經濟部

工控設備業工控物聯網資安實務指南

中華民國108年12月10日

前言

隨著全球數位科技快速發展與網路服務普及應用，政府「5+2」產業創新計畫積極推動產業邁向智慧製造，然而物聯網資安已成為各界關注的焦點，經濟部工業局為協助產業界之製造場域順利導入物聯網資安應用，特研訂產業資安實務指南提供企業規劃及導入物聯網資安時之重要依循，其撰寫時係基於「工控物聯網共通性資安應用指南」所述及之知識基礎，並參考「行政院國家資通安全會報-資通安全維護計畫範本」格式。為因應產業別之製造需求及特性，今完成「工控設備產業資安實務指南」（以下簡稱本實務指南），協助企業建構完善工控物聯網安全防護計畫，請企業在參考本實務指南進行工控物聯網安全防護計畫之擬定前，務必先行研讀「工控物聯網共通性資安應用指南」，以期理解工控物聯網環境中，所探討之資安議題，以及與工控物聯網安全防護有關之相關知識；另由於與工控物聯網安全防護所涉之專業術語數量繁多，若有特定術語不明其義或所指原文，請參閱「工控物聯網共通性資安指南-附錄 A-名詞定義」 部分以資明確。

有關企業研擬工控物聯網安全防護計畫之推動重點下：

1. 標定企業內需進行安全管理之範圍，並制訂相關安全政策與管理組織
2. 識別資產及其可能所涉風險，並採取適當防護與控制措施
3. 建立安全事件通報、應變、演練與情資評估因應相關機制
4. 強化系統或服務委外辦理之管理
5. 安全教育訓練之規劃與實施
6. 持續精進及績效管理

目　次

1. 工控物聯網適用範圍 1
2. 工控物聯網工控物聯網安全政策及目標 2
2.1 工控物聯網安全政策 2
2.2 工控物聯網資訊安全目標 3
2.2.1 量化型目標 3
2.2.2 質化型目標： 3
2.2.3 工控物聯網安全政策及目標之核定程序 3
2.2.4 工控物聯網安全政策及目標之宣導 3
2.2.5 工控物聯網安全政策及目標定期檢討程序 4
3. 工控物聯網安全推動組織 5
3.1 工控物聯網安全管理委員會主任委員 5
3.2 工控物聯網安全管理委員會 5
3.3 分工及職掌 6
3.4 人力及經費配置 6
3.4.1 資安人力及資源之配置 6
3.4.2 經費之配置 7
4. 資訊資產管理 9
4.1 資訊資產盤點 9
4.1.1 資訊資產盤點作業 9
5. 工控物聯網安全風險評估 14
5.1 工控物聯網安全風險評估準則 14
6. 工控物聯網安全防護及控制措施 16
6.1 可採取之控制措施及其安全等級（SL-C）分項說明 16
6.1.1 資訊及資訊系統之管理 16
6.1.2 資訊及資訊系統之使用 16
6.1.3 資訊及資訊系統之刪除或汰除 17
6.1.4 網路安全控管 17

6.1.5 資訊系統權限管理 18
6.1.6 特權帳號之存取管理 19
6.1.7 加密管理 19
6.1.8 防範惡意軟體之控制措施 20
6.1.9 遠距工作之安全措施 20
6.1.10 確保實體與環境安全措施 20
6.1.11 資料備份 21
6.1.12 媒體防護措施 21
6.1.13 行動設備之安全管理 22
6.1.14 系統獲取、開發及維護 22
6.1.15 工控物聯網安全防護設備 22
6.2 工控區域(PERA 初級至第三級) 22
6.2.1 工控非軍事區域(Industrial Demilitarized Zone, IDMZ) 23
7. 工控物聯網安全事件通報、應變及演練相關機制 28
8. 工控物聯網安全情資之評估及因應 31
8.1 安全情資之分類評估 31
8.1.1 工控物聯網安全相關之訊息情資 31
8.1.2 入侵攻擊情資 31
8.2 安全情資之因應措施 31
8.2.1 工控物聯網安全相關之訊息情資 31
8.2.2 入侵攻擊情資 31
9. 工控物聯網系統或服務委外辦理之管理 32
9.1 選任受託者應注意事項 32
9.2 監督受託者工控物聯網安全維護情形應注意事項 32
10. 工控物聯網安全教育訓練 33
10.1 安全教育訓練要求 33
10.2 安全教育訓練辦理方式 33
11. 工控物聯網安全防護計畫及實施情形之持續精進及績效管理機制 34
11.1 安全防護計畫之實施 34
11.2 工控物聯網安全防護計畫實施情形之稽核機制 34

11.3 工控物聯網安全防護計畫之持續精進及績效管理 35
12. 參考文獻 37
13. 附件 38
附件 1 系統目標安全等級建議 39
附件 2 元件目標安全等級建議 42
附件 3 威脅樣態與弱點對應 47

圖 目 次

圖 1 工控物聯網普渡企業參考架構（PERA for IIoT）模型 10
圖 2 一般製程資產模型範例 11
圖 3 工控設備 A、B、C 廠區實體參考架構圖 13
圖 4 IDMZ 架構圖 23
圖 5 IDMZ 的 NGFW 建置流程 24
圖 6 IT/OT 安全監控系統架構圖 25
圖 7 安全監控功能對應 PERA 示意圖 25
圖 8 資訊安全事件通報流程圖 28
圖 9 營運持續管理流程圖 29

表 目 次

表 1 工控物聯網資產清冊表範例 12
表 2 風險評估執行範例表 15
表 3 可強化安全控制措施等級表 26
表 4 關鍵任務／資產／衝擊分析表 29
表 5 控制措施目標安全等級表 39
表 6 元件目標安全等級建議表 42
表 7 威脅樣態與弱點對應表 47

1. 工控物聯網適用範圍

本計畫適用範圍涵蓋本公司〇〇廠區之工控設備產品產線相關資訊系統、生產製程設備及基礎設施，以下簡稱「本計畫適用範圍」。

2. 工控物聯網工控物聯網安全政策及目標

2.1 工控物聯網安全政策

為使本公司本計畫適用範圍之工控設備產線業務順利運作，防止資訊或資訊系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其資料流機密性(confidentiality)、完整性(integrity)，生產製程設備及基礎設施之高可用性(high availability)、高可靠度(high reliability)、運作安全(safety)及業務持續性 (Business continuous)，特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立以本公司〇〇廠區之〇〇產品產線工控物聯網為範圍，建立資訊安全風險管理機制，定期因應內外在工控物聯網安全情勢變化，檢討工控物聯網安全風險管理之有效性。

2. 應保護「本計畫適用範圍」企業區與生產製程設備，有關機敏資訊及資訊系統之機密性與完整性，避免未經授權的存取與竄改。

3. 應保護「本計畫適用範圍」內生產製程有關生產機台、輔助基礎設施的高可用性，避免生產機台、製程設備之資料被非授權存取或竄改，資源被刻意耗盡、維持應有的製造流程順暢及遭受攻擊後，可容忍中斷時間內快速復原正常運作。

4. 應強固核心資訊系統及相關生產製程設備之韌性，確保「本計畫適用範圍」業務持續營運。

5. 應因應資訊安全威脅情勢變化，辦理資訊安全教育訓練，以提高「本計畫適用範圍」同仁之資訊安全意識，「本計畫適用範圍」同仁亦應確實參與教育訓練。

6. 員工、監督和管理階層是企業資訊安全中最脆弱的一環，加強宣導，勿開啟來路不明或無法明確辨識寄件人之電子郵件，降低員工等為駭客開啟大門之風險。

7. 禁止多人共用單一資訊系統帳號，如因設備、系統先天性功能限制無法滿足前述要求者，應增設管理程序、安全措施加以控制資訊系統之使用。

8. 應加強資安管控來自供應鏈或第三方系統、元件服務供應商原生風險。

2.2 工控物聯網資訊安全目標

（由組織自行訂定工控物聯網安全目標，目標宜有量化與質化型指標，以下僅例示內容供參）

2.2.1 量化型目標

1.「本計畫適用範圍」核心資訊系統及產線製程設備可用性達 99.99%以上。(中斷時數/總運作時數≤ 0.1%)

2.知悉資安事件發生後，能於 1 小時內完成通報、應變，並於可容忍中斷時間內復原作業。

3.應納入客戶資訊安全要求作為本計畫適用範圍資訊安全控制考量，遇有客戶執行第二方稽核時，未達成之要求項目應低於總要求項目之 5%。

2.2.2 質化型目標：

1.應持續因應法令、組織目標與技術之變動、所造成潛在風險，調整工控物聯網安全政策，以避免或降低下列風險：

(1)因生產相關資訊系統/工控系統或生產資訊/設備遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性，並降低遭受工控物聯網安全風險之威脅。

(2)因工控系統、基礎設施之資訊安全事故造成生產製造效率降低、中斷、製程資料遭竄改造成生產品質下降，甚至造成人員傷亡或財產損失。

2.提升 IT(Information Technology)與 OT(Operational technology)人員資安防護意識、有效偵測與預防內、外部攻擊

2.2.3 工控物聯網安全政策及目標之核定程序

工控物聯網安全政策由本公司◯◯單位簽陳◯◯核定。

2.2.4 工控物聯網安全政策及目標之宣導

1.本公司之工控物聯網安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向公司內所有人員進行宣導，並檢視執行成效。

2.本公司應每年向利害關係人(例如設備、系統、服務供應商、與公司連線作業有關單位)進行工控物聯網安全政策及目標宣導，同時檢視執行成效。

2.2.5 工控物聯網安全政策及目標定期檢討程序

工控物聯網安全政策及目標應定期於工控物聯網安全管理審查會議（或其他足夠高階、涵蓋適用範圍之決策型會議）中檢討其適切性。

3. 工控物聯網安全推動組織

撰寫說明：

本章至少包含資訊安全長(或稱管理代表、主任委員等適足以反映其資訊安全領導職能之職稱)，工控物聯網安全推行組、技術支持、稽核組之組成及分工職掌等內容。組織規模較大者，亦可於資訊安全長下設置資訊安全指導小組及工控物聯網資訊安全推行組,分別負責資訊安全規劃及推動作業，資訊安全長應具有足夠權責、資源、權限、相當資歷、經驗及資安專業之人員兼任為宜，使資訊安全相關業務得以順利推展。組織針對資訊安全推動組織如已有規定及程序者，可直接引述內部文件編號及名稱。

範本：

3.1 工控物聯網安全管理委員會主任委員

組織訂定[○○主管]為工控物聯網安全管理委員會主任委員（該人員應具有足夠權責、資源、權限、相當資歷、經驗及資訊安全專業之人員兼任為宜，使工控物聯網安全相關業務得以順利推展），負責督導「本計畫適用範圍」工控物聯網安全相關事項，其任務包括：

1. 工控物聯網安全管理政策及目標之核定、核轉及督導。
2. 工控物聯網安全責任之分配及協調。
3. 工控物聯網安全資源分配。
4. 工控物聯網安全防護措施之監督。
5. 控物聯網安全事件之檢討及監督。
6. 工控物聯網安全相關規章與程序、制度文件核定。
7. 工控物聯網安全管理年度工作計畫之核定
8. 工控物聯網安全相關工作事項督導及績效管理。
9. 其他工控物聯網安全事項之核定。

3.2 工控物聯網安全管理委員會

為推動本公司之工控物聯網安全政策、落實資訊安全事件通報及相關應變處理，由工控物聯網安全管理委員會主任委員召集「本計畫適用範圍」各業務部門主管/副主管以上之人員代表成立工控物聯網安全管理委員會，其任務包括：

1. 跨部門工控物聯網安全事項權責分工之協調。

2. 應採用之工控物聯網安全技術、方法及程序之協調研議。

3. 整體工控物聯網安全措施之協調研議。

4. 工控物聯網安全防護計畫之協調研議。

5. 其他重要工控物聯網安全事項之協調研議。

3.3 分工及職掌

本公司之工控物聯網安全管理委員會依下列分工進行責任分組，並依工控物聯網安全管理委員會主任委員之指示負責下列事項，本公司工控物聯網安全管理委員會分組人員名單及職掌應列冊，並適時更新之：

1. 推行組：

(1)工控物聯網安全政策及目標之研議。

(2)訂定「本計畫適用範圍」工控物聯網安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

(3)依據工控物聯網安全目標擬定「本計畫適用範圍」年度工作計畫。

(4)傳達公司與「本計畫適用範圍」工控物聯網安全政策與目標。

(5)其他工控物聯網安全事項之規劃。

2. 技術支援組：

(1)工控物聯網安全技術之研究、建置及評估相關事項。

(2)工控物聯網安全相關規章與程序、制度之執行。

(3)資訊及資訊系統之盤點及風險評估。

(4)資料及資訊系統之安全防護事項之執行。

(5)工控物聯網之安全事件其通報及應變機制之執行。

(6)其他工控物聯網安全事項之辦理與推動。

3. 稽核組：

(1)辦理工控物聯網安全內部稽核。

(2)每年定期召開工控物聯網安全管理審查會議，提報工控物聯網安全事項執行情形。

3.4 人力及經費配置

3.4.1 資安人力及資源之配置

「本計畫適用範圍」設置工控物聯網資訊安全人員 4 人，其分工如下，組織現有工控物聯網安全人員名單及職掌應列冊，並適時更新。

1. 工控物聯網安全管理面業務 1 人，負責推動資訊系統安全等級需求分級、工控物聯網安全管理系統導入及驗證、內部工控物聯網安全稽核、公司資安治理成熟度評估、工控物聯網安全管理相關法遵事項業務及教育訓練等業務之推動。

2. 工控系統安全管理業務 1 人，負責工控系統資產盤點、劃分區域與管道、安全等級及防護基準評估與實作、安全性檢測、業務持續運作演練等業務之推動。

3. 工控物聯網安全防護業務 2 人，負責工控物聯網整體工控物聯網安全監控管理機制、安全組態基準導入，工控物聯網安全防護設施建置及工控物聯網安全事件通報及應變業務之推動。

4. 本公司之承辦單位於辦理工控物聯網安全人力資源業務時，應加強工控物聯網安全人員之培訓，並提升公司內工控物聯網安全專業人員之工控物聯網安全管理能力。本公司之相關單位於辦理工控物聯網安全業務時，如工控物聯網安全人力或經驗不足，得洽請相關學者專家或專業公司提供顧問諮詢或派駐委外專業技術服務。

5. 本公司負責重要資訊/工控系統之管理、維護、設計及操作之人員， 應妥適分工並分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

6. 本公司之首長及各級業務主管人員，應負責督導所屬人員之工控物聯網安全作業，防範不法及不當行為。

7. 專業人力資源之配置情形應每年定期檢討，並納入工控物聯網安全防護計畫持續改善機制之管理審查。

3.4.2 經費之配置

1. 工控物聯網安全管理委員會於規劃配置相關經費及資源時，應考量本公司之工控物聯網安全政策及目標，並提供建立、實行、維持及持續改善工控物聯網安全防護計畫所需之資源。

2. 各單位於規劃建置工控物聯網系統建置時，應一併規劃資安防護需求，並於整體預算中分配工控物聯網安全預算所佔之比例5～7%以上，後續維護費用佔原建置資安預算 10～25%。

3. 各單位如有資訊安全資源之需求，應配合公司預算、規劃期程向工控物聯網安全管理委員會推行組提出，由工控物聯網安全管理委員會推行組，審查整體資訊安全資源進行分配，並經資訊安全長核定後，

進行相關之建置。

4. 資訊安全經費、資源之配置情形應每年定期檢討，並納入工控物聯網安全防護計畫與持續改善機制之管理審查。

4. 資訊資產管理

4.1 資訊資產盤點

4.1.1 資訊資產盤點作業

1.「本計畫適用範圍」每年辦理資訊資產盤點，依管理責任指定對應之資產管理人，並依資產屬性的安全區域(security zone) 和保護要求(protection requirement)進行分類，分別為資訊類、軟體類（包含:工業自動化和控制系統(Industrial Automation and Control Systems; IACS）、實體設備類（包含場域生產區域、控制設備區域）、支援服務類等(分類僅供參考，公司可依實際情形調整)

2. 資訊資產分類及項目如下(供參)：

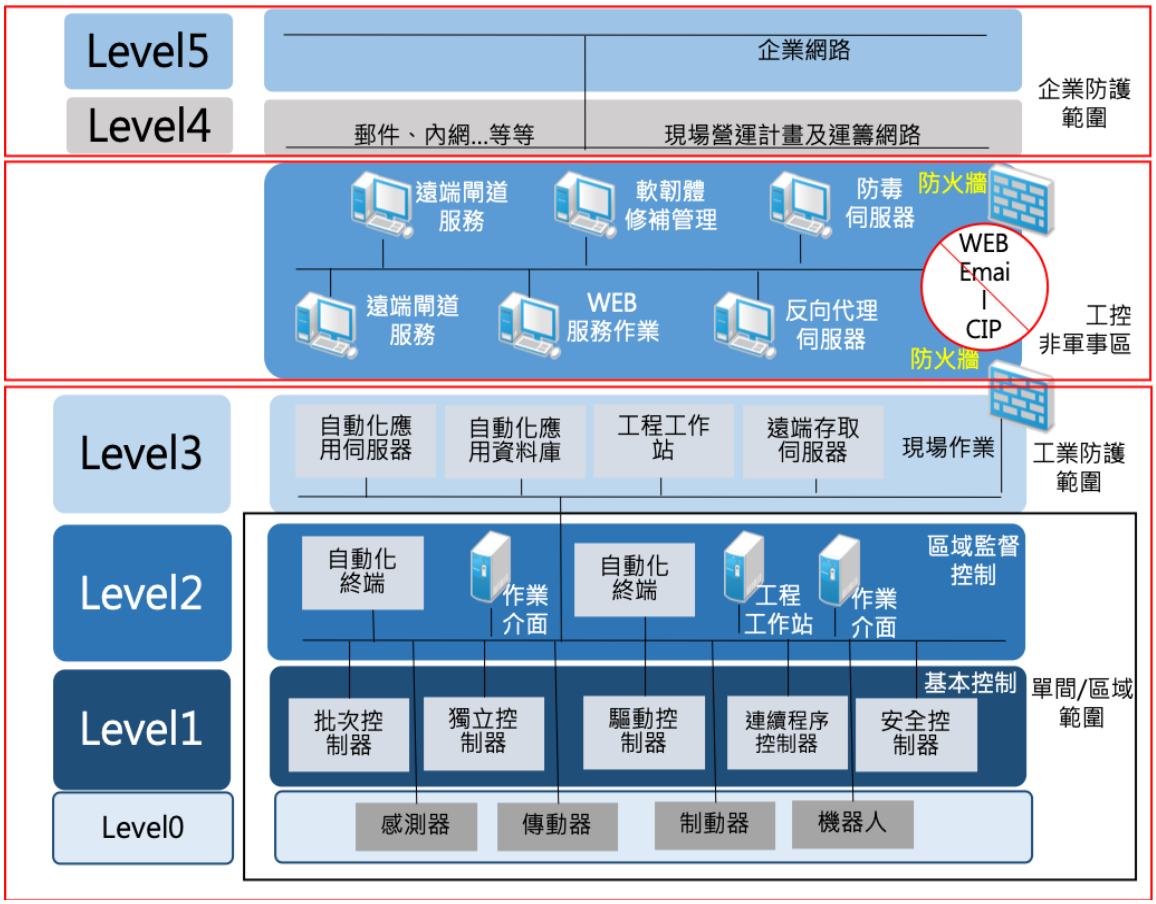
(1)實體設備類資產分區域: 包含的實體設備，舉例如下：

- 電腦硬體（例如:工作站、伺服器、儀器、控制器、電源、硬碟或磁帶備份）
- 網路設備（例如:路由器、交換機、集線器、防火牆或實體電纜）
- 通信鏈路（例如:匯流排、鏈路、數據機（Modem）和其他網路介面、天線）
- 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）
- 開發系統硬體
- 模擬和訓練系統硬體
- 外部系統硬體
- 備品盤點
- 監視和控制設備（例如:感應器、開關和控制器）

(2)軟體類資產包括區域中使用的所有軟體和資料，舉例如下：

- 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、分析工具和工具程式）
- 作業系統和應用程式工具集的修補和升級
- 資料庫軟體
- 供應商資源（例如:產品更新、修補、服務包、工具程式和驗證測試）。

3.資產盤點需參考普渡企業參考架構（Purdue Enterprise Reference Architecture, PERA）模型，簡稱「普渡(Purdue)模型」。將盤點所得資產依屬性放置於 Level 0~Level 5，以檢視其完整性及連線關係。其中包含介於 Level 3 與 Level 4 間的工控非軍事區（Industrial Demilitarized zone, IDMZ），資訊資產盤點結果與普渡模型之對應



關係如圖 1。

圖 1 工控物聯網普渡企業參考架構（PERA for IIoT）模型

4.除了上述分類外，另需參考「工控物聯網共通性資安應用指南」2.1.2 資產型式(Asset Model)，將資產的所在，劃分「企業」、「地理現場」、「本地或遠端區域」、「產線」、「單元」、「單間」、「機動車等」、「控制設備」、「場域 I/O」、「感測器或制動器」，以及將通訊管道區分為「網際網路」、「廣域網路」、「區域或分散網路」、「控制網路」及「I/O 網路」等，將群組資產群組與通訊管道以高階方式描繪其關聯圖，前述關聯圖之範例詳見圖 2。

圖 2 一般製程資產模型範例

5. 組織應每年 6 月及 12 月依系統盤點結果，製作「工控物聯網資訊資產清冊」，欄位可包含：資產類別、資產名稱、擁有者、管理者、使用者、存放位置、控制措施安全等級及目標安全等級，參考盤點結果如表 1。

註：有關控制措施安全等級（SL-C）、目標安全等級（SL-T）、現況安全等級（SL-A）之定義及判定方式，請參考「工控物聯網共通性資安指南」-2.5.2-安全等級類別相關章節說明（後續章節相關用詞亦同）。

表 1 工控物聯網資產清冊表範例

資產類別	資產名稱	擁有者	管理者	使用者	存放位置
實體資產	應用程式主機	○○部	王○○	陳○○	企業區
實體資產	資料庫主機	○○部	王○○	陳○○	企業區
實體資產	網頁伺服器 2 台	○○部	王○○	陳○○	企業區
實體資產	生產線控制電腦計 3 台	○○部	王○○	陳○○	產線區
實體資產	生產線控制電腦參數儲存主機 1 台	○○部	王○○	陳○○	產線區
實體資產	料件搬運車	○○部	王○○	陳○○	產線區
實體資產	錫膏印刷機	○○部	王○○	陳○○	產線區
實體資產	DIP 插件機	○○部	王○○	陳○○	產線區
實體資產	回焊爐	○○部	王○○	陳○○	產線區

6. 資訊資產應以標籤標示於設備明顯處，並載明財產編號、保管人、廠牌、型號等資訊。核心資訊系統及相關資產，並應加註標示。

7. 各單位管理之資訊資產如有異動，應即時通知工控物聯網安全管理委員會推行組更新資產清冊。

8. 繪製工控物聯網實體架構圖（請參考工控物聯網共通性資安應用指南 2.1.3）以並劃分「區域」及所需「管道」，前述架構圖之示意如圖 3。

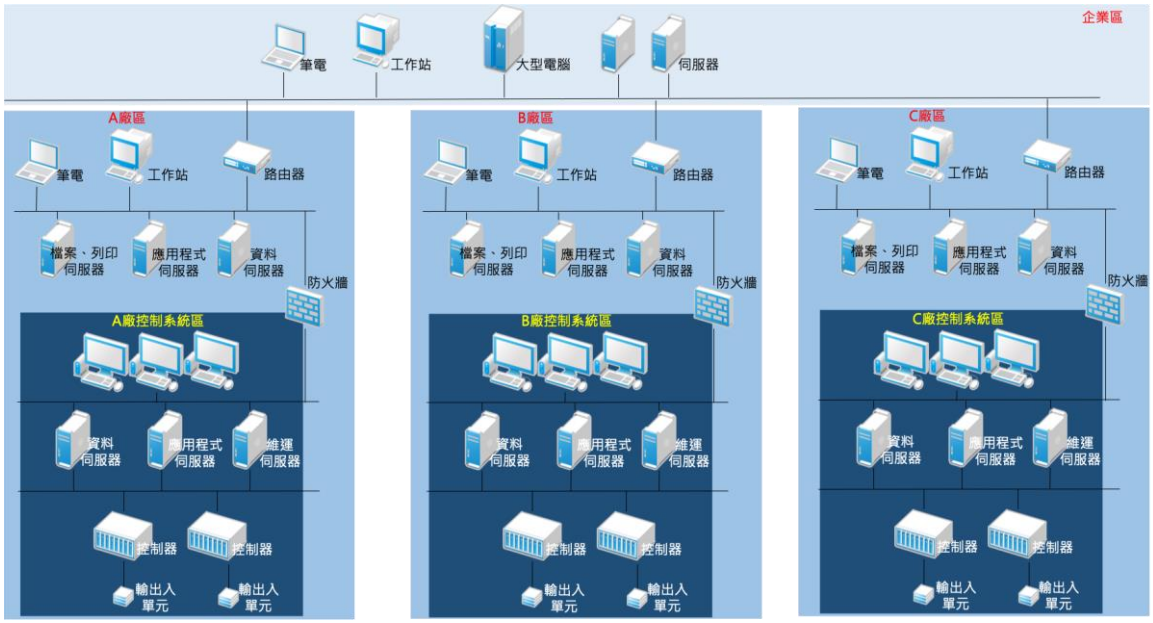


圖 3 工控設備 A、B、C 廠區實體參考架構圖

5. 工控物聯網安全風險評估

5.1 工控物聯網安全風險評估準則

1. 應每年針對「本計畫適用範圍」資訊及工控系統資產進行風險評估。
2. 執行風險評估時應參考相關國際標準及最佳實務，例如 ISO 27005、ISO31000、NIST SP 800-39，或參考 IEC 62443-2-1 並依其中之高階與詳細風險評鑑方法進行風險評估之工作。
3. 威脅和弱點評估

   在「本計畫適用範圍」企業區（PERA 之 Level 4~5）已建置完善資訊安全管理制度，各項資訊安全體系管理活動由品質管理部追蹤管考，並定期通過外部第三方驗證，平均的現況安全等級（SL-A）落在第 3 級。

   在○○產線（PERA 之 Level 0~3）鑑別出重要資產的價值與對應威脅／弱點之填表範例如表 2，以下針對該表中各欄位之填具與評估方式逐欄進行說明：

   （1）所在位置：係指該資產實際存放位置，例如○○廠區、○○產線、○○辦公室。

   （2）系統/元件：係指該資產於整體生產/控制任務中，所擔任之角色。

   （3）資產名稱：該資產之可識別名稱。

   （4）資產價值：可由該資產若遭到侵害，對組織可能造成的損失進行判定，組織可以量化方式制訂可能造成之損失金額區間，判定其高（3）中（2）低（1）分數，或僅由概念性之認定，推斷其高（3）中（2）低（1）分數。

   （5）威脅列表：該資產可能遭受何種型態之侵害，各項資產可能遭受的威脅，可參見「附件 3 – 威脅樣態與弱點對應」。

   （6）威脅等級：可由組織自身/同業遭受相關威脅之頻率，或近期較常聽聞及之攻擊趨勢進行判定，亦可參考「附件 3– 威脅樣態與弱點對應」中之建議值。

   （7）弱點列表：該資產面對特定威脅，可能遭利用之控管不良樣態，各項資產可能具備的弱點，可參見「附件 3– 威脅樣態與弱點對應」。

   （8）控制措施：針對該資產面對特定威脅，組織已採行之控制措施說明。

（9）控制措施安全等級（SL-C）：組織已採行之控制措施強度，可參考請參考「工控物聯網共通性資安指南」-2.5.2-安全等級類別相關章節說明，針對現行控制措施安全等級進行判定。

（10）弱點等級：組織自身對威脅之控制能力，可由前述控制措施安全等級進行判定：

- 若控制措施安全等級為 2~4，則弱點等級為 1，表示此項弱點遭利用之可能性為低。
- 若控制措施安全等級為 1，則弱點等級為 2，表示此項弱點遭利用之可能性為中等。
- 若控制措施安全等級為 0，則弱點等級為 3，表示此項弱點遭利用之可能性為高。

（11）風險估值：各重要資產之風險估值係以資產價值與威脅等級與弱點等級三者相乘而得

表 2 風險評估執行範例表

所在位置	系統／元件	資產名稱	資產價值	威脅列表	威脅等級	弱點列表	控制措施	控制措施安全等級（SL-C）	弱點等級	風險估值
產線區	○○產線基板組裝	生產線控制電腦	3	DDoS	2	資源不足	無	控制措施安全等級=0	3	18
產線區	○○產線基板組裝	SMT自動貼合機	3	未授權存取	2	無存取控制	本貼合機之控制面板，每個員工進行操作時需先以公司配發之帳號（每人帳號不重複）登入，具一定強度之密碼，且定期進行盤點。	控制措施安全等級=4	1	6

6. 工控物聯網安全防護及控制措施

承前章，當組織對 IACS 環境中相關資產進行風險評鑑後，應可從風險估值分數得知各項資產之曝險程度，組織應基於自身風險胃納程度，設置一合理之風險可接受水準分數，針對高風險事項採取相對應之控制措施，亦即由現況安全等級(SL-A)透過下列具備安全等級(SL-C)控制措施實作，達成目標安全等級(SL-T) ；以表 2 為例，若組織自訂之風險可接受水準為 12 分，則該風險評估範例中之第一項次，則是組織應優先採行控制措施進行處置之風險；各項資產之目標安全等級亦由組織依據自身之風險承受能力或對利害相關人之要求進行瞭解後自行訂定，建議值可參考本實務指南附件 1：系統目標安全等級建議

6.1 可採取之控制措施及其安全等級（SL-C）分項說明

於○○○ 年○○月○○日前由現況安全等級(SL-A)透過下列具備安全等級(SL-C)控制措施實作，達成目標安全等級(SL-T)，目標安全等級由組織依據自身之風險承受能力或對利害相關人之要求進行瞭解後自行訂定，建議值可參考本實務指南附件 1：系統目標安全等級建議。

6.1.1 資訊及資訊系統之管理

1. [控制措施安全等級=1]資訊及資訊系統管理人應確保資訊及資訊系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. [控制措施安全等級=2]資訊及資訊系統管理人應確保資訊及資訊系統被妥善的保存或備份。
3. [控制措施安全等級=2,3,4]資訊及資訊系統管理人應確保重要之資訊及資訊系統已採取適當之存取控制政策。考量風險執行結果，多個高風險事項均與缺乏存取政策有關，故組織應進行存取政策之研擬，以期達成較高之控制強度。

6.1.2 資訊及資訊系統之使用

1. [控制措施安全等級=1]本公司同仁使用資訊及資訊系統前應經其管理人授權。

2. [控制措施安全等級=1]本公司同仁使用資訊及資訊系統時，應留意其工控物聯網安全要求事項，並負對應之責任。
3. [控制措施安全等級=2,3,4]本公司同仁使用資訊及資訊系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上移除。
4. [控制措施安全等級=2,3,4]非本公司同仁使用本公司之資訊及資訊系統，應確實遵守本公司之相關工控物聯網安全要求，且未經授權不得任意複製資訊。
5. [控制措施安全等級=2,3,4]對於資訊及資訊系統，宜識別並以文件記錄及實作可被接受使用之規則。

6.1.3 資訊及資訊系統之刪除或汰除

1. [控制措施安全等級=2,3]資訊及資訊系統之刪除或汰除前應評估公司是否已無需使用該等資訊及資訊系統，或該等資訊及資訊系統是否已妥善移轉或備份。
2. [控制措施安全等級=3,4]資訊及資訊系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。
3. [控制措施安全等級=3,4]具機敏性之資訊或具授權軟體之資訊系統，宜採取實體銷毀， 或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

6.1.4 網路安全控管

1. [控制措施安全等級=1]本公司之網路區域劃分如下：(請公司視實際情形增列)
   (1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network , WAN)。
   (2) 非軍事區(DMZ)：放置公司對外服務伺服器之區段。
   (3) 內部區域網路 (Local Area Network , LAN) ：公司內部單位人員及內部伺服器使用之網路區段。
   (4) 工控區域網路:放置與生產製程有關網路區段,PERA Level 0~3
   (5) 工控非軍事區 (IDMZ) :介於 PERA Level 3,4 之間，用以放置工控與智慧連網的邊緣運算設備及安全監控伺服器
2. [控制措施安全等級=2,3,4]外部網路、非軍事區及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區

域。

考量風險執行結果，多個高風險事項均與缺乏網路存取清單（ACL, Access Control List）有關，故組織應進行相關資安設備之投資建置，以及合宜之存取規則設置，以期達成較高之控制強度。

3. [控制措施安全等級=3,4]應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新或升級。
4. [控制措施安全等級=3,4]對於通過防火牆之來源端主機 IP 位址、目的端主機 IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
5. [控制措施安全等級=1]本公司內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。
6. [控制措施安全等級=2,3,4]對網路系統管理人員或工控物聯網安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. [控制措施安全等級=1]使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。
8. [控制措施安全等級=2]網域名稱系統(DNS)防護
    （1） 一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。
    （2） DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。
    （3） DNS 伺服器應設定指向 GSN Cache DNS。（公務公司適用）
    （4） 內部主機位置查詢應指向公司內部 DNS 伺服器。
9. [控制措施安全等級=2]無線網路防護
    （1） 機密資料原則不得透過無線網路及設備存取、處理或傳送。
    （2） 無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。
    （3） 行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。
    （4） 用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

6.1.5 資訊系統權限管理

1.[控制措施安全等級=1]本公司之資訊系統應設置通行碼管理，通行碼之要求需滿足：

（1） 通行碼長度 8 碼以上。

（2） 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

（3） 使用者每 90 天應更換一次通行碼。

考量風險執行結果，多個高風險事項均與弱密碼設置有關，故組織應進行進行密碼政策之建立，並於設備/系統存取時要求密碼政策之落實，以期達成較高之控制強度。

2.[控制措施安全等級=1]使用者使用資訊系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3.[控制措施安全等級=2,3,4]使用者無繼續使用資訊系統時，應立即停用或移除使用者 ID， 資訊系統管理者應定期清查使用者之權限。

6.1.6 特權帳號之存取管理

1.[控制措施安全等級=1]資訊系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2.[控制措施安全等級=1]資訊系統之特權帳號不得共用。

3. [控制措施安全等級=2]對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。

4.[控制措施安全等級=2,3,4]資訊系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

5.[控制措施安全等級=2,3,4]資訊系統之管理者每季應清查系統特權帳號並劃定特權帳號逾期之處理方式。

6.1.7 加密管理

1.[控制措施安全等級=1]本公司之機密資訊於儲存或傳輸時應進行加密。

2.[控制措施安全等級=2,3,4]本公司之加密保護措施應遵守下列規定：

（1） 應落實使用者更新加密裝置並備份金鑰。

（2） 應避免留存解密資訊。

(3) 一旦加密資訊具遭破解跡象，應立即更改之。

6.1.8 防範惡意軟體之控制措施

1. [控制措施安全等級=1]本公司之主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。
   (1) 經任何形式之儲存媒體所取得之檔案,於使用前應先掃描有無惡意軟體。
   (2) 電子郵件附件及下載檔案於使用前,宜於他處先掃描有無惡意軟體。
   (3) 確實執行網頁惡意軟體掃描。
2. [控制措施安全等級=2,3,4]使用者未經同意不得私自安裝應用軟體，管理者並應每半年定期針對管理之設備進行軟體清查。
3. [控制措施安全等級=1]使用者不得瀏覽已知或疑似惡意之網站，或需建立機制攔阻已知或可疑惡意網站之瀏覽。
4. [控制措施安全等級=2,3,4] 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊，或需建制弱點攻擊的屏蔽機制。

6.1.9 遠距工作之安全措施

1. [控制措施安全等級=1]本公司資訊系統之操作及維護以現場操作為原則，避免使用遠距工作，如有緊急需求時，應申請並經工控物聯網安全管理委員會同意後始可開通。
2. [控制措施安全等級=2,3,4] 工控物聯網安全管理委員會應定期審查已授權之遠距工作需求是否適當。
3. [控制措施安全等級=2,3,4]針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。
   (1) 提供適當通訊設備，並指定遠端存取之方式。
   (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
   (3) 進行遠距工作時之安全監視。
   (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

6.1.10 確保實體與環境安全措施

1.[控制措施安全等級=1]資料中心及電腦機房之門禁管理

(1) 資料中心及電腦機房應進行實體隔離。

(2) 公司人員或來訪人員應申請及授權後方可進入資料中心及電腦機房,資料中心及電腦機房管理者並應定期檢視授權人員之名單。

(3) 人員進入管制區應配載身分識別之標示,並隨時注意身分不明或可疑人員。

(4) 僅於必要時,得准許外部支援人員進入資料中心及電腦機房。

(5) 人員及設備進出資料中心及電腦機房應留存記錄。

2.[控制措施安全等級=2,3,4]資料中心及電腦機房之環境控制

(1) 資料中心及電腦機房之空調、電力應建立備援措施。

(2) 資料中心及電腦機房之溫濕度管控範圍為:

(3) 資料中心及電腦機房應安裝之安全偵測及防護措施,包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備、入侵者偵測系統,以減少環境不安全引發之危險。

(4) 各項安全設備應定期執行檢查、維修,並應定時針對設備之管理者進行適當之安全設備使用訓練。

6.1.11 資料備份

1.[控制措施安全等級=1]重要資料及核心資訊系統應進行資料備份,其備份之頻率應滿足復原時間點目標之要求,並執行異地存放。

2.[控制措施安全等級=2,3,4]本公司應每季確認核心資訊系統資料備份之有效性。且測試該等資料備份時,宜於專屬之測試系統上執行,而非直接於覆寫回原資訊系統。

3.[控制措施安全等級=3,4]敏感或機密性資訊之備份應加密保護。

6.1.12 媒體防護措施

1.[控制措施安全等級=1]使用隨身碟或磁片等存放資料時,具機密性、敏感性之資料應與一般資料分開儲存,不得混用並妥善保管。

2.[控制措施安全等級=1]資訊如以實體儲存媒體方式傳送,應留意實體儲存媒體之包裝,選擇適當人員進行傳送,並應保留傳送及簽收之記錄。

3.[控制措施安全等級=2,3,4]為降低媒體劣化之風險,宜於所儲存資訊

因相關原因而無法讀取前，將其傳送至其他媒體。

4. [控制措施安全等級=1]對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

6.1.13 行動設備之安全管理

1. [控制措施安全等級=1,2,3,4]機密資料不得由未經許可之行動設備存取、處理或傳送。
2. [控制措施安全等級=2,3,4] 機敏會議或場所不得攜帶未經許可之行動設備進入

6.1.14 系統獲取、開發及維護

1. [控制措施安全等級=2,3,4] 本公司之資訊系統應依注意下列事項：
   (1) 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家工控物聯網安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。
   (2) 於資訊系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。
   (3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。
   (4) 執行資訊系統原始碼安全措施，包含原始碼存取控制與版本控管，並檢討執行情形。

6.1.15 工控物聯網安全防護設備

1. [控制措施安全等級=1,2,3,4]本公司應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。
2. [控制措施安全等級=2,3,4]資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

6.2 工控區域(PERA 初級至第三級)

於○○○ 年○○ 月○○ 日前由現況安全等級(SL-A)透過下列具備安全等級(SL-C)控制措施實作，達成目標安全等級(SL-T)，目標安全等級由組織依據自身之風險承受能力或對利害相關人之要求進行瞭解後自行訂定，建議值可參考本實務指南附件 1：系統目標安全等級建議。

6.2.1 工控非軍事區域(Industrial Demilitarized Zone, IDMZ)

建置企業區與工控區次世代防火牆(NGFW)2 部(現況安全等級=1,目標安全等級=3)

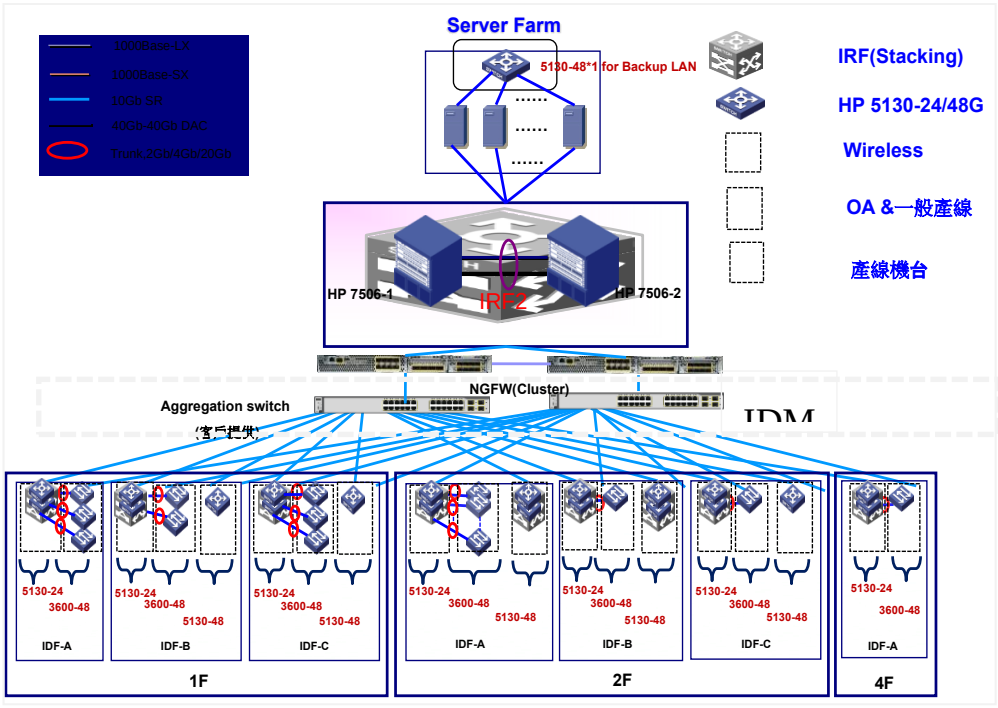


圖 4 IDMZ 架構圖

設備架構說明：

圖 5 採用兩台 NGFW Cluster 架構，各樓層流量經由各自 uplink port 分別導入不同 NGFW(inline mode)，檢查過後直接,進入 Core switch。

達成下列安全防護功能：

- [SR 5.1,控制措施安全等級=4]傳統防火牆功能，區隔 IT 與 OT 網路，進行網路存取控制。
- [SR 5.1,控制措施安全等級=4]縮短檢測和修復高級威脅（APT 入侵、木馬、後門等惡意程式）的時間
- [EDR 3.10,HDR3.10,NDR3.10]解決未修補或不可修補的漏洞
- [SR 5.2,控制措施安全等級=4]保護關鍵生產設備和網段安全
- [SR 7.1,控制措施安全等級=4]達成高安全性和卓越的吞吐量

因本計畫內搭配設備機台的工業級電腦均為 Windows XP/7 已無法或即將無法由微軟修補程式，且製造現場無法如辦公室網路的一般個人電腦可隨時更新並重新開機，僅能以「虛擬修補方式（以次世代防火牆阻擋由 IT 區向 OT 區的弱點運用）」進行補強。

6.2.1.1 建置〇〇廠 IT/OT 場域安全監控系統(〇〇〇年〇〇月〇〇日完成建置)

為建立〇〇廠 IT/OT 場域（包含企業區及網通產線 A/B/C 廠區）資產狀態及安全可視化，以早期偵測資產異動、惡意行為發動，以利 IT/OT 人員進行應變。

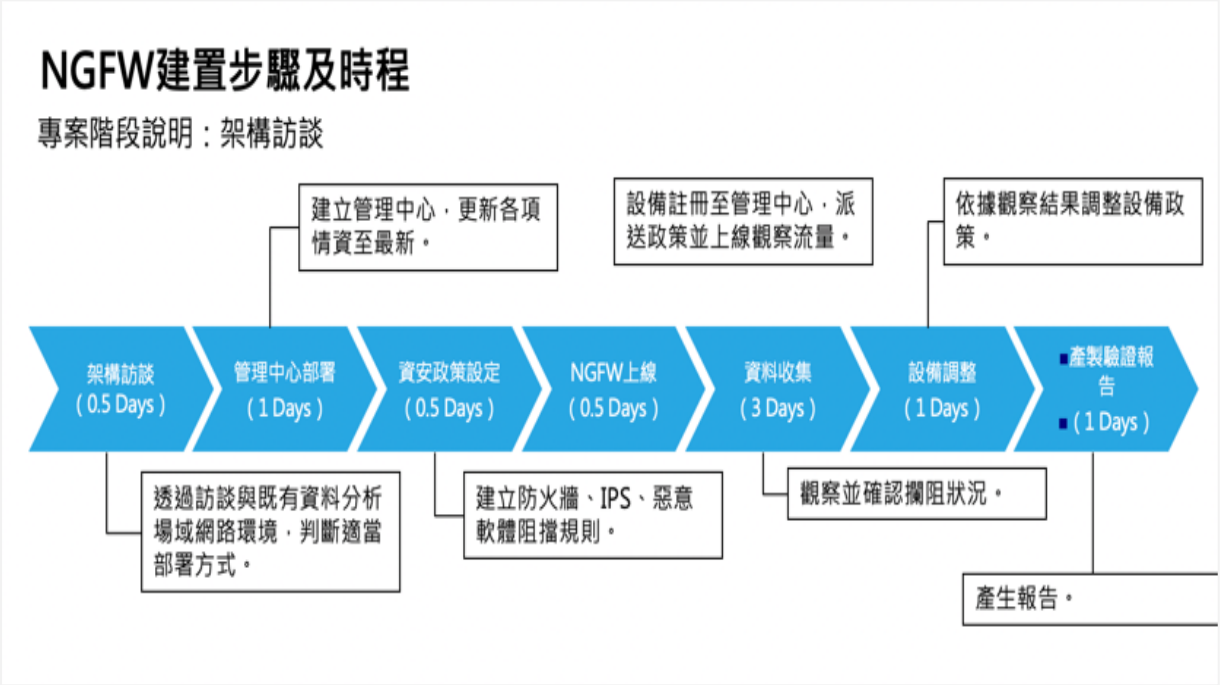


圖 5 IDMZ 的 NGFW 建置流程

預計部署架構如下圖：

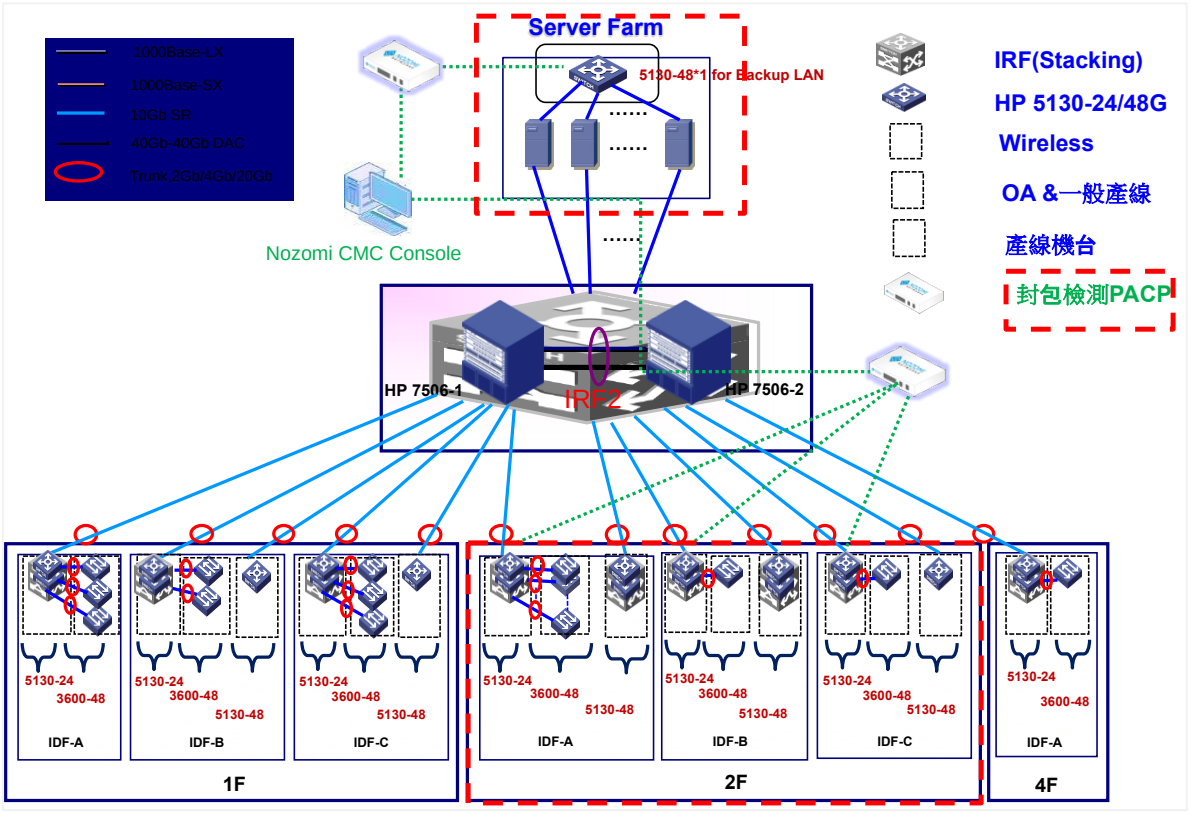


圖 6 IT/OT 安全監控系統架構圖

安全監控功能對應 PERA 示意如下圖

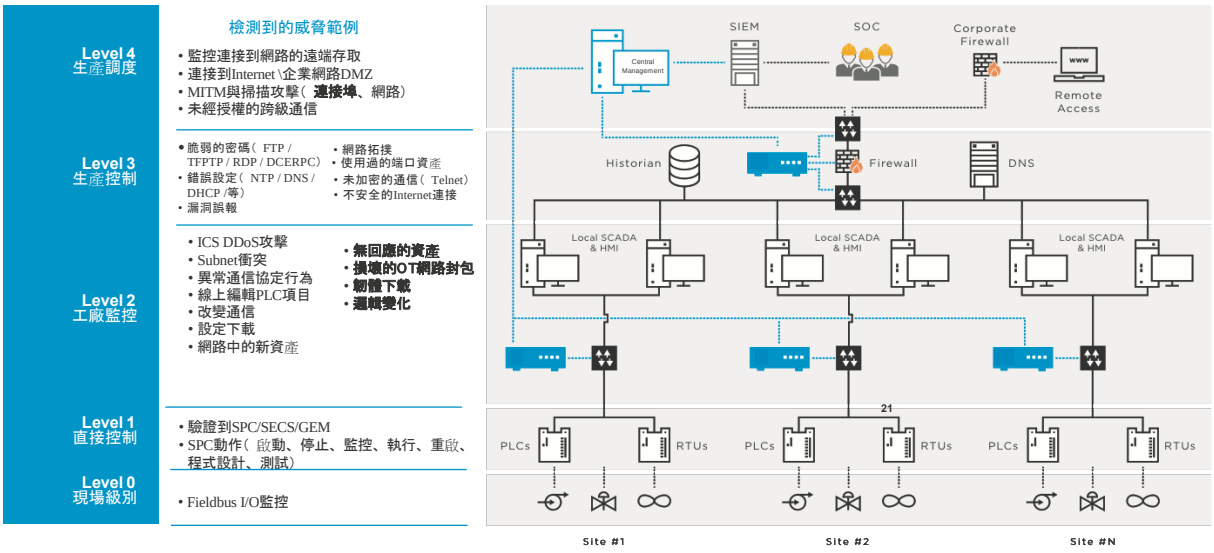


圖 7 安全監控功能對應 PERA 示意圖

可強化安全控制措施等級如表 3，茲針對其中各欄位說明如下：

- 控制編號與安全要求名稱：此二欄位係源自於 IEC62443-3-3 所定義之系統安全需求。
- 目標安全等級：係指組織對該項系統安全需求應達到的目標等級，此目標等級係經由參考本指南『附件 1 – 系統目標安全等級建議表』，並同時參酌組織自身之風險承受能力所訂定。
- 現況安全等級：係指經顧問或組織自行評估，組織對該項系統安全需求目前所具備之控制能力，所達到之安全等級。
- 控制措施安全等級：係指組織為彌補目標安全等級（SL-T）與現況安全等級(SL-A)之差距，所選用之控制措施，其滿足之安全等級。
- 差異值係指控制措施安全等級(SL-C)與目標安全等級(SL-T)之差異，如為正值（或為 0）代表控制措施安全等級優於（或等於）目標安全等級；倘各項強化措施之實作所能提供之控制措施安全等級低於目標安全等級，則代表組織仍應採取其他控制措施進行安全等級之強化。

表 3 可強化安全控制措施等級表

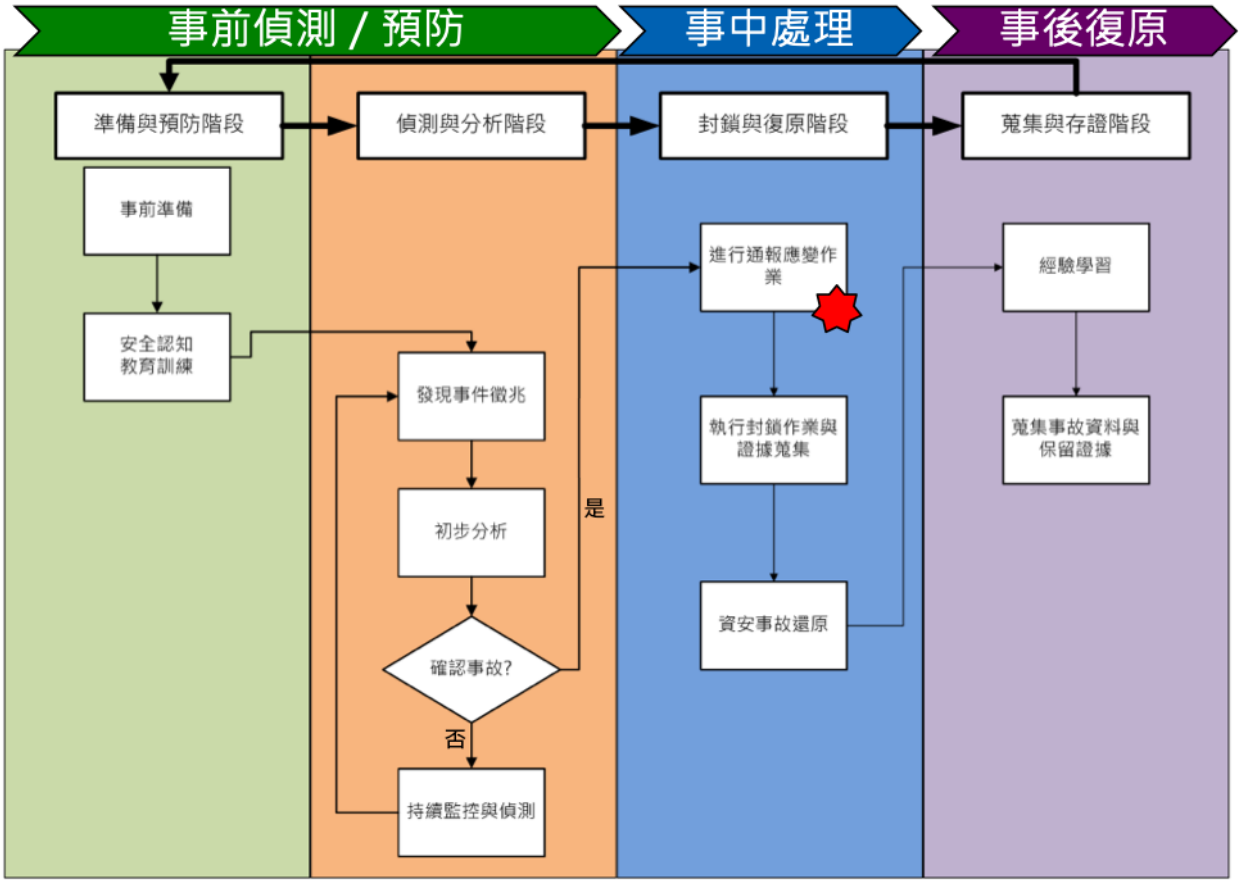
控制編號	安全要求名稱	目標安全等級(SL-T)	現況安全等級(SL-A)	控制措施安全等級(SL-C)	差異值(SL-C)減(SL-T)
SR 1.11	登錄嘗試失敗	2	1	3	+1
SR 1.12	系統使用通知	2	1	3	+1
SR 2.02	無線網路使用控制	2	1	2	0
SR 2.03	對可攜式和行動裝置使用控制	2	1	2	0
SR 2.08	可稽核的事件	2	1	3	+1
SR 2.09	稽核儲存容量	2	1	3	+1
SR 2.11	時間戳記	2	1	3	+1
SR 3.1	通訊完整性	3	1	3	0
SR 3.2	惡意程式碼保護	2	1	2	0

SR 5.3	限制一般人對人通訊	2	1	2	0
SR 6.2	持續監控	2	1	3	+1
SR 7.1	拒絕服務保護	2	1	3	+1
SR 7.2	資源管理	2	1	2	0
SR 7.8	控制系統元件盤點	3	1	3	0

7. 工控物聯網安全事件通報、應變及演練相關機制

為即時掌控資訊安全事件，並有效降低其所造成之損害，本公司應訂定資訊安全事件通報、應變及演練相關機制，安全事件通報、應變之管理流程可參考圖 8。

圖 8 資訊安全事件通報流程圖



另「本計畫適用範圍」應進行業務持續營運管理(BCM, Business Continuity Management)相關作為，業務持續營運管理之重要作業如圖 9，其中至少包含營運衝擊分析、業務持續計畫（BCP, Business Continuity Plan）及定期演練三大工作，

其中營運衝擊分析旨在識別組織之重要營運流程及其所仰賴之資源，應依企業區域及個別工控區域就機密性、完整性、可用性、安全性（Safety）等構面，企業先採取營運衝擊分析(Business Impact Analysis;BIA) 計算出關鍵營運流程中斷對企業造成之災害或損失，制定出較為合理的復原時間目標 RTO(Recovery Time Objective)，讓企業能夠更加速地，包括: 備份作業的完整性、資料的復原、資料的重新儲存、乃至主機的重新啟動，

若原機或其他設備因故失效，連同部置新設備所須耗費的時間也得列入 RTO 的計算範圍，使主機正常運行的時間。另外考量：復原點目標(Recovery Point Objective)，對系統及應用資料而言，意欲能夠復原至可支援各部門業務運作，則系統與資料應當恢復到何種程度？需透過與各業務部門主管的訪談互動，制定出較合宜的 RPO 目標，企業再依 RTO 及 RPO 進而推估最大可容忍中斷時間(Maximum Tolerable Period of Disruption; MTPD)以小時計，前述關鍵任務、資訊資產與最大可容忍中斷時間之分析範例，可參考表 4。

而 BCP（業務連續性計劃, Business Continuity Plan）之撰寫，旨在制訂組織之重要營運流程面對威脅，而有中斷之虞時，組織之因應方式。

最後，組織應針對已制訂之業務連續性計劃，每年至少辦理一次演練，透過不同方式之演練以驗證該計畫之可行性。

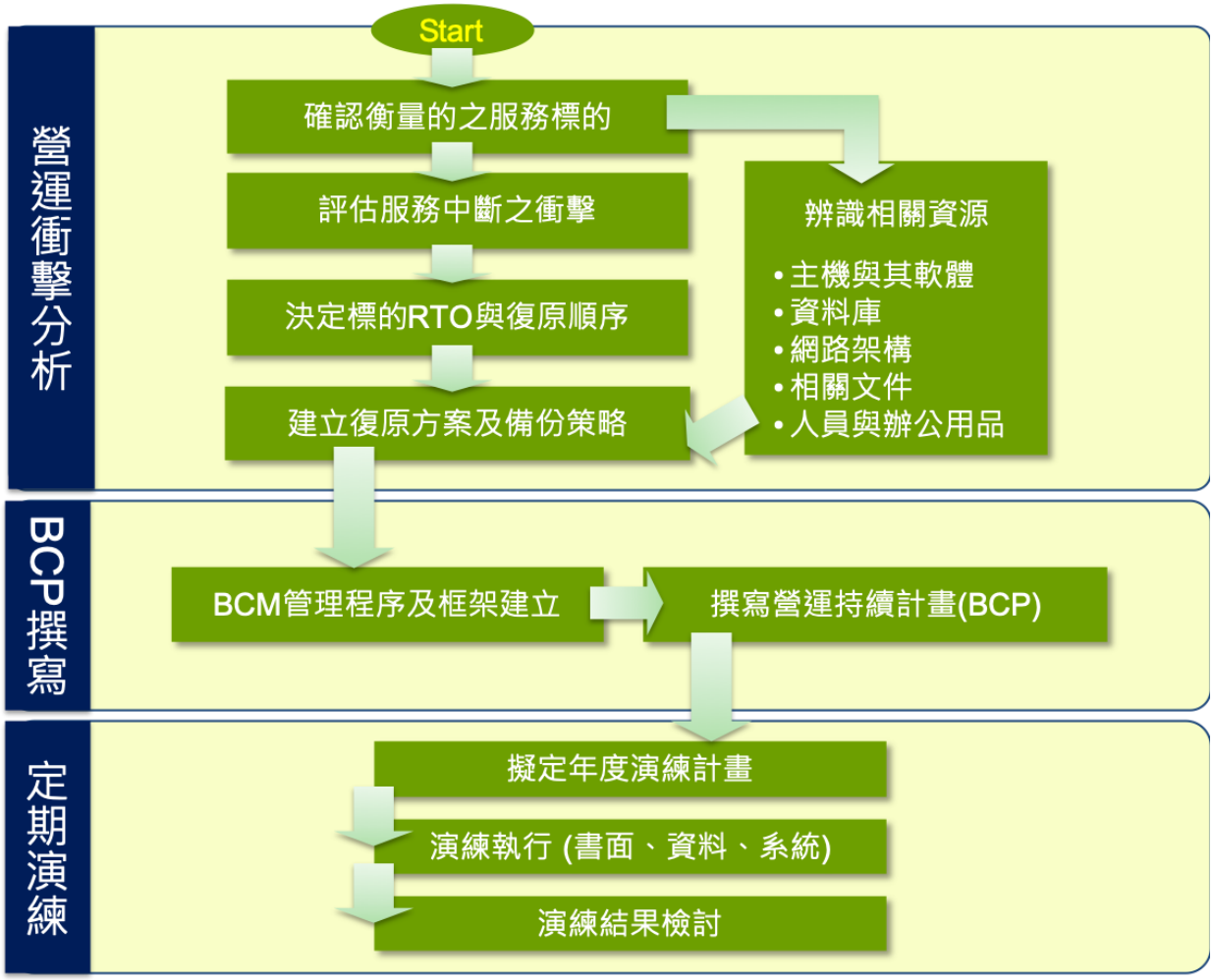


圖 9 營運持續管理流程圖

表 4 關鍵任務／資產／衝擊分析表

關鍵任務流程	資訊資產	RTO	RPO	最大可容忍中斷時間
MES 系統	1. 應用程式主機 2 部 2. 資料庫主機 2 部 3. 網頁伺服器 2 部	2 小時	2 小時	4 小時
○○生產部	1. 生產線控制電腦計 3 台 2. 生產線控制電腦參數儲存主機 1 台 3. SMT 自動貼合機 3 台 4. 網路交換器 2 台 5. 電子零件供應器 3 台	2 小時	2 小時	4 小時
○○生產部	1. 生產線控制電腦計 2 台 2. 生產線控制電腦參數儲存主機 1 台 3. 組裝機器手臂 3 台網路交換器 4. 外殼料件搬運車 2 台	2 小時	2 小時	4 小時

8. 工控物聯網安全情資之評估及因應

本公司計畫訂閱來自 NGFW 供應商的工控物聯網安全情資服務，提升事件判斷準確率，並依本公司資安事件通後處理辦法因應，必要時得調整工控物聯網安全防護計畫之控制措施，並做成紀錄。

8.1 安全情資之分類評估

本公司接受工控物聯網安全情資後，由工控物聯網安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

8.1.1 工控物聯網安全相關之訊息情資

工控物聯網安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬工控物聯網安全相關之訊息情資。

8.1.2 入侵攻擊情資

工控物聯網安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

8.2 安全情資之因應措施

本公司於進行工控物聯網安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整工控物聯網安全防護計畫之控制措施。

8.2.1 工控物聯網安全相關之訊息情資

由工控物聯網安全管理委員會彙整情資後進行風險評估，並依據工控物聯網安全防護計畫之控制措施採行相應之風險預防機制。

8.2.2 入侵攻擊情資

由工控物聯網安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施,並依據工控物聯網安全防護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

9. 工控物聯網系統或服務委外辦理之管理

本公司委外辦理資訊系統之建置、維運或資訊服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及工控物聯網安全需求，選任適當之受託者，並監督其工控物聯網安全維護情形。

9.1 選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之工控物聯網安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有工控物聯網安全專業證照或具有類似業務經驗之工控物聯網安全專業人員。
3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之工控物聯網安全維護措施。

9.2 監督受託者工控物聯網安全維護情形應注意事項

1. 受託業務包括客製化資訊系統開發者，受託者應提供該資訊系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
2. 受託者執行受託業務，違反工控物聯網安全相關法令或知悉工控物聯網安全事件時，應立即通知委託公司及採行之補救措施。
3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
4. 受託者應採取之其他工控物聯網安全相關防護措施。
5. 本公司應定期或於知悉受託者發生可能影響受託業務之工控物聯網安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

10. 工控物聯網安全教育訓練

本章為公司辦理工控物聯網安全教育訓練事宜，其內容教育訓練之要求及辦理方式。公司如已有對應之規定及程序者，可直引述內部文件編號及名稱。

撰寫範本如下：

10.1 安全教育訓練要求

1. 「本計畫適用範圍」資安人員每年至少 4 名人員接受 48 小時以上之資安專業課程訓練或資安職能訓練。
2. 「本計畫適用範圍」之一般使用者與主管，每人每年接受 2 小時以上之一般工控物聯網安全教育訓練。

10.2 安全教育訓練辦理方式

1. 工控物聯網安全管理委員會應於每年年初，考量管理、業務及資訊等不同工作類別之需求,擬定工控物聯網安全認知宣導及教育訓練計畫，以建立員工工控物聯網安全認知，提升公司工控物聯網安全水準，並應保存相關之工控物聯網安全認知宣導及教育訓練紀錄。
2. 本公司工控物聯網安全認知宣導及教育訓練之內容得包含：(請視實際情形增列)
   (1) 工控物聯網安全政策(含工控物聯網安全防護計畫之內容、管理程序、流程、要求事項及人員責任、工控物聯網安全事件通報程序等)。
   (2) 工控物聯網安全法令規定。
   (3) 工控物聯網安全作業內容。
   (4) 工控物聯網安全技術訓練。
3. 員工報到時，應使其充分瞭解本公司工控物聯網安全相關作業規範及其重要性。
4. 工控物聯網安全教育及訓練之政策，除適用所屬員工外，對公司外部的使用者，亦應一體適用。

11. 工控物聯網安全防護計畫及實施情形之持續精進及績效管理機制

11.1 安全防護計畫之實施

為落實本安全防護計畫，使本公司之工控物聯網安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本公司之工控物聯網安全政策、目標及本安全防護計畫之內容相符，並應保存相關之執行成果記錄。

11.2 工控物聯網安全防護計畫實施情形之稽核機制

1. 稽核機制之實施

(1) 工控物聯網安全管理委員會應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與公司之管理程序要求，並有效實作及維持管理制度。

(2) 辦理稽核前工控物聯網安全管理委員會應擬定工控物聯網安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

(3) 辦理稽核時，工控物聯網安全管理委員會應於執行稽核前 14 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

(4) 本公司之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

(5) 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為工控物聯網安全稽核計畫及稽核事件之證據。

(6) 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解工控物聯網安全政策及應負之資安責任、是否訂定人員之工控物聯網安全作業程序與權責、是否定期更改密碼）。

(7)

2. 稽核改善報告

(1) 受稽單位於稽核實施後發現有缺失或待改善項目者,應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

(2) 受稽單位於稽核實施後發現有缺失或待改善者,應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

(3) 受稽單位於判定缺失或待改善之原因後,應據此提出並執行相關之改善措施及改善進度規劃,必要時得考量對現行工控物聯網安全管理制度或相關文件進行變更。

(4) 公司應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

(5) 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

11.3 工控物聯網安全防護計畫之持續精進及績效管理

1. 本公司之工控物聯網安全管理委員會應於 12 月(每年至少一次)召開工控物聯網安全管理審查會議,確認工控物聯網安全防護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：

(1) 過往管理審查議案之處理狀態。

(2) 與工控物聯網安全管理系統有關之內部及外部議題的變更,如法令變更、上級公司要求、工控物聯網安全管理委員會決議事項等。

(3) 工控物聯網安全防護計畫內容之適切性。

(4) 工控物聯網安全績效之回饋，包括：

- ●工控物聯網安全政策及目標之實施情形。
- ●工控物聯網安全人力及資源之配置之實施情形。
- ●工控物聯網安全防護及控制措施之實施情形。
- ●內外部稽核結果。
- ●不符合項目及矯正措施。
- ●風險評鑑結果及風險處理計畫執行進度。
- ●重大工控物聯網安全事件之處理及改善情形。
- ●利害關係人之回饋。

●持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

12. 參考文獻

資通安全管理法施行細則

行政院國家資通安全會報資安維護計畫範本

ISA/IEC 62443

CNS 27001

13. 附件

附件 1 系統目標安全等級建議

附件 2 元件目標安全等級建議

附件 3 威脅樣態與弱點對應

附件 1 系統目標安全等級建議

重要系統如 ERP、MES、PLM、SCADA 等，建議控制措施目標安全等級如表 5，惟仍可依據組織之風險承受程度或利害相關者之要求，酌情進行調升或調降。

表 5 控制措施目標安全等級表

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
SR 1.01	人類使用者識別和認證		✓		
SR 1.02	軟體程序和設備識別和認證		✓		
SR 1.03	帳戶管理			✓	
SR 1.04	身份識別管理		✓		
SR 1.05	驗證器管理		✓		
SR 1.07	基於密碼的身份驗證的強度		✓		
SR 1.08	公鑰基礎結構（PKI）憑證		✓		
SR 1.09	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 2.01	授權執行		✓		
SR 2.02	無線網路使用控制		✓		
SR 2.03	對可攜式和行動裝置使用控制		✓		
SR 2.04	行動程式碼		✓		
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		✓		

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
SR 2.11	時間戳記		✓		
SR 2.12	不可否認		✓		
SR 3.1	通訊完整性			✓	
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 3.9	保護稽核資訊		✓		
SR 4.1	資訊保密		✓		
SR 4.2	資訊持久性		✓		
SR 4.3	密碼學的使用		✓		
SR 5.3	限制一般人對人通訊		✓		
SR 5.4	應用程序分區		✓		
SR 6.1	審核日誌可存取性		✓		
SR 6.2	持續監控		✓		
SR 7.1	拒絕服務保護		✓		
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			✓	

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
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			✓	

附件 2 元件目標安全等級建議

工控物聯網組成元件繁多，概分成共通性、主機、網路、嵌入式及軟體等，建議目標安全等級如下表

表 6 元件目標安全等級建議表

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
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 1.7	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			✓	
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			✓	

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
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	回應稽核記錄處理錯誤			✓	
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			✓	
CR 3.1	通訊完整性			✓	
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		✓		
CR 4.1	資訊機密性		✓		

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
CR 4.2	資訊持久性		✓		
CR 4.3	使用密碼學		✓		
CR 5.1	網路分段			✓	
CR 5.2	區域邊界保護			✓	
CR 5.3	一般用途人對人通訊限制		✓		
CR 5.4	應用程式分割		✓		
CR 6.1	稽核記錄存取性		✓		
CR 6.2	持續監控		✓		
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			✓	
SAR 2.4	行動程式碼			✓	
SAR 3.2	防範惡意程式碼			✓	
EDR 2.4	行動程式碼		✓		
EDR 2.13	使用實體診斷和測試介面		✓		
EDR 3.2	防範惡意程式碼		✓		
EDR 3.10	更新支援		✓		

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
EDR 3.11	防範與偵測實體篡改		✓		
EDR 3.12	供應產品供應商的信任根源		✓		
EDR 3.13	供應資產擁有者的信任根源		✓		
EDR 3.14	啟動程序完整性		✓		
HDR 2.4	行動程式碼		✓		
HDR 2.13	實體診斷和測試介面的使用		✓		
HDR 3.2	防範惡意程式碼		✓		
HDR 3.10	更新支援		✓		
HDR 3.11	防範與偵測實體篡改		✓		
HDR 3.12	供應產品供應商的信任根源		✓		
HDR 3.13	供應資產擁有者的信任根源		✓		
HDR 3.14	啟動程序完整性		✓		
NDR 1.6	無線存取管理			✓	
NDR 1.13	通過不受信任的網路存取			✓	
NDR 2.4	行動程式碼			✓	
NDR 2.13	使用實體診斷和測試介面			✓	
NDR 3.2	防範惡意程式碼			✓	
NDR 3.10	更新支援			✓	
NDR 3.11	防範與偵測實體篡改			✓	
NDR 3.12	供應產品供應商的信任根源			✓	
NDR 3.13	供應資產所有者信任的根源			✓	
NDR 3.14	啟動過程的完整性			✓	

控制編號	安全要求名稱	目標安全等級(SL-T)			
		1	2	3	4
NDR 5.2	區域邊界保護			✓	
NDR 5.3	一般用途,人對人通信限制			✓	

附件 3 威脅樣態與弱點對應

表 7 威脅樣態與弱點對應表

威脅樣態	威脅等級評分參考	對應弱點
DDoS	2	資源不足
注入攻擊	3	應用程式漏洞
身分憑據偷竊	3	弱密碼
資料竊取	2	明文儲存
密碼猜測	2	預設密碼未更改
惡意程式	2	作業系統漏洞
蠕蟲	3	未設定 ACL
未授權存取	2	無存取控制
資料篡改	2	作業系統漏洞

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