

行政院原子能委員會
委託研究計畫研究報告

數位儀控軟體故障植入測試平台電廠模式模擬研究

Simulation Study of Digital I&C Fault Injection on Testing Plant Models

計畫編號：982001INER003

受委託機關（構）：國立清華大學核子工程研究所

計畫主持人：施純寬

核研所聯絡人員：黃揮文

聯絡電話：03-4711400 Ext. 6352

E-mail address：hwhwang@iner.gov.tw

報告日期：中華民國九十八年 十 月 二十九 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。本計畫將藉著二項重要工作，(1)擴充 PCTTRAN-ABWR 預期暫態未急停系統，包括替代性控制插棒系統(Alternative Rod Insertion, ARI)、微調控制驅動插棒系統(Fine Motion Control Rod Drive Run-in, FMCRD Run-in)與備用硼液控制系統(Standby Liquid Control system, SLCS)，依照 FSAR 第十五章第 E 節所描述之各個設定值作設定並模擬預期暫態未急停事故，使 PCTTRAN-ABWR 分析預期暫態未急停事故的功能更加完備。(2)將擴充完備的 PCTTRAN-ABWR 電廠模擬程式植入到預期暫態未急停緩抑設施硬體建置架構，模擬 FSAR 第十五章第 E 節的事故並作暫態分析，確立電廠的多樣性與深度防禦。本計畫所模擬的事故包括主蒸汽隔離閥關閉事故、喪失廠外電源事故、主蒸汽管路斷管事故與飼水管路斷管事故等，並與核四廠最終分析報告比較討論。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。

關鍵字：PCTTRAN-ABWR、多重性、多樣性與深度防禦