 IPS。 預防技術可以包括但不限於應用程式黑名單和白名單技術，可攜式媒體控制，沙箱技術和特定計算平台機制，例如受限制的韌體更新功能，No Execute（NX）位，資料執行預防（DEP），地址空間佈局隨機化（ASLR），堆疊損壞檢測和強制存取控制。參見 SR 6.2 – 連續監測涉及控制系統監測工具和技術的相關要求。 預防和緩解機制可能包括為主機元素（如 IT 和伺服器）和基於網路的機制（如 IDS 和 IPS）設計的機制，以及側重於控制系統特定元件（如 PLC 和 HMI）的機制。
SR 3.2 RE(1)	增項要求	（1）進入和退出點的惡意程式碼防治 控制系統應提供在所有入口和出口點採用惡意程式碼防治機制的能力。 注意：此類機制通常在可攜式媒體、防火牆、單向網路閘道、Web 伺服器、代理伺服器或遠端存取伺服器上提供。

SR 3.2 RE(2)	增項要求	（2）集中管理和報告惡意程式碼防治 控制系統應提供管理惡意程式碼防治機制的能力。 注意此類機制通常由端點為基礎的架構集中管理或 SIEM 解決方案提供。
SR 3.2 SL-C	安全等級	·SL-C（SI，控制系統）1：SR 3.2 ·SL-C（SI，控制系統）2：SR 3.2（1） ·SL-C（SI，控制系統）3：SR 3.2（1）（2） ·SL-C（SI，控制系統）4：SR 3.2（1）（2）

3.2.2.3.4 SR 3.3 安全功能驗證

編　　號	區　　分	內　　容
SR 3.3	基本要求	控制系統應提供支援驗證安全功能的預期操作的能力，並報告在功能驗收測試（FAT），安全驗收測試（SAT）和定期維護期間發現異常時的情況。 這些安全功能應包括支援本指南建議的安全要求所需的所有功能。
SR 3.3	說明	產品供應商或系統整合商應提供有關如何測試設計的安全控制的指導。資產擁有者需要了解在正常操作期間如何運作這些驗證測試及可能造成後果。需要在仔細考慮連續操作要求（例如，安排或事先通知）的情況下指定執行這些驗證的詳細資訊。 安全驗證功能的例子包括： ● 由歐洲 IT 防病毒研究所（EICAR）測試控制系統文件系統驗證防病毒措施。防病毒軟體應檢測到此情況，並應觸發對應的事件處理程序。 ● 通過嘗試使用未經授權的帳戶來驗證身份，身份驗證和使用控制措施（對於某些功能，這可以自動化）。 ● 通過在 IDS 中包含一個規則來驗證 IDS 作為安全控制，該規則觸發不規則但已知的非惡意流量。然後可以通過引入觸發此規則的流量以及適當的 IDS 監視和事件處理過程來執行測試。 ● 確認稽核日誌記錄正在按照安全政策和流程的要求進行，並且未被內部或外部實體禁用。
SR 3.3 RE(1)	增項要求	（1）安全功能驗證的自動機制 控制系統應提供使用自動機制的能力，以支援 FAT、SAT 和定期維護期間的安全驗證管理。
SR 3.3 RE(2)	增項要求	（2）正常操作期間的安全功能驗證 控制系統應提供在正常操作期間支援驗證安全功能的預期操作的能力。 注意：謹慎實施此要求是一種普遍接受的良好做法，因為它可能導致不利影響。 它通常不被認為適用於安全系

		統。
SR 3.3 SL-C	安全等級	·SL-C（SI，控制系統）1：SR 3.3 ·SL-C（SI，控制系統）2：SR 3.3 ·SL-C（SI，控制系統）3：SR 3.3（1） ·SL-C（SI，控制系統）4：SR 3.3（1）（2）

3.2.2.3.5 SR 3.4 軟體和資訊完整性

編號	區分	內容
SR 3.4	基本要求	控制系統應提供檢測、記錄、報告和防止未經授權的軟體和資訊變更的能力。
SR 3.4	說明	未經授權的更改是嘗試更改的主體沒有所需權限所進行更改。 該 SR 補充了 FR 1 和 2 中的相關 SR.FR 1 和 2 涉及按照設計強制執行角色、特權和使用模式。 如果已經繞過其他保護機制（例如授權實施），則採用完整性驗證方法來檢測、記錄、報告和防止可能發生的軟體和資訊篡改。 控制系統應採用正式或推薦的完整性機制（例如加密雜湊函數）。 例如，這種機制可用於監視現場裝置的最新設定資訊，以檢測安全漏洞（包括未經授權的更改）。
SR 3.4 RE(1)	增項要求	（1）關於完整性違規的自動通知 控制系統應提供使用自動化工具的能力，這些工具在完整性驗證程序中發現差異時，可設定向的一組已定義的接收者提供通知。
SR 3.4 SL-C	安全等級	·SL-C（SI，控制系統）1：未選用 ·SL-C（SI，控制系統）2：SR 3.4 ·SL-C（SI，控制系統）3：SR 3.4（1） ·SL-C（SI，控制系統）4：SR 3.4（1）

3.2.2.3.6 SR 3.5 輸入驗證

編號	區分	內容
SR 3.5	基本要求	控制系統應驗證任何輸入的語法和內容，這些輸入用作工業程序控制輸入或直接影響控制系統動作的輸入。

SR 3.5	說明	應該制定檢查控制系統輸入的有效語法（如設定點）的規則，以驗證此資訊是否未被篡改並符合規範。 傳遞給程式碼解譯器的輸入應進行預篩選以防止內容來自被無意地解釋為命令。請注意，這是一個安全 SR，因此它不解決人為錯誤，例如提供超出預期範圍的合法整數。 輸入資料驗證是常見公認產業實務做法，包括驗證已定義字段類型的超出範圍值、資料字段中的無效字元、資料遺失或不完整以及緩衝區溢位。 無效輸入導致系統安全問題的其他例子包括 SQL 注入攻擊、跨站點腳本或格式錯誤的資料封包（通常由協議模糊器產生）。 需要考慮的準則可能包括開放式 Web 應用程式安全專案（OWASP）程式碼檢視指南 (https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf)。
SR 3.5 RE	增項要求	無
SR 3.5 SL-C	安全等級	·SL-C（SI，控制系統）1：SR 3.5 ·SL-C（SI，控制系統）2：SR 3.5 ·SL-C（SI，控制系統）3：SR 3.5 ·SL-C（SI，控制系統）4：SR 3.5

3.2.2.3.7 SR 3.6 確定性輸出

編　　號	區　　分	內　　容
SR 3.6	基本要求	如果由於攻擊導致無法維持正常操作，則控制系統應提供將輸出設置為預定狀態的能力。
SR 3.6	說明	控制系統輸出的確定性行為是對控制系統遭受攻擊威脅行為時應預期的結果，是確保正常操作完整性的重要特徵。 在理想狀況下，控制系統在受到攻擊時應維持繼續正常操作，但是如果控制系統不能維持正常操作，則控制系統輸出需要切換到預定狀態。 控制系統輸出的適當預定狀態取決於應用程式設計，使用者可設定選項可以是以下之一： ·無動力 – 輸出無法進入無動力狀態 ·保持 – 輸出未達到最後已知的良好值 ·已修復 – 輸出未達到由資產擁有者或應用程式確定的固定值
SR 3.6 RE	增項要求	無
SR 3.6 SL-C	安全等級	·SR-C（SI，控制系統）1：SR 3.6 ·SR-C（SI，控制系統）2：SR 3.6 ·SR-C（SI，控制系統）3：SR 3.6 ·SR-C（SI，控制系統）4：SR 3.6

3.2.2.3.8 SR 3.7 錯誤處理

編　　號	區　　分	內　　容
SR 3.7	基本要求	控制系統應以能夠進行有效補救的方式識別和處理錯誤狀況。 這應該以不提供可識別為被對手攻擊 IACS 的資訊的方式進行，除非披露這些資訊對於及時排除問題是必要的。
SR 3.7	說明	產品供應商或系統整合商應仔細考慮錯誤訊息的結構和內容。 控制系統產生的錯誤訊息應提供及時有用的資訊，而不會洩露可能被攻擊者用來利用 IACS 的潛在有害資訊。 由於可能不清楚特定錯誤條件是否是由安全事件引起的，因此在事件回應期間可能需要容易地存取所有錯誤訊息。 必須通過及時解決錯誤條件來證明披露這些資訊是合理的。 要考慮的準則可能包括應用程式安全專案（OWASP）程式碼檢視指南 (https://www.owasp.org/images/5/53/OWASP_Code_Review_Guide_v2.pdf)。
SR 3.7 RE	增項要求	無
SR 3.7 SL-C	安全等級	·SL-C（SI，控制系統）1：未選用 ·SL-C（SI，控制系統）2：SR 3.7 ·SL-C（SI，控制系統）3：SR 3.7 ·SL-C（SI，控制系統）4：SR 3.7

3.2.2.3.9 SR 3.8 會話完整性

編　　號	區　　分	內　　容
SR 3.8	基本要求	控制系統應提供保護會話完整性的能力。 控制系統應拒絕使用無效的會話 ID。
SR 3.8	說明	此控制側重於會話的通信保護與資料封包等級。 這種控制的目的是在通信會話的每一端建立對另一方的持續身份以及所傳輸資訊的有效性的信任的理由。 例如，該控制解決了中間人攻擊，包括會話劫持、將錯誤資訊插入會話或重送攻擊。 會話完整性機制的使用可能具有顯著的實施成本，因此應根據即時通信的要求來考慮它們的使用。
SR 3.8 RE(1)	增項要求	（1）會話終止後會話 ID 無效 控制系統應提供在使用者註銷或其他會話終止（包括瀏覽器會話）時使會話 ID 無效的能力。
SR 3.8 RE(2)	增項要求	（2）唯一會話 ID 產生 控制系統應提供為每個會話產生唯一會話 ID 的能力，並將所有意外會話 ID 視為無效。
SR 3.8 RE(3)	增項要求	（3）會話 ID 的隨機性 控制系統應提供產生具有普遍接受的隨機來源的唯一會話 ID 的能力。 注意會話劫持和其他中間人攻擊或虛假資訊注入通常利用易於猜測的會話 ID（密鑰或其他共享機密）或會話 ID 的使用，這些會話 ID 在會話終止後未正確失效。 因此，會話驗證器的有效性需要與會話的生命週期緊密相關。 在產生唯一會話 ID 時使用隨機性有助於防止暴力攻擊以確定將來的會話 ID。
SR 3.8 SL-C	安全等級	·SL-C（SI，控制系統）1：未選用 ·SL-C（SI，控制系統）2：SR 3.8 ·SL-C（SI，控制系統）3：SR 3.8（1）（2） ·SL-C（SI，控制系統）4：SR 3.8（1）（2）（3）

3.2.2.3.10 SR 3.9 保護稽核資訊

編　　號	區　　分	內　　容

SR 3.9	基本要求	控制系統應保護稽核資訊和稽核工具，防止未經授權的存取，修改和刪除。
SR 3.9	說明	稽核資訊包括成功稽核控制系統活動所需的所有資訊（例如，稽核記錄、稽核設置和稽核報告）。 稽核資訊對於錯誤修正、安全漏洞修補、調查和相關工作非常重要。 增強防止修改和刪除保護的機制包括將稽核資訊儲存到硬體強制的一次性寫入媒體。
SR 3.9 RE(1)	增項要求	（1）一次性寫入媒體的稽核記錄 控制系統應提供在硬體強制的一次寫入媒體上產生稽核記錄的能力。
SR 3.9 SL-C	安全等級	·SL-C（SI，控制系統）1：未選用 ·SL-C（SI，控制系統）2：SR 3.9 ·SL-C（SI，控制系統）3：SR 3.9 ·SL-C（SI，控制系統）4：SR 3.9（1）

力

3.2.2.4 FR 4 資料機密性（Data confidentiality, DC）

區　　分	內　　容
目的	確保通信管道和資料儲存庫中資訊的機密性，以防止未經授權的洩露
安全等級區分	·SL1 – 防止通過竊聽或隨意暴露，造成未經授權的資訊洩露。 ·SL2 – 防止使用資源少，一般技能和動機低的簡單方法，向正在積極搜索資訊的實體，造成未經授權的披露資訊。 ·SL3 – 防止使用具有適度資源、IACS 特定技能和適度動機的複雜手段向正在積極搜索資訊的實體，造成未經授權披露資訊。 ·SL4 – 防止使用具有擴展資源，IACS 特定技能和高度積極性的複雜手段，向正在積極搜索資訊的實體，造成未經授權披露資訊。
功能要求說明	一些控制系統產生的資訊，無論是在儲存狀態還是在傳輸途中，都具有機密性或敏感性。 這意味著某些通信管道和資料儲存需要防止竊聽和未授權存取。

3.2.2.4.1 FR 4 資料機密性的安全要求清單

安全要求編號	安　全　要　求　名　稱
SR 4.1	資訊保密
SR 4.2	資訊持久性
SR 4.3	密碼學的使用

3.2.2.4.2 SR 4.1 資訊保密

編　　號	區　　分	內　　容
SR 4.1	基本要求	控制系統應提供保護資訊機密性的能力，無論是儲存狀態還是在傳輸途中，都支援明確的存取授權。
SR 4.1	說明	受保護的資訊，無論是在儲存狀態還是在傳輸途中，都可以通過實體手段、分區或加密以及其他技術來保護。選擇的保護技術應考慮控制系統效能受影響的潛在後果和從系統故障或攻擊中恢復的能力等因素是是非常重要。 是否應保護特定資訊的機密性的決定係取決於個案具體情況，不完全能在產品設計中進行。但是，組織通過在控制系統中設定明確存取授權來限制對資訊的存取，這一事實表明該資訊被組織視為機密資訊。因此，控制系統應支援可分配明確存取授權的能力，所有資訊均應被視為潛在機密，因此控制系統應提供保護它的能力。 根據組織對資訊的敏感性以及產業標準和監管要求，不同的組織和產業可能要求不同類別的資訊具有不同等級的加密強度（參見 SR 4.3 – 密碼學的使用）。在某些情況下，在交換機和路由器中儲存和處理的網路設定資訊可能被視為機密資訊。 涉及暴露資訊傳輸的通信可能容易被竊聽或篡改。如果控制系統依賴於外部通信服務提供商，則可能更難以獲得關於建立通信機密性所需的安全性要求的必要保證。在這種情況下，實施補償對策或明確接受額外風險可能是適當的。 當使用可攜式媒體和行動裝置（例如，工程筆記型電腦和 USB 隨身碟）時，實體也應該認識到資訊的機密性。 根據 SR 1.5 – 驗證器管理要求，認證資訊，如密碼，應被視為機密，因此永遠不應被明文發送。
SR 4.1 RE(1)	增項要求	（1）通過不受信任的網路，保護靜置或傳送過程時的機密性 控制系統應提供保護靜置（儲存、快取）資訊和穿過不可信任網路的遠端存取會話的機密性的能力。 注意：密碼學是確保資訊機密性的常用機制。
SR 4.1 RE(2)	增項要求	（2）跨區域邊界保護機密性 控制系統應提供保護穿過任何區域邊界的資訊機密性的能力。
SR 4.1 SL-C	安全等級	·SL-C（DC，控制系統）1：未選用 ·SL-C（DC，控制系統）2：SR 4.2 ·SL-C（DC，控制系統）3：SR 4.2（1） ·SL-C（DC，控制系統）4：SR 4.2（1）

3.2.2.4.3 SR 4.2 資訊持久性

編號	區分	內容
SR 4.2	基本要求	控制系統應提供清除所有資訊的能力，從運作中服務或退役的元件中支援明確存取授權。
SR 4.2	說明	從運作中服務中刪除控制系統元件，不應該提供無意釋放支援明確存取授權的資訊的機會。這種資訊的一個例子包括'連接密鑰'（在某些無線現場裝置的情況下）在非易失性儲存或其他加密資訊中，這將有助於未經授權或惡意的活動。 由使用者或角色的動作產生的資訊（或代表使用者或角色的軟體程序的動作）不應以不受控制的方式向不同的使用者或角色公開。 控制系統資訊或資料持久性的控制可防止儲存在共享資源上的資訊在資源被釋放回控制系統後被無意洩露。
SR 4.2 RE(1)	增項要求	（1）清除共享記憶體資源 控制系統應提供防止通過易失性共享記憶體資源進行未授權和非預期資訊傳輸的能力。 注意易失性記憶體資源是指在釋放到記憶體管理後通常不會保留資訊的記憶體資源。 但是，存在對隨機存取記憶體（RAM）的攻擊，這些記憶體有可能在實際重寫之前提取密鑰材料或其他機密資料。 因此，當將該記憶體釋放回控制系統以供不同使用者使用時，從易失性共享記憶體清除所有唯一資料和連接到唯一資料是普遍接受的做法，使得該資料不可見或不可存取。 新使用者。」
SR 4.2 SL-C	安全等級	·SL-C（DC，控制系統）1：未選用 ·SL-C（DC，控制系統）2：SR 4.2 ·SL-C（DC，控制系統）3：SR 4.2（1） ·SL-C（DC，控制系統）4：SR 4.2（1）

3.2.2.4.4 SR 4.3 密碼學的使用

編號	區分	內容
SR 4.3	基本要求	如果需要加密，控制系統應根據普遍接受的安全產業實務常見做法和建議，使用加密算法、密鑰長度和密鑰的生命週期管理機制。
SR 4.3	說明	是否需要加密保護資料，應該取決受保護資訊的價值、資訊的機密性被破壞的後果、資訊保密的時間區段以及控制系統操作約束相匹配。這可能涉及靜置、傳輸或兩者均有的資訊。請注意，備份是靜置資訊的一個例子，

		應被視為資料機密性評估過程的一部分。 控制系統產品供應商應提供記錄與加密密鑰建立和管理相關的實行和程序。控制系統應利用已建立和經過測試的加密和雜湊演算法，例如先進加密標準（AES）和安全雜湊算法（SHA）系列，以及基於指定標準的密鑰長度。需要使用有效的隨機亂數產生器來執行密鑰產生。密鑰管理的安全政策和過程需要根據定義的標準處理定期密鑰更改、密鑰銷毀、密鑰分發和加密密鑰備份等生命週期的密鑰完整保護機制。普遍接受的做法和建議可以在 NIST SP800-57 等文件中找到。例如，可以在美國聯邦資訊處理標準（FIPS）140-2 中找到建立要求。 當滿足本指南中定義的許多其他要求時，此 SR 以及 SR 1.8 – 公鑰基礎結構（PKI）憑證可能適用。
SR 4.3 RE	增項要求	無
SR 4.3 SL-C	安全等級	·SL-C（DC，控制系統）1：SR 4.3 ·SL-C（DC，控制系統）2：SR 4.3 ·SL-C（DC，控制系統）3：SR 4.3 ·SL-C（DC，控制系統）4：SR 4.3

3.2.2.5 FR 5 受限制的資料流 (Restricted data flow, RDF)

區　　分	內　　容
目的	通過區域和管道對控制系統進行分段，以限制不必要的資料流。
安全等級區分	·SL1 – 防止區域和管道分割的偶然或巧合規避或繞過。 ·SL2 – 防止使用資源少，一般技能和動機低的簡單方法，實體對區域和管道分割的預期規避或繞過。 ·SL3 – 防止使用具有適度資源，以 IACS 特定技能和適度動機的複雜手段，對實體劃分區域和管道分段進行規避或繞過。 ·SL4 – 防止使用具有擴展資源，以 IACS 特定技能和高動力的複雜手段，對實體劃分區域和管道分段進行規避或繞過。
功能要求說明	使用他們的風險評估方法，資產擁有者需要確定必要的資訊流限制為何？因此，通過前述風險評估過程，確定用於提供此資訊的區域及管道的設定。 衍生的規範性建議和指南應包括從控制系統網路與業務或公共網路斷開連接，到使用單向網路閘道，狀態防火牆和 DMZ 來管理資訊流限制的機制。

3.2.2.5.1 FR 5 受限制的資料流的安全要求清單

安全要求編號	安　全　要　求　名　稱
SR 5.1	網路分段
SR 5.2	區域邊界保護
SR 5.3	限制一般人對人通信
SR 5.4	應用程式分區

3.2.2.5.2 SR 5.1 網路分段

編　　號	區　　分	內　　容
SR 5.1	基本要求	控制系統應提供從非控制系統網路邏輯分段控制系統網路的能力，並從其他控制系統網路邏輯分割出關鍵控制系統網路。
SR 5.1	說明	組織將網路分段用於各種目的，包括網路安全及效能。分割網路的主要原因是減少網路流量進入控制系統的風險，並減少網路流量的傳播或流出來自控制系統。 這提高了整體系統回應和可靠性，並提供了網路安全保

		護措施。它還允許控制系統內的不同網段，包括關鍵控制系統和安全相關系統，與其他系統分開提供額外的保護。 應根據控制系統的操作要求，明確說明從控制系統到網際網路的存取。 網路分段及其提供的保護等級將根據資產擁有者在其設施中使用的整體網路架構甚至其控制系統內的系統整合商而有很大差異。根據網路功能對網路進行邏輯分段可提供一定程度的保護，但如果網路裝置受到威脅，仍可能導致單點故障。實體分段網路通過消除單點故障情況提供了另一級保護，但將導致更複雜和昂貴的網路設計。這些權衡需要在網路設計過程中進行評估。 為了回應事件，可能有必要打破不同網段之間的連接。在這種情況下，支援基本操作所需的服務應該以這樣的方式保持，即裝置可以繼續正常運作或以有序的方式關閉。這可能需要在控制系統網路上複製某些伺服器以支援正常的網路功能，例如動態主機設定協議（DHCP），域名服務（DNS）或本地 CA.這也可能意味著一些關鍵控制系統和安全相關系統從一開始就被設計為與其他網路完全隔離。
SR 5.1 RE(1)	增項要求	（1）實體網路分隔 控制系統應提供從非控制系統網路與控制系統網路實體隔離的能力，並從非關鍵控制系統網路實體分隔關鍵控制系統網路。
SR 5.1 RE(2)	增項要求	（2）獨立於非控制系統網路 控制系統應能夠獨立提供網路服務，以控制系統網路，無論是關鍵還是其他方式，而無需連接到非控制系統網路。
SR 5.1 RE(3)	增項要求	（3）關鍵網路的邏輯和實體隔離 控制系統應提供邏輯或實體隔離關鍵控制系統網路與非關鍵控制系統網路的能力。
SR 5.1 SL-C	安全等級	·SL-C（RDF，控制系統）1：SR 5.1 ·SL-C（RDF，控制系統）2：SR 5.1（1） ·SL-C（RDF，控制系統）3：SR 5.1（1）（2） ·SL-C（RDF，控制系統）4：SR 5.1（1）（2）（3）

3.2.2.5.3 SR 5.2 區域邊界保護

編　　號	區　　分	內　　容

SR 5.2	基本要求	控制系統應提供監視和控制區域邊界通信的能力，以強制執行基於風險的區域和管道模型中定義的劃分。
SR 5.2	說明	與外部網路或其他控制系統的任何連接都應通過受管理介面進行，該介面由安裝在有效架構中的適當邊界保護裝置（例如，代理（proxy）伺服器、網路閘道、路由器、防火牆，單向網路閘道，防護和加密通道）組成，例如，防火牆，作為保護駐留在 DMZ 中的應用網路閘道。 任何指定的備用處理站點的控制系統邊界保護，應提供與主站點相同的保護等級。 作為縱深防禦保護戰略的一部分，應將更高影響控制系統劃分為單獨的區域，利用管道根據安全政策和程序限制或禁止網路存取，並對風險進行評估。 SL-T（系統）分類指導為區域劃分選擇合適的候選者。
SR 5.2 RE(1)	增項要求	（1）預設拒絕，允許例外 控制系統應提供監視和控制區域邊界通信的能力，以強制執行基於風險的區域和管道模型中定義的劃分。
SR 5.2 RE(2)	增項要求	（2）島嶼模式 控制系統應提供防止通過控制系統邊界（也稱為孤島模式）進行任何通信的能力。 註：可以使用此功能的例子包括在控制系統中檢測到安全違規或入侵，或者在企業網路發生攻擊的情況。
SR 5.2 RE(3)	增項要求	（3）關閉失敗 當邊界保護機制出現操作故障時（也稱為故障關閉），控制系統應提供防止通過控制系統邊界進行任何通信的能力。 這種失效關閉」功能的設計應使其不會干擾 SIS 或其他安全相關功能的運作。 註：可以使用此功能的例子包括硬體故障或電源故障導致邊界保護裝置在降級模式下運作或完全失效的情況。
SR 5.2 SL-C	安全等級	·SL-C（RDF，控制系統）1：SR 5.2 ·SL-C（RDF，控制系統）2：SR 5.2（1） ·SL-C（RDF，控制系統）3：SR 5.2（1）（2）（3） ·SL-C（RDF，控制系統）4：SR 5.2（1）（2）（3）

3.2.2.5.4 SR 5.3 限制一般人對人通信

編　　號	區　　分	內　　容
SR 5.3	基本要求	控制系統應提供防止從控制系統外部的使用者或系統接收一般人對人通信的能力。

SR 5.3	說明	一般人對人通信系統包括但不限於：電子郵件系統、社交媒體形式（Twitter、Facebook、圖片庫等）或允許傳輸任何類型的可執行文件的任何訊息系統。這些系統通常用於與控制系統操作無關的私人用途，因此這些系統所施加的風險通常超過任何可察覺的益處。 這些類型的一般通信系統是常用的攻擊媒介，用於向控制系統引入惡意軟體，將存在讀取授權的資訊傳遞到控制系統外部的位置，並引入可用於產生安全問題或啟動的過多網路負載攻擊控制系統。將本文件中其他地方描述的使用限制和限制資料流的廣泛的其他系統要求應用於一般的人對人通信系統可以提供足夠的補償對策以滿足該要求。 控制系統可以提供利用這些類型的雙向通信系統的能力，但是僅在控制系統內的伺服器或工作站之間。請注意，此 SR 需要支援與 SR 4.1 相關的要求 – 資訊機密性。 控制系統還可以限制使用提供內部 IT 到外部 IT 通信的電子郵件或其他訊息傳遞解決方案的外傳訊息。這些內部到外部通信可以限縮於將系統警報或其他 IT 產生的資訊訊息發送到控制系統外部的使用者或系統的目的。為了防止傳遞支援明確存取授權的資訊，應使用預先設定的訊息（可能包含一些有限的文本）來傳輸警報或狀態資訊。使用者可能無法在系統建立訊息時將文件或其他資訊附加到這些僅出站訊息。
SR 5.3 RE(1)	增項要求	（1）禁止所有一般的人對人通信 控制系統應提供防止發送和接收一般個人對個人資訊的能力。
SR 5.3 SL-C	安全等級	·SL-C（RDF，控制系統）1：SR 5.3 ·SL-C（RDF，控制系統）2：SR 5.3 ·SL-C（RDF，控制系統）3：SR 5.3（1） ·SL-C（RDF，控制系統）4：SR 5.3（1）

3.2.2.5.5 SR 5.4 應用程式分區

編　　號	區　　分	內　　容
SR 5.4	基本要求	控制系統應提供支援基於關鍵性劃分資料、應用程式和服務的能力，以便於實施分區模型。
SR 5.4	說明	可以通過使用不同的電腦設備、不同的中央處理單元、作業系統的不同實例，不同的網路地址以及這些方法的組合或適當的其他方法，通過實體或邏輯手段來完成分區。 可以考慮用於不同分區的應用程式和服務的例子包括但不限於緊急或安全系統、閉路環控制應用、操作員工作站和工程工作站。

SR 5.4 RE	增項要求	無
SR 5.4 SL-C	安全等級	·SL-C（RDF，控制系統）1：SR 5.4 ·SL-C（RDF，控制系統）2：SR 5.4 ·SL-C（RDF，控制系統）3：SR 5.4 ·SL-C（RDF，控制系統）4：SR 5.4

3.2.2.6 FR 6 及時回應事件 (Timely response to events, TRE)

區　　分	內　　容
目的	通過通知適當的執法機構，報告違規的必要證據並在發現事件時及時採取糾正措施來應對安全違規行為。
安全等級區分	·SL1 – 監控 IACS 的操作，並通過在查詢時收集和提供取證證據來發現事件。 ·SL2 –監控 IACS 的運作情況，通過積極收集和定期報告鑑識證據，並在發現事件時對事件做出回應。 ·SL3 – 監控 IACS 的運作情況，並通過積極收集鑑識證據並將鑑識證據推送給適當的機構來應對發現事故的事件。 ·SL4 – 監控 IACS 的運作情況，並通過近乎即時地向執法機構積極收集和推送鑑識證據來應對發現事故的事件。
功能要求說明	資產擁有者應使用風險評估方法，制定安全政策和程序，以及回應安全違規所需的適當通信和控制線。 衍生的說明性建議和指南應包括收集、報告、保存和自動關聯鑑識證據的機制，以確保及時採取糾正措施。 監測工具和技術的使用不應對控制系統的運作效能產生不利影響。

3.2.2.6.1 FR 6 及時回應事件的安全需求清單

安全要求編號	安　全　要　求　名　稱
SR 6.1	審核日誌可存取性
SR 6.2	持續監控

3.2.2.6.2 SR 6.1 審核日誌可存取性

編　　號	區　　分	內　　容

SR 6.1	基本要求	控制系統應為授權人員或工具提供以唯讀方式存取稽核日誌的能力。
SR 6.1	目的	控制系統產生有關系統中發生的事件的稽核記錄（參考 SR 2.8 – 可稽核事件）。 存取這些審核日誌對於支援過濾審核日誌，識別和刪除冗餘資訊，審核和報告安全事件事後調查期間的活動是必要的。 此存取不應更改原始審核記錄。 一般而言，稽核減少和報告產生應在單獨的資訊系統上進行。 手動存取稽核記錄（例如螢幕截圖或列印輸出）足以滿足基本要求，但不足以滿足更高的安全等級。 程序化存取通常用於向 SIEM 等分析機制提供稽核日誌資訊。
SR 6.1 RE(1)	增項要求	（1）以撰寫程式方式存取稽核日誌 控制系統應使用應用程式撰寫程式介面（API）提供對稽核記錄的撰寫程式存取。
SR 6.1 SL-C	安全等級	·SL-C（TRE，控制系統）1：SR 6.1 ·SL-C（TRE，控制系統）2：SR 6.1 ·SL-C（TRE，控制系統）3：SR 6.1（1） ·SL-C（TRE，控制系統）4：SR 6.1（1）

3.2.2.6.3 SR 6.2 持續監控

編　　號	區　　分	內　　容
SR 6.2	基本要求	控制系統應提供使用普遍接受的安全產業實務常見做法和建議持續監控所有安全機制效能的能力，以及時檢測、徵兆和報告安全漏洞。 註：回應時間是本指南範圍之外的因地制宜事項。

SR 6.2	說明	可以通過各種工具和技術（例如，IDS、IPS、惡意程式碼保護機制和網路監視機制）來建立控制系統監視能力。隨著攻擊變得更加複雜，這些監控工具和技術也需要變得更加複雜，包括例如基於行為的 IDS / IPS。 監控裝置應政策性地部署在控制系統內（例如，在選定的周邊位置和支援關鍵應用的伺服器集中場域附近）以收集基本資訊。還可以在控制系統內的臨時位置部署監視機制以追溯特定事件。 監測應包括適當的報告機制，以便及時回應事件。為了使報告集中並且報告的資訊量達到可以由接收者處理的水準，SIEM 等機制通常用於將各個事件關聯到聚合報告中，這些報告建立了原始事件發生的更大使用情境。 此外，這些機制可用於追溯安全更改對控制系統的影響（參見 SR 2.8 – 可稽核事件）。預先安裝取證工具可以促進事故分析。
SR 6.2 RE	增項要求	無
SR 6.2 SL-C	安全等級	·SL-C（TRE，控制系統）1：未選用 ·SL-C（TRE，控制系統）2：SR 6.2 ·SL-C（TRE，控制系統）3：SR 6.2 ·SL-C（TRE，控制系統）4：SR 6.2

3.2.2.7 FR 7 資源可用性（ Resource availability, RA）

區　　分	內　　容
目的	確保控制系統的可用性，防止降級或拒絕基本服務。
安全等級區分	·SL1 – 確保控制系統在正常生產條件下可靠運作，並防止由實體的偶然或巧合行為造成的 DoS 情況。 ·SL2 – 確保控制系統在正常和異常生產條件下可靠運作，並防止通過使用資源少，一般技能和動力不足的簡單方式造成的 DoS 情況。 ·SL3 – 確保控制系統在正常，異常和極端生產條件下可靠運作，並防止通過使用具有適度資源，IACS 特定技能和適度動力的複雜手段來 DoS 情況。 ·SL4 – 確保控制系統在正常、異常和極端生產條件下可靠運作，並防止通過使用具有擴展資源，IACS 特定技能和高動力的複雜手段來造成的 DoS 情況。
功能要求說明	此系列 SR 的目的是確保控制系統能夠抵禦各種類型的 DoS 事件。這包括各個等級的系統功能部分或完全不可用。 特別是，控制系統中的安全事件不應影響 SIS 或其他與安全相關的功能。

3.2.2.7.1 FR 7 資源可用性的安全需求清單

安全要求編號	安全要求清單
SR 7.1	阻斷服務攻擊防護
SR 7.2	資源管理
SR 7.3	控制系統備份
SR 7.4	控制系統恢復和重建
SR 7.5	緊急電源
SR 7.6	網路和安全設定設置
SR 7.7	功能最少
SR 7.8	控制系統元件盤點

3.2.2.7.2 SR 7.1 阻斷服務攻擊防護

編號	區分	內容
SR 7.1	基本要求	控制系統應提供在 DoS 攻擊事件期間以降級模式運作的能力。
SR 7.1	說明	存在各種技術來限制或在某些情況下消除 DoS 情況的影響。 例如，邊界保護裝置可以過濾某些類型的資料封包，以保護內部可信網路上的裝置不受 DoS 事件的直接影響或限制資訊流為單向出站。 具體而言，控制系統上發生的 DoS 事件不應對任何安全相關系統產生不利影響。
SR 7.1 RE(1)	增項要求	（1）管理通信負載 控制系統應提供管理通信負載（例如使用速率限制）的能力，以減輕資料流氾濫類型的 DoS 事件的影響。
SR 7.1 RE(2)	增項要求	（2）將 DoS 效應限制在其他系統或網路中 控制系統應提供限制所有使用者（人員、軟體程序或裝置）引起影響其他控制系統或網路的 DoS 事件的能力。
SR 7.1 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.1 ·SL-C（RA，控制系統）2：SR 7.1（1） ·SL-C（RA，控制系統）3：SR 7.1（1）（2） ·SL-C（RA，控制系統）4：SR 7.1（1）（2）

3.2.2.7.3 SR 7.2 資源管理

編號	區分	內容

SR 7.2	基本要求	控制系統應提供通過安全功能限制資源使用的能力，以防止資源耗盡。
SR 7.2	說明	資源管理（例如，網路分段或優先等級方案）防止較低優先等級的軟體程序延遲或干擾為任何較高優先等級的軟體程序提供服務的控制系統。 例如，在作業系統上啟動網路掃描、修補或防毒檢查可能會導致嚴重中斷正常操作。應將流量限制方案視為緩解技術。
SR 7.2 RE	增項要求	無
SR 7.2 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.2 ·SL-C（RA，控制系統）2：SR 7.2 ·SL-C（RA，控制系統）3：SR 7.2 ·SL-C（RA，控制系統）4：SR 7.2

3.2.2.7.4 控制系統備份

編號	區分	內容
SR 7.3	基本要求	控制系統應支援關鍵文件的身分識別和位置以及進行使用者層級和系統層級資訊（包括系統狀態資訊）備份的能力，而不影響正常的工廠運作。
SR 7.3	說明	從控制系統故障或設定錯誤中恢復，最新備份的可用性至關重要。 自動執行此功能可確保備份到所有必需的文件，從而減少操作員作業負擔。 雖然控制系統恢復通常不需要這些資訊，但事後事件取證所需的資訊（例如，稽核日誌）應特別包含在備份清單中（參見 SR 6.2 – 連續監控）。 如果產生的備份包含機密資訊，則應考慮加密（參見 SR 4.3 – 密碼術的使用）。
SR 7.3 RE(1)	增項要求(	(1)備份驗證 控制系統應提供驗證備用機制可靠性的能力。
SR 7.3 RE(2)	增項要求	(2)備份自動化 控制系統應提供基於可設定頻率自動執行備份功能的能力。
SR 7.3SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.3 ·SL-C（RA，控制系統）2：SR 7.3（1） ·SL-C（RA，控制系統）3：SR 7.3（1）（2） ·SL-C（RA，控制系統）4：SR 7.3（1）（2）"

3.2.2.7.5 SR 7.4 控制系統恢復和重建

編號	區分	內容
SR 7.4	基本要求	控制系統應提供在中斷或故障後恢復和重建到已知安全狀態的能力。

SR 7.4	說明	控制系統恢復和重建到已知安全狀態意味著所有系統參數（預設或可設定）都設置為安全值，在控制系統中斷或故障後可執行下列作業： 1. 執行重新安裝安全關鍵修補程序， 2. 備妥重新建立安全相關設定設置、系統文件和操作程序， 3. 重新安裝應用程式和系統軟體並使用安全設置進行設定， 4. 載入來自最新的已知安全備份的資訊， 5. 並對系統進行全面測試和運作。
SR 7.4 RE	增項要求	無
SR 7.4 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.4 ·SL-C（RA，控制系統）2：SR 7.4 ·SL-C（RA，控制系統）3：SR 7.4 ·SL-C（RA，控制系統）4：SR 7.4

3.2.2.7.6 SR 7.5 緊急電源

編　　號	區　　分	內　　容
SR 7.5	基本要求	控制系統應提供切換到應急電源和從應急電源切換回到正常電源的能力，而不會影響現有的安全狀態或記錄的降級模式。
SR 7.5	說明	可能存在諸如實體門禁控制之類的補償對策可能受到基本電源損失的影響的情況，在這種情況下，應急電源應該覆蓋那些相關系統。 如果不可能，則在這種緊急情況下可能需要其他補償措施
SR 7.5 RE	增項要求	無
SR 7.5 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.5 ·SL-C（RA，控制系統）2：SR 7.5 ·SL-C（RA，控制系統）3：SR 7.5 ·SL-C（RA，控制系統）4：SR 7.5

3.2.2.7.7 SR 7.6 網路和安全設定設置

編　　號	區　　分	內　　容
SR 7.6	基本要求	控制系統應提供根據控制系統供應商提供的指南中所述的推薦網路和安全設定進行設定的能力。 控制系統應為當前部署的網路和安全設定設置提供介面。
SR 7.6	說明	這些設定設置是控制系統元件的可調參數。 為了能夠檢測並糾正與核准或推薦的設定設置的任何偏差，控制系統需要支援根據安全政策和過程監視和控制設定設置的更

		改。 為了增強安全性，可以執行自動檢查，其中當前設置由代理自動收集並與核准的設置進行比較。
SR 7.6 RE(1)	增項要求	（1）當前安全設置的機器可讀報告 控制系統應能夠以機器可讀的格式產生列出當前部署的安全設置的報告。
SR 7.6 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.6 ·SL-C（RA，控制系統）2：SR 7.6 ·SL-C（RA，控制系統）3：SR 7.6（1） ·SL-C（RA，控制系統）4：SR 7.6（1）

3.2.2.7.8 SR 7.7 功能最少化

編號	區分	內容
SR 7.7	基本要求	控制系統應提供專門禁止或限制使用不必要的功能、介面、協議或服務的能力。
SR 7.7	說明	控制系統能夠提供各種功能和服務。 提供的某些功能和服務可能不是支援基本功能所必需的。 因此，預設情況下，應禁用基線設定之外的功能。 另外，有時從控制系統的單個元件提供多個服務是方便的，但這樣做會增加限制任何一個元件提供的服務的風險。 通常由商業現貨（COTS）裝置提供的許多功能和服務可以是禁止或限制的應用層服務，例如，電子郵件、網際網路協議語音（VoIP）、即時訊息（IM）、檔案傳輸協議（FTP）、 網頁服務（HTTP）和文件共享。
SR 7.7 RE	增項要求	無
SR 7.7 SL-C	安全等級	·SL-C（RA，控制系統）1：SR 7.7 ·SL-C（RA，控制系統）2：SR 7.7 ·SL-C（RA，控制系統）3：SR 7.7 ·SL-C（RA，控制系統）4：SR 7.7

3.2.2.7.10 SR 7.8 控制系統元件盤點

編號	區分	內容
SR 7.8	基本要求	控制系統應提供報告已安裝元件及其相關屬性的當前列表的能力。
SR 7.8	說明	控制系統元件盤點可以包括但不限於元件 ID、能力和修訂等級。 元件盤點應與控制系統當前構型一致。 應部署正式的設定管理過程，以控制元件盤點基線的變化。
SR 7.8	增項要求	無
SR 7.8	安全等級	·SL-C（RA，控制系統）1：未選用 ·SL-C（RA，控制系統）2：SR 7.8 ·SL-C（RA，控制系統）3：SR 7.8 ·SL-C（RA，控制系統）4：SR 7.8

3.2.3 元件安全 Component Security

本章前一節中定義的系統安全要求（SR）和增項要求（RE）擴展為 IACS 中包含的元件的一系列元件安全要求（CR）和增項要求（RE）。為了便於在 ISA-

62443-3-3 中將 CR 追溯到 SR，CR 編號將與相關的 SR 對應。這將導致本節中的產生一些空白和非順序編號。為了向讀者提供詳盡內容，為每個基本要求提供了基本原理和補充指導的說明，並為任何相關的要求提供了說明 RE 被認為是必要的。
本節定義的 IACS 元件類型包括：軟體應用程式、主機設備、嵌入式設備和網路設備。大多數 CR 和 RE 適用於所有四種類型的元件，並且組合成單個元件安全要求（CR）。
某些 CR 和 RE 對於特定類型的元件是唯一的。為便於參考，這些元件類型的特定要求已分為單獨的條款。從第 3.2.3.2 節開始介紹軟體應用程式、嵌入式設備、主機設備和網路設備的特定要求。如果元件滿足軟體應用程式、主機設備、嵌入式設備或網絡設備中的一個或多個的定義，則該元件應該是滿足它滿足的每種元件類型列出的所有要求。
參考 ISA-62443-1-1 中定義的七個 FR 中的每一個都具有一組定義的 4 個安全等級（SL）。這些 SL 源自 ISA-62443-3-3 中定義的系統安全等級。每個 FR 使用符號 SL -C（FR，元件）描述元件的安全等級，其對應值為 0 到 4 特定 FR 的控制系統能力等級 0 被視為定義為無要求。然後，將每個 FR 的基線要求和 RE（如果存在）對應到元件能力安全等級 SL-C（FR，元件）1 到 4。
在關鍵基礎設施提供者或是高度依賴工控物聯網並重視資安防護的資產擁有者，建議採用通過 IEC 62443 4-1 的內建安全開發（Secure by Design）要求的供應商，其開發過程安全要求的檢核表，如附錄 D「元件安全開發要求檢核表」。
重要工控元件建議採用已通過 IEC 62243 4-2 第三方獨立驗證的產品。
本節元件安全各控制項檢核表，請參考附錄 E「元件安全技術要求檢核表」。

3.2.3.1. 共通安全要求

3.2.3.1.1 FR 1 識別和認證控制（Identification and authentication control, IAC）

區　　分	內　　容
目的	在允許所有使用者存取系統或資產之前，識別並驗證所有使用者（人員、軟體程序和設備）。

安全等級區分	•SL 1 – 防止通過未經身份驗證的實體偶然或偶然存取的機制來識別和驗證所有使用者（人員、軟體程序和設備）。 •SL 2 – 防止通過機制識別和驗證所有使用者（人員、軟體程序和設備），這些機制使用簡單的方法，低資源，一般技能和低動機，實體進行有意的未經身份驗證的存取。 •SL 3 – 防止通過機制識別和驗證所有使用者（人員、軟體程序和設備），這些機制使用具有適度資源、IACS 特定技能和適度動機的複雜手段有意未經身份驗證的存取。 •SL 4 – 防止通過機制來識別和驗證所有使用者（人員、軟體程序和設備），這些機制可以防止實體使用具有擴展資源，IACS 特定技能和高動機的複雜手段進行有意的未經身份驗證的存取。
說明	使用者的身分識別與授權機制結合使用以達成元件的存取控制。 驗證請求存取的使用者的身份是必要的，以防止未經授權的使用者存取該元件。 建議和指南應包括將以混合模式運作的機制。 例如，通信信道上的某些元件需要強大的存取控制，例如強認證機制，而其他元件則不需要。 通過擴展，存取控制要求需要擴展到靜態資料。 建議最小化單個區域內的識別和認證機制的數量。 使用多種身份識別和身份驗證機制使得身份驗證和身份識別管理的任務更難以管理。「

3.2.3.1.2 FR 1 識別和認證控制的安全要求清單

安全要求清單	安全要求名稱
CR 1.1	人類使用者識別和認證
CR 1.2	軟體處理程序和設備識別和認證
CR 1.3	帳戶管理
CR 1.4	身份識別管理
CR 1.5	認證器管理
CR 1.6	無線存取管理

CR 1.7	基於密碼的身份驗證的強度
CR 1.8	公鑰基礎設施憑證
CR 1.9	基於公鑰的身份驗證的強度
CR 1.10	認證器回饋
CR 1.11	不成功登錄嘗試
CR 1.12	系統使用通知
CR 1.13	通過不受信任的網路存取
CR 1.14	對稱密鑰認證的強度

3.2.3.1.3 CR 1.1 人類使用者識別和認證

編　　號	區　　分	內　　容
CR 1.1	基本要求	根據 SR 1.1，元件應提供在所有能夠進行人類使用者存取的介面上識別和驗證所有人類使用者的能力。 此功能應在所有介面上強制執行此類識別和身份驗證，這些介面為人員提供對元件的存取權限，以根據適用的安全政策和程序支援職責分離和最小權限。該功能可由元件本地提供或整合到系統層級識別和認證系統。
CR 1.1	說明	根據 SR1.1，所有人類使用者都需要通過對元件的所有存取進行識別和身份驗證。 應該使用諸如以下方法來完成對這些使用者身份的認證密碼、令牌、生物識別或實體鍵控蓋等，以及多因素的情況身份驗證，它的某種組合。人類使用者的地理位置也可以用作身份驗證過程的一部分。這個要求應該適用於本地和遠端存取元件。此要求除了要求之外這種身份驗證和系統等級的識別。能夠進行人類使用者存取的介面是本地使用者界面，例如觸控螢幕、推送按鈕、鍵盤等以及為人類使用者交互而設計的網路協議作為網頁瀏覽（HTTP），安全 HTTP（HTTPS），文件傳輸協議（FTP），安全 FTP（SFTP），用於設備設定工具的協議（有時是專有的和其他時候使用開放協議）。使用者身分識別和認證可以是基於角色的或基於群組的（例如，對於某些元件介面，多個使用者可能共享相同的身分識別）。使用者識別和認證不應妨礙需要快速應變的本地緊急行動。 為了支援 IAC 政策，元件應該作為第一步，驗證所有人類使用者的身份。在第二步中，權限分配給應該強制執行已識別的人類使用者。
CR 1.1 RE(1)	增項要求	(1)唯一識別和認證： 元件應提供唯一身份識別和驗證所有人類使用者的能力。
CR 1.1 RE(2)	增項要求	(2)所有介面的多因素認證 元件應提供對所有人類使用者採用多因素身份驗證的能力存取該元件。
CR 1.1	安全等級	・SL-C（IAC，元件）1：CR 1.1

SL-C		・SL-C（IAC，元件）2：CR 1.1（1） ・SL-C（IAC，元件）3：CR 1.1（1）（2） ・SL-C（IAC，元件）4：CR 1.1（1）（2）「

3.2.3.1.4 CR 1.2 軟體處理程序和設備識別和認證

編　　號	區　　分	內　　容
CR 1. 2	基本要求	根據 SR1.2，元件應提供識別自身和驗證任何其他元件（軟體應用程式、嵌入式設備、主機設備和網路設備）的能力。如果元件，如應用程式的情況是在人類用戶的情境中運行，此外，根據 SR1.1 對人類用戶的識別和認證可以是元件識別的一部分， 對其他元件的身份驗證過程。
CR 1. 2	說明	識別和認證的功能是將已知身份對應到未知軟體處理器設備（以下稱為 CR 1.2 中的實例），以便在允許任何資料交換之前使其知曉。允許惡意實例發送和接收控制系統特定資料可能導致控制系統的有害行為。 應對所有實例進行識別和認證，以便對控制系統進行所有存取。 應通過使用諸如密碼，令牌或位置（實體或邏輯）之類的方法來完成對這些實體的身份的認證。此要求應適用於對控制系統的本地和遠端存取。但是，在使用單個實例連接到不同目標系統的某些情況下（例如，遠端供應商支援），實例具有多個身份在技術上可能是不可行的。在這些情況下，必須採用補償措施。 在識別和驗證可攜式媒體和行動裝置時，需要特別注意。這些類型的設備是將不希望的網路流量，惡意軟體或資訊暴露引入控制系統（包括其他隔離網路）的已知方法。 在實例作為單個組運行的情況下，識別和認證可以是基於角色的、基於群組的或基於實例的。是非常重要的是，當地的緊急行動以及控制系統的基本功能不得因識別或認證要求而受到阻礙。例如，在一般的保護和控制方案中，一組設備聯合執行保護功能，並與群組內的設備之間的多播訊息通信。在這些情況下，通常使用基於共享帳戶或共享對稱密鑰的組認證。 為了支援識別和認證控制政策，控制系統作為第一步驗證所有實例的身份。在第二步中，強制分配給所識別實例的權限（參見 CR 2.1 – 授權實施）。
CR 1. 2 RE(1)	增項要求	1）身份識別和認證元件應提供對任何其他元件進行唯一身份識別和認證的能力。
CR 1. 2 SL-C	安全等級	・SL-C（IAC，元件）1：未選用 ・SL-C（IAC，元件）2：CR 1.2 ・SL-C（IAC，元件）3：CR 1.2（1） ・SL-C（IAC，元件）4：CR 1.2（1）

3.2.3.1.5 CR 1.3 帳戶管理

編　　號	區　　分	內　　容
CR 1.3	基本要求	元件應提供直接支援所有帳戶管理或整合到管理帳戶的系統的能力。
CR 1.3	說明	元件可以通過整合到更高等級的帳戶管理系統來提供此功能。 如果該功能未整合到更高等級的帳戶管理系統中，則該元件應該本身提供該功能。 元件滿足此要求的常用方法是將身份驗證委派給目錄伺服器（例如，LDAP 或 Active Directory），該目錄伺服器提供 SR 1.3 所需的帳戶管理功能。 當元件整合到更高等級的系統中以提供帳戶管理功能時，需要考慮在更高等級的系統功能變得不可用的情況下對元件的影響。
CR 1.3 RE	增項要求	無
CR 1.3 SL-C	安全等級	• SL-C（IAC，元件）1：CR 1.3 • SL-C（IAC，元件）2：CR 1.3 • SL-C（IAC，元件）3：CR 1.3 • SL-C（IAC，元件）4：CR 1.3

3.2.3.1.6 CR 1.4 身份識別管理

編　　號	區　　分	內　　容
CR 1.4	基本要求	根據 SR 1.4，元件應提供整合到支援身分識別符號管理的系統或提供直接支援身分識別符號管理的能力的能力，
CR 1.4	說明	在 CR 1.3 下建立的帳戶 – 帳戶管理要求使用一個或多個身分識別符號來清楚地識別每個帳戶。 這些身分識別符號對於與其關聯的帳戶必須是唯一且明確的。 常用身分識別符號的一些舉例是帳戶名，UNIX 用戶 ID，Microsoft Windows 帳戶全局唯一身分識別符號（GUID）和綁定的 X.509 證書。 元件可以提供將身分識別符號與帳戶相關聯的本地能力。 如果將元件整合到強制執行系統範圍安全政策的系統中，則強烈建議將身分識別符號與系統中所有元件的同一帳戶相關聯。 為了達成這一點，元件必須能夠整合到系統範圍的身分識別符號管理功能中。
CR 1.4 RE	增項要求	無
CR 1.4 SL-C	安全等級	• SL-C（IAC，元件）1：CR 1.4 • SL-C（IAC，元件）2：CR 1.4 • SL-C（IAC，元件）3：CR 1.4 • SL-C（IAC，元件）4：CR 1.4

3.2.3.1.7 CR 1.5 認證器管理

編　　號	區　　分	內　　容
CR 1.5	基本要求	元件應提供以下功能： a）支援使用初始驗證器內容; b）支援識別在安裝時對預設驗證器進行的更改; c）通過定期驗證器更改/刷新操作正常運行; 和 d）保護認證器在儲存，使用和傳輸時不被未經授權的洩露和修改
CR 1.5	說明	「除了身分識別符號（見 CR 1.4）之外，還需要認證器來證明身份。控制系統認證器包括但不限於令牌、對稱密鑰、私鑰（公鑰/私鑰對的一部分）、生物識別、密碼、實體鑰匙和鑰匙卡。組織應該有安全政策，指示人類使用者必須採取合理的措施 保護身份驗證人員，包括保持對其個人身份驗證人的所有權，不與他人借用或共享身份認證器，並立即報告遺失或受損的身份認證器。 身份認證器有一個生命週期。自動建立帳戶時，需要建立新的身份驗證器，以便帳戶所有者能夠進行身份驗證。例如，在基於密碼的系統中，該帳戶具有與之關聯的密碼。初始認證者內容的定義可以解釋為管理員定義帳戶管理系統為所有新帳戶設置的初始密碼。能夠設定這些初始值使攻擊者更難以猜測帳戶建立和第一次帳戶使用之間的密碼（這應該涉及帳戶所有者設置新密碼）。某些控制系統安裝有無人值守的安裝程序，這些安裝程序使用預設密碼建立所有必需的帳戶，而某些嵌入式設備隨附預設密碼。隨著時間的推移，這些密碼通常成為一般知識，並在 Internet 上記錄。能夠更改預設密碼可以保護系統免受未經授權的使用者使用預設密碼進行存取。當在網路認證中使用時，可以從儲存或傳輸獲得密碼。這種複雜性可以通過加密保護（例如加密或雜湊）或通過根本不需要傳輸密碼的握手協議來增加。但是，密碼可能會受到攻擊，例如，蠻力猜測或破壞傳輸或儲存中密碼的加密保護。可以通過定期更改/刷新密碼來減少機會之窗。類似的考慮適用於基於加密密鑰的認證系統。可以通過使用硬體機制（如可信平台模組（TPM）等硬體安全模組）來達成增強的保護。 應在適用的安全政策和過程中指定認證器的管理，例如，更改預設驗證器的約束，刷新周期，認證器保護規範或驗證程序。 除了此要求中指定的身份驗證器管理功能外，身份驗證機制的強度還取決於所選身份驗證器的強度（例如，密鑰複雜性或公鑰身份驗證中的密鑰長度）以及在身份驗證過程中驗證身份驗證器的政策（例如，密碼有效期多

		長或在公鑰證書驗證中執行哪些檢查）。對於最常見的身份驗證機制，基於密碼和公鑰的身份驗證，CR 1.7,CR 1.8 和 CR 1.9 提供了進一步的要求。 某些操作的元件使用可能會受到限制，需要額外的身份驗證（例如令牌，密鑰和證書）才能執行某些功能。「
CR 1.5 RE(1)	增項要求	1）認證者的硬體安全性元件所依賴的認證者應通過硬體機制得到保護。
CR 1.5 SL-C	安全等級	・SL-C（IAC，元件）1：CR 1.5 ・SL-C（IAC，元件）2：CR 1.5 ・SL-C（IAC，元件）3：CR 1.5（1） ・SL-C（IAC，元件）4：CR 1.5（1）

3.2.3.1.8 CR 1.6 無線網路存取管理

無線存取管理要求是特定於網路元件的，可以 參考第 NDR 中對網路元件的要求。

3.2.3.1.9 CR 1.7 基於密碼的身份驗證的強度

編　　號	區　　分	內　　容
CR 1.7	基本要求	對於使用基於密碼的身份驗證的元件，這些元件應提供或整合到一個系統中，該系統根據國際公認的成熟密碼指南提供強制可配置密碼強度的功能。
CR 1.7	說明	無論是基於最小長度，多種字符還是持續時間（最小為一次性密碼），都必須能夠強制實施可設定的密碼強度，以幫助提高使用者所選密碼的整體安全性。 普遍接受的做法和建議可以在 NIST SP800-63-2，電子認證指南 NIST SP800-63-2，電子認證指南[27]等文件中找到。
CR 1.7 RE(1)	增項要求	（1）人類使用者的密碼產生和生命週期限制 元件應提供或整合到一個系統中，該系統提供防止任何特定的人類使用者帳戶在可設定的代數中重複使用密碼的能力。 此外，該元件應提供對人類使用者實施密碼最小和最大生命週期限制的能力。 這些功能應符合普遍接受的安全產業常見實務作法。 注意該元件應提供在到期前的可設定時間內提示使用者更改其密碼的功能。
CR 1.7 RE(2)	增項要求	（2）所有使用者（人員，軟體程序或設備）的密碼有效期限制 元件應提供或整合到一個系統中，該系統提供對所有使用者實施密碼最小和最大生命週期限制的能力。
CR 1.7 SL-C	安全等級	・SL-C（IAC，元件）1：CR 1.7 ・SL-C（IAC，元件）2：CR 1.7 ・SL-C（IAC，元件）3：CR 1.7（1）

		• SL-C（IAC，元件）4：CR 1.7（1）（2）

3.2.3.1.10 CR 1.8 公鑰基礎設施憑證

編　　號	區　　分	內　　容
CR 1.8	基本要求	當使用公鑰基礎設施（PKI）時，元件應提供或整合到一個系統中，該系統提供根據 SR1.8 進行交互和操作的能力。
CR 1.8	說明	選擇適當的 PKI 應該符合組織的證書政策，該政策應該基於違反受保護資訊機密性的風險。 關於政策定義的指導可以在普遍接受的標準和指南中找到，例如基於 X.509 的 PKI 的因特網工程任務組（IETF）評論請求（RFC）3647。 例如，證書頒發機構（CA）的適當位置，無論是在控制系統內還是在 Internet 上，以及可信 CA 的列表都應該在政策中考慮，並且取決於網路架構。
CR 1.8 RE	增項要求	無
CR 1.8 SL-C	安全等級	• SL-C（IAC，元件）1：未選用 • SL-C（IAC，元件）2：CR 1.8 • SL-C（IAC，元件）3：CR 1.8 • SL-C（IAC，元件）4：CR 1.8

3.2.3.1.11 CR 1.9 基於公鑰的身份驗證的強度

編　　號	區　　分	內　　容
CR 1.9	基本要求	對於使用基於公鑰的認證的元件，這些元件應直接提供或整合到在同一 IACS 環境中提供能力的系統中： a）通過檢查特定證書的簽名的有效性來驗證證書; b） 驗證證書鏈，或者在自簽名證書的情況下，通過將葉證書部署到與頒發證書的主題進行通信的所有主機; c）通過檢查特定證書的撤銷狀態來驗證證書; d）建立使用者 （人、軟體程序或設備）控制對應的私鑰; e）將經過身份驗證的身份對應到使用者（人員，軟體程序或設備）; f）確保用於公鑰認證的算法和密鑰符合 CR4.3 – 密碼學的使用。
CR 1.9	說明	要滿足 CR 1.9 中的要求，不一定需要與證書頒發機構進行即時連接。可以使用替代的帶外方法來滿足 CR 1.9 中的要求。例如，斷開連接的系統可以使用手動帶外進程安裝和更新認證。 公鑰/私鑰加密很大程度上取決於特定主題的私鑰的保密性以及對信任關係的正確處理。在基於公鑰認證驗證兩個實體之間的信任時，必須將公鑰證書跟踪到可信實體。證書驗證中的常見達成錯誤是僅檢查證書籤名的有效性，但不檢查簽名者中的信任。在 PKI 設置中，如果簽名者是受信任的 CA 或具有由受信任 CA 頒發的證書，則受信任者是受信任的，因此所有認證器都需要將呈現給他們的證書追溯回受信任的 CA.如果無法建立這樣的可信 CA 鏈，則不應信任所呈現的證書。 如果使用自簽名證書而不是 PKI，則證書主體本身會對其證書進行簽名，因此永遠不會存在受信任的第三方或 CA.這應該通過將自簽名公鑰證書部署到需要通過其他安全機制驗證它們的所有對等方（例如，受信任環境中所有對等方的配置）來進行補償。需要通過安全通道將可信證書分發給對等方。在驗證過程中，只有在自簽名證書已存在於驗證對等方的可信證書列表中時，才應信任該自簽名證書。應將受信任證書集配置為最小必需集。 在這兩種情況下，驗證還需要考慮撤銷證書的可能性。在 PKI 設置中，這通常通過維護證書吊銷列表（CRL）或運行在線證書狀態協議（OCSP）伺服器來完成。當由於控制系統約束而無法進行撤銷檢查時，諸如證書壽命短的機制可以補償缺少及時的撤銷資訊。請注意，短壽命證書有時會在控制系統環境中產生重大的操作問題。 預計大多數元件將整合到 IACS 中並利用底層 IACS 提供的密鑰認證機制。在 IACS 的元件級達成公鑰認證時，保護

		密鑰成為該元件密鑰儲存的主要關注點和目標。在實施過程中應注意確保元件中儲存的任何私鑰不能被檢索或篡改（參見CR 1.5 -Authenticator management）。 注意：可以使用防篡改設計方法和技術來幫助設計安全的私鑰保護機制。
CR 1.9 RE(1)	增項要求	（1）基於公鑰的認證的硬體安全性 元件應提供通過硬體機制保護關鍵的長期私鑰的功能。
CR 1.9 SL-C	安全等級	・SL-C（IAC，元件）1：未選用 ・SL-C（IAC，元件）2：CR 1.9 ・SL-C（IAC，元件）3：CR 1.9（1） ・SL-C（IAC，元件）4：CR 1.9（1）

3.2.3.1.12 CR 1.10 認證器回饋

編　　號	區　　分	內　　容
CR 1.10	基本要求	當元件提供身份驗證功能時，元件應提供 在認證程序中掩蓋認證者資訊反饋的能力
CR 1.10	說明	模糊反饋保護資訊免受未經授權的個人的可能利用，例如，當人類使用者鍵入使用者名或密碼時，顯示星號或其他隨機字符會掩蓋認證資訊的反饋。 其他舉例包括安全套接字 shell（SSH）令牌條目和一次性密碼的輸入。 身份驗證實體不應提供有關身份驗證失敗原因的任何提示，例如「未知使用者名」。
CR 1.10 RE	增項要求	無
CR 1.10 SL-C	安全等級	・SL-C（IAC，元件）1：CR 1.10 ・SL-C（IAC，元件）2：CR 1.10 ・SL-C（IAC，元件）3：CR 1.10 ・SL-C（IAC，元件）4：CR 1.10

3.2.3.1.13 CR 1.11 不成功登錄嘗試

編　　號	區　　分	內　　容
CR 1.11	基本要求	當元件提供身份驗證功能時，元件應提供以下功能： a）在可配置的時間段內對任何用戶（人、軟體過程或設備）強制執行可配置數量的連續無效訪問嘗試的限制; 和 b）在達到此限制時拒絕訪問指定的時間段或直到管理員

		解鎖
CR 1.11	說明	由於可能拒絕服務，可能會限制連續無效存取嘗試的次數。 如果啟用，則應用程式或設備可以在由適用的安全政策和過程建立的預定時間段之後自動重置為零存取嘗試次數。 將存取嘗試重置為零將允許使用者（人員，軟體程序或設備）獲得存取權限，如果他們具有正確的登錄憑據。 在緊急情況下需要立即操作員回應時，不應使用控制系統操作員工作站或節點的自動拒絕存取。 所有鎖定機制應考慮連續操作的功能要求，以便減少可能導致系統故障或損害系統安全性的不利拒絕服務操作條件。 允許對用於關鍵服務的帳戶進行交互式登錄可能會導致拒絕服務或其他濫用行為。
CR 1.11 RE	增項要求	無
CR 1.11 SL-C	安全等級	• SL-C（IAC，元件）1：CR 1.11 • SL-C（IAC，元件）2：CR 1.11 • SL-C（IAC，元件）3：CR 1.11 • SL-C（IAC，元件）4：CR 1.11

3.2.3.1.14 CR 1.12 系統使用通知

編　　號	區　　分	內　　容
CR 1.12	基本要求	當元件提供本地人類使用者存取/ HMI 時，它應提供顯示功能 在進行身份驗證之前系統使用通知訊息。 系統使用通知訊息 應由授權人員設定
CR 1.12	說明	隱私和安全政策和程序需要與適用的法律，指令，政策，法規，標準和指南保持一致。通常，這一要求的主要理由是對違法者進行法律起訴並證明故意違反。因此，此功能是支援政策要求所必需的，並且可能會提高 IACS 的安全性，因為它可以用作威懾。系統使用通知訊息可以以個人登錄控制系統時顯示的警告橫幅的形式達成。在控制系統工具中作為發布的實體通知實施的警告橫幅不能防止遠端登錄問題。 包含在系統使用通知訊息中的元素舉例如下： a）個人正在存取資產擁有者擁有的系統; b）可以監控，記錄系統使用情況並進行審核; c）禁止未經授權使用該系統，並受到刑事或民事處罰; d）使用該系統表示同意監測和記錄。
CR 1.12 RE	增項要求	無
CR 1.12 SL-C	安全等級	• SL-C（IAC，元件）1：CR 1.12 • SL-C（IAC，元件）2：CR 1.12 • SL-C（IAC，元件）3：CR 1.12

		• SL-C（IAC，元件）4：CR 1.12

3.2.3.1.15 CR 1.13 通過不受信任的網路存取

通過不受信任的網路存取要求是特定於元件的，可依軟體、嵌入式、主機型、網路元件個別要求納入考量。

3.2.3.1.16 CR 1.14 對稱密鑰認證的強度

編　　號	區　　分	內　　容
CR 1.14	基本要求	對於使用對稱密鑰的元件，元件應提供以下功能： a）使用對稱密鑰建立相互信任; b）安全儲存共享密鑰（只要共享密鑰保密，則認證有效）; c）限制對共享秘密的存取; 和 d）確保用於對稱密鑰認證的算法和密鑰符合 CR 4.3 – 使用密碼學。
CR 1.14	說明	應該定義用於將密鑰安裝到元件中的方法。這可能包括使用帶外方法安裝和管理元件密鑰。這是必要的，因為對元件中儲存的任何對稱密鑰的妥協可能導致完全妥協使用這些密鑰的系統。 實際上，有兩種基本方法可以將設備安全地驗證到另一種設備：使用非對稱加密（見 CR 1.9）或使用對稱加密。非對稱和對稱之間的選擇取決於幾個標準，如密鑰管理，信任供應，遺留支援和效率。對稱密鑰認證方案的舉例是 Needham-Schröder 或 Kerberos。當使用對稱密鑰認證時，該方使用他們過去學過的秘密密鑰（例如，通過信任提供）。該方通過證明秘密密鑰的知識證明了他們所聲稱的身份（例如，通過回答另一方，檢視員提交的質詢）。檢視員具有相同秘密的知識（也是過去通過信任供應學習的），並且能夠計算執行與證明者相同的加密操作的挑戰的答案。然後，檢視員可以將證明者的答案與其自己的計算進行比較。如果它們匹配，則檢視員確信證明者是他們聲稱的那個，並且該過程可以相反地進行，切換角色，以達成相互認證。只有當證明者和檢視員知道共享秘密並且每個證明者的秘密多樣化時，該機制才是安全的。這種機制的一個實例是正確使用基於密碼的訊息認證碼（CMAC）計算或者可選地使用 Galois 計數器模式（GCM）/ Galois 訊息認證碼（GMAC）操作模式。
CR 1.14 RE(1)	增項要求	（1）基於對稱密鑰的認證的硬體安全性 元件應提供通過硬體保護關鍵的長壽命對稱密鑰的能力 機制。

CR 1.14 SL-C	安全等級	• SL-C（IAC，控制系統）1：未選用 • SL-C（IAC，控制系統）2：CR 1.14 • SL-C（IAC，控制系統）3：CR 1.14（1） • SL-C（IAC，控制系統）4：CR 1.14（1）

3.2.3.1.17 FR 2 使用控制(Use control, UC)

區　　分	內　　容
目的	強制執行認證使用者（人員，軟體程序或設備）的分配權限，以對元件執行請求的操作並監視這些權限的使用。
安全等級區分	• SL 1 – 根據指定的特權限制使用 IACS，以防止偶然或巧合的濫用。 • SL 2 – 根據指定的特權限制 IACS 的使用，以防止實體使用資源少，一般技能和動機低的簡單手段進行規避。 • SL 3 – 根據指定的權限限制使用 IACS，以防止實體使用具有適度資源，IACS 特定技能和適度動機的複雜手段進行規避。 • SL 4 – 根據指定的特權限制使用 IACS，以防止實體使用具有擴展資源，IACS 特定技能和高動機的複雜手段進行規避。
功能需求說明	一旦識別並驗證了使用者，元件就必須將允許的操作限制為對元件的授權使用。資產擁有者和系統整合商必須為每個使用者（人員，軟體程序或設備），群組，角色等分配（見 4.5），這些權限定義了元件的授權使用。使用控制的目標是通過在允許使用者執行操作之前驗證已授予必要的權限來防止對元件資源的未授權操作。動作的舉例是讀取或寫入資料，下載程序和設置設定。建議和指南應包括將以混合模式運作的機制。例如，某些元件資源需要強大的使用控制保護，例如限制性權限，而其他元件則不需要。通過擴展，必須將使用控制要求擴展到靜止資料。使用者權限可能會根據時間/日期，位置和存取方式而有所不同。

3.2.3.1.18 FR 2 使用控制的安全要求清單

安全要求清單	安　全　要　求　名　稱
CR 2.1	授權執行
CR 2.2	無線使用控制
CR 2.3	對可攜式和行動裝置使用控制
CR 2.4	行動程式碼
CR 2.5	會話鎖定
CR 2.6	遠端會話終止

CR 2.7	並行會話控制
CR 2.8	可稽核事件
CR 2.9	稽核記錄儲存空間容量
CR 2.10	回應稽核記錄處理
CR 2.11	時間戳記
CR 2.12	不可否認性
CR 2.13	使用實體診斷和測試介面

3.2.3.1.19 CR 2.1 授權執行

編　　號	區　　分	內　　容
CR 2.1	基本要求	元件應為所有已識別的元件提供授權執行機制 經過身份驗證的使用者根據其分配的職責
CR 2.1	說明	「使用控制政策（例如，基於身份的政策，基於角色的政策和基於規則的政策）和相關的讀/寫存取強制機制（例如，存取控制列表，存取控制矩陣和加密）用於控制使用使用者（人、軟體程序和設備）和資產（例如，設備，文件，記錄，軟體程序，程序和域）之間的關係。 在控制系統驗證了使用者（人員，軟體程序或設備）的身份後（參見 CR 1.1 – 人類使用者識別和認證以及 CR 1.2 – 軟體程序和設備識別和認證），它還必須根據定義的安全政策和過程驗證是否實際允許所請求的操作。例如，在基於角色的存取控制政策中，控制系統將檢查分配給已驗證使用者或資產的角色以及分配給這些角色的權限 – 如果請求的操作由權限覆蓋，則執行，否則拒絕。這允許執行職責分離和最小特權。不應允許使用執行機制對控制系統的運作效能產生不利影響。 對控制系統元件的計劃內或計劃外更改可能對控制系統的整體安全性產生重大影響。因此，只有合格和授權的個人才能獲得控制系統元件的使用，以便啟動變更，包括升級和修改。「
CR 2.1 RE(1)	增項要求	（1）所有使用者（人、軟體程序和設備）的授權實施 元件應根據其分配的職責和最小權限為所有使用者提供授權強制執行機制。
CR 2.1 RE(2)	增項要求	（2）權限對應到角色 元件應直接或通過補償安全機制，提供授權角色來定義和修改所有人類使用者的角色權限對應。 註 1：角色不應限於固定的嵌套層次結構，其中較高等級的角色是較低特權角色的超級集合。 例如，系統管理員不一定包含操作員權限。 註 2：該 RE 也應適用於軟體程序和設備。
CR 2.1 RE(3)	增項要求	（3）主管覆蓋 元件應支援主管手動覆蓋，以設定可設定的時間或事件序列。

		註：通常需要在發生緊急情況或其他嚴重事件時實施受控，稽核和手動覆蓋自動化機制。 這允許管理員使操作員能夠快速回應異常情況而不關閉當前會話並將新會話建立為更高權限的人類使用者。
CR 2.1 RE(4)	增項要求	（4）雙重批准 當行動可能對工業過程產生嚴重影響時，元件應支援雙重批准。 注意雙重批准應限於需要非常高信度的行動，以確保可靠和正確地執行。 要求雙重批准強調了正確行動失敗可能導致的嚴重後果。 需要雙重批准的情況的一個例子是改變關鍵工業過程的設定點。 當需要立即回應以保護 HSE 後果時，不應採用雙重審批機制，例如，緊急關閉工業過程。
CR 2.1 SL-C	安全等級	・SL-C（UC，元件）1：CR 2.1 ・SL-C（UC，元件）2：CR 2.1（1）（2） ・SL-C（UC，元件）3：CR 2.1（1）（2）（3） ・SL-C（UC，元件）4：CR 2.1（1）（2）（3）（4）

3.2.3.1.20 CR 2.2 無線使用控制

編　　號	區　　分	內　　容
CR 2.2	基本要求	如果元件通過無線介面支援使用，則它應提供集成到系統中的能力，該系統根據普遍接受的產業慣例支援使用授權，監視和限制。
CR 2.2	說明	無線使用控制可以在構成系統的不同設備中達成。 網路設備可以是通過諸如網路准入控制之類的控制來協助使用控制的設備之一。 對於使用無線網路的設備和應用，這些設備應該能夠正確地利用無線網路保護，例如網路准入控制。 元件還可以基於存取是來自無線設備還是有線設備來達成對存取的不同限制。 這確實需要元件能夠區分介面是否通過無線。 一些網路設備提供掃描無線頻譜中的未授權無線網路活動的能力。 為了防止對控制系統功能的效能產生負面影響，最好部署專用設備來執行未經授權的網路活動檢查。
CR 2.2 RE	增項要求	無

CR 2.2 SL-C	安全等級	• SL-C（UC，元件）1：CR 2.2 • SL-C（UC，元件）2：CR 2.2 • SL-C（UC，元件）3：CR 2.2 • SL-C（UC，元件）4：CR 2.2

3.2.3.1.21 CR 2.3 對可攜式和行動裝置使用控制

沒有對元件層級的要求。

3.2.3.1.22 CR 2.4 行動程式碼

行動程式碼的使用控制要求是特定於元件的，可依軟體、嵌入式、主機型、網路元件個別要求納入考量。

3.2.3.1.23 CR 2.5 會話鎖定

編　　號	區　　分	內　　容
CR 2.5	基本要求	如果元件提供人工使用者界面，無論是本地存取還是通過網路存取，元件都應提供該功能 a）通過在可設定的不活動時間段之後或通過使用者（人、軟體程序或設備）手動啟動來啟動會話鎖定來防止進一步存取；和 b）使會話鎖保持有效直到擁有該會話的人類使用者或另一個授權的人類使用者使用適當的身分識別和認證過程重新建立存取。
CR 2.5	說明	會話鎖用於防止存取指定的工作站或節點。 元件應在可設定的時間段後自動激活會話鎖定機制。 在大多數情況下，會話鎖在系統等級設定。 作為此要求的一部分達成的會話鎖可能會被遠端會話終止所佔用或限制，如 CR 2.6 中所定義 – 遠端會話終止。
CR 2.5 RE	增項要求	無
CR 2.5 SL-C	安全等級	• SL-C（UC，元件）1：CR 2.5 • SL-C（UC，元件）2：CR 2.5 • SL-C（UC，元件）3：CR 2.5 • SL-C（UC，元件）4：CR 2.5

3.2.3.1.24 CR 2.6 遠端會話終止

編　　號	區　　分	內　　容

CR 2.6	基本要求	如果元件支援遠端會話，則元件應提供在可設定的不活動時間段後自動終止遠端會話的功能，由本地機構手動終止，或由啟動了該元件的使用者（人員，軟體程序或設備）手動終止遠端會話。會話。
CR 2.6	說明	只要在資產擁有者根據風險評估定義的區域邊界存取元件，就會啟動遠端會話。 此要求可能僅限於用於元件監視和維護活動（非關鍵操作）的會話，這些會話基於控制系統的風險評估以及安全政策和過程。 某些元件可能不允許會話終止，因為會話可能是元件基本功能的一部分。
CR 2.6 RE	增項要求	無
CR 2.6 SL-C	安全等級	• SL-C（UC，元件）1：未選用 • SL-C（UC，元件）2：CR 2.6 • SL-C（UC，元件）3：CR 2.6 • SL-C（UC，元件）4：CR 2.6

3.2.3.1.25 CR 2.7 並行會話總量控制

編　　號	區　　分	內　　容
CR 2.7	基本要求	元件應提供限制任何特定使用者（人員，軟體程序或設備）的每個介面的同時執行中會話數的能力。
CR 2.7	說明	如果沒有施加限制，可能會發生資源耗盡 DoS。 由於缺乏資源，可能會鎖定特定使用者與鎖定所有使用者和服務之間存在權衡。 產品供應商或系統整合商指南可能需要提供關於應如何分配同時執行中會話數量的充分資訊。
CR 2.7 RE	增項要求	無
CR 2.7 SL-C	安全等級	• SL-C（UC，元件）1：未選用 • SL-C（UC，元件）2：未選用 • SL-C（UC，元件）3：CR 2.7 • SL-C（UC，元件）4：CR 2.7

3.2.3.1.26 CR 2.8 可稽核事件

編　　號	區　　分	內　　容
CR 2.8	基本要求	元件應提供產生與以下類別的安全相關的稽核記錄的能力： a）存取控制; b）請求錯誤; c）控制系統事件; d）備份和恢復事件; e）設定變化; 和 f）審核日誌事件。

		個別稽核記錄應包括： a）時間戳; b）來源（發起設備，軟體程序或人類使用者帳戶）; c）類別; d）類型; e）事件 ID; 和 f）事件結果。
CR 2.8	說明	設備可能包含嵌入式韌體或運作作業系統。 雖然要求的目的是涵蓋事件類別，但至少包括可由韌體或 OS 產生的上述類別的所有事件。
CR 2.8 RE	增項要求	無
CR 2.8 SL-C	安全等級	・SL-C（UC，元件）1：CR 2.8 ・SL-C（UC，元件）2：CR 2.8 ・SL-C（UC，元件）3：CR 2.8 ・SL-C（UC，元件）4：CR 2.8

3.2.3.1.27 CR 2.9 稽核記錄儲存空間容量

編　　號	區　　分	內　　容
CR 2.9	基本要求	元件應 a）提供根據公認的日誌管理建議分配稽核記錄儲存容量的能力; 和 b）提供在元件達到或超過稽核儲存容量時防止元件故障的機制
CR 2.9	說明	元件應提供足夠的稽核儲存容量，同時考慮保留政策，要執行的稽核和在線稽核處理要求。 元件可以依賴於它們整合到的系統，以提供大部分稽核儲存容量。 但是，元件應提供足夠的本地儲存來緩衝稽核資料，直到可以將其發送到系統。 需要考慮的指南可能包括 NIST 特刊（SP）800-92。 審核儲存容量應足以在適用的政策和法規或業務要求所需的一段時間內保留日誌。
CR 2.9 RE(1)	增項要求	（1）達到稽核記錄儲存容量閾值時發出警告 元件應提供在分配的稽核記錄儲存達到可設定閾值時發出警告的功能。
CR 2.9 SL-C	安全等級	・SL-C（UC，元件）1：CR 2.9 ・SL-C（UC，元件）2：CR 2.9 ・SL-C（UC，元件）3：CR 2.9（1） ・SL-C（UC，元件）4：CR 2.9（1）

3.2.3.1.28 CR 2.10 回應稽核記錄處理

編　　號	區　　分	內　　容
CR 2.10	基本要求	元件應 a）提供在稽核處理失敗時防止遺失基本服務和功能的能力；和 b）根據普遍接受的產業慣例和建議，提供支援稽核處理失敗的適當行動的能力。
CR 2.10	說明	稽核產生通常發生在事件來源。 稽核處理涉及傳輸，可能的擴充（例如，添加時間戳記）和持久儲存稽核記錄。 稽核處理失敗包括例如軟體或硬體錯誤，稽核捕獲機制中的故障以及達到或超過稽核儲存容量。 在設計適當的回應操作時要考慮的準則可能包括 NIST SP 800-92，IT 安全日誌管理指南。 應該注意的是，不是覆蓋最早的稽核記錄，就是停止稽核日誌的產生，可能會超出稽核儲存容量的回應，但意味著可能必要的取證資訊的遺失。 警報人員也可以是回應稽核處理失敗的適當支援行動。
CR 2.10 RE	增項要求	無
CR 2.10 SL-C	安全等級	・SL-C（UC，元件）1：CR 2.10 ・SL-C（UC，元件）2：CR 2.10 ・SL-C（UC，元件）3：CR 2.10 ・SL-C（UC，元件）4：CR 2.10

3.2.3.1.29 CR 2.11 時間戳記

編　　號	區　　分	內　　容
CR 2.11	基本要求	元件應提供建立用於稽核記錄的時間戳（包括日期和時間）的功能
CR 2.11	說明	時間戳格式的一個很好的參考是 ISO 8601：2004，資料元素和交換格式 – 資訊交換 – 日期和時間的表示。 在設計定期時移事件（例如某些地點的夏令時）時考慮的系統應該謹慎。
CR 2.11 RE(1)	增項要求	（1）時間同步 元件應提供建立與系統範圍時間源同步的時間戳的功能。
CR 2.11 RE(2)	增項要求	（2）保護時間源的完整性 時間同步機制應提供檢測未經授權的更改並在更改時引起稽核事件的能力。
CR 2.11SL-C	安全等級	・SL-C（UC，元件）1：CR 2.11 ・SL-C（UC，元件）2：CR 2.11（1） ・SL-C（UC，元件）3：CR 2.11（1） ・SL-C（UC，元件）4：CR 2.11（1）（2）

3.2.3.1.30 CR 2.12 不可否認性

編　　號	區　　分	內　　容
CR 2.12	基本要求	如果元件提供人類使用者界面，則元件應提供確定特定人類使用者是否採取特定操作的能力。 元件文件檔案中應列出不支援此類功能的控制元素。
CR 2.12	說明	使用者採取的特定動作的舉例包括執行操作員動作，改變控制系統設定，建立資訊，發送訊息，批准資訊（如指示同意）和接收訊息。 不可否認性防止使用者未採取特定行動的後來虛假聲明，未由特定文件檔案撰寫的作者，未發送訊息的發送者，未接收訊息的接收者或簽署人未簽署文件。 如果使用者採取特定操作（例如，發送電子郵件和批准工作訂單）或接收到特定資訊，則可以使用不可否認服務來確定資訊是否源自使用者。 通過採用各種技術或機制（例如，使用者識別和授權，數位簽章，數位訊息接收和時間戳）獲得不可否認服務。
CR 2.12 RE(1)	增項要求	（1）所有使用者的不可否認性 元件應提供確定特定使用者（人員，軟體程序或設備）是否採取特定操作的能力。
CR 2.12 SL-C	安全等級	• SL-C（UC，元件）1：CR 2.12 • SL-C（UC，元件）2：CR 2.12 • SL-C（UC，元件）3：CR 2.12 • SL-C（UC，元件）4：CR 2.12（1）

3.2.3.1.31 CR 2.13 使用實體診斷和測試介面

實體診斷和測試介面要求的使用是特定於元件的，可以 依軟體、嵌入式、主機型及網路元件類型的需要納入考量。

3.2.3.1.32 FR 3 系統完整性(System integrity, SI)

區　　分	內　　容
目的	確保元件的完整性，以防止未經授權的操作或修改。
安全等級區分	• SL 1 – 保護 IACS 的完整性，防止偶然或巧合的操弄。 • SL 2 – 使用資源少，一般技能和動機不足的簡單方法，保護 IACS 的完整性免受操弄。 • SL 3 – 保護 IACS 的完整性，防止某人使用具有適度資源，IACS 特定技能和適度動機的複雜手段進行操弄。 • SL 4 – 保護 IACS 的完整性，防止人們使用複雜的手段進行操弄，具有擴展的資源，IACS 特定的技能和高度的動機。

功能需求說明	元件在開始生產之前經常經歷多個測試週期（單元測試，系統測試等），以確定元件在開始生產之前將按預期執行。 一旦運營，資產擁有者負責維護元件的完整性。 資產擁有者可以使用他們的風險評估方法，為 IACS 中的不同元件，通信渠道和資訊分配不同等級的完整性保護。 實體資產的完整性應在運營和非運營狀態下保持，例如在生產期間，儲存期間或維護停機期間。 邏輯資產的完整性應在傳輸和靜止時保持，例如通過網路傳輸或駐留在資料儲存庫中。

3.2.3.1.33 FR 3 系統完整性安全要求清單

安全要求清單	安　　全　　要　　求　　名　　稱
CR 3.1	通信完整性
CR 3.2	防範惡意程式碼
CR 3.3	安全功能驗證
CR 3.4	軟體和資訊完整性
CR 3.5	輸入驗證
CR 3.6	輸出確認
CR 3.7	錯誤處理
CR 3.8	會話完整性
CR 3.9	稽核資訊保護
CR 3.10	更新支援
CR 3.11	防範與偵測實體篡改
CR 3.12	供應產品供應商的信任根源
CR 3.13	供應資產擁有者的信任根源
CR 3.14	啟動程序完整性

3.2.3.1.34 CR 3.1 通信完整性

編　號	區　　分	內　　容
CR 3.1	基本要求	元件應提供保護傳輸資訊完整性的能力。
CR 3.1	說明	許多常見的網路攻擊都是基於傳輸中資料的操弄，例如，網路資料包的操弄。交換或路由網路為攻擊者提供了操作資料包的絕佳機會，因為對這些網路的未檢測存取通常更容易，並且切換和為了獲得對傳輸資訊的更多存取，也可以操弄路由機製本身。在控制系統環境中的操作可以包括從感應器傳送到接收器的測量值的改變或者從控制應用程式發送的命令參數的改變。到執行器。 取決於情境（例如，本地網路段內的傳輸與通過不可信網路的傳輸）和傳輸中使用的網路類型（例如傳輸控制協議（TCP）/網際協議（IP）與本地串行鏈路），可行且適當的機制會有所不同在具有直接鏈路（點對點）的小型網路上，如果端點的完整性也受到保護，則對較低 SL 的所有節點的實體存取保護可能就足夠了（參見 7.6，CR 3.4 – 軟體和資訊完整性），同時

		在分佈在員工定期實際存在的區域或廣域網上的網路上，實體存取很可能是不可執行的。如果商業服務用於提供作為商品項目的通信服務而不是完全專用的服務（例如租用線路與 T1 鏈路），則可能更難以獲得有關實施所需安全控制的必要保證。溝通完整性（例如由於法律限制）。如果滿足必要的安全要求是不可行或不切實際的，那麼實施適當的補償對策或明確接受額外風險可能是適當的。 工業設備經常受到可能導致完整性問題或誤報事件的環境條件的影響。很多時候，環境中含有微粒，液體，振動，氣體，輻射和電磁干擾（EMI），這些干擾會導致影響通信線路和信號完整性的條件。網路基礎設施的設計應盡量減少對通信完整性的實體/環境影響。例如，當顆粒，液體或氣體成為問題時，可能需要使用密封的註冊插孔 45（RJ-45）或 M12 連接器代替電線上的商用級 RJ-45 連接器。電纜本身可能需要使用不同的護套來代替處理顆粒，液體或氣體。如果出現振動問題，可能需要使用 M12 連接器，以防止 RJ-45 連接器上的彈簧銷在使用過程中斷開。在輻射或 EMI 成為問題的情況下，可能需要使用屏蔽雙絞線或光纖電纜來防止對通信信號的任何影響。如果計劃無線網路驗證這是一個可行的解決方案，也可能需要在這些領域進行無線頻譜分析。
CR 3.1 RE(1)	增項要求	1）通信認證 元件應提供在接收期間驗證接收資訊真實性的能力通信
CR 3.1 SL-C	安全等級	・SL-C（SI，元件）1：CR 3.1 ・SL-C（SI，元件）2：CR 3.1（1） ・SL-C（SI，元件）3：CR 3.1（1） ・SL-C（SI，元件）4：CR 3.1（1）

3.2.3.1.35CR 3.2 防範惡意程式碼

對惡意程式碼要求的保護是特定於元件的，可依軟體、嵌入式、主機型、網路元件個別要求納入考量

3.2.3.1.36 CR 3.3 安全功能驗證

編　號	區　　分	內　　容
CR 3.3	基本要求	根據 SR3.3，元件應提供支援驗證安全功能的預期操作的能力。
CR 3.3	說明	產品供應商或系統整合商應提供有關如何測試設計的安全控制的指導。資產擁有者需要了解在正常操作期間運作這些驗證測試的可能後果。這些驗證的執行細節需要是仔細考慮連續操作的要求（例如，安排或事先通知）。 安全驗證功能的舉例包括： ・通過歐洲計算機防病毒研究所（EICAR）測試控制系統文件系統來驗證防病毒對策。防病毒軟體應檢測 EICAR 測試樣本，並應觸發對應的事件處理程序。 ・通過嘗試使用未經授權的帳戶存取來驗證識別，身份驗證和使用控制對策（對於某些功能，這可以是自動化的）。 ・通過在 IDS 中包含一個規則來驗證入侵檢測系統（IDS）作為安全控制，該規則觸發不規則但已知的非惡意流量。然後可以通過引入觸發此規則的流量以及適當的 IDS 監視和事件處理過程來執行測試。 ・確認稽核日誌記錄正在按照安全政策和過程的要求進行，並且未被內部或外部實體禁用。
CR 3.3 RE(1)	增項要求	（1）正常操作期間的安全功能驗證 元件應提供支援在正常操作期間驗證安全功能的預期操作的能力。 注意需要仔細實施此 RE 以避免不利影響。 它可能不適合安全系統。
CR 3.3 SL-C	安全等級	・SL-C（SI，元件）1：CR 3.3 ・SL-C（SI，元件）2：CR 3.3 ・SL-C（SI，元件）3：CR 3.3 ・SL-C（SI，元件）4：CR 3.3（1）

3.2.3.1.37 CR 3.4 軟體和資訊完整性

編　號	區　　分	內　　容

CR 3.4	基本要求	元件應提供執行或支援軟體，設定和其他資訊的完整性檢查以及這些檢查結果的記錄和報告的功能，或者整合到可以執行或支援完整性檢查的系統中。
CR 3.4	說明	如果已經繞過其他保護機制（例如授權實施），則採用完整性驗證方法來檢測，記錄，報告和防止可能發生的軟體和資訊篡改。元件應採用正式或推薦的完整性機制（例如加密雜湊函數）。例如，這種機制可用於監視現場設備的最新設定資訊，以檢測安全漏洞（包括未經授權的更改）。
CR 3.4 RE(1)	增項要求	（1）軟體和資訊的真實性 元件應能夠執行或支援對軟體，設定和其他資訊的真實性檢查，以及這些檢查結果的記錄和報告，或者整合到可以執行或支援真實性檢查的系統中。
CR 3.4 RE(2)	增項要求	（2）完整性違規的自動通知 如果元件正在執行完整性檢查，則它應能夠在發現嘗試進行未經授權的更改時自動向可設定實體提供通知。
CR 3.4 SL-C	安全等級	・SL-C（SI，元件）1：CR 3.4 ・SL-C（SI，元件）2：CR 3.4（1） ・SL-C（SI，元件）3：CR 3.4（1）（2） ・SL-C（SI，元件）4：CR 3.4（1）（2）

3.2.3.1.38 CR 3.5 輸入驗證

編　號	區　　分	內　　容
CR 3.5	基本要求	元件應驗證任何輸入資料的語法，長度和內容，這些輸入資料用作工業程序控制輸入或通過外部介面輸入，直接影響元件的操作。
CR 3.5	說明	應檢查用於檢查輸入資料的有效語法（例如設定點）的規則，以驗證此資訊未被篡改並符合規範。應預先篩選傳遞給解釋器的輸入，以防止內容被無意地解釋為命令。請注意，這是一個安全CR，因此它不解決人為錯誤，例如提供超出預期範圍的合法整數。輸入資料驗證的公認產業慣例包括已定義字段類型的超出範圍值，資料字段中的無效字符，資料丟失或不完整以及緩衝區溢位。無效輸入導致系統安全問題的其他舉例包括 SQL 注入攻擊，跨站點腳本或格式錯誤的資料包（通常由協議模糊器產生）。要考慮的準則應包括眾所周知的準則，例如開放式 Web 應用程式安全項目（OWASP）程式碼檢視指南。

CR 3.5 RE	增項要求	無
CR 3.5 SL-C	安全等級	• SL-C（SI，元件）1：CR 3.5 • SL-C（SI，元件）2：CR 3.5 • SL-C（SI，元件）3：CR 3.5 • SL-C（SI，元件）4：CR 3.5

3.2.3.1.39 CR 3.6 輸出確認

編　號	區　　分	內　　容
CR 3.6	基本要求	實體或邏輯連接到自動化過程的元件應提供將輸出設置為預定狀態的能力，如果不能保持元件供應商定義的正常操作。
CR 3.6	說明	由於對控制系統設備和軟體的威脅行為，控制系統輸出的確定性行為是確保正常操作完整性的重要特徵。理想情況下，設備在受到攻擊時繼續正常運作，但如果控制系統 如果控制系統輸出不能保持正常運作，則控制系統輸出需要失效到預定狀態。控制系統輸出的適當預定狀態取決於設備，可以是以下使用者可設定選項之一： • 無動機 – 輸出未達到無動機狀態; • 保持 – 輸出未達到最後已知的良好值; • 已修復 – 輸出未達到由資產擁有者或應用程式確定的固定值; • 動態 – 根據當前狀態，輸出無法達到上述選項之一。
CR 3.6 RE	增項要求	無
CR 3.6 SL-C	安全等級	• SL-C（SI，元件）1：CR 3.6 • SL-C（SI，元件）2：CR 3.6 • SL-C（SI，元件）3：CR 3.6 • SL-C（SI，元件）4：CR 3.6

3.2.3.1.40 CR 3.7 錯誤處理

編　號	區　　分	內　　容
CR 3.7	基本要求	元件應以不提供攻擊者可利用的資訊攻擊 IACS 的方式識別和處理錯誤情況。

CR 3.7	說明	產品供應商或系統整合商應仔細考慮錯誤訊息的結構和內容。 元件產生的錯誤訊息應提供及時有用的資訊，而不會洩露可能被攻擊者用來利用 IACS 的潛在有害資訊。 必須通過及時解決錯誤條件來證明披露這些資訊是合理的。 要考慮的準則可能包括眾所周知的指南，如 OWASP 準則檢視指南。 注意：可以幫助攻擊者攻擊 IACS 的錯誤訊息的一個很好的例子是提供有關係統身份驗證失敗的原因的詳細資訊。 例如，在反饋中聲明無效使用者或無效密碼將有助於攻擊者攻擊 IACS，因此不應提供。
CR 3.7 RE	增項要求	無
CR 3.7 SL-C	安全等級	・SL-C（SI，元件）1：CR 3.7 ・SL-C（SI，元件）2：CR 3.7 ・SL-C（SI，元件）3：CR 3.7 ・SL-C（SI，元件）4：CR 3.7

3.2.3.1.41 CR 3.8 會話完整性

編　號	區　　分	內　　容
CR 3.8	基本要求	元件應提供保護通信會話完整性的機制，包括： a）在使用者註銷或其他會話終止（包括瀏覽器會話）時使會話身分識別符無效的能力; b）為每個會話產生唯一會話身分識別符並僅識別系統產生的會話身分識別符的能力; 和 c）使用普遍接受的隨機源產生唯一會話身分識別符的能力。
CR 3.8	說明	這種控制側重於會話的通信保護，而不是資料包，等級。這種控制的目的是在通信會話的每一端以另一方的持續身份和資訊的有效性建立信任的基礎。例如，這種控制解決了中間人攻擊，包括會話劫持，將錯誤資訊插入會話或重放攻擊。使用會話完整性機制可能會產生很大的作業負荷，因此應根據即時通信要求。 會話劫持和其他中間人攻擊或虛假資訊注入通常利用易於猜測的會話 ID（密鑰或其他共享機密）或使用在會話終止後未正確無效的會話 ID。因此，會話驗證器的有效性應與會話的生命週期緊密相關。在產生唯一會話 ID 時採用隨機性有助於防止暴力攻擊以確定將來的會話 ID。
CR 3.8 RE	增項要求	無

CR 3.8 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：CR 3.8 ・SL-C（SI，元件）3：CR 3.8 ・SL-C（SI，元件）4：CR 3.8

3.2.3.1.42 CR 3.9 稽核資訊保護

編　號	區　　分	內　　容
CR 3.9	基本要求	元件應保護稽核資訊，稽核日誌和稽核工具（如果存在），防止未經授權的存取，修改和刪除。
CR 3.9	說明	稽核資訊包括成功稽核控制系統活動所需的所有資訊（例如，稽核記錄，稽核設置和稽核報告）。 稽核資訊對於錯誤改正，安全漏洞修補，調查和相關工作非常重要。 增強防止修改和刪除保護的機制包括將稽核資訊儲存到硬體強制的一次寫入媒體。
CR 3.9 RE(1)	增項要求	（1）一次性寫入媒體的稽核記錄 元件應提供在硬體強制的一次寫入介質上儲存稽核記錄的功能。
CR 3.9 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：CR 3.9 ・SL-C（SI，元件）3：CR 3.9 ・SL-C（SI，元件）4：CR 3.9（1）

3.2.3.1.43 CR 3.10 更新支援

對更新要求的支援依不同類型元件有差異作法，可以根據可依軟體、嵌入式、主機型、網路元件個別要求納入考量。

3.2.3.1.44 CR 3.11 防範與偵測實體篡改

實體防篡改和檢測要求是元件依不同類型元件有差異作法，可依軟體、嵌入式、主機型、網路元件個別要求納入考量。

3.2.3.1.45 CR 3.12 供應產品供應商的信任根源

供應產品供應商信任要求的根源是依不同類型元件有差異作法，可依軟體、嵌入式、主機型、網路元件個別要求納入考量

3.2.3.1.46 CR 3.13 供應資產擁有者的信任根源

供應資產擁有者信任要求的根源是依不同類型元件有差異作法，可依軟體、嵌入式、主機型、網路元件個別要求納入考量。

3.2.3.1.47 CR 3.14啟動程序完整性

啟動程序要求的完整性是依不同類型元件有差異作法 ，可依軟體、嵌入式、主機型、網路元件個別要求納入考量

3.2.3.1.48 FR 4 資料機密性(Data confidentiality, DC)

區　　分	內　　容
目的	確保通信信道和儲存在儲存庫中的資料資訊的機密性，以防止未經授權的洩露。
安全等級區分	• SL 1 – 通過竊聽或隨意暴露防止未經授權的資訊洩露。 • SL 2 – 使用資源少，一般技能和動機低的簡單方法防止未經授權向正在積極搜索資訊的實體披露資訊。 • SL 3 – 使用具有適度資源，IACS 特定技能和適度動機的複雜手段，防止未經授權向正在積極搜索資訊的實體披露資訊。 • SL 4 – 使用具有擴展資源，IACS 特定技能和高度積極性的複雜手段，防止未經授權向正在積極搜索資訊的實體披露資訊。
功能需求說明	某些元件產生的資訊，無論是在休息還是在途，都具有機密性或敏感性。 這意味著某些通信信道和資料儲存需要防止竊聽和未經授權的存取。

3.2.3.1.49 FR 4 資料機密性安全要求清單

安全要求清單	安　全　要　求　名　稱
CR 4.1	資訊機密性
CR 4.2	資訊持久性
CR 4.3	使用密碼學

3.2.3.1.49 CR 4.1 資訊機密性

編　號	區　分	內　　容
CR 4.1	基本要求	元件應 a）提供保護靜態資訊機密性的能力，支援明確的讀取授權;和 b）支援保護 SR 4 中定義的傳輸中資訊的機密性。

CR 4.1	說明	是否應保護特定資訊的決定取決於具體情況，不能在產品設計中進行。 但是，組織通過在控制系統中設定顯式讀取授權來限制對資訊的存取這一事實表明該資訊應該受到組織的保護。 因此，元件支援分配顯式讀授權的能力的所有資訊都應被視為具有潛在敏感性，因此元件還應提供保護其機密性的能力。 傳輸中資訊的機密性需要元件應該能夠支援的系統級功能。對於機密性保護，8.5 CR 4.3 – 密碼學的使用提供了進一步的要求。
CR 4.1 RE	增項要求	無
CR 4.1 SL-C	安全等級	• SL-C（DC，元件）1：CR 4.1 • SL-C（DC，元件）2：CR 4.1 • SL-C（DC，元件）3：CR 4.1 • SL-C（DC，元件）4：CR 4.1

3.2.3.1.49 CR 4.2 資訊持久性

編號	區分	內容
CR 4.2	基本要求	元件應提供從有效服務中釋放或退役的元件擦除支援顯式讀授權的所有資訊的能力。
CR 4.2	說明	從活動服務中刪除控制系統元件不應該提供無意釋放支援顯式讀授權的資訊的機會。 這種資訊的舉例可以包括儲存在非易失性儲存器中的認證資訊和網路設定資訊或者將促進未授權或惡意活動的其他加密資訊。 由使用者或角色的動作產生的資訊（或代表使用者或角色的軟體程序的動作）不應以不受控制的方式向不同的使用者或角色公開。 控制系統資訊或資料持久性的控制防止在資源被釋放回控制系統之後無意地洩露儲存在共享資源上的資訊。

CR 4.2 RE(1)	增項要求	（1）擦除共享記憶體資源 元件應提供防止通過易失性共享記憶體資源進行未授權和非預期資訊傳輸的功能。 注意易失性儲存器資源是指在釋放到儲存器管理後通常不保留資訊的資源。 但是，存在對隨機存取儲存器（RAM）的攻擊，其可能在實際被覆蓋之前提取密鑰材料或其他機密資料。 因此，當易失性共享記憶體被釋放回控制系統以供其他使用者使用時，需要從資源中清除所有唯一資料和與唯一資料的連接，以使新使用者看不到或無法存取它。
CR 4.2 RE(2)	增項要求	（2）擦除驗證 元件應提供驗證資訊擦除的能力。
CR 4.2 SL-C	安全等級	• SL-C（DC，元件）1：未選用 • SL-C（DC，元件）2：CR 4.2 • SL-C（DC，元件）3：CR 4.2（1）（2） • SL-C（DC，元件）4：CR 4.2（1）（2）

3.2.3.1.49 CR 4.3 使用密碼學

編　　號	區　　分	內　　容
CR 4.3	基本要求	如果需要加密，元件應根據國際公認和經過驗證的安全實踐和建議使用加密安全機制
CR 4.3	說明	加密保護的選擇應基於威脅和風險分析，其中包括受保護資訊的價值，被破壞資訊的機密性和完整性的後果，資訊保密的時間段以及控制系統操作約束。這可能涉及靜止，傳輸或兩者中的資訊。請注意，備份是靜態資訊的一個舉例，應被視為資料機密性和完整性評估過程的一部分。控制系統產品供應商應記錄與加密密鑰建立和管理相關的實踐和程序。控制系統應利用已建立和經過測試的加密和雜湊算法，如高級加密標準（AES）和安全雜湊算法（SHA）系列，以及基於分配的密鑰大小標準。密鑰產生需要使用有效的隨機數產生器來執行。密鑰管理的安全政策和過程需要根據定義的標準處理定期密鑰更改，密鑰銷毀，密鑰分發和加密密鑰備份。普遍接受的做法和建議可以在諸如 NIST SP 800-57，密鑰管理建議書，第 1 部分：總則等文件中找到。例如，可以在 FIPS 140-2，加密模組的安全要求]或 ISO / IEC 19790，資訊技術 - 安全技術 - 加密模組的安全要求中找到達成要求。 當滿足本文件中定義的許多其他要求時，此 CR 以及 CR 1.8 - 公鑰基礎結構證書可能適用。

CR 4.3 RE	增項要求	無
CR 4.3 SL-C	安全等級	• SL-C（DC，元件）1：CR 4.3 • SL-C（DC，元件）2：CR 4.3 • SL-C（DC，元件）3：CR 4.3 • SL-C（DC，元件）4：CR 4.3

3.2.3.1.50 FR 5 限制資料流(Restricted data flow, RDF)

區　　分	內　　容
目的	通過區域和管道對控制系統進行分段，以限制不必要的資料流。
安全等級區分	• SL 1 – 防止區域和管道分割的偶然或巧合規避。 • SL 2 – 防止使用資源少，一般技能和動機低的簡單方法對，實體區域和管道分割的預期規避。 • SL 3 – 防止通過使用具有適度資源，IACS 特定技能和適度動機的複雜手段，對區域和管道分割的預期規避。 • SL 4 – 防止通過使用具有擴展資源，IACS 特定技能和高動機的複雜手段，對區域和管道分割的預期規避。
功能需求說明	使用 ISO 31000 中定義的風險評估方法，資產擁有者應確定必要的資訊流限制，從而通過擴展確定用於提供此資訊的管道的設定。 衍生的規範性建議和指南應包括從將業務或公共網路的控制系統網路斷開連接到使用單向網路閘道器、單一狀態防火牆或 DMZ 設定來管理資訊流的機制。

3.2.3.1.51 FR 5 限制資料流安全要求清單

安全要求清單	安　全　要　求　名　稱
CR 5.1	網路分段
CR 5.2	區域邊界保護
CR 5.3	一般用途人對人通信限制
CR 5.4	應用程式分割

3.2.3.1.52 CR 5.1 網路分段

編　　號	區　　分	內　　容
CR 5.1	基本要求	元件應支援分段網路，以根據需要支援區域和管道，以支援基於邏輯分段和關鍵性的更廣泛的網路架構
CR 5.1	說明	組織將網路分段用於各種目的，包括網路安全。 分割網路的主要原因是減少網路流量進入控制系統的暴露，並減少來自控制系統的網路流量的傳播或流出。 這可以提高整體

		系統回應和可靠性，並提供網路安全保護措施。 它還允許控制系統內的不同網段（包括關鍵控制系統和安全相關係統）與其他系統分開，以提供額外的保護。 應根據控制系統的操作要求，明確說明從控制系統到網際網路的存取。
CR 5.1 RE	增項要求	無
CR 5.1 SL-C	安全等級	・SL-C（RDF，元件）1：CR 5.1 ・SL-C（RDF，元件）2：CR 5.1 ・SL-C（RDF，元件）3：CR 5.1 ・SL-C（RDF，元件）4：CR 5.1

3.2.3.1.53 CR 5.2 區域邊界保護

區域邊界保護要求是專屬於網路元件的，可以根據網路設備要求（NDR）來落實限制。

3.2.3.1.54 CR 5.3 一般用途人對人通信限制

一般的人對人通信限制要求是專屬於網路元件的，可以根據網路設備要求（NDR）來落實限制。。

3.2.3.1.55 CR 5.4 應用程式分割

沒有與 SR 5.4 相關的元件層級要求。

3.2.3.1.56 FR 6 及時回應事件(Timely response to events, TRE)

區　　分	內　　容
目的	通過通知有關當局，報告違規行為的必要證據並在發現事件時及時採取糾正措施來應對安全違規行為。
安全等級區分	・SL 1 – 監控 IACS 元件的操作，並在發現時通過收集和提供查詢時的取證證據來回應事件。 ・SL 2 – 通過積極收集和定期報告鑑識證據，監控 IACS 元件的運作情況，並在發現事件時做出回應。 ・SL 3 – 監控 IACS 元件的運作情況，並通過積極收集鑑識證據並將鑑識證據推送到適當的權威機構，在發現事件時做出回應。 ・SL 4 – 監控 IACS 元件的運作情況，並通過主動收集鑑識證據並將鑑識證據近乎即時地推送到適當的權限來應對發現的事件。
功能需求說明	儘管系統可以在安全狀態下開始操作，但是能夠持續監視系統以確保其保持在該安全狀態是很重要的。 如果事件影響系統的安全性，及時通知事件可能對減輕相關風險是非常重要。 資產擁有者應制定安全政策和程序以及回應安全違規所需的適當通信和控制線。 衍生的說明性建議和指南應包括收集，報告，保存和自動關聯鑑識證據的機制，以確保及時採取糾正措施。 監測工具和技術的使用不應對控制系統的運作效能產生不利影響。

3.2.3.1.57 FR 6 及時回應事件安全要求清單

安全要求清單	安　　全　　要　　求　　名　　稱
CR 6.1	稽核記錄存取性
CR 6.2	持續監控

3.2.3.1.58 CR 6.1 稽核記錄存取性

編　　號	區　　分	內　　容
CR 6.1	基本要求	元件應為授權人員或工具提供以唯讀方式存取稽核日誌的能力。
CR 6.1	說明	儘管系統可以在安全狀態下開始操作，但是能夠持續監視系統以確保其保持在該安全狀態是很重要的。 如果事件影響系統的安全性，及時通知事件可能對減輕相關風險是非常重要。 資產擁有者應制定安全政策和程序以及回應安全違規所需的適當通信和控制線。 衍生的說明性建議和指南應包括收集、報告、保存和自動關聯鑑識證據的機制，以確保及時採取糾正措施。 監測工具和技術的使用不應對控制系統的運作效能產生不利影響。
CR 6.1 RE(1)	增項要求	（1）以應用程式方式存取稽核日誌 元件應通過使用應用程式介面（API）或將稽核記錄發送到集中式系統來提供對稽核記錄的應用程式存取
CR 6.1 SL-C	安全等級	・SL-C（TRE，元件）1：CR 6.1 ・SL-C（TRE，元件）2：CR 6.1 ・SL-C（TRE，元件）3：CR 6.1（1） ・SL-C（TRE，元件）4：CR 6.1（1）

3.2.3.1.59 CR 6.2 持續監控

編　　號	區　　分	內　　容
CR 6.2	基本要求	元件應提供使用普遍接受的安全產業實踐和建議持續監控的能力，以及時檢測，表徵和報告安全漏洞。
CR 6.2	說明	可以通過各種工具和技術（例如，入侵偵測系統[IDS]、入侵防禦系統[IPS]，防止惡意程式碼機制和網路監視機制）來達成控制系統監視能力。隨著攻擊變得更加複雜，這些監控工具和技術也需要變得更加複雜，包括例如基於行為的 IDS / IPS、網路行為分析、封包深層分析等。 監控設備應政策性地部署在控制系統內（例如，在選定的周邊位置和支援關鍵應用的伺服器場附近）以收集基本資訊。還可以在控制系統內的臨時位置部署監視機制以跟踪特定事務。 監測應包括適當的報告機制，以便及時回應事件。為了將報告的重點和報告的資訊量保持在可以由收件人處理的等

		級，SIEM 等機制通常用於將各個事件關聯到聚合報告中，以建立原始事件發生的更大全景。
CR 6.2 RE	增項要求	無
CR 6.2 SL-C	安全等級	• SL-C（TRE，元件）1：未選用 • SL-C（TRE，元件）2：CR 6.2 • SL-C（TRE，元件）3：CR 6.2 • SL-C（TRE，元件）4：CR 6.2

3.2.3.1.60 FR7 資源可用性(Resource availability, RA)

區　　分	內　　容
目　　的	確保元件可用於防止或拒絕基本服務。
安全等級區分	• SL 1 – 確保元件在正常生產條件下可靠運作，並防止因實體的偶然或巧合行為而導致的拒絕服務情況。 • SL 2 – 確保元件在正常和異常生產條件下可靠運作，並防止實體使用資源少，一般技能和動機不足的簡單方法拒絕服務。 • SL 3 – 確保元件在正常、異常和極端生產條件下可靠運作，並防止實體使用具有適度資源，IACS 特定技能和適度動機的複雜手段進行拒絕服務。 • SL 4 – 確保元件在正常，異常和極端生產條件下可靠運作，並防止實體使用具有擴展資源，IACS 特定技能和高動機的複雜方法的拒絕服務情況。
功能需求說明	此系列 CR 的目的是確保元件能夠抵禦各種類型的 DoS 事件。 這包括各個等級的元件功能的部分或完全不可用。 特別是，元件中的安全事件不應影響基本功能或其他與安全相關的功能。

3.2.3.1.61 FR7 資源可用性安全要求清單

安全要求清單	安　全　要　求　名　稱
CR 7.1	阻斷服務保護
CR 7.2	資源管理
CR 7.3	控制系統備份
CR 7.4	控制系統復原和重建
CR 7.5	緊急電力
CR 7.6	網路和安全設定

CR 7.7	最低功能
CR 7.8	控制系統元件盤點

3.2.3.1.62 CR 7.1 阻斷服務保護

編　號	區　分	內　容
CR 7.1	基本要求	元件應提供在 DoS 事件導致的降級模式下運作時維持基本功能的能力。
CR 7.1	說明	元件可能會受到不同形式的 DoS 情況的影響。 當這些阻斷服務攻擊發生時，應該以承受各種 DoS 的能力設計元件，使其保持在降級模式下繼續安全操作所必需的基本功能。
CR 7.1 RE(1)	增項要求	(1) 管理元件的通信負載 元件應提供減輕資訊或訊息傳播類型的 DoS 事件的影響的能力。
CR 7.1 SL-C	安全等級	• SL-C (RA，元件) 1：CR 7.1 • SL-C (RA，元件) 2：CR 7.1 (1) • SL-C (RA，元件) 3：CR 7.1 (1) • SL-C (RA，元件) 4：CR 7.1 (1)

3.2.3.1.63 CR 7.2 資源管理

編　號	區　分	內　容
CR 7.2	基本要求	元件應提供限制安全功能使用資源的能力，以防止資源耗盡
CR 7.2	說明	資源管理 (例如，網路分段或優先等級方案) 可防止低優先等級軟體程序延遲或干擾為任何更高優先等級的軟體程序提供服務的控制系統。 例如，在作業系統上啟動網路掃描、修補或防病毒檢查可能會導致嚴重中斷正常操作。 應將流量限制方案視為緩解技術。
CR 7.2 RE	增項要求	無
CR 7.2 SL-C	安全等級	• SL-C (RA，元件) 1：CR 7.2 • SL-C (RA，元件) 2：CR 7.2 • SL-C (RA，元件) 3：CR 7.2 • SL-C (RA，元件) 4：CR 7.2

3.2.3.1.63 CR 7.3 控制系統備份

編　號	區　分	內　容
CR 7.3	基本要求	元件應提供參與系統等級備份操作的能力，以保護元件狀態 (使用者和系統級資訊)。 備份過程不應影響正常的元件操作。

CR 7.3	說明	從控制系統故障或設定錯誤中恢復，最新備份的可用性是非常重要。自動執行此功能可確保捕獲所有必需的文件，從而減少操作員作業負荷。 在設計支援備份功能時，應考慮將儲存在備份中的資訊內容屬性。其中一些資訊可能包含加密密鑰和其他資訊，這些資訊在系統的一部分時通過安全控制進行保護。將資訊放入備份後，很可能沒有相同的控制措施來保護它。因此，元件備份能力需要包括支援備份中包含的資訊的必要保護的機制。這可能包括備份加密或敏感資料加密作為備份過程的一部分，或者不包括敏感資訊作為備份的一部分。如果備份是加密的，則重要的是不要將加密密鑰作為備份的一部分包括在內，而是將加密密鑰備份為單獨的更安全的備份過程的一部分。
CR 7.3 RE(1)	增項要求	（1）備份完整性驗證 元件應提供在開始恢復該資訊之前驗證備份資訊的完整性的功能。
CR 7.3 SL-C	安全等級	・SL-C（RA，元件）1：CR 7.3 ・SL-C（RA，元件）2：CR 7.3（1） ・SL-C（RA，元件）3：CR 7.3（1） ・SL-C（RA，元件）4：CR 7.3（1）

3.2.3.1.63 CR 7.4 控制系統復原和重建

編　號	區　分	內　容
CR 7.4	基本要求	元件應提供在中斷或故障後恢復並重建為已知安全狀態的能力
CR 7.4	說明	元件恢復和重建到已知安全狀態意味著所有系統參數（預設或可設定）都設置為安全值，重新安裝安全關鍵修補程序，重新建立安全相關設定設置，系統文件和操作過程可用，元件重新安裝並使用已建立的設定檔進行設定，將載入來自最新的已知安全備份的資訊，並且系統已經過全面測試和運作。
CR 7.4 RE	增項要求	無
CR 7.4 SL-C	安全等級	・SL-C（RA，元件）1：CR 7.4 ・SL-C（RA，元件）2：CR 7.4 ・SL-C（RA，元件）3：CR 7.4 ・SL-C（RA，元件）4：CR 7.4

3.2.3.1.63 CR 7.5 緊急電力

沒有與SR 7.5相關的元件等級要求。

3.2.3.1.63 CR 7.6 網路和安全設定

編　號	區　分	內　容
CR 7.6	基本要求	元件應提供根據控制系統供應商提供的指南中所述的推薦網路和安全設定進行設定的功能。 元件應提供當前部署的網路和安全設定設置的介面。
CR 7.6	說明	這些設定設置是控制系統元件的可調參數。 預設情況下，應將元件設定為建議的設置。 為了使元件檢測並糾正與批准或推薦的設定設置的任何偏差，元件需要支援根據安全政策和過程監視和控制設定設置的更改。
CR 7.6 RE(1)	增項要求	（1）當前安全設置的機器報告可讀性 元件應提供以產生機器可讀格式，列出當前部署的安全設置的報告的功能。
CR 7.6 SL-C	安全等級	・SL-C（RA，元件）1：CR 7.6 ・SL-C（RA，元件）2：CR 7.6 ・SL-C（RA，元件）3：CR 7.6（1） ・SL-C（RA，元件）4：CR 7.6（1）

3.2.3.1.63 CR 7.7 最低功能

編　號	區　分	內　容
CR 7.7	基本要求	元件應提供專門限制不必要的功能、介面、協議或服務的使用的能力。
CR 7.7	說明	元件能夠提供各種功能和服務。 提供的某些功能和服務可能不是支援 IACS 功能所必需的。 因此，預設情況下，應禁用基線設定之外的功能。 另外，從控制系統的單個元件提供多個服務有時很方便，但與限制任何一個元件提供的服務相比，這樣做會增加風險。
CR 7.7 RE	增項要求	無
CR 7.7 SL-C	安全等級	・SL-C（RA，元件）1：CR 7.7 ・SL-C（RA，元件）2：CR 7.7 ・SL-C（RA，元件）3：CR 7.7 ・SL-C（RA，元件）4：CR 7.7

3.2.3.1.63 CR 7.8 控制系統元件盤點

編　號	區　分	內　容
CR 7.8	基本要求	元件應提供根據 SR 7.8 支援控制系統元件盤點的能力。
CR 7.8	說明	元件可以將它們自己的元件整合到整個控制系統中。 在這種情況下，元件需要提供可被自動化解決方案機制來增加與相容的整體元件盤點中建立和維護所有設備及其軟體元件的盤點紀錄，包括廠牌、型號、軟體、韌體版本和序號等。
CR 7.8 RE	增項要求	無
CR 7.8 SL-C	安全等級	・SL-C（RA，元件）1：未選用 ・SL-C（RA，元件）2：CR 7.8 ・SL-C（RA，元件）3：CR 7.8 ・SL-C（RA，元件）4：CR 7.8

3.2.3.2. 軟體應用程式安全要求

這組要求的目的是特定適用於軟體應用程式元件的要求。

3.2.3.2.1 SAR 2.4 行動程式碼

編　號	區　分	內　容
SAR 2.4	基本要求	如果軟體應用程式使用行動程式碼技術，則該應用程式應提供對行動程式碼技術的使用實施安全政策的能力。 對於軟體應用程式中使用的每種行動程式碼技術，安全政策應至少允許以下操作： a）控制行動程式碼的執行; b）控制允許哪些使用者（人員、軟體程序或設備）將行動程式碼傳送到應用程式或從應用程式傳送行動程式碼; c）在執行程式碼之前根據完整性檢查的結果控制行動程式碼的執行。
SAR 2.4	說明	行動程式碼技術包括但不限於 Java，JavaScript，ActiveX，可攜式文件格式（PDF），Postscript，Shockwave 電影，Flash 動畫和 VBScript。 使用限制適用於選擇和使用安裝在伺服器上的行動程式碼以及在各個工作站上下載和執行的行動程式碼。 控制程序應防止在元件所在的控制系統內開發、獲取或引入不可接受的行動程式碼。 例如，可以在控制系統內直接禁止行動程式碼交換，但是可以允許在由 IACS 人員維護的受控相鄰環境中。
SAR 2.4 RE(1)	增項要求	（1）行動程式碼真實性檢查 應用程式應提供執行安全政策的功能，該政策允許設備根據執行程式碼之前的真實性檢查結果來控制行動程式碼的執行

SAR 2.4 SL-C	安全等級	• SL-C（UC，元件）1：SAR 2.4 • SL-C（UC，元件）2：SAR 2.4（1） • SL-C（UC，元件）3：SAR 2.4（1） • SL-C（UC，元件）4：SAR 2.4（1）

3.2.3.2.2 SAR 3.2 防範惡意程式碼

編　　號	區　　分	內　　容
SAR 3.2	基本要求	應用程式產品供應商應限定並記錄惡意程式碼機制的保護措施與應用程式相容，並記錄任何特殊設定要求。
SAR 3.2	說明	防惡意程式碼（例如，病毒、蠕蟲、特洛伊木馬和間諜軟體）可以由控制系統應用程式或外部服務或應用程式提供。 控制系統應用程式需要與用以保護它們免受惡意程式碼攻擊的機制相容。 此要求並不意味著產品供應商要對所有與應用程式相容的惡意程式碼保護機制進行資格認證和記錄，但暗示產品供應商要對至少一種機制進行資格認證和記錄。
SAR 3.2 RE	增項要求	無
SAR 3.2 SL-C	安全等級	• SL-C（SI，元件）1：SAR 3.2 • SL-C（SI，元件）2：SAR 3.2 • SL-C（SI，元件）3：SAR 3.2 • SL-C（SI，元件）4：SAR 3.2

3.2.3.3. 嵌入式裝置安全要求

本節要求的目的是記錄嵌入式設備特有的要求。

3.2.3.3.1 EDR 2.4 行動程式碼

編號	區分	內容
EDR 2.4	基本要求	在嵌入式設備利用行動程式碼技術的情況下，嵌入式設備應提供對行動程式碼技術的使用實施安全政策的能力。 對於嵌入式設備上使用的每種行動程式碼技術，安全政策應至少允許以下操作： a）控制行動程式碼的執行; b）控制允許哪些使用者（人、軟體程序或設備）將行動程式碼上傳到設備; c）在執行程式碼之前根據完整性檢查的結果控制行動程式碼的執行。
EDR 2.4	說明	行動程式碼技術包括但不限於 Java，JavaScript，ActiveX，PDF，Postscript，Shockwave 電影，Flash 動畫和 VBScript。 使用限制適用於選擇和使用安裝在伺服器上的行動程式碼以及在各個工作站上下載和執行的行動程式碼。 控制程序應防止在元件所在的控制系統內開發、獲取或引入不可接受的行動程式碼。 例如，可以在控制系統內直接禁止行動程式碼交換，但是可以允許在由 IACS 人員維護的受控相鄰環境中。
EDR 2.4 RE(1)	增項要求	（1）行動程式碼真實性檢查 嵌入式設備應提供強制執行安全政策的功能，該政策允許設備根據執行程式碼之前的真實性檢查結果來控制行動程式碼的執行
EDR 2.4 SL-C	安全等級	・SL-C（UC，元件）1：EDR 2.4 ・SL-C（UC，元件）2：EDR 2.4（1） ・SL-C（UC，元件）3：EDR 2.4（1） ・SL-C（UC，元件）4：EDR 2.4（1）

3.2.3.3.2 EDR 2.13 使用實體診斷和測試介面

編　　號	區　　分	內　　容
EDR 2.13	基本要求	嵌入式設備應防止未經授權使用實體工廠診斷和測試介面（例如 JTAG 除錯）。
EDR 2.13	說明	在嵌入式設備內的各個位置設置工廠診斷和測試介面，以達成幫助嵌入式設備的開發人員和工廠人員測試功能，以及何時發現錯誤以便隨後將其從嵌入式設備中移除。但是，必須小心保護這些相同的介面，以防止未經授權的實體存取，以保護嵌入式設備向 IACS 提供的基本功能。 如果診斷和測試介面不提供控制嵌入式設備或存取非公共資訊的能力，則它不需要認證機制。這應通過威脅和風險評估來確定。一個例子是 JTAG 除錯，其中 JTAG 用於控制處理器並執行任意命令，而 JTAG 邊界掃描使用 JTAG 來簡單地讀取資訊（可能是公開可用的資訊）。 可能存在工廠診斷和測試介面使用與設備的網路通信的情況。在這種情況下，這些介面將滿足本文件的所有要求。
EDR 2.13 RE(1)	增項要求	（1）主動監測 嵌入式設備應提供對設備診斷和測試介面的主動監控，並在檢測到存取這些介面的嘗試時產生審核日誌條目。
EDR 2.13 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：EDR 2.13 ・SL-C（SI，元件）3：EDR 2.13（1） ・SL-C（SI，元件）3：EDR 2.13（1）

3.2.3.3.3 EDR3.2 防範惡意程式碼

編　　號	區　　分	內　　容
EDR 3.2	基本要求	嵌入式設備應提供防止未授權軟體的安裝和執行的能力。
EDR 3.2	說明	未經授權的軟體可能包含惡意程式碼，因此對元件有害。如果嵌入式設備能夠使用補償控制，則無需直接支援惡意程式碼保護。假設 IACS 將負責提供所需的保護措施。但是，對於諸如具有本地一般串行總線（USB）主機存取的方案，應該通過風險評估來確定對惡意程式碼的保護需求。 檢測機制應該能夠檢測應用程式二進製文件和資料文件的完整性違規。技術可以包括但不限於二進製完整性和屬性監視，雜湊和簽名技術。 預防技術可包括但不限於可移動媒體控制，沙箱技術和特定計算平台機制，例如受限韌體更新功能，無執行（NX）位，資料執行保護（DEP），地址空間佈局隨機化（ASLR），堆疊損壞檢測和強制存取控制。
13.4.3 RE	增項要求	無

13.4.4 SL-C	安全等級	・SL-C（SI，元件）1：EDR 3.2 ・SL-C（SI，元件）2：EDR 3.2 ・SL-C（SI，元件）3：EDR 3.2 ・SL-C（SI，元件）4：EDR 3.2

3.2.3.3.4 EDR3.10 更新支援

編　　號	區　　分	內　　容
EDR 3.10	基本要求	嵌入式設備應支援更新和升級的能力
EDR 3.10	說明	嵌入式設備在其安裝的生命週期內可能需要安裝更新和升級。 在某些情況下，嵌入式設備也會支援或執行基本功能。 在這種情況下，嵌入式設備需要具備支援修補和更新的機制，而不會影響高可用性系統的基本功能）。 提供此功能的一個舉例是支援嵌入式設備內的冗餘。
EDR 3.10 RE(1)	增項要求	（1）更新真實性和完整性 嵌入式設備應在安裝之前驗證任何軟體更新或升級的真實性和完整性
EDR 3.10 SL-C	安全等級	・SL-C（SI，元件）1：EDR 3.10 ・SL-C（SI，元件）2：EDR 3.10（1） ・SL-C（SI，元件）3：EDR 3.10（1） ・SL-C（SI，元件）4：EDR 3.10（1）

3.2.3.3.5 EDR3.11 防範與偵測實體篡改

編　　號	區　　分	內　　容
EDR 3.11	基本要求	嵌入式設備應提供防篡改和檢測機制，以防止未經授權的實體存取設備
EDR 3.11	說明	防篡改機制的目的是防止攻擊者企圖對 IACS 設備執行未經授權的實體操作。 如果發生篡改事件，則預防、檢測和回應是次要的。 防篡改機制最有效地組合使用以防止存取任何關鍵元件。 防篡改包括使用專門的材料來使設備或模組難以篡改。 這可以包括硬化外殼、鎖、封裝或安全螺釘等功能。 放置緊密的氣流路徑會增加探測產品內部的難度。 篡改證據的目的是確保在發生篡改事件時仍然存在可見或電子證據。 許多簡單的證據技術由密封物件和膠帶組成，以明顯存在實體篡改。
EDR 3.11 RE(1)	增項要求	（1）通知篡改企圖 嵌入式設備應能夠在發現嘗試進行未經授權的實體存取時自動向可設定的一組接收者提供通知。 所有篡改通知都應記錄為整個稽核日誌記錄功能的一部分
EDR 3.11 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：EDR 3.11 ・SL-C（SI，元件）3：EDR 3.11（1） ・SL-C（SI，元件）4：EDR 3.11（1）

3.2.3.3.6 EDR3.12 供應產品供應商的信任根源

編　　號	區　　分	內　　容
EDR 3.12	基本要求	嵌入式設備應提供能夠提供和保護產品供應商密鑰和資料的機密性、完整性和真實性，以便在設備製造時用作為一個或多個「信任根源」。
EDR 3.12	說明	為了使元件能夠驗證產品供應商提供的硬體、軟體和資料的真實性和完整性，它必須擁有可靠的資料源來執行驗證過程。這種受信任的資料源被稱為系統的「信任根源」。該可信資料源可以是「已知良好」軟體的一組加密雜湊，或者它可以是用於驗證加密簽名的非對稱加密密鑰對的公鑰部分。此可信資料通常用於在引導元件的韌體或作業系統之前驗證關鍵軟體、韌體和資料，以驗證元件將啟動到「已知良好」狀態，其中已知硬體抽象層安全機制運作和未受到損害。 「信任根源」資料通常通過硬體機制得到保護，防止在元件的正常操作期間對資料進行任何修改。產品供應商信任資料根源的修改通常僅限於產品供應商的供應過程，其中產品供應商具有執行資料供應的可信過程。相反，要通過信任根源驗證的資訊通過硬體或軟體 API 提交給驗證過程，該 API 執行驗證並返回結果而不暴露受保護的資料。

EDR 3.12 RE	增項要求	無
EDR 3.12 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：EDR 3.12 ・SL-C（SI，元件）3：EDR 3.12 ・SL-C（SI，元件）3：EDR 3.12

3.2.3.3.7 EDR3.13 供應產品供應商的信任根源

編　　號	區　　分	內　　容
EDR 3.13	基本要求	嵌入式設備應： a）提供提供和保護資產擁有者密鑰和資料的機密性、完整性和真實性的能力，以用作「信任根源」；和 b）支援提供的能力，而不依賴於可能在設備安全區域之外的元件。
EDR 3.13	說明	產品供應商已建立機制以確保其元件上的軟體和韌體是可信的，並且該軟體和韌體的完整性未受到損害。這允許產品供應商向資產擁有者提供操作的「已知良好」狀態。然而，許多產品供應商還為資產擁有者提供了通過使用行動程式碼、使用者程序或其他此類手段來擴展其設備功能的機制。為了保護元件的安全性，重要的是還要對元件功能的這些擴展進行驗證，以確保它們得到授權並且資產擁有者已經證實了它們的來源。 為了執行這些驗證，元件必須包含提供區分有效和無效來源的方法的資料。有效和無效來源列表將在每個資產擁有者均不同，並且產品供應商不太可能在製造時擁有每個可能的有效來源的完整列表。因此，重要的是，產品供應商為資產擁有者提供了一種安全地提供他們自己的「信任根源」的方法，這種「信任根源」能夠區分資產擁有者的安全政策允許的來源和非資產擁有者的安全政策。必須保護這些「信任根源」的真實性和完整性，以便惡意行為者不能添加額外的信任根源，使其能夠對元件進行操作。 信任根源也可以用作基礎通信安全性，例如 CR 3.1 要求的通信完整性 - CR 4.1 要求的通信完整性或通信機密性 - 資訊機密性。 諸如 EDR 2.4 之類的要求 - 行動程式碼要求元件在執行行動程式碼之前完成對行動程式碼的真實性檢查。此要求提供的信任根源提供了驗證行動程式碼的來源和完整性所必需的資料，允許元件獨立確定是否允許執行程式碼。
EDR 3.13 RE	增項要求	無
EDR 3.13 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：EDR 3.13 ・SL-C（SI，元件）3：EDR 3.13

		• SL-C（SI，元件）4：EDR 3.13

3.2.3.3.8 EDR3.14 啟動程序完整性

編　　號	區　　分	內　　容
EDR 3.14	基本要求	嵌入式設備應在使用前驗證元件啟動和運作時程序所需的韌體、軟體和設定資料的完整性。
EDR 3.14	說明	為了向資產擁有者保證元件的安全功能未受到損害，有必要確保元件的軟體和韌體未被篡改，並且軟體和韌體在元件上執行是有效的。 因此，元件必須執行檢查以在啟動過程中使用之前驗證元件的韌體或軟體的完整性，以確保元件不會啟動到可能損壞元件或提供路徑的不安全或無效操作狀態，使惡意行為者獲得對其他元件、資產或資料的存取權限。
EDR 3.14 RE(1)	增項要求	（1）啟動過程的真實性 嵌入式設備應使用元件的產品供應商信任根源來驗證元件在啟動過程中使用之前所需的韌體、軟體和設定資料的真實性。「
EDR 3.14 SL-C	安全等級	• SL-C（SI，元件）1：EDR 3.14 • SL-C（SI，元件）2：EDR 3.14（1） • SL-C（SI，元件）3：EDR 3.14（1） • SL-C（SI，元件）4：EDR 3.14（1）

3.2.3.4 . 主機型裝置安全要求

本節要求的目的是特定適用於主機型裝置的安全要求。

3.2.3.4.1 HDR 2.4 行動程式碼

編　　號	區　　分	內　　容
HDR 2.4	基本要求	在主機設備利用行動程式碼技術的情況下，該主機設備應提供對行動程式碼技術的使用實施安全政策的能力。安全政策應至少允許對主機設備上使用的每種行動程式碼技術採取以下行動： a）控制行動程式碼的執行; b）控制允許哪些使用者（人、軟體程序或設備）將行動程式碼上載到主機設備; 和 c）基於對行動程式碼的完整性檢查以及在執行程式碼之前控制程式碼執行。
HDR 2.4	說明	行動程式碼技術包括但不限於 Java、JavaScript，ActiveX、PDF、Postscript、Shockwave 電影、Flash 動畫和 VBScript。使用限制適用於選擇和使用安裝在伺服器上的行動程式碼以及在各個工作站上下載和執行的行動程式碼。 控制程序應防止在主機設備所在的控制系統內開發、獲取或引入不可接受的行動程式碼。 例如，行動程式碼不允許可以直接與控制系統交換，但可以在由 IACS 人員維護的受控相鄰環境中被允許。 行動程式碼可以通過向程式碼本身（應用層）添加完整性、真實性和授權檢查來保護，或者通過提供這些屬性的安全通信通道傳輸行動程式碼來達成「即時」程式碼執行或任何等同於這些選項的機制。
HDR 2.4 RE(1)	增項要求	（1）行動程式碼真實性檢查 主機設備應提供強制執行安全政策的能力，該政策允許設備根據執行程式碼之前的真實性檢查結果來控制行動程式碼的執行。「…
HDR 2.4 SL-C	安全等級	• SL-C（UC，元件）1：HDR 2.4 • SL-C（UC，元件）2：HDR 2.4（1） • SL-C（UC，元件）3：HDR 2.4（1） • SL-C（UC，元件）4：HDR 2.4（1）

3.2.3.4.2 HDR 2.13 實體診斷和測試介面的使用

編　　號	區　　分	內　　容
HDR 2.13	基本要求	主機設備應防止未經授權使用實體工廠診斷和測試介面（例如 JTAG 除錯）。
HDR 2.13	說明	在主機設備內的各個位置設置工廠診斷和測試介面，以幫助元件的開發人員和工廠人員執行測試功能，以發現錯誤以隨後將其從元件中移除。但是，必須小心保護這些相同的介面，以防止未經授權的實體存取，以保護元件向 IACS 提供的基本功能。 可能存在工廠診斷和測試介面使用與設備的網路通信的情

		況。在這種情況下，這些介面需滿足本文件的所有要求。 如果診斷和測試介面不提供控制主機設備或存取非公共資訊的能力，則它不需要認證機制。這應通過威脅和風險評估來確定。一個例子是 JTAG 除錯介面，其中 JTAG 用於控制處理器並執行任意命令，而 JTAG 邊界掃描使用 JTAG 來簡單地讀取資訊（可能是公開可用的資訊）。
HDR 2.13 RE(1)	增項要求	（1）主動監測 主機設備應提供對設備診斷和測試介面的主動監控，並在檢測到存取這些介面的嘗試存取時產生稽核日誌記錄。
HDR 2.13 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：HDR 2.13 ・SL-C（SI，元件）3：HDR 2.13（1） ・SL-C（SI，元件）3：HDR 2.13（1）

3.2.3.4.3 HDR 3.2 防範惡意程式碼

編　　號	區　　分	內　　容
HDR 3.2	基本要求	IACS 產品供應商必須在主機設備上設置機制，以防止惡意程式碼。IACS 產品供應商應記錄與防止惡意程式碼相關的任何特殊設定要求。
HDR 3.2	說明	主機設備需要支援使用惡意程式碼保護（例如，針對病毒、蠕蟲、特洛伊木馬和間諜軟體）。 產品供應商應該對惡意程式碼機制的保護設定進行限定和記錄，以便維護控制系統的主要任務。
HDR 3.2 RE(1)	增項要求	（1）報告程式碼保護版本 主機設備應自動報告軟體和文件版本的保護，使其免受惡意程式碼的使用（作為整體日誌記錄功能的一部分）。
HDR 3.2 SL-C	安全等級	・SL-C（SI，元件）1：HDR 3.2 ・SL-C（SI，元件）2：HDR 3.2（1） ・SL-C（SI，元件）3：HDR 3.2（1） ・SL-C（SI，元件）4：HDR 3.2（1）

3.2.3.4.4 HDR 3.10 更新支援

編　　號	區　　分	內　　容
HDR 3.10	基本要求	主機設備應支援更新和升級的能力
HDR 3.10	說明	主機設備在其安裝的生命週期內可能需要安裝更新和升級。 在某些情況下，主機設備也支援或執行基本功能。 在這種情況下，主機設備應具有支援修補和更新的機制，而不會影響高可用性系統的基本功能。 提供此功能的一個舉例是支援主機設備內的冗餘。
HDR 3.10 RE(1)	增項要求	（1）更新真實性和完整性 主機設備應在安裝之前驗證任何軟體更新或升級的真實性和完整性。
HDR 3.10 SL-C	安全等級	• SL-C（SI，元件）1：HDR 3.10 • SL-C（SI，元件）2：HDR 3.10（1） • SL-C（SI，元件）3：HDR 3.10（1） • SL-C（SI，元件）4：HDR 3.10（1）

3.2.3.4.5 HDR 3.11 防範與偵測實體篡改

編　　號	區　　分	內　　容
HDR 3.11	基本要求	主機設備應提供支援防篡改和檢測機制的能力，以防止未經授權的實體存取設備。
HDR 3.11	說明	為了使元件能夠驗證產品供應商提供的硬體、軟體和資料的真實性和完整性，它必須擁有可靠的資料源來執行驗證過程。這種受信任的資料源被稱為系統的「信任根源」。該可信資料源可以是「已知良好」軟體的一組加密雜湊，或者它可以是用於驗證加密簽名的非對稱加密密鑰對的公開金鑰。此可信資料通常用於在啟動元件的韌體或作業系統之前驗證關鍵軟體、韌體和資料，以驗證元件將啟動到已知良好狀態，其中所有安全機制都已知運作和不妥協。 「信任根源」資料可以由軟體或硬體達成的機制保護，以防止在元件的正常操作期間對資料進行任何修改。產品供應商信任資料根源的修改通常僅限於產品供應商的供應過程，其中產品供應商具有執行資料供應的可信過程。相反，要通過信任根源驗證的資訊通過硬體或軟體 API 提交給驗證過程，該 API 執行驗證並返回結果而不暴露受保護的資料。
HDR 3.11 RE(1)	增項要求	（1）通知篡改企圖 主機設備應能夠在發現未經授權的實體存取嘗試時自動向可設定的一組接收者提供通知。 所有篡改通知都應記錄為整個稽核

		日誌記錄功能的一部分
HDR 3.11 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：HDR 3.11 ・SL-C（SI，元件）3：HDR 3.11（1） ・SL-C（SI，元件）4：HDR 3.11（1）

3.2.3.4.6 HDR 3.12 供應產品供應商的信任根源

編　　號	區　　分	內　　容
HDR 3.12	基本要求	主機設備應提供提供和保護產品供應商密鑰和資料的機密性、完整性和真實性的能力，以便在設備製造時用作一個或多個「信任根源」。
HDR 3.12	說明	為了使元件能夠驗證產品供應商提供的硬體、軟體和資料的真實性和完整性，它必須擁有可靠的資料源來執行驗證過程。這種受信任的資料源被稱為系統的「信任根源」。該可信資料源可以是「已知良好」軟體的一組加密雜湊，或者它可以是用於驗證加密簽名的非對稱加密密鑰對的公開金鑰。此可信資料通常用於在引導元件的韌體或作業系統之前驗證關鍵軟體、韌體和資料，以驗證元件將啟動到已知良好狀態，其中所有安全機制都已知運作和未受侵害。 「信任根源」資料可以由軟體或硬體達成的機制保護，以防止在元件的正常操作期間對資料進行任何修改。產品供應商信任資料根源的修改通常僅限於產品供應商的供應過程，其中產品供應商具有執行資料供應的可信過程。相反，要通過信任根源驗證的資訊通過硬體或軟體 API 提交給驗證過程，該 API 執行驗證並返回結果而不暴露受保護的資料。
HDR 3.12 RE	增項要求	無
HDR 3.12 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：HDR 3.12 ・SL-C（SI，元件）3：HDR 3.12 ・SL-C（SI，元件）4：HDR 3.12

3.2.3.4.7 HDR 3.13 供應資產擁有者的信任根源

編　　號	區　　分	內　　容
HDR 3.13	基本要求	主機設備應： a）提供提供和保護資產擁有者密鑰和資料的機密性、完整性和真實性的能力，以用作「信任根源」；和 b）支援提供的能力，而不依賴於可能在設備安全區域之外的元件。
HDR 3.13	說明	產品供應商已建立機制以確保其元件上的軟體和韌體是可信的，並且該軟體和韌體的完整性未受到損害。這允許產品供應商向資產擁有者提供操作的「已知良好」狀態。然而，許多產品供應商還為資產擁有者提供了通過使用行動程式碼、使用者程序或其他此類手段來擴展其設備功能的機制。為了保護元件的安全性，重要的是還要對元件功能的這些擴展進行驗證，以確保它們得到授權並且資產擁有者已經證實了它們的來源。 為了執行這些驗證，元件必須包含提供區分有效和無效來源的方法的資料。有效和無效來源列表在各資產擁有者間不同，並且產品供應商不太可能在製造時擁有每個可能的有效來源的完整列表。因此，重要的是，產品供應商為資產擁有者提供了一種安全地提供他們自己的「信任根源」的方法，這種「信任根源」能夠區分資產擁有者的安全政策允許的來源和非資產擁有者的安全政策。必須保護這些「信任根源」的真實性和完整性，以便惡意行為者不能添加額外的信任根源，使其能夠對元件進行操作。 諸如 HDR 2.4 之類的要求 - 行動程式碼要求元件在執行行動程式碼之前完成對行動程式碼的真實性檢查。此要求提供的信任根源提供了驗證行動程式碼的來源和完整性所必需的資料，允許元件獨立確定是否允許執行程式碼。 信任根源也可以用作基礎通信安全性，例如 CR 3.1 要求的通信完整性 - CR 4.1 要求的通信完整性或通信機密性 - 資訊機密性。
HDR 3.13 RE	增項要求	無
HDR 3.13 SL-C	安全等級	• SL-C（SI，元件）1：未選用 • SL-C（SI，元件）2：HDR 3.13 • SL-C（SI，元件）3：HDR 3.13 • SL-C（SI，元件）4：HDR 3.13

3.2.3.4.8 HDR 3.14 啟動程序完整性

編　　號	區　　分	內　　容
HDR 3.14	基本要求	主機設備應在啟動程序中使用之前驗證元件啟動程序所需的韌體、軟體和設定資料的完整性。
HDR 3.14	說明	為了向資產擁有者保證元件的安全功能未受到損害，有必要確保元件的軟體和韌體未被篡改，並且軟體和韌體在元件上執行是有效的。 因此，元件必須執行檢查以在啟動過程之前驗證元件的韌體或軟體的完整性和真實性，以確保元件不會啟動到可能損壞元件或提供元件的不安全或無效操作狀態。 惡意行為者存取其他元件，資產或資料的路徑。
HDR 3.14 RE(1)	增項要求	（1）啟動過程的真實性 主機設備應使用元件的產品供應商信任根源來驗證元件在啟動過程中使用之前所需的韌體、軟體和設定資料的真實性。
HDR 3.14 SL-C	安全等級	・SL-C（SI，元件）1：HDR 3.14 ・SL-C（SI，元件）2：HDR 3.14（1） ・SL-C（SI，元件）3：HDR 3.14（1） ・SL-C（SI，元件）4：HDR 3.14（1）

3.2.3.5　網路設備安全要求

本節要求的目的是列舉特定適用於網路設備的要求。

3.2.3.5.1 NDR 1.6 無線存取管理

編　　號	區　　分	內　　容
NDR 1.6	基本要求	支援無線存取管理的網路設備應提供識別和認證從事無線通信的所有使用者（人、軟體程序或設備）的能力。
NDR 1.6	說明	任何無線技術都可以，並且在大多數情況下應該被視為另一種通信協議選項。 因此，它應該受到與 IACS 使用的任何其他通信類型相同的 IACS 安全要求。 然而，從安全的角度來看，有線和無線通信之間至少存在一個顯著差異。 使用無線時，實體安全對策通常效果較差。
NDR 1.6 RE(1)	增項要求	（1）唯一的識別和認證 網路設備應提供唯一地識別和認證參與無線通信的所有使用者（人、軟體程序或設備）的能力
NDR 1.6 SL-C	安全等級	・SL-C（UC，元件）1：NDR 1.6 ・SL-C（UC，元件）2：NDR 1.6（1） ・SL-C（UC，元件）3：NDR 1.6（1） ・SL-C（UC，元件）4：NDR 1.6（1）

3.2.3.5.2 NDR 1.13 通過不受信任的網路存取

編　　號	區　　分	內　　容
NDR 1.13	基本要求	支援設備存取網路的網路設備應提供監視和控制通過不可信網路存取網路設備的所有方法的能力
NDR 1.13	目的	網路設備應防止未經授權的連接或顛覆授權連接。 通過不可信網路存取網路設備的舉例通常包括遠端存取方法（例如撥號、寬頻和無線）以及來自公司辦公室（非控制系統）網路的連接。 網路設備可以提供 ACL（存取控制列表）功能以通過以下方式限制存取： 以太網交換機等第 2 層轉發設備： a）MAC 地址 b）VLAN 第 3 層轉發設備，如路由器、網路閘道器和防火牆： a）IP 地址 b）連接埠和協議 c）虛擬專用網
NDR 1.13 RE(1)	增項要求	（1）顯式存取請求批准 除非被指定角色明確批准，否則網路設備應提供拒絕通過不受信任網路存取請求的功能。
NDR 1.13 SL-C	安全等級	・SL-C（UC，元件）1：NDR 1.13 ・SL-C（UC，元件）2：NDR 1.13 ・SL-C（UC，元件）3：NDR 1.13（1） ・SL-C（UC，元件）4：NDR 1.13（1）

3.2.3.5.3 NDR 2.4 行動程式碼

編　　號	區　　分	內　　容
NDR 2.4	基本要求	在網路設備利用行動程式碼技術的情況下，網路設備應提供實施用於行動程式碼技術的安全政策的能力。 對於網路設備上使用的每種行動程式碼技術，安全政策應至少允許以下操作： a）控制行動程式碼的執行; b）控制允許哪些使用者（人、軟體程序或設備）向/從網路設備傳輸行動程式碼; 和 c）基於對行動程式碼的完整性檢查以及在執行程式碼之前控制程式碼執行
NDR 2.4	說明	行動程式碼技術包括但不限於 Java、JavaScript、ActiveX、PDF、Postscript、Shockwave 電影、Flash 動畫和 VBScript。使用限制適用於選擇和使用安裝在伺服器上的行動程式碼以及在各個工作站上下載和執行的行動程式碼。 控制程序應防止在元件所在的控制系統內開發、獲取或引入不可接受的行動程式碼。 例如，行動程式碼交換可以直接在控制系統內降低，但可

		以在由 IACS 人員維護的受控相鄰環境中允許。 行動程式碼可以通過向程式碼本身（應用層）添加完整性，真實性和授權檢查來保護，或者通過通過提供這些屬性的安全通信通道傳輸行動程式碼來達成「即時」程式碼執行，或者 任何等同於這些選項的機制。
NDR 2.4 RE(1)	增項要求	（1）行動程式碼真實性檢查 網路設備應提供執行安全政策的能力，該政策允許設備基於在執行程式碼之前的真實性檢查的結果來控制行動程式碼的執行。
NDR 2.4 SL-C	安全等級	・SL-C（UC，元件）1：NDR 2.4 ・SL-C（UC，元件）2：NDR 2.4（1） ・SL-C（UC，元件）3：NDR 2.4（1） ・SL-C（UC，元件）4：NDR 2.4（1）

3.2.3.5.4 NDR 2.13 使用實體診斷和測試介面

編　　號	區　　分	內　　容
NDR 2.13	基本要求	網路設備應防止未經授權使用實體工廠診斷和測試介面（例如 JTAG 除錯）。
NDR 2.13	說明	在元件內的各個位置設置工廠診斷和測試介面，以幫助元件的開發人員和工廠人員測試功能達成，以及何時發現錯誤以便隨後將其從元件中移除。但是，必須小心保護這些相同的介面，以防止未經授權的實體存取，以保護元件向 IACS 提供的基本功能。 可能存在工廠診斷和測試介面使用與設備的網路通信的情況。在這種情況下，這些介面需滿足本文件的所有要求。 請注意，如果診斷和測試界面不提供控制產品或存取非公共資訊的能力，則不需要身份驗證機制。這應該通過威脅評估來確定。一個例子是 JTAG 除錯，其中 JTAG 用於控制處理器並執行任意命令，而 JTAG 邊界掃描使用 JTAG 來簡單地讀取資訊（可能是公開可用的資訊）。
NDR 2.13 RE(1)	增項要求	（1）主動監測 網路設備應提供對設備的診斷和測試介面的主動監視，並在檢測到存取這些介面的嘗試時產生稽核日誌記錄。
NDR 2.13 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：NDR 2.13 ・SL-C（SI，元件）3：NDR 2.13（1） ・SL-C（SI，元件）3：NDR 2.13（1）

3.2.3.5.5 NDR 3.2 防範惡意程式碼

編　　號	區　　分	內　　容

NDR 3.2	基本要求	網路設備應提供對惡意程式碼的保護
NDR 3.2	說明	如果網路設備能夠利用補償控制，則不需要直接支援惡意程式碼保護。 一種這樣的可能的補償控制將是使用網路分組過濾設備來識別和移除傳輸中的惡意程式碼。 假設 IACS 將負責提供所需的保護措施。 但是，對於具有本地 USB 主機存取權限的方案，應評估是否需要保護免受惡意程式碼的攻擊。
NDR 3.2 RE	增項要求	無
NDR 3.2 SL-C	安全等級	• SL-C（SI，元件）1：NDR 3.2 • SL-C（SI，元件）2：NDR 3.2 • SL-C（SI，元件）3：NDR 3.2 • SL-C（SI，元件）4：NDR 3.2

3.2.3.5.6 NDR 3.10 更新支援

編　　號	區　　分	內　　容
NDR 3.10	基本要求	網路設備應支援更新和升級的能力。
NDR 3.10	說明	安裝生命週期內的網路設備可能需要安裝更新和升級。 在某些情況下，網路設備也會支援或執行基本功能。 在這種情況下，網路設備應具有支援修補和更新的機制，而不會影響高可用性系統的基本功能。 提供此功能的一個舉例是支援網路設備內的冗餘。
NDR 3.10 RE(1)	增項要求	（1）更新真實性和完整性 網路設備應在安裝之前驗證任何軟體更新或升級的真實性和完整性。
NDR 3.10 SL-C	安全等級	• SL-C（SI，元件）1：NDR 3.10 • SL-C（SI，元件）2：NDR 3.10（1） • SL-C（SI，元件）3：NDR 3.10（1） • SL-C（SI，元件）4：NDR 3.10（1）

3.2.3.5.7 NDR 3.11 防範與偵測實體篡改

編　　號	區　　分	內　　容
NDR 3.11	基本要求	網路設備應提供防篡改和檢測機制，以防止未經授權的實體存取設備
NDR 3.11	說明	防篡改機制的目的是防止攻擊者企圖對 IACS 設備執行未經授權的實體操作。 如果發生篡改事件，則預防、檢測和回應是次要的。 防篡改機制最有效地組合使用以防止存取任何關鍵元件。 防篡改包括使用專門的材料來難以篡改設備或模組。 這可以包括硬化外殼、鎖、封裝或安全螺釘等功能。 放置緊密的氣流路徑會增加探測產品內部的難度。 篡改證據的目的是確保在發生篡改事件時仍然存在可見或電子證據。 許多簡單的證據技術由密封件和膠帶組成，以明顯存在實體篡改。 更複雜的技術包括開關。
NDR 3.11 RE(1)	增項要求	（1）通知篡改企圖 網路設備應能夠在發現未經授權的實體存取嘗試時自動向可設定的一組接收者提供通知。 所有篡改通知都應記錄為整個稽核日誌記錄功能的一部分。
NDR 3.11 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：NDR 3.11 ・SL-C（SI，元件）3：NDR 3.11（1） ・SL-C（SI，元件）4：NDR 3.11（1）

3.2.3.5.8 NDR 3.12 供應產品供應商的信任根源

編　　號	區　　分	內　　容
NDR 3.12	基本要求	網路設備應提供提供和保護產品供應商密鑰和資料的機密性、完整性和真實性的能力，以便在設備製造時用作一個或多個「信任根源」。
NDR 3.12	說明	為了使元件能夠驗證產品供應商提供的硬體、軟體和資料的真實性和完整性，它必須擁有可靠的資料源來執行驗證過程。這種受信任的資料源被稱為系統的「信任根源」。該可信資料源可以是「已知良好」軟體的一組加密雜湊，或者它可以是用於驗證加密簽名的非對稱加密密鑰對的公開金鑰。此可信資料通常用於在引導元件的韌體或作業系統之前驗證關鍵軟體、韌體和資料，以驗證元件將啟動到已知良好狀態，其中所有安全機制都已知運作和未受侵害。 「信任根源」資料通常由軟體或硬體達成的機制保護，以防止在元件的正常操作期間對資料進行任何修改。產品供應商信任資料根源的修改通常僅限於產品供應商的供應過程，其中產品供應商具有執行資料供應的可信過程。相反，要對其進行驗證的資訊

		信任根源通過硬體或軟體 API 提交給驗證過程，該 API 執行驗證並返回結果而不暴露受保護的資料。
NDR 3.12 RE	增項要求	無
NDR 3.12 SL-C	安全等級	・SL-C（SI，元件）1：未選用 ・SL-C（SI，元件）2：NDR 3.12 ・SL-C（SI，元件）3：NDR 3.12 ・SL-C（SI，元件）3：NDR 3.12

3.2.3.5.9 NDR 3.13 供應資產擁有者信任的根源

編　　號	區　　分	內　　容
NDR 3.13	基本要求	網路設備應 a）提供提供和保護資產擁有者密鑰和資料的機密性、完整性和真實性的能力，以用作「信任根源」；和 b）支援提供的能力，而不依賴於可能在設備安全區域之外的元件。
NDR 3.13	說明	產品供應商已建立機制以確保其元件上的軟體和韌體是可信的，並且該軟體和韌體的完整性未受到損害。這允許產品供應商向資產擁有者提供操作的「已知良好」狀態。然而，許多產品供應商還為資產擁有者提供了通過使用行動程式碼、使用者程序或其他此類手段來擴展其設備功能的機制。為了保護元件的安全性，重要的是還要對元件功能的這些擴展進行驗證，以確保它們得到授權並且資產擁有者已經證實了它們的來源。 為了執行這些驗證，元件必須包含提供區分有效和無效來源的方法的資料。有效和無效來源列表在各資產擁有者到間不同，並且產品供應商不太可能在製造時擁有每個可能的有效來源的完整列表。因此，重要的是，產品供應商為資產擁有者提供了一種安全地提供他們自己的「信任根源」的方法，這種「信任根源」能夠區分資產擁有者的安全政策允許的來源和非資產擁有者的安全政策。必須保護這些「信任根源」的真實性和完整性 惡意行為者無法添加額外的信任根源，使其能夠對元件進行操作。 諸如 NDR 2.4 之類的要求 - 行動程式碼要求元件在執行行動程式碼之前完成對行動程式碼的真實性檢查。此要求提供的信任根源提供了驗證行動程式碼的來源和完整性所必需的資料，允許元件獨立確定是否允許執行程式碼。 信任根源用於提供通信安全性，例如 CR 3.1 要求的通信完整性 - CR 4.1 要求的通信完整性或通信機密性 - 資訊機密性。
NDR 3.13 RE	增項要求	無

NDR 3.13 SL-C	安全等級	• SL-C（SI，元件）1：未選用 • SL-C（SI，元件）2：NDR 3.13 • SL-C（SI，元件）3：NDR 3.13 • SL-C（SI，元件）4：NDR 3.13

3.2.3.5.10 NDR 3.14 啟動過程的完整性

編　　號	區　　分	內　　容
NDR 3.14	基本要求	網路設備應在啟動過程中使用之前驗證元件啟動過程所需的韌體、軟體和設定資料的完整性。
NDR 3.14	說明	為了向資產擁有者保證元件的安全功能未受到損害，有必要確保元件的軟體和韌體未被篡改，並且軟體和韌體在元件上執行是有效的。 因此，元件必須執行檢查以在啟動過程之前驗證元件的韌體或軟體的完整性和真實性，以確保元件不會引導到可能損壞元件或提供路徑的不安全或無效操作狀態 使惡意行為者獲得對其他元件，資產或資料的存取權限。
NDR 3.14 RE(1)	增項要求	（1）啟動過程的真實性 網路設備應使用元件的產品供應商信任根源來驗證元件在啟動過程中使用之前所需的韌體、軟體和設定資料的真實性。
NDR 3.14 SL-C	安全等級	• SL-C（SI，元件）1：NDR 3.14 • SL-C（SI，元件）2：NDR 3.14（1） • SL-C（SI，元件）3：NDR 3.14（1） • SL-C（SI，元件）4：NDR 3.14（1）

3.2.3.5.11 NDR 5.2 區域邊界保護

編　　號	區　　分	內　　容
NDR 5.2	基本要求	區域邊界處的網路設備應提供監視和控制區域邊界通信的能力，以強制執行基於風險的區域和管道模型中定義的劃分。
NDR 5.2	說明	每個安全區域外部的任何連接都應通過受管理介面進行，這些介面由安裝在有效架構中的適當邊界保護設備（例如，代理、網路閘道器、路由器、防火牆、單向網路閘道器，防護和加密通道）組成（例如，防火牆保護應用程式） 駐留在 DMZ 的網路閘道器）。 任何指定的備用處理站點的控制系統邊界保護應提供與主站點相同的保護等級。
NDR 5.2 RE(1)	增項要求	（1）拒絕所有，允許例外 網路元件應提供預設拒絕網路流量的功能，並允許異常的網路流量（也稱為拒絕所有，允許例外）。
NDR 5.2 RE(2)	增項要求	（2）島嶼模式 網路元件應提供防止通過控制系統邊界（也稱為孤島模式）進行任何通信的能力。 注意可以使用此功能的舉例包括在控制系統中檢測到安全違規或違規，或者在企業等級發生攻擊的情況。
NDR 5.2 RE(3)	增項要求	（3）關閉失敗 當邊界保護機制發生操作故障（也稱為故障關閉）時，網路元件應提供防止通過控制系統邊界進行任何通信的能力。 注意可以使用此功能的舉例包括硬體故障或電源故障導致邊界保護設備在降級模式下運作或完全失敗的情況。
NDR 5.2 SL-C	安全等級	・SL-C（SI，元件）1：NDR 5.2 ・SL-C（SI，元件）2：NDR 5.2（1） ・SL-C（SI，元件）3：NDR 5.2（1）（2）（3） ・SL-C（SI，元件）4：NDR 5.2（1）（2）（3）

3.2.3.5.12 NDR 5.3 限制一般用途人對人通信

編　　號	區　　分	內　　容
NDR 5.3	基本要求	區域邊界處的網路設備應提供防止來自控制系統外部的使用者或系統的一般、人對人訊息的能力。
NDR 5.3	說明	一般的個人對個人通信系統包括但不限於：電子郵件系統，社交媒體形式（Twitter、Facebook、圖片庫等）或允許傳輸任何類型的可執行文件的任何訊息系統。這些系統通常用於與控制系統操作無關的私人用途，因此這些系統所施加的風險通常超過任何可察覺的益處。 這些類型的一般通信系統通常用作將惡意軟體引入控制系統的攻擊媒介，將存在讀取授權的資訊傳遞到控制系統外部的位置，並引入可用於產生安全問題或啟動的過多網路負載攻擊控制系統。 網路設備可以達成這樣的限制，例如，通過基於連接埠號和

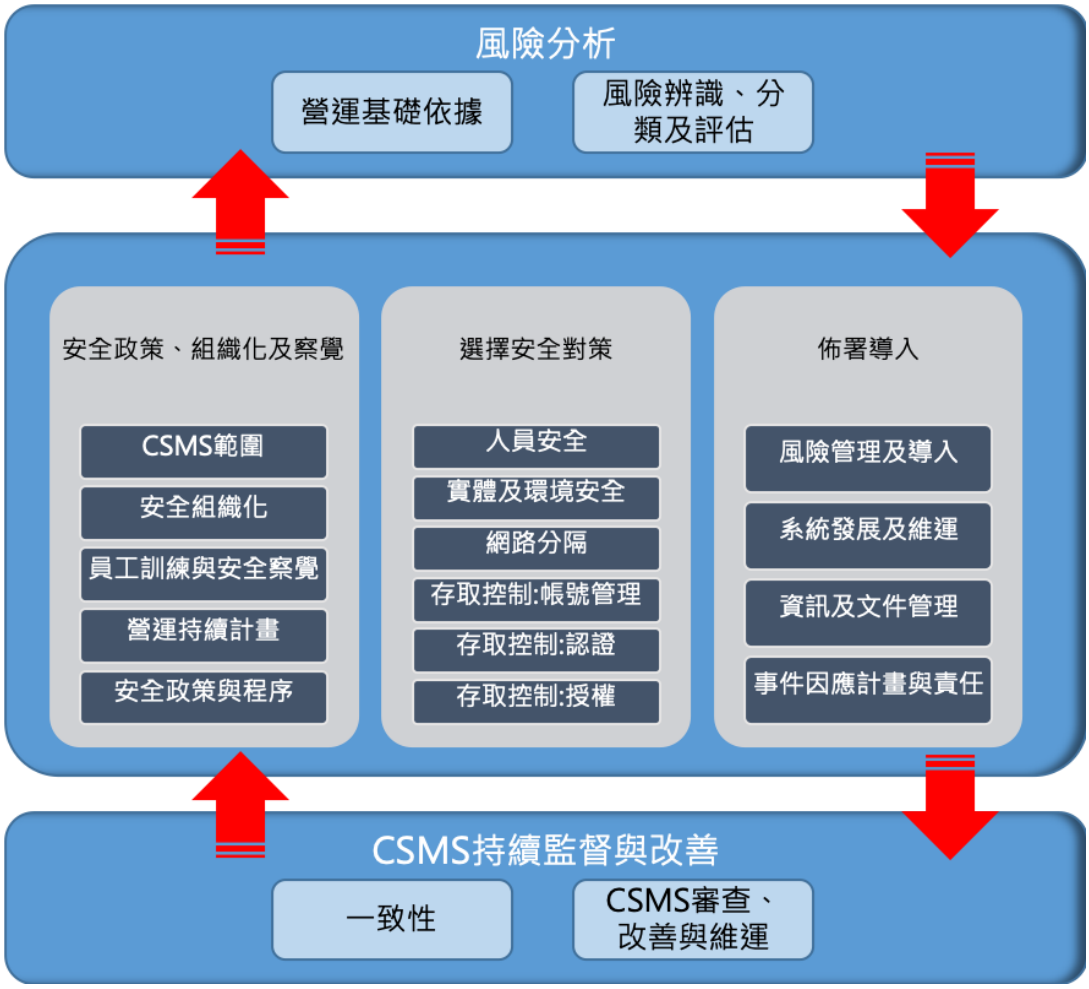
		源或目標地址阻止特定通信以及應用層防火牆進行更深入的檢查
NDR 5.3 RE	增項要求	無
NDR 5.3 SL-C	安全等級	・SL-C（SI，元件）1：NDR 5.3 ・SL-C（SI，元件）2：NDR 5.3 ・SL-C（SI，元件）3：NDR 5.3 ・SL-C（SI，元件）4：NDR 5.3

第 4 章 工控物聯網資安計畫（Security Program）

組織於制訂資安計畫時除應與現有的 IT 安全經驗、計畫和實作保持一致並整合外， 更必須考慮 IACS 技術和環境的具體要求和特點。組織更應定期檢

視和更新其工控物聯網資安計畫， 以反映技術、操作、標準和法規的變化，以及特定設施的安全需求。 一個完整的工控物聯網資安計畫應至少涵蓋以下三個層面：

- 風險分析
- 風險的應對
- 持續監控和改進



本章即依據上述三大重點說明工控物聯網資安計畫之發展和部署。

4.1 風險分析

建構工控物聯網資安計畫的第一個主要工作是風險分析。執行風險分析時需考量 CSMS 中的許多背景資訊。下圖顯示了此類別中的兩個元素：

- 業務目標

組織應確定和記錄其需求， 以應對在工控網路環境中導入、應用 IIoT 之網路風險，這些風險是基於如果發生 IACS 資安事件，可能對組織財務、人員安全、環境和其他潛在後果的性質和規模，建立業務目標對於組織確保管理層的支援，並維持在對 IACS 資安計畫的適當投資水準是是非常重要的。

- 風險識別、分類和評估

組織應識別業務運作上面臨的 IACS 網路風險， 並評估這些風險的可能性和嚴重性，透過使用公認的方法系統地識別、優先排序和分析潛在的安全威脅、漏洞和後果， 保護其執行任務的能力。其中包括脆弱性評估、高階風險評鑑與細部風險評鑑，以理解並降低風險。

4.1.1 高階風險評鑑與細部風險評鑑

高階風險評鑑是一個初步辨識風險並判別其優先次序的歷程，應由資訊安全團隊執行並適度邀集內部與外部的利害相關者參與確定和評估風險優先順序的過程；記錄風險辨識的結果和判斷優先程度的原因至為重要， 因為此階段的工作成果將會是細部風險評鑑的指導綱領和重要輸入來源。

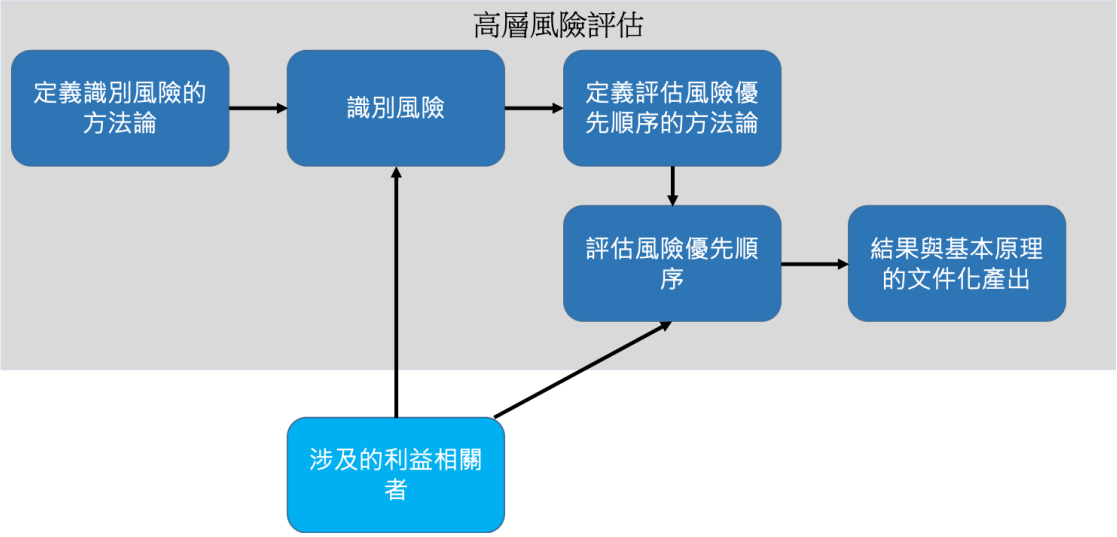
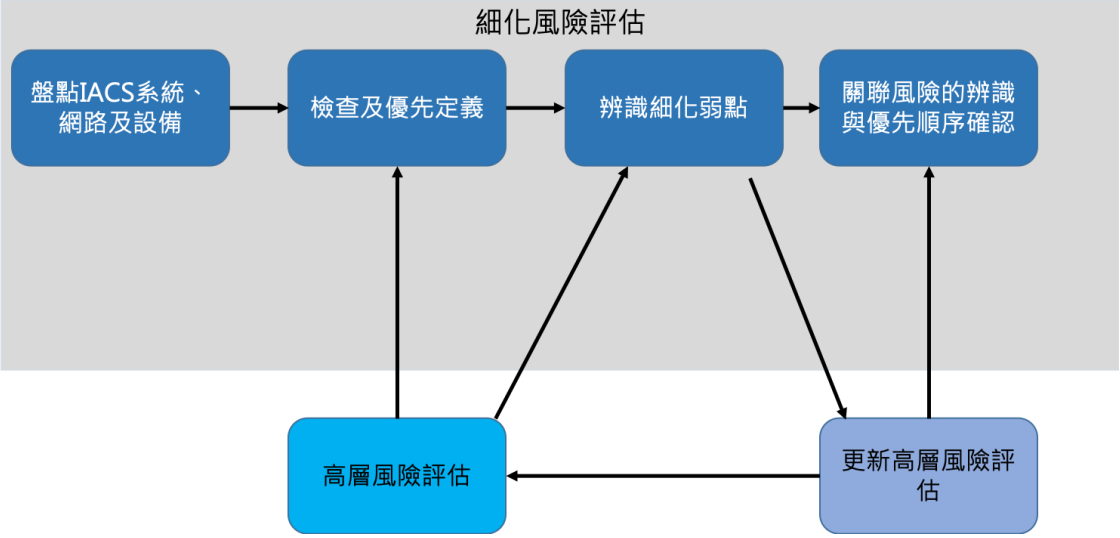


圖 35

高階風險評鑑的進行，通常會由組織預先定義辨識風險來源的方法，需特別注意的是，在本階段暫時先不會透過完整考量資產價值、威脅、脆弱性與後果等因素，進行系統化的「細部風險評鑑」，而是透過較直觀的方式，例如透過預先定義的資訊系統分類分級鑑別機制，針對工控環境中之資訊系統與資訊資產，找出每個資訊系統、資訊資產在該組織的營運業務價值，以及若發生 IACS 資安事件可能對關鍵任務帶來的衝擊，而在高階風險評鑑中被識別為「重要」或對組織業務目標可能帶來高風險、高衝擊影響的資訊系統、資產，組織可運用 「詳細風險評鑑作法」對其進行下一個風險評鑑循環，屬於「較不重要」或者較低風險/較低衝擊影響的資訊系統、資產，組織則可自行根據其安全要求與風險評鑑目標自行選擇適用的風險評鑑方法或者風險處理方式。

而「細部風險評鑑」活動首先對區域（Zone）及管道（Conduit）及其中的 IACS 系統、網路和設備進行盤點， 從而為風險評估提供了更詳細的資訊，接著透過完整考量資產價值、威脅、脆弱性與後果等因素來評定特定的 IACS 系統、網路和設備其曝險程度。其他因素， 如 IACS 環境所在地點的基礎設

施、人力支援完整性或曾發生的問題記錄， 也將有助於確定詳細風險評估。詳細脆弱性的確定以高等級風險評估中的脆弱性類型為指導， 但不限於這些類型。因此， 詳細的脆弱性評估不僅可能發現新類型的弱點， 還可能發現高等級風險評估期間未發現的潛在新威脅和相關後果--換言之， 新風險。在這種情況下， 應更新高等級評估， 以納入這些內容。發現的所有弱點都與特定風險（即威脅、可能性和後果）相關聯， 並以與高階風險評鑑期間使用的方法相一致的方式確定優先順序。



而工控環境由於本身之特殊性質，當事故發生在 IACS 網路中，其影響可能同時遍及資訊系統層面以及實體層面，故當組織對其進行風險評鑑時， 必須要特別關注在對傳統 IT 系統進行風險評鑑時， 較少列入考量之因素。

4.1.2 對實體影響層面及人身安全層面之側重

資訊安全風險評鑑主要的目的在於評估資訊資產可能的曝險程度，主要關心的客體是資訊本身，然而在 IACS 環境中，由於人員、設備、場域環境緊密交互影響，故除了對資訊面可能的曝險程度進行考量之外，更需要將實體資產、人身安全以及環境層面的曝險納入考量。 各組織在進行風險評估時，必須考慮安全風險管理的所有方面（例如風險框架、風險容忍度）以及安全評估結果。負責資訊安全風險評估的人員必須能夠識別和傳達已查明的可能對安全有影響的風險，而進行風險評鑑時，需特別專注實體層面的損害，至少應包括（但不限於）：

- 基於現有整體場域的人員、設備、流程及所處理的資訊，如何在這些條件的基礎上發生實體安全事件
- 事件如何操弄感測裝置和執行裝置的操作以影響實體環境
- 有哪些冗餘控制可防止事故對實體層面之影響

實體影響可能通過多種手段對周圍世界產生負面影響， 包括釋放危險材料（如污染、原油）、破壞性動能（如爆炸）以及接觸能源（如電力、電力、蒸汽）。實體事件可能會對 IACS 和支援基礎設施、IACS 執行的各種流程或較大的實體環境產生負面影響。對潛在實體影響的評估應包括 IACS 的所有部分， 首先是評估對感應器和執行器組的潛在影響，並評估網路事件對實體環境、人類安全、自然環境和其他關鍵基礎設施的潛在損害。應根據 IACS

故障是否可能造成傷害、疾病或死亡來評估人的安全影響。這應包括本組織以前對雇員和公眾進行的任何安全影響評估。還可能需要解決環境影響問題。這一分析應納入本組織為確定事件如何在短期或長期影響自然資源和野生生物而進行的任何現有環境影響評估。

4.1.3 對非數位元件的側重

執行風險評鑑時，若僅關注整個生產環境系統的數位層面，就無法充分確定對 IACS 的影響， 因為往往有非數位機制提供容錯能力， 防止 IACS 在可接受的參數之外進行作動。因此， 這些機制的規劃品質可能有助於減少數位事件對 IACS 產生的任何負面影響， 而且必須納入風險評鑑考量。例如， IACS 通常有非數位控制機制， 可以防止 IACS 在安全邊界之外運作， 從而限制攻擊的影響（例如機械安全閥）。此外， 類比機制（如儀錶、警報）可用於觀察實體系統狀態， 以便在數位讀數不可用或損壞時為操作員提供可靠的資料。

4.2 風險的應對

4.2.1 組織與權責的定義-資訊安全團隊之組建

資訊安全團隊至少應由組織的一名資訊技術工作人員、一名控制工程師、一名控制系統操作員、安全主題專家和一名企業風險管理人員組成，必要時甚至可以包含資安顧問、資服 SI 及工控 SI；資訊技術工作人員通常具有多年的安全經驗， 其中部分適用于 IACS，但由於控制工程和 IT 的文化往往有很大的不同， 資訊技術工作人員與其他內外部人士的整合對於開發協作安全設計和操作是非常重要。這個跨職能的資訊安全團隊必須分享其各種領域知識和經驗， 以評估和減輕 IACS 中的風險。安全知識和技能應包括網路架構和設計、安全流程和做法以及安全基礎設施設計和營運。資訊安全小組應直接向業向業務流程管理人（如產線主管）以及企業安全管理人（例如公司的 CIO/CISO）。最終的權力和責任在於企業高階治理團隊，此團隊應足以對組織提供了全面的風險管理方法，接受一定程度的剩餘風險和並承擔對 IACS 資訊安全的責任。管理層的可歸責制（accountability）將有助於確保對資訊安全工作的持續承諾。 雖然控制工程師將在確保 IACS 的安全方面發揮很大作用， 但如果沒有 IT 部門協作和管理階層的支援， 他們將無法達成任務。

4.2.2 工控物聯網全景及界定範圍

企業安全管理人應制定政策， 定義資訊安全團隊的指導章程以及系統擁有者、使命/業務流程經理和使用者的角色、責任。資訊安全管理者應決定並記錄安全計畫的目標、受影響的業務組織、所有涉及的電腦系統和網路、所需的預算和資源以及責任分工；相關計畫還必須包含業務、教育訓練、稽核、法律遵循和監管要求， 以及時程表和責任。

4.2.3 資安處理計畫

完成風險評鑑後，管理階層則需負責開發和傳達組織的風險承受能力，這使得企業安全管理人能夠確定風險必須降低的程度。將殘餘風險降低到可接受

的水準。資安處理計畫的制定應以風險評估為基礎， 該評估將確定本組織的安全優先事項和目標， 以便充分減輕威脅帶來的風險。

4.3 持續監控與改進

組織應確保 CSMS 隨著時間的推移繼續達成其目標，透過檢視、改進和維護 CSMS 建立對 CSMS 的持續監督， 以檢查其是否有效運行， 並隨著時間的推移管理對 CSMS 所需的更改，使得 CSMS 足以應對內部和外部威脅、漏洞和後果的變化， 以及風險承受能力、法律要求和不斷發展的技術和後果的變化。減少風險的非技術辦法。

- 組織應考量利害相關者之要求以及所辨識出之內外部議題，以持續監控、改進並維護資訊安全計畫
- 指定稽核過程與方法：組織應明訂稽核管理程序，以明確稽核進行的方法。
- 定期進行 IACS 稽核， 以驗證 IACS 是否符合 CSMS，並確認安全性原則和程式是否按預期運行以滿足區域的安全目標。
- 組織應定義效能指標和成功標準，建立一致性指標， 以監視與 CSMS 的一致性。每次定期量測的結果應以量化的形式針對這些指標表示， 以顯示安全效能和安全趨勢。
- 組織應說明不符合 CSMS 的含義， 並界定任何相關的改善措施。
- 組織應建構一個資訊安全團隊來管理和協調 CSMS 之實作， 並在進行和達成更改時使用定義的方法。
- 組織應至少每年評估整個 CSMS， 以確保安全目標得到滿足。
- 組織應建立可定量量測的資訊安全目標清單， 這將導致對 CSMS 的相關元素進行檢視， 並可能進行更改。這些觸發因素至少包括: 發生嚴重安全事件、法律和監管變化、風險變化以及 IACS 的重大變化。門檻應以組織的風險承受能力為基礎。
- 組織應確定並實施適當的糾正和預防措施， 以修改 CSMS 以滿足安全目標。
- 當組織、技術、業務目標、內部業務和外來事件發生重大變化時， 應開始檢視組織對風險的容忍度
- 組織應積極徵求員工對安全建議的回饋意見， 並酌情向高級管理層報告績效缺陷和機會。

第 5 章 工控物聯網資安控制措施建置

5.1 資安解決方案設計

承前章，組織基於風險評鑑結果所識別出的風險、重要度並擬定處理計畫，這些處理計畫極有可能指向組織需要建置各種技術控制措施以某種程度消弭風險，以下列示組織可考慮導入/建置的各種控制措施類型，以作為風險因應的解決方案。

- 身份驗證和授權技術
  - 基於角色的授權工具
  - 密碼身份驗證
  - 挑戰性/回應身份驗證
  - 實體/權杖身份驗證
  - 智慧卡身份驗證
  - 生物識別身份驗證
  - 基於位置的身份驗證
  - 密碼分發和管理技術
  - 設備與設備間的身份驗證
- 網路連線篩檢與控制技術
  - 網路防火牆
  - 主機防火牆
  - 虛擬網路
  - 單向式網路安全閘道器
- 加密技術和資料驗證
  - 對稱（秘密）金鑰加密
  - 公開金鑰加密和金鑰分發
  - 虛擬私人網路絡（Vpn）
- 管理、稽核、測量、監控和偵查工具
  - 日誌分析程式
  - 病毒和惡意程式碼檢測系統
  - 入侵偵測系統（IDS）
  - 弱點掃描程式取證和分析工具（FAT）
  - 主機建構管理工具（HCM）
  - 自動化軟體管理工具（ASM）
  - 資產與連線關係盤點工具
  - 操作行為監控分析工具

而組織的資源（人力、物力、財力、時間）始終有限，而可能造成資訊安全事件之威脅無處不在，組織若希望導入最有效率、最符合投資報酬率的解決方案，仍然應依據風險評鑑的結果以及風險處置計畫的擬定，購足以適切解決因應特定風險的資安解決方案，本指引不為特定廠商/解決方案特色進行深入介紹，惟當選購資安解決方案正式成為風險處置行動的一環，以下兩點 IACS 環境的特殊情形必須列入考量：

5.2.1 提高資產可視度是第一要務：

IACS 環境中充滿各式設備製造商獨有的設備型態與通信協定，甚至離數位化/IP 化都尚有一段距離，而組織無法保護組織不知道自己擁有的資產。持續瞭解和瞭解環境的能力應被視為預防、檢測和回應的先決條件。資產識別提供了了解和視覺化您的工業環境所包含的資產的能力。不過， 資產識別不應與資產管理相混淆。資產管理可包括對控制系統進行內部檢查以及對這些資產進行修補程式管理。在評估 IACS 相關資安解決方案時，必須最優先考慮對工控設備的支援性。

工控設備的設計可在不受干預的情況下長時間運作。它們是通常設計為最低限度的實體功率， 計算能力（處理）， 在通常惡劣的環境或遠端位置保持全天候正常執行時間。這固有的 "簡單性" 意味著工業設備的製造並不是為了特別能抵禦廣泛的 系統輸入或精心設計的惡意操作。 工業設備也經常一次部署幾十年， 遠遠超過現代電子設備。這意味著這些 "簡單" 的工業設備將保持不變， 不變， 即使現代技術的進步-特別是在更新或 與更新或升級的好處相比， 升級會產生更多的風險和停機時間。 IACS 安全解決方案必須能夠在能力範圍內運作它所保護的工業設備。例如， PLC 在收到一個未知的信號時可能會停止運作，在這種情況下，利用主動掃描的網路安全解決方案將是有害的影響。它可能被設計為自動重新開機， 而不是停止運作。或者它可能是一個為一組反應而程式設計的 PLC 網路。一個有效的 IACS 安全解決方案。 對這些工控設備的背景和理解也很重要。工 IACS 安全解決方案應該瞭解不同的類型、角色和關係存在於環境中。這不僅意味著解決方案應瞭解什麼角色人機界面發揮， 但它是如何不同于工程工作站， 這些不同的角色如何影響攻擊的潛在後果。最後， 不同的類型的設備具有不同的普及度與曝光率， 工控物聯網安全解決方案應瞭解這些差異， 並將重點放在與各種類型的設備最相關的攻擊。

5.2.2 理解設備間的操作與通信現況，並基於業務/生產任務所需的基線加以建立常模，並進一步辨識異常事件。工業發電廠、製造設施或加工廠包含大量互聯設備，但由於供應商的多樣性和缺乏標準化， 在不同的供應商設備之間以及同一供應商的設備之間傳輸和接收了許多異質的 IACS 協定。由於控制信號是通過這些協定發送到設備的， 因此工控物聯網安全解決方案必須能夠理解和解釋所有不同協定的含義和影響， 以防止安全方法中出現盲點。要瞭解協定及其固有的有價值資料， 深層封包檢視技術(DPI) 對於全面洞察網路上發生的設備通信是必要的。DPI 允許組織挖掘特定資料封包中的資料層，以獲取實際重要的資料， 例如應用程式資訊和協定標頭， 這將允許組織查看設備是否以不應該的方式進行通信。如果解決方案不提供 DPI， 組織就無法完全瞭解設備通信， 這意味著可疑操作行為或惡意活動可能被忽視。DPI 提供了更深層次的設備通信， 使得組織可以更快、更全面地識別威脅。

另外，從資安監控與維運的考量而言，威脅的識別固然重要，但通過有效的過濾與檢測機制緩解 IACS 安全分析人員的疲勞則更為關鍵，試想，若 IACS 安全分析人員每天接收數百到數萬張有關警報的通知， 這些警報不提供惡意原因、威脅檢測無效和回應效率低下的前後文。由於安全分析師是高需求和供不應求的資源庫， 最大限度地提高這些專業人員的效率是工控物聯網安全平臺的關鍵評價標準。安全分析/監控人員應該能夠存取背景資訊清晰明確的通知， 因為它們提供了警報本身的可見度、威脅等級的嚴重性， 並

提供了分析師應如何應對的建議。有幾種方法可以最大限度地提高安全分析師的工作效率， 例如機器學習、異常檢測和威脅行為分析（這些也是廠商愛用的宣傳語彙）。每種環境在不同的環境中都有價值， 要求不同。

5.2 資安解決方案概念驗證（PoC）

PoC 可以提高 IACS 資安解決方案技術專案成功的可能性，促使組織更加明確、深入地瞭解其需求，並有助於使 IT 和 OT 等部門建立共同目標，透過 PoC 的實施，將可證明相關解決方案可滿足組織需求，以下是執行 PoC 的幾個重點。

5.2.1 從內到外瞭解組織面對的問題

參考案例以及精確的問題陳述有助於確保專案和 PoC 保持正常。問題陳述可協助組織明確真正的需求，參考案例則揭示了解決方案對問題的相關回應，並概述了潛在解決方案如何滿足需求或問題陳述。如果沒有問題陳述和至少預先識別的一個案例，定義成功標準將變為臨時標準，從而增加了 PoC 失敗的可能性。

而典型的 PoC 交付成果應至少包括：

- 問題陳述
- 參考案例
- 專案範圍和計畫
- 成功標準
- 評估(評分)模型和專案計劃。

5.2.2 測試環境的備便

以 IACS 環境而言，尤其是與關鍵基礎設施營運有關之領域（如石油和天然氣、電力和水),在生產環境中執行 PoC 的情況非常少見。因此, PoC 的成功與否將取決於測試環境對生產環境的模仿程度，組織應盡可能確保測試實驗室使用與生產環境具有相同配置的基礎結構。

5.3 資安解決方案部署及上線

前二節闡述了選擇解決方案的切入點，以及驗證解決方案是否確為組織所需的參考方向，而當選定欲購置的解決方案後，接下來組織必須認清的是，PoC 是一時的，而部署與建置卻可能是長期的，在此階段，解決方案所採用的技術以及眼花繚亂的新功能已不是重點，而是必須紮實的規劃，如何將一個解決方案真正融入組織運作，以下提供三個重點供參考。

5.3.1 維運規畫-人員、程序缺一不可

沒有任何技術解決方案可以在完全無人維運的狀況下運作，即使組織跟解決方案廠家都一致的追求最大的自動化、最小的人員投入，但終究仍然需要適度的人員介入，在開始規劃部署上線之前，組織需先考量資安管理團隊的人員運作能力（通常同時需要考量質與量兩個面向），如何投入與編組才能最

短時間之內讓新購置的解決方案發揮效用；另一個重點則是，即便具備了足夠數量、素養的資安管理團隊，也購置了符合組織所需的解決方案，一個大型組織的運作仍然需要完備的程序、計畫、與流程控管，組織需要在此階段同時建構人員足以遵循、參考的工作流程/指引/簽核程序，此部分可以考量與原有生產/關鍵任務運作的程序相結合，以避免疊床架屋，文件化工作過於繁重的問題。

5.3.2 長期程、多里程碑的導入方式較適合工控物聯網環境

如本指南多次提到，工控物聯網環境的最重要任務仍然是其關鍵任務的運作（通常是生產），在效率最大化的追求之下，組織的資安管理團隊以及配合的廠商常常難以找到合適的時間點進行大規模的導入工作，在此前提下，組織必須試著將解決方案可以提供的效益進行適當的切割，以「異動最低、效益最大」做導入期間的指導原則，將一個解決方案分為多個期程，以小範圍漸進導入，同時兼顧導入效益以及降低導入、異動可能造成的風險。

5.3.3 量測指標的制訂與追蹤

在 PoC 階段，組織面對的問題通常是「解決方案是不是真的適合？」，這通常是簡單的是非題，另外則是「同時在評估的多個同性質解決方案，哪個最好？」，而這也是相較之下角簡單的選擇題；然而當開始逐漸導入一個解決方案以後，要面對的則是相對複雜的「解決方案是不是真的有效？怎麼評估？」，組織應結合現有的管理機制，制訂相關的量測指標，例如：

- 解決方案的自動化程度，是否足以減少分析人員某個程度以上的判讀時間？
- 導入該解決方案之後，中斷事件是否減少到組織期待的程度？
- 導入該解決方案之後，是否在操作行為、異動管理的追溯上，符合利害相關人的期待或監理要求？

量測指標可以依據導入的解決方案以及組織期待的效益不斷的新增與調整，並由資安管理團隊定期回報于高階管理人員，以對相關資源進行合宜之調整，並確保對解決方案的投資低卻產生的組織期待的效益。

5.4 選商條件

5.4.1 角色定義與安全議題

做為資產擁有者（asset owner）而言，於導入外部產品、服務時，可能會面對到的外部對象分別有系統整合商、供應商、資訊系統服務外部提供者，以下針對面對此三者購置服務、系統、設備…等資產時，需注意之安全要求。

5.4.1.1 系統整合商

系統整合商是那些為收購者提供客製化服務的實體， 包括自訂開發、測試、操作和維護。該小組通常會回復收購方的徵求建議書， 並提供描述根據收購方要求客製化的解決方案或服務的建議，而系統整合商提供的此類建議甚至可以包括多層供應商 。收購方應有能力要求嚴格的供應商驗收標準以及任何相關控制措施來解決已查明或潛在的風險，並要求系統整合商應確保對這些供應商進行檢視和核實， 以滿足收購方的信通技術安全要求。

5.5.1.2 供應商

供應商可以為資產擁有者供應商用解決方案，例如非開發專案、商用解決方案/產品， 其中包括開源解決方案 。供應商是一個多樣化的群體， 從非常小的到大的， 專業化到多樣化， 立足于一個國家到跨國， 在工藝和解決方案的複雜性、資源和透明度方面範圍廣泛。資產擁有者應考慮到， 與供應商做生意的成本可能會直接受到供應商如何將安全和供應鏈做法應用於其解決方案的能見度的影響。當組織或系統整合商要求供應商提供更高的透明度時，他們必須考慮這些要求可能涉及的費用問題。供應商可以選擇不參與採購，以避免其智慧財產權的成本增加或被認為存在風險， 從而限制組織的供應或技術選擇。供應商面臨的風險是可能產生他們可能必須單獨遵守的多套不同的要求， 而這些要求可能是不可擴展的。

5.4.1.3 資訊系統服務外部提供者

資訊技術系統和服務的外包產生了一套資訊和通信技術供應鏈問題， 降低了資產擁有者對外包職能的可見度和對外包職能的管理。因此， 它要求各組織在界定通信技術和客戶關係管理要求時更加嚴格， 必須在採購中說明這些要求， 然後監測所提供的服務， 並對其遵守所述要求進行評價。無論誰執行服務，資產擁有者最終都要對使用這些服務可能對組織的系統和資料造成的風險負責。各組織應實施有效的通信技術控制， 以應對這一風險， 並與風險主管合作接受這一風險。可採用各種方法， 通過合約、機構間協定、業務安排、許可證協定或供應鏈交易等工具， 溝通並隨後核實和監測相關控制措施之要求。

5.4.2 選商評估參考控制領域

採購方可參考前述章節對角色以及相關安全議題之陳述，結合實際購置標的可能對現有環境、資料流、營運型態之影響，選擇下列可能相關之安控領域設計控制要求，以達成對選商安全管理：建立要求-監測服務/產品水準-追蹤改善之循環。

- 帳戶管理 Account management
- 服務確保 Assurance
- 備份還原 Backup/Restore
- 組態管理 Configuration management
- 資料保護 Data Protection
- 事件管理 Event management

- 惡意軟體保護 Malware protection
- 網路安全 Network Security
- 修補程式管理 Patch Management
- 遠端存取 Remote Access
- 安全儀錶系統 Safety Instrumented System
- 解決方案強化 Solution Hardening
- 解決方案人員配置 Solution Staffing
- 無線網路應用 Wireless

第 6 章 工控物聯網資安維運

6.1 資產管理

組織對自身所擁有的資產必須有充分的理解及動態的追蹤，資產的可視度會重大的影響任何後續管理作業的運行，其中影響最大的應屬對 IACS 修補程式管理， 在進行分析和規劃之前， 需要大量有關當前環境的資訊。這些資料的收集成本可能非常高， 而且對潛在的攻擊者非常有啟發性， 因此應該對其進行適當的保護。

建立 IACS 修補程式管理程式首先要進行準確的清單評估， 以確定: 範圍內的設備以及正在使用的軟體和修補程式版本。如果資產庫存資訊不准確， 則基於該資訊的基於風險的決策也不准確。

此外， 當發現新的漏洞時， 準確的資產資訊環境將使資產擁有者能夠確定其設施中的哪些資產或設備具有該漏洞。這將使易受攻擊資產或設備的擁有者能夠採取緩解行動， 保護易受攻擊的設備。

第一步是確定作為 IACS 一部分的元件和設備。這包括所有可更新的裝置類型， 例如: 伺服器、工作站、交換器、路由器、防火牆、印表機、串列到乙太網轉換器、可程式設計邏輯控制器 (Plc)、遠端終端機單元 (Rtu) 和所有不可更新的設備，可以替換為修補或更新的設備。可使用一些資源和方法來描述現有環境的特點， 例如:

- 資產執行資訊系統， 可包括: 資產所有人擁有和維護的電子設備的購買記錄、序號、資產標籤和其他識別資料;
- IACS 文檔， 如: 設備清單、體系結構圖紙、設計文檔和原始 iacs 產品供應商文檔;
- IP 文檔， 如:IP 位址清單、網路拓樸圖;
- 對設施進行物理檢查， 以識別設備及其相對於設備的連線性.
- 現有的營運衝擊分析(BIA)、業務連續性規劃 (BCP) 和災害復原規劃 (DRP) 文件

在現有環境的清單中， 應利用上述方法， 制定一個準確的待考慮的設備及其關鍵性清單。

有了準確的設備清單清單， 下一步是從每個單獨的設備收集特定資訊。此資料收集的目的是確定可用於或需要用於建立和操作 IACS 修補程式管理程式的任何資訊。所收集的資料應包括:

- 擁有權 - 這識別資產擁有者或託管人員， 以及能夠支援資產的資源。這些資訊將在以後分配責任和關鍵決策時使用。
- 產品供應商、品牌、型號 - 此資訊將在以後與產品供應商聯繫時使用.
- 版本 - 與任何硬體元件及其關聯的韌體關聯的版本， 包括啟動代碼版本、韌體版本和啟動對應版本.
- 作業系統版本 - 與作業系統環境關聯的版本。這包括作業系統名稱、版本、服務包、修補程式、修補程式、服務版本等。根據環境的不同， 作業系統可能是虛擬化虛擬化虛擬機器管理程式解決方案的一部分， 並且還需要虛擬化主機的軟體。或者， 作業系統可能是嵌入式設備韌體的一部分。

- 軟體版本– 與安裝在作業系統頂部的軟體相關聯的版本。記錄每個軟體元件的產品供應商非常重要， 因為除了軟體標題外， 以後還需要此資訊。
- 冗餘– 這定義了硬體和軟體的容錯移轉和容錯功能。此資訊將在以後用於支援修補程式的評估、規劃和安裝。例如， 是需要完全中斷， 或者可以將修補程式應用於一個設備、冗餘集的一部分， 然後再應用到另一個設備， 而不會中斷 IACS 操作。
- 電腦角色– 這定義了單個電腦的功能， 對於評估在安裝軟體更新後重新開機電腦（如有必要）的影響是非常重要。例如， 如果電腦是運行關鍵商務應用程式的伺服器， 則建議將軟體更新安排在對業務影響最小的時間段。還可能需要為業務連續性做出安排， 以便使用者可以在重新開機伺服器時繼續操作。
- 電腦群組– 這定義了執行類似功能（例如， 網域控制站、操作員工作站）的設備的分類和分組， 這些設備預計具有相似甚至相同的硬體、軟體、配置和 IACS 修補程式管理原則。
- 網路架構和連線性– 這定義了網路架構和結構。瞭解網路基礎結構的佈局、功能、安全級別、連結速度和連結可用性對於有效修補非常重要。這種佈局還應包括遠端存取系統， 如支援和管理系統。軟體更新的大小可能會有所不同， 瞭解網路基礎結構的約束可能會減少分發軟體更新時的任何延遲。它還可以規定將軟體更新部署到特定用戶端電腦並將其安裝到特定用戶端電腦上的方式。
- 已安裝且未安裝軟體更新– 這將識別電腦上已安裝或未安裝的軟體更新，並且是必不可少的資訊.
- 支援狀態– 這識別每個電腦系統的支援狀態。如果沒有軟體或硬體更新，而且升級對於電腦系統來說是不可行的， 就需要記錄， 因為該系統將不屬於修補程式管理制度的範圍， 需要一個單獨的安全管理制度， 比如強化的安全管理制度配置或使用多層防禦（縱深防禦）。應記錄已知或預期的產品供應商支援日期。對這些資料的定期檢視將使支助計畫有控制地改變。
- 相互依存關係– 這描述了不同裝置類型、類別和設備組之間的相互依存關係。這些資訊將支援以後對修補程式的評估、規劃和安裝， 以確保減輕相互依存設備的風險。
- 關鍵度– 這描述了基於元件和系統組的關鍵性的任何更改約束管理。通常， 工控環境中的關鍵資料路徑沒有進行分析或記錄， 並包含識別關鍵相互依存關係所需的詳細資訊。修補的重點是將更新應用於在這些裝置上運行的軟體、韌體或作業系統。關於何時修補的決定將從徹底瞭解電腦和嵌入式控制器為系統操作提供的關鍵過程和關鍵資料流程開始。每個關鍵過程的操作都需要理解電腦系統的交互和相互依存關係。
- 漏洞評估工具的適用性– 這描述了評估工具是否可以自動或手動運行或從不運行。資產擁有者應將漏洞評估工具視為識別與其 IACS 相關的安全性漏洞的另一種方法。漏洞評估工具可以說明識別可通過配置更改、安裝修補程式或其他緩解控制來緩解的風險並確定其優先順序。主動漏洞掃描工具可能會對 IACS 產生負面影響， 並且只能在受控條件下和指定掃描級別下進行測試後使用。

- 設定檔- 請注意， 如果任何配置資訊需要在修改之前捕獲， 然後必須在修改之後重新應用.

6.2 資安監控與量測

IACS 的持續監控由組織選擇的合格人員 設計、記錄和實施。該組織應確保持續監測不會干擾 IACS 的功能。設計和進行持續監控的個人小組充分瞭解組織資訊安全政策和程式、IACS 安全政策和程式以及具體的健康、安全和環境風險與特定設施和/或工序相關聯的。組織確保持續監控不會影響系統操作或導致有意或無意的系統修改。補償控制實例包括外部監視。

無論採取何種措施來保護 IACS， 它都始終有可能受到有意或無意事件的影響。以下症狀可能是由正常的網路問題引起的， 但當幾個症狀開始出現時，則是 IACS 可能受到攻擊的徵兆， 值得進一步調查。隨著攻擊者使用的工具/技術精緻程度，可觀察的徵兆有可能會月趨減少，甚至完全不引人注意，以下列出部分值得供監測人員/系統進行細部分析的可能攻擊徵兆。

- 異常繁忙的網路流量
- 磁碟空間不足或顯著減少可用磁碟空間
- 異常高的 CPU 使用率
- 建立新的使用者帳戶
- 已嘗試或實際使用管理員等級的帳戶
- 鎖定的帳戶
- 當使用者不在工作時， 而卻有存取/操作活動的帳戶
- 日誌檔遭清除
- 具有異常多的事件的完整日誌檔
- 防病毒或 IDS 警報
- 禁用的防毒軟體和其他安全控制
- 意外的修補程式更改
- 連接到外部 IP 位址的電腦
- 要求有關系統的資訊（社交工程嘗試）
- 配置的意外更改
- 意外的系統關閉。

6.3 變更管理

有效的變更管理可以減少誤操作或有意舞弊肇生的資安事故，組織應針對實體層面（例如元件之間的配接）、系統上（作業系統或軟體的更迭）、配置上（既有軟硬體的參數變更），基於技術檢視及權責檢視兩大方向進行有效的變更管理。變更管理過程應遵循職責分離原則， 避免利益衝突。這意味著同一個人不能同時核決更改並達成更改。另外，異動的提出應由具備技術/生產管理知識的管理人員根據明確定義的政策， 考量對 HSE 風險和網路安全風險的潛在影響檢視對 IACS 的更改要求。如果其中一個政策因更改而違反，則可能需要由其他具備技術/生產管理知識的管理人員審核建議的更改， 以驗證其是否有效或不核決更改。 為了使變更管理有效， 應詳細記錄安裝/異

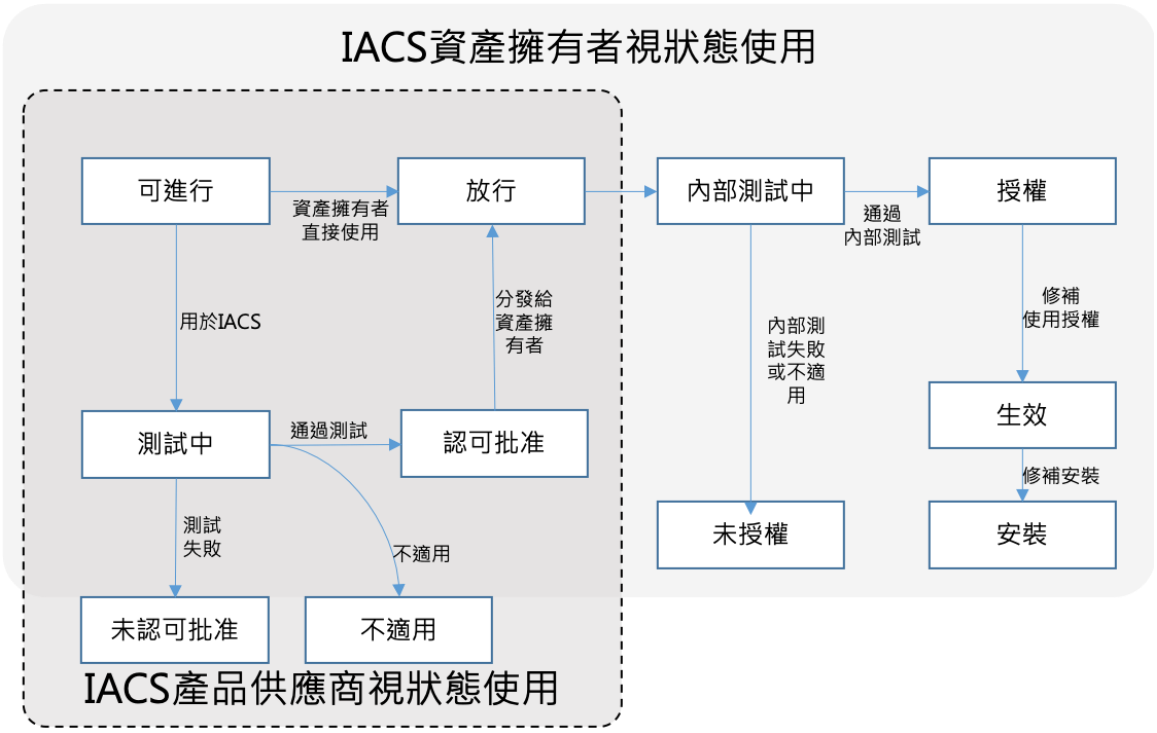
動了哪些內容，變更管理程序必須有經過檔證明和驗證的備份和還原過程來支援。
安裝修補程式、升級和政策更改可能會產生嚴重的網路安全（甚至是對生產結果）影響。但如果不安裝亦會造成嚴重的安全隱患。組織必須採取相關測試方法來確定新修補程式對弱點的緩解能力，以及安裝與否的急迫性，而所有系統升級、修補和政策變更都必須按照變更管理系統程式實施。

6.4 修補管理

資產擁有者在嘗試為其 IACS 實施修補程式管理計畫時面臨許多挑戰。修補 IACS 意味著更改 IACS， 亦即為變更管理工作之延伸，如果執行不正確，更改可能會對其安全性、可操作性或可靠性產生負面影響。準備要修補的 IACS 可能需要大量的工作， 資產擁有者可能難以獲得必要的資源來解決增加的工作量。對於每個修補程式和他們擁有的每個產品， 資產擁有者必須收集和分析每個設備的修補程式資訊， 在測試系統上安裝和驗證， 確保在之前和之後建立備份， 確保在將系統重新轉換為操作， 並最終跟蹤所有必要的更改文檔。 由於建議對 IACS 進行修補的資源和努力， 大多組織在其他正常的日常維護中斷期間安排修補程式安裝。有時， 這些停機視窗是季度、年度或更低的頻率。某些極其關鍵的系統可能沒有可用的中斷視窗， 因此，如果需要系統停機， 則無法對其進行修補。
應用修補程式是一項風險管理決策。如果應用修補程式的成本高於風險評估成本， 則修補程式可能會延遲， 特別是在存在其他安全控制以降低風險（如禁用或刪除功能）的情況下。
儘管執行修補作業可能對帶來如此多的負面影響與執行上的困難，但適當的修補對 IACS 是絕對必要的，常見修補作業不佳的意外後果可能包括:

- 修補程式和控制系統軟體之間的不相容性
- 防毒和反惡意軟體產生誤報
- 在測試不足的情況下， 系統效能、可靠性和可操作性下降

鑒於產品供應商和資產擁有者在保持系統更新以最大限度地減少漏洞造成的安全風險方面面臨的挑戰， 對手（例如， 惡意威脅行為者）將始終比目標具有優勢。一旦發現漏洞， 無論是出於善意還是惡意， 問題都會主要轉移到資產擁有者， 以便儘快應用修補程式。資產擁有者可能能夠也可能無法應用修補程式， 它成為有關如何降低漏洞風險的基於風險的決定。儘管可能永遠無法消除所有軟體漏洞， 但不評估漏洞的風險並確定何時以及如何應用修補程式是沒有任何藉口的。 對 IACS 修補程式管理不善的主要影響是 IACS 系統丟失或損壞的風險增加。例如， 與辦公室或企業系統不同， IACS 的危害可能會產生超出資料損失或系統停機時間的後果。IACS 的妥協可能會影響系統安全、操作人員的人身安全、生產產品的品質、生產產品的安全性和生產產品的可用性。
既然系統修補是所有資產管理人都必須面對的風險作業，本指引將接續介紹修補管理之生命週期模型如下圖，涵蓋了從可用到授權到有效和安裝等流程。並非所有可用的修補程式都與 IACS 相關， 也不是所有修補程式都與 IACS 應用程式相容。對於有效的 IACS 修補程式管理過程， 瞭解所有可用修補程式的狀態非常重要。

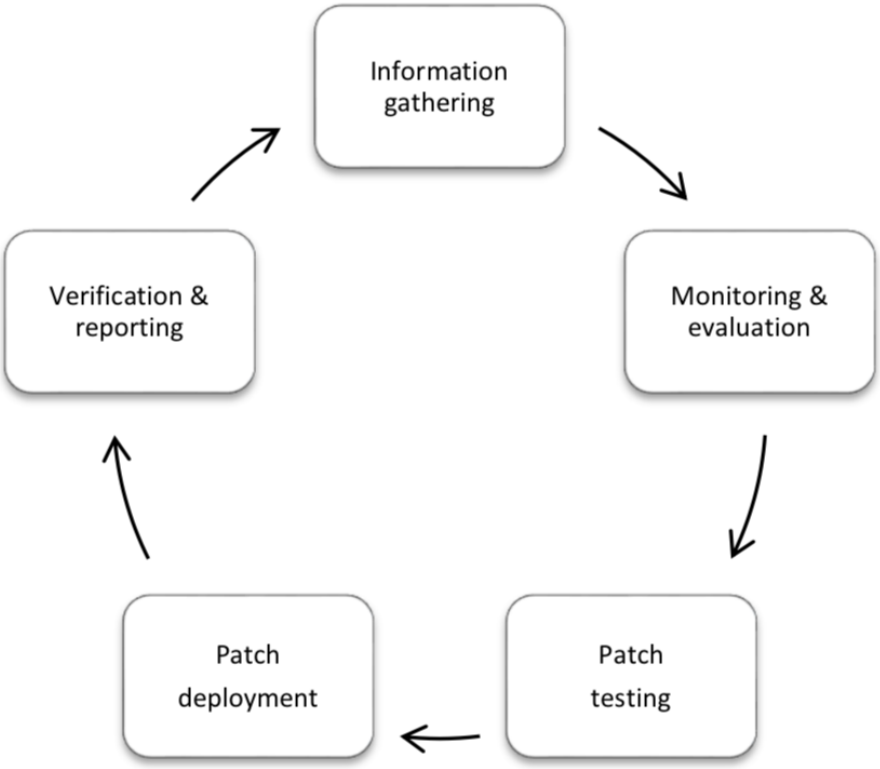


資產擁有者有義務維護其運營的安全性、可靠性、可操作性、安全性和品質。而透過修補 IACS 資產來達成網路安全保證是這一義務的關鍵作業。

IACS 資產擁有者應:

1. 建立和維護與 IACS 相關的所有電子設備的資產清單， 這些設備可能會通過以下方式進行更新: 修改其功能、配置、操作、軟體、韌體、操作代碼等。這些設備應稱為 "可更新" 設備;
2. 建立和維護每個設備當前安裝版本的準確記錄， 稱為 "已安裝" 版本;
3. 定期確定每個設備可使用哪些升級和更新， 稱為 "最新" 版本;
4. 定期確定由 IACS 產品供應商確定為相容的升級和更新的 "已發佈版本"，並符合資產擁有者 "可更新" 設備的標準;
5. 以準確反映生產環境的方式測試 IACS 修補程式的安裝， 以確保在實際生產中在 IACS 上安裝修補程式時， IACS 的可靠性和可操作性不會受到負面影響環境。成功通過這些測試的修補程式稱為 "授權修補程式";
6. 在系統設計（例如冗餘、容錯、安全）和操作要求（例如， 計畫外停機、計畫外停機）的限制下， 安排在下一個可用機會安裝的有效修補程式停機、進程等);
7. 按計劃的時間間隔更新記錄， 至少每季度更新一次， 以包括每個可更新設備: 已安裝的版本、授權版本、有效版本和已發佈的版本;
8. 確定安裝修補程式的計畫間隔， 例如: 當修補程式可用時， 或至少每年一次;和
9. 安裝修補程式和/或實施補償對策， 以緩解 IACS 中存在的安全性漏洞。

欲達成以上對資產擁有者於修補管理作業之要求，建議資產擁有者依照以下的循環進行相關作業：



- 資訊蒐集階段：

  對於 IACS 修補程式管理，在進行分析和規劃之前，需要大量有關環境的資訊。這些資料的收集成本可能非常高，而且對潛在的攻擊者非常有啟發性，因此應該對其進行適當的保護。建立 IACS 修補程式管理程式首先要進行準確的邀請評估，以確定: 範圍內的設備以及正在使用的軟體和修補程式版本。如果資產庫存資訊不准確，則基於該資訊的基於風險的決策也不准確。 此外，當發現新的漏洞時，準確的資產資訊將使環境擁有者能夠確定其設施中的哪些資產或設備具有該漏洞。這將使易受攻擊的資產或設備的擁有者能夠採取緩解行動，以保護易受攻擊的設備。 第一步是確定作為 IACS 一部分的元件和設備。這包括所有可更新的裝置類型，例如: 伺服器、工作站、交換器、路由器、防火牆、印表機、串列到乙太網轉換器、可程式設計邏輯控制器 (Plc)、遠端終端機單元 (Rtu) 和所有不可更新的設備,可以替換為修補或更新的設備。可使用一些資源和方法來描述現有環境的特點，例如:

  - 資產盤點系統，可包括: 資產所有人擁有和維護的電子設備的購買記錄、序號、資產標籤和其他識別資料
  - IACS 文件，如: 設備清單、體系結構圖紙、設計文檔和原始 IACS 產品供應商文檔
  - IT 文件，如 IP 位址清單，網路拓樸圖
  - 對設施進行實物檢查，以確定設備及其相對於現有檔的連線性
  - 對 MAC 和 IP 位址的交換器路由器進行查詢，以識別連接的系統
  - 網路連接設備發現工具，如:網路分析儀;和

- 現有的業務影響評估（BIA）、業務營運持續規劃（BCP）和災害復原規劃（DRP）文檔（如果存在）。

- 監控與評估階段：

本階段主要工作目標在於明確修補程式是否適用、對 IACS 環境的影響以及與修補程式相關和緩解的風險。在修補程式監視和評估過程結束時，可以明確決定是安裝修補程式、部署其他對策還是不執行任何操作。

- 修補程式測試階段：

測試修補程式的目的是通過技術驗證建立信心，證明修補程式不會對 IACS 的效能、安全性或可靠性產生負面影響，建議在具有類似硬體和軟體的非 IACS 環境上成功安裝和測試修補程式。

- 修補程式部署階段：

根據組織的規模和複雜性、設備數量、物理位置和可用的資料網路通信，在安裝修補程式之前可能需要進行大量準備。

最常見的挑戰是確定如何將更新檔分發到多個位置和設備。IACS 設備可能因為各式連線控制設備的限制導致禁止大量傳輸、發佈檔案。以下選項可用於派送修補程式:

- 利用支援傳送速率限制和低優先順序的自動修補程式部署工具，以減少對網路或設備的影響;
- 使用不會影響 IACS 的其他通信網路分發更新檔，包括將更新檔分發和發佈到本地或分散式檔案伺服器，人員可以從生產環境中下載這些檔;
- 從操作中刪除目標設備，將 IACS 網路移至處於離線狀態的效能 rm 修補程式;
- 將更新檔案複製到唯讀可攜式媒體，如 CD 或 DVD;和
- 將更新檔案複製到讀寫可攜式媒體，如 USB 記憶體或可攜式硬碟磁碟機。 在這種情況下，必須特別注意確保檔和存儲介質在傳輸過程中不會被惡意程式碼篡改或感染，這可能會增加 IACS 的風險。
- 負責修補程式安裝的人員可能沒有參與修補程式測試，並且可能必須查看提供給他們的所有說明和程式，以確保與測試和可靠安裝的一致性。

- 修補程式驗證階段：

驗證修補程式安裝的方法包括:

- 比較更改前後安裝的軟體版本;
- 檢視來自配置更改檢測系統的日誌;
- 檢查來自修補程式管理解決方案的報告，以驗證已安裝了對應的修補程式

- 計算計畫升級的設備數量，相對於已成功完成的設備數量;

另外，除資產擁有者應投入相關資源進行修補管理作業外，組織也應該從供應商方面著手，對供應商進行相關要求，以確保取得產品/設備時的風險以及內部管理作業能降到最低，以下是監督供應商時可參考的數個要求面向：

- 提供說明其提供的產品和系統的軟體修補政策的文件;
- 通過分析和驗證所有修補程式（包括所使用的作業系統供應商以及 IACS 產品可能使用的協力廠商軟體的所有供應商發佈的修補程式)， 在所有修補程式的適用性和相容性方面具有資格;
- 提供所有修補程式及其批准狀態的清單
- 針對達到產品壽命結束或不再提供網路安全修補的部件提供充分的警告(至少提前兩年);和向 IACS 使用者提供有關支援 IACS 產品的政策的資訊，包括安全更新。

6.5 事件回應

事件回應計畫是對一組預先確定的程序， 用於檢測、回應和限制針對組織資訊系統的事件的後果。應對措施首先應與 預定的服務水準相比較， 而不僅僅是被破壞的系統。如果發現事件， 應進行快速風險評估， 以評估攻擊的效果和應對選項。例如， 一個可能的回應選項是對受到攻擊的系統進行實體隔離。然而， 這可能對服務產生如此可怕的影響， 以至於被認為不可行。安全事件的處理包括準備、檢測和分析、遏制、根除和復原。控制還包括人員的事件回應培訓和測試資訊系統的事件回應能力。

整體事件回應的工作可分為以下三個階段

- 對事件進行分級：
  應查明各種類型的 IACS 事件， 並依據其潛在影響或已知影響程度進行分級， 以便對每一起潛在/已知事件作出適當反應，投入正確的資源。
- 回應操作：
  在發生事件時， 可以採取多種回應。這些措施從什麼都不做到完全關閉系統（儘管完全關閉 IACS 是一種極不可能的反應)。所採取的反應將取決於事件的類型及其對 IACS 系統和被控制的實體過程的影響。應編寫一份書面計畫， 記錄事件的類型和對每種類型的反應。這將在事件可能造成混亂或壓力的時候提供指導。該計畫應包括各組織應採取的逐步行動。如果有報告要求， 應注意這些要求以及報告應在何處提出， 並在何處提供電話號碼， 以減少報告的混亂。
- 復原操作：
  入侵的結果可能不大， 或者入侵可能會在 IACS 中造成許多問題。應進行風險分析， 以確定被控制的實體系統對 IACS 中的故障模式的敏感性。在每種情況下， 都應記錄分步復原操作， 以便系統能夠盡可能快速、安全地復原正常運作。影響 IACS 運作的入侵的復原行動將與系統的災害復原計畫密切保持一致， 並應考慮到已經建立的規劃和協調。

6.6 營運持續

6.6.1 業務持續性計畫的範圍

在制定業務持續性計畫之前， 重要的是要瞭解何時應該使用該計畫以及適用何種情況。 計畫外中斷可能採取自然災害（即颶風、龍捲風、地震或洪水）、無意的人為事件（即意外設備損壞、火災或爆炸或操作員錯誤）、故意人為事件（即颶風、龍捲風、地震或洪水）、故意人為事件（即破壞、駭客或病毒的攻擊）或設備故障。從潛在的停機角度來看， 這可能涉及典型的幾分鐘或幾小時的機械故障，甚至是自然災害中造成的幾天、幾周或幾個月的中斷。由於業務持續性也主要涉及生產中斷的長期影響， 一些組織還選擇對需要考慮的風險規定最低中斷限制。為了 IACS 網路安全的目的，長期停機（災後復原）和短期停機（業務復原）都應考慮在內。該計畫還包括災後復原的其他方面， 如應急管理、人力資源、媒體或新聞關係。
由於其中一些潛在的中斷涉及人為事件， 因此與實體安全性群組織合作瞭解這些事件的相對風險以及現有的實體安全控制措施也很重要。防止他們。實體安全性群組織還必須瞭解生產網站 IACS 中哪些區域可能會帶來更高等級的風險。

6.6.2 業務持續性規劃流程

在建立處理潛在停機的計畫之前， 必須根據典型的需求為所涉及的各種系統和子系統指定復原目標。系統復原涉及所有通訊連結和 IACS 功能的復原，通常是根據復原時間目標或復原這些連結和功能的時間來指定的。資料復原涉及復原描述過去生產或產品狀況的資料， 通常是根據復原點目標或可以容忍缺乏資料的最長時間來指定的。 一旦定義了復原目標， 就應該建立一個可能中斷清單， 並開發和記錄復原過程。對於大多數較小規模的中斷， 基於關鍵備件庫存的維修和更換活動可能足以達成復原目標。在其他情況下，需要制定應急計畫。 由於這些應急計畫的潛在費用， 應與負責業務持續性規劃的管理人員檢視這些計畫， 以確認這些計畫是否合理。 應確定業務持續性小組的要求， 並組建一個小組。該小組應包括 IACS 和其他工業營運擁有者。在發生重大中斷的情況下， 該團隊應確定關鍵業務和 IACS 系統重新建立操作的優先順序。 應制定一個計畫， 以測試全部或部分復原過程。通常每年對特定子系統的程式進行測試， 並對特定子系統進行輪換， 以便最終在 5-10 期間對整個系統程式進行測試。這些頻率只是實例， 必須由您的組織作為規劃過程的一部分來確定。 請特別注意驗證系統組態資料以及產品或生產資料的備份。不僅應在生產時對其進行測試， 還應在一定頻率上檢視其儲存所遵循的程式， 以驗證備份和支援資料是否可用和準確。這些備份應保存在不會使其無法使用的環境條件下， 並保存在安全的位置， 在需要時，授權的個人可以在那裡快速獲得備份。 如果發生事件， 可能要求該組織向調查人員提供有關該事件的鑑識資料， 無論是調查人員還是組織外的調查人員。 隨著時間的推移， 業務持續性計畫需要檢視和修訂， 以反映管理結構、組織、商業模式、產業等方面的變化。

第 7 章 工控物聯網資安稽核與持續改善

7.1 資安稽核

稽核的目的在於定期確認政策、計畫和控制措施是否按照預期規劃得到適當執行。在 IACS 環境中， 稽核員必須充分瞭解公司網路安全政策和計畫以及與特定設施或工業營運相關的特定 HSE 風險。必須注意確保稽核不會干擾 IACS 設備提供的控制功能，稽核應核實:

- 安全政策、過程和控制措施在系統驗證、測試期間仍在作業系統中安裝並正常運作。
- 生產系統不受安全威脅，如果發生事故，將生成日誌和記錄，以捕獲有關事件性質和影響程度之訊息。
- 嚴格遵循變更計劃管理，對所有變更進行審核和審批審核

任何網路安全檢視或審核（內部或外部）都將為組織提供有價值的資料，以改進 CSMS。這些檢視或稽核的結果應包括必要的詳細資訊，以確保滿足任何法律或監管要求，並且可以進行檢視或稽核所表明的任何修改。結果應發送給所有相關人員（即利益相關者，經理和安全人員）。

為確保稽核可以正確且有效的進行，對稽核員的教育訓練是非常重要， 稽核員應具備充分知識瞭解他們將稽核的系統、網路的性質以及已經制定的具體政策，組織可在必要時延請外部專家執行稽核工作。

7.2 資安成熟度評估

資安成熟度是指組織在工控物聯網在整體、區域或管道為範圍，其控制領域「安全等級目標（SL-T）」達成程度，即以「已達成安全等級(SL-A)」去對比目標安全等級(SL-T)，如果 SL-A 是大於等於 SL-T，則資安成熟度為已達成，反之則視為未達成，需要額外資安控制措施導入。

7.2.1 企業區的資安成熟度

企業區域為 IT 資安管理範圍以 ISO27001 的管理體系及控制領域，來綜合評估，與 OT 環境系統相關的系統、網路及人員則與工控區域一併評估，可以視為企業區域的例外。

參考 ISO27001 的要求領域區分：

- CSMS 管理體系 (Cyber Security Management System)
- 資訊安全政策(Information security policies)
- 資訊安全組織(Organization of information security)
- 人力資源安全(Human resource security)
- 資產管理(Asset Management)
- 存取控制(Access Control)
- 密碼學(Cryptography)
- 作業安全(Operation Security)
- 通信安全(Communications Security)

- 系統獲取、開發和維護(System acquisition, development and maintenance)
- 供應者關係(Supplier relationships)
- 資訊安全事件管理(Information security incident management)
- 營運持續管理之資訊安全層面(Information security aspects of business continuity management)
- 遵循性（Compliance）

可以由組織自行定義目標安全等級(SL-T)，透過各領域的細部量測指標，去評定組織在個別領域達成的安全等級（SL-A），如在資產管理等級，SL-A 可以區分為，等級 1：尚無正式的資產盤點程序及活動，等級 2：有定期資產盤點活動，但資產盤點準確率未達 90%，等級 3：有定期資產盤點活動，但資產盤點準確率達 90%以上，等級 4：隨時維持盤點異動更新，且資產盤點準確率達 98%以上。圖 39 是組織 CSMS 成熟度案例。

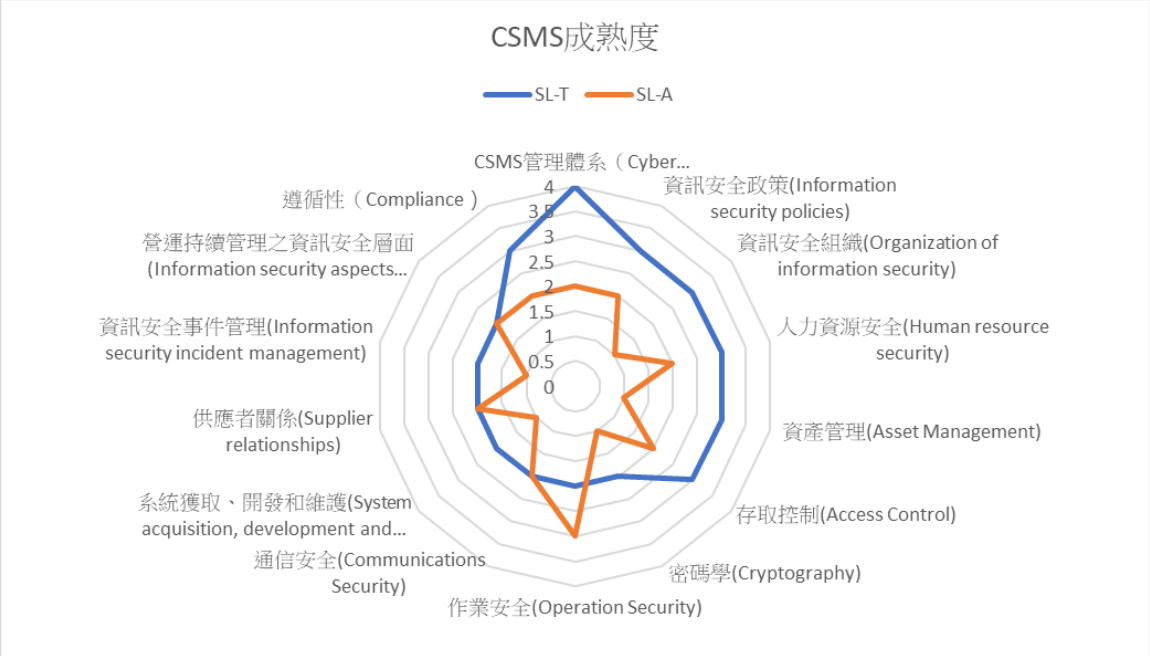


圖 39 企業 CSMS 成熟度案例

7.2.2 企業區的資安成熟度

在工控區域資安成熟度參考 IEC 62243 的 IACS 安全功能需求：

- FR 1 – 識別和認證控制（Identification and authentication control）

- FR 2 - 使用控制（Use control）
- FR 3 - 資料完整性（Data integrity）
- FR 4 - 資料機密性（Data confidentiality）
- FR 5 - 受限制的資料流（Restricted data flow）
- FR 6 - 及時回應事件（Timely response to event）
- FR 7 - 資源可用性（Resource availability）

假設某一區域的安全等級需求的的雷達圖表示如圖 40：

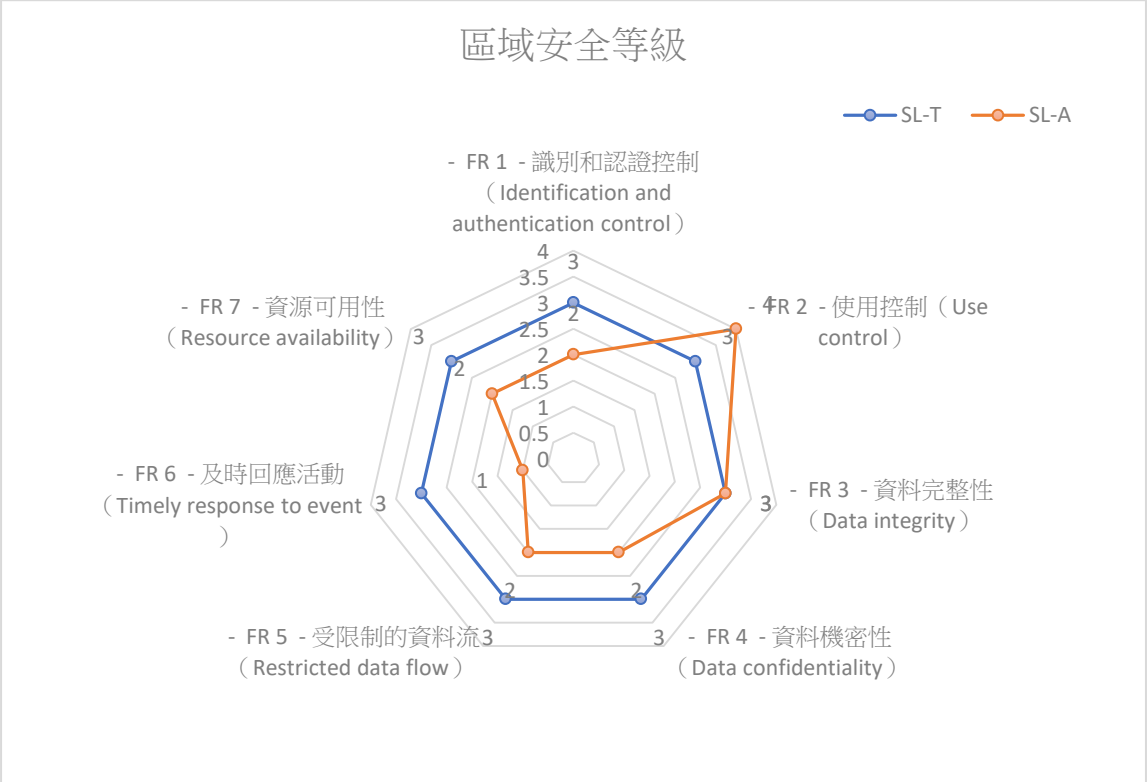


圖 40 區域安全成熟度

以這個例子來看，7 個功能需求的安全等級目標設定在等級 2，除了使用控制達成安全等級 3，其餘 5 個領為等級 1，1 個為等級 0。

7 .3 持續改善

通過持續監控和檢視的過程， 一個組織可以在有證據的情況下確定它正在達到安全目標、政策和計畫的要求。內部檢查方法， 如一致性稽核和事件調查，使組織能夠確定管理系統的有效性， 以及它是否按照預期運作。還必須確定管理制度仍然符合規劃過程中確定的目標、指標和目的。如果偏離了最初的目標、指標或目的， 可能需要對管理制度進行系統的改革。

由於解決安全問題的威脅和技術都在不斷發展， 預計組織的網路安全計畫將不斷發展， 反映出可用的新威脅和功能。各組織應跟蹤、衡量和改進安全工作， 以確保人員、財產、產品、工業營運、資料和資訊系統的安全。

總體目標是通過納入根據新威脅、新能力和定期檢視作出的改進， 確保整體安全計畫維持效力。對安全的持續關注為員工提供了一個指標， 表明資訊安全是公司的核心價值。

第 8 章 結論

本指南為以生產製造企業及基礎設施提供者的資產擁有者提供主要視角，提供在內部的高階管理階層、IT、OT 及資安人員在對工控物聯網導入到企業的同時提供一個資訊安全框架、安全計畫的規劃、實施、考核及改善的生命週期，並如何向資安顧問、資服、工控系統產品及服務提供者及安全實驗室提出安全需求，並據以監督服務水準，本指南並未以特定產業的專有需求來撰寫，在製程可靠度及效能優先考量下，如何發展一個可持續改善的安全計畫，提供建言，期望可以提供工控物聯網安全防護機制建置的各相關方參考。

本指南在發展初期以參考國際資訊安全、工控自動化安全標準設定本指南框架，結合我國資通安全管理法對關鍵基礎設施安全要求，由組織全景、風險管理角

度及傳統 IT 與 OT 架構及維運組織分立，藉由智慧製造數位轉型風潮下，以整合 IT/OT 為單一架構，並將人員適當依專長分工且促進合作，將不同國際資安標準、組織不同的功能單位，組合成跨部門合作的工控物聯網決策及維運單位，完成草案後並由本撰寫團隊憑藉多年擔任資訊安全顧問服務實務經驗，協助本計畫內受訪企業（資產擁有者）導讀本指南，訪談企業智慧製造的現況與安全風險，共協助依本指南擬訂產業別導入指南（防護計畫），作為企業導入並運用本指南進行工控物聯網資安防護可執行、可量測成果的計畫。

本指南發展同時也邀集資安顧問業、資訊服務業、工控系統服務業及資安實驗室業者（以上統稱資安產品／服務提供者）共同參與並回饋實務意見，期能透過本指南縮小工控物聯網資安需求與供給落差。由本指南引導企業客戶依組織目標、預算來源及安全風險，提出合理可行的安全需求，由資安產品／服務提供者提供對應合乎成本效益的資安解決方法。

本指南撰寫團隊期望本指南及依本指南產出產業別導入指南（防護計畫）能由主管機關及業界對各企業推廣，並能於導入後提供意見回饋，使本指南能逐年維護並持續擴大應用產業別，讓工控物聯網安全隨智慧製造興起同時能防範資安事件於未然，將安全管理及防護機制建立起來，並在事故發生時能快速回應資安事件，並由事故中回復，使企業智慧智造不停頓。

附錄

A. 名詞定義
B. 資訊安全管理體系統評估表
C. 系統安全技術要求評估表
D. 元件安全設計開發檢核表
E. 安全元件檢核表
F. 供應商能力評估檢核表
G. 工控物聯網資安自評

附錄 A 名詞定義

編號	中文名詞	英文名詞	定義說明
1	存取	access	與系統通信或以其他方式與系統互動以便使用系統資源的能力和手段。 注意：存取可能涉及實體存取（實體區域內允許授權，擁有實體密鑰鎖，PIN 碼或存取卡或允許存取的生物識別屬性）或邏輯存取（登錄系統和應用程式的授權），通過邏輯和實體手段的結合）
2	存取控制	access control	保護系統資源免受未經授權的存取;根據安全政策調整系統資源使用的過程，只有授權實體（使用者、程序、流程或其他系統）才允許根據該政策。
3	可歸責	accountability	系統的屬性（包括其所有系統資源），確保系統客體（Object）的操作可以唯一地追溯到該主體(Subject)，該主體可以對其操作負責。
4	應用程式	application	執行由使用者命令或軟體程序事件啟動的特定功能的軟體程式，可以在不存取系統控制、監視或管理權限的情況下執行。
5	區域	area	站點的實體，地理或邏輯資產群組的子集。 注意：區域可能包含生產線、製程單元和生產單元。 區域可以通過站點區域網路彼此連接，並且可以包含與在該區域中執行的操作相關的系統。
6	資產	asset	由組織的監管職責所擁有或擁有的實體或邏輯對象，對組織具有感知價值或實際價值。 附註：對於工控物聯網，具有最大可直接測量值的實物資產可能是受控制的設備。
7	協同	association	各系統實體之間的合作關係，通常是為了在它們之間傳遞資訊。
8	保證	assurance	系統的屬性，它提供了對系統運作的信心，以便實施系統安全政策的理由。
9	攻擊	attack	對源自智慧威脅的系統的攻擊 - 即，故意的意圖（特別是在方法或技

			術意義上）的智慧行為，以逃避安全服務並違反系統的安全政策。 注意：有不同的公認攻擊類別： 「主動攻擊」會嘗試更改系統資源或影響其操作。「被動攻擊」試圖學習或利用系統中的資訊，但不會影響系統資源。 「內部攻擊」是由安全範圍內的實體「內部人員」發起的攻擊 - 即被授權存取系統資源但以未授權授權的方式使用它們的實體。 由系統的未授權或非法使用者（包括從安全邊界外部攻擊的內部人員）從外圍發起「外部攻擊」。 潛在的外部攻擊者包括業餘惡作劇者、有組織犯罪分子、國際恐怖分子和敵對政府。
10	攻擊樹	attack tree	找到攻擊系統安全性的方法的正式、有條理的方法。
11	稽核	audit	對記錄和活動進行獨立檢視和檢查，以評估系統控制的充分性，確保遵守既定政策和操作程序，並建議對控制、政策或程序進行必要的修改。 注意：有三種形式的稽核。 （1）外部稽核由非本組織的員工或承包商進行。 （2）內部稽核由專門負責內部稽核的獨立組織單位進行。（3）控制措施的自我評估由部門功能的對等成員交互進行。
12	驗證	authenticate	驗證使用者、使用者設備或其他實體的身份，或者在資訊系統中儲存、傳輸或以其他方式暴露於未經授權的修改的資料的完整性，或建立傳輸的有效性。
13	身份驗證	authentication	用以確定傳輸、訊息或發起者的有效性的安全措施，或驗證個人接收特定類別資訊的授權的手段。
14	授權	authorization	權限或授予系統實體存取系統資源的權限。
15	自動車輛	automated vehicle	可移動的設備，包括一個控制系統，允許它自動或遠端控制進行移動。
16	可用性	availability	資產在其可靠性、可維護性和安全性的綜合影響下，能夠在規定的時間段內或在特定的時間點履行其所需的功能的概率。

17	基本製程控制系統	Basic Process Control System, BPCS	BPCS 系統泛指一切與安全無關對受控設備進行控制的系統或裝置，主要執行功能是： ● 在預先設定的操作條件下控制過程，優化工廠操作以生產高品質的產品，並嘗試將所有過程變量保持在其安全限制內。 ● 通過操作員控制台提供操作員界面以進行監視和控制（人機界面） ● 提供警報/事件記錄和趨勢設施 ● 產出生產資料報告
18	界限	border	實體或邏輯安全區域的邊緣或邊界。
19	殭屍網路	botnet	自動運作的軟體機器人或機器人的集合。 注意：殭屍網路的發起人可以遠端控制該群組軟體機器人，可能是出於惡意目的。
20	邊界	boundary	以軟體、硬體或其他實體障礙限制存取系統全部或系統一部分。
21	頻道	channel	在通信管道內建立的特定通信鏈路（見第 27 項管道 」）。
22	密文	ciphertext	已通過加密轉換的資料，使其語義資訊內容（即其含義）不再可理解或直接可用。
23	終端	client	從伺服器應用程式接收或請求服務或資訊的設備或應用程式。
24	商用現成產品	Commercial Off-The-Shelf，COTS	商用現貨軟體是指通過通常的商業行為和確定的市場價格進行銷售或交易的產品。 注意：採用商用現貨一般可獲得最新的技術和最快的達成方案，但產品通常只具有很低的、商業級的安全措施或者根本沒有安全考慮。
25	通信路徑	communication path	一個或多個目標之間的邏輯連接，兩端或是多邊客體可以是設備、實體過程、資料項，命令或應用程式介面。 注意：通信路徑不僅限於有線或無線網路，還包括其他通信方式，如記憶體，呼叫軟體程序、實體工廠狀態、可攜式媒體和人機互動。
26	通信安全	communication security	（1）在通信系統中實施和保證安全服務的措施，特別是那些提供資料機密性和資料完整性以及對通信實體進

			行認證的措施。 （2）通過應用安全服務達到的狀態，特別是資料機密性、完整性和成功通過認證的通信實體的狀態。 注意：該短語（phrase）通常被理解為包括加密演算法和密鑰管理方法和過程，達成它們的設備以及密鑰材料和設備的生命週期管理。 但是，加密演算法和密鑰管理方法和過程可能不適用於某些控制系統應用程式。
	通信系統	communication system	硬體、軟體和傳播介質的安排，以允許訊息 從一個應用程式傳輸到另一個應用程式。
27	破解	compromise	未經授權的揭露、修改、替換或使用資訊（包括明文加密密鑰和其他關鍵安全參數）。
28	管道	conduit	通信資產的邏輯分組，用於保護其包含的通道的安全性。 注意：這類似於實體管道保護電纜免受實體損壞的方式。
29	機密性	confidentiality	保證資訊不會洩露給未經授權的個人、流程或設備。
30	控制中心	control center	用於維運一組資產的中心位置。 注意：基礎設施提供商通常使用一個或多個控制中心來監督或協調其營運。 如果有多個控制中心（例如，位於不同站點的備份中心），則它們通常通過廣域網連接在一起。 控制中心包含 SCADA 主 IT 和相關的操作員顯示設備以及諸如歷史記錄的輔助資訊系統 。 注意 ： 在某些產業中，可能更常用「控制室」這個術語。
31	控制設備	control equipment	包括分散式控制系統、可程式邏輯控制器、SCADA 系統、相關操作員界面控制台以及用於管理和控制過程的現場感應和控制設備的課程。 注意：該術語還包括現場總線網路，其中控制邏輯和演算法在相互協調動作的智慧電子設備上執行，以及用於監視過程和用於維護過程的系統的系統。
32	控制網路	control network	時間關鍵型網路，通常連接到控制實體過程的設備（參見 第 100 項「安

			全網路」） 注意：控制網路可以細分為區域，並且在一個公司或站點內可以有多個單獨的控制網路。
33	成本	cost	對可以衡量的組織或個人的影響的價值。
34	對策	countermeasure	通過消除或阻止威脅、弱點或攻擊來減少威脅、弱點或攻擊的行為、設備、程序或技術，通過最小化它可能造成的傷害，或通過發現和 報告它以便採取糾正措施。 注意：術語「控制」也用於在某些情況下描述此概念。 已經為本指南選擇了對策一詞，以避免在「過程控制」的背景下與單詞控制混淆。
35	加密演算法	cryptographic algorithm	基於密碼學的算法，包括加密演算法、加密雜湊算法、數位簽名算法和密鑰協商算法。
36	加密密鑰	cryptographic key	輸入參數改變加密演算法執行的轉換。 注意：通常簡稱為「密鑰」。
37	資料機密性	data confidentiality	未向任何未經授權的系統實體提供或揭露資訊的財產，包括未經授權的個人，實體或程序。
38	資料完整性	data integrity	未經授權或以意外方式更改、銷毀或遺失資料的財產。 注意：該術語涉及資料值的恆定性和可信度，而不是以值表示的資訊或值的來源的可信度。
39	解密	decryption	使用加密演算法和密鑰將密文更改為明文的過程。
40	縱深防禦	defense in depth	提供多重安全保護，尤其是分層安全保護，如果不能防止攻擊，用意在延遲攻擊的進展。
41	非軍事區	demilitarized zone, DMZ	在內部和外部網路之間邏輯上的外圍網段。 注意：非軍事區的目的是強制執行內部網路的外部資訊交換政策，並為外部不受信任的來源提供對可釋放資訊的限制存取，同時保護內部網路免受外部攻擊。 注意：在工控物聯網的背景下，術語「內部網路」通常應用於作為主要保護焦點的網路或網段。 例如，當連

			接到「外部」業務網路時，控制網路可以被視為「內部」。
42	阻斷服務攻擊	denial of service, DoS	阻止或中斷對系統資源的授權存取或延遲系統操作和功能。 注意：在工控物聯網的背景下，阻斷服務可以指過程功能的遺失，而不僅僅是資料通信的遺失。
43	數位簽章	digital signature	資料加密轉換的結果，當正確實施時，提供原始認證、資料完整性和簽名者不可否認性服務。
44	分散式控制系統	distributed control system	控制系統的類型，其中系統元件分散但以耦合方式操作。 注意：分散式控制系統的耦合時間常數可能比 SCADA 系統中常見的短。 注意：分散式控制系統通常與連續過程相關，如發電; 石油和天然氣精煉; 化學，製藥和造紙，以及汽車和其他商品製造，包裝和倉儲等離散工藝。
45	領域	domain	由安全政策，安全模型或安全體系結構定義的環境或情境，包括一組系統資源和有權存取資源的系統實體集。
46	竊聽	eavesdropping	未經授權方監控或記錄通信資訊。
47	電子安全	electronic security	為防止對關鍵系統或資訊資產的未經授權的使用、阻斷服務、修改、揭露、損失或損壞的必要的行動。 注意：目標是降低造成人身傷害或危害公共健康、喪失公眾或消費者信心，揭露敏感資產，未能保護商業資產或未遵守法規的風險。 這些概念適用於生產過程中的任何系統，包括獨立和聯網元件。 系統之間的通信可以通過內部訊息傳遞，也可以通過任何人或機器介面來驗證、操作、控制或與這些控制系統中的任何一個交換資料。 電子安全包括識別、認證、責任、授權、可用性和隱私的概念。
48	加密	encryption	將明文加密轉換為密文，隱藏資料的原始含義以防止其被人知曉或使用。 注意：如果轉換是可逆的，則對應的反轉過程稱為「解密」，這是將加密資料復原到其原始狀態的轉換。
49	企業	enterprise	生產或運輸產品或營運和維護基礎設

			施服務的商業實體。
50	企業系統	enterprise system	整合資訊技術元素（即硬體、軟體和服務）於應用系統，用以提供在輔助組織的業務、管理或專案流程的順利運作的資訊或自動之作業。
51	受控制設備	equipment under control,EUC	用於製造、加工、運輸、醫療或其他活動的設備、機械、設備或工廠。
52	現場 I / 0 網路	field I/O network	將感應器和執行器連接到控制設備的通信鏈路（有線或無線）。
53	防火牆	firewall	網路間連接設備，限制不同連接網路之間的資料通信流量、路徑及通信協定，防止非授權或非預期的網路連接。 注意：防火牆可以是安裝在一般 IT 上的應用程式，也可以是在網路上轉發或拒絕/丟棄資料封包的專用平台（設備）。 通常，防火牆用於定義區域邊界。 防火牆通常具有限制哪些介面打開的規則。
54	閘道器	gateway	連接到兩個（或多個）IT 網路的中繼機制，這些 IT 網路具有相似的功能但實作方式不同，並且使一個網路上的主機能夠與另一個網路上的主機通信。 注意：也稱為中間系統，它是兩個 IT 網路之間的轉換介面。
55	地理站點	geographic site	企業的實體、地理或邏輯資產群組的子集合。 注意：地理站點可能包含區域、生產線、製程細胞、製程單元、控制中心和車輛，並且可能通過廣域網連接到其他站點。
56	保護	guard	插入在不同安全等級（一個網路通常比另一個網路更安全）的兩個網路（或 IT 或其他資訊系統）之間的閘道器，並且 可信任調解兩個網路之間的所有資訊傳輸，以確保不敏感來自更安全網路的資訊被洩露給不太安全的網路，或者保護更安全網路上資料的完整性。
57	主機	host	連接到通信子網或網路間的電腦，可以使用網路提供的服務與其他連接系統交換資料。
58	人機操作	Human-Machine	人機介面最簡單的定義是，在人員與

	介面	Interface, HMI	機器之間，透過某種介面，人能夠對機器下達指令，機器則能夠透過此介面，將執行狀況與系統狀況回報給使用者，換言之，正確的在人機之間傳達訊息以及指令，就是人機介面的主要定義。 人機介面設計出來，所需要達成的目標，卻不僅僅是單一的命令與回饋，反而相當複雜，主要分為四個面向： 1、發揮機器本身應有的功能。 2、提高機器的使用效率與發揮效能。 3、確保使用中之機器或系統在對使用者友善的情況下，能更經濟與安全，延長使用週期。 4、符合使用者的生理、心理需求，提高使用滿意度。
59	工業自動化和控制系統	industrial automation and control systems	集合直接或間接影響工業製程安全、可靠和可靠運作的人員、硬體和軟體元件成為一個運作互動系統。 注意：這些系統包括但不限於： a. 工業控制系統，包括分散式控制系統（DCS）、可程式邏輯控制器（PLC）、遠端終端單元（RTU）、智慧電子監控和資料採集（SCADA），網路電子傳感和控制以及監控和診斷系統。 在此背景下，過程控制系統包括基本過程控制系統和安全儀表系統(SIS）功能，無論它們是實體上分離還是整合。 b.相關資訊系統，如高級或多變量控制、線上優化器、專用設備監視器、圖形界面、過程歷史記錄、製造執行系統和工廠資訊管理系統。 c. 用於為連續、批次、離散和其他製程提供控制，安全和製造操作功能的相關內部的人、網路或機器介面。
60	初始風險	initial risk	施加控制措施或對策之前的風險。
61	內部人員	insider	「信任」的人、員工、承包商或供應商，其資訊通常不為公眾所知（參見第 77 項「外部人員」 ）。
62	完整性	integrity	系統的品質反映了作業系統的邏輯正確性和可靠性，達成保護機制的硬體

			和軟體的邏輯完整性，以及資料結構的一致性和儲存資料的出現。 注意：在正式的安全模式中，完整性通常被解釋得更為狹窄，意味著防止未經授權的修改或破壞資訊。
63	攔截	interception	捕獲和公開訊息內容或使用流量分析來基於訊息目的地或來源地、頻率或傳輸長度以及其他通信屬性來危害通信系統的機密性。
64	界面	interface	邏輯入口或出口點，提供對邏輯資訊流的模組的存取。
65	入侵	intrusion	未經授權的危害系統的行為。
66	入侵檢測	intrusion detection	用於監視和分析系統事件，以便以未經授權的方式搜尋並提供即時或接近即時的警告，以嘗試存取系統資源的安全服務。
67	IP 地址	IP address	使用 Internet 協議和其他協議分配用於識別和通信的 IT 或設備的地址。
68	國際標準化組織	International Organization for Standardization	成立於 1947 年 2 月 23 日，制定全世界工商業國際標準的國際標準建立機構。 ISO 總部設於瑞士日內瓦，成員包括 162 個會員國。該組織定義為非政府組織，官方語言是英語、法語和俄語。參加者包括各會員國的國家標準機構和主要公司。 ISO 與負責電子設備標準的國際電工委員會密切合作。
69	密鑰管理	key management	在加密系統的生命週期中處理和控制加密密鑰和相關材料（如初始化值）的過程，包括申請、產出、分發、儲存、載入、託管、歸檔、審核和銷毀密鑰及相關資料。
70	產線、單元、細胞	lines, units, cells	執行製造、現場設備控制或車輛功能的低階基礎元素。 注意：此等級的實體可以通過區域控制網路連接在一起，並且可以包含與在該實體中執行的操作相關的資訊系統。
71	區域網路	local area network，LAN	通信網路用以連接有限地理區域（通常不到 10 公里）的 IT 和其他智慧設備。
72	惡意程式	malicious code	為收集系統或使用者資訊、破壞系統

	碼		資料，為進一步入侵系統提供立足點，偽造系統資料和報告，或為系統操作和維護人員提供耗時的煩惱而編寫的程序或程式碼。 注意：惡意程式碼攻擊可能採取病毒、蠕蟲、特洛伊木馬或其他自動攻擊的形式。 注意：惡意程式碼通常也稱為「惡意軟體」。
73	製造業務	manufacturing operations	收集生產、維護和品質保證操作及其與生產設施其他活動的關係。 注意：製造業務包括： a. 製造或加工設施活動，協調將原材料或零件轉換為產品所涉及的人員，設備和材料。 b.可以由實體設備、人力和資訊系統執行的功能。 c. 管理有關製造工廠內所有資源（人員、設備和材料）的時間表、使用、能力、定義、歷史和狀態的資訊。
74	製造執行系統 工廠營運管制系統	Manufacturing Execution System, MES	是用來幫助企業從接獲訂單、進行生產、流程控制一直到產品完成，主動收集及監控制造過程中所產生的生產資料，以確保產品生產品質的應用軟體。
75	不可否認性	nonrepudiation	提供保護、防止虛假拒絕參與通信的安全服務。
76	開放平台通信	Open Platform Communications, OPC	在製程控制環境中交換資訊的規範集。 注意：縮寫「OPC」最初來自「用於過程控制的 OLE」，其中「OLE」是「對象鏈接和嵌入」的縮寫。 開放平台通訊的設計目的是提供 Windows-based 軟體應用程式以及程式控制硬體共同的橋樑。規範中定義從車間樓層裝置存取現場裝置的一致性方法。不論資料的來源及型態如何，方法都是不變的。某一硬體裝置的 OPC 伺服器提供 OPC Client 存取資料的方式，和其他裝置的 OPC 伺服器提供的方式都是一樣的。目的是為了減少硬體設計者、軟體合作廠商、SCADA 及 HMI 廠商花在處理這類問

			題，建立相關介面上的心力。只要硬體製造商針對其硬體裝置開發了 OPC 伺服器，他們的工作就已經完成，任何裝置都可以存取其資訊，只要 SCADA 製造商開發了 OPC client，就可以存取 OPC 相同的硬體。 OPC 伺服器提供方法給許多不同的軟體套件（前提是這些軟體要是 OPC client），讓程式控制裝置（例如 PLC、DCS）來存取資料。傳統上，若軟體需要從一個裝置存取資料，需要撰寫客製的介面（驅動程式）。OPC 的目的就是定義共同的介面，只要開發一次，任何 SCADA、人機介面或是電腦軟體都可以用此介面存取資料。新的 OPC UA（OPC Unified Architecture）已經有對應的規範，並且其早期 Adopters 版本已經部署並且進行測試。OPC UA 可以用 Java、Microsoft .NET、C 語言達成，避免了早期 OPC 版本需要用 Microsoft Windows 為基礎的系統才能達成的問題。UA 結合了現有 OPC 介面的功能，又加入了像 XML 及 Web Services 等技術，來支援高階的製造執行系統（MES）及企業資源計劃（ERP）等應用。 OPC 組織和 MTConnect 組織在 2010 年 9 月 16 日宣布會彼此合作，讓兩個標準之間有一致性及互操作性。
77	外部人員	outsider	內部存取不「信任」的人或團體，目標組織可能知道也可能不知道（參見「 內部人士 」）。
78	滲透	penetration	成功未經授權存取受保護的系統資源。
79	網路釣魚	phishing	通過提供偽造的電子郵件誘使收件人存取看起來與合法來源相關聯的網站，誘使受害者洩露資訊的安全攻擊類型。
80	明文	plaintext	未加密的資料，由加密過程輸入或轉換，或由解密過程輸出。
81	特權	privilege	授權或授權集以執行特定功能，尤其

			是在 IT 作業系統的環境中。 注意：通過使用權限控制的功能實例包括確認警報、 更改設定值和修改控制算法。
82	製程	process	在製造，處理或運輸產品或材料時執行的一系列操作。 注意：本指南廣泛使用術語「製程」來描述工控物聯網控制下的設備。
83	可程式化邏輯控制器	Programming Logic Control, PLC	一種具有微處理器的數位電子裝置，用於自動化控制的數位邏輯控制器，可以將控制指令隨時載入記憶體內儲存與執行。可程式控制器由內部 CPU，指令及資料記憶體、輸入輸出單元、電源模組、數位類比等單元所模組化組合成。PLC 可接收（輸入）及發送（輸出）多種型態的電氣或電子訊號，並使用他們來控制或監督幾乎所有種類的機械與電氣系統。 最初的可程式化序邏輯控制器只有電路邏輯控制的功能，所以被命名為可程式邏輯控制器，後來隨著不斷的發展，這些當初功能簡單的電腦模組已經有了包括邏輯控制，時序控制、類比控制、多機通訊等許多的功能，名稱也改為可程式控制器（Programmable Controller），但是由於它的簡寫也是 PC 與個人電腦（Personal Computer）的簡寫相衝突，也由於多年來的使用習慣，人們還是經常使用可程式邏輯控制器這一稱呼，並在術語中仍沿用 PLC 這一縮寫。
84	協議	protocol	一組規則（即格式和程序）來達成和控制系統之間的某種類型的關聯（例如，通信）。
85	參考模型	reference model	允許以一致的方式描述系統的模組和介面的結構
86	可靠性	reliability	系統在規定條件下在指定時間段內執行所需功能的能力。
87	遠端存取	remote access	使用位於安全區域周邊內的系統，該系統從不同的地理位置處理，具有與在該位置實際存在時相同的權限。 注意：「遠端」的確切定義可能因情況而異。 例如，存取可能來自遠離

			特定區域但仍在公司或組織邊界內的位置。 這可能比存取來自遠離公司邊界的位置的存取風險更低。
88	遠端客戶端	remote client	控制網路外部的資產，其通過通信鏈路臨時或永久地連接到控制網路內的主機，以便直接或間接地存取控制網路上的控制設備的部分。
89	否認	repudiation	參與通信的一個實體拒絕參與全部或部分通信。
90	殘餘風險	residual risk	採用安全控制措施或對策後的剩餘風險。
91	風險	risk	對損失的期望表示為特定威脅利用具有特定後果的特定弱點的概率。
92	風險評估	risk assessment	系統地識別有價值的系統資源的潛在弱點和對這些資源的威脅的過程，根據發生的可能性量化損失風險和後果，並（可選）建議如何將資源分配給對策以最小化總暴露。 注意：資源類型包括實體，邏輯和人工。 注意：風險評估通常與弱點評估相結合，以識別弱點並量化相關風險。 它們最初和定期進行，以反映組織的風險承受能力，脆弱性，程序，人員和技術變化的變化。
93	風險管理	risk management	根據風險評估確定和應用與受保護資產價值相對應的對策的過程。
94	風險緩解控制	risk mitigation controls	對策和業務持續性計劃的組合。
95	基於角色的存取控制	role-based access control	基於身份的存取控制的形式，其中被識別和控制的系統實體是組織或過程中的功能位置。
96	路由器	router	OSI 第 3 層的兩個網路之間的閘道器，通過該網路中繼和引導資料封包。 最常見的路由器形式傳遞 Internet 協議（IP）資料封包。
97	安全	safety	免於不可接受的風險。
98	安全儀表系統	safety-instrumented system, SIS	系統用於達成一個或多個安全儀表功能。 注意：安全儀表系統由感應器，邏輯解算器和執行器的任意組合組成。
99	安全完整性等級	safety integrity level	離散水準（四分之一），用於指定安全儀表功能的安全完整性要求，分配給安全儀表系統。

			註：安全完整性等級 4 具有最高等級的安全完整性; 安全完整性等級 1 最低。
100	安全網路	safety network	連接安全儀表系統以進行安全相關資訊通信的網路。
101	秘密	secret	任何系統實體都不知道資訊的條件，除了那些打算知道它的人。
102	安全	security	1.為保護系統而採取的措施。 2.建立和維護保護系統措施所產生的系統狀況。 3.系統資源不受未經授權的存取以及未經授權或意外更改，破壞或遺失的情況。 4.基於 IT 的系統能夠提供充分的信心，使未經授權的人員和系統既不能修改軟體及其資料，也不能獲得對系統功能的存取權限，同時確保不會拒絕授權人員和系統]。 5.防止非法或不必要地滲透或干擾工控物聯網的正常和預期操作。 注意：度量可以是與實體安全性（控制對計算資產的實體存取）或邏輯安全性（登錄到特定系統和應用程式的能力）相關的控制。
103	安全架構	security architecture	描述系統需要提供的安全服務的計劃和原則的集合，以滿足其使用者的需求，達成服務所需的系統元素以及處理威脅環境所需的效能等級。 注意：在此情境中，安全體系結構將是一種保護控制網路免受有意或無意安全事件的體系結構。
104	安全審核	security audit	對系統的記錄和活動進行獨立檢視和檢查，以確定系統控制的充分性，確保遵守既定的安全政策和程序，檢測安全服務中的違規行為，並建議針對反措施指出的任何變更。
105	安全元件	security components	用於提高工控物聯網安全效能的防火牆，認證模組或加密軟體等資產（參見第 34 項「對策」 ）。
106	安全控制	security control	參考第 34 項「對策」
107	安全事件	security incident	系統或網路中的不良事件或此類事件發生的威脅。 注意：術語「接近未命中」有時用於描述可能在稍微不同的情況下發生事

			件的事件。
108	安全入侵	security intrusion	安全事件或多個安全事件的組合，構成的安全事故，入侵者在未經授權的情況下獲得或試圖獲取對系統（或系統資源）的存取權。
109	安全等級	security level	根據對區域或管道風險的評估，對應於對策所需的有效性和區域或管道的裝置和系統的固有安全效能。
110	安全目標	security objective	要達成的安全方面是使用某些緩解措施的目的和目標，例如機密性、完整性，可用性、使用者真實性、存取授權及可歸責性。
111	安全範圍	security perimeter	安全政策或安全體系結構所適用的域的邊界（邏輯或實體），即安全服務保護系統資源的空間邊界。
112	安全效能	security performance	計劃的合規性，提供特定威脅防護的措施的完整性，折衷後分析，不斷變化的業務要求檢視，新的威脅和弱點資訊，以及對控制系統的定期稽核，以確保安全措施保持有效和適當。 注意：評估安全實踐效能需要測試、審核、工具、度量或其他方法。
113	安全政策	security policy	一套規則，用於指定或規範區域、系統或組織如何提供安全服務以保護其資產。
114	安全程序	security procedures	確切地說如何實施和執行實踐的定義。 注意：安全程序通過人員培訓和使用當前可用和已安裝技術的操作來實施。
115	安全計劃	security program	管理安全的所有方面的組合，從政策的定義和溝通到最佳產業實踐的實施以及持續的營運和稽核。
116	安全服務	security services	用於提供機密性、資料完整性、身份驗證或不洩露資訊的機制。
117	安全違規	security violation	通過入侵或善意內幕人士的行為違反或以其他方式違反安全政策的行為或事件。
118	安全區域	security zone	對具有共同安全要求的邏輯或實體資產進行分組。 注意：應假定本指南中「區域」一詞的所有不合格用途均指安全區。 注意：區域與其他區域具有清晰的邊界。區域的安全政策通常由區域邊緣

			和區域內的機制組合強制執行。區域可以是分層的，因為它們可以由子區域集合組成。
119	感應器和執行器	sensors and actuators	連接到過程設備和控制系統的測量或驅動元件。
120	伺服器	server	為客戶端應用程式和設備提供資訊或服務的設備或應用程式。
121	側錄	sniffing	見第 63 項「 攔截」。
122	偽冒	spoof	假裝是授權使用者並執行未經授權的行為。
123	監督控制和資料採集系統	supervisory control and data acquisition (SCADA) system	通常與電力輸配系統，石油和天然氣管道以及供水和排污系統相關的鬆散耦合的分散式監測和控制系統。 注意：監控系統也用於批次，連續和離散製造工廠，以集中監控這些站點的活動。
124	系統	system	相互作用，相互關聯或相互依存的元素形成一個複雜的整體。
125	系統軟體	system software	專用於特定 IT 系統或 IT 系統系列的專用軟體，便於 IT 系統及相關程序和資料的操作和維護。
126	威脅	threat	違反安全的可能性，當存在可能破壞安全並造成傷害的情況、能力、行動或事件時存在。
127	威脅行動	threat action	攻擊系統安全。
128	流量分析	traffic analysis	即使在資料被加密或不能直接獲得時，也可以從資料流的可觀察特徵推斷資訊，包括來源和目的地的身份和位置以及存在、數量、頻率和持續時間發生。
129	特洛伊木馬	trojan horse	IT 程序似乎具有有用的功能，但也有一個隱藏的和潛在的惡意功能，逃避安全機制，有時通過利用調用程序的系統實體的合法授權。
130	使用情境	use case	用於捕獲潛在功能需求的技術，其使用一個或多個場景來傳達系統應如何與最終使用者或另一系統互動以達成特定目標。 注意：通常，使用情境將系統視為黑盒子，並且與系統的互動（包括系統回應）是從系統外部感知的。使用情境很受歡迎，因為它們簡化了需求的描述，並避免了對如何達成此功能的假設的問題。

131	使用者	user	存取系統的人，組織實體或自動化過程，無論是否有權這樣做。
132	病毒	virus	自我複製或自動傳播有惡意程式碼，通過將自身的副本插入其他可執行程式碼或文件進行傳播。
133	弱點	vulnerability	系統的設計、實施或操作和管理中的缺陷或弱點，可能被利用來違反系統的完整性或安全政策。
134	廣域網路	wide area network, WAN	通信網路用以連接遠距離的 IT、網路和其他設備，如全國或世界。
135	竊聽	wiretapping	攔截和存取通信系統中流中包含的資料和其他資訊的攻擊。 注意：儘管該術語最初指的是與連接兩個節點的電導體進行機械連接，但它現在用於指從用於鏈路的任何介質或甚至直接從節點（例如閘道器）讀取資訊或子網交換機。 注意：「主動竊聽」會嘗試更改資料或以其他方式影響流量; 「被動竊聽」只是試圖觀察流動並獲得其所包含資訊的知識。
136	蠕蟲	worm	可以獨立運作的 IT 程序，可以將自身的完整工作版本傳播到網路上的其他主機上，並可能破壞性地消耗 IT 資源。
137	區域	zone	參見 第 118 項「 安全區域 」

主 辦 單 位：經濟部工業局

受委託單位：財團法人工業技術研究院

執 行 單 位：台北市電腦商業同業公會