(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201212037 A1
(43)公開日： 中華民國 101 (2012) 年 03 月 16 日

(21)申請案號：100125648 (22)申請日： 中華民國 100 (2011) 年 07 月 20 日
(51)Int. Cl.： *G11C29/42 (2006.01)* *G06F12/16 (2006.01)*
(30)優先權：2010/07/26 美國 12/843,617
(71)申請人：英特爾公司 (美國) INTEL CORPORATION (US)
美國
(72)發明人：史溫森 羅伯特C SWANSON, ROBERT C. (US)；威哈吉 艾瑞克R WEHAGE, ERIC R. (US)；利姆 文森特J ZIMMER, VINCENT J. (US)；布魯旭 麥可 BULUSU, MALLIK (IN)
(74)代理人：惲軼群；陳文郎
申請實體審查：無 申請專利範圍項數：20 項 圖式數：9 共 37 頁

(54)名稱

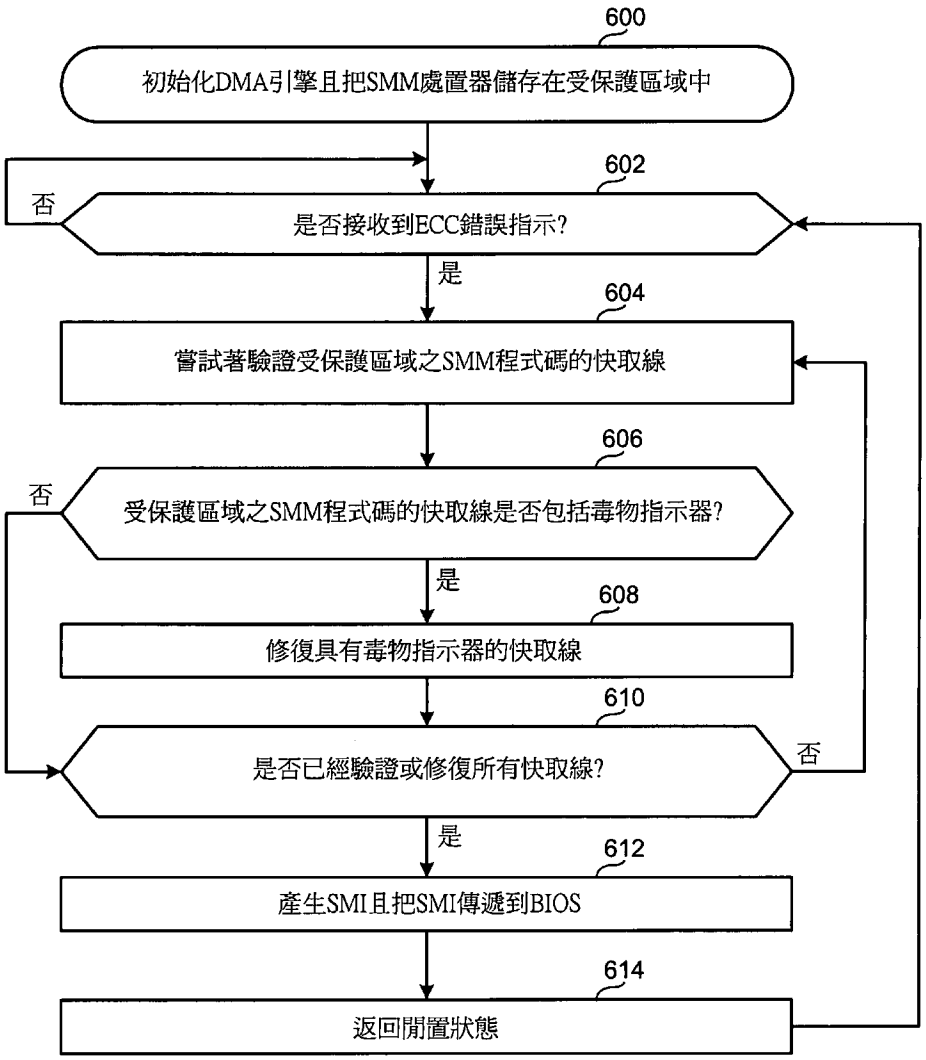
用以保護記憶體之區段的方法及裝置

METHODS AND APPARATUS TO PROTECT SEGMENTS OF MEMORY

(57)摘要

本發明揭露用以保護記憶體區段的方法與裝置。一種例示方法包括下列步驟：攔截表示一錯誤的一中斷請求；判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及響應於驗證該受保護記憶體區域的步驟，產生一中斷，該中斷致能利用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

600~614：步驟方塊


600
初始化DMA引擎且把SMM處置器儲存在受保護區域中
602
否
是否接收到ECC錯誤指示?
是
604
嘗試著驗證受保護區域之SMM程式碼的快取線
606
否
受保護區域之SMM程式碼的快取線是否包括毒物指示器?
是
608
修復具有毒物指示器的快取線
610
是否已經驗證或修復所有快取線?
否
是
612
產生SMI且把SMI傳遞到BIOS
614
返回閒置狀態

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201212037 A1
(43)公開日： 中華民國 101 (2012) 年 03 月 16 日

(21)申請案號：100125648 (22)申請日： 中華民國 100 (2011) 年 07 月 20 日
(51)Int. Cl.： *G11C29/42 (2006.01)* *G06F12/16 (2006.01)*
(30)優先權：2010/07/26 美國 12/843,617
(71)申請人：英特爾公司 (美國) INTEL CORPORATION (US)
美國
(72)發明人：史溫森 羅伯特C SWANSON, ROBERT C. (US)；威哈吉 艾瑞克R WEHAGE, ERIC R. (US)；利姆 文森特J ZIMMER, VINCENT J. (US)；布魯旭 麥可 BULUSU, MALLIK (IN)
(74)代理人：惲軼群；陳文郎
申請實體審查：無 申請專利範圍項數：20 項 圖式數：9 共 37 頁

(54)名稱

用以保護記憶體之區段的方法及裝置

METHODS AND APPARATUS TO PROTECT SEGMENTS OF MEMORY

(57)摘要

本發明揭露用以保護記憶體區段的方法與裝置。一種例示方法包括下列步驟：攔截表示一錯誤的一中斷請求；判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及響應於驗證該受保護記憶體區域的步驟，產生一中斷，該中斷致能利用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

六、發明說明：

【發明所屬之技術領域】

發明的技術領域

本發明係大致有關電腦系統平台的技術領域，且更確切來說，本發明係有關用以保護記憶體區段的方法與裝置。

【先前技術】

發明的技術背景

運算平台典型地包括在類型、大小、用途等方面可能不同的多個記憶體區段。與一第一記憶體結合儲存的一第一部件(例如，一使用者應用程式或程式)可能仰賴與一第二記憶體結合儲存的一第二部件(例如，一作業系統)，以適切地操作及/或進行操作(例如，在該第二部件無法操作的狀況下，而該第一部件無法受到初始化時)。因此，儘管需要額外的必需資源，某些記憶體類型或記憶體區段擔保一或多個保護機構、程式、常式、或裝置，其確保儲存在其中的一或多個部件能適當地操作。

【發明內容】

發明的概要說明

依據本發明之一實施例，係特地提出一種用以保護一運算平台中之一記憶體區段的方法，其包含下列步驟：攔截表示一錯誤的一中斷請求；判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及響應於驗證該受保護記憶體區

域的步驟，產生一中斷，該中斷致能利用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

圖式的簡要說明

第1圖以方塊圖展示出一種例示運算平台的例示部件，包括一例示保護機構。

第2圖為第1圖之該產生描述符的一例示實行方案。

第3圖為第1圖之該驗證描述符的一例示實行方案。

第4圖為第1圖之該修復描述符的一例示實行方案。

第5圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示BIOS，以執行一種例示開機自我測試(POST)。

第6圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示保護機構，以保護第1圖之例示SMRAM的一區域。

第7圖展示出受第1圖之該例示保護機構之一第一演算法保護之第1圖的該等程式碼區塊。

第8圖展示出受第1圖之該例示保護機構之一第二演算法保護之第1圖的該等程式碼區塊。

第9圖以方塊圖展示出一種例示處理器系統，其可用來執行第2圖的該等機器可讀指令及/或實行第1圖的該例示運算平台。

【實施方式】

較佳實施例的詳細說明

雖然以下說明揭露了例示方法、裝置、系統、及/或製造物品，包括在硬體上執行的韌體及/或軟體等，應該要注意的是，該等方法、裝置、系統、及/或製造物品僅為展示性的，且不應該被視為具有限制性。例如，所闡述的是，該等韌體、硬體、及/或軟體部件中的任一個或全部可獨佔式地體現於硬體中、獨佔式地體現於軟體中、獨佔式地體現於韌體中，或者可體現於硬體、軟體、及/或韌體的任何組合中。因此，儘管以下說明解說了例示方法、裝置、系統、及/或製造物品，本發明備置的實例並不是實行該等方法、裝置、系統、及/或製造物品的唯一方式。

本文所述的該等例示方法、裝置、系統、及/或製造物品針對一記憶體區段以及儲存在其中之任何程式碼及/或資料提供保護功能。針對展示目的且不具限制性，係在本文中結合主機動態隨機存取記憶體(DRAM)來說明該等例示方法、裝置、系統、及/或製造物品。尤其，本文所述的該等實例包含保護儲存在主機DRAM中的一錯誤處置系統。然而，本文所述的該等實例可結合儲存在主機DRAM中之不同類型的系統、機構、程式、裝置等來實行。例如，除了本文中所述對該錯誤處置系統提供的保護功能以外，或替代該種保護功能，本文所述的該等例示方法、裝置、系統、及/或製造物品可結合儲存在主機DRAM中而與圖形UMA (統一記憶體架構)相關的一可執行程式來實行、可結合儲存在主機DRAM中而與一電力管理單元(PMU) (例

如，MID上的8051程式碼)相關的一可執行程式來實行、及/或可結合儲存在主機DRAM中的任何其他部件、單元、機構、程式等來實行。再者，本文所述之該等例示方法、裝置、系統、及/或製造物品所提供的記憶體保護功能可結合除了主機DRAM以外的額外或替代類型或記憶體區段來實行。

習知運算平台包括錯誤校正碼(ECC)與記憶體保護單元，其用以回應於不欲、非預期、及/或無法令人接受的事件或與其相關聯的狀況，例如與一處理器或記憶體相關聯的操作。例如，在x86平台中，基本輸入/輸出系統(BIOS)使用一種系統管理模式(SMM)，其可透過一系統管理中斷(SMI)來喚起。與一SMM相關聯的部件係典型地儲存在主機DRAM的一區段中，其有時稱為系統管理隨機存取記憶體(SMRAM)。例如，SMRAM典型地包括一SMM處置器，該處置器具有受組配成能校正一運算平台中之一或多種錯誤類型的程式碼。

某些錯誤可能會影響或毀損該DRAM的區段，且依次地影響或毀損該SMM處置器及/或與該BIOS SMM相關聯的其他部件。在該種狀況下(例如，當一錯誤已經在該SMM處置器中發生時)，於SMM中執行的該BIOS可導致該處理器的毀損，其會導致一種完全關機狀況。因此，在先前系統中，記憶體保護單元典型地實行額外錯誤處置器以管理該種錯誤。例如，某些記憶體保護單元針對會毀損該SMRAM的錯誤在基板管理控制器(BMC)中使用一錯誤處置器，進

而使用專屬的額外資源來處置錯誤。

大致上，本文所述的該等例示方法、裝置、系統、及/或製造物品保護一處理器，使其免於遭受到在該SMRAM之一SMM區域中發生的一ECC錯誤。換言之，本文所述的該等實例令該BIOS能響應於一ECC錯誤而使用SMM部件(例如，該SMM處置器)來執行一中斷常式，即使是該ECC錯誤或另一種先前錯誤已經影響了與該SMM有關的程式碼。為了能對一錯誤進行校正，本文所述的該等實例把該SMRAM中的一受保護位址空間組配成能儲存該SMM處置器。再者，本文所述的該等實例提供一種硬體式保護機構，其用以攔截可能會觸發該BIOS於SMM模式中執行的一信號。在允許該BIOS於SMM中執行之前，該硬體式保護機構嘗試著把受保全位址空間的內容驗證為無錯誤的。響應於判定出一錯誤可能已經影響該SMM處置器的狀況，該硬體式保護機構重新產生或修復該受保全位址空間中受影響程式碼的一或多個片段，例如在SMRAM的一受保護位址空間中。在確保一無錯誤SMM空間之後，該例示保護機構(其將在下文中更詳細地解說)允許該BIOS能執行該SMM處置器以校正初始錯誤。

在本文所述之該等實例所提供的其他益處與優點中，此種保護、驗證、及/或校正情景(例如，影響SMM部件的ECC錯誤)可消除、或至少減少運算平台經由一BIOS與額外錯誤處置器(例如，一BMC式錯誤處置器)來“雙重投入”錯誤處置動作的需要。再者，本文所述的該等實例針對某種先前地

被視為無法利用SMM部件來校正的錯誤類型提供一種復原機構。在閱讀了本發明的詳細說明之後，將可容易地了解本文所述的該等實例所提供的其他益處與優點。

第1圖以方塊圖展示出一種例示運算平台100，其能夠根據本文所述的該等例示方法、裝置、系統、及/或製造物品來保護記憶體區段。平台100可為任何類型的運算平台，例如一個人電腦、一工作站、一伺服器、一PDA、一販賣亭、一智慧型電話等。

第1圖的例示運算平台100包括記憶體控制器102，其具有能夠以任何適當方式檢測在運算平台100中發生之一或多個錯誤的錯誤檢測單元104。例如，錯誤檢測單元104可由一處理器(例如，以下結合第9圖解說的例示處理器912)的一IIO (整合式輸入/輸出系統)來實行。響應於檢測到一錯誤的動作，例示錯誤檢測單元104針對一SMI產生一請求。該SMI請求可包括有關該錯誤之一位置的資訊，例如當中檢測到該錯誤之記憶體中的位址。再者，例示錯誤檢測單元104及/或記憶體控制器102的另一個部件可利用一毒物指示器(poison indicator)來標示當中出現該錯誤的該記憶體位址。

在先前系統中，該SMI請求可能對導致一SMI的一立即產生狀況，且依次地使BIOS 106執行一SMM中斷常式。然而，在所展示的實例中，記憶體控制器102所產生的該SMI請求受到根據本文所述之該等例示方法、裝置、系統、及/或製造物品組配之硬體式保護機構108的攔截。為了接收該

SMI請求，例示保護機構108包括一通訊介面(未展示)，其受組配成能接收來自記憶體控制器102的該等信號。在所展示的實例中，保護機構108係由一直接記憶體存取Crystal Beach (CB)直接記憶體存取(DMA)引擎來實行，但不受限於此。保護機構108可實行於例示運算平台100的額外或替代部件中，及/或由不同類型的引擎或裝置來實行。

如上所述，嘗試著處置已經影響該SMRAM之某些部分之一ECC錯誤的BIOS 106可能是危險的，因為欲受BIOS 106執行的該SMM中斷常式本身可能已經受到毀損。因此，在所展示的實例中，DMA引擎108所攔截的該SMI請求(例如，如由記憶體控制器102產生的請求)將使BIOS 106中止處置該對應ECC錯誤，直到可以驗證該等SMM部件(例如，一SMM處置器)的完整性為止。如以下更詳細說明地，DMA引擎108將在一或多個SMM毀損的狀況下驗證、重新產生或修復欲用來從該錯誤恢復的SMM程式碼。當與該SMM相關聯的該等記憶體區段(例如，快取線)各受到驗證及/或校正時，DMA引擎108產生對應於DMA引擎108所接收到之該SMI請求的一SMI，其可隨後由BIOS 106來處置。因為DMA引擎108確保了一無錯誤SMM程式碼，BIOS 106可使用該SMM程式碼，而不會有負面的結果(例如，不會造成完全當機的狀況)。

為了致能該種保護功能，運算平台100接受與DMA引擎108以及SMRAM 110有關的多個初始化動作。換言之，某些硬體機構與軟體元件的初始組態令例示運算平台100能

保護記憶體區段，如本文所述地。例如，把SMM處置器112設置於其區段頂端(TSEG)區域內之SMRAM 110的一受保護頁面114中。在所展示的實例中，受保護頁面114的大小為四千位元組(4kB)，且包括七個(7)程式碼區塊116至128。程式碼區塊116至128的內容為可執行碼，其用以校正記憶體錯誤。程式碼區塊116至128的內容為不變的，且僅包括程式碼區塊(即，沒有資料區塊)。SMM處置器112的最後512個位元組(512B)係保留給同位區塊130。BIOS 106使DMA引擎108在一初始化程序中(例如，開機自我測試(POST))產生同位區塊130。此外，BIOS 106以受保護區域114的位置來編碼DMA引擎108的暫存器134，並且以編碼在其中之受保護區域114的位置來鎖定暫存器134。

在所展示的實例中，程式碼區塊116至128係受組配成(例如，由BIOS 106組配)不允許資料欄位變化。因此，DMA引擎108在一初始化程序過程中(例如，在POST開機過程中)產生同位區塊130一次。然而，在某些實例中，程式碼區塊116至128可受組配成(例如，由BIOS 106組配)包括可改變的資料欄位。在該種狀況中，在程式碼區塊116至128中之一或多個的每次改變之後，DMA引擎108產生同位區塊130。

在某些實例中，記憶體控制器102的錯誤檢測單元104(例如，一整合式輸入/輸出(IIO)系統)受到初始化，以把ECC錯誤信號路由到DMA引擎108。儘管係在上面把DMA引擎108解說為攔截一ECC錯誤信號(例如，一SMI請求)，例示運算平台100可受組配成能透過DMA引擎108自動地路由該

等信號。

DMA引擎108亦受組配成包括一通道(例如，一隱藏通道)，其執行一產生操作碼(例如，以產生同位區塊130)、一驗證操作碼(例如，以檢查受保護區域114中之一快取線的完整性)、或被傳送到受保護區域114的一修復操作碼(例如，以修復受保護區域114中的一快取線)。在所展示的實例中，該通道係受限為以SMRAM 110的TSEG記憶體來存取受保護區域114。再者，該通道為可存取例示運算平台100之受保護區域114的唯一通道。在致能DMA引擎108的操作之前，BIOS 106驗證此種存取組態(例如，DMA引擎108的該通道為可存取受保護區域114的唯一通道，且受保護區域114係完全地位於TSEG中)。再者，該通道繞過一VT-d引擎(如果有的話)，以防止轉發狀況及/或一安全性違背狀況。

在所展示的實例中，上述的產生、驗證與修復操作係由多個描述符136來實行。該等例示多個描述符136包括產生描述符138，其用以產生受保護區域114的同位區塊130。在所展示的實例中，產生描述符138根據已經載入之程式碼區塊116至128之內容的下列方程式來使同位區塊130產生：parity_blk = Code_blk0 XOR Code_blk1 XOR Code_blk2 XOR Code_blk3 XOR Code_blk4 XOR Code_blk5 XOR Code_blk6。產生描述符138的一例示實行方案係展示於第2圖中。例示產生描述符138係根據一種使用同位產生的RAID-5演算法來組配。該4kB基本部分為可編程的。如第2圖所示，產生描述符138的操作碼為0x87。

請回頭參照第1圖，該等例示多個描述符136亦包括驗證描述符140，其用以驗證程式碼區塊116至128的內容。例示驗證描述符140檢查SMM處置器112的快取線(即，程式碼區塊116至128)，以判定該等快取線中的任一條是否標示有一毒物指示器。錯誤檢測單元104或記憶體控制器102標示快取線，包括以一毒物指示器來表示一經檢測錯誤。該種指示器的出現使驗證描述符140能判定出一對應快取線是否包括一錯誤。驗證描述符140的一例示實行方案係展示於第3圖中。例示驗證描述符140相似於上述的例示產生描述符138。然而，驗證描述符140的操作碼為0x88。在執行驗證描述符140的過程中，如果發現任何區塊具有一錯誤，如對一"不可校正ECC錯誤"設定的一毒物位元所指出地，將針對給定的快取線捕捉故障來源位址，並且使DMA引擎108停止。

該等例示多個描述符136亦包括修復描述符142，而如果程式碼區塊116至128中之一或多個包括一錯誤(例如，如上述驗證嘗試動作所判定地)，修復描述符142便用以修復SMM處置器112的內容。修復描述符142的一例示實行方案係展示於第4圖中。在所展示的實例中，僅有故障的快取線受到修復。第4圖的例示修復描述符142相似於產生描述符138。然而，可操作長度係被改變為一條快取線(64kB)。此外，在修復描述符142中，在上述驗證動作中檢測到的該故障來源位址(只需要位元[11:8])係作為該同位區塊位址，而該同位區塊位址係用來替換該故障來源區塊的位址。例

如，如第2圖中之程式碼區塊位址以及第4圖中之程式碼區塊位址之比較結果所示，當該錯誤發生在程式碼區塊5中時，修復描述符142的同位區塊位址將被程式碼區塊5位址(即，0xA00)來替換，且程式碼區塊5位址將被該同位區塊位址(0xE00)來替換。

請回頭參照第1圖，第1圖的例示DMA引擎108亦包括SMI產生器144。因為例示DMA引擎108係受組配成接收來自錯誤檢測單元104的錯誤指示(例如，SMI請求)，DMA引擎108的例示SMI產生器144能夠產生對應於DMA引擎108所接收到之該SMI請求的多個SMI。響應於DMA引擎108驗證及/或建立SMM處置器112之完整性的動作，例示SMI產生器144產生並傳達SMI到BIOS 106。BIOS 106可隨後使用SMM處置器112，而不會使SMM處置器112遭受到風險，包括歷經一錯誤。

儘管已經在第1圖中展示出實行第1圖之運算平台100的一種例示方式，可以藉由任何其他方式來結合、劃分、重新配置、省略、消除、及/或實行展示於第1圖中之該等元件、程序、及/或裝置中的一或多個。再者，第1圖的例示保護機構108、例示暫存器134、例示產生描述符138、例示驗證描述符140、例示修復描述符142、例示SMI產生器144、例示SMM處置器112、例示受保護區域114、及/或例示運算平台100可藉由硬體、軟體、韌體來實行，及/或由硬體、軟體及/或韌體的任何組合來實行。因此，例如，第1圖之例示保護機構108、例示暫存器134、例示產生描述符138、

例示驗證描述符140、例示修復描述符142、例示SMI產生器144、例示SMM處置器112、例示受保護區域114、及/或例示運算平台100中的任一個可由一或多個電路、可編程處理器、特定應用積體電路(ASIC)、可編程邏輯裝置(PLD)、及/或現場可編程邏輯裝置(FPLD)等來實行。當本發明之裝置請求項的任一項涵蓋一種純粹軟體及/或韌體實行方案時，第1圖之例示保護機構108、例示暫存器134、例示產生描述符138、例示驗證描述符140、例示修復描述符142、例示SMI產生器144、例示SMM處置器112、例示受保護區域114、及/或例示運算平台100中的至少一個便藉此明確地受界定以包括一種儲存該軟體及/或韌體的有形媒體，例如一記憶體、DVD、CD等。再者，第1圖的例示保護機構108、例示暫存器134、例示產生描述符138、例示驗證描述符140、例示修復描述符142、例示SMI產生器144、例示SMM處置器112、例示受保護區域114、及/或例示運算平台100可包括一或多個元件、程序、及/或裝置，除了展示在第1圖中的該等元件、程序、及/或裝置以外或者替代於展示於第1圖中的該等元件、程序、及/或裝置，及/或可不只包括該等展示元件、程序與裝置中之任一個或全部中的一個。

第5圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示BIOS 106，以執行一種例示開機自我測試(POST)。第6圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示保護機構

108，以保護第1圖之例示SMRAM的一受保護區域114。可利用一處理器、一控制器、及/或任何其他適當處理裝置來執行第5圖與第6圖的例示程序。例如，可利用儲存在一有形電腦可讀媒體上的編碼指令(例如，電腦可讀指令)來實行第5圖與第6圖的例示程序，例如一快閃記憶體、一唯讀記憶體(ROM)、及/或一隨機存取記憶體(RAM)。如本文中使用地，有形電腦可讀媒體一語係明確地受界定以包括任何類型的電腦可讀儲存體，並且排除了傳播信號。此外或替代地，可使用儲存在一非暫時性(non-transitory)電腦可讀媒體上的編碼指令(例如，電腦可讀指令)來實行第5圖與第6圖的例示程序，例如一快閃記憶體、一唯讀記憶體(ROM)、一隨機存取記憶體(RAM)、一快取記憶體、或任何其他儲存媒體，其中資訊受儲存達任何期間(例如，達延長期間、永久地、短暫時間、為了暫時緩衝目的、及/或為了快取該資訊目的)。如本文中使用地，非暫時性(non-transitory)電腦可讀媒體一語係明確地受界定以包括任何類型的電腦可讀媒體，並且排除了傳播信號。

替代地，可使用特定應用積體電路(ASIC)、可編程邏輯裝置(PLD)、現場可編程邏輯裝置(FPLD)、分立邏輯組件、硬體、韌體等的任何組合來實行第5圖與第6圖的例示程序。同樣地，可手動地或利用上述技術中之任一種的任何組合來實行第5圖與第6圖的例示程序中的某些或全部，例如韌體、軟體、分立邏輯組件、及/或硬體的任何組合。再者，雖然第5圖與第6圖的例示程序係參照第5圖與第6圖的

流程圖來解說，可以使用用以實行第5圖與第6圖的例示程序的其他方法。例如，可以改變該等方塊的執行順序、及/或可以改變、消除、細分、或結合所述之該等方塊中的某些。此外，可依序地或並行地執行第5圖與第6圖的例示程序中的任何或全部，例如由分別處理執行緒、處理器、裝置、分立邏輯組件、電路等來執行。

請參照第5圖，係把BIOS 106實行為呈機器可讀指令形式儲存在耦合至運算平台100之一處理器(例如，以下結合第9圖討論的例示處理器912)之一非依電性記憶體中的軟體及/或韌體。大致上，在開啟該作業系統之前，BIOS 106執行一或多個硬體與軟體組態以及測試活動(例如，記憶體初始化、記憶體劃分等)。

在第5圖展示的實例中，當BIOS 106開始一POST(方塊500)時，BIOS 106初始化第1圖之例示運算平台100的資源(方塊502)。除了BIOS 106在方塊502中執行的習知操作之外，例示BIOS 106執行根據本文所述之該等實例的初始化。尤其，BIOS 106組配受保護區域114以把例示SMM處置器112儲存在TSEG中(方塊504)。如上所述，此組態包括BIOS 106以TSEG中之受保護區域114的位置來編程DMA引擎108的暫存器134，並且鎖定暫存器134。再者，BIOS 106把SMM處置器112的程式碼載入到受保護區域114中，且一旦SMM處置器112碼已經受載入，觸發同位區塊130的產生(方塊506)。BIOS 106確認與受保護區域114以及DMA引擎108相關聯之該等設定與初始化的正確性(方塊508)，並且隨

後繼續及/或允許該經觸發POST (方塊510)。

請參照第6圖，保護機構108係由展示實例中一DMA引擎來實行。更確切來說，展示實例的例示保護機構108係由一Crystal Beach DMA引擎來實行，其使用RAID-5演算法以及其操作碼。該RAID-5演算法使用XOR邏輯來做為用以校正程式碼區塊116至128中之錯誤的一種同位式(parity-based)方法。

第6圖的例示流程圖對應於保護機構108的行為，一旦保護機構108已經受到初始化(例如，由BIOS 106初始化)，且SMM處置器112程式碼已經受載入到受保護區域114中(方塊600)。在展示於第6圖的實例中，保護機構108維持為一種閒置狀態，直到記憶體控制器102經由錯誤檢測單元104(例如，一整合式輸入/輸出(IIO))檢測到一ECC錯誤為止(方塊602)。如上所述，保護機構108受組配成能接收或攔截來自記憶體控制器102的一錯誤指示(例如，一SMI請求)。響應於在方塊602接收到該種指示的動作，保護機構108開始嘗試著驗證SMRAM 110之受保護區域114的內容(方塊604)。如本文中所述，保護機構108驗證SMM處置器112程式碼(例如，使用第1圖的驗證描述符140)，以確保BIOS 106在使用該SMM模式時並不執行毀損碼。

當正受檢查之程式碼區塊的一快取線(例如第5程式碼區塊126)包括一毒物指示器(例如，如由記憶體控制器102經由錯誤檢測單元104設置的)(方塊606)時，保護機構108修復(例如，使用第1圖的修復描述符142)具有該錯誤的該快

取線(方塊608)。例如，當該第五程式碼區塊126包括一錯誤時，以下的方程式係用以修復第五程式碼區塊126：code_blk5 = code_blk0 XOR code_blk1 XOR code_blk2 XOR code_blk3 XOR code_blk4 XOR parity_blk XOR code_blk6。

一旦已經修復了具有該錯誤的該快取線，保護機構108判定是否已經驗證了受保護區域114的完整SMM程式碼(方塊610)。替代地，請回頭參照第6圖的方塊606，如果嘗試著受驗證的該快取線並不包括一錯誤，保護機構108判定是否已經驗證了受保護區域114的完整SMM程式碼 (方塊610)。如果尚未驗證受保護區域114的完整SMM程式碼，保護機構108便嘗試著驗證受保護SMM程式碼的下一條快取線 (方塊604)。否則，如果已經驗證了受保護區域114的完整SMM程式碼，保護機構108的SMI產生器144便根據保護機構108從記憶體控制器102攔截或接收的該SMI請求來產生一SMI (方塊612)。保護機構108隨後返回到該閒置狀態(方塊614)，並且等待來自記憶體控制器102的另一個錯誤指示 (方塊602)。

第7圖展示出受第1圖之該例示保護機構之一第一演算法保護之第1圖的該等程式碼區塊116至128。第7圖的數行表示程式碼區塊116至128的快取線，以及第1圖的同位區塊130。例如，第7圖中標示為'C1'的一第一快取線代表一第一快取線。第7圖展示出對一Crystal Beach(CB)DMA引擎實行RAID-5同位演算法的保護機構108。如第7圖所示，多個

位元錯誤(以第7圖中的X來表示)可在一單一程式碼或同位區塊的任何一條快取線中累積，只要相關聯快取線並不包括無法校正的ECC錯誤。

第8圖展示出受第1圖之該例示保護機構之一第二演算法保護之第1圖的該等程式碼區塊。尤其，第8圖展示出對一Crystal Beach (CB) DMA引擎實行RAID-6同位演算法的保護機構108。該RAID-6組態提供額外保護，例如允許各行中的2條快取線受到保護。為了提供此種保護，該等程式碼區塊中之一(在展示實例中為程式碼blk6)被置換成一商數區塊。第8圖中的該商數區塊與同位區塊係根據RAID-6架構來使用，並且用來修復包括錯誤的快取線。

第9圖以方塊圖展示出一種例示處理器系統，其可用來執行第2圖的該等機器可讀指令、及/或實行第1圖的該例示運算平台100、及/或實行第1圖的例示BIOS復原模組102。如第9圖所示，處理器系統910包括耦合至互連匯流排914的處理器912。處理器912可為任何適當處理器、處理單元、或微處理器。雖然並未展示於第9圖，系統910可為一種多處理器系統，並且可因此包括一或多個額外處理器，其可能不同於、相同於、或相似於處理器912且係通訊式地耦合至互連匯流排914。

第9圖的處理器912係耦合至晶片組918，其包括記憶體控制器920與輸入/輸出(I/O)控制器922。晶片組918提供I/O與記憶體管理功能，以及多個一般用途及/或特殊用途暫存器、計時器等，其可由耦合至晶片組918的一或多個處理器

來存取或使用。記憶體控制器920執行令處理器912(或多個處理器，如果有多個處理器的話)能存取系統記憶體924與大量儲存記憶體925的多種功能。

系統記憶體924可包括任何所欲類型的依電性及/或非依電性記憶體，例如靜態隨機存取記憶體(SRAM)、動態隨機存取記憶體(DRAM)、快閃記憶體、唯讀記憶體(ROM)等。大量儲存記憶體925可包括任何所欲類型的大量儲存裝置，包括硬碟驅動機、光碟驅動機、磁帶儲存裝置等。

I/O控制器922執行令處理器912能經由I/O匯流排932與周邊輸入/輸出(I/O)裝置926和928以及網路介面930通訊的多種功能。I/O裝置926與I/O裝置928可為任何所欲類型的I/O裝置，例如一鍵盤、一視訊顯示器或監視器、一滑鼠等。例如，網路介面930可為一乙太網路裝置、一異步傳輸模式(ATM)裝置、一802.11裝置、一DSL數據機、一纜線數據機、一蜂巢式數據機等，其令處理器系統310能與另一個處理器系統通訊。

儘管在第3圖中係把記憶體控制器320與I/O控制器322解說為晶片組318中的分別區塊，可在一單一半導體電路中整合該等區塊所執行的功能，或者可使用二或更多個分別積體電路來實行該等功能。

雖然已經在本文中解說了某些方法、裝置與製造物品，本專利申請案的涵蓋範圍不受限於此。反之，本專利申請案涵蓋本質上屬於以下申請專利範圍內的所有方法、裝置與製造物品，或屬於等效方案之原理內的所有方法、裝置

與製造物品。

【圖式簡單說明】

第1圖以方塊圖展示出一種例示運算平台的例示部件，包括一例示保護機構。

第2圖為第1圖之該產生描述符的一例示實行方案。

第3圖為第1圖之該驗證描述符的一例示實行方案。

第4圖為第1圖之該修復描述符的一例示實行方案。

第5圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示BIOS，以執行一種例示開機自我測試(POST)。

第6圖以流程圖展示出一種可利用例示機器可讀指令來實行的例示程序，該等指令可受執行以實行第1圖的例示保護機構，以保護第1圖之例示SMRAM的一區域。

第7圖展示出受第1圖之該例示保護機構之一第一演算法保護之第1圖的該等程式碼區塊。

第8圖展示出受第1圖之該例示保護機構之一第二演算法保護之第1圖的該等程式碼區塊。

第9圖以方塊圖展示出一種例示處理器系統，其可用來執行第2圖的該等機器可讀指令及/或實行第1圖的該例示運算平台。

【主要元件符號說明】

100...運算平台

102...記憶體控制器

104...錯誤檢測單元

106...BIOS

108...保護機構、DMA引擎

110...SMRAM

112...SMM處置器

114...受保護頁面

116...程式碼區塊

118...程式碼區塊

120...程式碼區塊

122...程式碼區塊

124...程式碼區塊

126...程式碼區塊

128...程式碼區塊

130...同位區塊

134...暫存器

136...描述符

138...產生描述符

140...驗證描述符

142...修復描述符

144...SMI產生器

500~510...步驟方塊

600~614...步驟方塊

910...處理器系統

912...處理器

914...互連匯流排

918...晶片組

920...記憶體控制器

922...輸入/輸出(I/O)控制器

924...系統記憶體

925...大量儲存記憶體

926...周邊輸入/輸出(I/O)裝置

928...周邊輸入/輸出(I/O)裝置

930...網路介面

932...I/O匯流排

201212037

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：100125648

※申請日：100.7.20　　※IPC 分類：

G11C 29/42 (2006.01)

G06F 12/16 (2006.01)

一、發明名稱：(中文/英文)

用以保護記憶體之區段的方法及裝置

METHODS AND APPARATUS TO PROTECT SEGMENTS OF MEMORY

二、中文發明摘要：

本發明揭露用以保護記憶體區段的方法與裝置。一種例示方法包括下列步驟：攔截表示一錯誤的一中斷請求；判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及響應於驗證該受保護記憶體區域的步驟，產生一中斷，該中斷致能利用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

三、英文發明摘要：

Methods and apparatus to protect segments of memory are disclosed herein. An example method includes intercepting an interrupt request indicating an error; determining whether a first segment of memory is corrupt, the first segment of memory being designated as a protected region of memory; when the protected region of memory is corrupt, repairing the corrupted region of memory using a parity block of code; and in response to validating the protected region of memory, generating an interrupt enabling a utilization of code stored in the protected region of memory to handle the error associated with the interrupt request.

七、申請專利範圍：

1. 一種用以保護一運算平台中之一記憶體區段的方法，其包含下列步驟：

   攔截表示一錯誤的一中斷請求；

   判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；

   當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及

   響應於驗證該受保護記憶體區域的步驟，產生一中斷，該中斷致能使用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

2. 如申請專利範圍第1項之方法，其中該受保護記憶體區域包括受指定為處置該錯誤的一系統管理模式處置器。

3. 如申請專利範圍第1項之方法，其中該受保護記憶體區域僅為用以驗證該受保護記憶體區域的一保護機構能存取的。

4. 如申請專利範圍第1項之方法，其另包含產生一同位區塊以修復儲存在該受保護記憶體區域中的該程式碼。

5. 如申請專利範圍第1項之方法，其另包含把該受保護記憶體區域的一位置儲存在一或多個暫存器中，並且鎖定該等暫存器。

6. 如申請專利範圍第1項之方法，其中該攔截步驟防止一基本輸入/輸出系統處置該錯誤。

7. 如申請專利範圍第6項之方法，其中該基本輸入/輸出系

統在一初始化程序中把一系統管理模式處置器載入到該受保護記憶體區域中。

8. 一種上面儲存有指令的有形機器可讀媒體，該等指令受執行時使一機器進行下列動作：

攔截表示一錯誤的一中斷請求；

判定一第一記憶體區段是否毀損，該第一記憶體區段受指定為一受保護記憶體區域；

當該受保護記憶體區域毀損時，使用一同位程式碼區塊來修復該毀損記憶體區域；以及

響應於驗證該受保護記憶體區域的動作，產生一中斷，該中斷致能利用儲存在該受保護記憶體區域中的程式碼來處置與該中斷請求相關聯之該錯誤。

9. 如申請專利範圍第8項之有形機器可讀媒體，其中該受保護記憶體區域包括受指定為處置該錯誤的一系統管理模式處置器。

10. 如申請專利範圍第8項之有形機器可讀媒體，其中該受保護記憶體區域僅為用以驗證該受保護記憶體區域的一保護機構能存取的。

11. 如申請專利範圍第8項之有形機器可讀媒體，其中該等指令受執行時使一機器產生一同位區塊以供用來修復儲存在該受保護記憶體區域中的該程式碼。

12. 如申請專利範圍第8項之有形機器可讀媒體，其中該等指令受執行時使一機器把該記憶體區域的一位置儲存在一或多個暫存器中，並且鎖定該等暫存器。

13. 如申請專利範圍第8項之有形機器可讀媒體，其中該記憶體區段受指定為受一基本輸入/輸出系統保護。

14. 如申請專利範圍第13項之有形機器可讀媒體，其中該基本輸入/輸出系統在一初始化程序中把一系統管理模式處置器載入到該受保護記憶體區域中。

15. 一種用以保護一記憶體區段的裝置，其包含：

用以接收與一錯誤有關之一中斷請求的一通訊介面，其中該中斷請求指出該錯誤的一位置；

以一受保護記憶體區域之一位置被編程的一或多個暫存器，其中該等一或多個暫存器受鎖定以包括該受保護記憶體區域的該位置；

一修復描述符，其用以在該錯誤的該位置位於該受保護記憶體區域時，修復該受保護記憶體區域的一毀損區段；

一驗證描述符，其用以驗證該受保護記憶體區域；以及一中斷產生器，其用以響應於該驗證描述符驗證該受保護記憶體區域的動作，產生對應於該中斷請求的一中斷，以致能利用儲存在該受保護記憶體區域中之程式碼。

16. 如申請專利範圍第15項之裝置，其中該受保護記憶體區域係位於系統管理隨機存取記憶體之一頂部區段部分中。

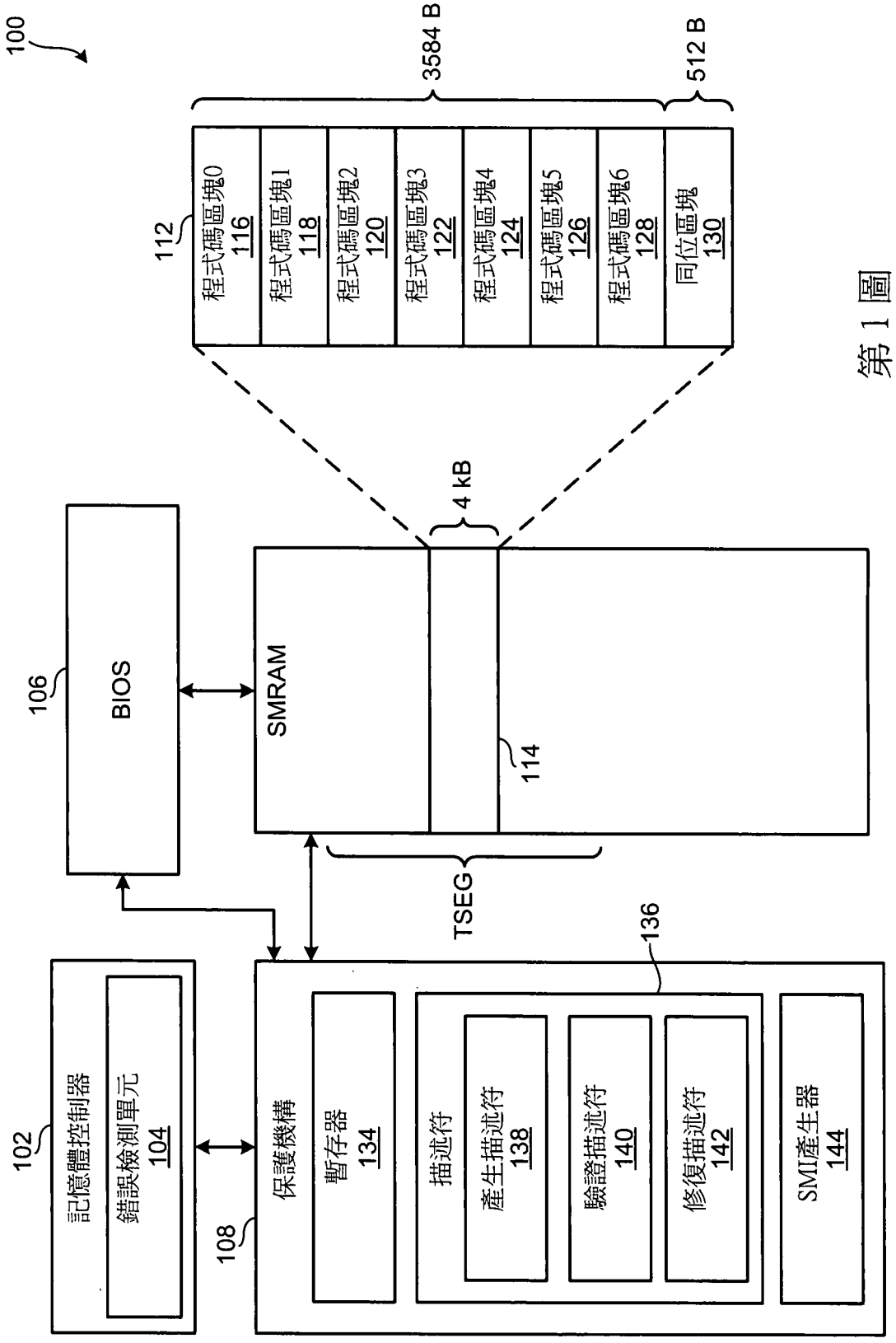
17. 如申請專利範圍第15項之裝置，其中該修復描述符利用一同位區塊來修復該受保護記憶體區域的該毀損區段。

18. 如申請專利範圍第17項之裝置，其另包含一產生描述符，其根據儲存在該受保護記憶體區域中之一系統管理模式處置器的程式碼來產生該同位區塊。

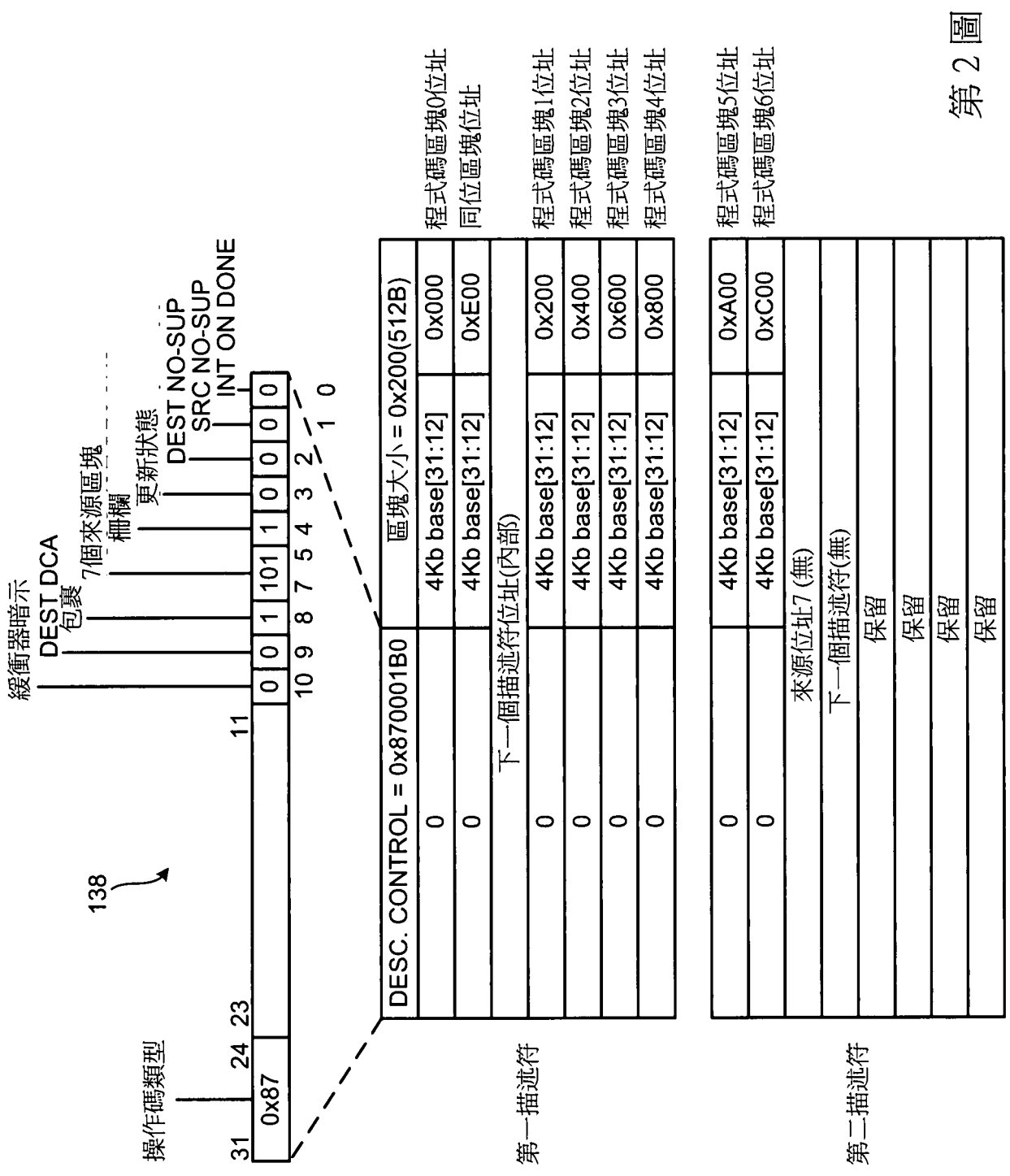
19. 如申請專利範圍第15項之裝置，其中該中斷產生器把對應於該中斷請求的該中斷傳達至一基本輸入/輸出系統。

20. 如申請專利範圍第19項之裝置，其中該基本輸入/輸出系統使用該受保護記憶體區域中的程式碼來處置一運算系統中的錯誤。

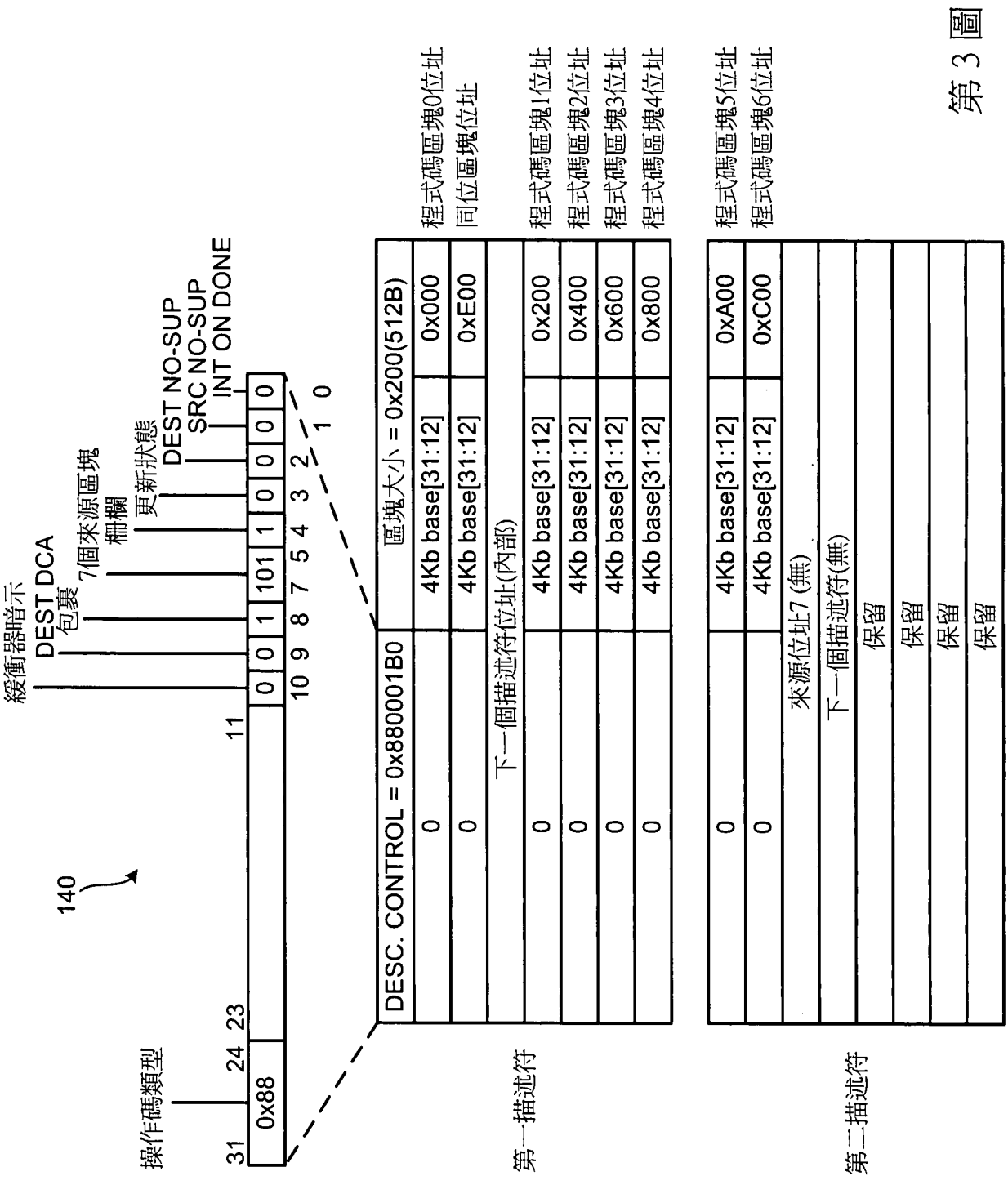
八、圖式


100
3584 B
512 B
112
程式碼區塊0 116
程式碼區塊1 118
程式碼區塊2 120
程式碼區塊3 122
程式碼區塊4 124
程式碼區塊5 126
程式碼區塊6 128
同位區塊 130
4 kB
106
BIOS
SMRAM
114
TSEG
136
102
記憶體控制器
錯誤檢測單元 104
108
保護機構
暫存器 134
描述符
產生描述符 138
驗證描述符 140
修復描述符 142
SMI產生器 144

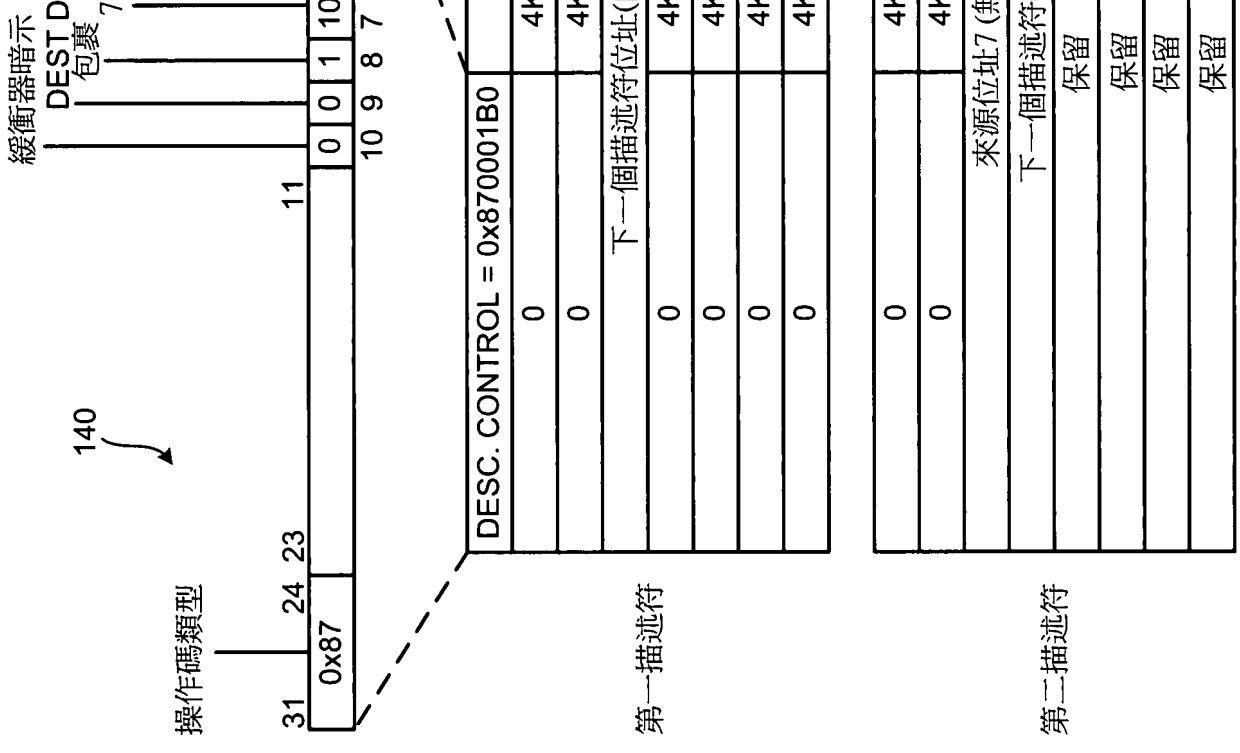
第 1 圖


緩衝器暗示
DEST DCA
包裹
7個來源區塊
柵欄
更新狀態
DEST NO-SUP
SRC NO-SUP
INT ON DONE
138
操作碼類型
31 24 23 11 10 9 8 7 5 4 3 2 1 0
0x87
0 0 1 101 1 0 0 0 0
DESC. CONTROL = 0x870001B0
區塊大小 = 0x200(512B)
第一描述符
0
4Kb base[31:12]
0x000
程式碼區塊0位址
0
4Kb base[31:12]
0xE00
同位區塊位址
下一個描述符位址(內部)
0
4Kb base[31:12]
0x200
程式碼區塊1位址
0
4Kb base[31:12]
0x400
程式碼區塊2位址
0
4Kb base[31:12]
0x600
程式碼區塊3位址
0
4Kb base[31:12]
0x800
程式碼區塊4位址
第二描述符
0
4Kb base[31:12]
0xA00
程式碼區塊5位址
0
4Kb base[31:12]
0xC00
程式碼區塊6位址
來源位址7 (無)
下一個描述符(無)
保留
保留
保留
保留

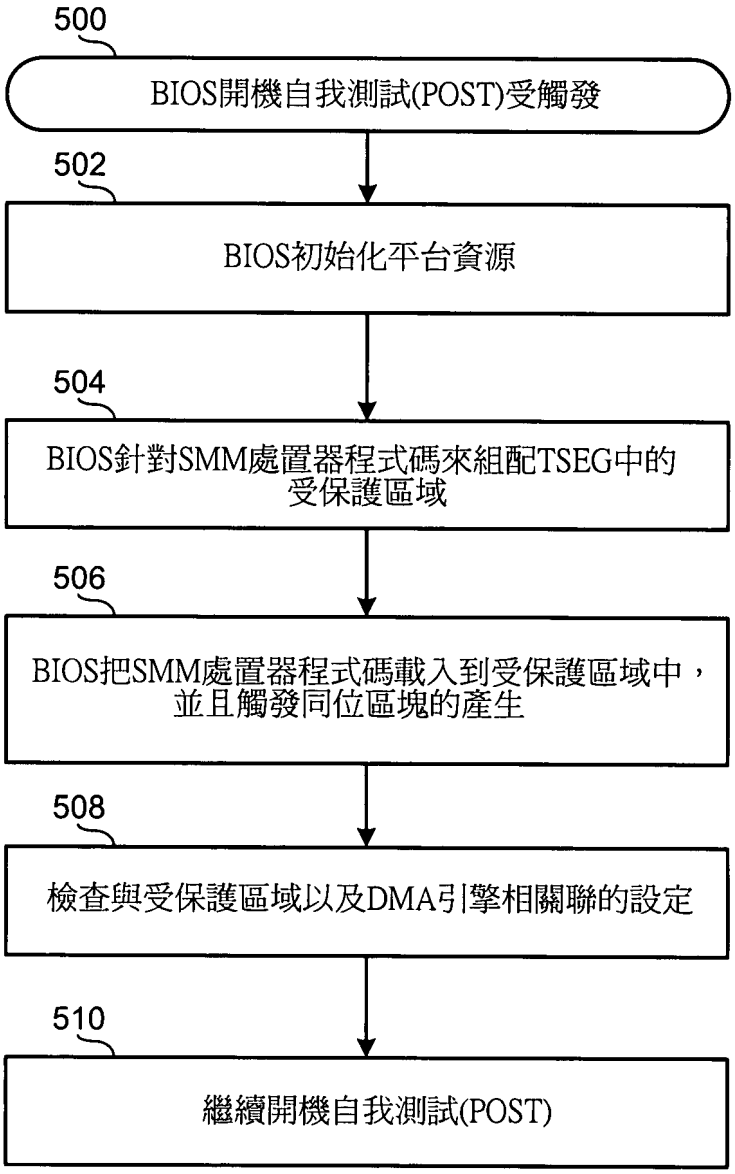
第 2 圖


140
緩衝器暗示
DEST DCA
包裹
7個來源區塊
柵欄
更新狀態
DEST NO-SUP
SRC NO-SUP
INT ON DONE
操作碼類型
31
24
23
11
10
9
8
7
5
4
3
2
1
0
0x88
0
0
1
101
1
0
0
0
DESC. CONTROL = 0x880001B0
區塊大小 = 0x200(512B)
4Kb base[31:12]
0x000
程式碼區塊0位址
0
4Kb base[31:12]
0xE00
同位區塊位址
下一個描述符位址(內部)
第一描述符
0
4Kb base[31:12]
0x200
程式碼區塊1位址
0
4Kb base[31:12]
0x400
程式碼區塊2位址
0
4Kb base[31:12]
0x600
程式碼區塊3位址
0
4Kb base[31:12]
0x800
程式碼區塊4位址
0
4Kb base[31:12]
0xA00
程式碼區塊5位址
0
4Kb base[31:12]
0xC00
程式碼區塊6位址
來源位址7 (無)
下一個描述符(無)
保留
保留
保留
保留
第二描述符

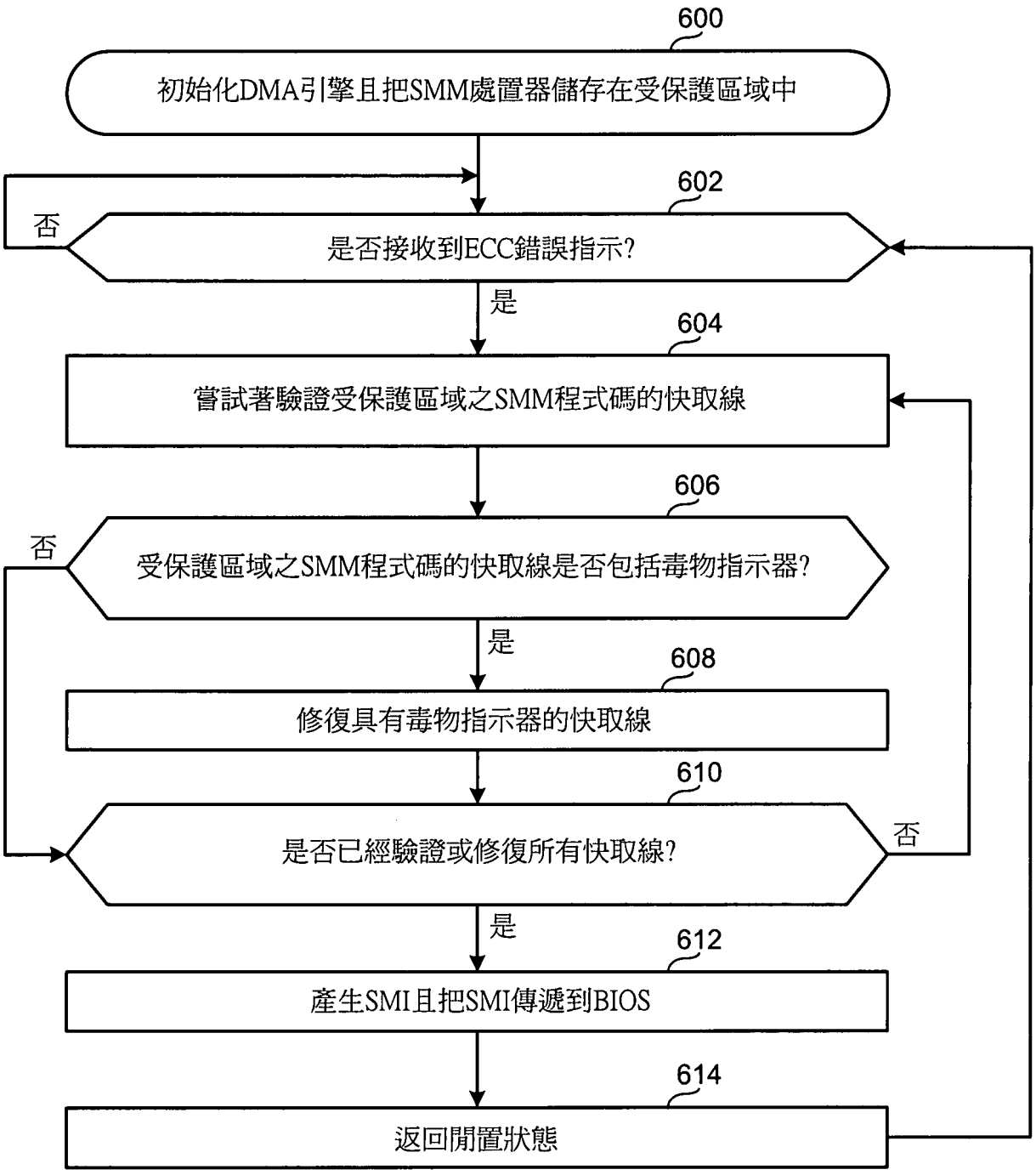
第 3 圖


140
操作碼類型
緩衝器暗示
DEST DCA
包裹
7個來源區塊
柵欄
更新狀態
DEST NO-SUP
SRC NO-SUP
INT ON DONE
31
24
23
11
10 9 8 7 5 4 3 2 1 0
0x87
0 0 1 101 1 0 0 0
DESC. CONTROL = 0x870001B0
區塊大小 = 0x200(512B)
第一描述符
第二描述符
0
4Kb base[31:12]
0x000
程式碼區塊0位址
0
4Kb base[31:12]
0xA00
同位區塊位址
下一個描述符位址(內部)
0
4Kb base[31:12]
0x200
程式碼區塊1位址
0
4Kb base[31:12]
0x400
程式碼區塊2位址
0
4Kb base[31:12]
0x600
程式碼區塊3位址
0
4Kb base[31:12]
0x800
程式碼區塊4位址
0
4Kb base[31:12]
0xE00
程式碼區塊5位址
0
4Kb base[31:12]
0xC00
程式碼區塊6位址
來源位址7 (無)
下一個描述符(無)
保留
保留
保留
保留

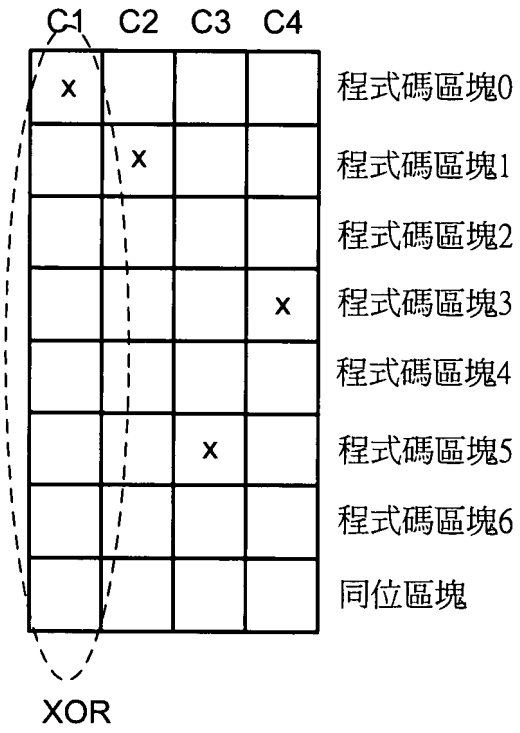
第 4 圖


500
BIOS開機自我測試(POST)受觸發
502
BIOS初始化平台資源
504
BIOS針對SMM處置器程式碼來組配TSEG中的受保護區域
506
BIOS把SMM處置器程式碼載入到受保護區域中，並且觸發同位區塊的產生
508
檢查與受保護區域以及DMA引擎相關聯的設定
510
繼續開機自我測試(POST)

第 5 圖


600
初始化DMA引擎且把SMM處置器儲存在受保護區域中
602
否
是否接收到ECC錯誤指示?
是
604
嘗試著驗證受保護區域之SMM程式碼的快取線
606
否
受保護區域之SMM程式碼的快取線是否包括毒物指示器?
是
608
修復具有毒物指示器的快取線
610
是否已經驗證或修復所有快取線?
否
是
612
產生SMI且把SMI傳遞到BIOS
614
返回閒置狀態

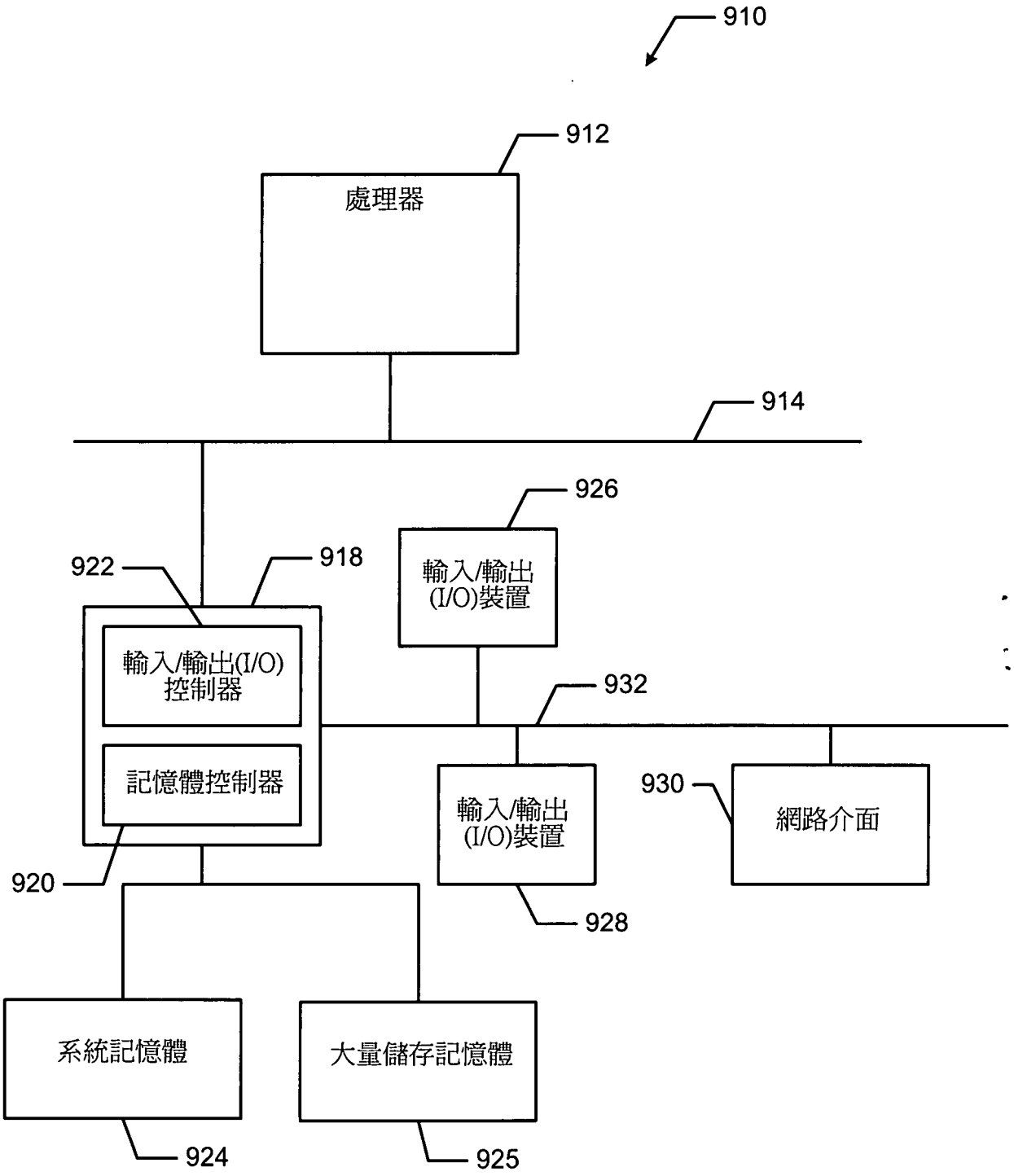
第 6 圖


C1
C2
C3
C4
x
x
x
x
程式碼區塊0
程式碼區塊1
程式碼區塊2
程式碼區塊3
程式碼區塊4
程式碼區塊5
程式碼區塊6
同位區塊
XOR

第 7 圖


C1
C2
C3
C4
x
x
x
x
x
x
x
x
程式碼區塊0
程式碼區塊1
程式碼區塊2
程式碼區塊3
程式碼區塊4
程式碼區塊5
商數區塊
同位區塊

第 8 圖


910
912
處理器
914
926
輸入/輸出
(I/O)裝置
922
918
輸入/輸出(I/O)
控制器
記憶體控制器
932
930
網路介面
輸入/輸出
(I/O)裝置
920
928
系統記憶體
大量儲存記憶體
924
925

第 9 圖

四、指定代表圖：

(一)本案指定代表圖為：第（ 6 ）圖。

(二)本代表圖之元件符號簡單說明：

600~614...步驟方塊

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

S