110年「經濟部關鍵基礎設施資安聯防服務專案」

經濟部能源及水資源領域工業控制系統防護基準及防護建議宣導會議

安碁資訊股份有限公司
Acer Cyber Security Inc.

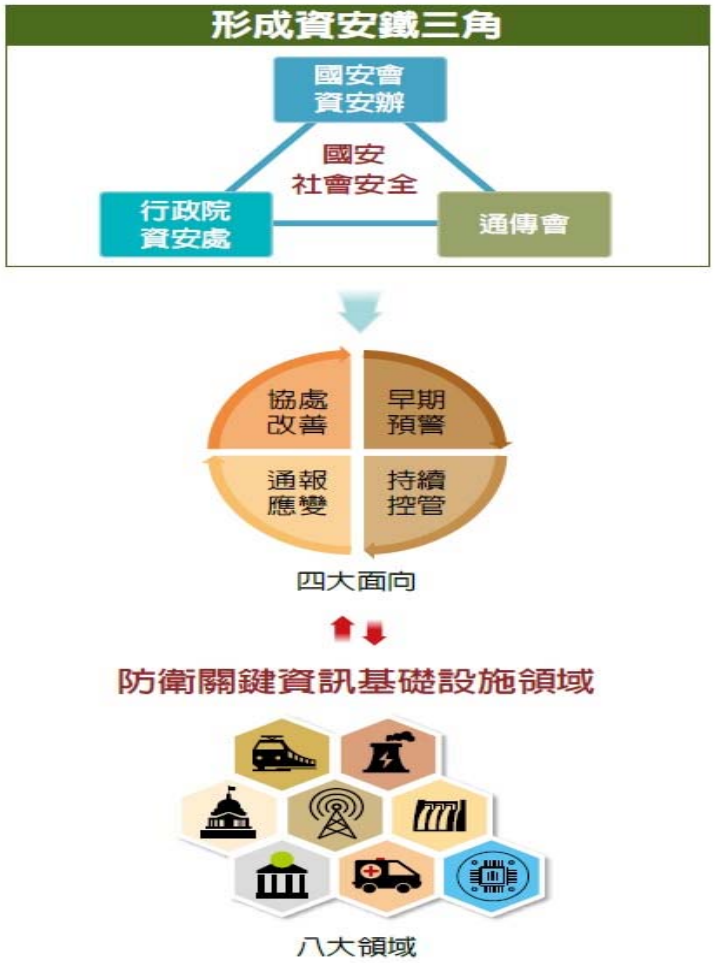
簡報大綱

- 能源及水資源領域工業控制環境資安防護基準與防護建議說明
- 能源及水資源領域工業控制系統資安防護作業實施建議
- 結論

能源及水資源領域工業控制環境資安防護基準與防護建議說明

安碁資訊

防護基準背景說明



資通安全管理法

特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。

資通安全責任等級分級辦法

各機關自行或委外開發之資通系統應依**附表九所定資通系統防護需求分級原則**完成資通系統分級，並依**附表十所定資通系統防護基準**執行控制措施；關鍵基礎設施提供者之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，**得自行擬訂防護基準**，報請主管機關核定後，依其規定辦理。

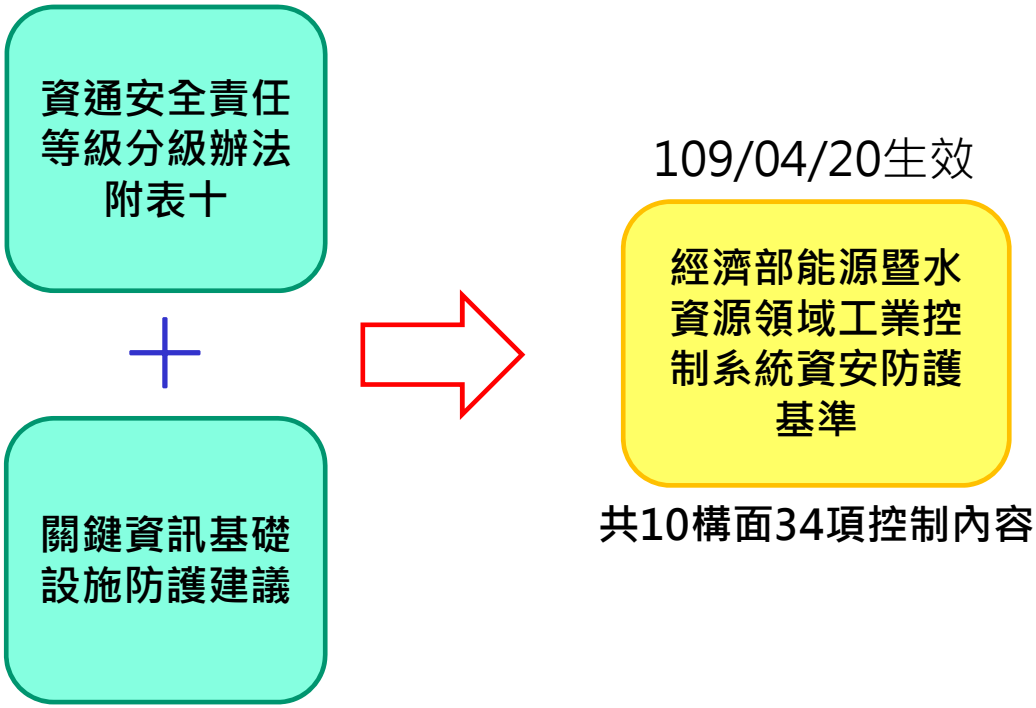
關鍵資訊基礎設施資安防護建議

由國家層級制定本防護建議，提供各關鍵基礎設施領域層級參考，再**由各關鍵基礎設施領域層級依領域特性，訂定資安防護基準相關文件**，以提升關鍵資訊基礎設施資安防護能力。

防護基準背景說明(cont.)

- 制訂防護基準考量因素
  - 資通安全責任分級辦法附表十防護基準偏屬IT範疇。
  - 行政院資通安全處「關鍵資訊基礎設施防護建議」屬指引性質，非強制規範。
  - 應考量能源與水資源領域工業控制系統共通需求，以及廠(場)站實際資安管控作為。

防護基準依據說明


資通安全責任等級分級辦法附表十
+
關鍵資訊基礎設施防護建議
109/04/20生效
經濟部能源暨水資源領域工業控制系統資安防護基準
共10構面34項控制內容

防護基準對照

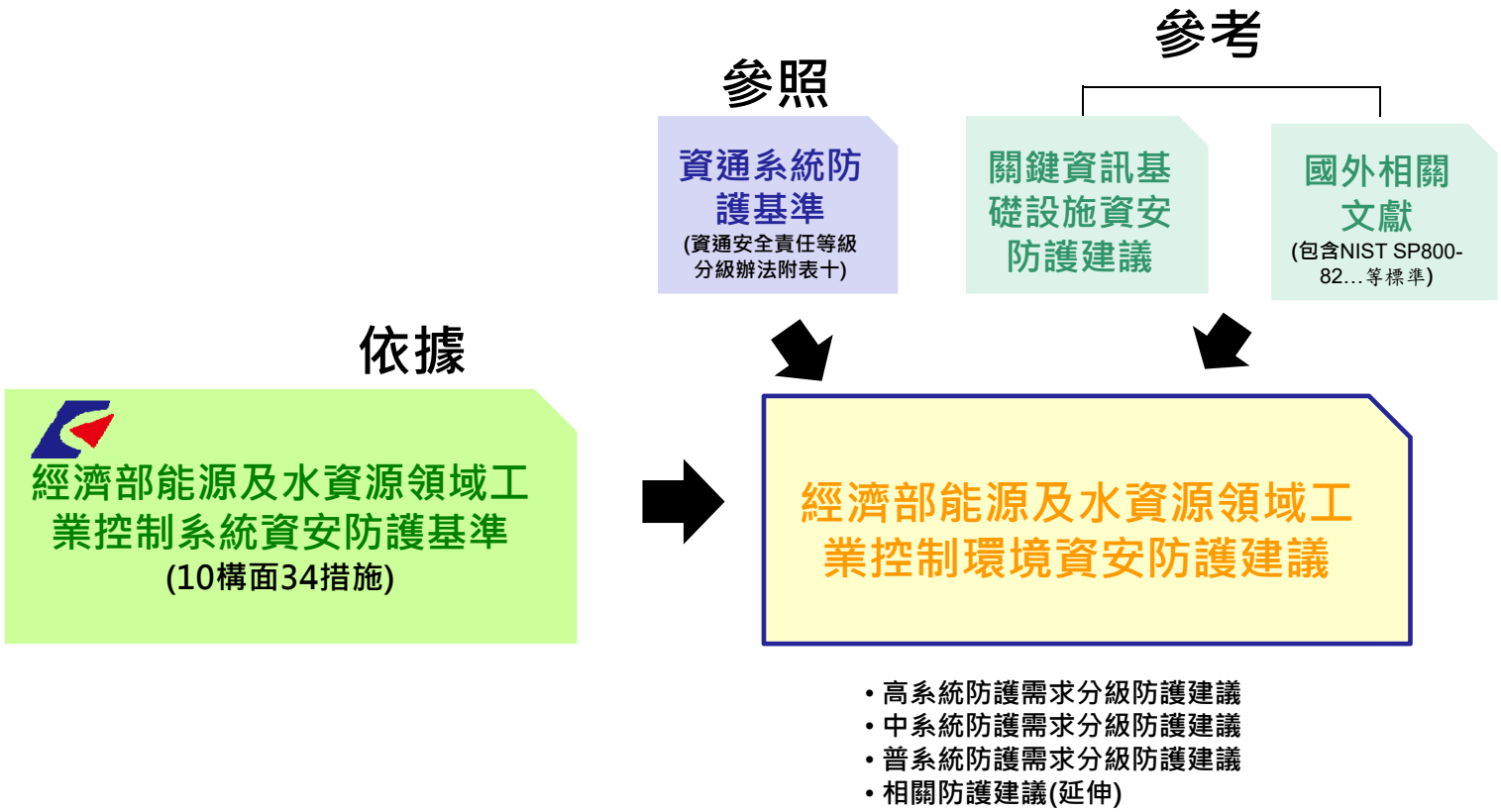
110年8月23日修正

經濟部防護基準					資通安全責任等級分級辦法—附表十、資通系統防護基準					關鍵資訊基礎設施資安防護建議(資通安全處)		
控制措施		系統防護需求分級			控制措施		系統防護需求分級			控制措施		
構面	措施內容	高	中	普	構面	措施內容	高	中	普	構面	措施內容	建議
存取控制	帳號管理	一、逾越預期閒置時間或可使用期限時，自動將使用者登出；但操作過程中有替代之監管措施者，不在此限。 二、依機關規定之情況及條件使用系統。 三、監控帳號異常使用情況並回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號予以刪除或禁用。 二、禁用閒置帳號。 三、定期審核帳號之建立、修改、啟用、禁用及刪除作業。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除程序。	存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情況及條件，使用資通系統。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	存取控制	4.2.1 帳號管理	● 建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。 ● 系統已逾期之臨時或緊急帳號需刪除或禁用 ● 禁用系統閒置帳號。 ● 定期審核系統帳號之建立、修改、啟用、禁用及刪除動作。 ● 當超過組織所規定之預期閒置時間或可使用期限時，系統需自動將使用者登出。 －對於設定閒置時間或可使用期限對於某些流程控制應用並非適切，如HMI與操作人員用於持續流程監視設備，建議考量並實作因應對策(如門禁系統等)與責任歸屬。 ● 依照組織所規定之情況及條件(如上班時間或指定IP來源等)使用系

防護建議目的說明

- 依據「經濟部能源及水資源領域工業控制系統資安防護基準」(109/04/20生效)，提供各控制措施之實施作業建議。
- 防護建議內容擬定之參考原則
  - 資通安全責任等級分級辦法之附表十「資通系統防護基準」
  - 行政院資通安全處「關鍵資訊基礎設施資安防護建議」
  - 包含NIST SP800-82在內之相關國外規範
  - 能源領域及水資源領域廠(場)站之運作現況和需求
- 因應不同防護需求分級之工業控制系統，提供自我檢核表(防護建議附件二)。

防護建議與國內外文獻之關連



安碁資訊

管控範圍說明

工業控制系統/OT 環境

依使用環境類別分為

監控系統

- 用於生產或運作流程之控制作業
- DCS/SCADA/PLC+圖控…等

監測系統

- 僅用於蒐集資料並呈現紀錄
- 水位、雨量監測、煙道、燃燒塔監測等
- 獨立於監控網路

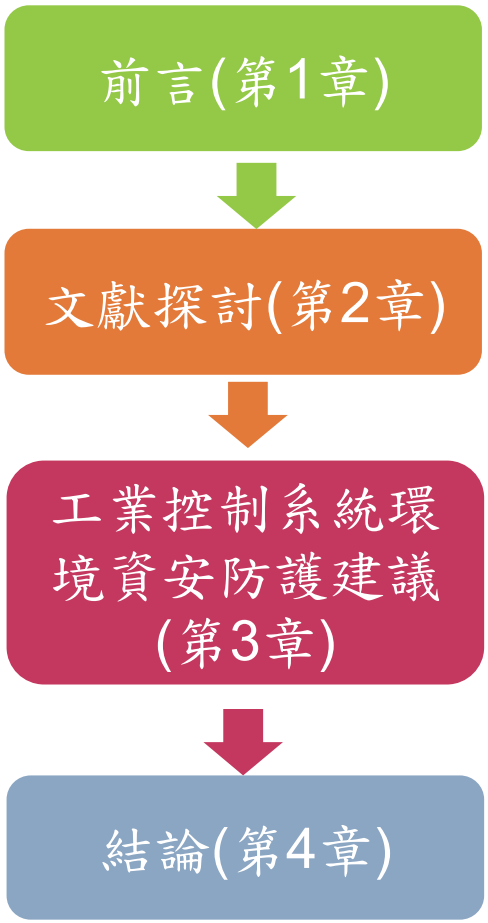
管控範圍說明

- 監測系統
  - 為直接與感測器(Sensor)連接，單純用以蒐集各項即時數據，例如獨立的煙道氣連續監測系統(Continuous Emission Monitoring Systems, CEMS)、水文資料蒐集系統等；或由數據轉換介面間接取得之數據，例如經由OPC(OLE for Process Control)取得來自於控制器(例如DCS、PLC等)之數據，並進行分析、通報、記錄等重要流程，以協助權責人員即時掌握廠(場)站/域狀況。
  - 直接與感測器(Sensor)連接並蒐集各項即時資訊者，需考量感測器(Sensor)設備連線運作的特性，避免造成資訊中斷的可能因素。在資安防護上，宜避免或限制與IT運作環境的網路連線。
  - 位於IT網路且由數據轉換介面間接取得數據者，與其數據來源之界接設備應限制與IT運作環境的網路連線及連線方式，且管控數據轉換介面之安全設定及資料交換存取方式，避免可能的資安風險。

管控範圍說明(cont.)

- 監控系統
  - 應用於工業生產或關鍵基礎設施之ICS，其包括SCADA(Supervisory Control And Data Acquisition)、分散式控制系統(Distributed Control Systems, DCS)及其它控制系統如 PLC(Programmable Logic Controllers)等，其經由ICS內部線路及實體線路(Sensor至 I/O模組)，控制各項製程變數(例如閘門開度、溫度、流量、壓力、液位等)，達到製程操作目的。
  - 與廠(場)生產製程息息相關，需更加重視其可用性(Availability)、可靠性(Reliability)與完整性(Integrity)的要求，除留意各項必要管控措施的落實，更應避免或限制與IT運作環境的網路連線及連線方式，並配合科技演進，持續評估、採用適合ICS現況之防護技術和設備。

能源及水資源領域工業控制環境資安防護建議架構說明



- 前言(第1章)
  - 目的與管控範圍(監測系統、監控系統)說明。
- 文獻探討(第2章)
  - 國內外法規與標準簡介。
  - 國內外文獻管控措施對表分析。
- 工業控制系統環境資安防護建議(第3章)
  - 依據經濟部防護基準10構面34項控制內容，針對高、中、普各等級系統防護需求，提列相關資安管控措施實施建議。
  - 部份控制內容進一步提出延伸性防護建議，以提醒與強化防護作為。
- 結論(第4章)
  - 附件一、資通系統防護需求分級原則
    資通安全責任等級分級辦法附表九
  - 附件二、經濟部能源及水資源領域工業控制系統資安防護基準檢核表
    高、中、普防護需求等級自我檢核表格

安碁資訊

防護基準構面與控制內容

控制措施構面(10)	措施內容(34)			
存取控制	帳號管理	最小權限	遠端存取	網路架構配置與隔離
稽核與可歸責性	稽核事件	稽核紀錄內容	稽核儲存容量	稽核處理失效之回應
	時戳及校時	稽核資訊之防護		
營運持續計畫	電源供應備援	通訊線路備援		
識別與鑑別	內部使用者之識別與鑑別	身份鑑別管理	鑑別資訊回饋	
系統與通訊防護	資料儲存之安全	傳輸之機密性與完整性		
系統與服務獲得	操作、營運及運作限制文件	安全措施文件		
實體與環境防護	實體存取授權	實體隔離與設備進出管控	實體監視與偵測	
系統與資訊完整性	日常操作與查檢紀錄	系統日誌資訊留存	系統監測工具/技術導入	系統異常告警與通報
	系統、設備漏洞評估	漏洞修補	故障預防	
組態管理	系統、設備變更管控	變更作業測試	變更作業紀錄	
組織管理	委外資安規範與要求	服務安全管理		

工業控制系統環境資安防護建議

經濟部能源及水資源領域
工業控制系統資安防護基準
(10構面34措施)

經濟部能源及水資源領域
工業控制環境資安防護建議

- 在「經濟部能源及水資源領域工業控制系統資安防護基準」基礎上，就高、中、普各等級系統防護需求，提列ICS環境下可能的資安管控作法與防護作為，並參考相關法規文獻之要求(例如執行週期、設定原則、建議作法等)
- 部份控制措施與防護作為更包含進一步之相關防護建議，廠(場)站可依營運狀況和需求，評估落實的程度及後續能加強的面向。
- 定期(建議每1年)實施自我查檢作業，藉以檢核施行成效。
- 依據廠(場)站既有之程序與作法，章節內容中提及之紀錄、文件或檔案，可為電子、紙本等之形態。

資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資 通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

經濟部能源及水資源領域工業控制系統資安防護基準-存取控制

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
存取控制	帳號管理	一、逾越預期閒置時間或可使用期限時，系統應自動將使用者登出；但操作過程中有替代之監管措施者，不在此限。 二、依機關規定之情況及條件使用系統。 三、監控帳號異常使用情況並回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號予以刪除或禁用。 二、應禁用閒置帳號。 三、定期審核帳號之建立、修改、啟用、禁用及刪除作業。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除程序。
	最小權限	採最小權限原則，僅允許使用者（或代表行為之程序依任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、監控遠端連線。 二、採用加密機制。 三、遠端存取來源為預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權建立使用限制、組態需求連線需求及文件化。
	網路架構配置與隔離	一、建立工控網路邊界監控機制，定期檢視並回報異常狀況予管理者。 二、等級「中」之所有控制措施。	一、區隔工控網路邊界，採取網路存取管控機制。 二、等級「普」之所有控制措施。	建立安全防護網路架構，管控網際網路連線存取。

存取控制-帳號管理防護建議說明

- **普級**
  - **停用或刪除帳號之例外處理建議**

    應停用或刪除之帳號，可考量運作上的需要，由負責人員取得或管理該帳號權限(例如已變更密碼)後，可暫不實施該停用或刪除作業。
- **中級**
  - **帳號清查作業建議**

    建立帳號清查管控程序(包含建立帳號清查清冊等)，於帳號清查清冊中紀錄各類帳號之權限、所屬人員及狀態(包含帳號申請、建立、修改、啟用、停用及刪除)。

    定期(建議每半年)或遇重大異動(例如最高權限帳號交接移轉)時，應執行帳號清查作業，並留存相關紀錄，妥善保存。

存取控制-帳號管理防護建議說明

- **高級**
  - **替代之監管措施建議**

考量系統、設備之運作需求，應設定帳號預期閒置時間或可使用期限，並於超過閒置時間或使用期限過後自動登出該帳號；或於操作過程中採取替代之監管措施(例如加強CCTV監視機制、落實交接班記錄)。

  - **帳號使用紀錄建議**

考量於系統、設備上建立帳號使用紀錄(例如登入、登出、錯誤嘗試、操作動作等)，並應定期(建議1週)進行檢視及通報異常狀況。(帳號使用紀錄之保護依循3.2.稽核與可歸責性之建議)

附表十、資通系統防護基準修正

高
一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。

存取控制-遠端存取防護建議說明

- **普級**
  - **遠端連線作業定義之建議**

    註：遠端連線意指透過非ICS網路進行ICS管控與資料存取之連線作業。

  - **遠端連線作業之結束處理建議**

    考量遠端連線作業時效結束後，進行必要之管控措施，例如拔除網路線、移除遠端連線工具等。

- **高級、中級**
  - **遠端連線監控機制建議**

    應建立遠端連線之監控機制，例如以特權管理機制記錄遠端連線動作、以網路閘道設備(如防火牆等) 記錄遠端連線來源、時間等...

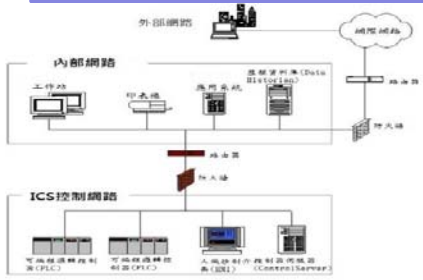
  - **遠端連線來源限制之建議**

    應預為建立遠端連線來源之限制機制，例如IP、設備、通訊埠等限制(包含未經申請不得連線等)，並加強ICS(包含各圖控伺服器與歷史資料主機等作業系統)遠端連線之防護。

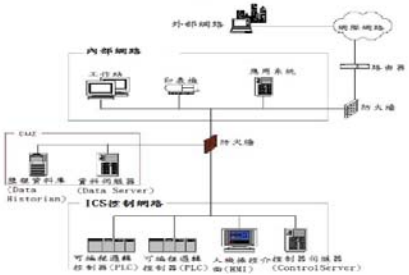
存取控制-網路架構配置與隔離防護建議說明

- **普級**
  - **網路管控原則建議**

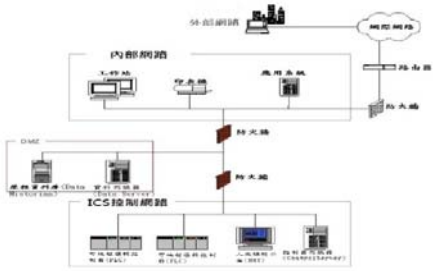
廠(場)站ICS網路應以建立具氣隙(Air Gap)之實體隔離機制或單向傳輸為優先考量，如需對外連線(內部網路或網際網路)，網路架構配置可參酌行政院資通安全處「關鍵資訊基礎設施資安防護建議」...



低安全防護網路架構



中安全防護網路架構



高安全防護網路架構

- **中級**
  - **網路存取規則設定申請程序建議**

建立網路存取規則設定申請程序，定期(建議每1年)檢視與維護存取規則，並留存相關紀錄。針對臨時性網路存取規則考量設定時效，或於作業期結束後即時關閉。

安碁資訊

存取控制-網路架構配置與隔離防護建議說明

- **高級**
  - **網路設備日誌與事件紀錄存放原則建議**

    考量網路管控設備之日誌與事件紀錄異機存放、保存時間長度、紀錄保護之必要防護措施。(日誌與事件紀錄留存和防護依循3.2.稽核與可歸責性之建議)

- **相關防護建議**
  - **網路拓璞繪製建議**

    繪製完整網路拓樸圖，內容需包含主要設備名稱(ICS與ICT)、所屬網段、網路邊界、使用通訊類型等，並考量高可用性機制(High Availability, HA)、區域位置等資訊。

  - **網路設置管理程序建議**

    建立網路設置管理程序，管控ICS所在環境之既有及新設各類連線機制(包含與ICS連結或未與ICS連結之連線機制，例如無線電、微波、VPN、WIFI、ADSL、LTE等)，以確保各類連線機制、技術已經安全評估(包含環境與設備的衝擊影響)、驗證及採取對應之連線控制措施等，並經管理層級核准。

經濟部能源及水資源領域工業控制系統資安防護基準-稽核與可歸責性

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保有稽核特定事件之功能，並決定應稽核之特定事件
	稽核紀錄內容	稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用日誌紀錄機制。		
	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。		
	稽核處理失效之回應	一、規定需即時通報之稽核失效事件發生時，系統應於於規定時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	稽核處理失效時，應採取適當之行動。	
	時戳及校時	一、系統內部時鐘應具備定期同步機制。 二、等級「普」之所有控制措施。		使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。
	稽核資訊之防護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、防護稽核資訊之完整性。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理僅限於有權之使用者。

稽核與可歸責性-稽核事件防護建議說明

- **普級**
  - **稽核事件紀錄留存期間建議**

    評估稽核事件紀錄留存期間(建議至少6個月)，應擬定留存方案，確保稽核紀錄的保存。

  - **稽核特定事件之能力建議**

    評估系統、設備應具備稽核特定事件之能力(例如更改密碼、登錄(入)失敗、作業系統事件紀錄、組態變更設定等)，並考量營運之需求，開啟、加強(例如啟用設定、設計程式等)與記錄稽核事件功能。

- **高級、中級**
  - **稽核事件紀錄審查週期建議**

    應定期(建議每季)進行稽核事件紀錄審查作業，並留存相關紀錄。

附表十、資通系統防護基準修正

普
一、訂定日誌之記錄時間週期及紀錄留存政策，並保留日誌至少六個月。

稽核與可歸責性-稽核處理失效之回應防護建議說明

- **中級、普級**
  - **稽核失效發生時之因應措施建議**

應考量稽核失效發生時之因應措施，例如暫停操作、稽核事件儲存空間已滿則覆蓋最早之稽核紀錄、中止稽核或系統部分功能、失效告警等。

- **高級**
  - **稽核失效事件類型與告警方式建議**

定義需及時通報之稽核失效事件(例如圖控系統、閥/閘門操控設備、資料庫系統、日誌已滿等)與通報時效，並應於規定的時效內向特定或管理人員以不限或任一之警示視窗、文字、聲音等方式提出告警。

經濟部能源及水資源領域工業控制系統資安防護基準-營運持續計畫

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
營運持續計畫	電源供應備援	一、考量廠(場)站營運之需求，規劃至少包含核心業務相關重要系統、設備在內之電源供應備援機制。 二、定期進行電源供應備援機制測試。		無要求。
	通訊線路備援	一、考量廠(場)站營運之需求，規劃至少包含核心業務相關重要系統、設備在內之通訊線路備援機制。 二、定期進行通訊線路備援機制測試。		無要求。

營運持續計畫-電源供應備援防護建議說明

- **高級、中級**
  - **電源供應備援範圍與機制建議**

應考量廠(場)站核心業務營運之需求，規劃與ICS設施、設備(例如操控室、資訊機房/工程師室、外站設施、水工設備等)之電源供應備援機制(例如發電機組、UPS機組、雙路市電、雙迴路電路等)。

應定期(例如每1年)於適當時機(例如年度營運持續演練、停俥大修)進行電力等備援機制測試，並留存保養及測試紀錄。

- **相關防護建議**
  - **發電機配置位置與保養作業建議**

發電機之配置評估設置位置(淹水考量)、儲油槽位置(工安考量)、日常儲備油量、輸油管路、油料運輸、通/排風、消防設施、輸出功率、備援機組、定期保養維護(建議每半年)等項目，並考量定期(建議每1年或停俥大修)進行一次長時間(例如4小時)運轉測試。

定期(建議每1個月)查檢UPS狀態，並留意電池汰換週期。另評估支援資訊機房UPS機組負載平衡及串連機制，並考量與ICT設備隔離之獨立空間，以及環境溫濕度監控。

經濟部能源及水資源領域工業控制系統資安防護基準-識別與鑑別

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
識別與鑑別	內部使用者之識別與鑑別	系統應具備唯一識別及鑑別使用者(或代表使用者行為之程序)之功能，禁止使用共用帳號；但操作過程中有替代之監管措施者，不在此限。		
	身分鑑別管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、等級「普」之所有控制措施。		一、使用預設密碼登入時，應於登入後要求立即變更。 二、身分鑑別相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，訂定帳號登入進行身分鑑別失敗次數，以及不允許該帳號繼續嘗試登入之時間；但操作過程中有替代之監管措施者，不在此限。 四、基於密碼之鑑別強制最低密碼複雜度；強制新密碼最少變更字元數；強制密碼最短及最長之期效限制。 五、訂定更換密碼時，異於使用過 密碼相同之次數。
	鑑別資訊回饋	應遮蔽鑑別過程中之資訊。		

識別與鑑別-身分鑑別管理防護建議說明

- **普級**
  - **帳號錯誤登入限制建議**

應考量帳號錯誤登入次數之限制(例如連續驗證失敗5次)，以及暫時中止該帳號嘗試登入之時限(例如至少15分鐘後得再行登入)。或於操作過程中採取替代之監管措施(例如加強監視機制、限制可執行登入作業之設備數量、落實交接班記錄)。

  - **密碼管控規則建議**

應建立密碼管控規則之要求，包含強制使用密碼最低複雜度(例如英文大寫、小寫、特殊符號或數字三種以上組合)、強制新密碼最少變更字元數(例如3個字元)和強制密碼最短期效(例如1天)及最長期效(例如90天)等。

  - **管理手段因應措施建議**

有關帳號密碼管控原則，宜考量利用管理手段(例如人員資安守則、例行資安防護查檢作業等)查檢落實程度，同時持續考量相關管控技術引進的可能及規劃。

附表十、資通系統防護基準修正

普
三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。

識別與鑑別-身分鑑別管理防護建議說明

- **高級、中級**
  - **自動化程式防護建議**

應考量及強化系統對於使用者身分之鑑別，考量於密碼輸入或密碼更換等視窗、頁面採用防護機制(例如雙因素認證、圖形驗證碼等)。

經濟部能源及水資源領域工業控制系統資安防護基準-系統與通訊防護

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
系統與通訊防護	資料儲存之安全	一、靜置資訊應予以防護。 二、機密資訊應加密儲存。	無要求。	無要求。
	傳輸之機密性與完整性	於資訊傳遞過程中採用加密機制；但傳輸過程中有替代之保護措施者，不在此限。	無要求。	無要求。

系統與通訊防護-資料儲存之安全防護建議說明

- **高級**
  - **資料儲存機制建議**

應識別儲存與備份之靜置資訊類別，包含系統與設備可提供之組態、日誌、事件、紀錄、程式、檔案、作業環境等，評估所需之儲存空間，考量資料增長速度及需留存之週期長度，配置足夠之儲存設備。

評估系統、設備之需求，於儲存系統上採用適宜之容錯機制，例如獨立磁碟容錯陣列(Redundant Array of Independent Disks, RAID)，並定義儲存空間使用警戒值(例如已使用空間超過85%)，評估適當之監控機制與因應措施(例如增加硬碟、移動檔案、刪除過舊檔案等)。

- **相關防護建議**
  - **備份檔案防護建議**

建立系統、設備資料儲存與備份作業完成之查檢機制，並考量和實施備份資料之完整性驗證(例如備份還原測試)。評估系統、設備之需求，建立資料備份之異機、異地存放機制，並考量備份資料傳遞與存放之安全防護。

附表十、資通系統防護基準修正

高
資通系統重要組態設定檔案及其他具保護需求之機密資訊應加密或以其他適當方式儲存。

系統與通訊防護-傳輸之機密性與完整性防護建議說明

- **高級**
  - **防護範圍與替代保護措施建議**

考量系統之運作需求，應評估經由非ICS網路進行ICS資料傳遞之過程採取可用的加密防護機制(例如SSH、SSL、TLS、加密雜湊函數、數位簽章等)；或於操作過程中採取替代之保護措施(例如專人傳遞、專線傳輸等)。

經濟部能源及水資源領域工業控制系統資安防護基準-系統與服務獲得

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
系統與服務獲得	操作、營運及運作限制文件	一、建立系統、設備操作與營運相關管理文件。 二、建立系統、設備運作限制之文件紀錄。 三、指派負責人員管理上述文件內容品質與完整，並妥善留存		
	安全措施文件	一、建立系統、設備安全防護措施之文件紀錄。 二、指派負責人員確保上述文件紀錄和實際狀態之一致性，並妥善留存。		無要求。

系統與服務獲得-安全措施文件防護建議說明

- **高級、中級**
  - **安全措施類別建議**

應建立系統、設備安全防護措施之文件紀錄，包含防護機制(例如閥/閘門開度、壓力限制、流量限制)、偵測機制(例如感測器數量與位置、感測數據之判讀原則、感測數據異常偵測機制等)、告警機制(例如警報、簡訊等)。

經濟部能源及水資源領域工業控制系統資安防護基準-實體與環境防護

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
實體與環境防護	實體存取授權	建立設施實體存取授權之人員清單，並定期或遇人員異動時進行更新。		
	實體隔離與設備進出管控	一、建立設施所在區域之實體隔離機制。 二、建立設備進出/維護申請之流程，並留存紀錄。		
	實體監視與偵測	一、於重要位置處架設監視設備，並留存監視紀錄。 二、建立實體偵測機制，包含即時告警與記錄。 三、建立外部人員陪同與記錄機制。		

實體與環境防護-實體隔離與設備進出管控防護建議說明

- **高級、中級、普級**
  - **設備進出/維護之查檢機制建議**

...具儲存元件(媒體)之攜出/入設備，評估必要之查檢機制(例如掃毒、抹除資料等)。

  - **汰換/除設備之儲存、記憶元件處理建議**

汰換/除設備依廠(場)站之報廢處理程序進行作業，委由委外廠商/外部人員攜離之汰換/除設備，應先完成移除或破壞儲存、記憶元件內之資料。

- **相關防護建議**
  - **行動裝置/媒體管控建議**

考量建立行動裝置/媒體(例如筆電、USB、隨身硬碟、手機、光碟片等)管控程序，設備連接ICS需經申請與授權，並留存紀錄。

建立行動裝置/媒體查檢機制，例如防毒軟體掃描、寫入禁止等，並於使用前後查檢行動裝置/媒體內之檔案，刪除未經允許或已無使用需求之資料。

實體與環境防護-實體監視與偵測防護建議說明

- **高級、中級、普級**
  - **監試器(CCTV)配置建議**

應考量於廠(場)站周圍、操控室、資訊機房/工程師室、工業控制設施區、外站設施、機箱與涉及重要操控之區域設置監視器(CCTV)，並評估監視影像之品質，以及紀錄保存長度(建議至少可留存1個月以上)。

前述項目之監視器(CCTV)設置，考量攝影角度，以及加強影像品質之輔助機制(例如低照度、紅外線、輔助光源等)。

- **相關防護建議**
  - **相關實體環境監控與告警建議**

建立溫濕度監控與告警機制(例如人工查檢、環控系統等)，評估設備運作之限制設定警戒值上/下限，以及量測感應裝置的配置位置。

建立消防偵測、告警機制，並配置緊急照明與適當之滅火裝置(例如資訊機房配置氣體滅火裝置)，並定期(建議每1年)進行消防設備維護與演練。

經濟部能源及水資源領域工業控制系統資安防護基準-系統與資訊完整性

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
系統與資訊完整性	日常操作與查檢紀錄	一、建立日常操作與查檢機制，並形成作業參照文件。 二、留存日常操作與查檢紀錄。		
	系統日誌資訊留存	建立日誌資訊留存機制，包含日誌資訊備份、保存。		
	系統監測工具/技術導入	導入系統營運監測工具/技術。		無要求。
	系統異常告警與通報	一、建立異常告警與通報機制。 二、留存異常告警與通報紀錄。		
	系統、設備漏洞評估	一、進行系統、設備之漏洞影響性評估，並留存相關紀錄，作為後續修補/更新規劃之依據。 二、等級「普」之所有控制措施。		蒐集、掌握既有/新進系統、設備之漏洞資訊。
	漏洞修補	二、評估已掌握之漏洞資訊，進行修補時程之規劃。 二、修補作業完成後，進行漏洞修補驗證作業，留存相關紀錄		
	故障預防	依據設備之保固或生命週期，建立故障預防機制。		無要求。

系統與資訊完整性-系統異常告警與通報防護建議說明

- **高級、中級、普級**
  - **系統異常偵測與告警建議**

應建立ICS運作邏輯檢測與告警機制，例如操作順序錯誤、參數異常(例如壓力過大、流量過大、開度指令過大、運轉速度過快、偵測數據不一致/誤差超過容許值等)、或權限衝突等，並留存相關紀錄。

系統與資訊完整性-系統、設備漏洞評估防護建議說明

- **普級**
  - **漏洞資訊蒐集來源建議**

    應蒐集、掌握既有與新建系統、設備之漏洞資訊(例如原廠資訊、弱掃報告、資安訊息/事件等)，並留存相關紀錄。

- **高級、中級**
  - **漏洞資訊影響性評估建議**

    針對已掌握之既有系統、設備之漏洞資訊，應進行影響性評估(例如漏洞嚴重程度、系統與設備資產價值、與核心業務之關連程度等)，並留存相關紀錄，作為後續修補、更新規劃之依據。

- **相關防護建議**
  - **弱掃報告處理建議**

    進行弱點掃描結果之評估，提出暫不修補之弱點項目評估原因，並留存相關紀錄。(需修補之弱點項目依循漏洞修補之建議)

系統與資訊完整性-故障預防防護建議說明

- **高級、中級、普級**
  - **平均故障時間衡量建議**

建立ICS故障預防機制，應依據過去之維護紀錄、運作紀錄、保固年限、產品生命週期等衡量其平均故障時間(Mean Time to Failures, MTTF)。

- **相關防護建議**
  - **相關設備維護措施建議**

考量電纜線與通訊線路之保護及必要標示，並評估兩類線路的適當隔離。室外線路鋪設考量地形、天災及人為破壞等各種可能因素，評估可行之屏障保護。

考量設備之地震偵測與防護措施，採取必要之固定機制(例如防震基座)和擬訂緊急應變程序(例如遇所在區域五級地震之查檢、遮斷、緊急停機作業)，並定期查檢。

考量設備(例如管線、儀器、CCTV等)之防爆機制，包含進出入設備管控程序，並定期查檢設備防爆保護。

經濟部能源及水資源領域工業控制系統資安防護基準-組態管理

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
組態管理	系統、設備變更管控	一、建立變更作業規劃及管控流程。 二、相關變更作業皆有管理階層核准確認。 三、指派負責人員執行變更作業，並留存相關紀錄。		
	變更作業測試	一、建立系統、設備變更作業之測試與驗證流程。 二、留存變更作業測試相關紀錄。		無要求。
	變更作業紀錄	建立系統、設備變更作業之紀錄，留存變更前後之相關資訊		

組態管理-系統、設備變更管控防護建議說明

- **高級、中級、普級**
  - **變更作業流程管控建議**

考量廠(場)站營運之需求，應評估系統、設備之狀態(例如故障頻率、使用年限、新技術趨勢等)，進行變更作業之規劃，並留存相關紀錄(例如執行期程、影響性評估、安全性評估、相關系統和設備介接評估等)。

應針對系統(例如組態、作業環境、版本、功能等)、設備(例如資訊設備、網路設備、DCS設備、PLC設備、外站設備、水工設備等)建立變更作業流程，並留存相關紀錄。

- **相關防護建議**
  - **緊急復原計畫建議**

建立系統、設備變更作業之緊急復原計畫，因應變更作業執行過程中可能發生的異常、失敗，即時執行復原作業。

組態管理-系統、設備變更管控防護建議說明

- **相關防護建議**
  - **軟體白名單管控建議**

評估系統、設備之需求，建立軟體白名單清冊(例如資料庫軟體、文件處理軟體、網路設備驅動軟體、防毒軟體、壓縮軟體等)，以及允許之使用版本。

定期(建議每1年)或遇重大變更時進行審查軟體白名單清冊，並確認系統、設備上所安裝軟體之符合性。

經濟部能源及水資源領域工業控制系統資安防護基準-組織管理

控制措施		系統防護需求分級		
構面	措施內容	高	中	普
組織管理	委外資安規範與要求	規劃與要求委外作業必要資安辦理事項及管控措施，並列入履約項目當中。		
	服務安全管理	一、訂定委外廠商遠端維護、到點服務及人員駐點等服務項目之管控程序。 二、等級「普」之所有控制措施。		一、依委外業務之需求，要求委外廠商/人員簽署保密合約。 二、留存相關委外服務紀錄。

組織管理-服務安全管理防護建議說明

- **普級**
  - **委外服務紀錄留存**

針對委外作業之內容，應留存各項委外服務紀錄，並妥善保存。

- **高級、中級**
  - **委外服務管控建議**

應針對委外廠商遠端維護、到點服務及人員駐點等服務項目訂定管控程序(例如人員進出管控、設備進出管控、存取帳號申請與管控、必要教育訓練要求等)。

- **相關防護建議**
  - **資安認知與專業技能訓練建議**

評估廠(場)站營運之需求，規劃人員資安認知與防護教育訓練，除基本認知課程(例如社交工程、個人資安防護等)外，另考量資安業務所需之進階技術課程(例如網路安全、防火牆管理、弱點掃描與修補等)。

自我檢核表(附件二)

廠(場)站名稱：	評估日期：　　年　　月　　日	評估人員：	
工控系統名稱：			防護需求：普
經濟部能源領域及水資源領域工業控制系統資安防護基準			
控制措施	系統防護需求分級	現況評估	發現說明
構面 / 措施內容	普		
存取控制 / 帳號管理	建立帳號管理機制，包含帳號之申請、開通、停用及刪除程序。	□符合 □部份符合 □不符合 □不適用	
存取控制 / 最小權限	無要求。	■符合 □部份符合 □不符合 □不適用	本系統屬普等級防護需求，並無規範應遵循之要求。
存取控制 / 遠端存取	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	□符合 □部份符合 □不符合 □不適用	
存取控制 / 網路架構配置與隔離	建立安全防護網路架構，管控網際網路連線存取。	□符合 □部份符合 □不符合 □不適用	

能源及水資源領域工業控制系統資安防護作業實施建議

防護建議擬定歷程

制訂階段
- 依據經濟部「防護基準」及參考行政院「防護建議」
- 配合資通安全管理法及其子法之修訂進行調整
- 參考相關國內外文獻

修訂調整階段
- 專家訪談與意見蒐集
- 舉辦草案說明會議，蒐集關鍵基礎設施提供者之看法與意見

微調與產出階段
- 進行「防護建議」內容之微調，產出最終正式版本

宣導階段
- 關鍵基礎設施提供者廠(場)站實地輔導作業
- 辦理宣導會議，進行「防護建議」說明與介紹

- 訪談專家、學者
- 防護建議草案說明會
- 試作及訪談3廠(場)站

防護基準實施建議

- 依據各領域廠(場)站針對防護建議內容提出之意見，與實地輔導作業發現，有關防護基準各控制措施防護與遵循上，有以下幾項建議與說明：

自我檢核表填寫之注意事項

存取控制構面：帳號管理；遠端存取；網路架構

營運持續計畫構面：電源供應備援；通訊線路備援

識別與鑑別構面：身份鑑別管理

系統與資訊完整性構面：系統、設備漏洞評估；漏洞修補

自我檢核表填寫之注意事項

- **填寫自我檢核表應留意：**
  - **可加強說明欄位內容之描述，包含現有具體採用之對應管控措施、執行週期、使用之紀錄表單等資訊**
  - **不適用選項原則上不建議勾選：**
    - 工控系統不支援相關功能、現有環境不存在該項作業(例如遠端存取)、經評估不適宜採用該像管控措施(例如弱點掃描)等，皆非屬不適用條件
    - 依據資安法規範，防護基準要求若屬不適用項目，需向行政院提報核准

存取控制構面建議與說明

- **帳號管理**
  - **工控系統僅提供預設帳號，不支援帳號管理功能，此可評估為「符合」。**

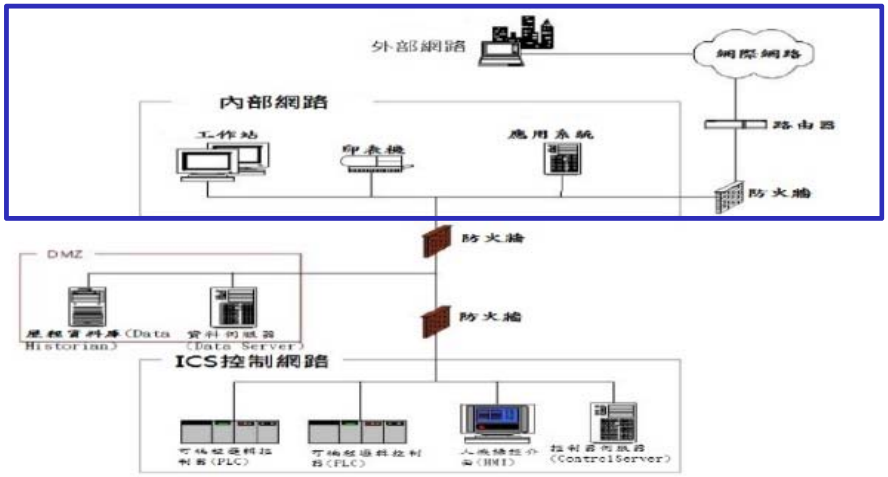
普級：
建立帳號管理機制，包含帳號之申請、開通、停用及刪除程序。
中級：
一、已逾期之臨時或緊急帳號予以刪除或禁用。
二、應禁用閒置帳號。
三、定期審核帳號之建立、修改、啟用、禁用及刪除作業。
四、等級「普」之所有控制措施。

  - **在操作過程有替代監管措施的條件下，高級防護需求應多可「符合」，但**

建議仍應定期確認帳號登錄與操作紀錄之可能異常狀況

存取控制構面建議與說明

- 遠端存取
  - 防護基準主要聚焦跨異質網路(與非ICS網路)連線之限制與管控



異質網路

  - 目前常見之遠端存取連線如RDP、Teamview、AnyDesk等多採取加密連線，可滿足高級防護需求「三、應採用加密機制」之要求。

安碁資訊

存取控制構面建議與說明

- **網路架構**
  - **目前有不少廠(場)站於工控網路邊界架設防火牆進行防護，但建議仍須注意：**

    - 防火牆規則盡量採「原則禁止、例外允許」之管控方式，並考量期效限制。
    - 防火牆規則應定期檢視。
    - 防火牆Log紀錄建議朝保留至少6個月做規劃，並應定期檢視。(檢視週期應短於Log紀錄長度)

行政院資通安全處 函

地址：10058 臺北市忠孝東路1段1號
聯絡人：侯舜仁
電子信箱：hsr@ey.gov.tw

受文者：

發文日期：中華民國110年3月2日
發文字號：院臺護字第1100165761號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：近期迭發生機關開放委外廠商自遠端進行資通系統維護致存取機制遭駭客利用，間接攻擊機關資通系統事件，為降低資安風險，請各機關加強遠端存取控制機制如說明，請查照並轉知所屬。

說明：

一、各機關開放機關內部同仁及委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理，若機關因地理限制、處理時效及專案特性等因素，須開放前揭人員自遠端存取資通系統時，應至少辦理下列防護措施：

(一)依資通安全管理法施行細則第4條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。

(二)開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。

(三)於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如 VPN)登入密碼。

營運持續計畫構面

- 電源供應備援與通訊線路備援
  - 有關備援機制測試之模式，應朝「實際演練」方式進行，其他紙本、模擬之演練作法不符合現階段防護基準之要求。
  - 定期實施備援機制測試可選擇適當時機，例如年度營運持續演練、停俥大修，以維持工控系統之穩定運轉與廠(場)站持續營運。

營運持續運作演練規劃表

承辦單位：
協辦單位：
規劃日期：

	演練規劃項目	規劃內容
1	規劃演練目標與範圍	演練目標：確保關鍵業務流程遭受重大故障和災難事件而中斷時，能以迅速、有效的方法回復正常運作。 演練範圍：
2	規劃演練腳本	如附件
3	規劃演練所需設備	
4	規劃演練所需系統	
5	規劃演練所需參與人員	
6	規劃演練時程及完成時限（完成時限參考營運衝擊分析）	
7	規劃演練測試方式與測試資源	
8	規劃演練成果的檢討時程	

營運持續運作計畫演練腳本

演練範圍：

時間	動作	參與人員	地點	備註

安碁資訊

識別與鑑別構面

- **身份鑑別管理**

- 密碼最短最長期效、變更週期、使用相同密碼代數限制等可由廠(場)站自行律定，但仍應有落實執行之作為。
- 身份驗證作業若於本機執行，無密碼傳輸情形。
- 帳戶鎖定機制可藉由實體進出管控與人員監控等方式作為替代監管措施。
- 系統除透過密碼管控機制外，若同時以License Key、原廠綁定設備序號等指定設備存取限制，可視為具有自動化程式攻擊之防護機制。
- 若工控系統因原始設計限制，僅能支援部份身份鑑別管理之功能，則屬「部份符合」狀態，建議於後續系統汰換、升級時將相關功能列入設計需求，並規劃可行之改善期程。

系統與資訊完整性構面

- **系統、設備漏洞評估**
  - **系統、設備之漏洞資訊來源包含原廠資訊、E-ISAC、資安事件/新聞等，並非僅限於弱點掃描工具。**
  - **取得系統、設備漏洞資訊後，應有影響性評估紀錄，以及應對措施規劃。**

短期對策：
1.與原廠確認該項漏洞資訊，並討論系統漏洞之防護對策，
2.加強防火牆與系統日誌紀錄查檢，檢視可能的異常狀況。

長期對策：
1.協調原廠於下次進行系統升級時，執行系統漏洞修補作業。(預計11X年實施)
2.持續蒐集與掌握系統漏洞資訊，並於年度管審會議上討論，滾動檢視漏洞修補計畫與時程。

- **漏洞修補**
  - **執行漏洞修補作業前，應依變更作業程序進行管控，並擬定緊急復原計畫。**
  - **應規劃漏洞修補之驗證作業，以確認漏洞修補完成。**

結論

結論

- 經濟部能源及水資源領域工業控制環境資安防護建議之制訂，目標在於：

可行的實作建議與方向	遵循資通安全管理法及其子法之相關規範，並在符合「經濟部能源及水資源領域工業控制系統資安防護基準」要求下，提供相關領域廠(場)站可行的實作建議方向。
引導實施資安控制措施	引導相關領域廠(場)站依據自身實際營運和資安防護需求，參酌實作建議之內容， 持續推動、實施必要之資安控制措施。
協助資安管理持續改善	協助相關領域廠(場)站持續評估各項資安管控措施的落實程度，並考量可能的資安風險，以及完成防護基準自評作業，作為工業控制系統資安防護評估之依據，達到資安管理持續改善之目的。

結論

核心→非核心

- 廠(場)站應優先檢視核心工業控制系統之防護基準要求遵循狀況，並持續擴大執行至各工業控制系統。

資通安全管理法修正

- 因應資通安全管理法之修正，經濟部防護基準與防護建議將配合進行調整，廠(場)站仍需持續留意可能的異動與變化。

敬請指導

活動滿意度問卷

https://reurl.cc/mv37MV