

行政院原子能委員會
委託研究計畫研究報告

數位儀控系統多樣性與深度防禦
電廠模擬研究

Simulation Study in Digital I&C Redundancy and Defense-in-Depth
Design

計畫編號：972001INER006

受委託機關（構）：國立清華大學工程與系統科學系

計畫主持人：施純寬

核研所參與人員：黃揮文

聯絡電話：03-4711400 Ext. 6352

E-mail address：hwhwang@iner.gov.tw

報告日期：中華民國九十七年十一月十六日

中文摘要

本研究計畫的成立是為了支援原能會執行核四建廠安全管制之施政目標。核能電廠的數位儀控設計的設備，可使核能電廠的系統更容易操控，且設定值無漂移問題而易於維持。然而，儀控系統數位化亦可能產生新的失效模式，而影響核能電廠安全所依賴的「多重性(Redundancy)」與「多樣性與深度防禦(Diversity and Defense in Depth)」設計的特性。

因此，法規要求應進行深度防禦能力分析，以瞭解核能電廠是否有足夠的深度防禦能力面對殘存的軟體設計缺失。本研究將藉著二項重要工作，(1) 電廠模擬程式爐心點動態模式初步基本研究，(2) 電廠模擬程式擴充飼水控制系統與多樣性與深度防禦應用。研究成果預期將協助分析人員瞭解事故之過程，建立分析數位儀控系統深度防禦之潛在設計弱點，藉以降低數位儀控系統失效事故之可能性，有助於提升數位儀控系統之安全性，並可支援原能會核電廠數位儀控系統審查管制工作。