核能電廠關鍵數位資產資通安全計畫審查導則

中華民國 104 年 6 月 17 日行政院原子能委員會
會技字第 1040016956 號令訂定發布

中華民國 112 年 12 月 22 日核能安全委員會
核應字第 11200194571 號令修正 1.1 依據、1.5 專有名詞，並自即日生效

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。第二章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。