公告本

申請日期	87.6.19
案號	87109859
類別	G06F 9/00

（以上各欄由本局填註）

90年5月29日 修正補充

A4
C4

457453

發明 新型 專利說明書

一、發明新型名稱	中文	無法預測的微處理機或微計算機（90年5月修正）
	英文	Unpredictable Microprocessor Microcomputer
二、發明創作人	姓名	米歇爾優剛（Michel UGON）
	國籍	法國
	住、居所	法國莫瑞巴斯78310狄斯色巴格斯路6號
三、申請人	姓名（名稱）	布爾第八特許公司（Bull CP8）
	國籍	法國
	住、居所（事務所）	法國78430路文西納斯第45號郵政信箱伯薩里斯路68號
	代表人姓名	米契爾可倫貝（Michel COLOMBE）

本案修正後是否變更原實質內容及准予修正。

90.5.29日所提之

經濟部中央標準局員工消費合作社印製

裝 訂 線

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

法國　國（地區）　申請專利，申請日期：　　案號：　　，☑有　□無主張優先權

1997年06月26日 案號 97 07995（主張優先權）

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（ 1 ）

本發明是有關一個無法預測的微處理機或微計算機。

如眾所周知微處理機或微計算機是依照順序執行記錄在記憶裝置內之程式的連續指令，而與一個或數個相對於由其內部或外部提供給微處理機或微計算機的時鐘信號之一的參考韻律信號而同步執行。

此被證實可以知道依據時間的程式執行不同階段，因爲此等指令的執行是按照程式預定的程序依順序進行執行，一般而言，是與時鐘信號同步，此時鐘信號有規律地韻律調節此處理機。事實上，所有的程式是藉由一系列的指令來表達，這些指令應在事先所知曉的順序中連續的被執行。每個指令開始以及結束的時刻是完全知曉的，因爲這些指令是按照時間依據事先預定的程序而執行。因此，可以原則上知道那一個指令在某一時刻執行，則交給處理機的處理裝置去執行，因爲程式的進行是由事先預定一系列的指令所構成。

吾人能夠確定，例如自程式開始所執行指令的數目，處理裝置的啓動，或者還有自從某一事件後所經過的時間，內部或外部的參考信號，或者還有處理機的值回復到 0。

此種可以觀察到程式在一個微處理機或微計算機中進行的可能性，在此微處理機或微計算機在用來作高度機密作業時是一大妨害。事實上，一個不懷好意的人可以如此認出此處理機所處的連續接續的狀態，並利用此等資訊來了解內部處理的某些敏感的結果。

五、發明說明（２）

吾人可以想像，例如依據特定安全作業的結果在不同的時刻，產生一項所給予的行動，例如，內部機密資訊的測試或是一項訊息的解碼，或者還有某些資訊完整性的控制。根據所考慮的時刻，吾人可以，例如，對處理機作些行爲，或者藉由實體的調查以獲得某些暫存器的值，以便得到機密資訊內容或結果的有關資料。並且甚至在計算密碼的情況之下，得到所使用的編碼密鑰的資料。

眾所周知，此等裝置提供微計算機一項重大的改進，它使人安心的是其所配備的電路能產生隨機的時鐘脈衝。以這種方式，如欲調查研究對於事件的觀察是尤其困難，因爲其同步性變得非常難以實行。此種裝置是例如由歐洲專利 EP660562 或其相對應之美國專利案 USP5,404,402 而爲熟知。

然而，此種解決方式呈現許多不便之處：

首先，此等電路的觀念是尤其特別精巧但又枯燥乏味，令人厭煩的，因爲它在如此複雜的微計算機電路的整體，不可能模擬其隨機的功能。而且在其生產完成時，也很困難去測試這些電路混亂的行爲表現。一系列隨機的時鐘脈衝事實上是非常困難去模擬去調整此等電路，但如想要精通掌握此處理機整體邏輯電路之行爲舉止表現，則更加困難，尤其是在其內部匯流排以及暫存器中的信號轉換期間，更是困難。

這說明它爲什麼是一項重大的改進，是由原提案人所提

五、發明說明（3）

的法國專利 07-03-96 的 NO9602903 申請專利範圍的目標，其標題"積體電路之功能，此種積體電路的使用方法"。此被提供用來允許處理機正常的功能，當其用習知的週期性的時鐘來調整及測試之期間。此處理機能夠自己本身在被保護模式或正常模式間轉換。爲了確保安全，吾人可輕易地設想此模式只可能藉由處理機呈現一個口令一或一個專此特設的訊息碼而處於活性狀態。

除了上述的困難之外，當此等序列是在隨機的時鐘控制之下，這即是說，在完全無規則的情況之下，其故障的診斷繼續有效。事實上，在這種混亂無規則的情況之中，我們如何能將此問題歸咎於較弱的一方，並確定在何種確實的情況之下它會出現。

吾人所看到的是隨機時鐘的應用，甚至它提供一個理論上令人感興趣的改進，但它並不提供一個令人完全滿意的解決方案，而且在實際上要容易使用。

此爲本發明的目標之一，爲處理機裝配裝置禁止前面描述方式的探究。並且通常禁止藉由運用對電路規則標準的完全精通而對處理機內部的行爲舉止作違法不正當的觀察。此對電路規則標準的精通是建立在傳統方法的簡單的觀念與缺乏診斷。

此目標的達成是由於無法預測的微處理機或微計算機的事實，它包括一個處理機，一個第一作業記憶體，一個主記憶體其包含一個應用系統，一個主要程式以及一個次要

五、發明說明（4）

程式，其特徵爲其包含

- 一個第二作業記憶體

- 轉換裝置，其允許當在程式執行時，如轉換作業記憶體的使用，朝向兩個作業記憶體中之一個，兩者均可保存其記憶內容。

- 此轉換裝置包含一個主記憶體中程式進展主文記憶暫存器至少一個區段(block)，以及一個切換電路用來使得作業記憶體之一有效，以及與每一個記憶體有關存取暫存器，而它由上述之切換電路來控制。

根據另一個特點，它具有一個第二程式進展主文記憶暫存器之第二區段。

根據另一個特點，它相對於等時性時鐘而言，具有程式進展不相關裝置。

本發明另一個目標是使得使用此等裝置是由處理機本身所保證，以致於由上述等裝置所產生的額外的安全性並不取決於位於微計算機之中的應用系統的決定，因此對於欺詐者而言，是無法預測的。

此目標是藉由此事實而達成，即主程式可以授權或禁止此等轉換機構。其藉由裝載了作業記憶體之有效電路以及與每一個作業記憶體有關之記憶體暫存器區段而達成。

根據另一個特點，此第二作業記憶體以及其存取暫存器，在其被主程式使用時，取代第一作業記憶體以及其特有的存取暫存器。

五、發明說明（ 5 ）

本發明的第三個目標是使得執行時間與程式本身獨立無關，但不因此被強迫使用時脈信號以及隨機記時信號。

此目標可藉由此事實而達成，即此等不相關裝置包含一個隨機變數產生器，其使得能夠由在處理機中程式執行非同步性的隨機中斷之中斷電路來啓動，此是經由第二程式的隨機分支而達成。

根據另一個特點，此等不相關裝置包含一個獨立於處理機 1 的時間計算系統。它可以在時間計算終了啓動一個中斷，而由第二程式回到主程式。

根據另一個特點，此作業記憶體的轉換裝置是由，處理機以及其程式，或是由隨機中斷系統，或是由時間計數器，或是以上三者之中至少兩個之任意組合，所支配控制。

本發明的第 4 個目標是避免暫存器的轉換，不能被理解爲用來直接或間接地接達存取敏感資訊。

此目標可藉由此事實而達成，即此作業記憶體之轉換裝置之成爲有效，是由於處理機執行一序列之主程式，因而載入之內容而使其有效。

根據另一個特點，此第二程式所使用的作業空間與在主記憶體之中主程式所使用的空間相同。

根據另一個特點，此第二程式所使用的作業空間比主程式所使用的作業空間要小很多。

根據另一個特點，此轉換裝置執行替換，用作業記憶體以及相關的上下文，來替代微處理機的指令之執行循環的

五、發明說明（6）

內容。

根據另一個特點，此第二程式並不修改主程式功能之一般性上下文內容，以便可以回到主程式，而無須重建其上下文內容。

根據另一個特點，主程式的上下文內容的重建，是由第2程式自動產生，或是由轉換裝置將控制交還給主程式之前自動產生。

根據另一個特點，它包含替代裝置，用第二程式的記憶來取代主程式的記憶。

根據另一個特點，此主程式可同時或交替式地使用第一作業記憶體及/或第二作業記憶體。

根據另一個特點，此切換電路的載入允許對此等不相關的中斷之遮蔽(mask)或解除遮蔽。

根據另一個特點，回到主程式的命令是被一個中斷指令所執行，此中斷指令是在切換暫存器被適時的載入之後，而由第2程式所啓動，或藉由執行主程式或第2程式的一個指令來啓動，其用來解除中斷的遮蔽。

根據另一個特點，它是在一個單體的積體電路中實現。本發明的其他的特點和優點，可由閱讀以下的描述並參考相關的附圖說明而更加清楚，其中：

第1圖是根據本發明實施例之積體電路之電子示意圖。第2圖是代表當中斷出現時執行指令的瞬時圖解，並將未遮蔽的中斷列入計算。

五、發明說明（7）

第 3 圖是代表積體電路的記憶體暫存器之一的載入電路的一個變化實施例。

第 4 圖是代表程式(P2)之部份之邏輯圖，其允許回到電路之正常功能。

第 1 圖代表本發明的一個實施例。本發明的標的此微處理機或微計算機，稱爲"自已無法預測的微電腦(SUMIC)，是由單一的積體電路所構成，其包括一個處理機(1)，一個不消逝記憶體(6)其包含要執行的程式，一個作業主要記憶體 ram(51)與其位址暫存器(A2)以及資料(D2)以及一個隨機或近似隨機信號產生器(2)，它提供，例如，以不規則且無法預測間隔的脈衝；一個中斷電路(4)，一個暫存器(R2)，一個計時器(R3)，一個電路序列發生器(8)，一個不消逝記憶體(7)(NVM)，一個可消逝式的虛擬記憶體(52)以及其位址暫存器(A3)以及資料暫存器(D3)，兩個堆疊暫存器(54,55)用來記憶回到正常功能的參數，以及一個切換電路(53)山例如一個暫存器構成，其有足夠的數目以用來控制位址暫存器(A1)及(A3)以及資料(D1)及(D3)以及記憶體暫存器之第一區段(54)及第二區段(55)之功能。此切換電路(53)被處理裝置(1)經匯流排(3)而載入。此切換電路(53)的狀態尤其可以使得在處理機作業記憶體空間之內或空間之外的 RAM 及/或 DUMRAM 爲有效。

在此單一的積體電路之內，處理裝置藉由匯流排(3)，連接至不同的記憶體，每次朝向一個各別的位址暫存器

五、發明說明（ 8 ）

(A1,A2,A3)以及一個各別的資料暫存器(D1,D2,D3)。此等位址暫存器以及資料暫存器的每一個，可以被由切換電路(53)出來各別的命令線路(531A,532A,536A)，以及(531D,532D,536D)所構成迴路。

此切換電路也包含其他的三個命令線路其中之一連接端(533)至一個埠 ET(11)及兩個輸入端，其中第二輸入端接受來自中斷電路匯流排(31)的一線。此埠 ET 的輸出端被直接連接至中斷有效暫存器(IER)，(能夠中斷暫存器)內之一位元(bit)，用來使能遮蔽由中斷電路(4)所獨特啓動的中斷，當此切換電路未被啓動，心於活性狀態並且因此線路(533)不處於活性狀態。

另外兩個線路(534,535)與記憶體(54,55)暫存器的兩個區段或堆中之每一個構成迴路。每一區段包含各別是複數個記憶體暫存器(54)或(55)，可以用來儲存以下所描述的資訊。此等暫存器(54,55)被連接至記憶體所共用的匯流排(3)。此相同的匯流排(3)可以允許切換電路(53)被載入所須要的值而使得此等命令線路(531A,532A,532D,536A,536D,533,534,535)根據所希望的功能模式，而處於活性狀態或非活性狀態。此不可消逝記憶體(6)包含電路應用系統(作業系統)，以及一個執行主要程式(P1)由於稱爲主要程式，以及一個第二程式(P2)由於被稱爲第二程式，以及順序產生器(8)，暫存器(R2)，定時器(R3)，以及隨機數產生器(R1)也被連接至匯流排(3)。並且此三元件

五、發明說明（9）

(R1,R2,R3)被連接至一個中斷產生電路(4)，其在處理機(1)之中斷輸入端上切換，其運用位元中之一的處理機中斷遮蔽暫存器，而此等位元是通常被保留用做爲某些使用者特殊用途之備用。

在一個主要的實施例中，此主程式(P1)是被包含在經修改的不消逝記憶體(6)。當須要的時候，藉由匯流排(3)切換電路的狀態，並沒有呈現任何實行上的困難。而將此暫時的放在作業主要記憶體 RAM(51)的電路之外，或此記憶體一部份之外，而對一個記憶體盒子有效輸入端 CE(使能晶片)使用，以及主要區段(54)所須要的所有暫存器，用來回到正常的功能。此等記憶體及暫存器可以是有利的屬於靜態，以便節省其維持所須的能源。此切換電路(53)因此以虛擬記憶體(52)取代作業主要記憶體 RAM(51),以便此等程式執行專只使用虛擬記憶體以取代作業主記憶體來執行。此虛擬記憶體(52)也許位於與它所欲取代記憶體的相同的位址，但是也可能位於不同的位址。一個有利而經濟的解決方式在於使用一種 RAM 記憶體，其對於此種虛擬記憶體而言尺寸是非常小。事實上，此虛擬記憶體對主程式而言，並不扮演任何功能角色。吾人可以非常簡單地藉由縮短尋址暫存器(A3)的長度而縮小可被位址的空間。吾人亦可藉由在位址暫存器數個區段之中做一個 EXCLO-OR，以此方式將位址折攏於其本身。如此，如果此作業主記憶體之可被定位址空間是 512 八位元，吾人可將此虛擬記憶體縮

五、發明說明（10）

小至32八位元而沒有任何問題，此導致一個非常經濟節省的實施例。此32八位元可對應於，例如，在作業主記憶體的短陣中添加RAM記憶體的一線路。此線路在此情況之中是其專有的位址暫存器(43)以及故障暫存器(D3)。當切換電路(53)啓動虛擬記憶體，它亦可完全禁止進入NVM來寫入，以便不干擾其內容。

在執行轉換方面，吾人可有利地交替使用暫存器的兩區段。一個第一區段(54)以及一個第二區段(55)，其中每一個均包含執行程式所須的所有內容，尤其是各別的程式計數器(PC1)對第一區段(54)以及(PC2)對第二區段(55)，此指令解碼暫存器(D1)用於第一區段，指令解碼暫存器(D2)用於第二區段，以及由(T11,T12,T21及T22)象徵代表的其他暫存器。

此等最後的暫存器(T11,T12,T21,T22)保存了功能參數，以致於例如吾人可在其中找到機器循環次數。所有此等暫存器被切換電路(53)自動替換。

在此情況中執行位址的瞬間的改變，沒有被強迫如同在微計算機大部份的情況之下，藉由特殊的指令來保存程式計數器的內容於一個暫存器堆之中。。如此在兩方面的轉換是非常的快(通常對一個時鐘循環而言是非常的小)。這大幅地增強了此裝置的安全水準。此同樣的機構可被使用於其他的暫存器以保護處理機功能內容，如T11至T22。

其應該好好地瞭解，當程式(P1)因被切換暫存器載入積

五、發明說明（11）

體電路虛擬模式的功能而處於活性狀態。此切換電路(53)，封鎖阻塞暫存器(54)的第一堆疊，在那裡保存了電路功能虛擬作業先前的參數，用來重新啓動在那裡被中止的程式(P1)。在它這方面，暫存器(55)的第二堆疊，被運用來使得具有正常功能的電路與虛擬記憶體來執行程式(P2)。在此情況之下，非常明顯的，中斷遮蔽暫存器 IER的位元，對應於虛擬模式之功能，此元位被解除遮蔽，這樣以便使得當一個中斷產生，不論是由隨機變量產生器，或是由隨機變量產生器將一個隨機數字事先載入計時器(R3)，此隨機數字代表時間進行的結束，或是由暫存器(R2)其被載入特殊的資訊。此中斷(31)被啓動，則從程式(P1)控制之下的正常功能轉入至程式(P2)控制之下的虛擬模式之功能。

第 2 圖說明中斷模式之功能，此圖顯示中斷 IT的第 1 脈衝，是由中斷電路在路線(31)上向處理機(1)發出，此並未列入考慮，因爲它由於對暫存器作用而被遮蔽，並且被一個"立即移動資料至 IER 暫存器"的指令作中斷遮蔽，而上述指令將資料載入遮蔽暫存器。吾人假設當前的指令替變更路線之中斷解除遮蔽(但此也可能在不同的時刻由其它所有的指令來執行)。第 2 個脈衝此次處理機(1)列入考慮。此切換電路(53)經由結果作轉換，此暫存器的第二區段(55)以及虛擬記憶體(52)變成活性而代替了第 1 區段(54)以及作業主要記憶體 RAM(51)。吾人注意到其考慮到，當在做狀態轉換從一個狀態到另一個狀態時此中斷不可發生

五、發明說明（12）

，例如在(S2)以及(S3)之間，這樣以便記憶一個穩定且與機器協調一致的狀態，並且當回到中斷程式，尤其可完全恢復相同的狀態。如果在一個指令的結束，如同在習知的情況，此種中斷被列入考慮，則當它在重新執行中斷程式時，就沒有特殊的問題，因爲它在隨後的指令本身運作正常。相反地，如果此中斷發生在一個指令執行之中，例如在狀態(S2)，當然此等電路序列應恢復到相同，以便當其重返中斷程式時，能正確接合狀態(3)。此可以藉由例如在暫存器(T11)以及順序發生器(8)之間經由匯流排(3)在重返時刻直接連結而實現。此連接也可很特殊的而不經由匯流排(S3)。吾人也可有利地將狀態記憶暫存器放入順序產生器本身，這可在此階段避免動用匯流排。

以此種方式，經由中斷，主要程式(P1)可以授權及/或引起轉換至次要程式(P2)如同下文所述。當此次要程式不再處於活性狀態，則切換電路(53)的狀態被改變，並且作業記憶體 RAM 則恢復到它原來的沒經修改的形構，此使得主程式能正好在它被中斷那一點，重拾它的執行路線。

吾人也可使得當主程式(P1)進行保護時，它藉由本身的路徑改變而啓動一個次要程式(P2)，它在由它自己選擇的時刻，產生一個長度隨機變量的處理，不論它是在處理的開始，或是處理之中，以便弄亂此等不同的諸序列。此處理機的功能可以被次要程式(P2)所導引，例如，啓動一個等候環其時間視由發生器(2)發出的隨機數字而定。此次要

五、發明說明（13）

程式可使用不被主程式所使用的記憶體的部份來執行，以便此後者能夠重拾它正常的路線，不論從此次要程式再一次傳送給它控制或是到下一次的中斷，或是像以前一樣地使用計時器，或使用此兩者的組合。此次要程式也可使用共同的資源，如果在它將控制權重新交給主要程式之前，能夠重新建立主要程式的內容。

我們可以企圖這麼說，此等機構類似執行將主要程式切換至次要程式，而在結束執行回到後者。但是此種發明是非常的困難。

- 此次要程式並未執行任何與主要程式有關的強迫性的功能。

- 此虛擬記憶體(52)的尺寸可能非常的小，而它在程式的正常進行中是必須的。

- 此虛擬記憶體(52)的內容並不重要，因爲它只是用來擾亂線索。

- 以此種快速的機構，是可能將主要程式的指令與次要程式的指令互相交錯編輯。

- 並沒有必要挽救次要程式的內容，因爲它只用來擾亂線索。

在一個第2實施例之中，當處理機轉接電路(53)時，它在同時藉由隨機變量產生器(2)之助，或是根據不消逝記憶體NVM(7)的內容，將計時器(R3)啓動爲活性狀態。此NVM是E2-型的PROM，例如是鐵電式的，可以事實上包含一個

五、發明說明（14）

在每次NVM使用時修改的一個獨特的數字。當此計時器(R3)到達一個無法預測時間的終點時，它啓動回到主要程式並轉換切換電路(53)來將主記憶體重新置放入作業空間。此機構能執行，或是從傳統的中斷方面，或是藉由計時器(R3)直接對切換電路(53)的行動以及對暫存器(PC1)及(PC2)的行動，來控制程式的執行，此控制是藉由處理裝置(1)例如(PC1)及(PC2)而爲。

在一個變化例之中，可以使用主要程式(P1)的任何一部份其在起初指向一個隨機選擇的位址，而作爲次要程式(P2)；並實現將產生於位址的八進位元組轉化，及/或轉化例如暫存器(ID2)的內容，藉接線至其背面或者還有藉由在一個位址內容左邊的一個切換電路。吾人可確信，此程式執行此等指令是完全充滿想像的。

在另外一個變化例用來使得指令執行具有想像是由第3圖所構成。其中一個指令解碼暫時暫存器IDT，一方面藉由匯流排的一部份(33)來接至匯流排(3)；另一方面，連接至暫存器(55)的第二堆，以使得匯流排(34)的一部份能記憶住電路的狀態。匯流排(34)的此部分則實體上藉由特別的接線連接至堆(55)的暫存器(ID2)其連接暫存器IDT之位元(B7)至暫存器(ID2)之位元(B4)，連接暫存器IDT之位元(B6)至暫存器(ID2)之位元(B1)，連接暫存器IDT之位元(B5)至暫存器(ID2)之元位(B3)，等等。

在最後，最後一個變化例使得指令的執行完全具有想像

五、發明說明（ 15）

是由第 3B 圖所構成的實施例。其中之匯流排(3)藉由匯流排(35)之一部份而連接至暫時指令解碼暫存器 IDT。匯流排另外的一部份(37)連接此 IDT 暫存器至一個互斥一或(Excloive-OR)埠(39)的數個輸入端子。此 OR 埠的基他輸入端子則藉由匯流排(38)連接至一個暫存器(R'2)而由匯流排的一部份(36)載入，其使得暫存器(R'2)與匯流排(3)發生關連。此暫存器(R'2)可被載入所有的資訊，以致於它可引發隨機變量產生器(R1)，或計時器或不消逝記憶體 NVM(7)，藉由一個指令(例如)"移動暫存器 R1(之內容)至暫存器 R'2"。這種移動指令爲從事-微處理機領域此行業人士所熟知，所以在使用上不會造成任何困難。此互斥-或(Exclusive-RO)是介於來自暫存器(R'2)的資訊以及載入暫存器 IDT 之中的值之間，其允許修改程式(P2)所有的指令以及如此執行具有完全想像的指令。

吾人亦可運用程式(P2)之中，多數個序列，其可被稱爲隨機的方式，並且此等序列中之每一個使用一組不同的指令。其一次驅動在每一個分支內的處理參數以及驅動微處理機不同的行爲表現。此等序列可稱做隨機方式，例如，在主要程式執行跳變(jump)至次要程式之後，此次要程式被載入一個來自兩個暫存器之中之記憶體(7)之隨機變量 V 的一個值，例如，是微處理機(1)之(T21)及(T22)。此次要程式則增加此 V 值，然後此程式命令記憶中的此值在不消逝記憶體(7)中增加此值。此在不消逝記憶體(7)之中記憶的

五、發明說明（16）

此值目的是在以後的使用。此次要程式隨後從(T21)之中抽取 n-位元，以便獲得一個 r 值其允許在次要程式的各種不同的序列之中，指定某個程式序列來執行。

在第三個實施例之中，隨機變量產生器(2)是可以被處理機(1)經由匯流排(3)而由一個閱讀指令所查閱以便了解其狀況。不論是直接地察看一個既定的脈衝，或者是將幾個重新組合，或者是考慮到將隨機變量產生器(2)之內容載入至暫存器(R2)之內。當此主要程式要進行保護時，以與前面所看到的機構類似的方式將控制權交給次要程式。

當然，是可能將先前實施例的效果組合的，其一方面具有一個隨機時鐘，而另外一方面，是具有主要程式進行中斷的可能性。而此不論是其本身，或者經過授權或無授權之一個隨機中斷系統。

吾人同樣看到主要程式進展的實現是根據其所依靠的絕對無法預測的序列；其不論是隨機變量產生器，或是程式，或是計時器或是次要程式，或是還有以上第二，第三，第四要項同時的組合。當此主要程式執行在平常安全上不敏感的功能時，它也能重新執行正常的功能，例如，將一些結果提供給外界，或是還有遮蔽計時器(R3)或是隨機變量產生器(2)不相關的中斷，以便將處理時間最佳化。當安全功能一開始使用，此主要程式(P1)就授權功能進入隨機模式，而使此等不相關的中斷有效，以便干擾此功能。

在第四實施例，藉由第 1 圖來說明使得記憶體(51)及

五、發明說明（17）

(52)可同時使用。事實上，我們假設如果能夠達成發覺此等記憶體以及其相關的暫存器之間的轉換，則可以可能做一個分析來去除使用虛擬記憶體(52)的序列。爲了避免此種可能性，此實施例允許在第一階段之中，記憶體(51)及(52)兩者同時平行有效。在此假設，當然，記憶體(52)擁有在此種情況之下，其尺寸大小至少等於記憶體(51)中程式(P1)所使用區域的尺寸大小，此爲當其與此一起工作之時。以此方式，程式(P1)分別在記憶體(51)及(52)中所使用的記憶體的兩個區域內容，是在此第一階段被此程式以相同的方式啓始以及運用。一個變化例是在於使得切換電路(53)所載的內容不生效，以及在使一讀取的循環當中，兩個暫存器(D2)或(D3)之一所須的形構不生效，這樣用來避免可能的衝突，但這基本上並不改變本發明。但並不能因此能分辨那一個記憶體是真正地在此階段使用。而其可能在一個第二階級之中，由切換電路(53)之暫存器的修改，以隨機的方式交替轉換此等記憶體，全部都繼續執行相同的程式(P1)，因此不能將執行一個或另一個程式與RAM或是使用的暫存器說成太相關。在第三階段，在虛擬記憶體上轉換成如同先前所描述的經過程式(P2)，而此是在無法預測的時刻執行。而同樣的是在無法預測的時刻執行，則重新回到了作業主要記憶體 RAM(51)。此種過程可以在主要程式(T1)的保護與控制之下隨心所欲地複製。

最後，本發明所呈現的最後問題在於，要能夠離開程式

五、發明說明（18）

(P2)的虛擬模式，而回到程式(P1)之正常功能模式。正好在將控制交給程式(P2)之前，程式(P1)授權此等中斷，其或來自隨機變量產生器，或者計時器，而並不知道它啓始了後者。而在混亂無秩序的程式(P2)進行之中，由電路(4)所產生的中斷突然發生，它將控制交給中斷程式(PIT)。此程式是以傳統習知的方式藉由一個中斷向量而接連存取，並分析例如當前執行程式的內容。如果程式(P2)是處於活性狀態，則程式(PIT)重新將控制交給程式(P1)。此種機構可以下列的方式執行：當執行程式 PIT 第一個指令時，在此可例如如同第 4 圖所代表的方式構成。經由切換電路(53)之內容之一個讀取器(41)，然後一個測試器(42)用來確定是否電路(53)中所包含的資訊對應於虛擬模式的功能。如果是肯定的，則程式 PIT 執行一個由步驟(43)所代表的回到程式(P1)的指令，此返回是被根據步驟(44)之切換電路(53)所登錄的文字所引發，而此返回在於修改路線(534)及(531)之值。此在切換電路(53)之內新登錄的文字(44)允許回到正常的模式，修改路線(534)及路線(531)之值，以便授權堆疊(54)以及作業主要記憶體 RAM(51)新的使用。此回到程式(P1)的指令可以在虛擬測試(42)之後或是在執行某個數目次數不具代表性的其他指令，其允許產生一個隨機變量的時間，在此之後，直接執行。如果在此情況之中測試器(42)的結果是否定的，此程式藉由切換電路(53)之一個登錄而繼續步驟(45)；用來在虛擬模式中改變方向，

五、發明說明（19）

以便修改線路(535)及(532)之值，以授權使用暫存器(55)的堆疊以及虛擬記憶體，以及以便藉由 (531)及(534)來鎖上命令電路。

吾人注意到，在所有的實施例之中，並不須要使用一個隨機時鐘。相反的，時脈的分布可以是完全傳統習知式而且是等時的，此容許一個電路簡易的觀念如同其模擬與測試。事實上安全並不再因爲來自處理機而隨機節奏，它是處於與正確執行上述程式同一水準，並與等時的時鐘同步或沒有同步；此種執行本身是混亂的。此處理機所執行程式的組織結構能以這種方式來實現以致於此處理機的功能是由一個確實的安全應用系統所導引。它根據此機器所執行程式的型式以決定所實施的混亂的型式。在此情況之中是應用系統，它如同像是它自己的一樣來管理各種各樣來自隨機變量產生器的訊號：中斷，以及主要程式及次要程式的開始。其爲明顯的，此以要程式除了作爲一個簡單的等待之環(loop)外，還可用來現實其他的功能，尤其是它能夠對主要程式作有益的處理，以便利用提供給次要程式的時間，此種處理可以由，例如，主要程式於外部使用的計算之準備來構成。當然，我們可以輕易地歸納概括本發明的機構，當此處理機作多重應用運作時，此等應用程式可以被認爲和主要程式一樣。

前面所看到的隨機變量產生器以及計時器，並不提出實施例獨特的問題，而被知曉此項技藝的人認爲，當以上此

五、發明說明（>0）

二者被分別使用作其它用途時，則與本發明無任何關聯。

對於隨機變量產生器而言，吾人可以例如使用具有不同週期的計數器來重新關閉，此時計數器被儲存在不消逝記憶體(7)內之一個初設資訊所初設(Initialization)。當此處理機啓動之時，此等計數器取其儲存值作爲起始值。在計算的過之中或在其結束，此不消逝記憶體顯示一個新的值，作爲初設值，而在下次初設時初設此等計數器。前面所看到的中斷脈衝的產生是可以被製造，而當產生的數字具有某些特徵以致與程式的某些資料相同。我們也可取一個或數個計數器之中的一個或數個位元之值。其爲相同的可能藉由前面所看到的初設資訊的初設以使用一個密碼的算法或是一個散列函數來實現一個很好的隨機變量產生器。在此情況之下，此產生器可以在程式使用算法的形式下來實現。我們可很輕易的看到此隨機變量產生器可被相同的用來產生各種各樣在前面所看到的隨機變量。另外一個製造像此種產生器的方式是放大一個跨越“雜訊(noise)的二極體”端子所產生的電壓，以形成低通(low pass)過濾後的訊號，以確保太快的雜訊脈衝對微處理機的作業不會產生干擾。

參考符號說明

1.....處理機

2.....隨機變量產生器

3.....匯流排

五、發明說明（21）

4.....中斷電路

6,7.....不消逝記憶體

8.....順序產生器

11.....埠 ET

33,34,35,36.匯流排的一部份

41.....讀取器

42.....測試

51.....作業主要記憶體 RAM

52.....虛擬記憶體

53.....切換電路

54,55.....記憶暫存器

A1,A2,A3....位址暫存器

531,532,534,535.....路線

D1,D2,D3....資料暫存器

P1.....主要程式

P2.....次要程式

P3.....計時器

PIT.中斷程式

ID1,ID2,T11,T12,T21,T22.....暫存器

四、中文發明摘要（發明之名稱：　無法預測的微處理機或微計算機　）

本發明是有關於一種無法預測的微處理機或微計算機，其包括一個處理機(1)，一個第一作業記憶體，一個包含一個應用系統的不消逝記憶體(6)，一個主要程式(P1)，以及一個次要程式(P2)，其中還包含：

- 一個第二作業記憶體；

- 轉換裝置，其允許在程式執行之中，轉換使用相同的作業記憶體成爲兩個作業記憶體中之一，兩者都保存其內容。

- 此等轉換裝置其包含在主要記憶體之中之程式進展內容之記憶暫存器(54)之至少一個區段，以及一個切換電路(53)，用來使得作業記憶體之一以及與每一個記憶體(51,52,6)有關的接達存取暫存器(A1-A3)(01-03)，使它們有效，以上並且由切換電路(53)來控制。

90年5月9日修正補充

A8
B8
C8
D8

六、申請專利範圍

第 87109859 號「無法預測的微處理機或微計算機」專利案

(90年5月修正)

六申請專利範圍：

1. 一種無法預測之微處理機或微計算機，其包含一個被連接的處理機(1)，一個第一作業記憶體(51)藉由匯流排 3 連接至一個主要記憶體(6)，其包含一個作業系統，一個主要程式(P1)及一個次要程式(P2)，並連接至：

- 一個第二作業記憶體(52)；以及連接至

- 切換裝置，其允許當執行此等程式時，從兩個作業記憶體(51,52)之一個切換至另一個作業記憶體，同時保存兩個作業記憶體以及與每一個記憶體(6,51,52)有關的存取暫存器(A1-A3)(D1-D3)之內容，該切換裝置至少包括暫存器(54)之第一區段，用於儲存主記憶體至少一程式之作業內容，以及一切換電路(53)，其使得至少一作業記憶體以及與每一個記憶體(51,52,6)有關的存取暫存器(A1-A3)(D1-D3)能夠運作，並且由該切換電路(53)控制。

2. 如申請專利範圍第 1 項之微處理機或微計算機，其中更包含暫存器(55)之第二區段(block)以儲存次要程式的作業內容。

3. 如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中作業內容是由程式計數器(PC1 用於第一區段(54)

六、申請專利範圍

，並且 PC2 用於第二區段(55))，指令解碼暫存器(D1,D2)，以及其他的暫存器(T1.1,T1.2)與(T2.1,T2.2)所構成，以儲存例如是機器週期…的作業參數。

4.如申請專利範圍前第 1 或第 2 項之微處理機或微計算機，其中更包含裝置(R1,R2,R3)其使得程式對於等時性時鐘以隨機方式運作。

5.如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中此主要程式可授權或禁止此或此等切換裝置，其藉由將切換電路(53)載入資料，使得作業記憶體(51,52)，以及與每一個各別的作業記憶體(51,52)有關的儲存暫存器(54,55)之區段能夠運作並切換，並且各自儲存在主記憶體中程式的作業內容與次要程式的作業內容。

6.如申請專利範圍第 3 項之微處理機或微計算機，其中此主要程式可授權或禁止此或此等切換裝置，其藉由將切換電路(53)載入資料，使得作業記憶體(51,52)，以及與每一個各別的作業記憶體(51,52)有關的儲存暫存器(54,55)之區段能夠運作並切換，並且各自儲存在主記憶體中程式的作業內容與次要程式的作業內容。

7.如申請專利範圍第 4 項之微處理機或微計算機，其中此主要程式可授權或禁止此或此等切換裝置，其藉由

六、申請專利範圍

將切換電路(53)載入資料，使得作業記憶體(51,52)，以及與每一個各別的作業記憶體(51,52)有關的儲存暫存器(54,55)之區段能夠運作並切換，並且各自儲存在主記憶體中程式的作業內容與次要程式的作業內容。

8.如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中在第一階段期間切換電路(53)被載入資料使得能夠使用兩個作業記憶體，並且在第二階段期間此切換電路被載入資料，使得能夠交替地使用兩個作業記憶體之一。

9.如申請專利範圍第 3 項之微處理機或微計算機，其中在第一階段期間切換電路(53)被載入資料使得能夠使用兩個作業記憶體，並且在第二階段期間此切換電路被載入資料，使得能夠交替地使用兩個作業記憶體之一。

10.如申請專利範圍第 5 項之微處理機或微計算機，其中在第一階段期間切換電路(53)被載入資料使得能夠使用兩個作業記憶體，並且在第二階段期間此切換電路被載入資料，使得能夠交替地使用兩個作業記憶體之一。

11.如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中在被主程式使用時，第二作業記憶體(52)及其存取暫存器(A3,D3)，取代第一作業記憶體(51)及其存

六、申請專利範圍

取暫存器(A2,D2)。

12.如申請專利範圍第3項之微處理機或微計算機，其中在被主程式使用時，第二作業記憶體(52)及其存取暫存器(A3,D3)，取代第一作業記憶體(51)及其存取暫存器(A2,D2)。

13.如申請專利範圍第8項之微處理機或微計算機，其中在被主程式使用時，第二作業記憶體(52)及其存取暫存器(A3,D3)，取代第一作業記憶體(51)及其存取暫存器(A2,D2)。

14.如申請專利範圍第4項之微處理機或微計算機，其中此產生隨機的裝置包括一亂數產生器(2)，其用以經由一中斷電路(4)觸發一隨機中斷，藉由隨機跳變(jump)至次要程式(P2)，而解除在處理機中所執行此等程式之同步性。

15.如申請專利範圍第5項之微處理機或微計算機，其中此等產生隨機的裝置包含與處理機(1)無關的一個時間計算系統(R3)，其允許在時間計算之後，觸發一個中斷，使得系統由次要程式回到主要程式。

16.如申請專利範圍第14項之微處理機或微計算機，其中此等產生隨機的裝置包含與處理機(1)無關的一個時間計算系統(R3)，其允許在時間計算之後，觸發一個中斷，使得系統由次要程式回到主要程式。

17.如申請專利範圍第5項之微處理機或微計算機，其中

六、申請專利範圍

用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是由處理機及其程式，或者是由隨機中斷系統(2,4)，或者是由時間計數器(R3)，或者該三個裝置中至少兩個的任何組合所控制。

18.如申請專利範圍第14項之微處理機或微計算機，其中用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是由處理機及其程式，或者是由隨機中斷系統(2,4)，或者是由時間計數器(R3)，或者該三個裝置中至少兩個的任何組合，所控制。

19.如申請專利範圍第15項之微處理機或微計算機，其中用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是由處理機及其程式，或者是由隨機中斷系統(2,4)，或者是由時間計數器(R3)，或者該三個裝置中至少兩個的任何組合所控制。

20.如申請專利範圍第1或2項之微處理機或微計算機，其中用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是藉由被執行主要程式序列之處理機(1)載入資料而使甚能作業。

21.如申請專利範圍第15項之微處理機或微計算機，其中用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是藉由被執行主要程式序列之處理機(1)載入資料而使甚能作業。

22.如申請專利範圍第17項之微處理機或微計算機，其中

六、申請專利範圍

用於切換作業記憶體的裝置(53,54,55,A2,A3,D2,D3)是藉由被執行主要程式序列之處理機(1)載入資料而使其能作業。

23.如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間與主要記憶體(6)中主要程式(P1)所使用的空間相同。

24.如申請專利範圍第 11 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間與主要記憶體(6)中主要程式(P1)所使用的空間相同。

25.如申請專利範圍第 20 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間與主要記憶體(6)中主要程式(P1)所使用的空間相同。

26.如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間比主要程式(P1)所使用的空間小。

27.如申請專利範圍第 15 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間比主要程式(P1)所使用的空間小。

28.如申請專利範圍第 20 項之微處理機或微計算機，其中此次要程式(P2)所使用的作業空間比主要程式(P1)所使用的空間小。

29.如申請專利範圍第 1 或第 2 項之微處理機或微計算機，其中，在執行微處理機的一個指令的周期中，此切

六、申請專利範圍

換裝置執行記憶體(51,52,53,54,55,A2,A3,D2,D3)以及其相關內容的替換。

30.如申請專利範圍第23項之微處理機或微計算機，其中，在執行微處理機的一個指令的周期中，此切換裝置執行記憶體(51,52,53,54,55,A2,A3,D2,D3)以及其相關內容的替換。

31.如申請專利範圍第26項之微處理機或微計算機，其中，在執行微處理機的一個指令的周期中，此切換裝置執行記憶體(51,52,53,54,55,A2,A3,D2,D3)以及其相關內容的替換。

32.如申請專利範圍第1或2項之微處理機或微計算機，其中此次要程式(P2)並不修改主要程式(P1)之一般性作業內容，以便允許此主程式返回而無須重建其內容。

33.如申請專利範圍第23項之微處理機或微計算機，其中此次要程式(P2)並不修改主要程式(P1)之一般性作業內容，以便允許此主程式返回而無須重建其內容。

34.如申請專利範圍第29項之微處理機或微計算機，其中此次要程式(P2)並不修改主要程式(P1)之一般性作業內容，以便允許此主程式返回而無須重建其內容。

35.如申請專利範圍第32項之微處理機或微計算機，其中此主要程式(P1)的內容是在將控制交還主要程式(P1)之前，由次要程式(P2)自動重建，或是由切換裝置(53)

六、申請專利範圍

自動重建。

36. 如申請專利範圍第 32 項之微處理機或微計算機，其中此次要程式是主要程式的一部份，其藉由隨機地決定構成此次要程式(PC2)之主要程式(PC1)之該部份之開始位址而實現。

37. 如申請專利範圍第 35 項之微處理機或微計算機，其中此次要程式是主要程式的一部份，其藉由隨機地決定構成此次要程式(PC2)之主要程式(PC1)之該部份之開始位址而實現。

38. 如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中更包含裝置用來以次要程式(P2)的記憶體來替代主要程式(P1)的記憶體。

39. 如申請專利範圍第 17 項之微處理機或微計算機，其中更包含裝置用來以次要程式(P2)的記憶體來替代主要程式(P1)的記憶體。

40. 如申請專利範圍第 35 項之微處理機或微計算機，其中更包含裝置用來以次要程式(P2)的記憶體來替代主要程式(P1)的記憶體。

41. 如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中此主要程式(P1)可交替地或同時使用第一作業記憶體(51)及／或第二作業記憶體(52)。

42. 如申請專利範圍第 29 項之微處理機或微計算機，其中此主要程式(P1)可交替地或同時使用第一作業記憶體

六、申請專利範圍

(51)及／或第二作業記憶體(52)。

43.如申請專利範圍第36項之微處理機或微計算機，其中此主要程式(P1)可交替地或同時使用第一作業記憶體(51)及／或第二作業記憶體(52)。

44.如申請專利範圍第5項之微處理機或微計算機，其中將資料載入切換電路(53)，使得能夠將此等解除相關的中斷予以遮蔽或解除遮蔽。

45.如申請專利範圍第14項之微處理機或微計算機，其中由次要程式(P2)所觸發的中斷造成在將資料適當載入切換暫存器(53)後此系統回到主要程式(P1)；此資料載入是藉由執行主要程式(P1)或次要程式(P2)的一個指令而實施，以便解除此等中斷的遮蔽。

46.如申請專利範圍第1或2項之微處理機或微計算機，其中此作業系統根據處理機所執行之主要程式的型式，來決定啓動或載入何種裝置(切換電路，或磁鼓產生器，或中斷電路，或計時器)，以修改此不可預測微處理器機之作業。

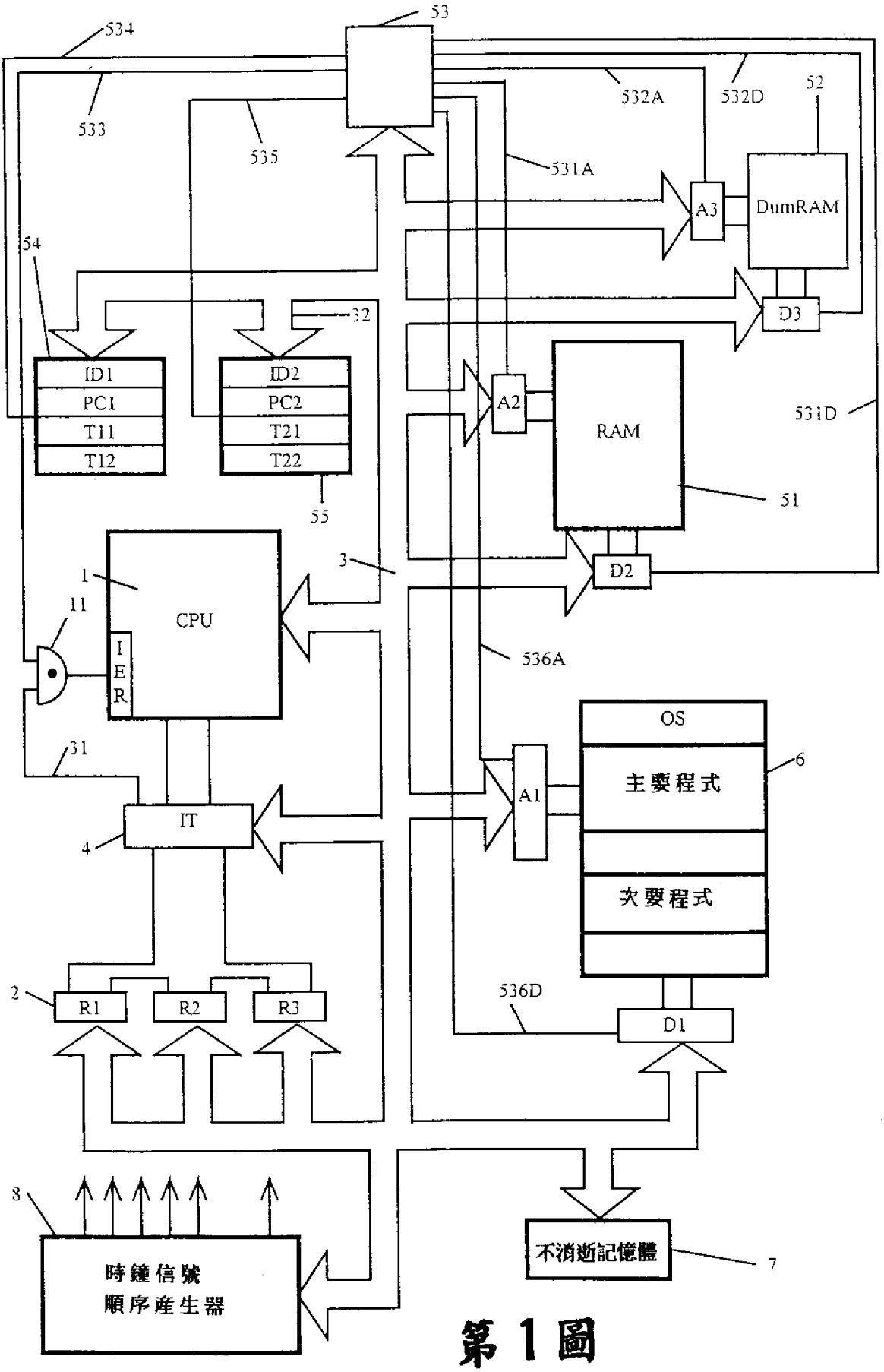
47.如申請專利範圍第23項之微處理機或微計算機，其中此作業系統根據處理機所執行之主要程式的型式，來決定啓動或載入何種裝置(切換電路，或磁鼓產生器，或中斷電路，或計時器)，以修改此不可預測微處理器機之作業。

48.如申請專利範圍第41項之微處理機或微計算機，其中

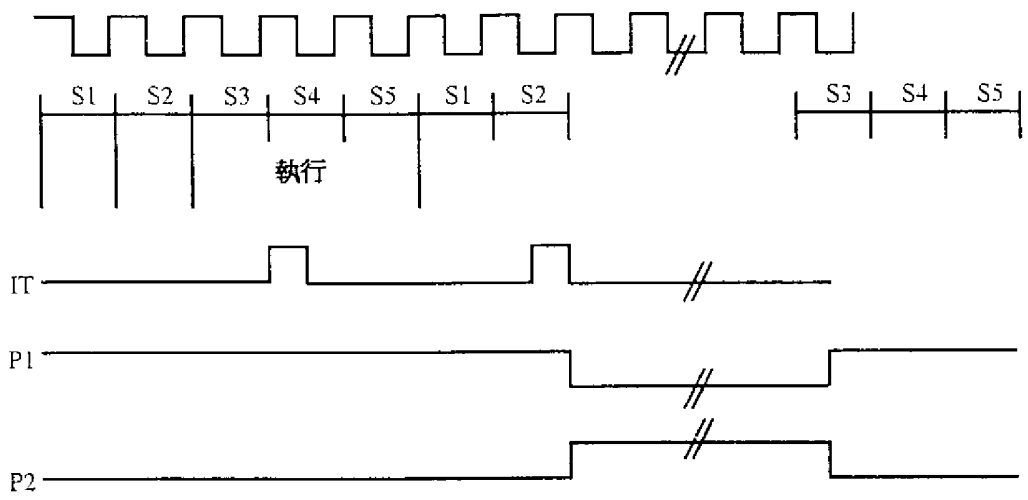
六、申請專利範圍

此作業系統根據處理機所執行之主要程式的型式，來決定啓動或載入何種裝置(切換電路，或磁鼓產生器，或中斷電路，或計時器)，以修改此不可預測微處理器機之作業。

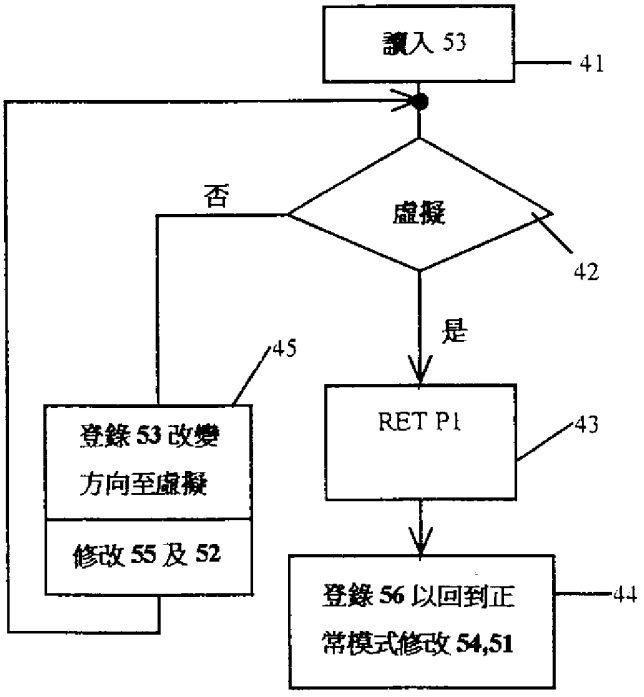
49.如申請專利範圍第 2 項之微處理機或微計算機，其中，此微處理機或微計算機是在一個單獨體的積體電路中實現。


53
534
533
535
532A
532D
52
531A
A3
DumRAM
54
D3
32
ID1
PC1
T11
T12
ID2
PC2
T21
T22
55
A2
RAM
531D
51
3
D2
1
CPU
11
IER
536A
OS
主要程式
次要程式
6
31
A1
IT
4
2
R1
R2
R3
536D
D1
8
時鐘信號
順序產生器
不消逝記憶體
7

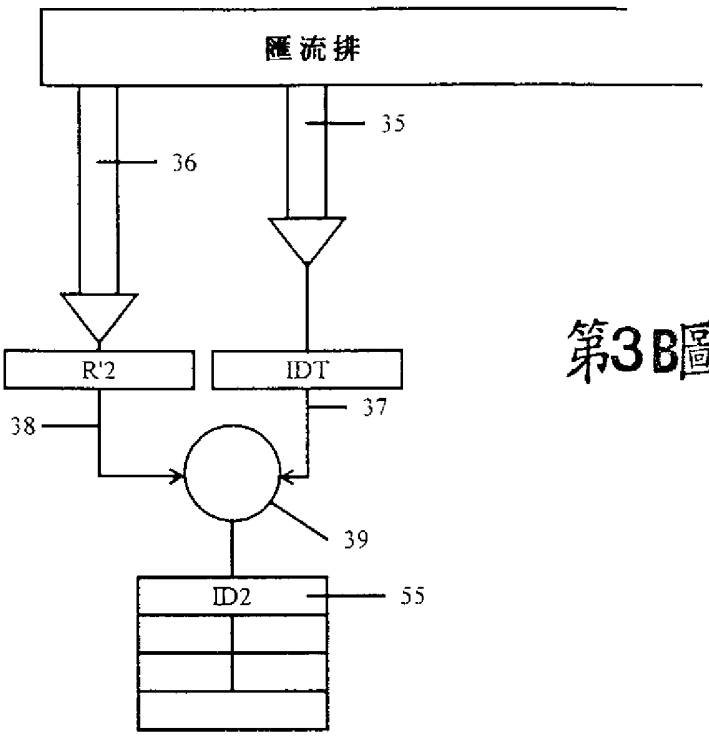
第 1 圖


S1
S2
S3
S4
S5
S1
S2
S3
S4
S5
執行
IT
P1
P2

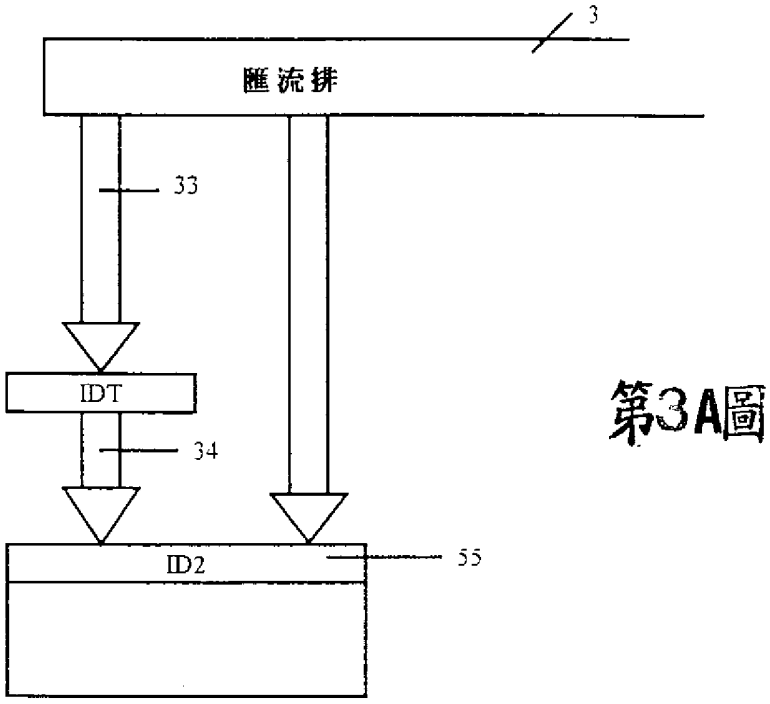
第 2 圖


讀入 53
41
虛擬
42
否
是
45
登錄 53 改變
方向至虛擬
修改 55 及 52
RET P1
43
登錄 56 以回到正
常模式修改 54,51
44

第 4 圖



第3B圖



第3A圖

公告本

申請日期	87.6.19
案號	87109859
類別	G06F 9/00

（以上各欄由本局填註）

90年5月29日 修正補充

A4
C4

457453

發明 新型 專利說明書

一、發明新型名稱	中文	無法預測的微處理機或微計算機（90年5月修正）
	英文	Unpredictable Microprocessor Microcomputer
二、發明創作人	姓名	米歇爾優剛（Michel UGON）
	國籍	法國
	住、居所	法國莫瑞巴斯78310狄斯色巴格斯路6號
三、申請人	姓名（名稱）	布爾第八特許公司（Bull CP8）
	國籍	法國
	住、居所（事務所）	法國78430路文西納斯第45號郵政信箱伯薩里斯路68號
	代表人姓名	米契爾可倫貝（Michel COLOMBE）

本案修正後是否變更原實質內容及准予修正。

90.5.29日所提之

經濟部中央標準局員工消費合作社印製

裝 訂 線

90年5月9日修正補充

A8
B8
C8
D8

六、申請專利範圍

第 87109859 號「無法預測的微處理機或微計算機」專利案

(90年5月修正)

六申請專利範圍：

1. 一種無法預測之微處理機或微計算機，其包含一個被連接的處理機(1)，一個第一作業記憶體(51)藉由匯流排 3 連接至一個主要記憶體(6)，其包含一個作業系統，一個主要程式(P1)及一個次要程式(P2)，並連接至：

- 一個第二作業記憶體(52)；以及連接至

- 切換裝置，其允許當執行此等程式時，從兩個作業記憶體(51,52)之一個切換至另一個作業記憶體，同時保存兩個作業記憶體以及與每一個記憶體(6,51,52)有關的存取暫存器(A1-A3)(D1-D3)之內容，該切換裝置至少包括暫存器(54)之第一區段，用於儲存主記憶體至少一程式之作業內容，以及一切換電路(53)，其使得至少一作業記憶體以及與每一個記憶體(51,52,6)有關的存取暫存器(A1-A3)(D1-D3)能夠運作，並且由該切換電路(53)控制。

2. 如申請專利範圍第 1 項之微處理機或微計算機，其中更包含暫存器(55)之第二區段(block)以儲存次要程式的作業內容。

3. 如申請專利範圍第 1 或 2 項之微處理機或微計算機，其中作業內容是由程式計數器(PC1 用於第一區段(54)