複合系統安全驗證技術發展與應用

Development and Application of Safety Verification Techniques for Hybrid Systems

易俗	游原昌	李朝河	王立莘
核能研究所	核能科技協進會	核能研究所	核能研究所
syih@iner.gov.tw	ycyu@iner.gov.tw	clee@.iner.gov.tw	lhwang2@iner.gov.tw

摘要

複合系統是指一系統中同時包含在連續領域中依物理定律動態變化的程序、組件，以及含在離散領域中以狀態轉變方式變化的程序、組件。兩者個別存在時其行為所遵循的變化規則各不相同，在整合成複合系統後經由交互作用常會呈現原各別獨立時不具有的浮現性質。針對個別系統，工程師已發展出成熟有效的分析驗證方法可以驗證所設計產品是否符合需求，但對混合兩種特性的複合系統目前尚無完整的方法可以分析子系統間互動形成的複雜現象。 本項研究的目的是為發展有效分析複合系統行為的技術與工具，使用事故序列模擬方式以驗證複合系統之安全性。

ABSTRACT

Hybrid Systems are systems composed of both dynamical continuous processes and discrete, state transition processes. A typical example is the computer controlled petrochemical plant .The petrochemical processes (i.e., temperature, pressure changes, etc) are dynamical continual evolving processes, while the software part of the controller is a discrete device that exhibits discrete state transition behavior. Mature mathematical analysis techniques have been developed for these two areas individually. However, when combining two into an integrated system, emergent properties come form closed interaction may appear, which cannot be observed when each system is considered independently. Moreover, currently there is few studies in the analysis and verification techniques for these emergent proportions. In recent years, many safety critical applications have adopted computer control techniques for improving their operation flexibility and efficiency. Such application domains include aviation, nuclear power plant, and medical devices, etc. There are also related accidents reports indicating poor interfacing design is the major root cause of these accidents. The purpose of this paper is to present a simulation based approach to verify the safety of Hybrid Systems.

關鍵詞：複合系統（Hybrid System），安全驗證（Safety Verification），事故序列模擬（Accident Sequence Simulation），競爭過程（Competing Processes）。

1、前言

「複合系統(Hybrid Systems)」[5]的定義是指一系統中同時包含在連續領域（Continuous domain）中依物理定律動態變化的程序（process）、組件，以及含在離散領域（Discrete domain）中以狀態轉變方式變化的程序、組件。例如一個由電腦控制的石化工廠，工廠中的化學物理（溫度、壓力變化）反應為一連續動態變化過程，負責調控化學程序的電腦軟體本質上則為一離散結構的狀態集合，依程式設計邏輯在不同狀態間轉換。兩者個別存在時其行為所遵循的變化規則各不相同，在複合系統內整合後經由交互作用常會呈現原各別獨立時不具有的「浮現性質（Emergent Property）」，因此對這兩種情形所用的分析驗證數學技巧也不相同。針對個別系統工程師已發展出成熟有效的分析驗證方法可以驗證所設計產品是否符合需求，但對混合兩種特性的系統尚無一統一的方法分析複合系統的行為，目前則仍靠經驗法則、Ad hoc 或試誤的式予以驗證，如何針對複合系統的整體行為發展有效的分析驗證方法仍是目前此領域待突破的研究課題。

由於計算機軟硬體技術的快速進步，近年來許多安全關鍵應用領域，例如核電廠、高速鐵路、飛航自動駕駛及導引等，均已廣泛的應用計算機設備與技術，這些具有離散結構特質的組件與原有具連續動態特質的程序、設備及人員間構成一複雜的複合系統。從安全的角度來看，我們必須確認此一系統在運作過程中永遠不會進入危險狀態，靠 Ad hoc、試誤的做法，不能對此提供令人安心的保證，因此需要發展較嚴謹周詳的驗證方法，以確保此類系統的安全性。以核電廠安全為例，核電廠為一對安全性要求極高的複雜設施，為保障核電廠安全基本原則是採用「保守設計」及「深度防禦」。保守設計即採用較高的安全系數，例如經分析計算需要 1 寸鋼筋，則實際用 2 或 3 寸鋼筋，即為保守設計，深度防禦則是為預防設備因故障而影響正常功能，相關設備採重複佈置或以多種不同的設計達成相同的功能，如遇單一零組件故障甚至單一系統設計缺失仍能維持整體的安全。但此種深度防禦設計結構經常包含性質不同的元件，例如類比控制系統、數位控制系統、互鎖系統、操作人員等，亦即形成一典型的「複合系統」，增加了驗證其安全特性的複雜度與困難度。核研所目前正針對核電廠複雜的深度防禦系統發展有效的複合系統安全驗證技術，本文目的即為報告本研究初步工作成果。本文第二節說明複合系統的定義及特性，第三節說明複合系統安全驗證原則，第四節說明核研所發展之複合系統模擬環境，第五節說明初步模擬結果，第六節為結論及未來發展。

2、複合系統的定義及特性

複合系統的組成分子包含

1.**依物理定律特性以連續方式變化的程序（process）或組件（component）**

2.**依邏輯規則特性以離散直接轉換方式變化的程序或組件**

複合系統的整體行為表現則依所包含程序組件本性及相互之間互動所構成。互動時對所產生個別系統單獨存在時不具有的新性質，稱之為浮現性質（Emergent Property）。

汽車駕駛手排檔速度控制就是一個典型的複合系統，引擎內的燃燒過程、活塞、飛輪運動等是依循熱力學、機構學定律運作的

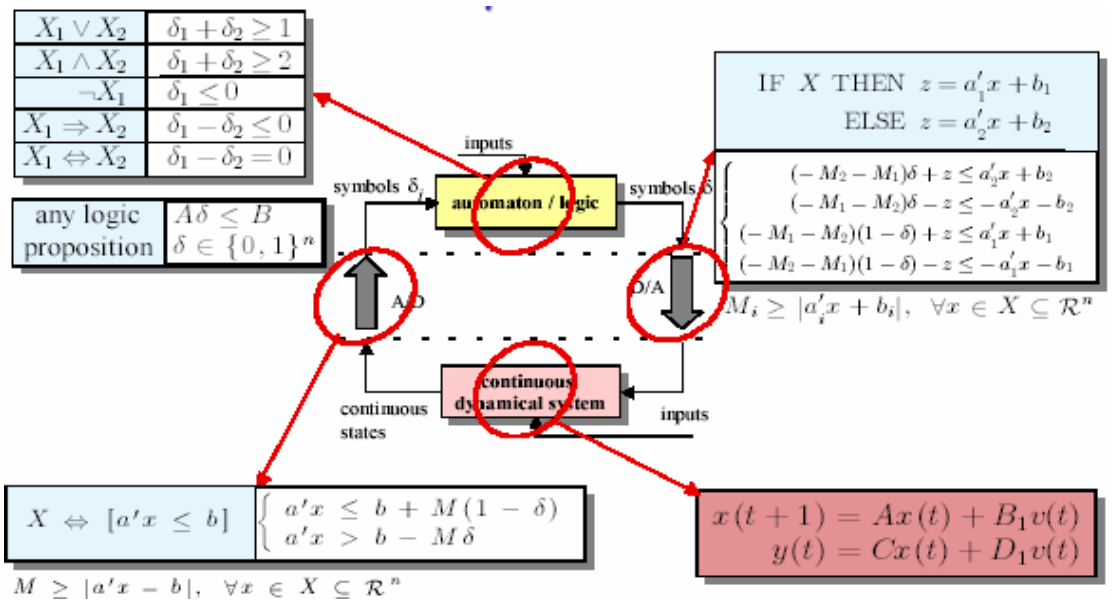
連續變化系統。排檔操作則是在(R, N, 1, 2, 3, 4, 5) 7 個狀態間作分離的轉換，駕駛依照給定的規則操作排檔秩序即能有效的操控汽車。而汽車的有效運作也賴於這兩個連續與離散系統間的協調配合，達到最佳的效率表現。但此一簡單的複合系統仍存有潛在的危險，例如在高速前進中如直接跳換到倒車檔，則可能會對車輛或人員造成重大傷害，因此在設計上應採取互鎖方法防止發生此種情形。

汽車駕控是一單純易於瞭解的系統，近年民航機飛航駕駛採用線控操作（fly by wire）技術，引進功能強大但結構複雜的電腦控制系統，駕駛員須面對各種不同的畫面（Display）及控制模式（Model）作出正確的操控判斷反應，而在複雜的運作規則中不免隱藏危險但未知的動作路徑，駕駛員如未能及時發現並正確處理，就可能造成嚴重事故。在航空事故調查分類中此類事件定義為「模式混淆（Mode Confusion)」問題，例如華航名古屋空難事件中，駕駛員誤以為系統是在手動模式，但實際系統是自動重飛模式，在 Cali 空難事故中駕駛員則誤認飛機畫面數據為機身角度模式，但實際是下降速度模式。因在一個複雜的複合系統設計中如何驗證其運作安全性是工程師的一重大挑戰。

3、核電廠典型深度防禦儀控系統架構

3.1 數學模式

由數學觀點看一個複合系統包含離散有限狀態機及連續動態系統兩種數學結構，兩系統間經由離散與連續信號轉換機制而產生互動作用。目前發展中的數學分析方法有 Piecewise Affine Systems, Complementarily Systems, 及 Mixed Logical Dynamic Systems[3]，圖一為 MLD 分析方法示意圖，其基本概念是將自動狀態機的狀態變換關係（規則）轉換為一組線性不等式，再將此不等式依兩系統間介面關係代入動態系統方程式中，並定義一組限制方程式（Constraint）約束系統的反應。對於結構單純的複合系統可以數學工具如 Mat Lab 求出 MLD 方程式的封閉解答，但對較複雜大規模的實際問題，求解仍是一困難的工作。



圖一：MLD 分析方法示意圖

3.2 安全驗證

安全驗證程序是先定義系統的危險狀態（Hazardous States）集合 H，設複合系統初始狀為

$x_0, S_1 = x_0^1, x_1^1, x_2^1 \cdots x_n^1, S_n \in H$ 表示系統由初始狀態 x_0 最終進到危險狀態的一個事故序列（Accident Sequence），此事故造成的損失是 C_1，此事故序列的發生機率是 P_1，則安全驗證工作內容為有系統的分析與蒐集完整的事故序列 $S_1, S_2, \cdots S_n$，再據對應的損失大小與發生機率高低列成安全表現（Profile），工程師或政府安全主管單位則根據此表資料判定本系統安全為可接受、須修改或判定不安全而禁止使用。

4、複合系統模事故序列模擬環境

基於以數學分析方法驗證安全目前技術尚不可行，因此採用事故序列模擬方式驗證其安全性。複合系統事故序列模擬環境之目標為建立執行核電廠數位儀控系統軟體安全分析與測試相關能力。全數位化核電廠儀控系統之軟體本身因邏輯結構龐大複雜，無法僅以數學分析或測試進行安全驗證，必須藉由建立較簡化但操作便利的模擬工作環境，包括建立核電廠主要核子、熱水力程序，各種設備狀態及功能之模擬環境，然後在此環境下觀察儀控軟體在正常及異常（失誤）下整個系統的反應，做為驗證數位儀控系統安全性能的重要依據。針對特定安全顧慮議題也可在此環境下進行對應的測試工作，以澄清所顧慮之議題。

本項工作平台規格如圖二，為建構於小型區域網路之分散式計算系統。主要模擬設備包括：

1. 物理程序模擬系統（Physical Process Simulation System）

本系統負責模擬核電廠主要物理現象包括：核子反應、中子通量動態變化、熱水力、壓力變化及重要設備（壓力容器、主要管路、泵、馬達等）。本系統軟體採用核儀組由美國 Miorosimulation 公司購入的 PCTRAN 暫態分析軟體並依實際情形作必要的修改。

2. 控制邏輯模擬系統（Control logic Simulation System）

本系統負責模擬核電廠主要儀控系統執行之偵測、控制及保護等功能，此系統之建立方式有二，一是直接應用儀控廠商所發展之完整軟體系統如 Foxboro 之 Foxview, ICC 等，一是以 PCTRAN 原始控制軟體為基礎進行對應的修改或抽換。

3. 操作員監控程序模擬系統（Supervising Process Simulation System）

本系統負責模擬核電廠操作員在運轉過程中所執行之監控程序，包括研判系統狀況並視情形決定採取必要動作以維持電廠安全之過程，此部份之模擬軟體將自行開發，設計參考依據為電廠一般及緊急操作程序書。

4. 模擬作業控制系統（Simulation Control System）

本系統負責上述三項模擬軟體程式之管理協調功能，研究人員透過本系統設定模擬作業之起始條件，設定錯誤狀況，本系統亦負責三項模擬軟體間資料傳輸、通訊記錄、House Keeping 等支援功能。

5. 模擬資料展示系統

由於在一次複雜模擬作業過程中，需引用及產生的數據數量龐大且關聯關係複雜，須完整記錄以支援軟體安全肇因分析作業。

模擬過程中三項主要模擬系統將配置雙 LCD 螢幕，即時輸出模擬計算數據以供分析研判。各 LCD 配置情形如下：

PP-LCD1：展示核電廠主要程序參數動態變化趨勢圖

PP-LCD2：展示核電廠主要程序流程相關設備佈置關係及正常／異常狀況

LP-LCD1：展示控制系統由偵測儀器讀入之各項重要程序參數動態變化圖

LP-LCD2：展示控制系統正在執行之控制邏輯算法（Algorithm）進行中路徑相關資料

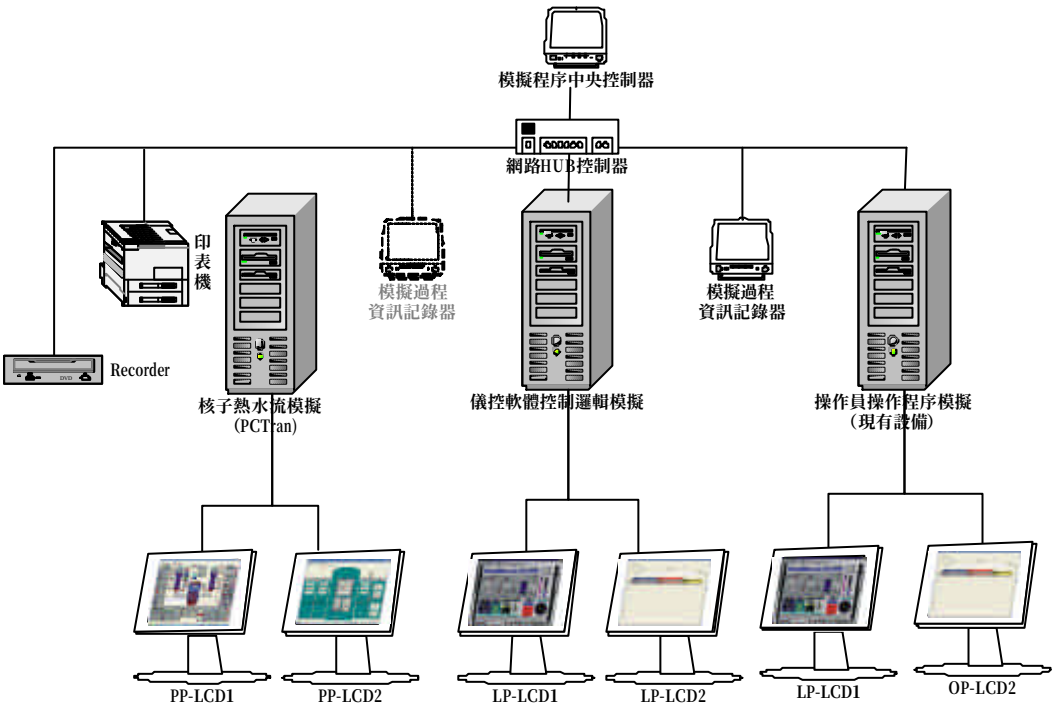
OP-LCD1：展示操作員對正在模擬事件所認知（Perceived）到的電廠狀況，包括操作員認知到的各項程序參數、設備狀況等。

OP-LCD2：展示操作員對正在模擬事件將採取的操作邏輯步驟圖。

對特定複雜個案如所屬展示資訊過多時，另將以機動方式以個別記錄顯示裝置跨接在模擬系統上，以支援模擬輸出之記錄展示。

6. 模擬資料記錄儲存系統

模擬計算將產生大量數據必須保留供進一步比較分析，因此本工作平台並配置高容量 DVD 燒錄器及高速雙面印表機以支援模擬輸出大量資料之記錄保存。

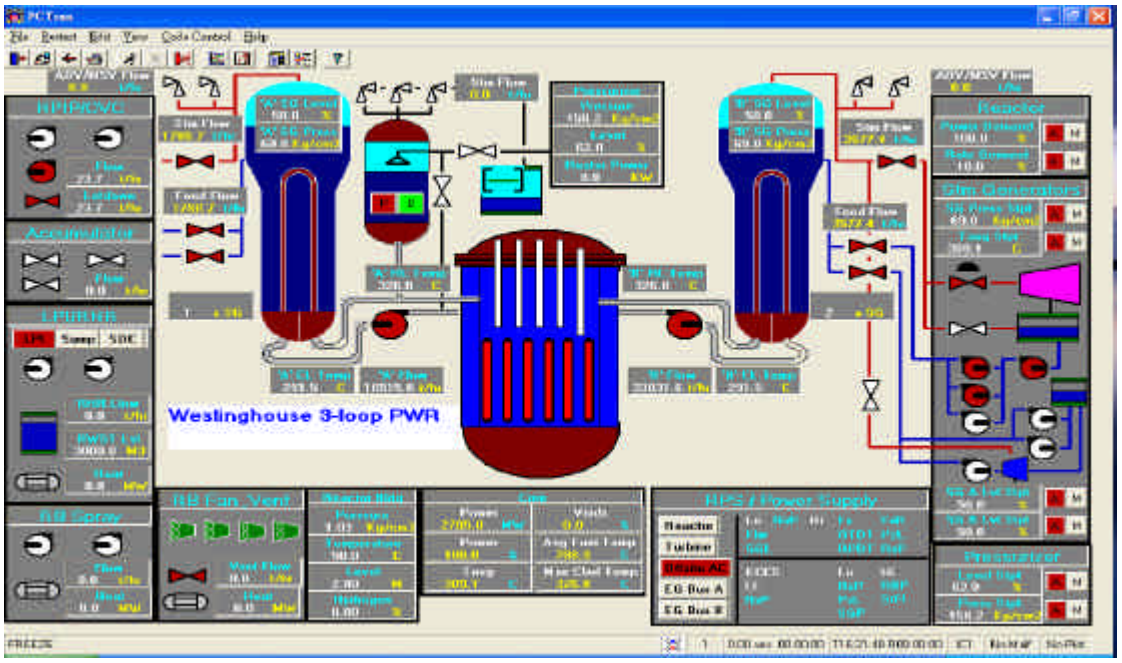


圖二:數位儀控系統故障事件模擬環境

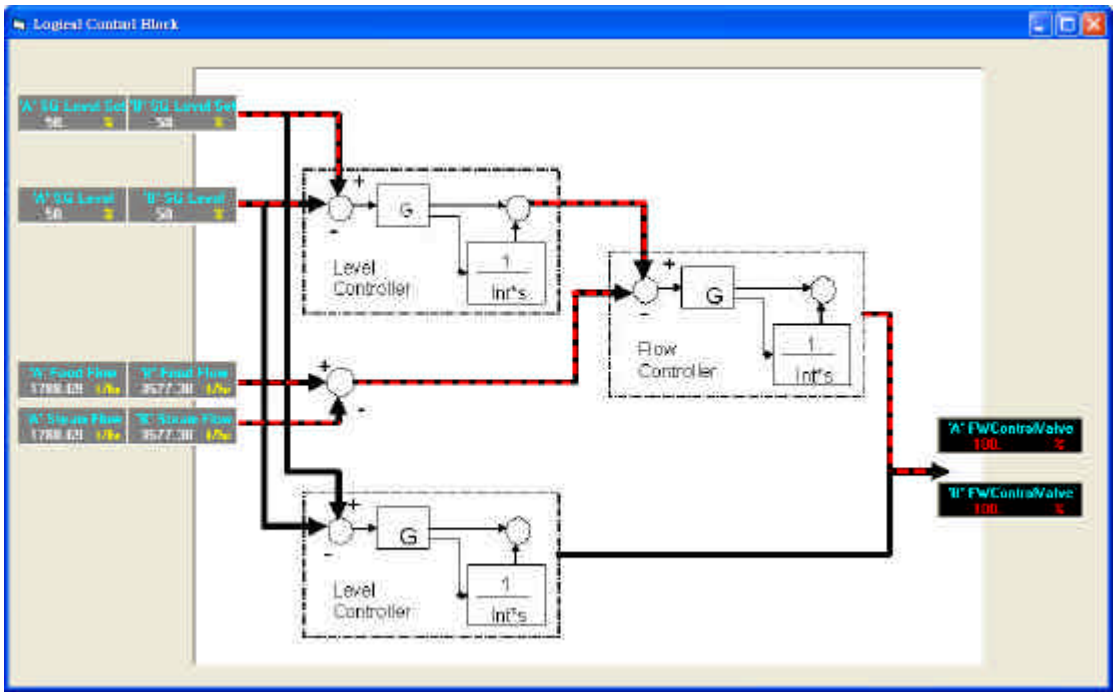
5、複合系統安全驗證 – 競爭過程之模擬

我們在所開發的模擬平台上對複合系統的競爭過程現像作了初步的模擬，競爭過程（Competing Processes）是在複雜的複合系統中常發生的一種浮現性質（Emergent Property），競爭過程發生的主要原因是存在於系統中的眾多計算程序間，某兩個（或兩個以上）的計算程序，各程序為到達目標狀態所

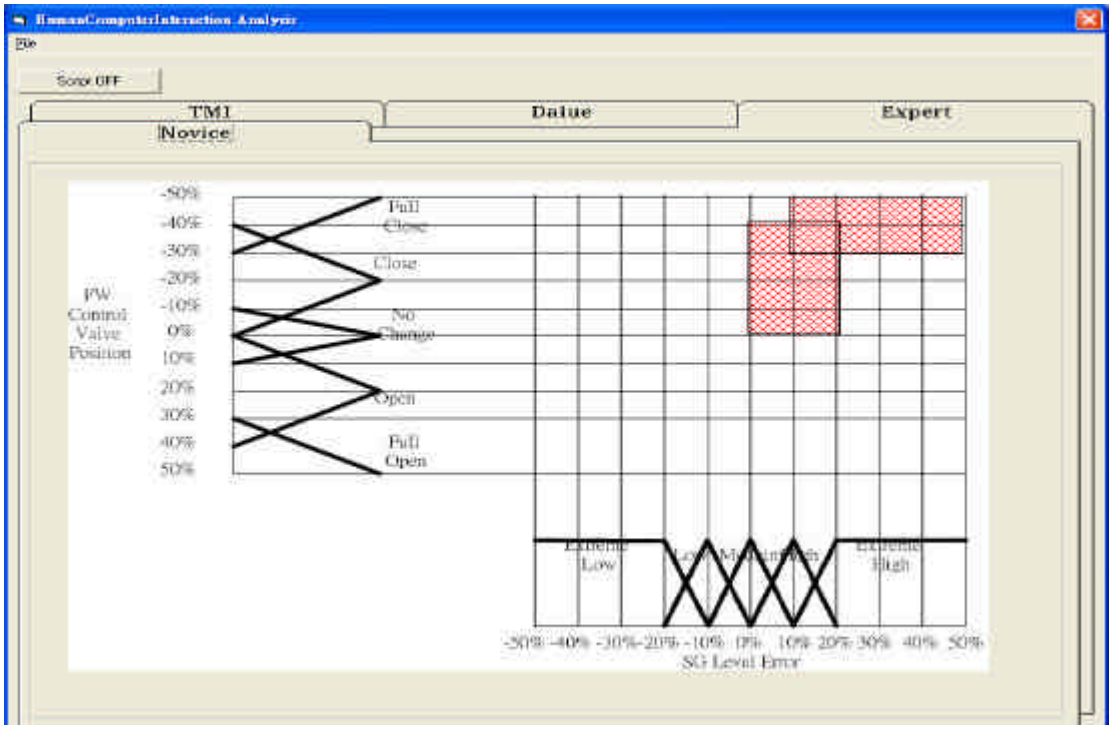
執行的計算指令在程序間相互造成抑制對方的現像。以華航名古屋空難事件為例，自動駕駛設定為重飛模式，駕駛員則執行降落動作，雙方相同時互發出操控方向舵、水平翼的指令，造成飛機機身角度變化過大而致失速墜機。三哩島核電廠事故也是一典型的競爭過程，電廠自動安全系統為防止爐心過熱而啟動救援的緊急高壓補水系統，但操作員誤判爐心為高水位，擔心在高水位情形下再進水會破壞壓力槽，因而將已啟動的高壓補水系統關閉，此一動作正是造成三哩島核電廠發生不可挽回的破壞之關鍵動作。這些都是在複合控制系統中實際發生的競爭過程，因此我們在設計複雜的複合控制系統時為確保其安全性，應有系統的搜尋操作過程中發生競爭程序的可能性，評估成因及影響後果，作必要的設計變更，偵測機制或加強人員訓練，我們所發展複合系統模擬平台提供了執行此項安全驗證的工具。目前已完成核電廠蒸汽產生器水位控制競爭過程現象的模擬。核電廠運轉過程中當蒸汽產生器水位偏低時，自動控制系統會打開進水閥補充水量，使水位回復到安全設定值，由於一般進水水溫遠較蒸汽產生器現有水溫為低，而液態水體積具有熱漲冷縮（Shrink and Swell）效應，當大量溫度較低補水進入溫度較高之蒸汽產生器時，由於熱漲冷縮效應，使蒸汽產生器水位不升反降，當自動控制系統判斷所補充之(冷)水已足夠時，即開始調降進水閥開度，但因前述熱漲冷縮效應致水位指示仍偏低時，操作員從表面數據判斷，為避免發生低水位跳機事件而採取手動控制「調升」進水閥開度，形成操作員與自動控制系統的競爭過程。模擬計算過程及結果如下圖所示。圖三為物理程序模擬系統（Physical Process Simulation System），圖四為控制邏輯模擬系統（Control Logic Simulation System），圖五為操作員監控程序模擬系統（Supervising Process Simulation System）。參考資料（CALVERT CLIFFS 2 - Event Date: 3/17/1986 - LER Number: 93-003）為核電廠實際發生類似事件之報告。



圖三：物理程序模擬系統



圖四：控制邏輯模擬系統



圖五：操作員監控程序模擬系統

6、結論及未來發展

隨著計算機技術應用的日益成熟普及，愈來愈多與人們日常生活相關的設備都引進計算機自動控制，以大幅增加系統的彈性及效能。但是在享受計算機自動控制技術的彈性效益之際，計算機與其所控制、介面的環境、操作人員所形成的複合體系中間也隱藏著表面不易發現的危險程序。文中所提及的飛航、核電廠事件，都是明顯的事例，因此每工程師在繼續開發更多、更複雜的計算機控制系統應用時，也應相對的同時開發複合系統的安全驗證技術，以確保此類系統日後應用時不會威脅使用人的安全。

本文提出以模擬技術對複合系統進行安全驗證的方法，也完成初步模擬環境發展建立，並完成針對核電廠蒸汽產生器水位控制競爭程序之模擬，初步顯示所建立之模擬環境及驗證方法有效可行，未來將針對核電廠分散式安全系統之深度防禦能力繼續發展更完整的安全驗證技術。

7、參考文獻

[1] Eugene Asarin, Thao Dang, and Oded Maler, "A Verification Tool for Hybrid Systems" *Proceeding of the 40th IEEE Conference on Decision and Control*", Orlando, Florida USA, December 2001.

[2] PAUL I.BARTON and CHA KUN LEE, "Modeling, Simulation, Sensitivity Analysis, and Optimization of Hybrid Systems" *ACM Transactions on Modeling and Computer Simulation*, vol. 12, no. 4, pp. 256-289, October 2002.

[3] Alberto Bemporad, "Model Predictive Control of Hybrid Systems" *Automatic Control Laboratory ,Swiss Federal Institute of Technology(ETH)*.

[4] Oded Maler and VERIMAG, "A Unified Approach for Studying Discrete and Continuous Dynamical Systems" *Proceeding of the 37th IEEE Conference on Decision and Control*", Tampa, Florida USA, December 1998.

[5] Oded Maler, CNRS-VERIMAG, and Centre Equation, "Verification Hybrid System" *The European Journal of Control*

[6] Amy R. Pritchertt, Seungman Lee, David Huang, and David Goldsman, "Hybrid-System Simulation for National Airspace System Safety Analysis" *Proceedings of the 2000 Winter Simulation Conference*.