# 行政院國家科學委員會專題研究計畫　期中進度報告

## 混合系統的全符號式自動化分析軟體工具環境(1/3)

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-002-131-
執行期間：91 年 08 月 01 日至 92 年 07 月 31 日
執行單位：國立臺灣大學電機工程學系暨研究所

計畫主持人：王凡

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 92 年 7 月 9 日

# 行政院國家科學委員會專題研究計畫期中報告

## 混合系統的全符號式自動化分析軟體工具環境(1/3)

## Full-Symbol Automatic Analyzed software tool for Hybrid System

: 計畫編號 NSC 91-2213-E-002-131

: 執行期限 91 年 8 月 1 日至 92 年 7 月 31 日

: 主持人 王凡 國立台灣大學電機工程學系暨研究所 副教授

### 一、 中文摘要:

我們藉著國科會三年長期的支持,我們要在根本上探討混合式自動機的自動分析、驗證問題，並進而提出經驗上有效率解決方案。而此一根本，在於資料結構與其配合的演算法。我們也將進一步提升我們的軟體工具的可親近性與功能性，譬如發展功能強大的全符號式模擬器、與視窗圖形介面。在經過一年努力後，已經有了一個雛形可用，並通過數項驗證實驗。

### Abstract

With the three-year support from NSC, we want to invesigate the root of the complexity of the analysis and verification problems of hybrid automata and move to

the development of empirically efficient solutions. The root of the complexity lies with the data-structures and their manipulation algorithms. we shall also enhance the friendliness and functionalities of our verification tools. For example, we shall develop the window GUI and fully symbolic simulators. After almost one year's effort, we now have a usable SGM which has already passed several small benchmarks.

## 二、 計畫原由與目的:

即時系統的自動驗證問題，具有極高的複雜度。依我們的經驗，要提升自動驗證技術，到達工業可用的地步，不只需要在工具功能性上大幅提昇，即使如基本演算法效能，也需要大幅翻新。

目前關於即時系統的自動驗證，有許多理論模型出現，譬如時間自動機（timed automata）[ACD90]與混合式自動機（hybrid automata）[ACHH93,AHH93]。時間自動機可以視爲混合式自動機的一種特例，而其特性可以讓我們設計出較高效率的資料結構與自動驗證演算法。但也因爲此特性的限制，導致許多工程性質、行爲的無法表達。簡言之，這兩種數學模型的差異在於

- 混合式自動機容許稠密性（dense）變數，以任意速率，增減其值。而時間自動機，則只容許速率爲 1。
- 混合式自動機容許任意線性條件的描述，如 x-3y+4w≦7；而時間自動機，則只允許兩個時中間的讀值差，如 x-y＜-3，來被比較。

但是混合式自動機的彈性，卻導致了驗證問題的不可決定性（undecidability）。在這樣嚴峻的挑戰下，只有設計出在經驗下具有良好效能的基本技術，才能發展出能爲工業界接受的混合式自動機自

動驗證、分析工具軟體。

本計畫的目的在於發展新一代、具有工業可用性的即時系統自動驗證分析系統環境。詳言之，可分爲三方面來說。第一，依據我們在 red 3.0 版、與 3.1 版的經驗，我們計畫發展經驗上具有高度效率的混合式自動機基礎自動分析技術，包括了資料結構與計算程序創新。第二，我們計畫針對混合式系統，設計出新的情境分析計算程序，希望能夠提供更豐富多元的系統設計工具。第三，我們計畫提供更易於使用的自動驗證軟體環境，其中含有全符號式的模擬環境、視窗式的使用者介面，並將這套環境推廣到工業界去。

## 三、 研究方法與成果:

由於本實驗室在執行上一 SGM 的國科會三年計畫期間，已經將前置可行性作業分析完成，並有了初步的運作平台，因此本計畫的執行可以節省此一步驟，直接進行理論的修飾、定稿、與程式的製作。

- **混和式系統驗證基本技術的新發展:**

  自動驗證原本就是極其複雜的技術，而混合式自動機的自動驗證又比一般時間自動機更爲複雜，等同於第一階邏輯的 satisfiability 問題。因此在實際運用上，必須設計出在經驗上有卓越上校能的計算程序，才有可能推展到工業應用上去。自從 1993 年，混合式自動機的模型被提出後，目前主要的技術大抵是以線性不等式條件的集合來表達一個凸多面體的狀態空間。至於凹多面體的狀態空間，則可以在此線性不等式條件的冪集合中，進行推理。而此類冪集合的複雜度，可想而知是超出了目前電腦科技

的處理能力。我們針對混合式自動機的狀態空間，提出新的資料結構、與經驗上有效率的計算程序。

- **時間自動機的基本技術的改良再創新:**

  時間自動機是混合式自動機的一個特例。因其特性，容許我們用二爲矩陣來表達其凸多面體的狀態空間。在我們發展 red 3.0 與 3.1 的過程中，我們開發了新的類 BDD 資料結構，並突破了 all-pair shortest-path 的窠臼，創新了處理計算程序的設計，從而獲得了超越前人效能的成果。我們以即時系統的行爲特性，設計出新的資料結構與演算法。

  我們從 red 3.1 的發展經驗上起手，針對時間自動機與混合式自動機，各設計出一種獨特的新資料結構，並進行一連串的實驗，找尋出最佳的資料結構與計算程序的組合。

## 四、 結論與討論:

由於本實驗室計畫內容的不斷擴充，並尋求工業界應用的可能性，有系統發展的管理的困難挑戰，需要我們克服。並且由於同時將有四個版本的新程式在發展階段。而我們預期到了第二、三年，還會有個種不同平台（如 MS Windows）的版本出現，因此這麼多不同版本間的相容性就變得十分重要了。我們計畫要將各個版本間的功能性擴充模組化。不同版本間的修改，也希望留下完整的資料記錄，以備將來不同版本間整合時的需要。

## 五、 參考資料:


**[ABKMPR97]** Asarain, Bozga, Kerbrat, Maler, Pnueli, Rasse.
Data-Structure for the Verification of Timed Automata. In proc. HART'97, LNCS 1201, pp.346-340.

**[ACD90]** R. Alur, C. Courcoubetis, D.L. Dill.
Model Checking for Real-Time Systems, IEEE LICS, 1990.

**[ACHH93]** R. Alur, C.Courcoubetis, T.A. Henzinger, P.-H. Ho.
Hybrid Automata: an Algorithmic Approach to the Specification and Verification of Hybrid Systems. in Proceedings of Workshop on Theory of Hybrid Systems, LNCS 736, Springer-Verlag, 1993.

**[ACH95]** R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine.
The algorithmic analysis of hybrid systems. Theoretical Computer Science, 138:3-34, 1995

**[AH89]** R. Alur, T.A. Henzinger.
A really temporal logic, in Pro. 30th IEEE Symp. Found. of Computer Sciences, pp. 164-169, 1989.

**[AH90]** R. Alur, T.A. Henzinger.
Real-time logics: Complexity and expressiveness, proceeding of IEEE LICS, 1990.

**[Wang95a]** F. Wang.
A Temporal Logic for Real-Time Partial-Ordering with Named Transactions. In Proceedings of Latin American Theoretical Informatics Symposium, Santiago, Chile, April, 1995. LNCS 911, Springer-Verlag.

**[Wang95b]** F. Wang.
Timing Behavior Analysis for Real-Time Systems. IEEE LICS 1995.

**[Wang95c]** F. Wang.
Reachability Analysis at Procedure Level through Timing Coincidence. in Proceedings of the 6th CONCUR, Philadelphia, USA, August 1995, LNCS 962.

**[Wang95d]** F.Wang.
An Experiment on Efficient Real-Time System Verification through Refutation by Positive Cycles. In Proceedings of the 1st RAMS (Real-time And Media Symposium), Taipei, ROC, July, 1995.

**[Wang01a]**F. Wang.
RED: Model-Checker for Timed Automata with Clock-Restriction Diagram.

In proceedings of Workshop on Real-Time Tools, Aalborg University, Denmark, August 20, 2001. Technical Report 2001-014, ISSN 1404-3203, Department of Information Technology, Uppsala University.

**[Wang01b]** F. Wang.
Symbolic Verification of Complex Real-Time Systems with Clock-Restriction Diagram. In proceedings of FORTE 2001(the 21st International Conference on Formal Techniques for Networked and Distributed Systems), Cheju Island, Korea. 25-28 Aug, 2001.