**C regulatory position**

**C.1 一般規定**

RG 5.71 「核能設施資通安全程序」(Cyber Security Programs for Nuclear Facility)提供核電廠工作人員一個保護數位電腦、通訊系統和網路所遵守的規定。

**C.2 計畫核心項目**

* 確保下列相關功能的電腦、通訊、網路系統受到保護免於資通攻擊
  + 與安全相關與對安全性重要的功能
  + 安全功能
  + 應變整備功能(包括離線通訊)
  + 如果受到牽連將對SSEP功能產生不良影響的支援系統與裝備
* 持照者如何保護電腦、通訊、網路系統，免於下列方式的資通攻擊
  + 對資料或軟體的完整性或機敏性產生不良影響
  + 禁制對系統、服務、或資料的使用(存取)，系統、服務、或資料產生不良影響
* 對系統、網路、與有關裝備之操作有不良影響
* 辨識關鍵數位資產(CDA)的方法
* 持照者如何建立、實施、維護資通安全程序
* 持照者如何將資通安全程序整合於實體保安程序中
* 安全管控措施應用
* 縱深防禦策略如何應用於資通攻擊中保護、偵測、反應、回復系統
* 減緩資通攻擊不良影響之資通安全程序項目
* 如何設計資通安全程序以確保數位資產的功能不受資通攻擊的不良影響
* 資通安全感知與訓練計畫提供必要的任務訓練
* 持照者評估與管理資通安全風險的流程
* 廠區組態管理管控措施
* 設計管控流程確保
  + 電廠資產修改與新增裝備不會對資通安全產生不良影響
  + 系統設計週期中提出通資安全議題
  + 對安全系統的設計與開發流程提供額外指導
* 特定廠區條件如何影響資通安全實施
* 資通攻擊事件反映與復原之評量
  + 保持資通攻擊的即時偵測與反應能力
  + 減輕資通攻擊後果
  + 改正已發現的弱點
  + 恢復被資通攻擊的系統、網路、裝備
* 實施資通安全計畫之特定資通安全政策與流程(廠區能夠運作、 可受NRC檢驗)
* 資通安全程序成為實體安全程序的一部分接受審查，包括定期受檢
* 持照者管理所有紀錄與支持建立技術文件

**C.3 建立與實施資通安全程序**

10 CFR 73.54建立一個全方位效能基底需求確保數位電腦及通訊與網路系統的功能免於資通攻擊。遵守這些規定的方法就是實施與維護資通安全程序，內含C.3.2.1所描述之防護架構與C.3.3所描述之安全管控措施。

如10 CFR 73.54(b)(2)與10 CFR 73.55(b)(8)所要求，核電廠持照者必須建立、實施、及維護資通安全程序，以保護與SSEP功能相關或支持此一系統的任何數位系統、網路、獲通訊系統。C.3與C.4節描述一個可接受的方法用來建立、實施、及維護資通安全程序，以符合規定。圖1展示建立、實施、及維護資通安全程序的流程。



圖1安全生命週期流程

在一個廠域建立資通安全程序的步驟如下

1. 分析數位電腦及通訊與網路系統
2. 執行關鍵數位資產(CDA)審查
3. 佈署防護架構
4. 對CDA的可能資通威脅描述
5. 實施安全生命週期活動

**C.3.1 分析數位電腦系統與網路**

依據10 CFR 73.54(b)(1)需求，執行特定廠區電腦與通訊系統及網路分析以辨識出關鍵數位資產(CDA)，這些資產可能對核能設施的安全與應變整備(SSEP)功能產生不良影響，或牽連危及。辨識CDA並與以文件化的可行方法如下：

* 獲得安全評估授權
* 定義資通人員角色與責任，並組成資通安全小組
* 辨識與記錄設施的CDA
* 審查與確認CDA組態

**C.3.1.1安全評估與授權**

實施資通安全程序的首要步驟，由單位指派人員與資源，組織及建立權責人員，獲得委任以發展、傳播、審查(年度)、及更新下列文件；

* 一個正式、文件化的安全評估與授權政策，定義與描繪出目的、範圍、角色、責任、管理委任、持照部門間協調、及實施本文件附錄B與C描述的安全管控措施
* 一個正式、文件化的安全評估實施流程

**C.3.1.2定義CST角色、責任、及組成**

持照者可以組成一個資通安全小組(Cyber security team; 簡稱CST)，定義資通安全小組的角色、責任、職權、功能關聯性，以確保組織各階層單位與個人(包括職員、下包合約商、臨時雇員、訪問學者、與廠商代表)都了解此一小組。CST成員應包含以下四種類型人員

* 資通安全程序推動者：可對推動資通安全程序負全責與可提供計畫推動必要資源之管理高層。
* 資通安全程序管理者，負責工作如下
  + 監督通資安全運作
  + 資通安全相關事務之聯絡窗口
  + 提供有關資通安全事務管理與指導
  + 啟動與協調資通安全事件反應小組(CSIRT)功能
  + 資通安全事件期間或後續，與NRC, DHS, 能源部, FBI間協調
  + 資通安全計畫、政策、與流程建立與實施之監督與核訂
  + 確保與核訂資通安全教育、認知、與訓練活動
* 資通安全技術人員，負責工作如下
  + 保護CDA免受資通攻擊
  + 設定、操作、維護資通安全裝備
  + 了解電廠整體架構下之資通安全面向
    - 網路作業系統、硬體平台、軟體平台、作業系統；電廠特定應用程式、及其相關的服務與通訊協定
  + 執行數位系統的資通安全評估
  + 執行針對CDA之安全稽核、弱點評估、網路掃描、穿透測試
  + 保存資通安全調查鑑識證據已避免損失證據價值
  + 保持資通安全領域之專家技能與知識
  + 擔任資通安全事件反應小組(CSIRT)主任或組長，CSIRT小組成員包括單位之安全、營運、工程應變整備人員，其負責工作如下
    - 啟動當CDA遭受已知或懷疑的安全事件之反應行動，並協助受牽連系統之復原
    - 抑制與緩和CDA之資通事件，並確保受牽連之系統適當地復原
* 輔助工作人員，包括操作、維護、或設計數位系統之作業人員、工程師、技術人員、使用者、合約商、銷售代表…等。

CST組成人員之知識領域涵蓋如下

* 資訊與數位系統技術
  + 資通安全、軟體開發、外部通訊、電腦系統管理、電腦工程、與電腦網路
  + 數位系統知識包含電廠運作，如數位儀控系統與電廠資訊系統
    - 電廠運作系統包含可程式邏輯控制器，控制系統、分散式控制系統
    - 資訊系統包含電腦系統、CDA設計、運作、維護之資料庫
  + 電廠內部及對外之網路
* 核能設施運作、工程、及安全
  + 包含整體設施營運與電廠技術規格
  + 人員必須能夠向外沿電廠系統與子系統追蹤CDA弱點(相連數位資產的弱點)，以便能評估電廠之安全與應變整備功能所受到的不良影響
* 實體安全與應變整備
  + 包含廠區實體安全，及應變整備系統與程序

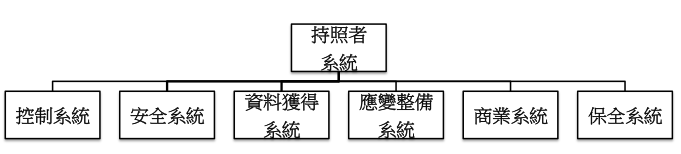
CST的角色與責任如下

* 執行或監督資通安全與管理流程每個階段
* 在評估過程中，記錄重要的觀察、分析、與發現，以便運用這些記錄資訊作為應用安全管控措施的依據
* 評估資通攻擊之威脅、弱點及後果；評估現有資通安全管控措施、防護策略、減緩攻擊方法、認知與訓練活動之效益
* 確認在CDA與相連數位資產及相關安全管控措施之現場查驗過程中資訊蒐集，包括實體與電子驗證活動中現場檢查
* 新資通管控措施的發掘與實施
* 備便文件與監督資通安全管控措施實施，記錄無法實施安全管控措施的依據，記錄安全管控措施替代或補償方法的依據
* 依據10 CFR 73.54(h)與本文件C.5規定，確認保存所有評估文件，包括筆記與支援資訊

**C.3.1.3 關鍵數位資產辨識**

持照者所要保護的資產為關鍵數位資產(Critical Digital Assets, CDA)，如果沒有對設備中的系統做廣泛的評估，CDA的辨識工作是相對困難的。一個核能電廠包含數以百計的系統以支持整體運作與安全性，與SSEP功能相關的系統受到連累，可能造成嚴重輻射災害，持照者精確地辨識與SSEP功能相關的系統是建立有效資通安全程序(Cyber Security Program)的首要工作，運用這些系統資訊，持照者才能經由資通安全程序保護相關裝備。

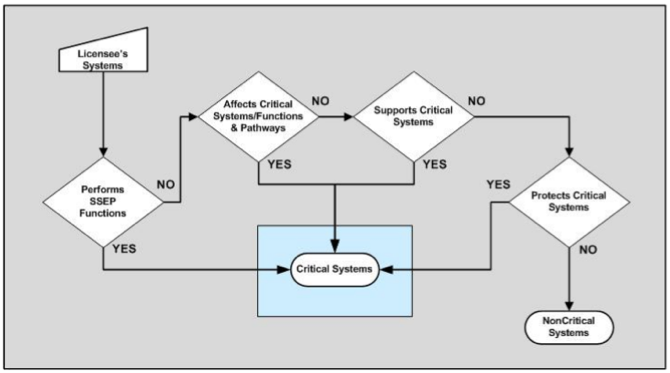
核電廠系統的分類如下圖；



辨識與SSEP功能相關之電廠系統、裝備、通訊系統、及網路，或支援系統的分佈與組織，根據上述基礎找出的系統稱為關鍵系統 (Critical Systems, CSs)，依據是否受到數位控制，可決定納入或排除於資通安全程序範圍，持照者先進行初步後果分析，以決定哪些系統(包含受牽連的系統)將影響核能設備的SSEP功能。

對於沒有直接影響SSEP功能的支援系統或裝備，持照者應執行相依性分析，是否這些受牽連的系統或裝備對SSEP功能有不良影響。關鍵系統包括(1)執行SSEP功能或SSEP功能賴以之系統，(2)影響SSEP功能或影響執行SSEP的CSs與CDAs，(3)針對CSs與CDA，攻擊、減損SSEP功能的路徑，(4)支援CS與CDA。

決定關鍵系統的評估流程如下圖；

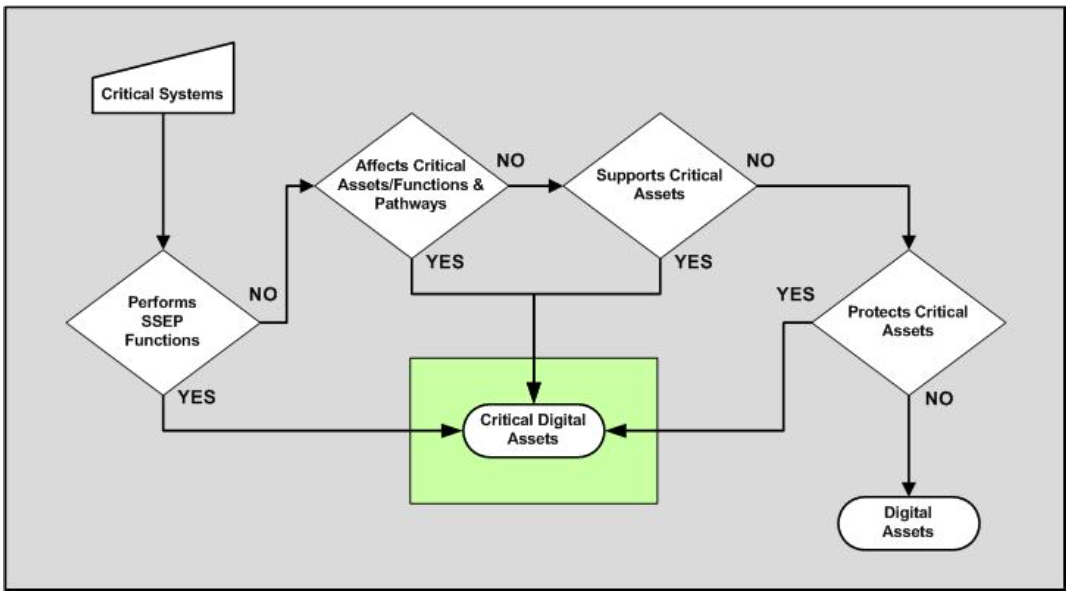


CDA可能是CS的一個組件，以保護CS不受資通攻擊，或可能直接或間接連接到一個CS，直接連結可包含有線或無線的通路(包括一些串連方式)，間接連結包含 “air-gapped” 系統, CDAs 在一個單項安全邊界裝置之後，或 “sneaker nets”，其資料或軟體是以人工方式由一個數位裝置送到另一個裝置，並且使用實體媒介傳輸，如軟碟、拇指碟、可攜式硬碟、或其他模式的資料傳輸。以下的資料來源有助於辨識CSs與CDAs，包括全安分析最終報告、場域特定機率風險評估、技術規格、及有關維護規定程序(Maintenance Rule Program)之文件(10 CFR 50.65所提出的需求)。

CDA包含下列數位資產

* 執行SSEP功能
* 可能對SSEP功能或執行SSEP功能的CSs或CDAs有不良影響
* 提供一條可能連累、減損、攻擊SSEP功能的路徑
* 支援CSs及/或CDAs
* 保護上述相關數位資產(包含DBT)不受資通攻擊

辨識關鍵數位資產的評估流程如下圖



在核電廠有一些CDAs及系統可能是自主性的或單獨的系統(亦即與其他系統無資料連結)，缺乏與其他電廠系統連結將增強自主性CDAs與系統或網路的資通安全狀態，缺乏連結性降低遭受源於電廠外部的資通威脅連累的可能性，然而，這些系統仍具有受到來自內部威脅源的脆弱性，如插入系統媒介具有惡意程式，診斷系統、或其他離線連結及存取，此外，由於支援通訊技術的商品化周邊裝置，當通訊裝備故意或不經意導入系統時，自主系統的架構將遭受改變，10 CFR 73.54未區分自主或非自主系統，故持照者應小心謹慎地保護自主系統的安全狀態。

持照者應保護一各自主系統的安全態勢，與互連系統有相同的努力。為要記錄辨識過程的結果，持照者應蒐集以下資訊

* 對於每個辨識為CDAs與CS的系統、資產、或網路的一般描述
* 每個CDA與CS功能的摘要描述
* 描述CS與SSEP功能因CDA或CS受損的潛在後果的分析
* CDA的功能（如防護、控制、監督、回報、或通訊）
* 每個CS中CDA的辨識
* 下列安全功能需求與規範
  + 開發與評估相關的確保需求
  + 對於銷售商與開發商維護採購系統完整性的資訊安全需求

本文件附錄3.1.3節提供持照者一個範例，用於建立資通安全計畫中的CDA辨識。

**C.3.1.4 審查與確認**

審查的目的在審查與確認每個CDA的直接與間接的連接性，及找出連結路徑。持照者可利用這個資訊在審查的下一階段確認(1)CDA部屬在正確的安全架構階層(2)對CDA潛在的資通安全風險(3)變動管制程序中每個CDA的基準組態。

執行審查與確認的可接受的方法包括下列活動

* 辨識與記錄每個CDA的實體與邏輯位置
* 辨識與記錄每個CDA直接與間接連接路徑
* 辨識與記錄基礎架構下CDA相依性
* 辨識與評估任何安全管控措施的效益及防護架構中CDA的位置
* 持照者確認系統實體與電氣調查的資訊。確認過程包括下列活動：
  + 執行每個CDA的組態的實體調查，包括追蹤進出CDA的所有的通訊連接至所有通訊路徑中的每個終端點
  + 檢查防護每個CDA及其通訊路徑的實體安全
  + 檢查與存取沿通訊路徑的安全管控組態與效益（如防火牆，入侵偵測系統，資料通道閘）
  + 檢查CDA與CS間的相依性，及CDA與CS間信任關係
  + 檢查基礎架構支援系統間相依性，強調電力、環境控制、及滅火裝置受損連累
  + 解決審查中發現資訊或組態不一致，包括出現未文件化或遺失的連結，以及其他與CDA與CS間資通安全相關的不正常