(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 201044276 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 16 日

(21)申請案號：098144754 (22)申請日： 中華民國 98 (2009) 年 12 月 24 日
(51)Int. Cl.： *G06F9/455 (2006.01)*
(30)優先權：2008/12/31 美國 12/347,978
(71)申請人：英特爾公司 (美國) INTEL CORPORATION (US)
美國
(72)發明人：波津 索哈 BOGIN, ZOHAR (US)；卡林納哈里 蘇耶普拉薩 KAREENAHALLI, SURYAPRASAD (IN)；拿拉瓦迪 拉吉夫K NALAWADI, RAJEEV K. (US)；費拉拉 艾利克 FERRARA, ERIC (US)
(74)代理人：惲軼群；陳文郎
申請實體審查：有 申請專利範圍項數：1 項 圖式數：2 共 19 頁

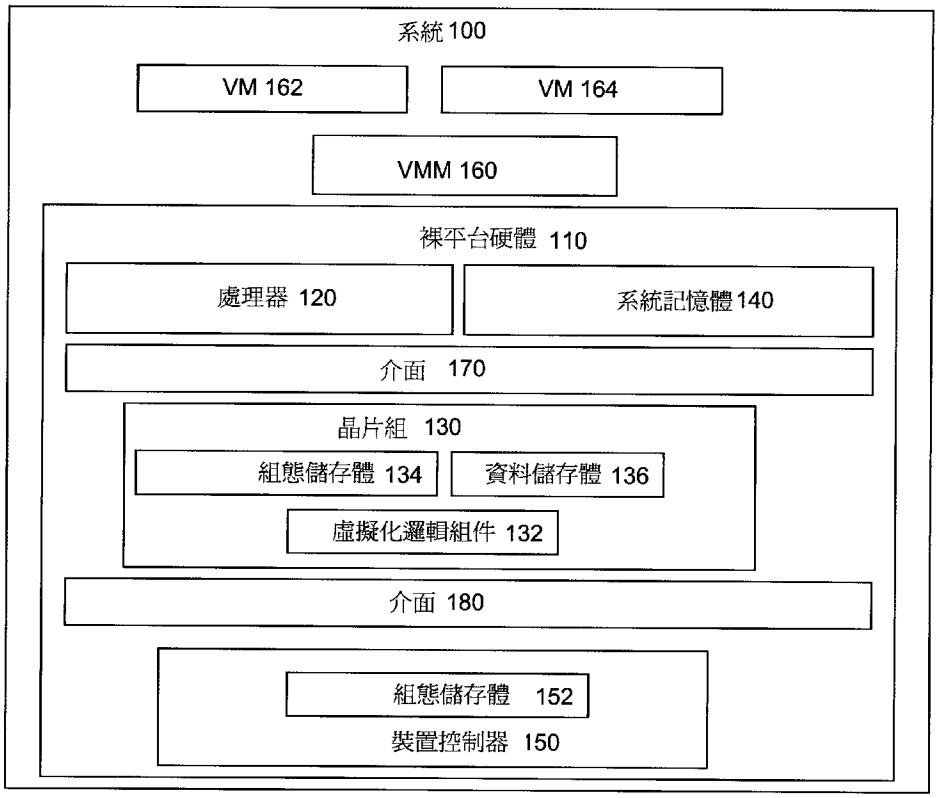
(54)名稱

注入異動以支援實體裝置控制器之虛擬化的技術

INJECTING TRANSACTIONS TO SUPPORT THE VIRTUALIZATION OF A PHYSICAL DEVICE CONTROLLER

(57)摘要

本發明揭露用以注入異動以支援實體裝置控制器之虛擬化的裝置、方法與系統之實施例。在一實施例中，一種裝置包括一處理器、系統記憶體、一實體裝置控制器、以及一虛擬化代理器。該實體裝置控制器欲由安裝在一處理器上之一虛擬機器監視器所產生的多個虛擬機器共享。該虛擬化代理器透過一第一介面耦合至該系統記憶體且透過一第二介面耦合至該實體裝置控制器，以把該實體裝置控制器表示為可對該等多個虛擬機器分配的多個虛擬裝置控制器，並且代表該等多個虛擬裝置控制器注入異動到該第一介面以及該第二介面上。



100：資訊處理系統
110：裸平台硬體
120：處理器
130：晶片組
132：虛擬化邏輯組件
134：組態儲存體
136：資料儲存體
140：系統記憶體
150：裝置控制器
152：組態儲存體
160：虛擬機器監視器(VMM)
162：虛擬機器(VM)
164：虛擬機器(VM)
170：介面
180：介面

(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 201044276 A1
(43)公開日： 中華民國 99 (2010) 年 12 月 16 日

(21)申請案號：098144754 (22)申請日： 中華民國 98 (2009) 年 12 月 24 日
(51)Int. Cl.： *G06F9/455 (2006.01)*
(30)優先權：2008/12/31 美國 12/347,978
(71)申請人：英特爾公司 (美國) INTEL CORPORATION (US)
美國
(72)發明人：波津 索哈 BOGIN, ZOHAR (US)；卡林納哈里 蘇耶普拉薩 KAREENAHALLI, SURYAPRASAD (IN)；拿拉瓦迪 拉吉夫K NALAWADI, RAJEEV K. (US)；費拉拉 艾利克 FERRARA, ERIC (US)
(74)代理人：惲軼群；陳文郎
申請實體審查：有 申請專利範圍項數：1 項 圖式數：2 共 19 頁

(54)名稱

注入異動以支援實體裝置控制器之虛擬化的技術

INJECTING TRANSACTIONS TO SUPPORT THE VIRTUALIZATION OF A PHYSICAL DEVICE CONTROLLER

(57)摘要

本發明揭露用以注入異動以支援實體裝置控制器之虛擬化的裝置、方法與系統之實施例。在一實施例中，一種裝置包括一處理器、系統記憶體、一實體裝置控制器、以及一虛擬化代理器。該實體裝置控制器欲由安裝在一處理器上之一虛擬機器監視器所產生的多個虛擬機器共享。該虛擬化代理器透過一第一介面耦合至該系統記憶體且透過一第二介面耦合至該實體裝置控制器，以把該實體裝置控制器表示為可對該等多個虛擬機器分配的多個虛擬裝置控制器，並且代表該等多個虛擬裝置控制器注入異動到該第一介面以及該第二介面上。

六、發明說明：

【發明所屬之技術領域】

發明的技術領域

本發明係有關資訊處理的技術領域，且更確切來說，係有關資訊處理系統中的虛擬化技術。

【先前技術】

發明的技術背景

大致上來說，資訊處理系統中的虛擬化概念允許一或多個作業系統(各稱為"OS")的多個事例能在一單一資訊處理系統上運作，即使係把各個 OS 設計為具有對該系統以及其資源的完整、直接控制。虛擬化技術典型地係藉著使用軟體(例如，一虛擬機器監視器或稱為一"VMM")來對各個 OS 呈現具有虛擬資源的一"虛擬機器"("VM")來實行，其包括該 OS 可完全地且直接地控制的一或多個虛擬處理器，而該 VMM 維持用以實行虛擬化策略的一系統環境，例如在該等 VM (該"虛擬化環境")之間共享且分配實體資源。係把各個 OS 以及在一 VM 上執行的任何其他軟體稱為一"客戶"或"客戶軟體"，而一"主機"或"主機軟體"則是在該虛擬化環境外部運作的軟體，例如一 VMM。

一資訊處理系統中的一實體處理器可支援虛擬化技術，例如藉著支援用以進入一虛擬化環境以於一 VM 中的一虛擬處理器(即，受到一 VMM 施加之限制的一實體處理器)上執行一客戶軟體的一指令。在該虛擬化環境中，可截取到某些事件、操作、以及狀況，例如外部中斷或嘗試著

存取具特權暫存器或資源，即，使該處理器退出該虛擬化環境，以使一 VMM 可運作以實行虛擬化策略。

可依據專屬方式把該系統中的一實體資源，例如一輸入/輸出裝置控制器，分派或分配給一VM。替代地，可藉著截取所有包含該資源的異動使由多個VM共享一實體資源，以使該VMM可進行各個異動、使各個異動重新導向、或者限制各個異動。第三種方法可為設計該實體資源以提供供其作為多重虛擬資源的能力

【發明內容】

發明的概要說明

依據本發明之一實施例，係特地揭露一種裝置，其包含：一處理器；系統記憶體；一實體裝置控制器，其欲由安裝在該處理器上之一虛擬機器監視器所產生之多個虛擬機器共享；透過一第一介面耦合至該系統記憶體且透過一第二介面耦合至該實體裝置控制器的一虛擬化代理器，其用以把該實體裝置控制器表示為可對該等多個虛擬機器分配的多個虛擬裝置控制器，並且用以代表該等多個虛擬裝置控制器注入異動到該第一介面以及該第二介面上。

圖式簡要說明

係以舉例方式且不具限制性的方式在圖式中展示出本發明的實施例。

第 1 圖展示出根據本發明一實施例之一種用以注入異動的裝置。

第2圖展示出根據本發明一實施例之一種用以注入異動

的方法。

【實施方式】

較佳實施例的詳細說明

本發明可體現於一種用以注入異動以支援實體裝置控制器之虛擬化的裝置或方法，如下所述。在詳細說明中，將列出多種特定細節，例如部件與系統組態，以便提供本發明的完整說明。然而，熟知技藝者將可了解的是，不需要該等特定細節亦可實現本發明。此外，並不詳細地說明已為人熟知的結構、電路等，以避免不必要地模糊本發明的焦點。

所欲的是使一單一實體裝置控制器能受到多個虛擬機器共享，而不需要一 VMM 截取所有包含該裝置控制器的所有異動，或者重新設計該裝置控制器以支援虛擬化技術。因此，本發明的實施例可藉著抑制包含該實體裝置控制器的異動並且代表該等虛擬裝置控制器注入異動來支援把一單一實體裝置控制器表述成多重虛擬裝置控制器的方式。

本發明實施例的元件可實行於硬體、軟體、韌體中、或者可實行於硬體、軟體、或韌體的任何組合中。"硬體"一語大致上表示一種具有一實體結構的元件，例如電子、電磁、光學、電光學、機械性、電機械性零件等。"軟體"一語大致上表示一種邏輯結構、一種方法、一種程序、一種程式、一種常式、一種處理方式、一種演繹法、一種方程式、一種表式等。"韌體"一語大致上表示一種邏輯結構、一種方法、一種程序、一種程式、一種常式、一種處理方

式、一種演繹法、一種方程式、或一種實行於或體現於一硬體結構(例如，快閃記憶體或唯讀記憶體)的表式。韌體的實例為微碼、可覆寫控制儲存庫、以及微編程結構。

第 1 圖展示出根據本發明一實施例的資訊處理系統 100，其中可注入異動。資訊處理系統 100 包括裸平台硬體 110，其可為能執行任何 OS、VMM、或其他軟體的任何裝置。例如，裸平台硬體 110 可為一個人電腦、一大型主機電腦、一可攜式電腦、一手持式裝置、一機上盒、一伺服器、或任何其他運算系統的硬體。在此實施例中，裸平台硬體 110 包括處理器 120、晶片組 130、系統記憶體 140、以及裝置控制器 150。

處理器 120 可為具有一或多個執行核心的任何部件，其中各個執行核心可依據多種不同類型處理器中的任一種，包括一般用途微處理器，例如 Intel® Pentium®處理器系列、Itanium®處理器系列、或美商英特爾公司出品的其他處理器系列，或另一家公司出品的另一種處理器，或一數位信號處理器或微控制器。雖然第 1 圖僅展示出一個處理器 120，裸處理硬體 110 可包含任何數量的處理器，包括任何數量的多核心處理器，各個多核心處理器具有任何數量的執行核心，以及任何數量的多執行緒處理器，各個多執行緒處理器具有任何數量的執行緒。

晶片組 130 可為支援記憶體操作、輸入/輸出操作、組態、控制、內部或外部介面、連線、或通訊功能(例如，"膠合(glue)"邏輯組件與匯流排橋接器)的任何群組電路與邏

輯組件，及/或用於處理器 120 及/或系統 100 的任何相似功能。可把晶片組 130 的個別元件聚集在一單一晶片上、一對晶片上、在多個晶片之間散佈、及/或部分地、全部地、或冗餘地整合、或根據一種分散方式分散到包括處理器 120 的一或多個處理器中。在此實施例中，晶片組 130 包括根據本發明一實施例來注入異動的虛擬化邏輯組件 132，如下所述。在其他實施例中，虛擬化邏輯組件 132 可包括在系統 100 的他處中。

系統記憶體 140 可包括上面可儲存資訊(例如資料及/或指令)的任何媒體，例如靜態或動態隨機存取記憶體、半導體式唯讀或快閃記憶體、磁性或光學碟片記憶體、或任何其他可由處理器 120 讀取的媒體類型、或該等媒體的任何組合。

裝置控制器 150 可代表 I/O、周邊裝置、或為一中斷請求之來源之其他裝置中任一種的一控制器，例如一硬碟控制器、一音訊控制器、一網路介面控制器、一周邊匯流排控制器等。裝置控制器 150 可體現於一分立部件中，或者可包括在具有任何其他裝置控制器的一種整合式部件中。在一實施例中，裝置控制器 150 可代表多功能 I/O、周邊裝置、或其他裝置控制器中的一項功能。裝置控制器 150 可包括用以儲存組態資訊的組態儲存體 152。

處理器 120、晶片組 130、系統記憶體 140、以及裝置控制器 150 可根據任何已知方法彼此耦合或彼此通訊，例如透過一或多個並列式、連續式、管道式、異步式、同步

式、有線、無線、或其他匯流排或點對點連線或通訊構件直接地或間接地耦合或通訊。例如，在此實施例中，處理器 120 與晶片組 130 可透過介面 170 耦合至系統記憶體 140，且晶片組 130 可透過介面 180 耦合至裝置控制器 150。例如，系統 100 亦可包括任何數量的額外代理器、部件、或連線。

系統 100 亦包括 VMM 160 以及 VM 162 與 VM 164。VMM 160 可為任何軟體、韌體、或受安裝以在裸平台硬體 110 上執行或受裸平台硬體 110 存取的硬體主機，以把 VM (即裸平台硬體 110)的抽象概念呈現給客戶，或者以產生 VM、管理 VM、並且在系統 100 中實行虛擬化策略。在其他實施例中，一主機可為任何 VMM、超級監督器(hypervisor)、OS、或能夠控制裸平台硬體 110 的其他軟體、韌體、或硬體。一客戶可為任何 OS、任何 VMM，包括 VMM 160 的另一個事例、任何超級監督器、或任何應用程式、或其他軟體。

各個客戶期望能存取資源，例如裸平台硬體 110 或由 VMM 160 虛擬化之一平台的處理器與平台暫存器、記憶體、以及輸入/輸出裝置，根據該處理器的架構以及呈現在該 VM 中的該平台而定。第 1 圖展示出 2 個 VM 162 與 VM 164，其各安裝有一客戶 OS 以及任何數量的客戶應用程式。雖然第 1 圖展示出 2 個 VM，在本發明的範圍中，可產生任何數量的 VM，並且可安裝任何數量的客戶 OS 與客戶應用程式以在各個 VM 上執行。

請回頭參照晶片組 130，虛擬化邏輯組件 132 可包括任何電路、邏輯組件、或其他結構，例如韌體，其把實體裝置控制器 150 表示成多個虛擬裝置控制器，各個虛擬裝置控制器被 VMM 160 分配到一不同 VM。晶片組 130 亦包括組態儲存體 134 以及資料儲存體 136。組態儲存體 134 與資料儲存體 136 可包括上面儲存有資訊的任何媒體；例如，組態儲存體 134 可包括可編程暫存器，且資料儲存體 136 可包括靜態隨機存取記憶體。虛擬化邏輯組件 132 可從組態儲存體 134 及/或資料儲存體 136 讀取出資訊，並且把資料寫入到組態儲存體 134 及/或資料儲存體 136 中，以判定並維持與在介面 170 與 180 上抑制並注入異動之狀態有關的資訊。

晶片組 130 可在介面 180 上接收針對系統記憶體 140 的異動，且在介面 170 上接收針對實體裝置控制器 150 的異動。該異動的目標可藉著該異動所傳達的資訊來表示，例如位址欄位的內容。然而，為了支援裝置控制器 150 的虛擬化，該異動可受到虛擬化邏輯組件 132 的抑制。有關於抑制一異動，虛擬化邏輯組件 132 可把與實體裝置控制器 150 相關聯或由其使用的一位址或識別符轉譯成或映射到與從實體裝置控制器 150 摘取出之該等虛擬裝置控制器中之一相關聯或使用的一位址或識別符。虛擬化邏輯組件 132 亦可進行與該受抑制異動相關聯的任何其他處理動作。可把轉譯、映射、或其他處理資訊儲存在組態儲存體 134 或資料儲存體 136 中。虛擬化邏輯組件 132 隨後可做

為一代理器或者介面 170 或介面 180、代表該虛擬裝置控制器啟始或注入一新進異動。

例如，在當中裝置控制器 150 係透過一快速周邊部件互連("PCI-Express")匯流排耦合至晶片組 130 的一實施例中，一異動頭標可包括由系統組態軟體或韌體分派給裝置控制器 150 之匯流排編號、裝置編號、或功能編號("BDF")的一獨特識別符。虛擬化邏輯組件 132 可針對從實體裝置控制器 150 摘取出的各個虛擬裝置控制器使用一個不同的 BDF，因此它可利用實體裝置控制器 150 的 BDF 來抑制異動，並且注入具有對應虛擬裝置控制器之 BDF 的異動，或反之亦然。

第 2 圖展示出根據本發明一實施例的資訊處理系統 100，其中可注入一異動。在第 2 圖之方法實施例的說明中，係參照第 1 圖之系統實施例的元件來進行說明；然而，本發明的方法實施例並不限於此。

在方塊 210 中，係把虛擬化邏輯組件 132 組配成可抑制在通往實體裝置控制器 150 之介面 170 上起始的異動，以及來自實體裝置控制器 150 之介面 180 上的異動。在一實施例中，虛擬化邏輯組件 132 可包括利用基址或其他指示符來編程以識別出欲受抑制之異動之組態儲存體 134 中的一位置。

在方塊 220 中，虛擬化邏輯組件 132 辨識出通往代表實體裝置控制器 150 之一虛擬裝置控制器之介面 170 上的一第一異動。在方塊 222 中，虛擬化邏輯組件抑制該第一

異動，而不是把它轉送到介面 180 供實體裝置控制器 150 接收。在方塊 224 中，虛擬化邏輯組件 132 進行與虛擬化實體裝置控制器 150 有關的轉譯動作或其他處理。在方塊 226 中，虛擬化邏輯組件注入一第二異動到通往實體裝置控制器 150 的介面 180 中。該第二異動用以從該第一異動傳達經轉譯或處理的資訊、訊息、或請求到實體裝置控制器 150，差異在於虛擬化邏輯組件已經進行包含在虛擬化實體裝置控制器 150 中的該轉譯動作或其他處理。

在方塊 230 中，虛擬化邏輯組件 132 辨識出由實體裝置控制器 150 在介面 180 上啟始的一第三異動。在方塊 232 中，虛擬化邏輯組件抑制該第三異動，而不是把它轉送到介面 170。在方塊 234 中，虛擬化邏輯組件 132 進行與虛擬化實體裝置控制器 150 有關的轉譯動作或其他處理。在方塊 236 中，虛擬化邏輯組件代表對應於實體裝置控制器 150 的一虛擬裝置控制器注入一第四異動到介面 170。該第四異動用以傳達來自該實體裝置控制器 150 而從該第三異動轉譯或處理的資訊、訊息、或請求，差異在於虛擬化邏輯組件已經進行包含在虛擬化實體裝置控制器 150 中的該轉譯動作或其他處理。

在本發明的範圍中，可不使用展示出的方塊來進行方法 200、可在方法 200 中增加額外方塊、或者可重新排列方塊、省略方塊、或額外方塊的組合來進行方法 200。

可在各種不同階段中設計根據本發明一實施例的任何部件或一部件部分，從產生到模擬到製成。代表一項設計

的資料可利用多種方式來代表該設計。首先，如模擬方式中使用地，可利用一種硬體描述語言或另一種功能描述語言來表示該硬體。此外或替代地，可在該設計程序的某些階段產生具有邏輯組件及/或電晶體閘的一電路階層模型。再者，大部分的設計在某個階段會到達可藉由代表各種不同裝置之實體配置的資料來模型化的一階層。在當中使用習知半導體製程技術的實例中，代表該裝置配置模型的該資料可為針對用以產生一積體電路的光罩而指明各種不同特徵在不同光罩層上出現或不出現的資料。

在該設計的任何表述中，可把該資料儲存成一機器可讀媒體的任何形式。經調變或產生以發送該種資訊的一光學或電氣波、一記憶體、或一磁性或光學儲存體媒體(例如，一碟片)可為機器可讀媒體。任何該等媒體可"攜載"或"指出"該設計，或用於本發明一實施例的其他資訊。當發送指出或攜載該資訊的一電氣載波而使複製、緩衝、或重新發送該電氣信號的動作能進行時，將可做出一新副本。因此，一通訊提供者或一網路提供者的動作可構成製造出體現本發明技術之一物件(例如，一載波)之副本的動作。

因此，已經揭露了用以注入異動以支援實體裝置控制器之虛擬化的裝置、方法與系統。儘管已經說明了某些實施例並且把該等實施例展示於圖式中，要了解的是該等實施例僅用於展示目的，且不限制本發明的廣泛精神，且本發明並不受限於所展示且解說的特定建構方式與配置，因為熟知技藝者在研讀了本發明的揭示後能進行各種不同的其

他修改方案。在例如本發明的技術領域中，其中已經不容易再看到科技的成長與進步，仍可因能在不偏離本發明的原則或以下申請專利範圍的範圍之狀況下產生技術上的進步，而可容易地修改本發明所揭露實施例的配置方式與細節。

【圖式簡單說明】

第 1 圖展示出根據本發明一實施例之一種用以注入異動的裝置。

第2圖展示出根據本發明一實施例之一種用以注入異動的方法。

【主要元件符號說明】

100	資訊處理系統	150	裝置控制器
110	裸平台硬體	160	虛擬機器監視器 (VMM)
120	處理器		
130	晶片組	162、164	虛擬機器(VM)
132	虛擬化邏輯組件	170、180	介面
134、152	組態儲存體	200	方法
136	資料儲存體	210~236	步驟方塊
140	系統記憶體		

201044276

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：98146734

※申請日：98-12-24　※IPC分類：G06F 9/455 (2006.01)

一、發明名稱：（中文/英文）

注入異動以支援實體裝置控制器之虛擬化的技術

INJECTING TRANSACTIONS TO SUPPORT THE VIRTUALIZATION OF A PHYSICAL DEVICE CONTROLLER

二、中文發明摘要：

本發明揭露用以注入異動以支援實體裝置控制器之虛擬化的裝置、方法與系統之實施例。在一實施例中，一種裝置包括一處理器、系統記憶體、一實體裝置控制器、以及一虛擬化代理器。該實體裝置控制器欲由安裝在一處理器上之一虛擬機器監視器所產生的多個虛擬機器共享。該虛擬化代理器透過一第一介面耦合至該系統記憶體且透過一第二介面耦合至該實體裝置控制器，以把該實體裝置控制器表示為可對該等多個虛擬機器分配的多個虛擬裝置控制器，並且代表該等多個虛擬裝置控制器注入異動到該第一介面以及該第二介面上。

三、英文發明摘要：

Embodiments of apparatuses, methods, and systems for injecting transactions to support the virtualization of a physical device controller are disclosed. In one embodiment, an apparatus includes a processor, system memory, a physical device controller, and a virtualization agent. The physical device controller is to be shared by a plurality of virtual machines created by a virtual machine monitor installed on a processor. The virtualization agent is coupled to the system memory through a first interface and coupled to the physical device controller through a second interface, to represent the physical device controller as a plurality of virtual device controllers available to be allocated to the plurality of virtual machines, and to inject transactions onto the first interface and the second interface on behalf of the plurality of virtual device controllers.

七、申請專利範圍：

1. 一種裝置，其包含：

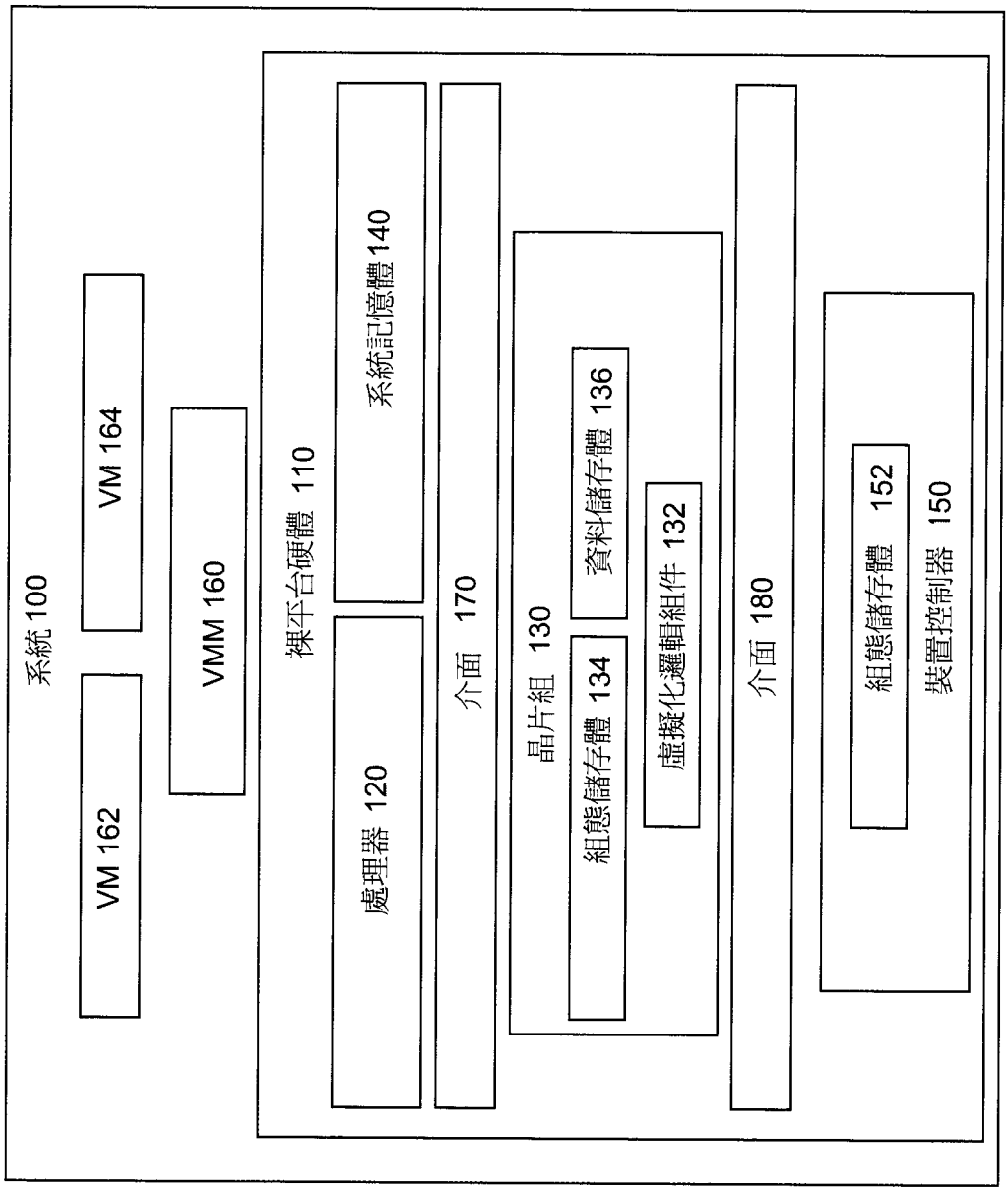
一處理器；

系統記憶體；

一實體裝置控制器，其欲由安裝在該處理器上之一虛擬機器監視器所產生之多個虛擬機器共享；

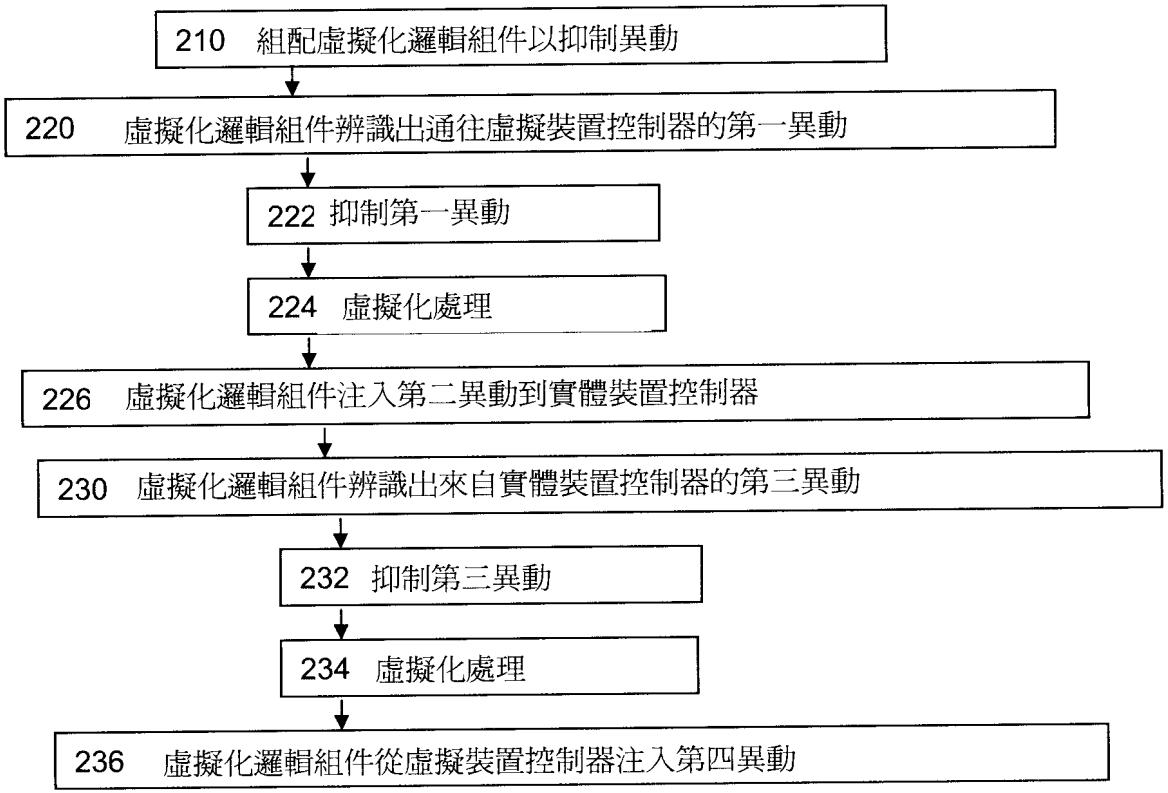
透過一第一介面耦合至該系統記憶體且透過一第二介面耦合至該實體裝置控制器的一虛擬化代理器，其用以把該實體裝置控制器表示為可對該等多個虛擬機器分配的多個虛擬裝置控制器，並且用以代表該等多個虛擬裝置控制器注入異動到該第一介面以及該第二介面上。

第 1 圖


系統 100
VM 162
VM 164
VMM 160
裸平台硬體 110
處理器 120
系統記憶體 140
介面 170
晶片組 130
組態儲存體 134
資料儲存體 136
虛擬化邏輯組件 132
介面 180
組態儲存體 152
裝置控制器 150

第 2 圖

方法 200


210 組配虛擬化邏輯組件以抑制異動
220 虛擬化邏輯組件辨識出通往虛擬裝置控制器的第一異動
222 抑制第一異動
224 虛擬化處理
226 虛擬化邏輯組件注入第二異動到實體裝置控制器
230 虛擬化邏輯組件辨識出來自實體裝置控制器的第三異動
232 抑制第三異動
234 虛擬化處理
236 虛擬化邏輯組件從虛擬裝置控制器注入第四異動

四、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100 資訊處理系統
110 裸平台硬體
120 處理器
130 晶片組
132 虛擬化邏輯組件
134、152 組態儲存體
136 資料儲存體
140 系統記憶體
150 裝置控制器
160 虛擬機器監視器(VMM)
162、164 虛擬機器(VM)
170、180 介面

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：