行政院原子能委員會
委託研究計畫研究報告

數位儀控系統深度防禦能力模擬研究

計畫編號：952001INER005

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

所內共同主持人：黃揮文

報告日期：中華民國九十五年十二月十五日

中文摘要

本計畫為因應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」與「深度防禦」設計的特性，特此進行擴充改善相關分析軟體。多重性可因軟體共因故障而失效，軟體的高度複雜性則可能潛藏能中斷或繞道深度防禦設計功能的路徑。因此對於新的儀控數位化核能電廠設計，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。深度防禦分析方法中，核能電廠數位儀控系統之電腦程式模擬為其中重要項目。藉著模擬各種深度防禦失效案例可協助研究人員瞭解事故之過程，亦可推演各種失效的可能性以尋找殘存設計弱點。本次計畫研究的對象為核四廠版本 PCTRAN-ABWR 程式，針對緊急爐心冷卻系統(ECCS) 大幅修改，增進程式模擬的多樣性及能力，並在保持原有程式架構前提下擴建系統功能。緊急爐心冷卻系統(ECCS)包括三個子系統—反應爐爐心隔離冷卻系統(RCIC)、高壓爐心灌水系統(HPCF)、及餘熱移除系統(RHR)。改進內容包括 (1)擴充三個完全獨立分區之緊急爐心冷卻系統(ECCS)設備 (2) 擴充緊急爐心冷卻系統(ECCS)多種運轉模式之運轉與連鎖(Interlock)邏輯 (3) 釐清緊急爐心冷卻系統(ECCS)取水量、注水量及熱焓改變量對於圍阻體乾/溼井、反應爐之影響 (4)改進緊急爐心冷卻系統(ECCS)流程壓降模式 (5)改進餘熱移除系統(RHR)系統熱交換器模式。改進後之系統模式驗證工作以廠家設

計資料[1]與 LOCA 事故分析報告[2]為基礎，藉由數個核電廠事故案例驗證流程流量與壓降計算模式、熱交換器模組運算模式及動作邏輯；此外事故探討上，本研究報告更深入地討論因不同分區電源失效所造成 ECCS 系統失效對於喪失全部飼水事故的影響，此平行展開與縱深探討之角度也可作為未來事故分析的示範。同時，為使本程式之深度防禦之模擬能力更加強化，已著手發展替代性控制棒插棒系統（Alternate Rod Insertion，ARI）以及微調控制棒驅動系統（Fine Motion Cortrol Rod Drive Run-in，FMCRD Run-in）等緊急插棒模式，在本研究報告中亦有簡單說明與成果的初步介紹。

ABSTRACT

Modern Instrumentation and Control (I&C) Systems of Nuclear Power Plant (NPP) are moving into complete digitalization. However, digitalization for I&C could induce new failure modes, and impact the diversity and defense-in-depth （D^3） design characteristic which nuclear power plants rely on. The redundancy characteristic can be defeated by software common mode failure. The complexity of software could possess some paths which can interrupt or bypass defense-in-depth design. Therefore, the regulation requests that the new digitalized I&C NPP designs shall be performed defense-in-depth analysis to understand whether the defense-in-depth design is capable to resist the software design defects. In various defense-in-depth analysis methods, computer simulation for digital I&C systems of NPP is a crucial item. By simulating various case studies for defense-in-depth failure, the research people can understand and realize the event sequence, and can also derive various possible events to search the residual design vulnerability. We focus on the improvements and modifications of the Emergency Core Cooling system(ECCS) of the PCTran-ABWR. Basing on the original structure, we modify three subsystems of the ECCS system, which includes of Reactor Core Isolation Cooling System（RCIC）, High Pressure Core Flooder System（HPCF） and Residual Heat Removal System（RHR）. The approaches are as followings:

(1) Three indepandant divisions of ECCS are builded.

(2) The essential operation modes and interlock logics are builded.

(3) The Thermal-Hydraulic relationships among the ECCS, the reactor core model and the containment are clarified.

(4) The process flow models for ECCS are improved.

(5) The heat exchanger of RHR is improved.

The data like the process flow diagrams[1] and the LOCA Analysis[2] of GE are utilized as benchmarks for the modified simulation of the ECCS system. The advanced discussions, like the failure of the ECCS by division, on the case of loss of all feedwater flow can be an example of extended analysis in the future. By the way, the Alternate Rod Insertion（ARI）and Fine Motion Cortrol Rod Drive Run-in（FMCRD Run-in）are also developed to reinforce the abilities of PCTRAN-ABWR. Some brief introductions and basic efforts are also included in this report.