

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.