

行政院原子能委員會
委託研究計畫研究報告

數位網路安全弱點防護研究
A Study on Vulnerabilities of Digital Networks

計畫編號：962001INER007

受委託機關(構)：長庚大學

計畫主持人：廖耕億

核研所參與人員：鄭宗杰

聯絡電話：(03)2118800 ext.5852

E-mail address：gyliao@mail.cgu.edu.tw

報告日期：96.11.30

中文摘要

為了增強擴充性與互通性，近來核電廠的數位網路系統紛紛採用具有開放性與標準化的產品，導致了攻擊者可以透過標準化的工具以及增多的管道進行入侵攻擊。因此，研究報告開始針對核電廠的數位網路進行安全檢驗並提出安全指引，希望能夠藉此提高核電廠的安全防護，以減少相關的弱點。

為了瞭解核電廠數位網路的可能弱點，本研究採用BS7799安全管理標準，針對兩份具有權威性的弱點檢測相關研究報告，進行比較分析。比較結果發現，目前核電廠數位網路弱點的防護，已經涵蓋了政策面、組織面、作業面許多議題，不過資產管理與持續營運，似乎還沒有受到廣泛的注意。

除了歸納出核電廠的安全防護議題之外，本研究還針對核電廠內部所用的網路協定進行改良研究。由於核四廠將使用Modbus協定作為控制網路的協定之一，然而Modbus協定在設計之初並未納入安全考量，因此本研究引用密碼學的雜湊函數，設計一個安全協定，讓遠端被控制裝置可以驗證Master的身份。即使遠端設備在無人看管的情況下，本研究所提出的協定仍可以避免遠端設備因接受偽造指令而錯誤運作的機會。預期這個協定將可以增加安全性，而且遠端設備的儲存空間與計算成本的增加相當有限。