I431533

附件 3A: 第 096118973 號中文說明書修正頁

民國 100 年 3 月 29 日修正

(此處由本局於收文時黏貼條碼)

852535 本

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：096118973

※申請日期：96 年 05 月 28 日　　※IPC 分類：G06F 9/46

一、發明名稱：

(中) 微處理器系統及用以初始化安全操作之方法與處理器

(英) Microprocessor system, methods and processor for initiating secure operations

二、申請人：(共 1 人)

1.姓　名：(中) 英特爾股份有限公司
(英) INTEL CORPORATION
代表人：(中) 1.大衛　賽門
(英) 1.SIMON, DAVID
地　址：(中) 美國加州聖大克拉瑞密遜學院路２２００號
(英) 2200 Mission College Blvd., Santa Clara, CA 95052, USA
國籍：(中英) 美國　　U.S.A.

三、發明人：(共 2 人)

1.姓　名：(中) 莎瑪那　戴塔
(英) DATTA, SHAMANNA
國　籍：(中) 美國
(英) U.S.A.

2.姓　名：(中) 莫漢　庫瑪
(英) KUMAR, MOHAN
國　籍：(中) 印度
(英) INDIA

四、聲明事項:

◎本案申請前已向下列國家（地區）申請專利☐主張國際優先權：
【格式請依：受理國家（地區）；申請日；申請案號數　順序註記】
1.美國　　；2006/05/26；11/442,230 ☑有主張優先權

附件 3A: 第 096118973 號中文說明書修正頁
民國 100 年 3 月 29 日修正

五、中文發明摘要

發明之名稱：微處理器系統及用以初始化安全操作之方法與處理器

本發明說明了用來初始化微處理器系統中之安全作業之方法及裝置。在一實施例中，一系統包含：一處理器，用以執行一安全進入指令；以及一晶片組，用以在該安全進入指令的執行期間使該系統進入一靜止狀態。

六、英文發明摘要

發明之名稱：

Microprocessor system, methods and processor for initiating secure operations

Methods and apparatus for initiating secure operations in a microprocessor system are described. In one embodiment, a system includes a processor to execute a secured enter instruction, and a chipset to cause the system to enter a quiescent state during execution of the secured enter instruction.

七、指定代表圖：

（一）、本案指定代表圖為：第（ 4 ）圖

（二）、本代表圖之元件代表符號簡單說明：無

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

九、發明說明

【發明所屬之技術領域】

本發明係大致有關微處理器系統，尤係有關可在可信賴或安全環境中操作之微處理器系統。

【先前技術】

由於愈來於多的金融及個人交易係在本地或與端的微處理器上執行，所以已促進了建立“可信賴的”或“安全的”微處理器環境。這些環境嘗試解決的問題在於隱私的喪失或資料被篡改或濫用。使用者不希望其私人資料被公開。使用者也不希望其資料被更改或被用於不適當之交易。這些狀況的例子包括醫療記錄的非故意外流或線上銀行或其他存款機構的資金之電子盜取。同樣地，內容提供者嘗試保護數位內容(例如，音樂、其他音訊、視訊、或其他一般類型的資料)不會受到未經授權的複製。

現有的可信賴系統可使用一整組封閉的可信賴的軟體。此種方法較易於實施，但有不容許同時使用常見的可自市場購得的作業系統之缺點。該缺點限制了此種可信賴系統的接受度。

其他的方法要求系統使其各處理器經由一匯流排而相互連接。

【發明內容】

本發明說明了用來初始化微處理器系統中之安全作業

之方法及裝置。在一實施例中，一系統包含：一處理器，用以執行一安全進入指令；以及一晶片組，用以在該安全進入指令的執行期間使該系統進入一靜止狀態。

【實施方式】

下文的實施方式說明了用來初始化微處理器系統中之可信賴或安全環境之技術。在下文的說明中，可能述及諸如邏輯實施例、軟體模組配置、加密技術、匯流排信令(signaling)技術、以及作業細節等的許多特定細節，以便提供對本發明的更徹底之了解。然而，對此項技術具有一般知識者將可了解：可在沒有這些特定細節之情形下實施本發明。在其他的情形中，並未詳細示出控制結構、閘層級的電路、以及完整的軟體指令序列，以便不會模糊了本發明。對此項技術具有一般知識者在參閱本發明中包含的說明之後，將可在無須過度實驗之情形下實施適當的功能。係以一微處理器系統之形式揭示本發明。然而，亦可以諸如數位信號處理器、迷你電腦、或大型主機電腦等的其他形式實施本發明。

現在請參閱第1圖，圖中示出在一微處理器系統中執行之一例示軟體環境。第1圖所示之該軟體不是可信賴的(不可信賴的)。當在一高特權等級中作業時，作業系統(150)的大小及持續之更新使其難以用及時之方式執行任何信賴分析。作業系統的大部分係處於特權級別(ring)零(0)內，亦即，處於最高特權等級。應用軟體(152)、(154)

、及(156)具有低許多的特權，且通常係處於特權級別三(3)之內。由於存在有不同的特權級別，且作業系統(150)以及應用軟體(152)、(154)、及(156)被隔離在這些不同的特權級別，所以看來根據決定信賴作業系統(150)所提供的能力，將可使第1圖所示之軟體在一可信賴的模式下操作。然而，實際上，作出此種信賴決定經常是不切實際的。產生該問題的因素包括作業系統(150)的大小(程式碼的行數)、作業系統(150)可能是許多更新(新的程式碼模組及修補程式)的接收者之此一事實、以及作業系統(150)也可能包含並非作業系統開發者的各方所供應的諸如裝置驅動程式等的程式碼模組之此一事實。作業系統(150)可以是諸如Microsoft® Windows®、Linux、或 Solaris®等常見的作業系統，或者可以是任何其他適當的習知或可取得之作業系統。應用軟體或作業系統的特定類型或名稱不是緊要的。

現在請參閱第2圖，圖中示出根據本發明的一實施例之某些例示可信賴或安全的軟體模組以及例示系統環境(200)。在第2圖所示之實施例中，係將處理器(202)、處理器(212)、處理器(222)、以及或有的其他處理器(圖中未示出)示爲獨立的硬體實體。雖然第2圖示出三個處理器，但是本發明之實施例可包含任何數目的處理器，其中包括單一的處理器。

系統(200)亦包含晶片組(240)，晶片組(240)可包括輸入／輸出(I/O)控制器或控制中心、以及將於下文中述及

的任何其他的系統或其他的邏輯。其他實施例可包括用來取代或增添到第2圖所示組件之其他組件，且處理器或其他組件的數目可以是不同的，且該等處理器及其他組件間之相互配置也可以是不同的。

處理器(202)、(212)、及(222)可包含諸如核心(203)、(205)、(213)、(215)、(223)、及(225)等的一或多個執行核心。在某些實施例中，可以在一或多個實體處理器或核心中執行的各別的硬體執行緒(execution thread)取代該等處理器或核心。這些執行緒擁有額外的實體處理器之許多屬性。爲了在解說使用了多個實體處理器及在處理器上的多個執行緒之任何混合情形時有一般性之詞語，可將詞語“邏輯處理器”用來描述實體處理器或在一或多個實體處理器中操作之執行緒。因此，可將單一執行緒式處理器視爲一邏輯處理器，並可將多執行緒式或多核心處理器視爲多個邏輯處理器。

處理器(202)、(212)、及(222)亦可包含諸如非核心邏輯(201)、(211)、及(221)等的“非核心邏輯”，其中非核心邏輯是與任何執行核心分離的邏輯。非核心邏輯可包括諸如可被用來儲存與其所在的處理器有關的資訊之暫存器(207)、(217)、及(227)等的暫存器或任何其他儲存位置。此種暫存器或儲存位置可以是可程式的或硬編碼的，且此類資訊可包括對應的處理器中包含的核心及(或)邏輯處理器之數目。暫存器(207)、(217)、及(227)可以是於開機重定期間被更新的標準全域記憶體映射式暫存器。

處理器(202)、(212)、及(222)亦可包含用來支援安全或可信賴作業之某些特殊電路或邏輯元件。例如，處理器(202)可包含安全進入(SENTER)邏輯(204)，用以支援可初始化可信賴作業的特殊SENTER指令之執行。處理器(202)亦可包含互連訊息邏輯(206)，用以在支援特殊SENTER作業時支援各處理器與其他組件間之特殊互連訊息。使用特殊互連訊息時，因數項原因而可增加該系統的安全或可信賴性。諸如處理器(202)、(212)、及(222)或晶片組(240)等的電路元件在其包含本發明揭示的實施例的適當邏輯元件之情形下，可只發出或回應此種訊息。因此，特殊互連訊息的成功交換可協助確保適當的系統組態設定。特殊互連結構訊息亦可容許諸如重定一平台組態設定暫存器(278)等的正常應被禁止的活動。只容許回應特殊安全指令而發出特殊互連結構訊息，而可降低可能有敵意的不可信賴的程式碼暗中監視某些互連結構交易之能力。可使用其中包括邏輯電路、微碼、及韌體之習知的方法實施SENTER邏輯(204)、互連訊息邏輯(206)、以及本發明的實施例中使用的任何其他邏輯。

此外，處理器(202)可包含用來支援安全初始化作業之安全記憶體(208)。在一實施例中，安全記憶體(208)可以是處理器(202)之或許在一特殊模式下工作的一內部快取記憶體。在替代實施例中，安全記憶體(208)可以是特殊記憶體。諸如處理器(212)及處理器(222)等的其他處理器亦可包含SENTER邏輯(214)、(224)、匯流排訊息邏輯

(216)、(226)、以及安全記憶體(218)、(228)。

可將“晶片組”定義爲用來支援被連接的一或多個處理器的記憶體及(或)I/O作業之一組電路及邏輯。可將一晶片組的一些個別元件聚集在一單一晶片或一對對晶片中，或分散在其中包括處理器的多個晶片中。在第2圖所示之實施例中，晶片組(240)可包含用來支援處理器(202)、(212)、及(222)的I/O作業之電路及邏輯，而每一處理器包含用來支援記憶體作業之電路及邏輯。或者，晶片組(240)亦可包含用來支援處理器(202)、(212)、及(222)的記憶體作業之電路及邏輯。在替代實施例中，可將晶片組(240)的功能分配到一或多個實體裝置中。

晶片組(240)又可包含其本身的互連訊息邏輯(242)，用以在支援特殊SENTER作業時支援PTP結構(230)上之特殊互連訊息。某些這種特殊互連訊息可包括：將一金鑰暫存器(244)的內容傳輸到一處理器(202)、(212)、及(222)；容許一處理器設定或清除一特殊“靜止”指示器(246)，以便讓晶片組(240)使系統(200)進入或退出靜止狀態(將於下文中說明其中情形)；或容許一處理器檢查一特殊“靜止狀態”旗標(248)。匯流排訊息邏輯(242)的一額外功能是可將系統(200)中各處理器的存在或參與資訊登記在一“存在”暫存器(270)。

可經由點對點(PTP)互連結構(230)而使處理器(202)、(212)、及(222)相互連接，被連接到晶片組(240)，且被連接到任何其他組件或代理器(agent)。處理器(202)、(212)

、及(222)、以及晶片組(240)可分別包含介面單元(209)、(219)、(229)、及(239)，用以連接到PTP結構(230)，且用以在各處理器及晶片組之間以及與系統(200)中存在或參與的任何其他代理器之間進行訊息的傳輸及接收。介面單元(209)、(219)、(229)、及(239)中之每一介面單元可包含任何數目的單向及(或)雙向埠，用以與任何數目的其他組件通訊。可根據諸如分層點對點互連架構而經由PTP結構(230)進行通訊，其中包括代表訊息及(或)資料的信號之封包被鏈結層、協定層、路由層、傳輸層、實體層、以及任何此種層中之任一層或所有層組成訊框，且係自一代理器傳輸到另一代理器(點對點)。因此，介面單元(209)、(219)、(229)、及(239)中之每一介面單元可包含用來產生與每一層對應的信號之電路或邏輯。該等封包亦可包含用於偵錯或改錯的冗餘資訊或其他資訊。

包含一或多個平台組態設定暫存器(PCR)(278)、(279)的符記(276)可被連接到PTP結構(230)。在一實施例中，符記(276)可包含特殊安全功能，且在一實施例中可包含由信賴運算平台聯盟(Trusted Computing Platform Alliance；簡稱TCPA)於2001年12月1日發佈的TCPA Main Specification 1.1a 版(可自www.trustedpc.com取得)中揭示之可信賴平台模組(Trusted Platform Module；簡稱TPM)(281)。

系統環境(200)中被識別的兩個軟體組件是一安全虛擬機器監視器(SVMM)(282)模組以及一安全初始化驗證程

式碼(Secure Initialization Authenticated Code；簡稱SINIT-AC)(280)模組。SVMM(282)可被儲存在系統磁碟或其他大量儲存裝置中，且可視需要而被移到或複製到其他位置。在一實施例中，在開始該安全進入程序之前，可先將SVMM(282)移到或複製到系統(200)中之一或多個記憶體分頁。在該安全進入程序之後，可產生一虛擬機器環境，其中SVMM(282)可以該系統內的最高特權等級程式碼之方式工作，且可將SVMM(282)用來允許或拒絕所產生的該虛擬機器內之作業系統或應用軟體對某些系統資源的直接使用。

該安全進入程序所需的某些行動可能超出了簡單硬體實施例之範圍，且可代之有利地使用其執行可被默認信賴之軟體模組。在一實施例中，可由安全初始化(SINIT)程式碼執行這些行動。一例示行動可能要求代表該系統組態的關鍵性部分之各控制被測試，以便確保該組態支援該安全環境的正確實體化。第二例示行動可能要計算並登記SVMM(282)模組的身分，並將系統控制轉移給該SVMM(282)模組。此處，“登記”意指將SVMM(282)的信賴量測值放置到一暫存器或其他儲存位置，例如，將SVMM(282)的信賴量測值放置到PCR(278)或PCR(279)。當採取該第二行動時，可能的系統使用者可檢查SVMM(282)的可信賴度。

處理器或晶片組的製造商可產生該SINIT程式碼。因此，該SINIT程式碼可被信賴，而協助晶片組(240)的安全

啓動。爲了配送該SINIT程式碼，在一實施例中，係由整個SINIT程式碼構成一習知的密碼雜湊值(cryptographic hash)，而產生了被稱爲摘要(digest)的一值。一實施例產生用於該摘要的160位元之值。然後可以在一實施例中爲處理器的製造商持有的一私密金鑰(private key)將該摘要加密，以便形成一數位簽章。當將該SINIT程式碼與對應的數位簽章放在一起時，可將該組合稱爲安全初始化驗證程式碼(SINIT-AC)(280)。以後可以下文中所述之方式確認SINIT-AC(280)的拷貝。

SINIT-AC(280)可被儲存在系統磁碟或其他大量儲存裝置中，或被儲存在固定媒體中，且可視需要而被移到或複製到其他位置。在一實施例中，在開始該安全進入程序之前，可先將SINIT-AC(280)移到或複製到系統(200)的一或多個記憶體分頁，以便形成常駐在記憶體中之一SINIT-AC拷貝。

在系統(200)中執行的諸如作業系統等的任何有特權之軟體可在一邏輯處理器上啓動該安全進入程序，此時可將該邏輯處理器稱爲啓動邏輯處理器(ILP)。在本例子中，處理器(202)是該ILP，但是PTP結構(230)上的任何處理器都可以是該ILP。此時，並不將SINIT-AC(280)的常駐記憶體的拷貝或SVMM(282)的常駐記憶體的拷貝視爲可被信賴的。

該ILP(處理器(202))執行一特殊指令，以便啓動該安全進入程序。可將該特殊指令稱爲安全進入(SENTER)指

令，且可由SENTER邏輯(204)支援該SENTER指令。該SENTER指令可先證實系統(200)中之每一邏輯處理器都被登記在晶片組(240)中，例如，被登記在存在暫存器(270)中。每一處理器以及被連接到PTP結構(230)的其他代理器包含諸如暫存器(207)、(217)、及(227)等的暫存器或其他儲存位置，用以指示該系統包含的邏輯處理器之數目。讀取這些暫存器，以便證實晶片組(240)中準確地代表了系統拓撲。

在該證實之後，該SENTER指令寫到靜止指示器(246)，以便由晶片組(240)使系統(200)進入靜止狀態。晶片組(240)開始PTP結構(230)上的一交握(handshake)序列，以便使一處理器(靜止狀態主控處理器)之外的所有處理器及PTP結構(230)上的其他代理器都進入靜止狀態。在該實施例中，處理器(202)是靜止狀態主控處理器以及ILP。該靜止序列可包括：將一"STOP_REQ"信號傳送到每一非主控處理器，以便使該等非主控處理器結束其事件處理，空出其緩衝器，並將一"STP-ACK"信號傳送回晶片組(240)，以便確認該等非主控處理器已進入靜止狀態。靜止狀態是一種處理器不執行任何指令而且不在PTP結構(230)上產生任何交易之狀態。在晶片組(240)自代表晶片組(240)中登記的每一邏輯處理器之每一代理器接收一STOP_ACK信號之後，靜止狀態旗標(248)可被設定。

在該系統進入靜止狀態之後，SENTER指令可以下文所述之方式安全地執行一或多個安全模組。爲達到此一目

的，PTP結構(230)仍然處於工作狀態，且靜止狀態主控處理器仍然可使用TPM(281)。在完成了該一或多個安全模組的執行之後，該靜止狀態主控處理器可清除靜止指示器(246)，以便讓晶片組(240)使系統(200)退出靜止狀態。

爲了執行該一或多個安全模組，該ILP(處理器(202))可先將SINIT-AC(280)及金鑰(284)的一份拷貝移到安全記憶體(208)，以便進行驗證並隨後執行SINIT-AC(280)中包含的SINIT程式碼。在一實施例中，該安全記憶體(208)可以是該ILP(處理器(202))之或許在一特殊模式下工作的一內部快取記憶體。金鑰(284)代表與用來將SINIT-AC(280)模組中包含的數位簽章加密的私密金鑰對應之公開金鑰，且金鑰(284)被用來證實該數位簽章，且因而驗證該SINIT程式碼。在一實施例中，金鑰(284)可或許以SENTER邏輯(204)的一部分之方式已被儲存在處理器中。在另一實施例中，金鑰(284)可被儲存在晶片組(240)的一唯讀金鑰暫存器(244)，且由該ILP讀取金鑰(284)。在又一實施例中，該處理器或該晶片組的金鑰暫存器(244)都可實際存放金鑰(284)的一密碼摘要，而金鑰(284)本身則被包含在SINIT-AC(280)模組中。在該最後一個實施例中，該ILP自金鑰暫存器(244)讀取該摘要，經由SINIT-AC(280)中嵌入的金鑰(284)計算出一等效的密碼雜湊值，並比較該等兩個摘要，以便確保所供應的金鑰(284)是確實可信賴的。

SINIT-AC的一份拷貝以及公開金鑰的一份拷貝此時可存在於安全記憶體(208)中。該ILP現在可使用公開金鑰

的該拷貝將SINIT-AC的該拷貝中包含的數位簽章解密，而確認該SINIT-AC的該拷貝。該解密產生了密碼雜湊值的摘要之一原始拷貝。如果新產生的摘要與該原始的摘要相符，則可將SINIT-AC的該拷貝及其包含的SINIT程式碼視爲可信賴的。

該ILP現在可以將於下文中概述之方式，將該SINIT-AC模組的密碼摘要值寫到安全符記(276)中之一平台組態設定暫存器(272)，而登記該SINIT-AC模組的唯一身分。現在可將執行控制轉移到該ILP的安全記憶體(208)內存放的SINIT程式碼之可信賴的拷貝，而終止該ILP對其SENTER指令的執行。該可信賴的SINIT程式碼然後可執行其系統測試及組態設定行動，且可根據前文所述“暫存器”的定義而登記SVMM的常駐記憶體的拷貝。

可以數種方式執行SVMM的常駐記憶體的拷貝之登記。在一實施例中，在該ILP上執行的該SENTER指令將所計算出的SINIT-AC之摘要寫到安全符記(276)內之PCR(278)。然後，該可信賴的SINIT程式碼可將所計算出的常駐記憶體的SVMM之摘要寫到相同的PCR(278)、或安全符記(276)內之另一PCR(279)。如果該SVMM摘要被寫到相同的PCR(278)，則安全符記(276)計算原始內容(SINIT摘要)與新值(SVMM摘要)間之雜湊值，並將結果寫回到PCR(278)。在第一次(初次)寫到PCR(278)限於SENTER指令的實施例中，可將所產生的摘要用來作爲該系統的信賴根源(root of trust)。

一旦該可信賴的SINIT程式碼完成了其執行，且將SVMM的身分登記在一PCR之後，該SINIT程式碼可將ILP執行控制轉移到該SVMM。在一典型的實施例中，該ILP所執行的第一SVMM指令可代表該SVMM的自行初始化常式。系統(200)然後可以將於下文中參照第3圖所概述之方式，在SVMM的現在執行拷貝之監督下，於可信賴的模式下操作。自此時點之後，整體系統係以將於下文中參照第3圖所概述之方式，於可信賴的模式下操作。

現在請參閱第3圖，圖中示出根據本發明的一實施例的一例示可信賴或安全的軟體環境。在第3圖所示之實施例中，可信賴的及不可信賴的軟體可同時被載入，且可同時在一單一電腦系統中執行。一SVMM(350)選擇性地容許或禁止一或多個不可信賴的作業系統(340)及不可信賴的應用軟體(310-330)直接使用硬體資源(380)。在該環境中，“不可信賴的”並不必然意指作業系統或應用軟體有蓄意的不當行爲，而是意指：由於交互影響的程式碼之大小及多樣化，使得可靠地斷言該軟體具有所需的行爲且並無介入該軟體執行的病毒或其他外來程式碼是不切實際的。在一典型的實施例中，該不可信賴的程式碼可能包含被設置在目前的個人電腦中之正常的作業系統及應用軟體。

SVMM(350)亦選擇性地容許或禁止一或多個可信賴或安全的核心(360)及一或多個可信賴的應用軟體(370)直接使用硬體資源(380)。該可信賴或安全的核心(360)可能在大小及功能上有所限制，以便支援對該核心執行信賴性分

析的能力。可信賴的應用軟體(370)可以是考在安全環境中執行的任何軟體碼、程式、常式、或常式組。因此，可信賴的應用軟體(370)可以是各種應用軟體或程式碼序列，或者可以是諸如Java程式等的較小的應用軟體。

SVMM(350)可對被作業系統(340)或核心(360)正常執行的且可能改變系統資源保護或特權之指令或作業預設陷阱(trap)，且可選擇性地容許、部分地容許、或拒絕該等指令或作業。舉例而言，在一典型的實施例中，SVMM(350)將對要改變處理器的分頁表(正常係由作業系統(340)或核心(360)執行此動作)之指令取代性地預設陷阱，因而將確保該要求不會嘗試改變其虛擬機器的領域以外之分頁特權。

現在請參閱第4圖，圖中示出根據本發明的方法(400)的一實施例的軟體及其他程序步驟之一流程圖。

在方法(400)之步驟(410)中，一邏輯處理器使SINIT-AC及SVMM模組的拷貝可爲後續的SENTER指令所使用。在該例子中，一LIP將SINIT-AC及SVMM程式碼自大量儲存裝置載入實體記憶體。在替代實施例中，不只該ILP，任何邏輯處理器都可執行上述步驟。在步驟(412)中，一處理器執行SENTER指令，而成爲ILP。

在步驟(420)中，該SENTER指令證實系統(200)中之每一邏輯處理器被登記在晶片組(240)中，例如，被登記在存在暫存器(270)中。在步驟(422)中，該SENTER指令寫到靜止指示器(246)，以便讓晶片組(240)使系統(200)進入靜

止狀態。在步驟(424)中，晶片組(240)將“STOP_REQ”信號傳送到每一非主控處理器，以便使該等非主控處理器：結束其事件處理，清空其緩衝器，並將一“STOP_ACK”信號傳送回晶片組(240)，以便確認該等非主控處理器已進入靜止狀態。在步驟(426)中，設定靜止狀態旗標(248)，以便指示晶片組(240)已自代表在晶片組(240)中登記的每一邏輯處理器之每一代理器接收一STOP_ACK信號。

在步驟(430)中，該ILP將該晶片組的公開金鑰以及SINIT-AC的常駐記憶體之拷貝移到其本身的安全記憶體，以便進行安全執行。在步驟(432)中，該ILP將該金鑰用來驗證SINIT-AC的該常駐記憶體之拷貝，然後執行SINIT-AC的該常駐記憶體之拷貝。執行SINIT-AC時，可執行對系統組態及SVMM拷貝之測試，然後登記SVMM的身分，且最後開始步驟(434)中對SVMM的執行。在步驟(436)中，該靜止狀態主控處理器清除靜止指示器(246)，以便讓晶片組(240)在步驟(438)中使系統(200)退出靜止狀態。

在前文的說明書中，已參照本發明的一些特定實施例而說明了本發明。然而，在不脫離最後的申請專利範圍中述及的本發明的廣義精神及範圍下，顯然可可對本發明作出各種修改及改變。因此，應將本說明書及各圖式視爲舉例而非限制。

【圖式簡單說明】

各附圖以舉例而非限制之方式示出本發明，在該等附

圖中，相同的代號參照到類似的元件，其中：

第1圖示出在一微處理器系統中執行之一例示軟體環境。

第2圖示出根據本發明的一實施例之某些例示可信賴或安全的軟體模組以及例示系統環境。

第3圖示出根據本發明的一實施例的一例示可信賴或安全的軟體環境。

第4圖是根據本發明的一方法實施例的軟體及其他程序步驟之一流程圖。

【主要元件符號說明】

150,340：作業系統

152,154,156,310,320,330,370：應用軟體

200：系統

202,212,222：處理器

240：晶片組

201,211,221：非核心邏輯

204,214,224：安全進入邏輯

206,216,226,242：互連訊息邏輯

272,278,279：平台組態設定暫存器

208：安全記憶體

230：點對點結構

244：金鑰暫存器

246：靜止指示器

248：靜止狀態旗標

270：存在暫存器

209,219,229,239：介面單元

276：符記

281：可信賴平台模組

282,350：安全虛擬機器監視器

280：安全初始化驗證程式碼

284：金鑰

380：硬體資源

360：可信賴或安全的核心

101年9月18日
修正本

民國 101 年 9 月18 日修正

十、申請專利範圍

1. 一種微處理系統，包含：

一晶片組，包括一靜止指示器；以及

一第一處理器，用以執行一安全進入指令，係藉由寫到該靜止指示器以使該晶片組在該安全進入指令的執行期間靜止該系統。

2. 如申請專利範圍第 1 項之系統，進一步包含一點對點結構，用以將該第一處理器耦合到該晶片組。

3. 如申請專利範圍第 2 項之系統，進一步包含被該點對點結構耦合到該晶片組之一第二處理器，其中該晶片組也用以在該安全進入指令的執行期間靜止該第二處理器。

4. 如申請專利範圍第 2 項之系統，其中該晶片組也用以使該系統進入只有該第一處理器與該晶片組經由該點對點結構通訊之該靜止狀態。

5. 如申請專利範圍第 1 項之系統，進一步包含一可信賴平台模組，其中該第一處理器在該靜止狀態期間可存取該可信賴平台模組。

6. 如申請專利範圍第 1 項之系統，其中該第一處理器也用以執行一安全初始化驗證程式碼模組。

7. 如申請專利範圍第 1 項之系統，其中該第一處理器也用以執行一安全虛擬機器監視模組。

8. 如申請專利範圍第 3 項之系統，其中：

該晶片組包含：

一第一儲存位置，用以指示該系統中之每一處理器的身分；

該第二處理器包含一第二儲存位置，用以指示該第二處理器被連接到該點對點結構；以及

該第一處理器包含用以驗證之邏輯，該邏輯在存取該指示器而讓該晶片組靜止該系統之前，先驗證該第一儲存位置中指示該第二處理器之身分。

9. 一種用以初始化安全操作之方法，包含下列步驟：

開始在經由一點對點結構被耦合到一代理器之一第一處理器中執行一安全進入指令；以及

該第一處理器寫到該代理器中之靜止指示器使該代理器在該安全進入指令的執行期間靜止被耦合到該點對點結構之一第二處理器。

10. 如申請專利範圍第 9 項之方法，進一步包含下列步驟：該晶片組維護被耦合到該點對點結構的其他晶片組之一清單。

11. 如申請專利範圍第 10 項之方法，進一步包含下列步驟：讀取該第二處理器中之一儲存位置，以便識別經由該第二處理器而被耦合到該點對點結構的代理器之數目。

12. 如申請專利範圍第 9 項之方法，進一步包含下

列步驟：該第一處理器在該靜止狀態期間存取一可信賴平台模組。

13. 如申請專利範圍第 12 項之方法，進一步包含下列步驟：執行一安全初始化驗證模組。

14. 如申請專利範圍第 13 項之方法，進一步包含下列步驟：讀取該晶片組中之一靜止指示器，以便證實在執行該安全初始化驗證模組之前已進入了該靜止狀態。

15. 如申請專利範圍第 12 項之方法，進一步包含下列步驟：執行一安全虛擬機器監視模組。

16. 如申請專利範圍第 15 項之方法，進一步包含下列步驟：讀取該晶片組中之一靜止指示器，以便證實在執行該安全虛擬機器監視模組之前已進入了該靜止狀態。

17. 如申請專利範圍第 9 項之方法，進一步包含下列步驟：在進入該靜止狀態之前，使該第二處理器結束其事件處理並清空其緩衝器。

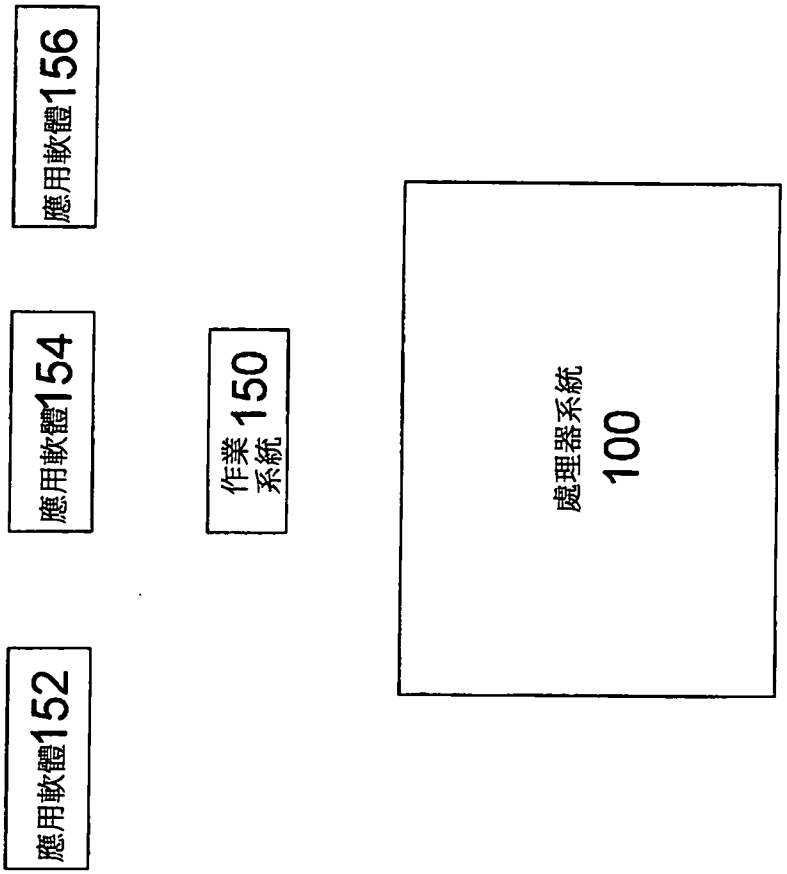
18. 如申請專利範圍第 17 項之方法，進一步包含下列步驟：該第二處理器將一信號傳送到該晶片組，以便確認其進入該靜止狀態。

19. 一種用以初始化安全操作之處理器，包含：

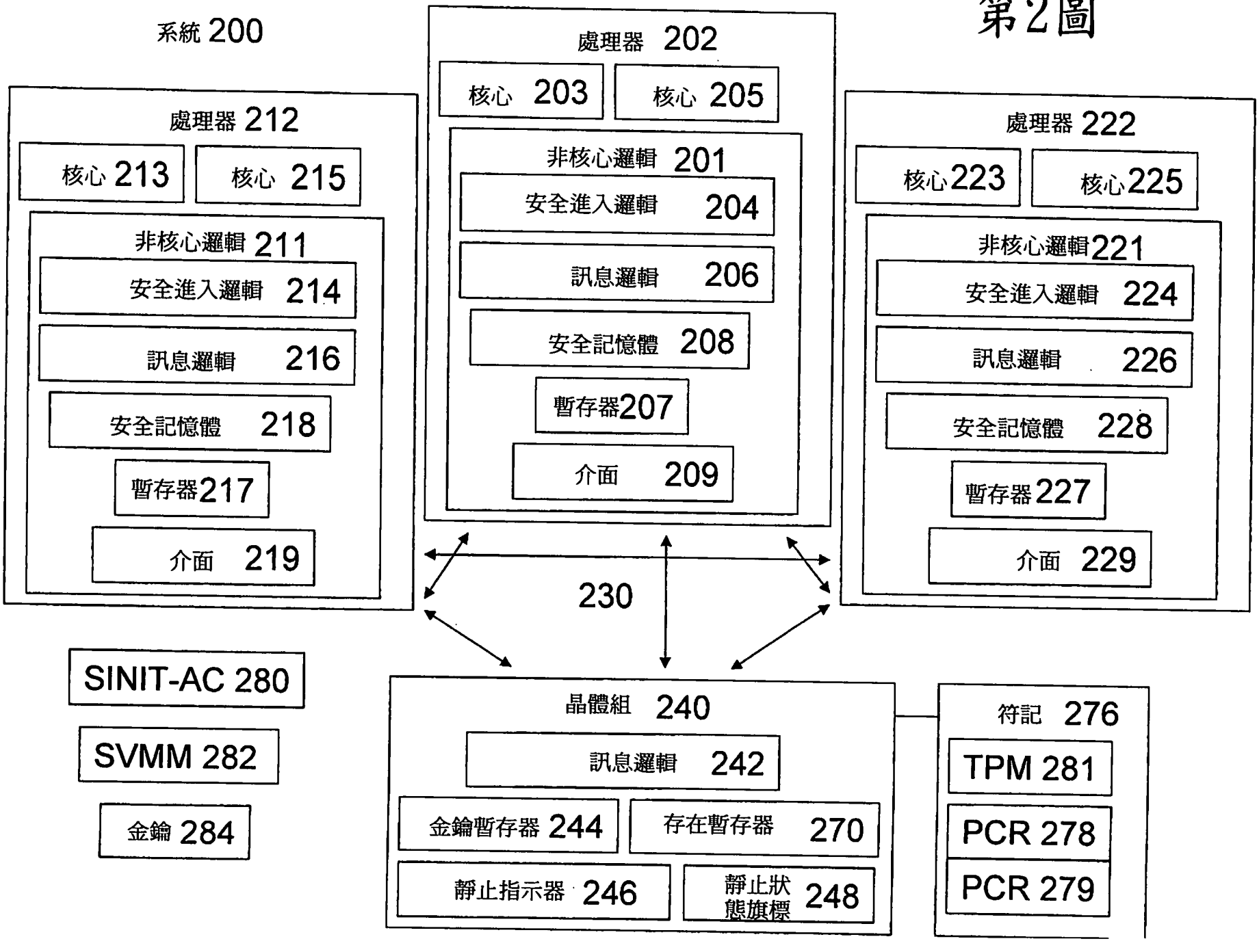
安全進入邏輯，用以執行啓用安全作業初始化之一第一指令；以及

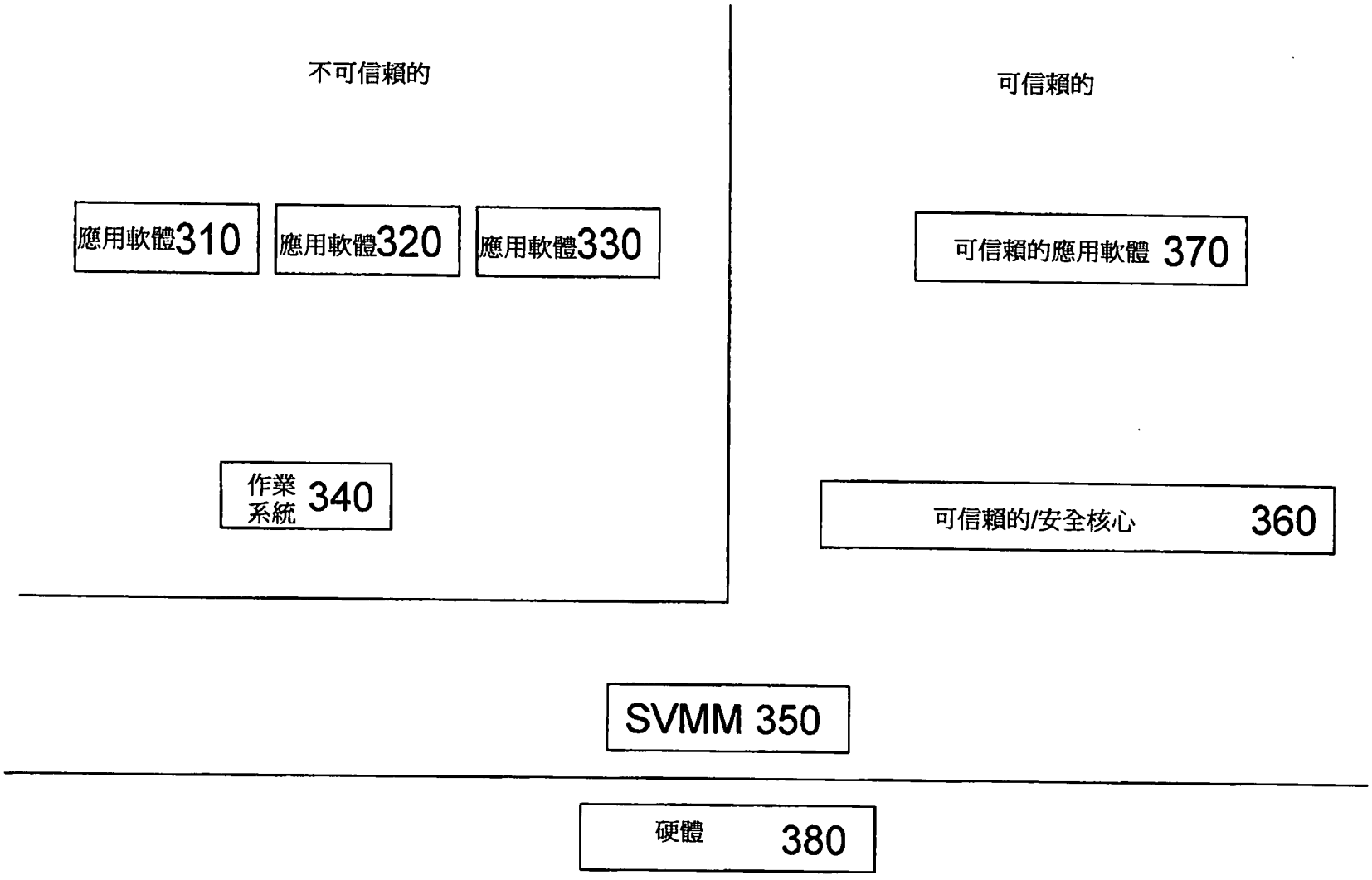
互連訊息邏輯，用以寫到第一代理器中之靜止指示器以使該第一代理器經由一點對點結構靜止被耦合到該第一代理器之一第二代理器。

第1圖



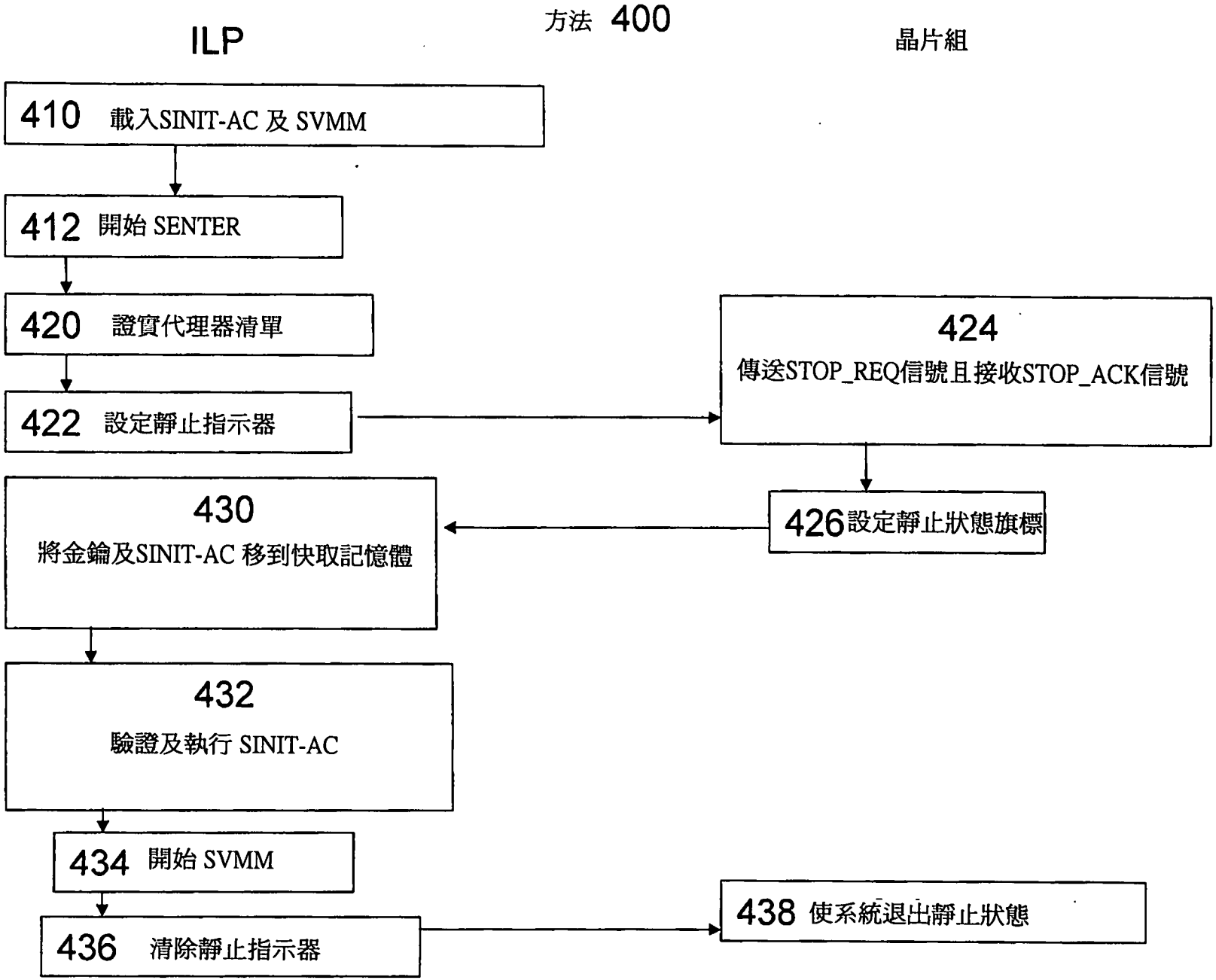
第2圖


系統 200
處理器 212
核心 213
核心 215
非核心邏輯 211
安全進入邏輯 214
訊息邏輯 216
安全記憶體 218
暫存器217
介面 219
處理器 202
核心 203
核心 205
非核心邏輯 201
安全進入邏輯 204
訊息邏輯 206
安全記憶體 208
暫存器207
介面 209
處理器 222
核心223
核心225
非核心邏輯221
安全進入邏輯 224
訊息邏輯 226
安全記憶體 228
暫存器227
介面 229
230
SINIT-AC 280
SVMM 282
金鑰 284
晶體組 240
訊息邏輯 242
金鑰暫存器 244
存在暫存器 270
靜止指示器 246
靜止狀態旗標 248
符記 276
TPM 281
PCR 278
PCR 279


不可信賴的
可信賴的
應用軟體310
應用軟體320
應用軟體330
可信賴的應用軟體 370
作業系統 340
可信賴的/安全核心 360
SVMM 350
硬體 380

第3圖

第4圖


方法 400
ILP
晶片組
410 載入SINIT-AC 及 SVMM
412 開始 SENTER
420 證實代理器清單
422 設定靜止指示器
424
傳送STOP_REQ信號且接收STOP_ACK信號
426設定靜止狀態旗標
430
將金鑰及SINIT-AC 移到快取記憶體
432
驗證及執行 SINIT-AC
434 開始 SVMM
436 清除靜止指示器
438 使系統退出靜止狀態