

核能電廠關鍵數位資產資通安全計畫 審查導則

行政院原子能委員會
中華民國 104 年 6 月

目 錄

1. 概述.....	
1.1 依據.....	
1.2 目的.....	
1.3 審查導則內容.....	
1.4 適用範圍.....	
1.5 專有名詞.....	
1.6 修訂.....	
2. 核能電廠關鍵數位資產資通安全計畫.....	
3. 核能電廠關鍵數位資產資通安全計畫實施.....	
3.1 分析數位電腦系統.....	
3.1.1 安全評估與核可.....	
3.1.2 核能電廠關鍵數位資產資通安全小組.....	
3.1.3 關鍵數位資產辨識.....	
3.1.4 深度防禦保護策略.....	
3.1.5 安全管控措施.....	
3.1.5.1 技術管控.....	
3.1.5.1.1 存取控制.....	
3.1.5.1.2 稽核及當責.....	
3.1.5.1.3 關鍵數位資產系統及通訊保護.....	
3.1.5.1.4 辨識及驗證.....	
3.1.5.1.5 系統強化.....	
3.1.5.2 操作管控.....	
3.1.5.2.1 儲存媒介保護.....	
3.1.5.2.2 人員保安.....	
3.1.5.2.3 系統及資訊完整.....	
3.1.5.2.4 關鍵數位資產設備維護.....	
3.1.5.2.5 實體及環境保護.....	
3.1.5.2.6 事件回應.....	

3.1.5.2.7	意外事件應變/SSEP 功能持續計畫.....
3.1.5.2.8	認知及訓練.....
3.1.5.2.9	構型管理.....
3.1.5.3	管理管控.....
3.1.5.3.1	系統及服務取得.....
3.1.5.3.2	安全評鑑及風險管理.....
3.2	納入實體保安計畫.....
3.3	政策及實施程序.....
4.	核能電廠關鍵數位資產資通安全計畫維護.....
4.1	持續監測及評估.....
4.2	變更控制.....
4.3	核能電廠關鍵數位資產資通安全計畫內部審查.....
5.	文件控制及紀錄保存.....
	中英名詞對應.....
	章節對照表.....

1. 概述

1.1 依據

美國聯邦法規 10 CFR 73.54 “Protection of digital computer and communication systems and networks.”，要求美國核能電廠對執行安全、保安、對安全重要及緊急應變等功能(Safety-related and important-to-safety functions, Security functions, Emergency Preparedness function, and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions，以下稱SSEP)的系統，以及支援系統和設備，若遭受損害，會導致應有功能有不良影響之相關關鍵數位資產實施資通安全計畫(以下稱關鍵數位資產資通安全計畫或資通安全計畫)。

行政院科技顧問組（現稱行政院科技會報）於「2010 資通安全政策白皮書」將關鍵資訊基礎建設保護列為重要行動方案，並於2011 年完成「關鍵資訊基礎建設保護政策指引」，建置我國關鍵資訊基礎建設保護機制。

本審查導則內容以美國核能管制委員會 2010 年發布的法規指引RG 5.71 “Cyber Security Programs for Nuclear Facilities.”為範本，參酌 NUREG-0800 “Standard Review Plan”第13.6.6 節 “Cyber Security Plan”審查內容，並依據我國環境以及核能安全委員會審查導則格式，完成本審查導則。

1.2 目的

為完備我國核能電廠關鍵數位資產資通安全防護體系，要求核能電廠必須針對執行安全、保安、對安全重要及緊急應變等相關之關鍵數位資產提出資通安全計畫，並接受管制單位審查及視察。

1.3 審查導則內容

『核能電廠關鍵數位資產資通安全計畫審查導則』以核能電廠關鍵數位資產為保護主體，採用美國核能管制委員會 2010 年 2 月頒布之 RG 5.71 “Cyber Security Programs for Nuclear Facilities.”為範本，並參酌 NUREG-0800 “Standard Review Plan” 第 13.6.6 節 “Cyber Security Plan”以及我國行政院科技顧問組「2010 資通安全政策白皮書」內容，完成本審查導則，作為審查我國興建中核能電廠提報關鍵數位資產資通安全計畫之依據。

本審查導則內容分第一章概述，描述關鍵數位資產資通安全計畫依據、目的、範圍及專有名詞 關鍵數位資產資通安全計畫，

描述核能電廠關鍵數位資產安全小組架構、成員及責任。第三章關鍵數位資產資通安全計畫實施，描述安全管控措施。第四章為關鍵數位資產資通安全維護，透過不斷的評鑑和修訂，以確保關鍵數位資產資通安全計畫之效能。第五章文件控制及紀錄保存。

1.4 適用範圍

本審查導則適用範圍為我國興建中核能電廠執行SSEP功能之關鍵數位資產保護。

1.5 專有名詞

A. SSEP(Safety-related and important-to-safety functions, Security functions, Emergency Preparedness function, and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.): 執行安全、保安以及緊急應變功能與支援上述功能之系統或裝置，其損害會危害上述功能。

B. 關鍵系統(Critical System): 包括(1)執行或被依賴以執行SSEP功能；(2)影響SSEP功能或影響關鍵系統及/或關鍵數位資產執行SSEP功能；(3)提供路徑至關鍵系統及/或關鍵數位資產，這些路徑可被用來危害、攻擊或降低SSEP功能；(4)支援關鍵系統及/或關鍵數位資產；(5)保護任何上述系統免於受網路攻擊乃至設計基礎威脅之系統。

C. 關鍵數位資產(Critical Digital Asset, CDA): 為關鍵系統之子元件，包含數位設備、電腦、通訊系統和網路等。

D. 資通安全攻擊(Cyber Attack): 駭客或內部人員透過網路、連接線與連接點，對關鍵數位資產發動或導致蓄意或非蓄意的資通安全危害事件。

E. 資通安全評鑑(Cyber Security Assessment): 初始關鍵數位資產資通安全計畫與後續年度之審查，以評鑑關鍵數位資產資通安全計畫的適當性。

F. 深度防禦保護策略(Defense-in-Depth Protective Strategies): 利用備援與多重功能的安全管控措施，以建立多層防禦來保護關鍵數位資產。在深度防禦防護策略下，單一保護策略或安全管控措施的失效須不會導致危害安全、對安全重要、保安或緊急應變功能。

G. 風險：由於從事某項特定活動過程中存在的不確定性，而產生的經濟或財務損失、自然破壞或損傷的可能性。

H. 威脅：意指天然災害或人為事件對生命、資訊、運轉、環境或財產可能造成損害。

I. 弱點：任何會導致應用程式、系統或設備出現隱含或外顯問題，使得資料失去機密性、完整性或可用性的因素。

J. 弱點掃描：模擬攻擊者所發出的攻擊動作，以無傷害性的攻擊來檢查連接到關鍵數位資產之網路設備，或是應用於數位資產內的作業系統。

K. 弱點評估：對弱點的威脅及風險進行分級，再根據弱點風險及嚴重性決定修補的優先順序。

L. 風險評鑑：對關鍵數位資產及設施的威脅、衝擊及弱點及其發生可能性的評鑑。

M. 風險管理：以可接受的成本，對可能影響關鍵數位資產的安全風險進行評鑑、控制及降低或排除的過程。

N. 安全邊界(Security Boundary)：一個實體或邏輯上的分隔，具有不同安全要求的防禦水準之分界點。

O. 安全管控措施：RG 5.71 附錄B 及C 所列之項目，附錄B 是指技術性的安全管控措施的項目，包含存取控制、稽核和責任歸屬、關鍵數位資產和通訊的保護、辨識和鑑定，以及系統強化；附錄 C 說明操作和管理的安全管控措施的項目，包含儲存媒介的保護、人員資安管制、系統和資訊整合、維護、實體和環境保護、防禦策略、事故反應、意外事故應變計畫、認知及教育訓練、構型管理，以及在取得系統和服務的相關事項、安全評估及風險管理上所需的安全管控措施。

P. 關鍵數位資產資通安全計畫：計畫內容敘述數位電腦通訊系統和網路保護之需求，及保護關鍵數位資產免於資通安全攻擊。

Q. 關鍵數位資產資通安全計畫生命週期：指關鍵數位資產資通安全計畫之計畫建置、整合、持續監控、管控計畫審查、變更管理及文件保存等循環維護過程。

R. 工作人員：對核能電廠關鍵數位資產負責操作之人員，包含營運操作、現場施工及電廠陪同人員。

S. 一般使用者：非關鍵數位資產資通安全計畫小組成員之使用人員。

T. 廠商：指提供核能電廠系統設備的供應商、維護商或製造商。

U. 管制單位：指核准、監督之單位，現為核能安全委員會。

V. V.FIPS 140-2 加密模組：FIPS(Federal Information Processing Standard) 140-2 規範由 NIST(National Institute of Standards and Technology) 2001 年修定公布，為目前國際業界密碼學模組共同規範標準。美國政府要求政府機關採購資訊相關設備時，必須符合此規範。

W. 雙重授權(Dual Authorization)：兩個(含)以上授權執行特殊權限工作，授權方式可為技術或管理方式實施。

1.6 修訂

本審查導則如有未盡事宜，得視需要修訂之。

2. 核能電廠關鍵數位資產資通安全計畫

本章描述核能電廠應針對執行安全有關及對安全重要、保安功能及緊急應變功能(SSEP)之關鍵數位資產擬訂關鍵數位資產資通安全計畫，並督促所屬部門及成員依規定實施關鍵數位資產資通安全計畫。

(一) 審查範圍

審查人員應審查核能電廠提供執行安全、保安、緊急應變計畫相關之關鍵數位資產資通安全計畫，其中包含資通安全政策、資通安全小組、關鍵數位資產辨識、防禦策略、安全管控措施，關鍵數位資產資通安全計畫紀錄與維護。

(二) 程序審查

審查人員應審查核能電廠關鍵數位資產資通安全計畫是否符合上述審查範圍所規定之基本要求，並決定資料詳細程度是否足以提供審查人員進行關鍵數位資產資通安全計畫之細部審查，以保障關鍵數位資產的安全高度保證。審查人員應確認計畫之內容包含以下資訊：

1. 核能電廠關鍵數位資產資通安全計畫目標。
2. 核能電廠的位置及地址。
3. 專有名詞。
4. 引用之法規及準則。
5. 參考文獻。
6. 關鍵數位資產資通安全計畫相關圖件及安全管控措施與程序。

(三) 審查要點與接受基準

核能電廠關鍵數位資產資通安全計畫應包含如下內容：

1. 關鍵數位資產資通安全概述。
2. 目標及範圍。
3. 關鍵數位資產資通安全小組組織與權責。
4. 安全管控措施概述。
5. 計畫實施與維護。
6. 關鍵數位資產資通安全計畫內部審查。

(四) 審查發現

審查人員應確認核能電廠關鍵數位資產資通安全文件圖表完整齊備。目標及程序必須完整涵蓋關鍵數位資產生命週期、資通安全生命週期內容完整、專有名詞定義須明確，並提供法規依據及參考文獻以供審查。

(五) 參考法規與技術規範

1. 10 CFR 73.54, “Protection of digital computer and communication systems and networks”.
2. 10 CFR 73.55, “Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage”.
3. RG 5.71 “Cyber security program for nuclear facilities”.
4. NUREG-0800 “Standard Review Plan” 13.6.6.

3. 核能電廠關鍵數位資產資通安全計畫實施

本章描述核能電廠實施關鍵資訊系統資通安全計畫所必要的作業範圍及內容。參考 10 CFR 73.54 要求，核能電廠應建置和維護關鍵數位資產資通安全計畫，以確保核能電廠安全有關與對安全重要、保安功能及緊急應變功能(Safety-related and important-to-safety, Security and Emergency Preparedness, SSEP)及其支援系統，維持高度安全運轉保證。實施範圍包含防禦策略、安全管控措施及維護資通安全計畫等。

核能電廠應提供所有關鍵數位資產的安全管制措施詳實文件，以供管制單位查閱。管制措施之變更，若將導致關鍵數位資產資通安全計畫之效能降低，核能電廠應備具理由，向管制單位提出申請，並取得管制單位核准。當發現資通安全攻擊和事件時，應向管制單位報告。

3.1 分析數位電腦系統

3.1.1 安全評估與核可

(一) 審查範圍

核能電廠應定期檢查核能電廠關鍵數位資產資通安全計畫及更新，以確保關鍵系統安全運轉之高度保證

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全計畫安全評估與核可：

1. 核能電廠應擬訂關鍵數位資產資通安全實施計畫，並每年就下列事項進行內部審查和更新：
 - A. 明文擬訂關鍵數位資產資通安全規劃、評估和授權政策，定義目的、範圍、角色、責任和管理者承諾，並協調相關單位部門推動關鍵數位資產資通安全計畫。
 - B. 明文擬訂作業程序以實施關鍵數位資產資通安全計畫及安全評估。

(四) 審查發現

審查人員應確認核能電廠關鍵數位資產資通安全計畫實施證明文件齊備，並確實擬訂符合本導則規範之關鍵數位資產資通安全計畫實施內容。當核能電廠無法實施安全管控措施，應確實說明理由及採取替代安全管控措施(如可證明攻擊不存在，可以不實施替代安全管控措施)。

(五) 參考法規與技術規範

1. 10 CFR 73.54(b)(2) “Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.1.1, Appendix A.3.1.1.

3.1.2 核能電廠關鍵數位資產資通安全小組

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全小組，包含資通安全小組成員、角色任務及應具有之專業知識等。資通安全小組應被充分授權協調各部門和資源，以達資通安全目的。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 核能電廠關鍵數位資產資通安全小組必須被充分授權進行客觀評估、執行決策與實施深度防禦保護策略。
2. 核能電廠關鍵數位資產資通安全小組成員至少必須包含下列人員：
 - A. 核能電廠副廠長(含)以上人員擔任關鍵數位資產資通安全計畫負責人及資源整合任務。
 - B. 關鍵數位資產資通安全計畫經理：負責監督關鍵數位資產資通安全計畫實施及對外連絡事宜。
 - C. 關鍵數位資產資通安全專家：負責核能電廠資通安全之防

護作為，包括廠區的網路、軟、硬體設備及其作業環境之了解、關鍵數位資產稽核、弱點評估、網路掃描及滲透測試等，並於發生事件期間指揮資通安全事件回應小組，及資通安全事件調查期間的證據搜集與保存。

- D. 關鍵數位資產資通安全事件回應小組：當懷疑資通安全事件發生時，負責採取適當的回應及保護措施，並協助受損的系統回復作業。
 - E. 其他相關人員：必須包括運轉、維護和設計等相關人員。必要時得要求工程師、一般使用者、合約廠商及供應商人員參與。
3. 核能電廠關鍵數位資產資通安全小組成員應具有下列專業知識：
- A. 資訊及數位系統技術：包含網路安全、軟體開發、通訊、計算機管理、計算機工程和計算機網路等。數位系統涵蓋數位儀控系統、程式化邏輯控制器(PLC)、控制系統和分散式控制系統等。資訊系統包含計算機系統、資料庫和關鍵數位資產設計、操作及維護等。
 - B. 核設施之操作、工程和安全：包含整體設施運作和電廠技術規範。
 - C. 實體保安和緊急應變計畫。
4. 核能電廠關鍵數位資產資通安全小組應具有下列角色及責任：
- A. 執行或監督各階段資通安全及管理程序。
 - B. 在評估過程中，記錄所有重要的觀察、分析和發現可供選擇做為安全管控措施所需的資訊。
 - C. 持續評估現有資通安全的威脅、潛在的弱點和受攻擊後的後果之假設與結論、現存的資通安全控制措施、防禦策略和攻擊減緩的方法；對負責關鍵數位資產工作人員進行資通安全管控措施的認知和訓練。
 - D. 以實體或電子方式逐項檢查所有關鍵數位資產及其連接設備所取得的資訊，並且確認其受安全管控措施保護。
 - E. 辨識與實施潛在的新資通安全管控措施。
 - F. 記錄或監督資通安全計畫的安全管控措施實施，對於未能實施者要有說明文件或是提供其它替代安全管控措施。
 - G. 依本導則第 5 章所述，保存所有評估紀錄，包含筆記及其它支援資訊。

(四) 審查發現

審查人員應確認核能電廠關鍵數位資產資通安全小組成立，小組負責人為擁有協調指揮全廠資源職權之高層人員擔任。小組成員確實包含所有資通安全作業相關人員。所有小組成員具有足以勝任之專業知識。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C3.1.2.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix A.3.1.2.

3.1.3 關鍵數位資產辨識

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產辨識，包含：(1)關鍵系統及關鍵數位資產辨識流程；(2)關鍵數位資產之描述；(3)關鍵數位資產之審查及驗證。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 核能電廠應依如下有關數位資產辨識方法與流程：
 - A. 辨識並記錄核能電廠之所有與安全、保安及緊急應變(SSEP)有關或支援 SSEP 之系統、裝置、通訊及網路，簡稱關鍵系統(CS)。關鍵數位資產資通安全小組應進行廠區初步辨識分析，當這些系統、裝置、通訊或網路遭受到危害、利用或破壞時，將影響安全、保安及緊急應變之功能。
 - B. 對所有關鍵系統執行路徑分析。
 - C. 對每關鍵系統辨識關鍵數位資產(CDA)。
 - D. 對每關鍵系統，應有如下紀錄文件：
 - (1) 關鍵系統、資產或網路一般描述。
 - (2) 關鍵系統的關鍵數位資產辨識。
 - (3) 關鍵數位資產功能簡要說明。

- (4) 分析關鍵數位資產遭受到危害時，將會造成關鍵系統和安全、保安及緊急應變的潛在影響。
 - (5) 辨識關鍵數位資產的數位設備直接或間接所扮演的角色(如保護、控制、監視、報告或通訊)。
 - (6) 資通安全功能需求或規格，包含如下：
 - a. 供應商和開發商為維持系統完整性而提供資通安全資訊。
 - b. 關鍵數位資產的安全構型、安裝及作業。
 - c. 如何有效的使用及維護資通安全的特性及功能。
 - d. 管理(administrative)功能（例如特別權限等）之設定與使用上之已知弱點。
 - e. 使用者可存取的資通安全和特性/功能，以及使用者如何有效的使用這些資通安全特性/功能。
 - f. 使用者與關鍵數位資產間之互動方式，使用者如何安全使用這些系統。
 - g. 使用者維護關鍵數位資產安全的責任。
2. 核能電廠應對所有關鍵數位資產實施下列描述及防禦措施：
- A. 列出直接或間接之連接路徑。
 - B. 相互依存的基礎建設。
 - C. 防禦策略，包含防禦模式、安全管控措施及其它防禦措施。
3. 核能電廠關鍵數位資產資通安全小組應對上述第 2 點的動作進行如下審查及驗證：
- A. 進行每個關鍵數位資產連結和構型的實體查驗。
 - B. 追蹤所有關鍵數位資產通訊傳輸終端設備之連入及連出路徑。
 - C. 檢查關鍵數位資產及其連線路徑設備的實體安全措施。
 - D. 沿著通訊路徑檢查既有安全設備的構型（例如防火牆、入侵偵測系統、單向網路(diode)等），並評估其效能。
 - E. 檢查所有關鍵系統/關鍵數位資產間相互依存關係。
 - F. 檢查與基礎建設類支援系統的相互關係，特別注意電力、環境控制和消防設備的可能潛在危害。
 - G. 檢查廠區的系統、網路及通訊系統受到攻擊的潛在路徑。
 - H. 當審查時，需找出關鍵數位資產和關鍵系統中，資訊與構型差異的解決計畫，包含未記錄或失去連線的異常事項，及關鍵數位資產與資通安全相關的違規行為。

(四) 審查發現

審查人員應確認核能電廠關鍵數位資產辨識文件圖表完整齊備，並提出完整審查及驗證參考文件以供審查。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.1.3, C 3.1.4.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix A.3.1.3, A.3.1.4.

3.1.4 深度防禦保護策略

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產深度防禦保護策略計畫，至少應包含第 1 層、第 2 層、第 3 層和第 4 層等，關鍵數位資產應受保護於第 3 層或第 4 層，以及資通安全邊界設備之安全管控措施。核能電廠關鍵數位資產資通安全深度防禦保護策略，包含：(1)深度防禦保護策略政策及程序；(2)不同安全邊界設備安全管控措施。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠應依如下所列，完成關鍵數位資產資通安全計畫深度防禦保護策略：

1. 核能電廠應實施和記錄深度防禦保護策略：
 - A. 將核能電廠區域安全分級(如第 1 層、第 2 層、第 3 層及第 4 層等)，對安全、對安全重要及保安之關鍵數位資產設備應配置於最高安全層級區域(如第 4 層)，以防止受到低安全層級的影響。
 - B. 不得對最高安全層級區域的關鍵數位資產進行遠端存取。
 - C. 防止不同安全層級間的網路位址欺騙。
 - D. 僅允許由第 4 層至第 3 層，以及由第 3 層至第 2 層之單向資料流(data diodes)。
 - E. 禁止從低安全層級(第 1、2 層)的數位資產向高安全層級(第 3、4 層)的數位資產進行通訊。

- F. 所有非安全系統對安全系統進行雙向通訊時，其亦要給予和安全系統相同等級的安全保護。
 - G. 在各安全級別的邊界設備必須具有入侵防禦及偵測的能力。
 - H. 確保在不同安全層級的雙向資料流設備，具有偵測、防止、延遲、減緩和復原從低安全層級過來之安全攻擊。
 - I. 將低安全層級資料、軟體、韌體和設備移至較高安全層級，必須經記錄驗證程序或流程，以確保這些設備的資料、程式碼或資訊是值得信賴的，未被植入惡意程式(Malware)、木馬程式(Trojan Horse)，蠕蟲或其它攻擊程式。
2. 不同安全層級間邊界設備應包括如下內容：
- A. 在實體和邏輯上保護和強化關鍵數位資產，以防止未經授權的存取或操作。
 - B. 採用安全的通訊管理及加密等安全管控措施。
 - C. 提供日誌和警報功能。
 - D. 提供入侵偵測和防禦的功能。
 - E. 在防禦邊界偵測並防止惡意程式。
 - F. 具有執行跨越於防禦邊界設備之通訊協定狀態檢查以上之能力(如透過應用代理伺服器)。
 - G. 若無法實施單向資料流，至少應實施包含如下規則：
 - (1) 採取正向表列，列舉授權流量，其餘全部禁止。
 - (2) 提供通訊協定、來源、目的過濾功能例如 IP 位址、MAC 位址、TCP 埠及 UDP 埠。
 - (3) 阻斷功能支援來源和目的位址、服務、通訊埠。
 - (4) 不允許原廠預設的通訊傳輸設定(例如允許雙向傳輸)。
 - (5) 由直接連接(例如筆電)或經由專屬的介面連接到安全的中央網路來管理防火牆。
 - (6) 除了上述第(5)項外，不允許由其他介面連接至防火牆進行管理設定作業。
 - (7) 記錄接受或拒絕之連接、傳輸監控、分析及入侵偵測等資訊。
 - (8) 集中日誌管理。
 - (9) 實施目標授權，僅授予使用者連接必要的 CDA，達其目標所需功能之權限。
 - (10) 記錄資訊流，以監控流量、分析與入侵行為偵測。

- (11) 部署和維護授權之人員擁有適當技術教育訓練。
- (12) 應事先規劃必要之網路連線，當發生重大資安事件或授權人員下令時，可及時隔離企業網路與資料收集及控制網路。
- (13) 修改防火牆防禦規則韌體和軟體佈署前，必須經評估、分析和測試。
- (14) 時間同步必須透過信任網路、直接連接至關鍵數位資產或經由 SNTP，及信任之安全金鑰。
- (15) 與關鍵數位資產時間同步，以確保取得的相關事件記錄與時間參考基準一致。
- (16) 以資訊標準格式，將紀錄檔送至紀錄伺服器主機或單向傳送至外部紀錄蒐集設備上。
- (17) 以經適當訓練之人員進行例行審查和分析紀錄檔，以偵測惡意程式或不正常活動。
- (18) 每季檢查、更新規則設定一次。
- (19) 使用已實體或邏輯安全強固的計算設備以及流量控制，以防止未授權存取或操作資料。
- (20) 不允許任何從低安全層級之網路、系統或關鍵數位資產執行訊號交換(handshaking)通訊協定至最高安全層級之網路、系統或關鍵數位資產。
- (21) 防止病毒、惡意程式或不必要之程式，散播至不同安全層級間。

(四) 審查發現

審查人員應確認核能電廠實施深度防禦策略，具安全、保安及緊急應變(SSEP)功能設備，均設置於第 4 層或第 3 層安全層級區域內。置於安全防禦邊界之設備符合上述安全防護措施。

(五) 參考法規與技術規範

1. 10 CFR 73.54(c)(2) “Apply and maintain defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber attacks.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.2.
3. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.6, C.7.
4. RG 1.152 “Criteria for use of computers in safety systems of

nuclear power plants” B.

3.1.5 安全管控措施

核能電廠應依實施和記錄下列事項，以建置深度防禦保護策略：

1. 描述防禦架構模式。
2. 建立實體及行政安全管控措施。
3. 操作及管理的安全管控措施，並檢驗其在關鍵數位資產的保護效能。

核能電廠應依 3.1.5.1 所述實施安全管控措施，當安全管控措施無法實施時，應採取替代安全管控措施並記錄如下資訊：

1. 記錄所採用的替代技術安全管控措施之基準。
2. 實施並記錄關鍵數位資產之攻擊向量或攻擊樹分析，並確認替代技術安全管控措施之替代安全管控措施具有相同或優於 3.1.5.1 所述安全保護層級。
3. 不實施關鍵數位資產安全管控措施，應執行下列步驟：
 - A. 執行關鍵數位資產攻擊向量和攻擊樹分析。
 - B. 記錄攻擊向量和攻擊樹不存在，以表示安全管控措施是沒有必要的。

因實施 3.1.4 深度防禦保護策略及本節安全管控措施而會影響到 SSEP 的正常功能或效能時，不得採用這些安全管控措施。核能電廠應採取替代安全管控措施來保護關鍵數位資產，以免擴及 DBT 的資通安全攻擊。

核能電廠應實施效益分析、弱點評估/掃描，以驗證安全管控措施，確保關鍵數位資產具有防禦資安攻擊的高度保證(High Assurance)。

3.1.5.1 技術管控

審查人員依據本導則，審查核能電廠技術、操作及管理安全管控措施。技術管控措施係以硬體、韌體、作業系統或應用軟體等非人為管理機制作為。包含：(1)存取控制；(2)稽核與當責；(3)關鍵數位資產及通訊保護；(4)辨識及驗證；(5)系統強化。

技術安全管控措施，採取自動化機制，以事先設計方式，當系統發現違反經設計之作業或攻擊事件時，會自動觸發反制或利

用電子機制強化安全政策。

3.1.5.1.1 存取控制

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產存取控制安全管控措施。核能電廠應擬訂存取管理政策及實施程序，以確保僅有被授權人員具有存取權。包含：(1)存取控制政策及程序；(2)帳號管理；(3)存取強化；(4)資訊流；(5)功能分離；(6)權限最小化；(7)失敗之登入嘗試；(8)系統使用通知；(9)登入通知；(10)連線階段鎖定；(11)存取管控監督與審查；(12)允許不驗證和授權之活動；(13)自動標示；(14)自動標籤；(15)網路存取控制；(16)通訊協定；(17)無線存取限制；(18)不安全及非法連線；(19)可攜式和行動裝置；(20)當採用第三方(Third party)產品；(21)外部系統使用；(22)公開可存取的內容等。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

存取控制的目的是確保只有經過授權程序的人員或程式可以對關鍵數位資產進行存取。核能電廠應完成如下之存取控制項目，審查人員依如下規範審查：

1. 存取控制政策及策略

核能電廠依年度更新關鍵數位資產存取控制策略正式文件，內容敘述目的、範圍、角色、責任及管理者的承諾，以及對於此策略的內部協調，存取控制政策敘述內容含如下事項：

- A. 存取控制權和存取控制特許權。
- B. 關鍵數位資產管理。
- C. 保護密碼/金鑰資料庫，以避免主要使用者及密碼清單遭未授權存取。
- D. 對關鍵數位資產人員權責變更，或系統設定，或功能變更調整後，進行稽核存取控制。
- E. 存取權限必須經過指定授權，責任獨立(separation of

duties)。

2. 帳號管理

核能電廠應執行下列帳號管理項目：

- A. 管理和記錄關鍵數位資產的帳號，內容包含授權、啟用、活動、變動、審核、失效和移除。
- B. 至少每月執行一次：審查關鍵數位資產帳號符合由資通安全程序所提供的存取控制名單，並且在關鍵數位資產帳號上啟動必要的動作。
- C. 依工作性質提供需要的存取權限。
- D. 當人員工作性質變更時，內部審查其存取權限，以確保兩者相符。
- E. 採用自動機制支援關鍵數位資產帳號管理功能和啟動。包含：
 - (1) 至少每月執行一次：終止臨時、來賓及緊急帳號。
 - (2) 至少每月執行一次：關閉沒使用的帳號。
 - (3) 對帳號之新增、修改和刪除，建立及保護稽核紀錄。
 - (4) 使用者帳號的新增、修改和刪除動作，記錄並通知管理者，使得管理者注意到任何帳號的修改，以確保能及時發現潛在的資安攻擊事件。

3. 存取強化

核能電廠應執行下列事項：

- A. 依據既定的政策和程序，對關鍵數位資產指定存取授權。
- B. 賦予所有使用者的權限，以符合其對關鍵數位資產的權限。
- C. 定義並記錄關鍵數位資產相關的特定功能及安全相關資訊。
- D. 人員執行特定存取功能及安全相關資訊必須符合既定的政策及程序。
- E. 限制特定存取功能(如佈署軟體、硬體和韌體等)及安全相關資訊給授權人員。
- F. 關鍵數位資產使用者對特定存取功能，必須採取雙重授權。
- G. 確保並記錄存取機制不會影響到關鍵數位資產的安全，並且當無法執行安全管控時，必須採取相應的替

代補足安全管控措施。

4. 資訊流

核能電廠應執行下列資訊流管控措施：

- A. 依據防禦策略，對關鍵數位資產及相連接系統間，即時加強管控資訊流之授權紀錄。
- B. 依據擬訂的防禦策略，電廠維護相關人員維護描述關鍵數位資產、資通安全邊界設備和邊界之間允許與否的資訊流類型，及允許資訊流授權的需求程度之文件。
- C. 實施並記錄受保護設備的資訊流管控，作為管控的決策基礎。
- D. 具有即時偵測、防止和回應非法或未授權的資訊流之能力。
- E. 加密資料不得規避內容檢查機制。
- F. 以硬體機制實施單向資訊流。
- G. 基於狀態變更或營運考量，執行允許或不允許的應變資訊流政策。
- H. 存取控制政策中，設定關鍵數位資產，使得使用者認證資料不會以明碼形態傳輸。

5. 功能分離

核能電廠應執行下列的功能分離管控措施：

- A. 建立並記錄各部門的責任及功能分離，並消除利害衝突及確保每人責任及功能獨立行使。
- B. 透過存取授權分派，實施關鍵數位資產的功能分離。
- C. 當系統無法提供功能分離時，必須有對關鍵數位資產採取替代安全管控方案之判斷理由，及其相對的稽核對策。

6. 權限最小化

核能電廠應實施使用者權限最小化：

- A. 設定關鍵數位資產最嚴格權限或使用者之存取需求。
- B. 當系統無法提供權限最小化時，必須有對關鍵數位資產採取替代安全管控措施之判斷理由，及其相對應的稽核對策。

7. 失敗的登入嘗試

核能電廠應對失敗的登入嘗試，進行下列事項：

- A. 限制使用者嘗試無效登入的次數，規範在特定時間內

- 嘗試登入失敗的次數後，系統自動執行鎖定模式。
- B. 當關鍵數位資產無法支援帳號鎖定，或因效能考量而採取替代安全管控措施時，應敘明判斷理由。
 - C. 應設定當連續嘗試登入不成功的即時警報。
 - D. 應有嘗試登入不成功的日誌和紀錄。
8. 系統使用通知
- A. 當下列情形時，系統必須於使用者存取資訊前，顯示系統使用通知訊息：
 - (1) 使用者存取受管制的系統。
 - (2) 使用被監控、記錄及接受稽核的系統。
 - (3) 禁止未經授權者使用關鍵數位資產，違反者將受懲處。
 - B. 關鍵數位資產系統使用通知訊息必須為隱密和安全的。
 - C. 關鍵數位資產系統使用通知訊息，事先應經核准。
 - D. 系統使用通知訊息會持續顯示，直至使用者採取對應登入措施。
 - E. 當系統無法支援系統使用通知訊息給使用者時，應安裝其它實體通知機制。
9. 登入通知
- 核能電廠應執行下列事項：
- A. 當使用者登入成功後，顯示出上次登入的時間和日期及自從上次成功後，登入失敗的次數。
 - B. 要求所有使用者必須向關鍵數位資產資通安全小組經理回報任何可疑的網路安全活動。
10. 連線階段(Session)鎖定
- 核能電廠應下列事項：
- A. 當網路連線 30 分鐘沒動作時，鎖住此連線階段。
 - B. 提供使用者自動鎖住連線階段機制。
 - C. 維持鎖定狀態，直至使用者重新辨識驗證程序。
 - D. 當關鍵數位資產無法提供連線階段鎖定功能時，應採取下列替代管控措施：
 - (1) 實體限制存取。
 - (2) 監控和記錄實體存取，以即時偵測和回應入侵。
 - (3) 採取稽核和驗證。
 - (4) 確認使用者為被授權者。

(5) 確認被授權人員值得信賴。

11. 存取管控監督與審查

核能電廠應執行下列事項：

- A. 對於使用者存取控制所執行的動作進行記錄、監督和審查。
- B. 於關鍵數位資產及設施，採取自動化機制協助審查使用者活動。

12. 允許不辨識及驗證之活動

核能電廠應執行下列事項：

- A. 於正常或特殊狀態下，允許不辨識及驗證的帳號操作關鍵數位資產，應確認和記錄。
- B. 僅在特定需求和任務要求下，允許不辨識及驗證之活動，且其活動不得影響安全、保安及緊急應變(SSEP)功能。

13. 自動標示

核能電廠應執行下列事項：

- A. 確定實施標準的定名規則，以供傳播、處理或分佈時的識別。
- B. 確保關鍵數位資產之列印報表和電子檔使用標準命名，以供傳播、處理或分佈時的識別。

14. 自動標籤

核能電廠應對列印報表及電子檔儲存、處理和傳送過程粘貼標籤。

15. 網路存取控制

核能電廠應採用 MAC 位址鎖定、實體或電子隔離、靜態列表、加密或監控等資安攻擊減緩技術。

16. “開放的/不安全的”(Open/Insecure)通訊協定的限制

核能電廠應執行下列事項：

- A. 當通訊協定缺乏安全管控措施時，應記錄和實施額外預防措施，以保護網路和匯流排(Bus)通訊，避免未授權存取。
- B. 應防止從不同安全層級外，發送網路通訊協定命令。
- C. 不可由“開放的/不安全的”通訊協定發送降低關鍵數位資產變更安全狀態的命令。

17. 無線存取限制

核能電廠應執行下列事項：

- A. 核能電廠應將無線連結設備視同為安全邊界外的設備，所有無線設備存取關鍵數位資產需經由安全邊界設備。
 - B. 不得使用無線技術執行關鍵數位資產與安全相關和重要安全功能。
 - C. 無線不使用時應關閉。
 - D. 建立無線技術之使用限制和實施指引。
 - E. 為確保防禦策略，需有紀錄、說明、授權、監控對關鍵數位資產無線存取等安全管控措施。
 - F. 至少每週執行一次：頻率掃描，以防止未授權之無線通訊頻率，發現未授權無線通訊接收點，應予以關閉。
18. 不安全及非法連線
核能電廠關鍵數位資產變更佈署時或至少每月執行一次查驗，確認沒有不安全及非法的連結。
19. 可攜式和行動裝置
核能電廠對可攜式設備應：
- A. 建立並記錄可攜式和行動設備裝置的使用限制及使用說明。
 - B. 對關鍵數位資產存取的上述設備進行授權與管控。
 - C. 所有允許存取關鍵數位資產的可攜式和行動裝置，其安全層級應視同關鍵數位資產。
 - D. 確保可攜式和行動裝置僅在相同安全層級上使用。
20. 當採用第三方(Third Party)產品，應確保：
- A. 不可使用未經授權第三方設備商的安全解決方案。
 - B. 第三方產品應經合約供應商的認可，否則應採取其它替代安全管控措施。
21. 核能電廠外部系統使用
- A. 核能電廠應確保第4層及第3層無法存取外部系統。
 - B. 禁止外部系統存取第4層及第3層之關鍵數位資產。
 - C. 禁止使用者從外部系統進行存取、處理、或傳送組織管控資訊，除非核能電廠驗證其安全管控措施等效於關鍵數位資產。
22. 公開可存取的內容
核能電廠應執行下列事項：
- A. 選定人員授予公開發布資訊權利。
 - B. 訓練經授權公開資訊之人員，確保其公開的資訊不會

影響核能電廠安全、保安及緊急應變(SSEP)功能或受外部資安攻擊利用。

- C. 確保會影響安全、保安及緊急應變(SSEP)功能或受外部資安攻擊利用的資訊不會公開。

(四) 審查發現

審查人員確認核能電廠存取控制證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”.
C.3.3.1.1
2. RG 5.71 “Cyber security program for nuclear facilities”.
Appendix B.1.

3.1.5.1.2 稽核及當責

(一) 審查範圍

審查人員依據本導則，審查核能電廠稽核與當責，核能電廠應擬訂稽核與當責政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)稽核與當責政策及程序；(2)事件稽核；(3)稽核內容；(4)稽核儲存容量；(5)稽核失敗回應；(6)稽核審查；(7)時間戳記；(8)稽核資訊保護；(9)稽核紀錄保存。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠關鍵數位資產通安全計畫應完成下列要點：

1. 稽核及當責之政策及程序
核能電廠應並每年更新和審查明文擬訂稽核及當責的目的、範圍、角色、責任和管理階層承諾，以及廠區內部相互協調的政策及程序。

2. 事件稽核

核能電廠應依下列設計稽核列表：

- A. 擬訂並說明有安全、保安及緊急應變(SSEP)功能的關鍵數位資產相關的事件稽核項目。
- B. 定義稽核項目列表的稽核事件及頻率。
- C. 關鍵數位資產的稽核項目至少應包含：與關鍵數位資產的所有連接、使用者的登入/登出、構型/軟體/韌體的變更、稽核設定變更、特別允許的存取、命令及任何關鍵數位資產安全功能的變更等。
- D. 對無法自動稽核的關鍵數位資產，實施非自動化的機制和程序之替代安全管控措施並說明理由。
- E. 每年至少執行一次：審查和更新稽核清單之稽核事件項目。
- F. 在關鍵數位資產的稽核列表中，應包含執行權限的功能。
- G. 防止關鍵數位資產的事件紀錄於重新啟動時被清除。
- H. 在設施間協調資通安全稽核功能，以加強相互支援和協助選擇稽核事件。
- I. 設定所有關鍵數位資產稽核事件能適當地支援資安事件的事後調查。
- J. 以現今威脅資訊和效益分析，判斷所需的稽核事件。

3. 稽核內容

核能電廠應依如下設計稽核內容：

- A. 確定由關鍵數位資產所產生的稽核紀錄，包含有足夠資訊證實何種事件發生、何時發生、何地發生、事件的來源和結果等。
- B. 確定關鍵數位資產的稽核事件紀錄，具有事件型態、位置和主題等額外的分析能力。
- C. 實施集中控管所有關鍵數位資產所產生的稽核紀錄內容，並且避免關鍵數位資產改變或稽核紀錄損毀。

4. 稽核儲存容量

事件稽核的儲存容量，應足以保留至下次審查的容量。

5. 稽核失敗回應

核能電廠應依如下設計稽核程序失敗的回應程序：

- A. 應設計稽核紀錄的最大儲存容量，當儲存容量到達預先設定之百分比時，關鍵數位資產應提供警告。

- B. 對無法回應稽核失敗的關鍵數位資產，應設計替代安全管控方案，並說明理由。
- C. 應對稽核失敗的關鍵數位資產或安全邊界設備，依據設備技術規範(例如操作手冊)處理。
- D. 為防止 SSEP 功能受危害，須將稽核失敗的關鍵數位資產轉移至多重(Redundant)的關鍵數位資產，僅覆蓋最舊的稽核紀錄或停止產生稽核紀錄。

6. 稽核審查、分析及報告

核能電廠應執行下列審查、分析及報告之稽核：

- A. 至少每月執行一次：審查分析關鍵數位資產的稽核紀錄，並將不適當或不正當的活動回報給授權管理單位。
- B. 當收到來自於管制單位或其它可信來源單位通報對安全、保安及緊急應變(SSEP)的威脅及風險改變時，應調整稽核審查、分析與報告的等級。
- C. 採取自動化機制，將關鍵數位資產的稽核紀錄審查、分析及報告，整合至核能電廠可疑的活動調查和回應處理。

7. 時間戳記

- A. 所有關鍵數位資產的時間的來源應為相同或更高安全層級設備，所有稽核紀錄的關鍵數位資產時間同步。
- B. 核能電廠採用關鍵數位資產時間同步方法不得引發資安弱點。當關鍵數位資產無法使用時間同步時，實施替代性管控措施(如人工校時)，以管理潛在的資通安全風險。

8. 稽核資訊保護

核能電廠應依下述實施稽核紀錄保護：

- A. 應防止未經授權的存取、修改或刪除關鍵數位資產的稽核紀錄和工具。
- B. 確保所有稽核資訊與其來源設備，均被保護在相同安全水準上。

9. 稽核紀錄保存

核能電廠稽核紀錄應足以提供資安事件調查所需的紀錄，並且符合核能電廠關鍵數位資產資通安全計畫紀錄保存的要求。

(四) 審查發現

審查人員確認核能電廠稽核與當責證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.1.2
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix B.2

3.1.5.1.3 關鍵數位資產系統及通訊保護

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產及通訊保護，核能電廠應擬訂關鍵數位資產系統及通訊保護政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)系統與通訊保護政策及程序；(2)應用程式區隔與資安功能隔離；(3)資源分享；(4)阻斷服務防護；(5)資源優先權；(6)傳輸完整性；(7)傳輸機密性；(8)信賴路徑；(9)金鑰建立及管理；(10)加密；(11)未經授權的遠端服務；(12)安全參數的傳輸；(13)公開金鑰驗證(14)行動碼；(15)安全名稱/位址的解析服務；(16)名稱/位址解析服務的架構與調配；(17)可靠的連線；(18)最小功能的節點。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產及通訊保護：

1. 關鍵數位資產系統和通訊保護政策和程序
核能電廠須有明文的政策，定義目的、範圍、角色、責任以減緩非授權系統或通訊存取的風險，引發危害安

全、保安及緊急應變(SSEP)功能結果的攻擊，以及能促進並維持系統和通訊保護政策的管控程序。

2. 應用程式區隔及資安功能隔離
 - A. 將關鍵數位資產設備應用程式設定分離成使用者功能及管理功能。
 - B. 設定關鍵數位資產，透過分隔網域隔離資安與非資安功能，此隔離包括存取控制和執行保安功能完整的軟體、硬體及韌體。
 - C. 以硬體隔離機制為基礎，區隔關鍵數位資產。
 - D. 關鍵資安功能必須與非資安及一般資安功能隔離。
 - E. 設定關鍵數位資產將包含資安功能的隔離邊界內的非資安功能數量降至最低。
 - F. 設定資安功能為獨立模組，並避免模組間不必要的互動。
 - G. 設定資安功能為階層式結構，並避免不同層級間互動和關聯。
 - H. 採取替代安全控制方案者，應記錄並說明判斷理由和採用的方法。
3. 設定資源分享權限
 - A. 設定關鍵數位資產，防止未經授權及非故意的資訊經由分享系統傳輸。
 - B. 使用網路設備實體分離，以建立和維護其它安全層級與第3層和第4層間的邏輯分離。
4. 阻斷服務(Denial of Service, DoS)保護
 - A. 設定關鍵數位資產以防禦或限制阻斷服務攻擊所造成的影響。
 - B. 設定關鍵數位資產限制使用者能力，以防止其對其它關鍵數位資產或網路發動阻斷服務攻擊。
 - C. 設定關鍵數位資產管理額外的容量、頻寬及備援系統，以限制資訊泛濫和阻斷服務攻擊的影響。
5. 資源優先權

核能電廠應設定關鍵數位資產不同優先權的資源使用，防止低優先權程序延遲或干擾高優先權程序的執行。
6. 設定傳輸完整性
 - A. 設定關鍵數位資產以保護傳輸資訊的完整性。
 - B. 採用密碼學機制以防傳輸資訊被竄改。

- C. 利用 MAC 位址鎖定及網路存取控制等傳輸安全機制，以防止遭中間人攻擊。
- D. 實施網路監控找出中間人和網址解析協定軟體病毒。
- E. 如無法提供保護傳輸資訊的完整性之資通安全管控措施，採取替代安全管控措施時，應記錄並說明判斷理由和採用方法。

7. 傳輸機密性

- A. 設定關鍵數位資產以保護傳輸資訊的機密性。
- B. 採用密碼學機制以防止傳輸資料被揭露。
- C. 採取替代安全管控措施時，應記錄並說明判斷理由和採用方法。

8. 信賴路徑

設定關鍵數位資產，以確保使用者和安全功能間的操作，完全在可信賴的路徑上。

9. 金鑰建立及管理

當關鍵數位資產需採用金鑰時，核能電廠應採取自動機制或人工管理金鑰，以符合 FIPS 140-2 之密碼模組安全要求。

10. 使用密碼(Cryptography)

核能電廠設定密碼機制應符合 FIPS 140-2 之密碼模組安全要求。

11. 未經授權的遠端服務

- A. 關鍵數位資產應設定禁止遠端協同計算 (Collaborative Computing) 機制。
- B. 除非用於控制或監控，否則，關鍵數位資產應與攝影機和麥克風斷線，以防止被利用。

12. 安全參數的傳輸

應設定關鍵數位資產間資訊交換安全參數。

13. 公開金鑰驗證

核能電廠應在公開金鑰憑證政策下，發布公開金鑰憑證或從憑證提供者取得公開金鑰憑證。

14. 行動碼

核能電廠應執行下列事項：

- A. 制定對關鍵數位資產有潛在危險之行動碼(如 Java、Activx、Javascript 等)使用限制及實施指引。
- B. 授權、監控和管控在關鍵數位資產使用行動碼。

15. 安全名稱/位址的解析服務
 - A. 網域名稱伺服器的子網域架構設定必須經父網域信任核查。
 - B. 設定從權威(Authoritative)來源主機取得網域名稱解析具有身份驗證及資料完整性驗證。
 - C. 設定名稱/網址解析資料來源確認及完整性驗證。
16. 可靠的連線階段(Session)

核能電廠應設定關鍵數位資產，提供可靠的連線階段通訊。
17. 簡單節點作業

應關閉關鍵數位資產非必要的功能，使其具有最小的操作功能及資料儲存設備。
18. 未工作時資產保護

設定關鍵數位資產，在未使用時受安全保護。
19. 異質性/多樣性保護

核能電廠應採取多樣性關鍵數位資產的保護技術。
20. 已知狀態失效處置
 - A. 核能電廠應確保關鍵數位資產在已知狀態下失效，並不會影響 SSEP 功能。
 - B. 核能電廠應確保關鍵數位資產或其元件在已知狀態下失效，並不會影響機密性、完整性及可用性。

(四) 審查發現

審查人員確認核能電廠 關鍵數位資產及通訊保護證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.1.3.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix B.3.

3.1.5.1.4 辨識及驗證

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產辨識及驗證，核能電廠應擬訂辨識、驗證政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)辨識及驗證政策及程序；(2)使用者辨識及驗證；(3)密碼設定；(4)無驗證之人機互動安全；(5)設備辨識及驗證；(6)識別符管理；(7)驗證管理；(8)驗證工具回饋；(9)加密模式驗證。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全計畫人員辨識及驗證：

1. 辨識及驗證政策及程序

核能電廠需擬訂並每年審查一次如下要點：

- A. 人員識別和驗證的政策，定義目的、範圍、角色、職責和管理層的承諾與協調，並設計辨識使用者、主機、網路、應用程式、服務和資源程序。
- B. 管理使用者的辨識
 - (1) 每位使用者和處理程序活動均具有唯一辨識。
 - (2) 檢驗每位使用者和處理程序活動均具有唯一的辨識。
 - (3) 從組織內適當的長官授權核發，取得使用者身份辨識。
 - (4) 確保使用者的身份辨識發布給所預期的一方。
 - (5) 定義時間內，關閉不活動的使用者。
 - (6) 當使用者終止存取的需求時，應立即予關閉。
 - (7) 使用者身份識別符存檔。
- C. 管理關鍵數位資產的驗證
 - (1) 定義初始驗證內容。
 - (2) 建立初始驗證工具的分佈、遺失、受損害及回收

之管理程序。

(3) 於系統安裝時，需改變預設的驗證機制。

(4) 每年變更驗證碼。

2. 使用者辨識及驗證

核能電廠應執行下列事項：

A. 實施辨識和驗證技術，以確認關鍵數位資產互動者唯一的身份識別。

B. 採取多因子的驗證技術，以保護關鍵數位資產安全。

C. 當核能電廠未實施辨識及驗證管控措施，應實施如下替代安全管控措施並說明理由：

(1) 實體限制存取。

(2) 監控和記錄實體存取，以即時偵測並回應發現入侵者。

(3) 採取稽核和驗證。

(4) 確認存取關鍵數位資產使用者為被授權者。

(5) 確認使用者為可信賴的。

D. 若實施安全網域為基礎之驗證，亦應執行下列事項：

(1) 基於服務，維持所指定的安全層級。

(2) 實體或邏輯安全網域控制，以防止未授權存取和操作。

(3) 不同層級的安全網域，不得建立彼此信任關係。

(4) 實施以角色為基礎的控制措施，僅允許執行工作的使用者，擁有存取權限。

E. 若未採取網域為基礎之驗證，核能電廠應執行下列事項：

(1) 記錄和說明未採取網域為基礎之驗證理由。

(2) 可行的話，實施區域驗證 (Localized Authentication)。

(3) 實施儘可能 (Strongest Possible) 之挑戰-回應驗證 (Challenge-response Authentication) 機制。

(4) 實施以角色為基礎的控制措施，僅允許執行工作的使用者，擁有存取權限。

3. 密碼

核能電廠使用者密碼，應符合下列要求：

A. 使用者密碼應於長度、強度、複雜度之安全與使用者存取關鍵數位資產難易度間取得平衡。

- B. 使用者密碼之長度及複雜度應符合安全要求。
- C. 密碼應定期更改。
- D. 使用者密碼不得使用字典單字及包含可以猜測之數字或字母。
- E. 主要密碼副本應存放安全位置，並限制存取。
- F. 僅有被授權的使用者方可修改管理者主密碼。

4. 無驗證之人機互動(Nonauthenticated Human Machine Interaction, NHMI)安全

核能電廠應執行下列事項：

- A. 確保所有人機互動使用者操作均已被驗證，使用者均已被適當的辨識和驗證。
- B. 控制無驗證之人機互動，不得影響人機互動之正常運作。
- C. 確保未因身份驗證、連線階段鎖定和連線階段中止而影響安全、保安及緊急應變(SSEP)功能。
- D. 實施稽核，以確保所有無驗證之人機互動作業活動均在監控中。

5. 設備辨識及驗證

核能電廠應執行下列事項：

- A. 使用者與關鍵數位資產建立連線前，應實施與記錄辨識和驗證設備。
- B. 當未使用或無法使用設備辨識及驗證時，應說明理由及採取下列替代管控措施：
 - (1) 實體限制存取。
 - (2) 監控和記錄實體存取，以即時偵測和回應發現入侵者。
 - (3) 採取稽核和驗證。
 - (4) 確認使用者為被授權的。
 - (5) 確認被授權操作人員為值得信任的。

6. 識別符管理

核能電廠應依下列事項管理和記錄識別符：

- A. 每位使用者僅有唯一識別符。
- B. 驗證每位使用者識別符。
- C. 接受來自電廠授權發行的使用者識別符。
- D. 發行使用者識別符。
- E. 定期每月審視無使用帳號，關閉此帳號。

7. 驗證工具管理

核能電廠應依下列管理關鍵數位資產驗證工具管理：

- A. 定義初始驗證工具的內容，如密碼長度和組合、權杖、金鑰和其它驗證規則。
- B. 建立初始驗證工具的分佈、遺失、受損、損壞及回收之管理程序。
- C. 更改關鍵數位資產安裝後，預設的身份驗證工具。
- D. 每年變更或更新驗證工具。

8. 驗證工具回饋

核能電廠應執行下列事項：

- A. 確保關鍵數位資產驗證回饋資訊受保護，以防遭未授權者利用。
- B. 確保關鍵數位資產和關鍵數位資產之回饋資訊不提供给予危及驗證機制之未授權者。

9. 加密模組驗證

核能電廠關鍵數位資產如使用驗證加密模組，應確保其模組符合 FIPS 140-2 加密模組安全需求。

(四) 審查發現

審查人員確認核能電廠 辨識及驗證證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.1.4.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix B.4.

3.1.5.1.5 系統強化

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產系統強化，核能電廠應擬訂系統強化政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)系統強化政策及程序；(2)移除非必要的服務和程式；

(3)主機的入侵偵測系統；(4)變更檔案系統和作業系統的權限；(5)硬體構型；(6)安裝作業系統、應用程式和第三方軟體更新

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產系統強化：

1. 系統強化政策及程序
須有明文的政策定義目的、範圍、角色、責任和管理層承諾，以提供高度保證現存關鍵數位資產的安全設定，以防止未授權存取和使用，以及需有能促進並維持系統強化政策的管控程序。
2. 移除非必要的服務和程式
 - A. 應記錄和關鍵數位資產有關所有必要的應用程式、公共程式、系統服務、描述、構型設定檔、資料庫和其它軟體及其適當的構型環境，包含版本和修補程式等。
 - B. 維持/保有關鍵數位資產服務清單，內容可包含所有正常和緊急作業所需要的通訊埠和服務，並且描述其需要之原因，並且僅有經允許之服務和程式被使用。
 - C. 驗證和記錄所有弱點評估或掃描之關鍵數位資產程式修補和攻擊減緩補救措施。
 - D. 記錄軟體和服務於弱點進行修補或攻擊減緩修改期間，採取妥善的安全措施，以維持安全層級。
 - E. 記錄關鍵數位資產作業系統和軟體的修補程式，以追蹤和確認無額外的服務被重新安裝或重新啟動。
 - F. 於關鍵數位資產加入運作環境前，應移除或禁用不需要的軟體元件。
 - G. 記錄移除或禁用的軟體元件，例如：
 - (1) 未正式送交的網路設備驅動程式。
 - (2) 未使用的週邊設備驅動程式。
 - (3) 社群訊息服務(如：MSN, AOL, Facebook...)
 - (4) 未使用的用戶端及伺服器端服務。

- (5) 工作站或伺服器上非供開發之編譯軟體。
- (6) 非供控制系統使用之程式語言編譯軟體。
- (7) 未使用的網路和通訊協定。
- (8) 未使用的管理程式、診斷、網路管理和系統管理功能。
- (9) 備份的檔案、資料庫和程式僅在系統發展時才使用。
- (10) 所有未使用的資料和構型檔案。
- (11) 範例程式和指令檔。
- (12) 未使用的文件處理程式(如：MS Word, Excel, PowerPoint, Adobe Acrobat, Openoffice...)
- (13) 未使用的儲存媒介播放程式。
- (14) 遊戲程式。

3. 主機入侵偵測系統

A. 應建置、實施並記錄下列需求：

- (1) 設定主機入侵偵測系統，包含如靜態檔案名稱和動態檔案名稱樣式、系統和使用者帳號、執行未經授權的程式碼、主機利用率、程式的許可證等，以使系統能偵測包含設計基礎威脅(DBT)資安攻擊。
- (2) 設定主機入侵偵測系統之日誌紀錄系統和使用者帳號連線，當連線出現異常時，系統會發生警示通知。
- (3) 確保主機入侵偵測系統的設定，沒有影響核能電廠的安全、保安與緊急應變功能。
- (4) 設定主機入侵偵測系統的紀錄檔案僅能以附加方式儲存，以防止更改儲存設備之紀錄。
- (5) 執行主機入侵偵測系統之系統更新或漏洞修補時，應確保其維持在原設定安全層級。

B. 僅允許被授權人員，可存取主機入侵偵測系統。

4. 變更檔案系統和作業系統的權限

建置、實施並記錄如下：

- A. 應設定關鍵數位資產最少的權限、資料、命令、檔案及使用者帳號。
- B. 設定系統服務儘可能在最低的使用權，並記錄此構型設定。

- C. 記錄變更或關閉使用者存取檔案及函式。
 - D. 驗證系統修改或升級後，不會改變權限基準及安全設定。
5. 硬體構型
- 建置、實施並記錄下列需求：
- A. 經由軟體或實體的斷線，關閉不需要的網路、無線網路和通訊埠及外接式的儲存媒介設備或提供工程屏障。
 - B. BIOS 設定密碼，以防止未經授權的變更。
 - C. 當 BIOS 密碼保護技術不可行，記錄攻擊減緩措施。
 - D. 記錄硬體構型。
 - E. 利用網路設備，以設定特定網路來源的存取限制。
 - F. 當設備遭軟體關閉，允許系統管理員能重新啟動和記錄其構型。
 - G. 確認替代的設備具有相同或高於原設備的資通安全功能。
6. 安裝作業系統、應用程式和第三方軟體更新
- A. 建置、實施並記錄下列需求：
- (1) 修補程式、升級程序及負責安裝人員。
 - (2) 於接獲弱點通報後 4 小時內，應進行影響關鍵數位資產的弱點通知。
 - (3) 通知被授權人員進行修補作業。
 - (4) 修補程式應維持在相同安全水準。
- B. 建置、實施並測試下列需求：
- (1) 接到資通安全更新程式時，系統或設備應先離線進行測試，無異狀才能上線。
 - (2) 包含會影響資通安全的所有更新程式。

(四) 審查發現

審查人員確認核能電廠系統強化證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”.

C.3.3.1.5.

2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix B.5.

3.1.5.2 操作管控

審查人員依據本導則，審查核能電廠技術、操作及管理安全管控措施。操作管控措施係以人的行為為主的安全管控機制，包含：(1)儲存媒介保護；(2)實體及環境保護；(3)人員安全；(4)系統及完整性；(5)緊急應變計畫；(6)事件回應；(7)關鍵數位資產維護；(8)攻擊減緩；(9)功能持續性；(10)認知及訓練；(11)構型管理。

3.1.5.2.1 儲存媒介保護

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產儲存媒介保護，核能電廠應擬訂儲存媒介保護政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)儲存媒介保護政策及程序；(2) 儲存媒介存取；(3)儲存媒介標記；(4)儲存媒介儲存；(5)儲存媒介傳送；(6) 儲存媒介清潔與處置。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 儲存媒介保護政策及程序(Media Protection Policy and Procedures)

核能電廠應發展並每年審查和更新儲存媒介保護政策及程序，包含：

- A. 正式並記錄儲存媒介保護政策，定義目的、範圍、角色、責任和管理階層的承諾與相關單位間協調。規範儲存媒介的接收、保存、作業、消磁、移除、再利用和處理等需提供高度保證，以防止未經授權的資訊披露被資安攻擊所利用，而影響安全、保安及緊急應變(SSEP)功能。
- B. 任何可以提供資通安全攻擊的儲存媒介，均視為敏感

儲存媒介。

2. 儲存媒介存取(Media Access)

- A. 記錄並限制僅有被授權的人員方可存取關鍵數位資產儲存媒介，儲存媒介包含數位儲存媒介(如磁片、磁帶，外部或可移式硬碟、快閃記憶體、隨身碟、光碟和數位播放儲存媒介等)和非數位儲存媒介(紙本和微縮片等)。
- B. 除了被授權人員外，限制任何使用具資訊儲存能力的行動計算和通訊設備(如筆記型電腦、個人電腦、和智慧型手機等)存取任何資通安全資訊。
- C. 採用自動機制，限制存取儲存媒介儲存區，並稽核記錄(audit log)存取嘗試和授權存取。

3. 儲存媒介標記(Media Labeling/ Marking)

根據資訊分類，標記可移動關鍵數位資產儲存媒介和關鍵數位資產的輸出，指出散布限制和注意事項的處理。標記須擬訂一套特殊的傳播、處理和散布方法，並使用讓人容易辨識的命名法則為儲存媒介標籤。

4. 儲存媒介儲存(Media Storage)

關鍵數位資產儲存媒介的實體保護和安全儲存，應採取與其資料敏感性相符合方式。

5. 儲存媒介傳送(Media Transport)

- A. 關鍵數位資產儲存媒介的傳送過程的實體保護與儲存，應採取與其資料敏感性相符合方式。
- B. 關鍵數位資產儲存媒介在控制區外傳送時，應限定僅有被授權人員可進行相關活動。
- C. 核能電廠應對數位和非數位儲存媒介在控制區外傳送時，需有安全管控措施(如上鎖、保安人員和加密等)。
- D. 記錄關鍵數位資產儲存媒介傳送過程相關的活動。
- E. 關鍵數位資產儲存媒介傳送所有過程中，需有明確的保管人員。

6. 儲存媒介徹底清除與處置(Media Sanitization and Disposal)

- A. 關鍵數位資產之數位或非數位關鍵數位資產儲存媒介處置或再使用，應先將原來的數位資料儲存媒介內容破壞或徹底清除，以防止惡意的利用。

- B. 需有明確關鍵數位資產儲存媒介徹底清除的技術和程序，並確定安全管控措施與儲存媒介徹底清除一致。
- C. 核能電廠應每季檢查、記錄和查證儲存媒介徹底清除與處置行動，以確保裝置和程序正常運行。

(四) 審查發現

審查人員確認核能電廠儲存媒介保護證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

- 1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.1..
- 2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.1.

3.1.5.2.2 人員保安

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產人員保安，核能電廠應擬訂人員保安政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)人員保安政策及程序；(2)人員離職或轉職。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列要點，完成關鍵數位資產執行人員保安：

- 1. 人員保安政策及程序
 - A. 須有明文的政策，定義人員涉及範圍、角色、責任和當責的人員保安政策及程序，以確保在無陪同人員下

存取關鍵數位資產，均值得信賴。

B. 核能電廠應審查賦予無陪同人員存取權限於特定人員，確認其對系統設備的知識與了解，不會影響安全、保安及緊急應變(SSEP)正常運作。

2. 人員離職或轉職

A. 終止所有關鍵數位資產與系統的存取權限。

B. 進行離職或轉職人員面談。

C. 通知相關人員身份變更與終止事項。

D. 檢查所有與安全相關的財產。

E. 保留離職前對關鍵數位資產與組織關鍵數位資產的存取控制紀錄資料。

(四) 審查發現

審查人員確認核能電廠人員保安證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.2.

2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.2.

3.1.5.2.3 系統及資訊完整

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產系統及資訊完整，核能電廠應擬訂系統及資訊完整政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)系統與資訊完整之政策及程序；(2)瑕疵修補；(3)惡意程式碼防護；(4)監控工具及技術；(5)資通安全警示及建議；(6)資通安全功能驗證；(7)軟體和資訊完整性；(8)資訊輸入限制；(9)錯誤處理；(10)資訊輸出與保存；(11)預期錯誤回應。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產安全計畫系統及資訊完整性：

1. 系統與資訊完整性之政策及程序
 - A. 須有明文的政策，定義涵蓋範圍、角色、責任，以確保提供高度保證關鍵數位資產內資訊受到完整保護。
 - B. 核能電廠系統與資訊完整性流程包含：
 - (1) 偵測惡意或可疑的存取控制或發生在既定的防禦水準之內的異常現象。
 - (2) 當發現惡意或可疑活動時，使用安全的通訊管道通知相關人員，以防網路被監視。
 - (3) 隔離惡意活動。
 - (4) 消除惡意活動。
 - (5) 集中記錄相關的網路安全事件。
 - (6) 提供安全的監控和管理機制。
 - (7) 提供所有保安相關的設備時間同步。
2. 瑕疵修補
 - A. 建立、實施並記錄如下的瑕疵修補流程：
 - (1) 確定資安警示和弱點評估程序。
 - (2) 傳送弱點資訊。
 - (3) 利用構型管理程序儘速修正瑕疵。
 - (4) 修正關鍵數位資產的瑕疵。
 - (5) 關鍵數位資產正式上線前，執行弱點掃描安全管控措施及評估，以確保瑕疵已被消弭(若可掃描，須做掃描及評估；若不可掃描，只須做評估)。
 - B. 核能電廠於執行修補前，應記錄和測試相關的修補軟體，以決定是否對關鍵數位資產有效或產生潛在的副作用。
3. 惡意程式碼防護
 - A. 應在網路上建立、發展並記錄即時惡意程式碼防護機制，保護防禦邊界設備出入點、關鍵數位資產、工作站、伺服器及移動式設備，以免遭惡意程式以下列方

式利用：

- (1) 系統、關鍵數位資產及可移動儲存媒介或其它通訊。
 - (2) 利用關鍵數位資產的弱點。
- B. 當發布新版本，應符合核能電廠構型管理的政策及程序，記錄並更新惡意程式碼保護機制。
- C. 記錄並設定惡意程式碼保護機制以確保：
- (1) 每週掃描安全邊界設備、關鍵數位資產(如果可行)、工作站、伺服器或移動計算設備，並即時掃描下載、開啟或執行的檔案。
 - (2) 刪除和隔離受感染的檔案。
- D. 記錄並採用多來源的惡意程式碼保護軟體產品，並因應偵測與刪除過程中誤判，以及因其結果而產生對關鍵數位資產的潛在可用性影響。
- E. 應集中管理惡意程式碼保護機制，以完成下列事項：
- (1) 防止關鍵數位資產使用者有規避惡意程式碼保護機制之能力。
 - (2) 只有被授權的使用者，才有更新關鍵數位資產惡意程式碼保護機制的功能。
- F. 關鍵數位資產不允許使用者使用非授權(如 USB)的可移動儲存媒介。
- G. 關閉所有關鍵數位資產作業不需使用的儲存媒介連接介面(如 USB PORT)。
- H. 當關鍵數位資產面臨資料未明確符合安全政策時，記錄並實施惡意程式碼保護機制，以識別包含惡意程式碼資料及相對回應。
4. 監控工具及技術
- A. 核能電廠應執行下列事項：
- (1) 監控關鍵數位資產的事件。
 - (2) 偵測關鍵數位資產的攻擊。
 - (3) 偵測並阻斷未經授權的連線。
 - (4) 依據資訊保留之要求，保存事件紀錄。
 - (5) 識別未經授權使用關鍵數位資產。
 - (6) 佈建關鍵數位資產的監控設備，具有蒐集資訊，以偵測資通安全攻擊、未經授權存取的行為與追蹤對核能電廠關注的特定型態存取(Transaction)。

- B. 核能電廠應依照管制單位對提高核能電廠安全、保安及緊急應變(SSEP)風險的要求或指示，提高監測活動層級。
 - C. 核能電廠使用共同協定，並整合個別的入侵偵測工具至整廠入侵偵測系統。
 - D. 記錄和採用自動化支援近乎即時(Near-real-time)的事件分析工具。
 - E. 核能電廠應記錄並採用自動化工具整合入侵偵測工具至存取管控和流量管控機制，迅速回應攻擊活動。
 - F. 核能電廠應監控、記錄不正常或未授權的進出通訊活動或狀況，監控能力需具有遇到損害或潛在感染時能即時警示能力。
 - G. 核能電廠應有防止使用者規避入侵偵測和預防的能力。
 - H. 核能電廠應以最小影響安全、保安及緊急應變(SSEP)行為，通知並記錄可疑事件，以調查和終止可疑事件。
 - I. 核能電廠應記錄及保護從入侵偵測工具取得的資訊，以防止未授權的存取、修改和刪除。
 - J. 核能電廠應有足夠適合的網路安全人員，以隨機測試和記錄入侵監視工具。
 - K. 核能電廠應記錄並提供確保監控工具可監視加密流量。
 - L. 核能電廠應分析並記錄在關鍵數位資產外圍邊界上由內對外的通訊流量。
 - M. 核能電廠應確認並記錄所採用的監控工具不會影響關鍵數位資產的功能，否則應採用具充分功能的替代工具。
5. 資通安全警示及建議
- A. 核能電廠有責任：
 - (1) 從第三方及廠商等可信的來源組織取得警示、公告、通知和命令。
 - (2) 獨立評估並決定關鍵數位資產安全管控措施之需求、嚴重程度、方法以及時間表，以實施與安全管控措施一致的安全指令。
 - B. 核能電廠應：
 - (1) 產生並記錄必要的內部資通安全警示、通知和命

令。

- (2) 傳播並記錄資通安全警示、通知和命令到指定人員，以採取適當行動和追蹤狀態。
- (3) 實施並記錄資通安全命令以符合時間範圍內的資通安全措施。
- (4) 實施並記錄任何減緩攻擊所需的措施。
- (5) 必要時，採取自動化或其他機制(如電子郵件)提供安全警示和通知訊息給廠內相關人員。

6. 資通安全功能驗證

- A. 核能電廠應驗證並記錄關鍵數位資產資通安全功能正確操作。
- B. 於技術可行情形下，核能電廠應記錄保存關鍵數位資產資通安全測試失敗的通知訊息。
- C. 核能電廠應於技術可行情形下，記錄關鍵數位資產提供自動管理分散式的資通安全測試和結果。
- D. 當關鍵數位資產無法支援自動化機制管理分散式的資通安全測試和結果時，採取非自動化機制和流程測試資通安全功能，核能電廠應記錄採取替代管控措施之判斷理由，包含：
 - (1) 人員可勝任。
 - (2) 人員可信任。
 - (3) 有測試流程和結果。
 - (4) 能限制對關鍵數位資產的實體存取。
 - (5) 可監控和記錄對關鍵數位資產的實體存取。
 - (6) 稽核和確認措施。

7. 軟體和資訊完整性

核能電廠應執行下列事項：

- A. 偵測和記錄對軟體和資訊的非授權變更。
- B. 應於技術可行情形下，採取硬體存取控制(如硬體開關)，以防止軟體遭受非授權修改。
- C. 至少每季或依生產商或供應商建議，掃描軟體和資訊的完整性、操作性和功能性，以符合要求。
- D. 應於技術可行情形下，採取自動化工具，於發現差異現象時，提供通知予指定的相關人員。
- E. 採取並記錄集中管理完整性驗證工具。
- F. 系統元件(System Component)必須有包裝和封印，以

防止遭受實體竄改。

G. 確保並記錄所使用的完整性驗證應用程式，不會影響關鍵數位資產的執行效能，並且當無法使用這些驗證程式時，採取替代管控措施。

8. 資訊輸入限制

核能電廠應執行下列事項：

A. 限定僅有授權人員方具有關鍵數位資產輸入資訊能力。

B. 關鍵數位資產的輸入資訊的有效語法分析，應儘可能被精確地、完全地、有效地和確實地接近原輸入點，以確認輸入字元格式和內容指令與定義相符。

9. 錯誤處理

核能電廠應記錄並實施如下錯誤管控措施：

A. 辨識錯誤狀態。

B. 產生的錯誤資訊不會暴露潛在傷害資訊給未授權人員利用。

C. 僅有被授權人員可取得錯誤資訊。

D. 錯誤資訊不得包含如密碼等敏感資訊。

10. 資訊輸出與保存

核能電廠保存關鍵數位資產輸出之敏感性資訊，僅允許被授權人員使用，並且保證其處置過程，無顯露於未授權人員。

11. 預期錯誤回應

核能電廠應對關鍵數位資產可用性實施如下措施，以符合技術規範、防護計畫、維護計畫、保安計畫、緊急應變計畫、或矯正行動計畫等要求。當無法應用上述計畫時，採取以下方法來提供關鍵數位資產可用性：

A. 必要時提供替代元件，與切換現役及備援元件。

B. 考慮作業環境內，各元件的平均有效壽命。

C. 提供適量的備品庫存。

(四) 審查發現

審查人員確認核能電廠系統及資訊完整證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.3.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.3

3.1.5.2.4 關鍵數位資產設備維護

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產設備維護，核能電廠應擬訂關鍵數位資產設備維護政策及實施程序，以確保核設施關鍵數位資產資通安全計畫有效和正確。審查內容包含：(1)關鍵數位資產設備維護政策及程序；(2)系統維護工具；(3)人員執行維護及測試工具。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產系統維護作業：

1. 系統維護政策及程序
核能電廠應擬訂、宣示並且每年審查一次關鍵數位資產系統維護政策，包含如下：
 - A. 須有明文的政策，定義涵蓋範圍、角色、責任和管理階層的承諾，協調廠區所有部門，共同的關鍵數位資產的維護管控和要求。
 - B. 須有明文的實施關鍵數位資產的維護政策和共同的維護管控。
 - C. 核能電廠內數位資產維護策略及程序涵蓋區域：
 - (1) 公開進出區：為核能電廠實體控制區以外之地區。
 - (2) 控制區：為電廠內防護的最外層，以防止外界侵入。
 - (3) 保護區：在控制區內，被實體屏蔽包圍並有入侵偵測系統。

- (4) 緊要區：包含任何裝置、系統、設備或材料發生錯誤時，會產生輻射破壞，直接或間接危害大眾健康和 safety。緊要區也包含需要的裝置或系統以防止輻射洩漏。

2. 系統維護工具

核能電廠執行下列事項：

- A. 同意、監控和記錄關鍵數位資產維護工具的使用。
- B. 檢查和記錄維護工具(例如診斷和測試裝置及行動設備)是否遭維護人員不當的修改。
- C. 關鍵數位資產在使用儲存媒介及行動設備前，應檢查和記錄是否有惡意程式碼。
- D. 經由下列其中一項，作為控制、防止及記錄未經授權移動的維護裝置：
 - (1) 確認該裝置上沒有包含核能電廠的資訊，並在新用於設施前，驗證設備的完整性。
 - (2) 清除或破壞該裝置。
 - (3) 維護裝置應保留於設施內。
 - (4) 應取得明確授權者核准後，方可將該裝置從設施中移動。
- E. 採取自動化，限制授權人員使用維護工具，只有在無法採取自動化機制時，可採取手動機制。

3. 執行維護及測試作業人員

核能電廠應執行下列事項：

- A. 現有授權維護人員清單必須符合授權存取程序和內部攻擊減緩程序。
- B. 採取自動化或非自動化機制，偵測非授權使用或執行指令，或指定具有關鍵數位資產知識的人員監督陪同。

(四) 審查發現

審查人員確認核能電廠關鍵數位資產設備維護證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”.
C.3.3.2.4.
2. RG 5.71 “Cyber security program for nuclear facilities”.
Appendix C.4.

3.1.5.2.5 實體及環境保護

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產實體及環境保護，核能電廠應擬訂實體及環境保護政策及實施程序，以確實減緩關鍵數位資產及關聯通訊路徑的非授權實體存取的風險，以及保護關鍵數位資產及其關聯通訊路徑基礎支援系統，防止因環境條件造成功能失效。審查內容包含：

- (1)實體及環境保護政策及程序；
- (2)第三方/陪同人的存取管控；
- (3)實體與環境保護程序；
- (4)實體存取授權；
- (5)實體存取管控；
- (6)傳輸儲存媒介的存取管控；
- (7)顯示儲存媒介的存取管控；
- (8)監控儲存媒介的存取管控；
- (9)訪客存取管控。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產實體及環境保護：

1. 實體與環境保護政策與程序
 - A. 須有明文擬訂並每年審查和更新實體及環境保護政策，定義人員涵蓋範圍和角色、責任和管理層承諾，以提供下列事項之高度保證(High Assurance)：
 - (1) 減緩關鍵數位資產及其相關聯通訊路徑的實體設備，遭受未經授權存取的風險。
 - (2) 保護關鍵數位資產及其相關聯通訊路徑基礎支援系統，防止因環境條件造成功能失效。
 - B. 須有明文記錄實體及環境保護安全管控程序。
2. 第三方/陪同人的存取管控
 - A. 篩選、強制和記錄並監控第三方人員遵從安全管控措施，對象包含系統操作、維護、開發、資訊技術服務、

- 外包應用程式、網路及安全管理等合約商或組織。
- B. 合約書或同意書應明確指出人員的安全管控措施。
3. 實體與環境保護
- 核能電廠應保護並記錄關鍵數位資產的實體存取，實體安全管控(如上鎖等)為限制關鍵數位資產的存取，及防止因作業環境(如溫度、濕度、灰塵、電磁干擾等)影響，而降低其操作效能。
4. 實體存取授權
- A. 建立及維護授權存取(進出)設施之人員名單，及發予授權憑證。
- B. 上述名單需經核能電廠授權人員審查及核准，並符合存取授權程序。
5. 實體存取管控
- A. 管控實體進出點(包括進入和離開點)，所有人員進出須事先核准，並確認個人存取授權。
- B. 核准個人存取權及強化其與關鍵數位資產變更相關的實體和邏輯存取限制。
- C. 透過電子設備或軟體，管控人員之邏輯存取權。
- D. 產生、保留和審查和存取限制相關的紀錄。
- E. 僅有具有資格和授權人員可對關鍵數位資產存取。
- F. 管控關鍵數位資產存取獨立於設施的實體存取管控措施。
6. 傳輸及顯示儲存媒介的存取管控
- 管控並記錄關鍵數位資產實體存取之通訊路徑，防止非授權人員觀察顯示資訊。
7. 監控存取管控
- A. 監控和記錄實體存取關鍵數位資產和安全邊界以偵測和回應實體安全事件。
- B. 檢查實體存取的紀錄檔。
- C. 協同與核能電廠事件回應人員調查事件結果。
- D. 監控即時實體入侵偵測警示及監視裝置。
- E. 採取自動化機制評估和辨識潛在入侵者和設計適當的回應措施。
- F. 提供充足光度照明的存取監控設備。
8. 訪客存取管控
- A. 於訪客進入前，驗證是否具存取權，以控制和記錄訪

客關鍵數位資產實體存取。

- B. 陪同訪客以監視其行為，防止影響安全、保安及緊急應變(SSEP)功能。

(四) 審查發現

審查人員確認核能電廠實體及環境保護證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.5.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.5.

3.1.5.2.6 事件回應

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全事件回應，核能電廠應擬訂事件回應政策及實施程序，以確保核設施遭受資安攻擊時，能提供高度安全保證。審查內容包含：(1)事件回應計畫政策及程序；(2)事件回應訓練；(3)事件回應測試與演練；(4)事件處理；(5)事件監控；(6)事件報告；(7)事件回應協助；(8)事件回應計畫。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產安全計畫事件回應：

1. 事件回應政策及程序
 - A. 核能電廠應明文擬訂並每年審查一次事件回應政策，以定義目的、範圍、角色、責任及管理階層承諾，

並協調各部門遵循。

- B. 核能電廠應明文擬訂正式的處理程序，以因應實施事件回應處理。包含：
 - (1) 通知員工和操作人員。
 - (2) 確認意外徵兆或錯誤情況是否為資安攻擊的結果。
 - (3) 採用矯正行動措施(Corrective action program)執行分析，以查明潛藏於關鍵數位資產之進入機制和關閉弱點。
 - (4) 建置快速事件復原計畫。
- C. 實施復原計畫演練，以確保人員充分熟悉，符合事件復原計畫、持續營運和緊急應變計畫之要求。並依據訓練、演習及實際事件處理等結果，修改復原計畫。
- D. 核能電廠關鍵數位資產資通安全回應計畫之重要關係人應包含有：
 - (1) 實體保安人員。
 - (2) 關鍵數位資產資通安全小組人員。
 - (3) 操作人員。
 - (4) 工程人員。
 - (5) 資訊技術人員。
 - (6) 人力資源人員。
 - (7) 系統支援廠商。
 - (8) 組織管理人員。
 - (9) 法務人員。

2. 事件回應訓練

核能電廠應執行下列事項：

- (1) 每年至少依人員職司，實施一次關鍵數位資產事件回應教育訓練。
- (2) 事件回應教育訓練應結合事件模擬，以確保在緊急情況下有效回應。
- (3) 記錄事件回應訓練成效，並確認訓練人員合格。

3. 事件回應測試與演練

核能電廠應執行下列事項：

- (1) 至少每年實施關鍵數位資產事件回應測試和演練一次。
- (2) 依據核能電廠定義的測試或演練或兩者，提昇事件回

應能力，以維持其效能。

- (3) 提供測試和演練的處理流程。
- (4) 採用自動化機制徹底有效地提升事件回應的能力。
- (5) 實施和記錄定期、不定期的測試及演練。

4. 事件處理

A. 核能電廠應執行下列事項：

- (1) 實施和記錄現有事件處理能力，包含準備、偵測和分析、攔截、消滅和回復之事件處理計畫。
- (2) 蒐集事件處理活動，納入事件回應程序及處理程序中。
- (3) 組織關鍵數位資產資通安全事件回應小組。
- (4) 當發生未預期之事件，導致資訊安全人力不足時，可調動現場所有訓練合格人員支援，或電話通知 2 小時內可抵達現場之非值勤人員。
- (5) 提供回應小組人員技術能力和充分授權，以有效回應潛在資安事件。
- (6) 擬訂和記錄關鍵數位資產資通安全回應小組處理程序和管控措施，以發現或識別潛在或實際的資通安全攻擊。
- (7) 回應內容包含：
 - a. 辨識資安攻擊種類。
 - b. 識別其威脅等級。
 - c. 描述事件回應與復原 (Incident Response & Recovery, IR&R) 程序的行動。
 - d. 描述攻擊類型或分類及其減緩方法。
 - e. 確定防禦策略可以協助辨識和攔截資安攻擊。
 - f. 描述事件回應小組事件通知過程。
 - g. 與內部人員或外部機構相關人員連繫。

B. 關鍵數位資產資通安全回應小組成員應具有下列知識和經驗：

- (1) 資訊與數位系統技術。
- (2) 核設施操作、工程與安全。
- (3) 實體保安。
- (4) 核能電廠可對外延聘資通安全專業組織或專家協助。

C. 可視情況以下列人員組成關鍵數位資產資通安全事

件回應小組：

- (1) 核能電廠實體保安人員。
- (2) 核能電廠管理人員。
- (3) 公關人員。
- (4) 法務人員。

D. 事件資料蒐集內容包含：

- (1) 事件標題。
- (2) 事件日期。
- (3) 報告的可靠性。
- (4) 事件的型式。
- (5) 進入點。
- (6) 犯罪者。
- (7) 系統、硬體或軟體的影響類型。
- (8) 事件簡要說明。
- (9) 對電廠的影響。
- (10) 預防復發安全管控措施。
- (11) 參考資料。

5. 事件監控

以自動機制追蹤記錄資安事件發生歷程，以利事後之蒐集分析。

6. 事件報告

核能電廠應依通報程序，報告資通安全事件。

7. 事件回應協助

A. 核能電廠應有訓練合格、可全時提供建議及協助使用者回應與事件報告之稱職人員。

B. 核能電廠採取增加提供事件回應相關資訊與支援的機制。

8. 事件回應計畫

A. 核能電廠擬訂關鍵數位資產資通安全回應計畫：

- (1) 描述關鍵數位資產資通安全事件回應之組織與結構。
- (2) 提供資安事件回應之方法。
- (3) 定義可報告的資安事件內容。
- (4) 量測組織事件回應的能力。
- (5) 定義有效支援維持事件回應所需的資源與管理。
- (6) 關鍵數位資產資通安全計畫負責人審查核准。

- B. 核能電廠應分送事件回應計畫予相關事件回應人員，並每年審查一次，以修改實施或演練時遭遇問題。

(四) 審查發現

審查人員確認核能電廠事件回應證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.6.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.8.

3.1.5.2.7 意外事件應變/SSEP 功能持續計畫

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產意外事件應變/SSEP 功能持續計畫(以下簡稱意外事件應變計畫)。核能電廠應擬訂意外事件應變計畫政策及實施程序，以維持核能電廠意外事件應變作業，能維持於可接受程度及功能回復的高度保證。審查內容包含：(1)意外事件應變計畫政策及程序；(2)意外事件應變計畫；(3)意外事件應變計畫測試；(4)意外事件應變計畫訓練；(5)備份儲存位置；(6)關鍵數位資產備份；(7)復原與重建。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全意外事件應變計畫：

1. 意外事件應變計畫政策與程序
 - A. 核能電廠應擬訂、宣示，並每年審查和修訂意外事件應變計畫如下：

- (1) 制定和執行意外事件應變計畫的政策，定義的目的、範圍、角色、責任和管理層承諾，並協調各部門。
 - (2) 明文擬訂意外事件應變計畫處理程序。
- B. 意外事件應變計畫包含：
- (1) 必須針對不同事件或條件的持續時間和嚴重程度，擬訂意外事件應變計畫啟動時機。
 - (2) 關鍵數位資產與外界中斷連線，直至回復安全狀態之手動作業模式程序。
 - (3) 回應者的角色與責任。
 - (4) 備份及安全資訊的處理與程序。
 - (5) 完整和最新的網路邏輯架構圖。
 - (6) 授權處理及網路存取關鍵數位資產人員的清單。
 - (7) 於緊急情況下，通知相關人員。
 - (8) 記錄更換元件的要求。

2. 意外事件應變計畫

核能電廠應執行下列事項：

- A. 實施關鍵數位資產資通安全意外事件應變計畫，以維持安全、保安及緊急應變(SSEP)的功能正常。
- B. 協調核能電廠意外事件應變計畫與緊急應變計畫及保安計畫等相關的計畫和需求。
- C. 記錄與維持必要的資源和容量，以確保危機狀況下，必要的資訊處理、電信及支持維運環境。
- D. 建置關鍵數位資產，使其當某些關鍵數位資產程式失效或通訊設備失效之事件發生時，關鍵數位資產執行預先設定動作。

3. 意外事件應變計畫測試

核能電廠應執行下列事項：

- A. 至少每年測試和演練意外事件應變計畫一次，以驗證計畫有效及電廠可迅速執行此計畫。
- B. 審查意外事件應變計畫測試和演練的結果與適當的修正措施。
- C. 協調核能電廠與意外事件應變計畫測試和演練相關的計畫。
- D. 記錄測試演練意外事件應變計畫之突發狀況，使其熟悉設施及可用的資源，以評估核能電廠的應變處理能

力。

- E. 採取自動化機制，以有效地測試演練，以涵蓋更完整的意外事件應變之議題。
- F. 復原和重建應納入意外事件應變計畫測試和演練。
- G. 當意外事件應變計畫測試和演練會影響安全、保安及緊急應變(SSEP)功能而無法實施時，核能電廠應建立和記錄替代管控措施。
- H. 應利用定期和不定期的維護活動，進行意外事件應變計畫測試和演練。

4. 意外事件應變計畫訓練

核能電廠應執行下列事項：

- A. 核能電廠應依意外事件應變計畫成員角色及責任，提供必要的訓練，並至少每年實施一次再教育。
- B. 保存訓練程序和人員訓練文件紀錄。
- C. 實施意外事件應變計畫人員演練教育，以確保熟悉設施、關鍵數位資產和資源，和評估電廠支援意外事件應變計畫的能力。
- D. 採取自動化機制，以徹底有效地測試演練，以涵蓋更完整的意外事件應變計畫議題。
- E. 選擇真實的測試環境和演練劇情，有效實施關鍵數位資產壓力測試。

5. 備份儲存位置

- A. 核能電廠應記錄關鍵數位資產備份儲存的位置、備份頻率及備份資訊傳送儲存位置之傳送率，以利於核能電廠復原計畫實施。
- B. 核能電廠應執行下列事項：
 - (1) 確定備份資料儲存位置和實體主儲存環境不同地理區隔。
 - (2) 配置備份儲存環境，以利於設施復原作業。
 - (3) 確認備份儲存位置潛在存取的問題，當發生廣域的破壞或災害時，可採取有效的減緩措施。

6. 關鍵數位資產備份

核能電廠應執行下列事項：

- A. 進行使用者層級和系統層級資訊備份。
- B. 採取時間或事件觸發關鍵數位資產備份。
- C. 保護備份資訊於儲存位置。

- D. 定期每半年測試，以驗證儲存媒介可靠性及資訊完整性。
- E. 意外事件應變計畫測試，包含以備份資料回存至關鍵數位資產。
- F. 保護備份資訊，以防止遭受未授權者修改。
- G. 關鍵數位資產備份之資料，應和設施分開儲存，並採用防火容器保存。
- H. 建立和記錄關鍵數位資產資料必須回存的時間間隔，以及重要資料和構型變更頻率。

7. 復原與重建

核能電廠採用將關鍵數位資產回復和重建至損壞之前已知的安全狀態之機制，並在設備返回正常作業前執行測試，以確保關鍵數位資產正常運作。

(四) 審查發現

審查人員確認核能電廠意外事件應變計畫證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. 10 CFR 73.54(c)(4) “Ensure that the functions of protected assets identified by paragraph (b)(1) of this section are not adversely impacted due to cyber-attacks.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.7.
3. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.9.

3.1.5.2.8 認知及訓練

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產認知及訓練，核能電廠應擬訂認知及訓練政策及實施程序，對核能電廠人員及合約廠商實施教育訓練，使其維持資通安全適當防護水準，以確保關鍵數位資產高度安全保證。審查內容包含：(1)認知及訓練政策及程序；(2)認知訓練；(3)技術訓練；

(4)特殊資通安全訓練；(5)跨功能關鍵數位資產資通安全小組；(6)狀態認知；(7)回饋；(8)訓練紀錄；(9)與資安組織接觸互動；(10)角色與職責。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產認知與訓練：

1. 認知及訓練政策及程序
 - A. 擬訂實施並記錄核能電廠人員及合約廠商訓練需求，以滿足其職責所需之要求。
 - B. 訓練所有相關人員具有其職責所需之資通安全知識。
 - C. 制定、發布、定期審查和更新程序，以促進和維持資通安全訓練。
2. 認知訓練
 - A. 核能電廠認知訓練以提高人員對資安威脅和弱點的敏感度，使員工和合約廠商了解核能電廠的關鍵數位資產資通安全政策，以使關鍵數位資產資通安全計畫有效實施，及了解其責任所必須依循政策和標準要求。
 - B. 建立實施並記錄下列需求：
 - (1) 提供核能電廠人員基本關鍵數位資產資通安全認知訓練計畫，於員工再教育或持續教育中，認知更新的網路威脅及技術教育。
 - (2) 利用海報、顯示螢幕、電子郵件等宣示方式，實施員工認知教育。
 - (3) 訓練包括實際演練，以模擬實際資安事件、復原計畫、回應計畫和資安攻擊等。
 - C. 核能電廠基於下列事項擬訂與記錄關鍵數位資產資通安全訓練內容：
 - (1) 賦予之角色及職責。
 - (2) 防禦策略需求。
 - (3) 關鍵數位資產授權存取人員。

D. 擬訂核能電廠員工及合約廠商認知訓練，以使其了解如下：

- (1) 電廠的目標、管理期許、角色和責任、政策、程序等，以及違反資安計畫的後果。
- (2) 一般的資安攻擊方法。
- (3) 資安攻擊跡象，例如：
 - a. 不正常的網路高流量。
 - b. 不正常的 CPU 高使用率。
 - c. 建立新使用者。
 - d. 嘗試或使用管理者帳號。
 - e. 使用關閉帳號。
 - f. 使用未值勤之使用者帳號。
 - g. 清除紀錄檔。
 - h. 紀錄檔出現大量的不正常事件紀錄。
 - i. IDS 或防毒軟體警告。
 - j. 防毒軟體被停用。
 - k. 非預期的修補程式。
 - l. 連線至外界的網路位址。
 - m. 要求系統資訊(社交工程)。
 - n. 非預期的構型變更。
 - o. 非預期的系統關機。
 - p. 控制設備不正常活動。
 - q. 控制設備失去訊號。
 - r. 不正常的裝置於安全區域內。
- (4) 發現可疑資通安全活動時，應如何反應及向何人通報。
- (5) 說明存取和管控方法。
- (6) 使用者能降低風險的管控措施。
- (7) 未整合的控制方法對組織的影響。

3. 技術訓練

- A. 建立實施和記錄技術訓練，以確保維持其熟練程度。包含關鍵數位資產的設計、修改、維護的教育訓練。
- B. 核能電廠應建立實施和記錄如下：
 - (1) 提供人員資通安全相關教育訓練：
 - a. 授權存取關鍵數位資產或指派任務前。
 - b. 政策和程序變更時。

- c. 每年至少辦理一次教育訓練。
 - (2) 提供人員職責相關的關鍵數位資產資通安全技術教育訓練概念和實務，包含關鍵數位資產之設計、安裝、操作、維護和管理或資通安全：
 - a. 特殊的資通安全、工程程序、實務和技術等。
 - b. 一般的關鍵數位資產潛在資通安全弱點、資安攻擊及風險降低方法等。
 - C. 提供系統管理員、關鍵數位資產資通安全專家、系統負責人、網管人員和其他人員具有存取資通安全技術相關系統層級軟體之訓練。
4. 特殊資通安全訓練
- A. 核能電廠人員須有計畫、有程序的授權與訓練資通安全專家，使其具有順利執行職責所需的能力，必須接受包含設計、執行、管理防禦策略等內容之特殊資通安全訓練。
 - B. 建立實施和記錄關鍵數位資產資通安全專家人員進階訓練，包含角色、職責、事件回應、以及深度防禦策略的執行和管理，進階訓練內容應含：
 - (1) 建立並維持必須資料安全、作業系統安全、應用程式安全、網路安全、安全管控措施、入侵分析、事件管理及回應、數位鑑識、滲透測試及電廠系統功能與運作等的最新技術和核心能力。
 - (2) 實體和邏輯強化關鍵數位資產，以降低網路遭弱點攻擊之工具和技術。
 - (3) 提供對其他人員資通安全的指導、協助或訓練。
 - (4) 審查關鍵數位資產資通安全計畫與實務。
 - (5) 評估關鍵數位資產、網路及資產是否符合資通安全政策。
 - (6) 設計、取得、安裝、操作、維護或管理等安全管控措施。
5. 跨功能關鍵數位資產資通安全小組
- A. 核能電廠應組成具跨功能的關鍵數位資產資通安全小組。
 - B. 核能電廠應擬訂和記錄關鍵數位資產資通安全小組成員分享專業知識和多領域知識之計畫。
 - C. 核能電廠關鍵數位資產資通安全小組至少應由資訊

專業、儀器及控制系統工程師、控制系統現場操作人員、網路安全專家及電廠管理階層人員組成。

D. 關鍵數位資產資通安全專家必須具有網路架構和設計、安全處理及實務及安全基礎建設之設計和操作技能。

E. 核能電廠關鍵數位資產資通安全小組必要時應包含控制系統供應商及系統整合人員。

6. 狀態認知

核能電廠安全訓練需敘述實體處理的控制以及相關的關鍵數位資產和其安全管控措施。

7. 回饋

核能電廠應建立實施和記錄人員和承攬商的訓練回饋程序，以改善資通安全計畫和訓練落差。

8. 訓練紀錄

核能電廠應記錄員工之資通安全訓練。

9. 與資安組織接觸

核能電廠應與管制單位或信任組織維持連繫，以取得最新資通安全實務、技術，並彼此分享相關威脅、弱點和事件等資訊。

10. 成員與責任

核能電廠相關資通安全組織、成員職務與責任如下：

A. 資深管理人員由電廠副廠長(含)以上人員擔任，負責：

- (1) 核能電廠關鍵數位資產資通安全計畫總負責人。
- (2) 負責整合整體資通安全計畫的發展、實施與維護所需的資源。

B. 關鍵數位資產資通安全計畫經理

- (1) 監督關鍵數位資產資通安全作業實施。
- (2) 關鍵數位資產資通安全相關議題的單一聯絡窗口。
- (3) 關於關鍵數位資產資通安全問題的監督和指導。
- (4) 必要時，啟動和協調資通安全事件回應小組(CSIRT)。
- (5) 必要時，於關鍵數位資產資通安全事件發生時及發生後，負責與管制單位聯繫協調。
- (6) 監督和核准關鍵數位資產資通安全計畫之發展與實施。

- (7) 確保與核准關鍵數位資產資通安全教育、認知及其訓練活動的實施。
- C. 關鍵數位資產資通安全專家
- (1) 防護關鍵數位資產以免受資安威脅。
 - (2) 配置、操作及維護資通安全設備。
 - (3) 從關鍵數位資產資通安全角度了解整體核能電廠的網路作業環境、硬體平台、軟體平台、作業系統及應用程式。核能電廠內特殊的應用程式及其服務及協定。
 - (4) 實施數位系統的資通安全評估。
 - (5) 進行關鍵數位資產的稽核、弱點評估、網路掃描及滲透測試。
 - (6) 資通安全事件調查期間，證據搜集及證據保存。
 - (7) 維持資通安全領域的專業和知識技能。
- D. 關鍵數位資產資通安全回應小組
- (1) 當已知或懷疑關鍵數位資產發生關鍵數位資產資通安全事件時，採取適當的回應和措施，以保護關鍵數位資產，並協助受損系統的復原。
 - (2) 抑制並減緩關鍵數位資產資通安全事件波及其他關鍵數位資產，並確保事件後受損系統能及時回復。

(四) 審查發現

審查人員確認核能電廠認知及訓練證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. 10 CFR 73.54(d)(1) “Ensure that appropriate facility personnel, including contractors, are aware of cyber security requirements and receive the training necessary to perform their assigned duties and responsibilities.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.8.
3. RG 5.71 “Cyber security program for nuclear facilities”.

3.1.5.2.9 構型管理

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產構型管理，核能電廠應擬訂構型管理政策及實施程序，提供完善可靠的構型管理，以確保(1)關鍵數位資產構型變更不會降低現有的安全及(2)防止任何未經授權或無意的修改。審查內容包含：(1)構型管理政策及程序；(2)基準構型；(3)構型變更管理；(4)構型變更影響分析；(5)構型變更之存取限制；(6)構型設定；(7)最小功能；(8)備品庫存。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產構型管理：

1. 構型管理政策及程序
 - A. 核能電廠應發展宣示並且每年審查和更新明文制訂構型管理策略及實施程序，定義核能電廠的構型管理政策、範圍、作用、要求、責任和管理階層的承諾，提供完善可靠的構型管理。
 - B. 核能電廠關鍵數位資產構型管理內容包含硬體構型、軟體構型及存取權限，軟硬體之變更並須符合政策及程序要求。
 - C. 構型變更流程，在變更前應評估和管控關鍵數位資產變更，確保不會引發新的弱點。
2. 基準構型
 - A. 核能電廠應發展和記錄並維持關鍵數位資產基準構型，其包含關鍵數位資產之構型設定、連接之介面設定、資通安全要求和通訊連接特性。核能電廠應採自動或人工機制保存所有關鍵數位資產最新、最完整、最精確且立即可用的基準構型。
 - B. 核能電廠應記錄最新的基準構型，並每季稽核一次。基準構型內容包含關鍵數位資產所有軟硬體元件清

單、週邊之構型、目前所使用軟體版本和硬體設定等。核能電廠應記錄構型變更人員、日期和目的等變更設定紀錄。

- C. 核能電廠應記錄並維護開發中基準構型和測試環境，必須與現行維運之基準構型隔離。
- D. 核能電廠應採取「正向表列」授權政策，管理關鍵數位資產之存取或變更權利，以確保關鍵數位資產之安全。當授權變更後，須經驗證維持於適當安全水準。
- E. 必須經適當的訓練和認定資格之人員，執行關鍵數位資產修改。核能電廠應擬訂上述人員所需之適合存取權限。核能電廠應採電子監控方式，以確保僅被授權人員可存取關鍵數位資產。當無法採取電子監控方式時，應說明理由並採取如下措施：
 - (1) 實體限制存取。
 - (2) 監控和記錄實體存取，以即時偵測和回應發現入侵者。
 - (3) 採取稽核和驗證。
 - (4) 確認被授權人員值得信賴。
 - (5) 確認被授權人員作業在管理階層管控中。
 - (6) 變更後檢測，以確認是否正確。
- F. 至少每季稽核一次變更紀錄。

3. 構型變更管理

核能電廠應執行下列事項：

- A. 核准和記錄關鍵數位資產變更。
- B. 保存及審查關鍵數位資產變更、查核關鍵數位資產構型變更與運用自動或人工紀錄：
 - (1) 記錄關鍵數位資產變更。
 - (2) 通知指定核准人員。
 - (3) 在未經批示之前，不得實施變更。

4. 構型變更影響分析

- A. 核能電廠關鍵數位資產資通安全小組負責評估記錄構型變更風險。
- B. 核能電廠應將安全影響分析列入變更核准處理流程。

5. 構型變更之存取限制

- A. 核能電廠應定義、核准和強制實施實體和邏輯存取限制，每季產生、稽核和保存變更紀錄。實施構型管理

計畫因應發現的差異。

- B. 採取自動化機制強制偵測未授權變更、存取限制、支援事後稽核。
- C. 當無法以自動化實施存取限制時，應說明理由，並採取如下強制措施：
 - (1) 實體存取限制。
 - (2) 監控和記錄實體存取，以即時偵測和回應發現入侵者。
 - (3) 採取稽核和驗證。
 - (4) 確認被授權人員值得信賴。
 - (5) 確認被授權操作人員在管理階層管控中。
 - (6) 變更後檢測，以確認是否正確。

6. 構型設定

- A. 核能電廠採用嚴謹限制模式 (Most Restrictive Mode)；評估作業需求及強化構型設定作業等三方式，以管理關鍵數位資產構型設定。完成如下：
 - (1) 依循嚴謹限制模式建立關鍵數位資產構型設定。
 - (2) 基於作業需求評估，依據對關鍵數位資產設定之嚴謹模式，記錄和核准例外狀況。
 - (3) 監控關鍵數位資產構型設定，以符合電廠資通安全政策及程序。
 - (4) 採取自動化機制，管理(例如集中式管理)、應用和驗證構型設定。
 - (5) 採取自動或人工回應未授權之構型變更。
 - (6) 若無法採自動化機制管理、應用和驗證構型設定，核能電廠應採取如下替代管控措施：
 - a. 實體存取限制。
 - b. 監控和記錄實體存取，以即時偵測和回應發現入侵者。
 - c. 採取稽核和驗證。
 - d. 確認被授權人員值得信賴。
 - e. 確認被授權操作人員在管理階層管控中。
 - f. 變更後檢測，以確認是否正確。

7. 最小功能

- A. 設定與記錄關鍵數位資產構型設定，僅提供必要能力，以保護、限制不安全的功能、通訊埠、通訊協定

和服務。核能電廠應每月檢查關鍵數位資產，辨識清除沒必要的功能、通訊埠、通訊協定與服務。

B. 核能電廠應採取自動化與正向表列/負向表列或兩者結合(White-lists, Black-lists, Gray-lists)之應用管控技術，防止未授權的程式執行。

8. 備品庫存

核能電廠應實施和維持關鍵數位資產元件備品庫存：

A. 反應現行系統精確的構型。

B. 確保關鍵數位資產所有元件之實體或邏輯位置均位於與關鍵數位資產相同安全層級內。

C. 提供元件組成的適當劃分，以俾利追蹤、報告與財產清點。

D. 系統元件庫存更新。

E. 採取自動化機制維持最新、完整、精準的和立即可用的系統元件庫存。

F. 採取自動化機制偵測增加的未授權之元件或設備，禁制(Disable)此元件或設備之存取功能或通知負責人員。

G. 記錄元件管理員所應負之責任。

(四) 審查發現

審查人員確認核能電廠構型管理證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. 10 CFR 73.54(d)(3) “Ensure that modifications to assets, identified by paragraph (b)(1) of this section, are evaluated before implementation to ensure that the cyber security performance objectives identified in paragraph (a)(1) of this section are maintained.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.2.9.
3. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.11.

3.1.5.3 管理管控

審查人員依據本導則，審查核能電廠技術、操作及管理安全管控措施。管理管控措施集中於管理風險及安全政策環境保護。包含：(1)系統與服務取得；(2)安全評鑑與風險管理。

3.1.5.3.1 系統及服務取得

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產系統及服務取得，核能電廠應擬訂系統及服務取得政策及實施程序，提供系統及服務取得完整性，以及維持實施與有關廠商與發展生命週期的採購安全。審查內容包含：(1)系統與服務取得之政策及程序；(2)供應鏈保護；(3)信任機制；(4)安全能力整合；(5)系統開發商安全測試；(6)核能電廠測試。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全計畫系統及服務取得：

1. 系統與服務取得之政策及程序
 - A. 核能電廠應明文擬訂並每年審查和更新一次系統及服務取得政策，定義目的、範圍、角色、責任及管理階層承諾，協調要求各部門依循，提供維持系統及服務取得完整性的高度保證。
 - B. 核能電廠應明文擬訂並每年審查和更新一次系統服務取得作業程序，供系統服務取得作業依循。
2. 供應鏈保護
 - A. 核能電廠進行下列的措施維護關鍵數位資產的完整性，防止受到供應鏈的威脅：
 - (1) 建立可信任的配送途徑。
 - (2) 供應商的驗證。
 - (3) 產品必須有防竄改證明或防竄改封裝。
 - B. 核能電廠所有取得關鍵數位資產必須分析，以確認取

得關鍵數位資產符合資通安全需求。

3. 信任機制

要求軟體系統供應商使用軟體品質和驗證方法，以減少軟體的缺陷。建立、實施及記錄要求，以要求所有用來執行網路安全任務或 SSEP 功能的工具，是經過商業品管程序與軟體工程工具開發之數位儀控系統。

4. 安全能力整合

A. 核能電廠應實施並記錄以下事項：

- (1) 識別不斷變化的資安威脅和弱點。
- (2) 認識先進的資通安全保護策略和安全管控。
- (3) 分析先進資通安全功能可能對關鍵數位資產、系統和網路的資通安全、安全和操作之影響，並能及時實施先進資通安全功能。
- (4) 當更新舊系統時，新系統需考量資通安全功能。

5. 系統開發商安全測試

A. 核能電廠應要求關鍵數位資產系統開發商與整合商實施安全測試評估計畫，以確保所取得之關鍵數位資產滿足：

- (1) 提供免於遭受已知和可測知的弱點和惡意程式碼危害之產品，查明並刪除下列弱點：
 - a. 脆弱、未被驗證、非標準的加密模組。
 - b. 敏感通訊之不安全網路協定
 - c. 已知不安全之軟體元件或函式庫。
 - d. 已知弱點。
 - e. 應用程式使用控制特性之不安全構型設定或選項。
 - f. 不當的存取控制機制，存取系統資源。
 - g. 不當的授權機制。
 - h. 不當或未進行輸入/輸出資料驗證。
 - i. 不安全或不足夠地記錄系統錯誤或安全相關資訊。
 - j. 不足夠的資料緩衝。
 - k. 字串格式弱點。
 - l. 使用者權限提升弱點。
 - m. 不安全的資料庫交易。
 - n. 不安全使用之原生函數呼叫(native function

call)。

o. 包含在程式碼中隱藏的功能和弱點。

p. 實施安全作為不能增加安全弱點之風險，增加資安攻擊容易度及降低可靠度。

q. 使用不支援或無記載之方法或函數。

r. 使用無記載程式碼或惡意函數可能導致未授權之存取或超越系統需求之行為。

(2) 系統開發商實施與本導則相同之安全管控措施，以防止取得系統被竄改，維持取得系統完整性，直至交付核能電廠。

B. 核能電廠要求系統開發商實施並記錄安全需求和驗證與確認安全管控措施，以符合資通安全要求。

C. 系統開發商應提供下列文件：

(1) 系統設計轉換成程式碼、資料庫結構以及機器可執行的表示方式。

(2) 軟硬體配置和安裝。

(3) 軟體程式撰寫和測試。

(4) 通訊配置和安裝。

(5) 單元測試結果證明程式碼正確、精確和完全符合需求設計。

(6) 記錄所有資通安全功能需求之程式庫實施的細節，包括資通安全功能的程式碼、函式與參照的模組。

(7) 安全設定符合需求書安全規範。

(8) 作業系統安全設定符合需求書安全規範。

(9) 程式語言支援源碼檢測，並能產生如下檢測報告

a. 靜態原始碼弱點分析找出潛在安全缺陷、程式碼常式和潛藏功能。

b. 採取安全缺陷追蹤度量，以追蹤原始碼缺陷識別、型態、類別、原因和修補。

c. 將需求轉換到程式碼過程中，所產生的缺陷。

(10) 對所有程式語言應記載如下：

a. 在建置程式庫和方法期間，執行動態原始碼弱點分析，以檢查潛在安全缺陷、不良程式設計習慣、隱藏的功能和程式碼內弱點，以刪除弱點。

- b.採取安全缺陷追蹤度量，以追蹤原始碼缺陷識別、型態、類別、原因和修補。
 - c.將需求轉換到程式碼過程中，所產生的缺陷。
- D. 核能電廠應要求關鍵數位資產系統開發商或整合商：
- (1) 關鍵數位資產設計、開發、實施、運作過程中，實施構型管理。
 - (2) 關鍵數位資產的變更管理。
 - (3) 僅允許經核能電廠同意之變更。
 - (4) 記錄關鍵數位資產的同意變更。
 - (5) 追蹤安全缺陷及解決方案。

6. 電廠測試

- A. 核能電廠應驗證開發商提供前述之測試結果。
- B. 核能電廠應執行下列事項：
- (1) 以備品或相容關鍵數位資產離線測試安全設備、安全管控及軟體，以確保不會危及或相互影響其它關鍵數位資產。
 - (2) 測試通訊路徑，以確保無提供通訊路徑危及關鍵數位資產或其它關鍵數位資產。
 - (3) 依關鍵數位資產資通安全計畫實施安全管控措施，並測試安全管控措施效力。
 - (4) 實施弱點掃描、校正、消除程序。
 - (5) 安裝至目標環境。
 - (6) 實施驗收審查和測試關鍵數位資產的安全特性。
- C. 核能電廠應有如下紀錄：
- (1) 依據關鍵數位資產資通安全計畫實施安全管控措施。
 - (2) 驗證安全管控措施符合資通安全計畫需求。
 - (3) 實施關鍵數位資產之弱點掃描、校正及消除。
- D. 核能電廠每年應稽核關鍵數位資產以驗證如下：
- (1) 安全管控措施功能正常。
 - (2) 關鍵數位資產無受已知弱點與安全危害，核能電廠並持續提供弱點危害資訊。
 - (3) 變更管理功能有效運作，適當地記錄構型變更。

(四) 審查發現

審查人員確認核能電廠系統及服務取得證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.3.1.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.12.

3.1.5.3.2 安全評鑑及風險管理

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產安全評鑑及風險管理，以確保核能電廠關鍵數位資產資通安全適當的管理與評估。審查內容包含：(1)威脅和弱點管理；(2)風險減緩；(3)矯正行動方案。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產安全評鑑及風險管理：

1. 威脅和弱點管理
 - A. 核能電廠應執行下列事項：
 - (1) 定期至少每季一次及當有新的潛在關鍵數位資產弱點報告或識別時，實施關鍵數位資產弱點評估與掃描。
 - (2) 採取弱點掃描工具和技術，依下列程序，促進工具與自動弱點管理間的協調：
 - a. 列舉具有弱點之作業系統平台、軟體缺陷和不適當的構型設定。
 - b. 製作清晰的核對清單和測試程序。

c. 衡量弱點影響。

- (3) 即時分析弱點掃描報告和修補弱點，以確保關鍵數位資產的高度安全，以免遭受資安攻擊。
- (4) 刪除其它關鍵數位資產相似的弱點。
- (5) 採用之掃描工具，應具有定期每個月或當有新的關鍵數位資產報告或識別時，進行弱點掃描和更新之能力。
- (6) 弱點掃描程序應執行最深最廣之掃描範圍。
- (7) 辨別和記錄關鍵數位資產可能暴露何種資訊。
- (8) 執行資通安全測試，以確定使用者難以規避關鍵數位資產安全管控措施。測試方法包含滲透測試 (Penetration Testing)、惡意使用者測試 (Malicious User Testing)、及獨立的驗證與確認 (Independent Verification and Validation) 等。
- (9) 給與弱點掃描特別存取權限，以達徹底掃描。
- (10) 採取自動化機制比較弱點掃描結果，以了解關鍵數位資產弱點和修補的趨勢。
- (11) 採取自動化偵測關鍵數位資產未授權軟體，並通知相關人員。
- (12) 實施弱點掃描過程不可以危害關鍵數位資產安全、保安及緊急應變 (SSEP) 功能，若有危害關鍵數位資產，應該移除此服務或複製，或於停機期間進行。

B. 核能電廠應審查歷史紀錄，以確定關鍵數位資產發現的弱點是否先前已遭利用。

2. 風險減緩

核能電廠應實施如下風險保護和減緩措施：

- (1) 深度防禦策略。
- (2) 安全管控措施。
- (3) 數位裝置和軟體資安攻擊偵測、預防和復原技術。
- (4) 詳細的安全管控措施資訊，以提供管制單位人員視察和稽核。

3. 矯正行動方案

核能電廠建立實施和記錄證明關鍵數位資產資通矯正行動與本導則及 RG 5.71 是一致的。資安事件進行評估、追蹤，採取矯正行動方案以符合本導則。

(四) 審查發現

審查人員確認核能電廠安全評鑑及風險管理證明文件齊備，符合上述(三)審查要點接受基準要求。當核能電廠無法實施(三)所述安全管控措施，可依 3.1.5 第二~三段所述採取替代安全管控措施及說明理由。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.3.3.3.2.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.13.

3.2 納入實體保安計畫

本節要求核能電廠應將關鍵數位資產資通安全計畫納入電廠實體保安計畫中。

(一) 審查範圍

核能電廠應建立與實施關鍵數位資產資通安全計畫，並納入實體保安計畫。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 關鍵數位資產資通安全計畫納入核能電廠實體保安計畫
建立實體保安和關鍵數位資產資通安全整合管理：
 - A. 建立統一的安全組織包含資通安全及實體保安，並獨立運作。
 - B. 記錄實體保安及資通安全間依存。
 - C. 發展完整和統一實體保安及資通安全管控措施之政策及程序。
 - D. 統合政策及程序，以保護關鍵數位資產免受設計基礎威脅 (DBT)之攻擊。
 - E. 協調實體保安及資通安全服務、訓練、設備及裝置。
 - F. 協調實體保安及資通安全人員活動和訓練。

- G. 整合和協調實體保安及資通安全事件回應。
- H. 訓練高階管理人員同時具有實體保安與資通安全兩方面的知識。
- I. 定期實施結合資通安全與實體保安的情境演練。

(四) 審查發現

審查人員應確認核能電廠關鍵數位資產資通安全計畫實施證明文件齊備，並確實擬訂符合本導則規範之關鍵數位資產資通安全計畫實施內容。

(五) 參考法規與技術規範

1. 10 CFR 73.54(b)(2) “Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.4, Appendix A.3.2.

3.3 政策及實施程序

(一) 審查範圍

核能電廠應擬訂與實施關鍵數位資產資通安全計畫政策及實施程序，以確保核能電廠安全有關與對安全重要的功能、保安功能、緊急應變功能及其支援系統，以確保關鍵系統安全運轉之高度保證。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 核能電廠應擬訂政策與實施程序，以符合本審查導則安全管控目的，並指定由副廠長以上人員負推動和督導之責。
2. 核能電廠應記錄、審查、核准、發布、推動及修改資通安全計畫之政策及實施程序，以及相關人員的責任和實施監督報告應陳核副廠長等高層批核。
3. 實施 3.1.5 安全管控措施。

(四) 審查發現

審查人員應確認核能電廠資通安全計畫實施證明文件齊備，並確實擬訂符合本導則規範之資通安全計畫實施內容

(五) 參考法規與技術規範

1. 10 CFR 73.54(b)(2) “Establish, implement, and maintain a cyber security program for the protection of the assets identified in paragraph (b)(1) of this section.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.3.5, Appendix 3.3.

4. 核能電廠關鍵數位資產資通安全計畫維護

本章在於建立核能電廠關鍵數位資產生命週期中，維護關鍵數位資產資通安全計畫所必要的工作項目，以確保核能電廠關鍵數位資產資通安全的目的。

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全計畫維護，核能電廠應擬訂關鍵數位資產資通安全計畫維護政策及實施程序，以確保核能電廠關鍵數位資產資通安全計畫順利實施。審查內容包含：(1)持續監控與評估；(3)變更控制；(3)資通安全計畫審查。

4.1 持續監測及評估

(一) 審查範圍

核能電廠應建立持續監控與評估程序，以確保安全管控措施及其變更，維持系統、網路及環境不影響安全和效益。審查內容包含：(1)定期評估安全管控措施；(2)核能電廠持續監控及評估。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 定期評估安全管控措施

核能電廠應視情況，至少每年檢視一次電廠安全現況是否符合安全管控措施要求，以確保核能電廠在資通安全生命週期內，能維持強健、彈性和有效。

2. 核能電廠持續監控及評估應依如下執行：

A. 弱點掃描：

(1) 核能電廠應定期至少每季執行一次所有關鍵數位資產設備的弱點掃描及評估(若可掃描，須做掃描及評估；若不可掃描，只須做評估)。

(2) 核能電廠應確保進行弱點掃描程序時，不會影響安全、保安及緊急應變(SSEP)的功能；若會影響，應於掃描前，先將這此服務移除或複製備份。

B. 核能電廠每年至少一次檢視電廠安全管控措施的效益，內容包含：

(1) 定期稽核實體保安計畫、安全管控措施、實施程序、資通安全計畫。

- (2) 安全/保安間之介面活動。
- (3) 對當前資通安全威脅的假設和結論再評估。
- (4) 測試、維護及校準計畫。
- (5) 對外部的回饋資訊的處理。

(四) 審查發現

審查人員應確認核能電廠持續監控及評估證明文件齊備，定期實施弱點掃描及檢視安全管控措施之效益。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.4.1.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.13.

4.2 變更控制

(一) 審查範圍

核能電廠應依據變更管控構型管理規範建立關鍵數位資產軟體/硬體元件清單，設備及軟體構型、現有軟體版本、硬體/軟體元件設定等基準，並確定在控制及協調方式下，進行核能電廠關鍵數位資產變更。審查內容包含：(1)變更管理；(2)構型管理；(3)影響分析；(4)更新資通安全實務。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 有效的變更管理，至少應記錄以下：
 - A. 構型變更的日誌。
 - B. 變更的日期及時間。
 - C. 變更的目的。
 - D. 有效的變更管控證明。
 - E. 任何在變更過程中的觀察發現。
2. 構型管理
 - A. 核能電廠應確保關鍵數位資產構型和變更管理過程中，維持資通安全規範。任何修改，均需經過安全評估，確保符

合資通安全要求。

- B. 核能電廠於維運生命週期中，對關鍵數位資產的變更作業，應立即有效地實施構型管理程序，以避免引發額外的弱點或風險。

3. 影響分析

- A. 核能電廠應評估與記錄與其它關鍵數位資產或系統之安全和保安的相互依賴之安全影響分析，更新與記錄下列事項：
 - (1) 關鍵數位資產的位置和連接的資產。
 - (2) 連接路徑。
 - (3) 基礎建設的相互關係。
 - (4) 防禦策略的應用，包含防禦架構、安全管控措施，及其他防禦策略措施。
 - (5) 全廠實體和資通安全防禦策略及程序的文件，包含減緩攻擊及事故回應和復原。
 - (6) 篩選、評估、減緩和處理威脅的程序，以及從可信賴的來源獲得的弱點通知。

4. 關鍵數位資產資通安全更新實務

- A. 核能電廠審查和更新關鍵數位資產資通安全政策、程序、實務、現存資通安全管控、網路實體和邏輯架構、資通安全設備及任何與關鍵數位資產安全管控措施之相關資訊，包含如下：
 - (1) 與核能電廠關鍵數位資產資通安全相關之政策、程序及現存實務。
 - (2) 網路架構圖。
 - (3) 資通安全設備或關鍵數位資產之構型資訊。
 - (4) 新的防禦策略、安全管控措施發展與佈署。
 - (5) 核能電廠實體和作業安全計畫。
 - (6) 資通安全相關的廠商與連絡人。
 - (7) 潛在的資安攻擊。
 - (8) 最近的資通安全研究或稽核。
 - (9) 支援關鍵系統正常功能之基礎建設。

(四) 審查發現

審查人員應確認核能電廠變更管理證明日誌圖表及其它證明文件齊備，核能電廠關鍵數位資產資通安全計畫之影響分析與更新實務規範確實。

(五) 參考法規與技術規範

1. RG 5.71 “Cyber security program for nuclear facilities”. C.4.2.
2. RG 5.71 “Cyber security program for nuclear facilities”. Appendix A.4.2.

4.3 核能電廠關鍵數位資產資通安全計畫內部審查

(一) 審查範圍

審查人員依據本導則，審查核能電廠關鍵數位資產資通安全計畫資通安全計畫內部審查，核能電廠應擬訂資通安全計畫內部審查政策及實施程序，以確保核能電廠關鍵數位資產資通安全計畫順利實施。內部審查內容包含：(1)審查計畫管控程序；(2)審查時機。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

核能電廠必須依下列規範，完成關鍵數位資產資通安全計畫內部審查：

1. 核能電廠應擬訂實施與審核計畫，指出目的、範圍、角色、責任、需求及管理階層承諾，維持本計畫效力。
2. 核能電廠至少每 24 個月實施內部審查關鍵數位資產資通安全計畫一次，並於下列情形下，亦須進行計畫內部審查：
 - A. 於首次啟動關鍵數位資產資通安全計畫後 12 個月內，或對資通安全具有潛在影響之人員、流程、裝置或設施實施變更後 12 個月內。
 - B. 作業環境變更有可能影響關鍵數位資產安全時。
 - C. 基於核能電廠特定分析、評估或用來評估負責計劃管理或執行的績效指標需要時。
3. 核能電廠應記錄關鍵數位資產資通安全計畫內部審查結果、建議、管理發現、及先前的計畫內部審查所提建議方案的執行結果。
4. 核能電廠應設計稽核表格，以方便稽核人員檢查。

(四) 審查發現

審查人員應確認核能電廠內部審查證明文件齊備，確實定期審查安全計畫。

(五) 參考法規與技術規範

1. 10 CFR 73.54(g) “The licensee shall review the cyber security program as a component of the physical security program in accordance with the requirements of § 73.55(m), including the periodicity requirements.”
2. RG 5.71 “Cyber security program for nuclear facilities”. C.4.3.
3. RG 5.71 “Cyber security program for nuclear facilities”. Appendix C.12.

5. 文件控制及紀錄保存

本章在於要求核能電廠應建立必要的程序，記錄關鍵數位資產資通安全計畫所必須的相關紀錄和文件，以供管制單位查閱。

(一) 審查範圍

審查人員依本導則，審查核能電廠資通安全計畫文件之紀錄與保存。核能電廠應建立資通安全發展、審核、驗證、發行和版本等相關活動紀錄。

(二) 程序審查

審查人員依據本審查導則，審查核能電廠是否充分提供上述審查範圍之內容及文件。

(三) 審查要點與接受基準

1. 核能電廠應保存如下紀錄和相關技術文件，直至管制單位停止核能電廠執照：
 - A. 字元所有數位資料紀錄。
 - B. 紀錄檔。
 - C. 稽核檔。
 - D. 非數位資料檔。
 - E. 網路分析紀錄。
 - F. 關鍵數位資產的歷史事件。
2. 核能電廠應保存影響資通安全的紀錄至少 3 年以上。

(四) 審查發現

審查人員應確認核能電廠紀錄與文件保存齊備，並依規定期限實施保存。

(五) 參考法規與技術規範

1. 10 CFR 73.54(h) “The licensee shall retain all records and supporting technical documentation required to satisfy the requirements of this section as a record until the Commission terminates the license for which the records were developed, and shall maintain superseded portions of these records for at least three (3) years after the record is superseded, unless otherwise specified by the Commission.”

2. RG 5.71 “Cyber security program for nuclear facilities”. C.5.

中英名詞對應

Access control：存取控制

Accountability：當責

Audit：稽核

Authentication：驗證

Authoritative server：權威主機

Availability：完整性

Basic Input/output System (BIOS)：基本輸入輸出系統

Challenge-response authentication mechanism：挑戰-回應驗證

Change management：變更管理

Client：用戶端

Command：命令

Common area：共用區

Compiler：編譯程式

Confidentiality：機密性

Configuration：組態或構型

Configuration management：組態管理或構型管理

Control area：控制區

Critical Digital Asset(CDA)：關鍵數位資產

Critical System(CS)：關鍵系統

Cryptography：密碼

Cyber Security Team(CST)：資通安全小組

Cyber Security Incident Response Team(CSIRT)：資通安全事件回應小組

Cyber attack：資安攻擊

Data diodes：單向資料流

Design Based Threat(DBT)：設計基礎威脅

Defense-Strategy：防禦策略

Defense-in-Depth Protective Strategies：深度防禦保護策略

Denial of Service(DOS)：阻斷服務

Equipment：裝置

File：檔案

Handshaking：訊息交換

Host Intrusion Detection System (HIDS)：主機入侵偵測系統

Human machine interface (HMI)：人機介面

Identification：辨識

Incident：資安事件

Integrity：完整性

Internet Protocol(IP)：網際網路協定位址

Intrusion Detection System (IDS)：入侵偵測系統

Localized authentication：區域驗證

Log：日誌

Media Access Control Address(MAC)：儲存媒介存取控制位址

Management Control：管理管控措施

Malware：惡意程式

Mobile code：全部或部份程式取自遠端控制系統之移動碼

Most restrictive mode：最多限制模式

National Institute of Standards and Technology(NIST)：美國國家標準與技術局

Near-real-time：近乎即時

Network：群體電腦連接分享資源之網路

Nonauthenticated human machine interactions (NHMI)：無驗證之人機互動

Nuclear Regulatory Commission(NRC)：美國核能管制委員會

Operation Control：操作管控措施

Open/insecure protocol：開放/不安全的通訊協定

Patch：CDA 修補程式

Programming language：程式語言

programmable logic controller(PLC)：可程式化邏輯控制制器

Protect area：保護區

Recovery：事件發生後回復至發生前狀態之復原作業

Remote access：遠端存取

Review：審查

Risk：風險

Security control：安全管控措施

Safety-related and important-to-safety functions, Security functions, Emergency preparedness function (SSEP), and support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.：執行安全、保安以及緊急應變功能與支援上述功能之系統或設備，其損害會危害上述功能。

Server：伺服器

Session：連線階段

Simple Network Time Protocol (SNTP)：簡單網路時間協定

System component：系統元件

Transmission Control Protocol(TCP)：傳輸控制協定

Technology control：技術管控措施

Third party：第三方

Threat：威脅

Time Stamp：時間戳記

Trojan Horse：木馬程式

User Datagram Protocol (UDP)：使用者資料包協定

Verification：驗證

Verification and validation：驗證與確認

Vital area：緊要區

Vulnerability：弱點

本文章節	RG 5.71
3.1.5.3.1 系統及服務取得	Appendix C.12
3.1.5.3.2 安全評鑑及風險管理	Appendix C.13
3.2 納入實體保安計畫	Appendix A.3.2
3.3 政策及實施程序	Appendix A.3.3
4. 資通安全計畫維護	Appendix A.4
4.1 持續監測及評估	Appendix A.4.1
4.2 變更控制	Appendix A.4.2
4.3 資通安全計畫審查	Appendix A.4.3
5. 文件控制及紀錄保存	Appendix A.5