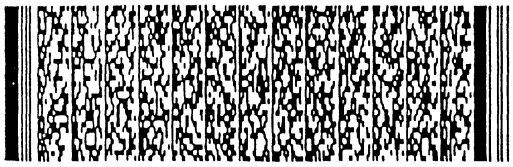
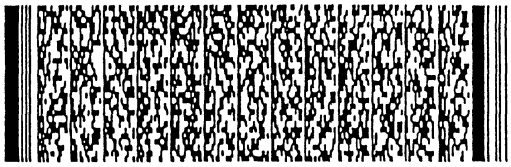
申請日期：92.12.17	IPC分類 G06F 9/30
申請案號：92135673	

（以上各欄由本局填註）

發明專利說明書 200424930

一、發明名稱	中文	智慧型電話或PDA之安全模式指示器
	英文	SECURE MODE INDICATOR FOR SMART PHONE OR PDA
二、發明人（共2人）	姓名（中文）	1. 達罕 2. 柯尼洛
	姓名（英文）	1. DAHAN, FRANCK B. 2. CORNILLAULT, BERTRAND (NMI)
	國籍（中英文）	1. 2.
	住居所（中文）	1. 法國尼斯市倫特路130號 2. 法國雷巴市傑尼斯路87號
	住居所（英文）	1. 130 Avenue de la Lanterne, Nice, 06200 France 2. 87, Chemin des Genets, Le Bar-sur-Loop, 06620 France
三、申請人（共1人）	名稱或姓名（中文）	1. 美商德州儀器公司
	名稱或姓名（英文）	1. TEXAS INSTRUMENTS INCORPORATED
	國籍（中英文）	1. 美國 US
	住居所（營業所）（中文）	1. 美國德克薩斯州達拉斯市丘爾奇路7839號 （本地址與前向貴局申請者相同）
	住居所（營業所）（英文）	1. 7839 Churchill Way, Mail Station 3999, Dallas, Texas 75251, U.S.A.
	代表人（中文）	1. 康威廉
	代表人（英文）	1. KEMPLER, WILLIAM B.





92582(9TI).ptd

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先權
美國 US	2002/12/18	10/322,893	有

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主

日期:

四、□有

寄存國家:

寄存機構:

無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期:

無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明（1）

發明所屬之技術領域

本申請案係為聲稱對2002年1月16日歐洲專利申請案序號第02290115.1號，名稱為"支援MMU與中斷之處理器之安全模式"（授權備忘號33762.1EU）、以及2002年6月30日歐洲專利申請案序號第02100727.3號，名稱為"支援MMU與中斷之處理器之安全模式"（授權備忘號33762.2EU）之優先權。

本發明概與微處理器有關，更特別言之，與用以支援安全軟體服務之保全機制之改善有關。

先前技術

微處理器係提供高指令運算量以執行其上之軟體之通用處理器，並視其所含特定軟體應用而具廣泛處理需求。許多不同類型之處理器均屬已知，微處理器僅係其一。例如數位信號處理器（DSP）即泛為使用，並以針對特定應用如行動處理應用為最。DSP一般係配置以使相關應用之性能最佳化，為達此目的，其使用更特定化之執行單元與指令集。欲提供持續攀升之DSP性能，同時盡能降低功率耗損於特別是、但不限於行動電訊之應用中。

為進一步改善數位系統性能，可使兩或多具處理器互連。例如可在數位系統中將DSP與通用處理器互連。DSP施行數值強化信號處理演算法，而通用處理器綜理所有控制流程。兩具處理器經由共用記憶體傳遞並轉移資料供信號處理之用。直接記憶體存取（DMA）控制器常與處理器連

五、發明說明（2）

結，以接管記憶體或週邊資源間資料區塊轉移之重擔，藉以改善處理器性能。

一般均具有作業系統（OS），俾藉由對資源控制及各種程式模組或任務之執行排程而管理數位系統。在具有數具處理器之系統中，各處理器均具個別 OS 較為便利。概言之，OS 係假定其在所有系統資源之控制下。多種 OS 均未被設計為可與其它 OS 共用記憶體與資源。因此當將兩或更多個 OS 併在單一系統中時，即可能發生資源分配問題。在記憶體或週邊裝置使用上之衝突，均可能對系統操作造成不良後果。

大部分處理器之建構均具 2 特權等級：其一供 OS 使用，另一則供用戶任務之用。曾有人提出第三特權等級，但在現行 CPU 中從未付諸實現。

針對特定財務或安全關鍵應用，一些作業系統已被確認為安全無虞。部分通用作業系統聲稱有內建保全，但其不堪一擊係眾所週知。

可利用硬體機制改善保全。例如美國專利第 4590552 號，名稱為"用以標示儲存於非揮發性記憶體中之資訊保全狀態之保全位元"，揭示一種藉由提供可永久設定為禁止晶片外（off-chip）資源進入晶片上（on-chip）記憶體之一或多個保全位元，因而保護資料儲存之機制，藉以保護儲存於晶片上記憶體中之碼或資料。但作業系統之誤判操作可破解此類保全方法。

在能施行安全類別之應用如商務（行動商務）或 e-銀行

五、發明說明（3）

（電子銀行）之智慧裝置上，要求用戶以鍵盤輸入私密資訊如密碼，或於螢幕上顯示之訊息簽署。在執行此動作時，用戶除完全仰賴其裝置之健全性外，別無其它選擇。但用戶無法檢測駭客或病毒是否已入侵其裝置之保全架構。

發明內容

因此，確需改善系統保全。概言之，在本發明之一型式中，提供一具有以非侵入性方式建於處理器系統之安全模式（特權等級第三級）之數位系統。安全執行模式因而位於一平台上，該平台之唯一信賴軟體係儲存於晶片上 ROM 中之碼。並提供數位系統用戶可見之指示器手段，其中該指示器手段僅可於安全模式之操作下，以信賴程式碼啟動之。

在一實施例中，經由一獨特進入點進入安全模式。可以進/出條件之充分硬體評估，動態出入安全執行模式。

實施方式

與用戶交換如密碼或螢幕上顯示之訊息之機密資訊，須僅於處理裝置處於安全模式下時才施行。一種提供安全模式之裝置與方法述如 2002 年 6 月 30 日提出之歐洲申請案序號第 02100727.3 號相關專利申請案"供支援 MMU 及中斷之處理器用之安全模式"。在此納入安全模式之充分描述，俾使熟悉此技藝者瞭解其操作。

在安全模式中，實體用戶介面（如鍵盤或顯示器）之進入受限於經由受信賴驅動器之安全應用。以安全模式為進入鍵盤及顯示器把關，並不足以充分保障與用戶間之訊息交換。現本發明人已發現需以一手段指示用戶，OS 呼叫適當

五、發明說明（4）

受信賴之鍵盤或顯示器驅動器，亦即儲存於安全記憶體中之驅動器，並進入安全模式執行。否則若病毒/駭客欲下載智慧裝置上之偽驅動器，則用戶無從得知其無法仰賴其裝置。

依本發明之一態樣，執行安全應用之智慧裝置除具顯示器與袖珍鍵盤外，尚具一安全模式指示器。此指示器將告知用戶該裝置處於安全模式。此指示器可為例如小型 LED。若安全模式指示器未啟動，則用戶不應輸入任何私密資訊（密碼）或不應於螢幕上之顯示之任何東西簽署。若在指示器未啟動時欲輸入其個人識別碼，則用戶將得知其裝置已遭破解，而裝置無法提供安全操作。

為達此目的，於圖 1 之數位系統上提供一僅可於安全模式下進入之通用輸入/輸出（GPIO）閂鎖位元 154。以此安全 GPIO 閂鎖驅動保全指示器 LED 155。刻正於來自安全 ROM/SRAM（唯讀記憶體/靜態隨機存取記憶體）之安全模式下執行之受信賴鍵盤與顯示器驅動器負責管理安全 GPIO 閂鎖。

安全模式指示器須獨立於鍵盤及顯示器之外，因為非安全應用軟體會於非安全模式下進入這些裝置。特別言之，螢幕上顯示之訊息如"現在輸入密碼"一般並不可靠。此外，由於駭客碼可進入螢幕，故螢幕上顯示之用以指示安全操作之符號或訊息（如鎖狀符號）並不可靠。安全模式指示器須可靠指示何時裝置係於安全模式下運作，且僅當裝置處於安全模式下時才有指示。除非安全模式指示器已啟動，否則應通知用戶不要輸入任何如密碼之私密資訊或不要在螢幕上簽署

五、發明說明（5）

任何東西。

圖 1 係在具有複數個處理器 102、104 之兆位單元（mega cell）100 中之包含本發明之一實施例之數位系統之方塊圖。為利明晰之故，圖 1 僅顯示兆位單元 100 中與本發明之一實施例之瞭解有關之部分。數位信號處理器（DSP）之一般架構細節係眾所週知，且易於在它處得見。例如 Frederick Boutaud 等人在美國專利第 5,072,418 號中詳述一種 DSP。Gary Swoboda 等人在美國專利第 5,329,471 號中詳述如何測試與模擬 DSP。以下將對兆位單元 100 中與本發明之一實施例有關之部分作充分描述，俾使熟悉微處理器技術者施行與利用本發明。

雖然本發明發現對施行例如在特殊應用積體電路（ASIC）上之數位系統之特殊應用，亦發現對其它形式系統之應用。ASIC 可包含一或多個兆位單元，其各自包含針對客戶設計之功能性電路以及出自設計庫中之預先設計之功能性電路。

在兆位單元 100 中具有一種分佈保全系統，其採用選擇硬體方塊與受保護軟體執行環境之組合。該分佈保全系統係用以解決行動電話環境內之電子商務（e-商務）與行動商務（m-商務）保全議題之方法。保全議題包含以下所列：

-機密度：確保僅有通信者可理解傳輸資訊之內容；

-完整性：確保資訊在傳送期間不變；

-驗證性：確保另一通信者係即為其所宣稱者；

-無否定性：確保傳送者不能否認傳送訊息；

五、發明說明（6）

-用戶保護性：假名與匿名；

-無法複製之保護。

現行作業系統（OS）無法被視為安全。部分 OS 聲稱安全，但其複雜性導致不易達成或保證安全。對電子商務及其它安全交易而言，亟需安全軟體層。此須易於在既有 OS 施行，但又支援記憶體管理單元（MMU）與快速緩衝儲存區使用，同時支援及時中斷與 OS 支援。

在許多應用中已證實僅具軟體之解決方式不夠健全，且僅能透過軟硬體架構之妥善併用解決這些議題。在此實施例中採用之安全模式之發展，係為將硬體健全性導入整體保全機制中，其係根據以下前提為之：

-作業系統（OS）不可信賴；

-在平台上執行之所有本質軟體均不可信；

-唯一可信之軟體為儲存於安全程式 ROM/SRAM 中之碼；

-可因性能之故啟動快速緩衝儲存區；

-為即時之故可啟動中斷；

-為彈性之故可啟動 MMU。

上述前提驅動下列結果。首先，OS 記憶體管理並不可信。換言之，MMU 操作與 OS 定義之轉譯表並不可靠。安全模式應可抗拒 MMU 之任何誤用以及 OS 定義之轉譯表可能錯誤百出的事實。其次，OS 定義之中斷向量表以及中斷服務例行程序並不可信。需於安全模式下施行中斷之特定管理，致使安全模式得以抗拒中斷之任何誤用以及中斷向量表及 ISR 可能錯誤百出的事實。第三，OS 基本操作之完整性

五、發明說明（7）

（如背景保存、快速緩衝儲存區快取、TLB 快取、寫入緩衝汲取等）並不確定，故安全模式不應仰仗之。最後但非最不重要處在於，在安全模式下，需將所有的測試、錯誤移除與模擬能力去除。

在此實施例中，針對處理器 102 產生分割"安全模式"，使之可如個別"虛擬保全處理器"般操作，並同時執行保全操作。可將安全模式視為處理器 102 之第三特權等級。其啟動端視特定目的硬體之存在於否而定，該硬體可藉由不受信賴之軟體產生一環境，以保護機密資訊不被存取。安全模式係由宣告一專屬之保全信號 152 設定之，保全信號 152 傳播過系統，並於受信賴軟體可進入之資源與任何軟體皆可進入之資源間建立邊界。

安全模式啟動亦視保全軟體之適當控制而定。保全軟體係儲存於安全程式 ROM/SRAM 中，並於該處執行。該處不可能存在藉由欺瞞硬體而得以進入安全模式，或取得受信賴碼而施行其不應施行之任務之流動。若適當建立邊界，則除經由受控制之操作外，應無利用處理器之正常操將資訊作自邊界內向外移之管道。注意處理器之正常操作包含執行有潛在瑕疵之"用戶碼"。

安全軟體層受安全記憶體之信賴並儲存於其中。其係藉由通過單一安全閘道至安全模式，同時保護免於 MMU 修改，而進入一軟體序列，向硬體保全狀態引擎（SSM）150 展示其確實在執行安全碼。當安全軟體正在在執行安全模式時，將中斷向量重新定向，致使保全控制軟體得以視需要開

五、發明說明（8）

始適當離開安全模式。重新定向過程對 OS 為透明的，並可在過渡後避免顯現安全資料。

GPIO 閂鎖 154 係以習知方式操作之記憶體映對閂鎖，例外處在於其僅可為安全軟體存取與啟動。指示器 155 耦合至 GPIO 154，並響應於 GPIO 而發亮。藉由寫入一如邏輯 1 之邏輯值於閂鎖 154 而打開指示器 155；並藉由寫入一如邏輯 0 之互補邏輯值於閂鎖 154 而將其關閉之。核心 103 經週邊匯流排信號 156 存取閂鎖 154。但係以受控於 SSM 150 之安全信號 152 限定 GPIO 閂鎖 154 之操作。如此一來，僅可於安全信號 152 處於指示處理器 102 正執行安全軟體例行程序之啟動狀態時對 GPIO 154 寫入。在本實施例中，指示器 155 係發光二極體（LED），但在其他實施例中，可採用得以顯現兩相異狀態：開與關之任何類型之指示器。例如可採用各類燈，諸如氖、電漿等。可採用各種機械裝置，諸如轉動顯示不同色而指示開/關狀態之碟，或移動一指示器以代表開/關狀態之致動器。在其他實施例中，可以結構、高度、溫度等之表面變化表示兩狀態，使得視力有缺陷或其他肢體受損人士得以檢測兩種狀態。例如可將接觸式指示器置於捲動式顯示器裝置中。在另一實施例中，指示器可提供音頻指示，例如可播放音調以指示安全模式開啟，但由於可以非安全音頻源模仿該音調，故需有一定程度之注意。

復參閱圖 1，兆位單元 100 包含具 32 位元核心 103 之微處理器（MPU）102，以及具 DSP 核心 105 之數位信號

五、發明說明（9）

處理器（DSP）104，兩者共用一稱之為第二等級（L2）記憶體子系統之記憶體方塊 113。流量控制方塊 110 接收來自連結至主介面 120b 之主處理器之轉移要求、來自控制處理器 102 之要求，以及來自 DSP104 中之記憶體存取節點之轉移要求。流量控制方塊插入這些要求，並將之呈現於共用之記憶體與快速緩衝記憶區。亦經流量控制方塊存取共用週邊 116。直接記憶體存取控制器 106 可於外部來源如晶片外記憶體 132 或晶片上記憶體 134 與共用記憶體間轉移資料。亦可視各應用需要將各種特定應用處理器或硬體加速器 108 納入兆位單元中，並經由流量控制方塊與 DSP 及 MPU 交互作用。

在兆位單元之外，第三等級（L3）控制方塊 130 響應於來自 DSP 或 MPU 之明確要求，連結接收來自內部流量控制方塊 110 之記憶體要求。晶片外之外部記憶體 132 及/或晶片上記憶體 134 連結至系統流量控制器 130；這些稱之為 L3 記憶體子系統。時框緩衝器 136 及顯示裝置 138 均連結至系統流量控制器，以接收用以顯示圖像之資料。主處理器 120a 與外部資源經由系統流量控制器 130 交互作用。連結至流量控制器 130 之主介面可為主處理器 120a 存取至外部記憶體及其他連結至流量控制器 130 之裝置。因此，在各實施例中，可於第三等級或第二等級下連結主處理器。一組私人週邊 140 連結至 DSP，同時另一組私人週邊 142 連結至 MPU。

圖 2 係在圖 1 之系統中之 MPU 102 之方塊圖，其闡釋

五、發明說明（10）

採用選擇硬體方塊與由保全狀態引擎 300 執行之受保護軟體執行環境之組合之分散保全。在數位系統之另一實施例中，舉例來說，處理器 102 可為單一處理器，或可耦合至一或更多個處理器供協同操作之用。

安全模式係處理器 102 之"第三特權等級"。安全模式提供硬體手段，以限制對於在適當執行環境下設定之處理器子系統（CPU）200 之安全資源之存取。安全模式係建於 CPU 200 周圍，CPU 200 包含處理器核心、資料及指令快速緩衝儲存區 204、206 與 MMU 210。優點在於本實施例之保全特性對 CPU 200 不具侵入性，故在另一實施例中，可採用另一處理器取代本處理器處。

保全硬體有兩類：控制保全信號之邏輯，以及受限於安全模式之硬體資源。前者主要由保全狀態引擎（SSM）300 組成。SSM 300 負責監視進入安全模式之條件；宣告/取消保全信號 302；以及偵側安全模式違反。藉由宣告連結至重置電路系統 306 之違反信號 304 而指示違反，其在檢測到保全違反時即使系統重置。保全狀態引擎監視來自處理器 200 外部介面之各信號 330，尤其是在指令匯流排上為處理器取得之位址。保全狀態引擎緊密耦合至來自進入序列之低階組合碼。其對由所監視信號上之進入序列產生之事件作出反應。

當宣告保全信號 302 時即進入安全模式。當宣告保全信號時，其傳遍整個系統，俾開放對安全資源之存取。在安全模式下，僅有處理器 200 可存取安全資源。在本實施例

五、發明說明（11）

中，因設計規範之限，DSP 104 與 DMA 106 不得存取安全資源。在本實施例中之安全資源包含：安全 ROM 310（整體 ROM 的一部份）、安全 SRAM 312，及各安全週邊裝置 316a、b。對 GPIO 閂鎖 318 之存取亦由保全信號 302 核可，造成僅可於保全信號 302 處於指示 CPU 200 正執行安全軟體例行程序之啟動狀態時才可對 GPIO 318 寫入。以保全狀態引擎（SSM）300 在特定條件下宣告保全信號 302。在安全模式下，CPU 200 僅可執行儲存於安全 ROM 310 或安全 SRAM 312 中之碼。任何嘗試執行儲存於這些受信賴位置以外之碼，均將由宣告信號 304 產生"保全違反"，其將導致重置電路系統 306 施行整體系統重置。

此 ROM 被分割為兩部分：受安全位元保護，並且僅可於安全模式下存取之 ROM 之安全部；以及可隨時存取並具開機區之 ROM 之公用部。公用 ROM 311 亦具各種保全程序，並參與整體保全機制。

安全儲存 RAM 312 係安全工作資料儲存處（安全堆疊、安全整體資料、安全堆積）。安全程式 RAM 312（選用）係專為執行非既有安全碼之用。非既有安全碼係先自外部記憶體裝置下載至安全程式 RAM 中，接著再於執行前先行認證。

以由整體重置信號重置之暫存器 306 施行在安全儲存 SRAM 中之數個位元組位址。這些暫存器會遮蔽一些正常 SRAM 位置，並可充作一般 SRAM 位址之用。唯一之差別在於這些暫存器/SRAM 位置將被重置為皆為 1 之一值。在

五、發明說明（12）

安全模式下具有少許可被重置之變數，因而具有已知且僅可於安全模式下改變之初使值係屬有利。例如此特性可用以：在安全模式下檢測第一入口；設定適當離開模式值（正常、例外、違反）；檢測電源開啟等。在另一實施例中，可以其它方式施行這些可重置值，諸如藉由將暫存器置於未與 SRAM 重疊之位址空間中；藉由連結重置信號至 SRAM 內之所選記憶體單元等。

並無可用以宣告保全信號 302 或改良狀態引擎行為之軟體方式。SSM 緊密耦合至將參閱圖 5 詳述之啟動序列。SSM 監視來自處理器 200 之實體指令位址匯流排 330 以及自各資源接收之各進入條件信號 321-327。出自處理器 200 之指令介面信號 331 與資料介面信號 333 亦被監視，並分別界定在指令匯流排 330 與資料匯流排 332 上施行何種匯流排處置。

安全模式係藉由分支為公用 ROM 中之一特定位址而進入，其稱之為單一進入點，此係 SSM 中之硬編碼位址。進入點係"啟動序列"之開始位址。啟動序列係儲存於耦合至保全狀態引擎之公用 ROM 之一組碼，並確保符合安全模式之部分進入條件。其他進入條件係由監視特定進入條件信號而直接評估。

啟動序列於保全狀態引擎所監視之部分信號上產生界定之事件序列。這些事件確保進入安全模式所需之條件已符合。保全狀態引擎認知此模式並宣告保全信號。在安全模式下，保全狀態引擎持續監視一些信號，俾檢測安全模式違反

五、發明說明（13）

及確保符合安全模式離開程序。不論何時發生違反情事，SSM 均會釋出保全信號並宣告保全違反信號 304。典型違反係嘗試取出 ROM/SRAM 位址範圍外之指令。

啟動序列係儲存於公用 ROM 中。其確保安全模式進入條件已符合。環境設定序列係儲存於安全 ROM 中。其針對用於可致動快速緩衝儲存區、中斷與 MMU 處之安全模式設定適當執行環境。離開序列係儲存於安全 ROM 中。其強制執行符合安全模式離開程序。其藉由一 BRANCH 或在中斷下提供一安全離開安全模式之方式。其亦於離開時保護安全 ROM 與 RAM 之"私密"內容。

仍參閱圖 2，保全控制暫存器 319 僅在安全模式下可充作記憶體映對暫存器而可以存取，並用以致動/關閉可被駭客用以破壞保全，但對系統硬體與軟體之認證及除錯仍屬需要而使用之測試、除錯與模擬設施。例如以信號 321 表示之一位元致動/關閉供程式發展用之嵌入追蹤巨集單元（ETM）350 之運作。信號 322 致動/關閉在處理器 200 上之 JTAG 介面之運作。信號 323 致動/關閉在處理器 200 上之除錯介面（dbg I/F）之運作。

在非安全模式下，保全條件暫存器 320 可充作記憶體映對暫存器而被存取，並藉由控制可為駭客用以破壞保全之各資源之操作模式而設定在安全模式下之部分進入條件。自保全條件暫存器提出之信號亦受狀態引擎監視。例如直接記憶體存取（DMA）致動信號 324 係用以致動可以存取安全記憶體 312 之 DMA 控制器（未圖示）。

五、發明說明（14）

在本實施例中，為測試而提供掃瞄串介面（掃描 I/F），並可提供保全破壞點。但處理器 200 未提供關閉掃描串輸出之手段。為避免修改處理器 200 之內部信號，自外部提供掃描閘 342，俾於遮蓋處理器 200 之掃瞄輸出，其時鐘長度等於處理器 200 內最長掃描串之數目。於重置時初始化此遮蔽機制（計數器重置），且每次均以在外部測試設備（未圖示）之控制下之掃描致動將裝置自功能模式切換為測試模式。

提供外部中斷操作器 360 以接收一組中斷信號，並將之多重發訊為接著為處理器 200 接收之兩中斷信號 362、363。中斷處理器 360 具有可由軟體設定之整體遮蔽位元 364，並致使軟體得以對處理器整體關閉所有中斷。不論何時設定整體遮蔽位元，中斷控制器均宣告遮蔽信號 325，並將中斷信號 362、363 關閉。在宣告遮蔽信號 325 後，直到由軟體清除整體遮蔽位元前，均無法再宣告中斷控制器所輸出之中斷信號 362、363。SSM 300 監視遮蔽信號 325 以決定是否致動或遮蔽中斷。

自外部記憶體開機係駭客破壞系統保全之常見手段。在本實施例中，避免外部開機。此外，SSM 300 監視於嘗試外部開機時會被宣告之開機信號 327。但在程式發展期間，較佳允許外部開機以利軟體除錯。提供熔絲電路 328 以區分發展裝置與生產裝置。裝置型信號 326 為 SSM 300 所監視，故得以於發展裝置上提供釋放之保全模式。對發展裝置而言，SSM 300 會忽略開機信號 327。

五、發明說明（15）

圖 3 係闡釋圖 2 之 ROM 內容及用以將 ROM 分割為公用部與安全部之電路系統之方塊圖。在本實施例中之公用 ROM 311 與安全 ROM 310 係以單一 ROM 實施之。在另一實施例中，則可於不影響此處之發明性態樣下分割之。位址解碼器電路 370a 係用以對 ROM 之存取解碼之解碼電路 370 的一部份。對 SRAM 與其他指令或資料匯流排連結之裝置提供類似電路。

不論何時，響應於分別和公用 ROM 位址或安全 ROM 位址對應之位址解碼信號 406 或 407，因而宣告在指令位址匯流排 330a 上對應於 ROM 310、311 之位址，均致動驅動器電路 400 以於指令匯流排 330b 上提供要求指令資料。

如上揭，若非於安全模式下存取安全資源，則提供假資料。閘電路 404 監視保全信號 302 與安全 ROM 解碼信號 407，並且若存取安全 ROM 但未宣告保全信號，則使驅動器電路 400 通過無效資料。

安全模式

圖 4 係闡釋對圖 2 系統上安全模式操作之存取流程圖，現將更加詳述之。步驟 500、502、504 代表在一正常非特權等級執行中，在處理器 200 上執行之應用程式。有時為在特權等級操作中之服務，如步驟 510、512、514 及 516 所示對作業系統（OS）產生一呼叫 502。只要一呼叫，OS 在步驟 510 中儲存狀態並切換至特權模式；在步驟 514 中施行特權操作；在步驟 516 中恢復狀態；並在 504 中返回非特權應用。這兩個等級之操作係眾所周知。

五、發明說明（16）

在步驟 512 中，以測試決定所要求之服務是否為安全操作；若是，則系統將進入稱之為安全模式之第三等級保全。在步驟 520 中，OS 驅動器施行管家工作，將系統置於適當狀態以進入安全模式。此包含遮蔽中斷；設定保全條件暫存器 320 以關閉存在保全風險之各種資源；以及確認是否致動記憶體管理單元 210，其係使對應於啟動序列之頁表入口標示為"非可快速儲存緩衝"。此將於稍後進一步詳述。

在步驟 522 中，復參閱圖 3，跳至一位於公用 ROM 311 中之進入序列 412 中之進入點 410。進入序列係一組碼，其每次在於平台上執行任何類型之保全碼之前，在"安全服務"為應用所呼喚時執行。此序列亦於自己中斷保全碼執行之例外處恢復時執行。進入序列始於 ROM 中界定之位址，其係為硬編碼並稱之為"進入點"。進入序列係由兩部分組成：保全信號啟動序列 413 及安全模式環境設定序列 414。

啟動序列之目的係為取代處理器 200 之執行流動，並確保任何其他非受信賴碼無法優先占有。在進入序列之此部份期間之某些點處，宣告保全信號 302 以進入安全模式，並解除對安全資源（ROM、SRAM、周邊裝置等）之存取。

環境序列 414 之目的係為設定全碼執行之環境。優點在於藉由設定安全環境，即可安全致動程式與資料快速緩衝儲存區，並操作中斷例外。

保全信號啟動序列 413 位於公用 ROM 中，而安全模式環境設定序列 414 則位於安全 ROM 中。進入序列之總碼大

五、發明說明（17）

小（部份 1＋部份 2）需小於 1 千位元組，使之得以映對於 1 千位元組頁，對此實施例而言為 MMU 轉譯表中最小記憶體段落。以此方式為之，則進入序列虛擬位址無法映對於兩段落上，以在進入序列執行期間，於部分明斷點處優先佔有處理器。於進入序列之記憶體頁為非可快速緩衝儲存，或於執行進入序列時將指令快速緩衝儲存區關閉亦屬重要。

隨後將描述安全轉譯表（STT）420 與安全中斷向量表（SIVT）430。

若所見 1 千位元組碼大小對給定之實施例而言被視為限制過大，則 MMU 可於啟動序列 413 關閉，並於環境序列 414 末處再致動。在此情況下，1 千位元組限制將僅對啟動序列作用。

復參閱圖 4，在步驟 524 中，為修正之故，以 SSM 300 檢查啟動序列。如下將參閱圖 5 所詳述。若未正確施行啟動序列，則於步驟 540 中以 SSM 300 宣告違反信號並將系統重置。在步驟 526 中，藉由執行環境設定序列 414 而設定安全環境，如後將詳細描述。

只要一建立安全環境，即從安全碼 416 於步驟 528 中執行要求之安全操作，如同以非特權應用於開始時要求一般。依本發明之一態樣，安全碼 416 包含在步驟 528.1 中寫入 GPIO 閂鎖 318 之一指令，其僅於安全模式下開啟安全模式指示器 319。安全碼 416 接著可於步驟 528.2 中要求用戶提供機密資訊，隨後於步驟 528.3 中藉由再度寫入 GPIO 閂鎖而關閉安全模式指示器。在步驟 528.4 中執行附

五、發明說明（18）

加安全處理。應知此特殊序列僅供闡釋之用。例如，可於開啟安全模式指示器前施行其他安全處理。例如可開啟安全模式指示器一會兒，關閉一會兒，接著再度開啟。無數種其他序列均可視應用程式需要施行之。

在完成安全操作後，在步驟530中離開安全模式之正常方式係於安全ROM離開序列418中跳至"正常離開序列"。正常離開序列之目的係為符合安全模式離開程序並確保離開時對"私密"內容之保護。正常離開序列可位於安全ROM中任何位置；在保全狀態引擎中並無硬編碼位址檢查。

安全模式中，SSM 300仍持續監視信號321-327與331。SSM可根據這些信號檢測保全違反。不論違反安全模式何時發生，SSM均檢測之，釋放保全信號並產生保全違反，如弧線542所示。違反啟始裝置之整體重置。保全違反驅動SSM至僅可藉由重置離開之封鎖狀態。可檢測下列違反：違反1-於完整ROM與RAM位址範圍外之位址處取得指令；違反2-重置處理器200；違反3-制動測試、模擬或除錯特性。

當例外發生時，處理器200即跳至中斷向量表（IVT）中之對應例外向量，自該處將之重新指向特定中斷例行程序。IVT一般係以OS管理，但其非位於安全SRAM中。因此，其內容未受保護而不可信賴。此外，就保全觀點而言，不允許處理器直接跳至例外向量之原因有二：（1）與整體保全機制不符；將"跳"出安全記憶體位址範圍外視為保全違反；（2）快速緩衝儲存區與處理器暫存器充斥"私密"內

五、發明說明（19）

容，需於釋放安全位元與執行非安全碼前清除之。為於安全模式下允許中斷，需提供安全 IVT。

圖 5 係更詳述保全狀態引擎 300 操作之狀態圖。保全狀態引擎在於 ROM 中執行啟動序列期間，於某些點處宣告保全信號，以進入安全模式。此部分進入序列之目的係為在保全狀態引擎所偵測之信號上產生界定之事件序列。這些事件確保設定保全信號所需之條件為符合，並可以 SSM 搜尋之。於整個啟動序列中監視"條件"信號。若在啟動序列結束前有任何進入條件不符或停止有效，保全狀態引擎將過渡至違反狀態 630 並宣告保全違反信號 304。在以 SSM 監視進入條件之背後有兩關鍵目的：（1）處理器 200 正在汲取且淩駕執行啟動序列碼；（2）受信賴碼已完全取代 CPU 執行流程，除非經過受控操作，不論在設定保全信號之前後，無任何者可優先占有而不被檢測到。

啟動程序之建構方式係於指令位址匯流排上產生獨特原型。該原型係由啟動序列碼之（實際）位址值以及在時間中之相對時機製成，這些位址應出現在匯流排上。但原型之製成與記憶體系統存取潛伏期無關。確切啟動序列匯流排原型係自 SSM 中之模擬及硬編碼而得。SSM 因而確保與啟動序列匯流排原型完全符合。典型上，啟動序列之最終指令係分支指令，且異於快速緩衝儲存區清除指令或快速緩衝儲存區關閉指令，在啟動序列中之所有其他指令均為 NOP 指令。

在進入安全模式並已宣告保全信號後，進入條件無需有

五、發明說明（20）

效，且 SSM 不對其持續測試。但 SSM 持續偵測各信號以檢測安全模式違反，以下將描述之。直到有效進入安全記憶體後，始測試安全模式離開條件。

復參閱圖 5，狀態 600 係一閒置狀態，在該段期間 SSM 監視位址匯流排 330，尋找進入序列之進入點位址（ESA[EP]）。只要一檢測到進入點位址，若符合所有進入條件，SSM 即過渡至狀態 601；若非如此，則過渡至宣告違反信號 304 之違反狀態 630 處。

須藉由檢測正確進入序列位址及對應之進入條件信號而依序經過各狀態 601-615，否則 SSM 即過渡至違反狀態 630。若這些序列無誤地經過，則進入安全模式狀態 620 並宣告保全信號 302。

例如為自狀態 600 過渡至狀態 601，進入點指令之位址須與所有的正確條件信號一併出現。次一出現位址須為次一序列指令之位址，以過渡至狀態 602，否則 SSM 即過渡至違反狀態 630。在一類似方法中，啟動序列之各位址均須出現，以過渡至狀態 602-615，且最終至安全模式狀態 620。在一條件信號中之錯誤位址、位址計時或錯誤變化，均將造成過渡至違反狀態 630，諸如弧線 601a 所示。類似地，若狀態信號指示任一啟動序列存取均為可快速緩衝儲存，則啟動序列會失敗。

在安全模式狀態 620 中，以及在有效檢測用以指示已進入安全記憶體之安全例行程序（ESA[SR]）之位址後，若以位於公用 ROM 內之 SSM 檢測出一位址，則 SSM 過渡回

五、發明說明（21）

到閒置模式 600，如弧線 621 所示。若以 ROM 或 SRAM 外之 SSM 檢測出一位址，或者若以受監視信號中之錯誤變化指示保全違反，則 SSM 過渡至違反狀態 630，如弧線 622 所示。

在啟動序列期間無需關閉指令快速緩衝儲存區；指令之不可快速緩衝儲存性即足以確保進入序列之健全。但使快速緩衝儲存區關閉將消弭根據快速緩衝儲存區清除機制之不當使用所為之侵入嘗試。

安全模式環境設定序列

復參閱圖 4，在步驟 526 中，藉由執行來自安全 ROM 之環境設定序列 414 而設定安全環境。此序列之目的在設定供安全碼執行用之適當環境。安全環境允許制動程式與資料快速緩衝儲存區、即時中斷及潛在之 MMU。這些步驟中之某一些特定針對安全模式操作，某些則係在呼叫啟動序列前正常應已為 OS 施行之操作。如前述，安全模式不能仰賴基本 OS 操作。因此，環境設定序列需施行部分背景切換操作如快速緩衝儲存區清除、TLB 清除等對安全模式完整性為基本者。

系統實施例

圖 6 闡釋在一行動電信裝置中實現本發明之積體電路之示例性施行，諸如行動個人數位助理（PDA）10，其具有顯示器 14 以及位於顯示器 14 周圍之整合輸入感測器 12a、12b。數位系統 10 包含如圖 1 之兆位單元 100，其經接合器（未圖示）連結至輸入感測器 12a、12b，作為 MPU

五、發明說明（22）

私人周邊 142 用。可利用尖筆或手指經輸入感測器 12a、12b 輸入資訊至 PDA。顯示器 14 經由類似於時框緩衝器 136 之局部時框緩衝器連結至兆位單元 100。顯示器 14 提供在疊置視窗如 MPEG 影像視窗 14a、共用文字文件視窗 14b 及三維遊戲視窗 14c 中之圖像與影像輸出。

射頻（RF）電路系統（未圖示）連結至天線 18，其為兆位單元 100 驅動作為 DSP 私人周邊 140 並提供無線網路鏈。接頭 20 連結至電纜接合器-數據機（未圖示），並自該處連結至兆位單元 100 作為 DSP 私人周邊 140，提供有線網路鏈供例如辦公室環境中靜態使用。短距無線鏈 23 亦"連結至"耳機 22，並為連結至兆位單元 100 作為 DSP 私人周邊 140 之低功率發射機（未圖示）所驅動。麥克風 24 亦以類似方式連結至兆位單元 100，因而得以利用麥克風 24 及無線耳機 22 與無線或有線網路上之其他用戶交換雙向聲音資訊。

兆位單元 100 對經由無線網路鏈及/或以有線為基之網路鏈傳送與接收之聲音與影像/圖像資訊提供所有的編碼與解碼。優點在於兆位單元 100 亦提供安全操作模式。如此處所述，安全模式指示器燈 30 受控於一閂鎖，其在兆位單元 100 正於安全模式下執行時，僅可由執行碼開啟之。安全模式指示器燈 30 藉以於安全時指示 PDA 10 之用戶，以提供在 PDA 上執行之應用之機密資料。在此方法中，PDA 10 對在行動電話環境內提出之電子商務（e-商務）及行動商務（m-商務）保全議題提供解決方法。

五、發明說明（23）

預期許多其他類型之通訊系統與電腦系統理當亦可自本發明獲益。此類其他電腦系統之實例包含可攜式電腦、智慧型電話、網路電話等。由於在桌上型與線供電（line-powered）電腦系統與微控制器應用中亦關心保全問題，尤以自可靠性觀點視之為最，故亦預期本發明有益於此類線供電系統。

數位系統100之製造包含將不同量雜質佈植於半導體基板以及將雜質擴散至基板內所選深度以形成電晶體裝置之多個步驟。形成罩以控制雜質位置。沉積與蝕刻多層導電性材料與絕緣性材料俾與各裝置互連。這些步驟係於清淨室環境下施行。

在資料處理裝置之生產成本中，測試所佔比重顯著。在晶圓形式下，將各裝置偏壓至操作狀態並針對基本操作功能做探針測試。接著將晶圓分割為個別方塊，可以裸晶粒或封裝後販售之。在封裝後，將完成部分偏壓至操作狀態並針對操作功能做測試。

此處所採用之術語"施加"、"連結"及"連接"係指電氣連結，包含附加構件在電器連接路徑中可能位置。"相關"係指控制關係，諸如受控於相關埠之記憶體資源。術語宣告、取消及無效係用以避免處理啟動高與啟動低信號之混合時之混淆。宣告係用以指示一信號呈現啟動或邏輯真。取消與無效係用以指示一信號呈現關閉或邏輯非。

數位系統因而具有以非侵入性方式內建於處理器系統上之安全模式（第三特權等級），該處理器系統包含一處理器

五、發明說明（24）

核心、指令與資料快速緩衝儲存區、寫入緩衝器及記憶體管理單元。安全執行模式位於一平台上，其中唯一信賴軟體為儲存於 ROM 中之碼。特別言之，OS 不受信賴，所有本質應用亦不受信賴。安全模式指示器係為告知用戶裝置處於安全模式用。

雖已參閱圖解實施例描述本發明，此描述並無因而限制之意。熟悉本技藝者，參閱此描述即可了解本發明之各種其他實施例。例如此處所述安全模式態樣均可用以改善所有處理器類型如精簡指令集運算（RISC）、複雜指令集運算（CISC）、寬字組、DSP 等。

在另一實施例中，可擴充安全環境以於數個起始器資源如 DSP 間共享安全資源。在此一實施例中，可以保全狀態引擎監視各指示器資源，以強制實施上述保全原理。

在各實施例中，可具有安全硬體之不同補充物，包含各周邊如監視計時器、加密/解密硬體加速器、隨機數產生器（RNG）等；以及各種 I/O 裝置如鍵盤、LCD、觸控螢幕等。

復參閱圖 1，在另一實施例中，第二 SSM 可位於 DSP 104 中，俾以處理器 102 上類似方式產生保全信號，供在 DSP 104 上執行之安全軟體層用。在此實施例中，可將匯流排版本之保全信號納入流量控制匯流排 110 中，俾使處理器 102 或 DSP 104 啟動之各項處置得以存取安全資源，諸如在依各 SSM 產生之保全信號之特定共享周邊 116。

復參閱圖 1，在另一實施例中，保全信號可能延伸超出

五、發明說明（25）

兆位單元 100，使得第三等級之資源得以在安全方式下操作。

啟動序列、環境設定序列及離開序列均可視各實施例之需求而變。例如不同的指令管線長度及不同的快速緩衝儲存區線長均需於啟動序列中變動。在另一實施例中，可將步驟 520 中施行之管家工作納入啟動序列中。

在另一實施例中，進入安全模式之手段可與此處所述 SSM 相異。只要一以任何手段獲得安全模式操作，即可存取僅當處於安全模式時可得之安全模式指示器，用以指示用戶系統係於安全模式下操作。

在另一實施例中，可提供 GPIO 閂鎖以外之手段，俾啟動安全模式指示器。例如可採用來自保全控制暫存器 319 之位元。類似地，可採用來自安全裝置 316a 或 316b 之一之位元。主要需求在於僅當在安全模式下可對手段進行存取。

在另一實施例中，安全模式指示器可直接響應於安全信號，使得安全模式指示器在處理器處於安全模式時全時啟動。但在此一實施例中，用戶可察知指示器處於開啟模式，因而欲略之，故此並非較佳實施例。

復參閱圖 2，安全裝置 316a 可為輸入裝置，用以接收來自用戶之機密資訊。如此一來，即可僅於系統在安全模下操作時，致動此輸入裝置以接收機密資訊。圖 2 欲顯示安全裝置係在晶片上。此並非對所有實施例均為必要之情況。亦可為晶片外裝置如獨立指印辨識裝置。對外部裝置之存取

五、發明說明（26）

在安全模式下可受限。典型而言，與安全外部裝置交換之資料，除加密者外，無需為機密資料。當操作裝置時，用戶可看到外部安全裝置。若該裝置無法於安全模式外之狀況下操作，則對駭客而言，更不易欺瞞用戶。

復參閱圖 2，可選擇性地提供竄改檢測裝置 380。來自竄改檢測裝置 380 之輸出 380.1 提供指示在包含 CPU 200 之封套上之存取封蓋已被竄改。接著以 SSM 300 監視信號 380.1，俾當檢測到竄改時，將不進入安全模式。類似地，若在發生竄改時處於安全模式下，則 SSM 300 檢測此經過信號 380.1，並離開安全模式指示違反，如前述。竄改檢測裝置亦可為外部晶片外裝置。可以 SSM 監視竄改檢測裝置之輸出或登入安全 GPIO。由於 GPIO 之存取受限於安全模式，使得駭客無法清除之。以此方式為之，安全軟體將於下次進入安全模式時看到。

因而將隨附之申請專利範圍視為涵蓋在本發明之真實範疇與精神下之實施例之任何此類改良。

圖式簡單說明

以上參閱隨附圖式，僅藉由實例描述依本發明之特殊實施例，其中所用類似代號係表類似部分，且除非另有描述，其中圖式均與圖1之數位系統有關，其中：

圖1係在具有多重處理器核心之兆位單元中之包含本發明之一實施例之數位系統之方塊圖；

圖2係在圖1之系統中之MPU方塊之方塊圖，其闡釋以選擇硬體方塊併同由安全狀態引擎（SSM）強化之受保護

五、發明說明（27）

軟體執行環境之組合之分散安全；

圖3係闡視圖2之ROM內容以及將該ROM分隔為公用部與安全部之電路之方塊圖；

圖4係闡釋進入圖2之系統之安全模式之操作之流程圖；

圖5係闡釋在圖2之系統中之安全狀態引擎之操作狀態圖；及

圖6闡釋包含本發明之一實施例之無線個人數位助理。

除另作指陳者外，不同圖表中對應之數字與符號係指對應部分。

圖式之代號說明

10	個人數位助理	12a,12b	整合輸入感測器
14	顯示器	14a	影像視窗
14b	共用文字文件視窗	14c	三維遊戲視窗
18	天線	20	接頭
22	耳機	23	無線鏈結
24	麥克風	30	安全模式指示器燈
100	兆位單元	102	微處理器
103	核心	104	數位信號處理器(DSP)
105	數位信號處理器核心	106	直接記憶體存取控制器
108	硬體加速器	110	流量控制方塊
113	記憶體方塊	116	共享週邊
120a	主處理器	120b	主介面
130	流量控制器	132	晶片外記憶體
134	晶片上記憶體	136	時框緩衝器
138	顯示裝置	140,142	私人週邊
150	保全狀態引擎（SSM）	152	保全信號

五、發明說明（28）

154	通用輸入/輸出（GPIO）閂鎖位元	155	保全指示器LED
156	週邊匯流排信號	200	中央處理單元(CPU)/處理器子系統
204	資料快速緩衝儲存器	206	指令快速緩衝儲存器
210	記憶體管理單元(MMU)	300	保全狀態引擎(SSM)
302	保全信號	304	違反信號
306	重置電路系統	310	安全唯讀記憶體(ROM)
311	公用唯讀記憶體(ROM)	312	安全靜態隨機存取記憶體(SRAM)
316a,316b	安全週邊裝置	318	通用輸入/輸出(GPIO)閂鎖
319	保全控制暫存器/安全模式指示器	321~327	進入條件信號
328	熔絲電路	330	指令匯流排
330a	指令位址匯流排	330b	指令匯流排
324	致動信號	326	裝置型信號
327	開機信號	331	指令介面信號
332	資料匯流排	333	資料介面信號
342	掃描閘	350	嵌入追蹤巨集單元
360	中斷操作器	362,363	中斷信號
364	整體遮蔽位元	370	解碼電路
370a	位址解碼器電路	380	竄改檢測裝置
380.1	信號	400	驅動器電路
404	閘電路	406	公用唯讀記憶體(ROM)編碼信號
407	安全唯讀記憶體(ROM)解碼信號	410	進入點

五、發明說明（29）

413	保全信號啟動序列	414	安全模式環境設定序列
416	安全碼	418	安全唯讀記憶體(ROM)離開序列
420	安全轉譯表（STT）	430	安全中斷向量表(SIVT)
500,502,504,510,512,514,516,520,522,524,526,528,528.1,528.2,528.3,528.4,530,540	步驟	542,601a,621,622	弧線
600	閒置狀態	601~605	狀態
620	安全模式狀態	630	違反狀態

（一）、本案指定代表圖：第4圖

（二）、本代表圖之元件代表符號簡單說明：

500,502,504,510,512,514,516,520,522,524,526,528 , 528.1,528.2, 528.3,528.4, 530,540	步驟

A5
B5

四、中文發明摘要（發明之名稱 智慧型電話或 PDA 之安全模式指示器 ）

本發明揭示一種數位系統，其具有以非侵入性方式建於處理器系統（10）之安全模式（特權等級第三級），該處理器系統（10）包含一處理器核心、指令與資料快速緩衝儲存區、一寫入緩衝器及一記憶體管理單元。安全執行模式因而位於一平台上，該平台之唯一信賴軟體係儲存於唯讀記憶體（ROM）中之碼。特別言之，不信賴作業系統（OS），且不信賴所有的本質應用(14a、 14b、14c)。而係經由獨特進入點進入安全模式。以出/入條件之完整硬體評估，即可動態出入安全執行模式。提供安全模式指示器（30）以告知數位系統用戶，裝置處於安全模式。此指示器可為例如小型發光二極體（LED）。若安全模式指示器並未啟動，用戶不應輸入任何私密資訊（密碼），或不應對螢幕上顯示之任何東西簽署。

英文發明摘要（發明之名稱：SECURE MODE INDICATOR FOR SMART PHONE OR PDA）

A digital system is provided with a secure mode (3rd level of privilege) built in a non-invasive way on a processor system (10) that includes a processor core, instruction and data caches, a write buffer and a memory management unit. A secure execution mode is thus provided on a platform where the only trusted software is the code stored in ROM. In particular the OS is not trusted, all native applications (14a, 14b, 14c) are not trusted. The secure mode is entered through a unique entry point. The secure execution mode can be dynamically entered and exited with full hardware assessment of the entry/exit conditions. A secure mode indicator (30) is provided to tell a user of the digital system that the device is in secure mode. This indicator may be a small LED, for example. The user should not enter any secret information (password) or should not sign anything displayed on the screen if the secure mode indicator is not active.

六、申請專利範圍

1. 一種操作一數位系統之方法，包括步驟：

提供僅可執行信賴程式碼之安全模式操作；及

提供一該數位系統之用戶可見之安全模式指示器手段，其中僅可於該安全模式操作下以該信賴程式碼啟動該指示器手段。

2. 如申請專利範圍第1項之方法，進一步包括步驟：

執行一應用程式；

進入該安全模式操作以執行該應用程式之安全部分；

響應於該應用程式之該安全部分，啟動該安全模式指示器手段；及

在啟動該指示器手段之同時，要求一用戶提供機密資訊予該應用程式之該安全部分。

3. 如申請專利範圍第2項之方法，進一步包括在接收該機密資訊後，在該應用程式之該安全部分持續於安全模式下執行時，關閉該安全模式指示器手段之步驟。

4. 如申請專利範圍第2項或第3項之方法，其中啟動該安全模式指示器手段之步驟包括執行一寫入一記憶體映對閂鎖之指令，其中僅當在該安全模式操作下執行該指令時，可寫入該記憶體映對閂鎖。

5. 如申請專利範圍第1項至第4項中任一項之方法，其中提供一安全模式操作之步驟進一步包括步驟：

跳至位於一指令記憶體中之特定位址處之進入位址；

自該進入位址開始執行一啟動序列指令；及

僅當由中央處理單元（CPU）於一預定順序充分執行

六、申請專利範圍

之該啟動序列指令處時，進入該安全模式操作。

6. 如申請專利範圍第1項至第5項中任一項之方法，進一步包括提供竄改檢測手段之步驟，以檢測該數位系統是否遭竄改；及

其中，若該竄改檢測手段指示該數位系統已遭竄改，則禁止提供一安全模式操作之步驟。

7. 一種數位系統，包括：

一用以執行指令之中央處理單元（CPU）；

一連結至一該CPU之指令匯流排之用以保存非安全指令之公用記憶體，該CPU隨時可進入該公用記憶體；

一連結至該CPU之該指令匯流排之用以保存安全指令之安全記憶體，僅當宣告一保全信號時，始可存取該安全記憶體；

保全電路，其具有一輸出，俾於建立一安全模式操作時，用以宣告該保全信號；及

一響應於該保全信號之安全模式指示器，一該數位系統之用戶可看到該安全模式指示器，其中僅可在宣告該保全信號時，藉由執行一指令使該安全模式指示器處於一啟動模式下。

8. 如申請專利範圍第7項之數位系統，其中該安全模式指示器包括：

一連結之記憶體映對閂鎖，以響應於一寫入指令而自該CPU接收一資料位元信號，該記憶體映對閂鎖之操作受控於該保全信號，使得僅當宣告該保全信號時，始寫入該記

六、申請專利範圍

憶體映對閂鎖，該記憶體映對閂鎖具有一輸出信號，以指示該閂鎖之狀態；及

一安全模式指示器裝置，其連結至該記憶體映對閂鎖之該輸出信號，該安全模式指示器裝置係響應於該閂鎖之狀態，其中該安全模式指示器裝置係一燈，或一可指示開啟狀態或關閉裝置之機械裝置，或一可指示開啟狀態或關閉裝置之聲音裝置。

9. 如申請專利範圍第7項或第8項之數位系統，進一步包括用以檢測之竄改手段，其可操作以指示是否該數位系統已遭竄改，其中該保全電路監視該用以檢測竄改之手段，並可操作以避免響應於該用以檢測竄改之手段而建立一安全操作模式。

10.如申請專利範圍第7-9項中任一項之數位系統係一無線裝置，進一步包括：

一經一鍵盤轉接器連結至該CPU之整合鍵盤；

一經一顯示器轉接器連結至該CPU之顯示器；

連結至該CPU之射頻（RF）電路系統；及

一連結至該RF電路系統之天線；及

其中該安全模式指示器包括一與該顯示器安排在視距範圍內之發光二極體（LED）。

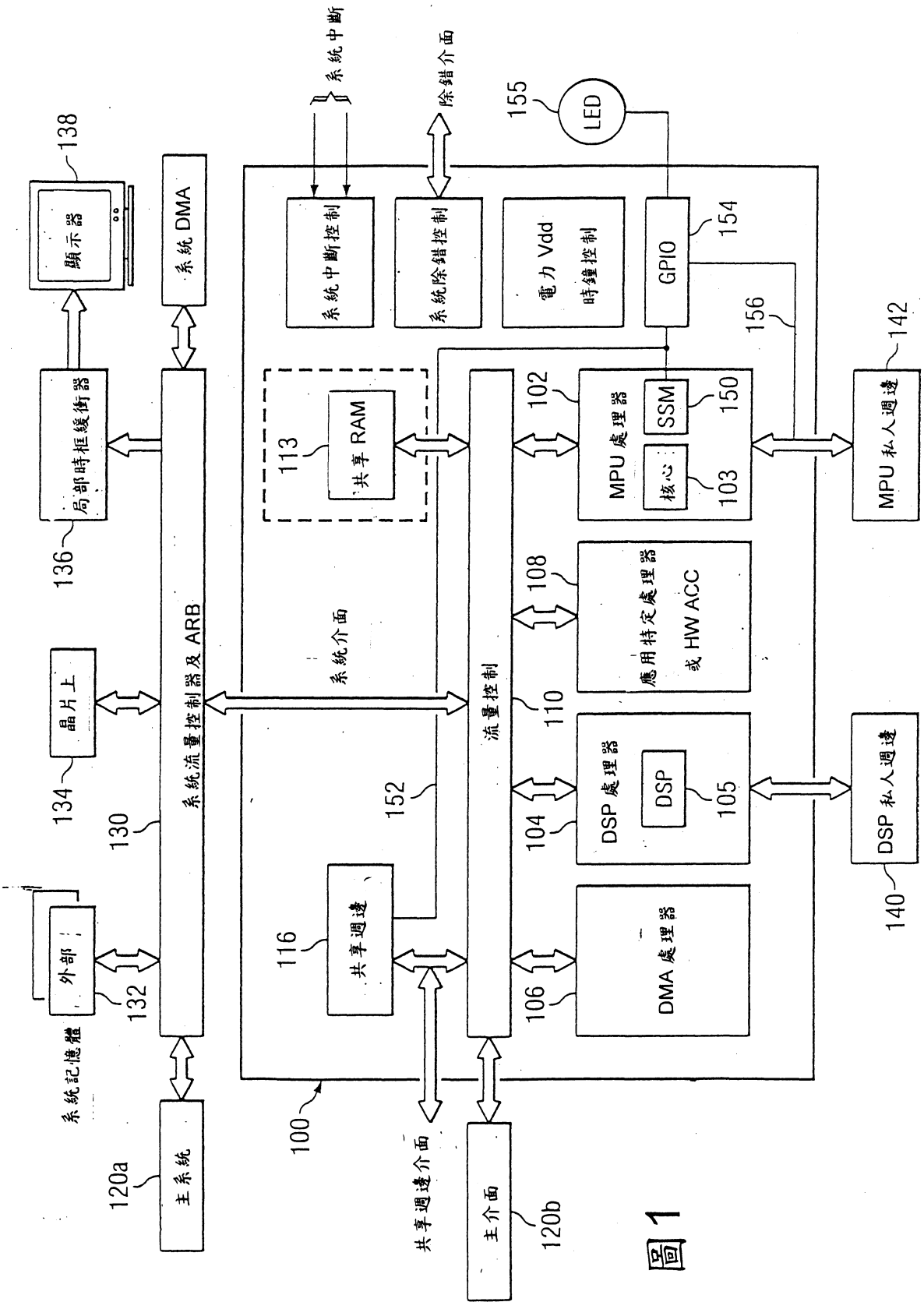

顯示器
138
系統 DMA
局部時框緩衝器
136
晶片上
134
外部
132
系統記憶體
130
系統流量控制器及 ARB
主系統
120a
100
共享通達介面
主介面
120b
系統中斷
除錯介面
系統中斷控制
系統除錯控制
電力 Vdd
時鐘控制
LED
155
GPIO
154
156
113
共享 RAM
系統介面
流量控制
102
MPU 處理器
核心
103
SSM
150
MPU 私人通達
142
108
應用特定處理器
或 HW ACC
110
152
DSP 處理器
DSP
105
104
DSP 私人通達
140
116
共享通達
106
DMA 處理器

圖 1

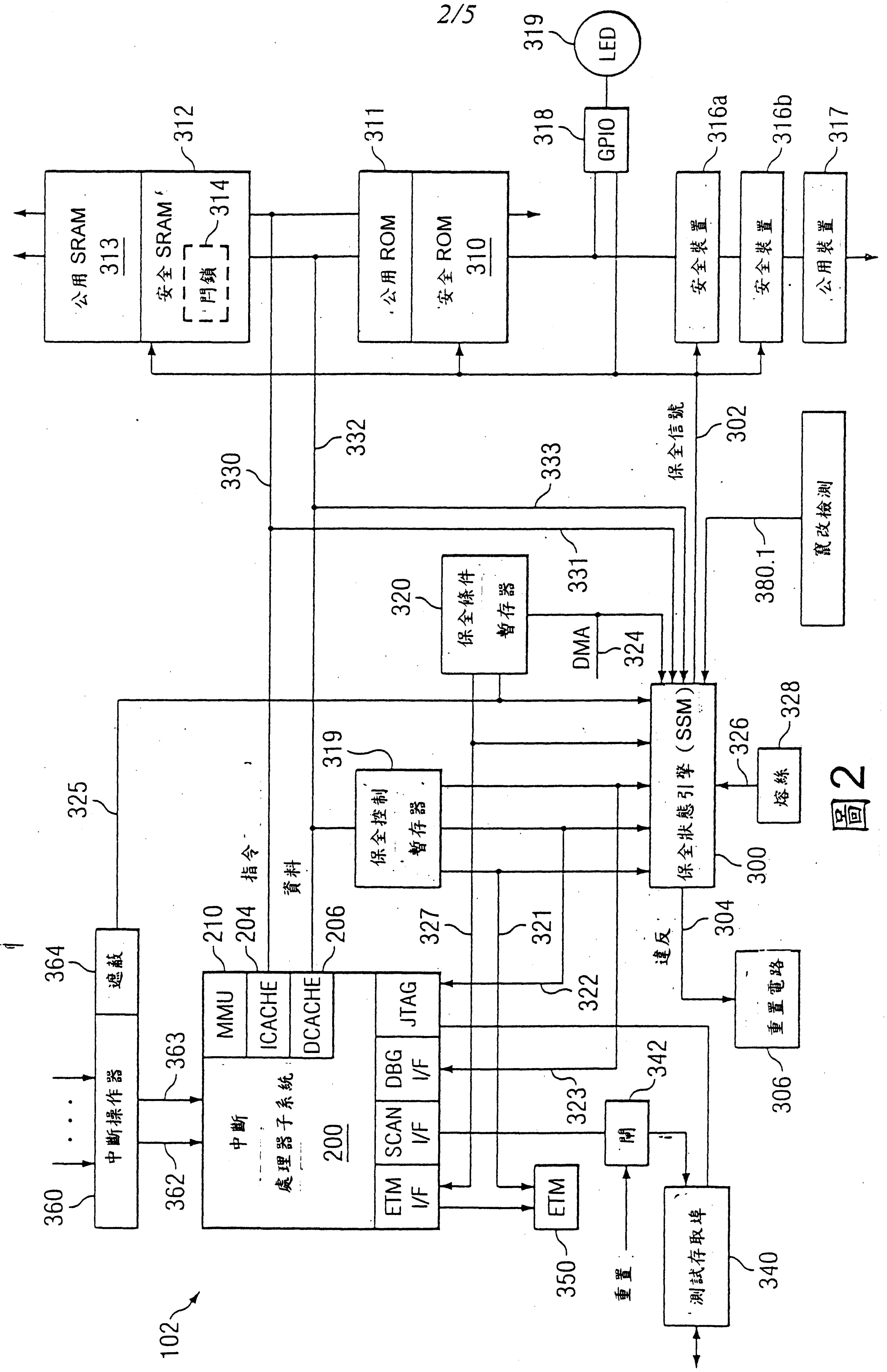

公用 SRAM 313
安全 SRAM 314
門鎖
312
公用 ROM
安全 ROM 310
311
GPIO 318
LED 319
安全裝置 316a
安全裝置 316b
公用裝置 317
保全信號 302
330
332
333
331
竄改檢測 380.1
保全條件暫存器 320
DMA 324
保全狀態引擎（SSM）300
熔絲 328
326
保全控制暫存器 319
325
指令
資料
MMU 210
ICACHE 204
DCACHE 206
327
321
322
323
違反 304
重置電路 306
遮蔽 364
中斷操作器 360
363
362
中斷處理器子系統 200
JTAG
DBG I/F
SCAN I/F
ETM I/F
閘 342
ETM 350
重置
測試存取埠 340
102

圖2

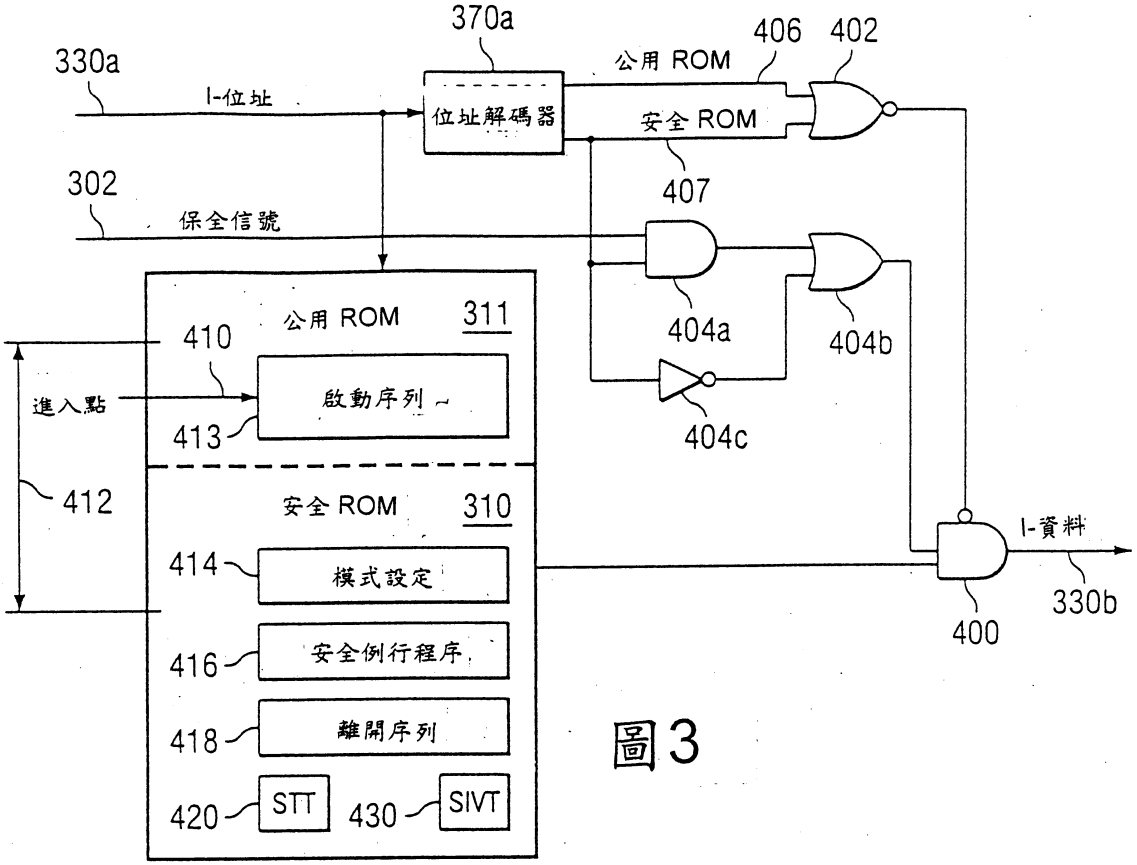

370a
406
402
330a
I-位址
位址解碼器
公用 ROM
安全 ROM
407
302
保全信號
404a
404b
404c
公用 ROM
311
410
啟動序列
進入點
413
412
安全 ROM
310
414
模式設定
416
安全例行程序
418
離開序列
420
STT
430
SIVT
I-資料
330b
400

圖3

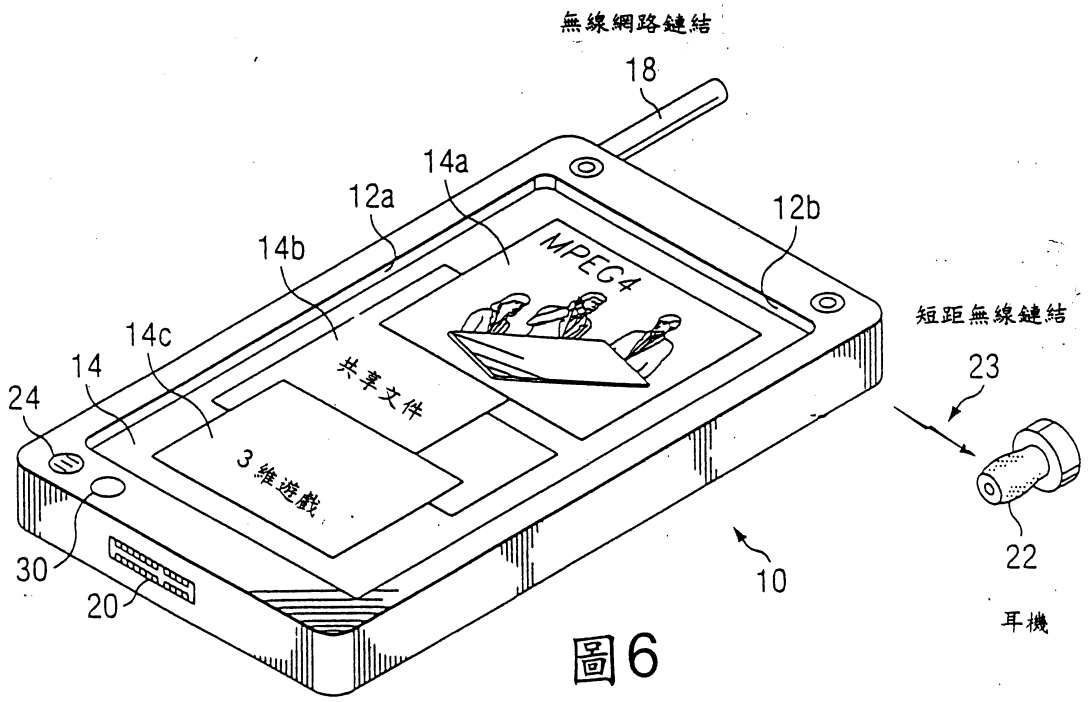

無線網路鏈結
18
14a
12a
12b
14b
MPEG4
14c
14
24
共享文件
3維遊戲
短距無線鏈結
23
22
30
20
10
耳機

圖6

圖4

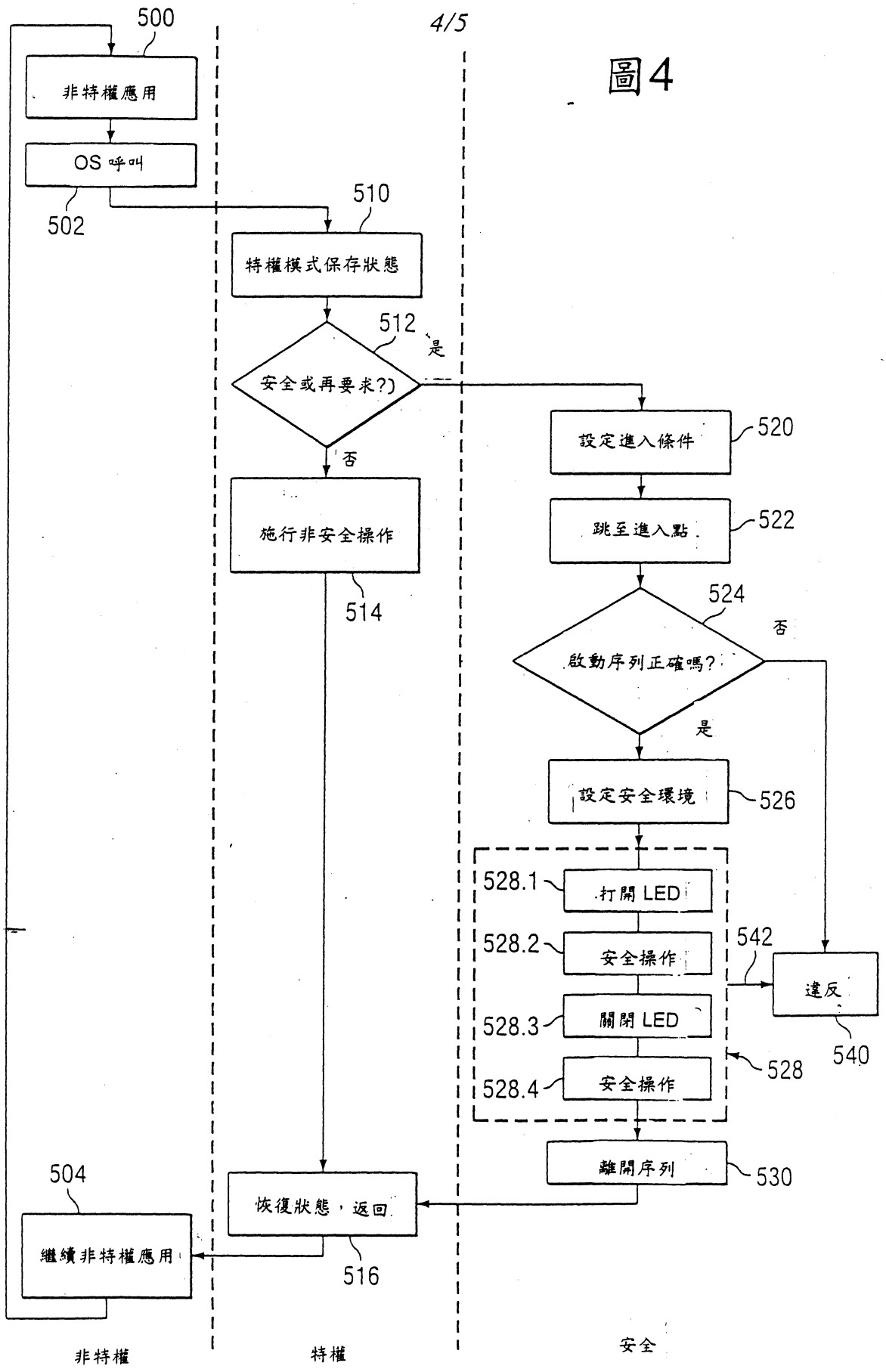
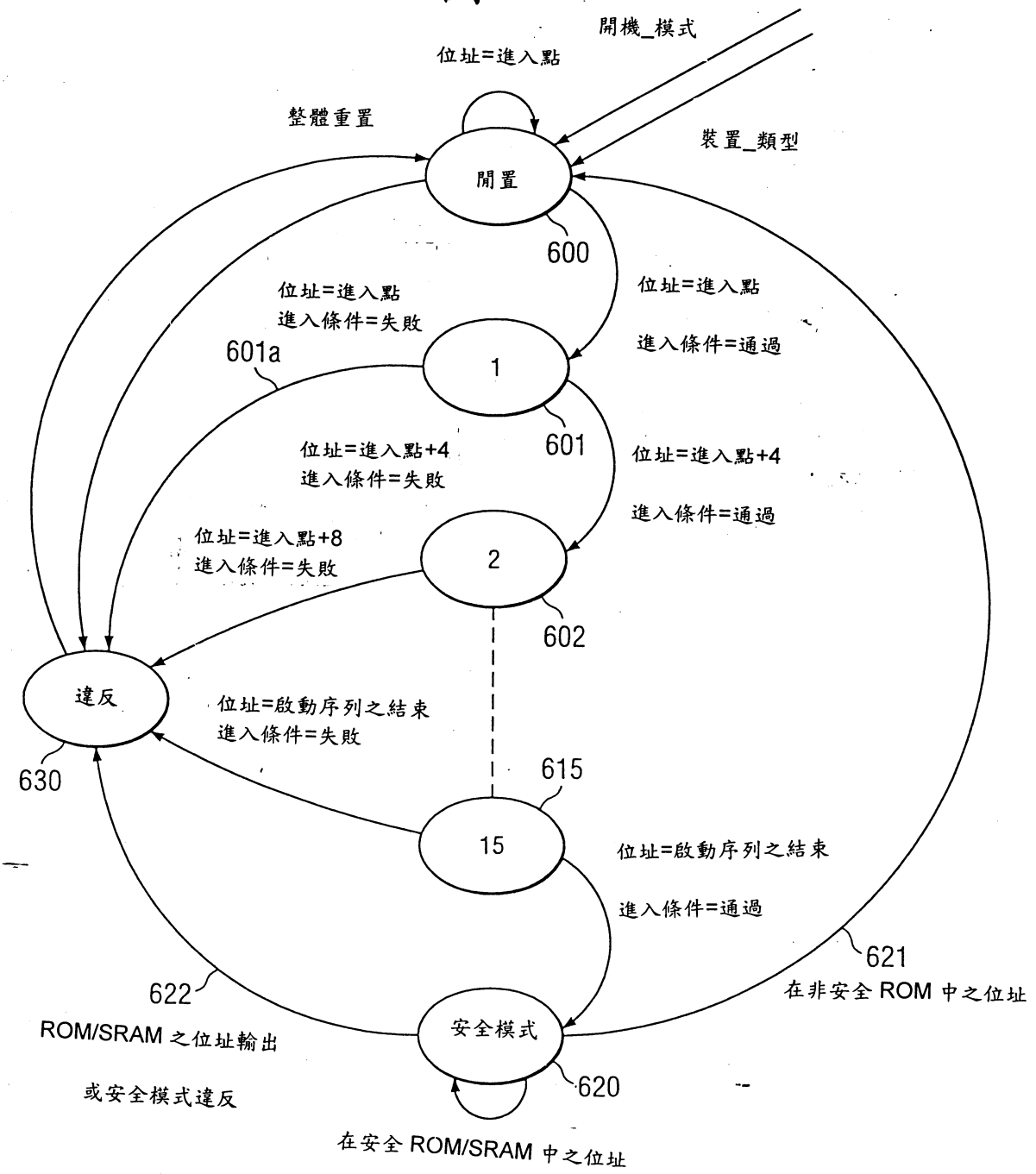

500
非特權應用
OS 呼叫
502
510
特權模式保存狀態
512
安全或再要求?)
是
否
施行非安全操作
514
設定進入條件
520
跳至進入點
522
524
啟動序列正確嗎?
否
是
設定安全環境
526
528.1
打開 LED
528.2
安全操作
542
違反
528.3
關閉 LED
540
528.4
安全操作
528
離開序列
530
504
恢復狀態，返回
繼續非特權應用
516
非特權
特權
安全

圖5


開機_模式
位址=進入點
整體重置
裝置_類型
閒置
600
位址=進入點
進入條件=失敗
601a
1
601
位址=進入點
進入條件=通過
位址=進入點+4
進入條件=失敗
位址=進入點+4
進入條件=通過
位址=進入點+8
進入條件=失敗
2
602
違反
630
位址=啟動序列之結束
進入條件=失敗
615
15
位址=啟動序列之結束
進入條件=通過
621
在非安全 ROM 中之位址
622
ROM/SRAM 之位址輸出
或安全模式違反
安全模式
620
在安全 ROM/SRAM 中之位址

(一)、本案指定代表圖爲：第 4 圖

(二)、本代表圖之元件代表符號簡單說明：

500,502,504,510,512,514,516,520, 522,524,526,528, 528.1,528.2, 528.3,528.4, 530,540	步驟

本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無