



(19)中華民國智慧財產局

(12)發明說明書公告本

(11)證書號數：TW I844082 B

(45)公告日：中華民國 113 (2024) 年 06 月 01 日

(21)申請案號：111132505

(22)申請日：中華民國 111 (2022) 年 08 月 29 日

(51)Int. Cl. : G06F9/455 (2006.01)

G06F9/44 (2018.01)

(30)優先權：2022/06/30 美國

17/853,950

2021/09/17 美國

63/245,235

(71)申請人：聯發科技股份有限公司 (中華民國) MEDIATEK INC. (TW)

新竹市篤行一路一號

(72)發明人：蕭志祥 HSIAO, CHIH-HSIANG (TW)；隋培倫 SUEI, PEI-LUN (TW)；許育淇 CHU, YU-CHI (TW)

(74)代理人：吳豐任；戴俊彥

(56)參考文獻：

TW 201944280A

EP 2606450B1

US 9520994B2

US 2013/0347131A1

審查人員：易昶霈

申請專利範圍項數：18 項 圖式數：6 共 30 頁

(54)名稱

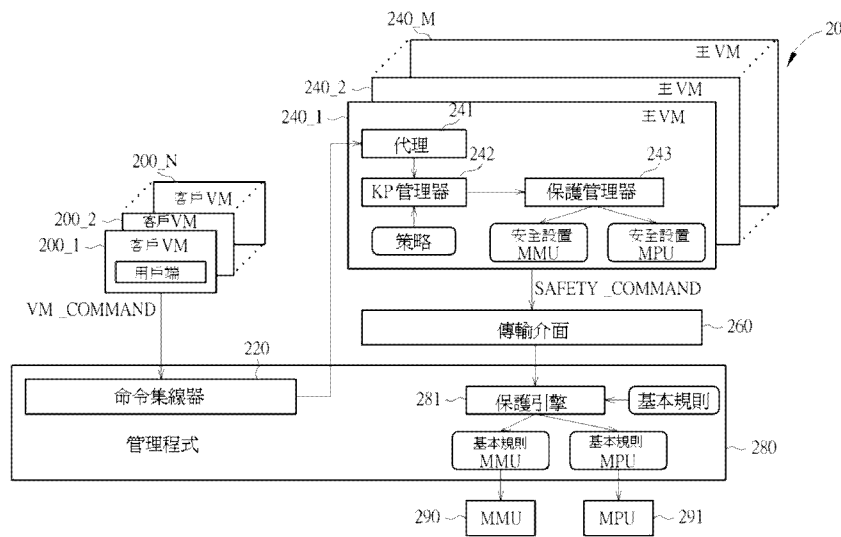
用於內核保護的系統、命令集線器以及主虛擬機

(57)摘要

本發明提供了一種內核保護的系統、命令集線器以及主虛擬機。內核保護系統包括處理器和傳輸介面。處理器執行至少一個客戶虛擬機(VM)、至少一個主 VM 和管理程式。至少一個客戶 VM 可以將至少一個命令發送到命令集線器。至少一個主 VM 接收命令集線器發送的至少一個命令，接收對應於至少一個客戶 VM 的至少一個策略，並根據命令和策略來管理和配置安全設置。管理程式接收基本規則和至少一個安全設置命令，並根據基本規則和設置命令，管理和配置至少一個安全保護元件。傳輸介面將至少一個主 VM 綁定到管理程式，執行至少一個主 VM 與管理程式之間的通信。

The present invention provides a system for kernel protection, a command hub and a primary virtual machine. The system for kernel protection includes a processor and a transmission interface. The processor is arranged to execute at least one guest virtual machine (VM), at least one primary VM, and a hypervisor. The at least one guest VM is arranged to send at least one command to a command hub. The at least one primary VM is arranged to manage and configure a safety setting according to the at least one command from the command hub and at least one policy, and manage and configure a safety protection component according to the safety setting. The hypervisor is arranged to manage and configure the safety protection component according to a ground rule and at least one safety setting command from the at least one primary VM. The transmission interface is arranged to bind the at least one primary VM to the hypervisor.

指定代表圖：



281:保護引擎

第2圖



I844082

【發明摘要】

公告本

【中文發明名稱】用於內核保護的系統、命令集線器以及主虛擬機

【英文發明名稱】A SYSTEM FOR KERNEL PROTECTION, A COMMAND HUB
AND A PRIMARY VIRTUAL MACHINE

【中文】

本發明提供了一種內核保護的系統、命令集線器以及主虛擬機。內核保護系統包括處理器和傳輸介面。處理器執行至少一個客戶虛擬機(VM)、至少一個主VM和管理程式。至少一個客戶VM可以將至少一個命令發送到命令集線器。至少一個主VM接收命令集線器發送的至少一個命令，接收對應於至少一個客戶VM的至少一個策略，並根據命令和策略來管理和配置安全設置。管理程式接收基本規則和至少一個安全設置命令，並根據基本規則和設置命令，管理和配置至少一個安全保護元件。傳輸介面將至少一個主VM綁定到管理程式，執行至少一個主VM與管理程式之間的通信。

【英文】

The present invention provides a system for kernel protection, a command hub and a primary virtual machine. The system for kernel protection includes a processor and a transmission interface. The processor is arranged to execute at least one guest virtual machine (VM), at least one primary VM, and a hypervisor. The at least one guest VM is arranged to send at least one command to a command hub. The at least one primary VM is arranged to manage and configure a safety setting according to the at least one command from the command hub and at least one policy, and manage and configure a safety protection component according to the safety setting. The

第 1 頁，共 3 頁(發明摘要)

hypervisor is arranged to manage and configure the safety protection component according to a ground rule and at least one safety setting command from the at least one primary VM. The transmission interface is arranged to bind the at least one primary VM to the hypervisor.

【指定代表圖】第（ 2 ）圖。

【代表圖之符號簡單說明】

- 20:內核保護系統
- 260:傳輸介面
- 220:命令集線器
- 280:管理程式
- 200_1~200_N:客戶VM
- 240_1~240_M:主VM
- 241:代理
- 242:內核保護管理器
- 243:保護管理器
- 290:MMU
- 291:MPU
- 281:保護引擎

【特徵化學式】

無

【發明說明書】

【中文發明名稱】用於內核保護的系統、命令集線器以及主虛擬機

【英文發明名稱】A SYSTEM FOR KERNEL PROTECTION, A COMMAND HUB
AND A PRIMARY VIRTUAL MACHINE

【技術領域】

【0001】 本發明涉及對於作業系統中內核進行保護，以提高包含內核保護系統的產品的性能。

【先前技術】

【0002】 對於使用單片（monolithic）作業系統(例如Linux)作為內核的Android高級作業系統(operating system，OS)，如果內核運行過多的驅動器或軟體，內核中就會出現安全性漏洞。為了解決這個問題，通常通過管理程式（hypervisor）為帶有網路應用程式的設備制定內核保護產品，其中內核保護機制通過監控、過濾和保護來確保能夠感知和阻止漏洞和洩漏。

【0003】 另外，基於性能和成本的考慮，通常使用更薄更輕的管理程式（hypervisor）來進行內核保護。帶有管理程式的系統支援太多客戶（guest）虛擬機（virtual machine，VM）時，管理程式的管理能力可能會不足（例如，管理程式可以運行的軟體的複雜度會受到限制，管理程式可能會難以有效地進行安全分析），並且系統可能存在安全問題（例如管理程式內部的內核保護機制會對管理程式造成危害）。因此，迫切需要一種新型系統可以為管理程式共用管理以釋放（release）管理程式的複雜度。

第 1 頁，共 17 頁(發明說明書)

【發明內容】

【0004】 有鑑於此，本發明提供了一種用於內核保護的系統、命令集線器、以及主虛擬機(VM)，來解決上述問題。

【0005】 根據本發明的至少一個實施例，提供了一種內核保護系統。該系統可以包括處理器和傳輸介面。處理器可以被佈置為執行至少一個客戶虛擬機(VM)、至少一個主VM和管理程式。至少一個客戶VM可以被佈置為將至少一個命令發送到命令集線器。所述至少一個主VM可以被設置為：接收命令集線器發送的至少一個命令，接收對應於至少一個客戶VM的至少一個策略，並根據所述至少一個命令和所述至少一個策略來管理和配置安全設置。管理程式可用於接收基本規則和至少一個主VM發送的至少一個安全設置命令，並根據基本規則和至少一個安全設置命令，管理和配置至少一個安全保護元件。傳輸介面可用於將至少一個主VM綁定到管理程式，並執行至少一個主VM與管理程式之間的通信。

【0006】 根據本發明的至少一個實施例，提供了一種在處理器上運行或由純硬體實現的命令集線器。命令集線器可以被佈置成接收從至少一個客戶虛擬機(VM)發送的至少一個命令，並且將至少一個命令發送到至少一個主VM，其中從命令集線器發送的至少一個命令與對應於至少一個客戶VM的至少一個策略一起用於管理和配置至少一個客戶VM的安全設置，並且安全設置用於管理和配置安全保護元件。

【0007】 根據本發明的至少一個實施例，提供了一種在處理器上運行的主虛

擬機(VM)。主VM可以包括代理、內核保護管理器和保護管理器。該代理可以被佈置為接收從至少一個訪客VM發送的至少一個命令。內核保護管理器可用於接收代理發送的至少一個命令和至少一個策略，並根據至少一個命令和至少一個策略，管理和配置至少一個客戶虛擬機的安全設置。保護管理器可用於根據內核保護管理器提供的安全設置來管理和配置安全保護元件。

【0008】 本發明的優勢之一是，通過主VM共用對管理程式的管理（即將管理程式的至少一部分管理任務卸載到主VM），管理程式的複雜度可以被緩解，並且可能使得客戶VM能夠運行更複雜的軟體。此外，客戶VM的供應商無需將策略集成到管理程式中，只需將策略提供給主VM即可。因此，可以提高包括內核保護系統的產品在量產階段的成本、便利性和安全性。換句話說，管理程式只需要執行一個基本規則（即，分別對應客戶VM的策略可以由主VM執行），這使得管理程式更加安全。由於策略的執行損失不是主要損失，因此包含內核保護系統的產品性能不會下降。

【0009】 在閱讀了在各種附圖和附圖中示出的優選實施例的以下詳細描述之後，本發明的這些和其他目的對於本領域習知技藝者無疑將變得顯而易見。

【圖式簡單說明】

【0010】

第1圖為本發明一實施例的電子設備的示意圖。

第2圖為根據本發明一實施例的內核保護系統的示意圖。

第3圖為根據本發明另一實施例的內核保護系統的示意圖。

第4圖是例示根據本發明的實施例的具有一個客戶VM和兩個主VM用於內核保

護和DMA保護的系統的示意圖。

第5圖是例示根據本發明實施例的具有兩個客戶VM和三個主VM用於內核保護、DMA保護和隔離執行環境保護的系統的示意圖。

第6圖是例示根據本發明實施例的具有一個客戶VM和兩個主VM的用於兩個應用程式(APP)保護的系統的示意圖。

【實施方式】

【0011】 在說明書及申請專利範圍當中使用了某些詞彙來指稱特定的元件。本領域技術人員應可理解，電子設備製造商可以會用不同的名詞來稱呼同一元件。本說明書及申請專利範圍並不以名稱的差異來作為區別元件的方式，而是以元件在功能上的差異來作為區別的基準。在通篇說明書及後續的申請專利範圍當中所提及的“包括”是開放式的用語，故應解釋成“包括但不限定於”。此外，“耦接”一詞在此是包含任何直接及間接的電氣連接手段。因此，若文中描述第一裝置電性連接於第二裝置，則代表該第一裝置可直接連接於該第二裝置，或通過其他裝置或連接手段間接地連接至該第二裝置。

【0012】 下面的描述是為了說明本發明的一般原理而作出的，不應理解為限制性的。本發明的範圍最好通過參考所附申請專利範圍來確定。

【0013】 第1圖為本發明一實施例的電子設備10的示意圖。作為示例而非限制，電子設備10可以是可攜式設備，例如智慧手機或平板電腦。電子設備10可以包括處理器12、存放裝置14和硬體電路16。處理器12可以是單核處理器或多核處理器。存放裝置14是電腦可讀介質，用於存儲電腦程式代碼PROG。處理器12配備有軟體執行能力。電腦程式代碼PROG可以包括多個軟體模組。因此，當

第 4 頁，共 17 頁(發明說明書)

由處理器12載入並執行時，電腦程式代碼PROG可以指示處理器12執行軟體模組的指定功能。電子設備10可以被視為使用電腦程式產品的電腦系統，該電腦程式產品包括具有電腦程式代碼的電腦可讀介質。硬體電路16是純硬體，其可以僅由邏輯門組成，並且無需軟體執行即可執行指定功能。關於本發明提出的內核保護系統，它可以實現在電子設備10上。例如，內核保護系統可以包括由在處理器12上運行的電腦程式代碼PROG實現的基於軟體的功能和由硬體電路16實現的基於硬體的功能。

【0014】 第2圖為根據本發明一實施例的內核保護系統20的示意圖。系統20可以包括處理器(例如第1圖中所示的處理器12)和傳輸介面 (transmission interface) 260。處理器可以被佈置為執行軟體模組，軟體模組包括一個或多個客戶 (guest) 虛擬機(virtual machine, VM) 200_1、200_2、...、200_N ($N \geq 1$)、一個或多個主 (primary) VM 240_1、240_2、...、240_M ($M \geq 1$)、以及管理程式 280。客戶 VM 200_1、200_2、...、200_N 可以由不同的供應商提供，並且“N”和“M”是可以相等也可以不同的正整數。此外，處理器還可被設置為執行命令集線器 (command hub) 220，命令集線器220是集成在管理程式280中的軟體模組，但本發明不限於此。在一些實施例中，命令集線器220可以是在處理器上執行的管理程式280外部的硬體元件。在一些實施例中，傳輸介面260可以通過軟體或硬體來實現。

【0015】 參照第2圖，客戶VM 200_1、200_2、.....、200_N中的每一個可以用於將至少一個命令VM_COMMAND發送到命令集線器220。例如，客戶VM 200_1可以是具有Linux內核的Android VM，其中Android VM中的至少一個用戶端 (client) 可以將至少一個命令VM_COMMAND發送到命令集線器220。在一

些實施例中，Android VM中的至少一個應用程式也能夠將至少一個命令VM_COMMAND發送到命令集線器220。主VM 240_1、240_2、...、240_M中的每一個可以包括代理（agent）241、內核保護管理器242（為了簡潔，在第2圖中標記為“KP管理器”）和保護管理器（protection manager）243。命令集線器220可以被佈置成將至少一個命令VM_COMMAND廣播到主VM 240_1、240_2、...、240_M中的每個代理241，或者可以根據至少一個命令VM_COMMAND 的類型將至少一個命令VM_COMMAND發送到從主VM 240_1、240_2、...、240_M中選擇的主VM的特定代理。因此，命令集線器220可以被佈置為執行客戶VM 200_1、200_2、...、200_N和主VM 240_1、240_2、...、240_M之間的通信。

【0016】 代理241可以被佈置成接收從命令集線器220發送的至少一個命令VM_COMMAND。內核保護管理器242可以被佈置成接收來自代理241的至少一個命令VM_COMMAND以及接收至少一個策略（policy），其中策略可例如與要設為僅可讀取或不能運行的區間、監控或過濾的信號、發生事件的錯誤處理等相關的資訊，並且根據至少一個命令VM_COMMAND和至少一個策略，管理和配置用於客戶VM 200_1、200_2、...、200_N的安全設置（safety setting），其中安全設置可以包括內核保護、直接記憶體存取(direct memory access，DMA)保護、隔離的執行環境（isolated execution environment）保護、應用程式保護或任何其他類型的內核保護，並且至少一個策略對應於客戶VM 200_1、200_2、...、200_N。需要注意的是，主VM 240_1、240_2、...、240_M的安全設置是相互獨立的。

【0017】 主VM 240_1、240_2、.....、240_M中的每一個可以具有相同或相似的架構。以主VM 240_1 為例，主VM 240_1可以包括代理241、內核保護管理器242和保護管理器243。代理241可以被佈置為接收從命令集線器220發送的至少

一個命令VM_COMMAND。內核保護管理器242可以用於接收代理241發送的至少一個命令VM_COMMAND以及接收對應於客戶VM 200_1的策略，並根據至少一個命令VM_COMMAND和策略，管理和配置客戶VM 200_1的安全設置。

【0018】 在本實施例中，對應于客戶VM 200_1的策略(policy)由主VM 240_1的內核保護管理器242接收；對應于客戶VM 200_2的策略由主VM 240_2的內核保護管理器(未示出)接收；並且對應于客戶VM 200_N的策略由主VM 240_M的內核保護管理器(未示出)接收(即， $N = M$ 並且客戶VM 200_1、200_2、...、200_N分別對應於主VM 240_1、240_2、...、240_M)。然而，本發明不限於此。在一些實施例中，主VM 240_1、240_2、...、240_M可以僅包括一個主VM 240_1(即 $M = 1$)，並且與客戶VM 200_1、200_2、...、200_N分別對應的多個策略可以由主VM 240_1的內核保護管理器242接收。在一些實施例中，客戶VM 200_1、200_2、...、200_N可以僅包括一個客戶VM 200_1(即 $N = 1$)，並且對應于客戶VM 200_1的策略可以由主VM 240_1、240_2、...、240_M的內核保護管理器接收。

【0019】 保護管理器243可以被佈置為根據內核保護管理器242提供的安全設置來管理和配置安全保護元件(safety protection component)，其中安全保護元件可以包括記憶體管理單元(Memory Management Unit, MMU)290和/或記憶體保護單元(Memory Protection Unit, MPU) 291。例如，客戶VM 200_1通過命令集線器220向主VM 240_1發送用於內核保護的命令，代理241可以被佈置為從命令集線器220接收該命令，並且內核保護管理器242可用於接收來自代理241的命令以及接收對應于客戶VM 200_1的策略，並根據命令和策略來管理和配置客戶VM 200_1的安全設置(即內核保護)。之後，保護管理器243可根據內核保護管理器242提供的安全設置，管理和配置安全保護元件(例如，MMU 290和/或MPU 291)。

【0020】 傳輸介面260可以被佈置為將主VM 240_1、240_2、...、240_M綁定（bind）到管理程式（hypervisor）280，並執行主VM 240_1、240_2、...、240_M和管理程式280之間的通信。以這種方式，只有通過傳輸介面260綁定到管理程式280的主VM才能與管理程式280進行通信（例如發送安全設置命令給管理程式280以進行後續操作），從而防止其他非法使用者使用系統20。管理程式280可以包括保護引擎（protection engine）281，其中保護引擎281可以被佈置為接收基本規則（ground rule）和由主VM 240_1、240_2、...、240_M通過傳輸介面260發送的至少一個安全設置命令SAFETY_COMMAND，並根據基本規則和至少一個安全設置命令SAFETY_COMMAND，管理和配置安全保護元件(例如MMU 290和/或MPU 291)。需要注意的是，基本規則由管理程式280執行，並且主VM 240_1、240_2、...、240_M和管理程式280均遵循該基本規則，基本規則的一個示例可例如為在區塊開機後就一定是僅可讀取不可寫入，任何策略都不讓其設為可寫入。

【0021】 通過主VM 240_1、240_2、...、240_M共用對管理程式280的管理，即，將管理程式280的至少一部分管理任務卸載到主VM 240_1、240_2、...、240_M，可以減輕管理程式280的複雜度（即管理程式280可以只需要執行保護機制的操作），並且客戶VM 200_1、200_2、...、200_N能夠運行更複雜的軟體。此外，客戶VM 200_1、200_2、...、200_N的供應商只需將策略提供給主VM 240_1、240_2、...、240_M，而不是將策略集成到管理程式280中。因此，可以提高包括系統20的產品在大規模生產階段的成本、便利性和安全性。換言之，管理程式280只需要執行基本規則（其中分別對應于客戶VM 200_1、200_2、...、200_N的策略可以由主VM 240_1、240_2、...、240_M執行），這使得管理程式 280 更

加安全。由於策略的執行損失不是主要損失，包含系統20的產品的性能不會下降。

【0022】 第3圖為根據本發明另一實施例的內核保護系統30的示意圖。系統30可以包括處理器(例如第1圖中所示的處理器12)、命令集線器320和傳輸介面360。處理器可以被佈置為執行軟體模組，軟體模組包括一個或多個客戶VM 300_1、300_2、...、300_N ($N \geq 1$)、一個或多個主VM 340_1、340_2、...、340_M ($M \geq 1$) 和管理程式380。客戶VM 300_1、300_2、...、300_N 可以由不同的供應商提供，並且“N”或“M”是可以彼此相等或不同的正整數。第3圖所示的系統30與第2圖所示的系統20的不同之處在於系統30的命令集線器320是在處理器上執行的管理程式380外部的硬體元件。例如，命令集線器320可以是第1圖所示的硬體電路16的一部分。在一些實施例中，傳輸介面360可以通過軟體或硬體來實現。為簡潔起見，本實施例類似的描述在此不再贅述。

【0023】 第4圖是例示根據本發明的實施例的具有一個客戶VM和兩個主VM用於內核保護和DMA保護的系統40的示意圖。第4圖中所示的系統40可以由第2圖所示的系統20來實現。技術人員應該容易理解也可以採用第3圖中所示的系統30來實現具有一個客戶VM和兩個主VM用於內核保護和DMA保護的系統。系統40可以包括處理器(例如，第1圖中所示的處理器12)和傳輸介面460。處理器可以被佈置為執行客戶VM 400、命令集線器420、兩個主VM 440_1和440_2、以及管理程式480。在本實施例中，命令集線器420是集成在管理程式480中的軟體模組，但本發明不限於此。命令集線器420也可以在管理程式480外部實現。如第4圖所示，客戶VM 400可以是具有Linux內核的安卓Android虛擬機，客戶VM 400中有兩個用戶端。例如，一個用戶端是手機製造商 (phone maker)，另一個用戶

端是晶片廠商 (chip vendor)，其中手機製造商可以向命令集線器420發送命令COMMAND_KERNEL，用於對在客戶VM 400上運行的Linux進行內核保護，並且晶片供應商可以向命令集線器420發送命令COMMAND_DMA，用於對在客戶VM 400上運行的Linux進行DMA保護。

【0024】 主 VM 440_1 可以被佈置為：從命令集線器 420 接收命令COMMAND_KERNEL 以及接收對應于客戶 VM 400 的策略；根據命令COMMAND_KERNEL 和策略，管理和配置客戶VM 400的安全設置（例如內核保護）；根據安全設置，管理和配置安全保護元件（例如MMU 490和/或MPU 491）。另外，主VM 440_1可以被佈置為通過傳輸介面460向管理程式480發送安全設置命令SAFETY_KERNEL_COMMAND(在第4圖中標記為“SKC”)。簡潔起見，在第4圖中標記的“內核保護”可以包括代理、內核保護管理器、保護管理器以及主VM 440_1的上述操作。

【0025】 主 VM 440_2 可以被佈置為：接收來自命令集線器 420 的命令COMMAND_DMA 以及接收對應于客戶 VM 400 的策略；根據命令COMMAND_DMA 和策略，管理和配置用於客戶VM 400的安全設置（例如DMA 保護）；根據安全設置，管理和配置安全保護元件（例如MMU 490和/或MPU 491）。另外，主VM 440_2可以被佈置為通過傳輸介面460向管理程式480發送安全設置命令SAFETY_DMA_COMMAND(在第4圖中標記為“SDC”)。簡潔起見，在第4圖中標記的“DMA保護”可以包括代理、內核保護管理器、保護管理器以及主VM 440_2的上述操作。

【0026】 管理程式480可以被佈置為接收基本規則 (ground rule) 和兩個安全

第 10 頁，共 17 頁(發明說明書)

設置命令SAFETY_KERNEL_COMMAND和SAFETY_DMA_COMMAND，並根據基本規則和兩個安全設置命令 SAFETY_KERNEL_COMMAND 和 SAFETY_DMA_COMMAND，管理和配置安全保護元件（例如，MMU 490和/或MPU 491）。簡潔起見，在第4圖中標記的“KP”可以包括管理程式480的保護引擎和上述操作。在本實施例中，主VM 440_1的安全設置(即內核保護)和主VM 440_2的安全設置(即DMA保護)彼此獨立。因此，手機製造商和晶片供應商可以分別獨立地執行內核保護和 DMA 保護，而無需在管理程式480中整合式軟體。

【0027】 需要理解的是，在一些實施例中，內核保護和DMA保護可以根據設計需求通過同一個主VM來執行。例如，處理器可以被佈置為僅執行一個主VM(例如，主VM 440_1)。主VM 440_1可以被佈置為：從命令集線器420接收命令COMMAND_KERNEL和COMMAND_DMA以及接收對應于客戶VM 400的策略；根據命令COMMAND_KERNEL、命令COMMAND_DMA和策略，管理和配置客戶VM 400的安全設置（例如內核保護和DMA保護）；根據安全設置，管理和配置安全保護元件（例如MMU 490和/或MPU 491）。此外，主VM 440_1可以被設置為通過傳輸介面 460 向管理程式 480 發送安全設置命令 SAFETY_KERNEL_COMMAND和SAFETY_DMA_COMMAND。簡潔起見，對於這些實施例的類似描述在此不再詳細重複。

【0028】 第5圖是例示根據本發明實施例的具有兩個客戶VM和三個主VM用於內核保護、DMA保護和隔離執行環境保護的系統50的示意圖。第5圖所示的系統50可以由第2圖所示的系統20來實現。技術人員應該容易理解，也可以採用第3圖中所示的系統30，來實現具有兩個客戶VM和三個主VM的系統，用於內核保護、DMA保護和隔離執行環境保護。系統50可以包括處理器(例如第1圖中所示

的處理器12)和傳輸介面560。處理器可以被佈置為執行兩個客戶VM 500_1和500_2、命令集線器520、三個主VM 540_1、540_2和540_3、以及管理程式580。在本實施例中，命令集線器520是集成在管理程式580中的軟體模組，但本發明不限於此。如第5圖所示，客戶VM 500_1可以是具有Linux內核的Android VM，客戶VM 500_1中有兩個用戶端。例如，一個客戶是電話製造商，另一個客戶是晶片供應商，其中電話製造商可以向命令集線器520發送命令COMMAND_KERNEL，用於對在客戶VM 500_1上運行的Linux的內核保護，晶片供應商可以向命令集線器520發送命令COMMAND_DMA，用於對在客戶VM 500_1上運行的Linux的DMA保護。客戶VM 500_2可以用於隔離執行環境(isolated execution environment)(在第5圖中標記為“IEE”)的VM，其中客戶VM 500_2中的用戶端可以向命令集線器520發送用於隔離執行環境保護的命令COMMAND_IEE。

【0029】 主VM 540_1可以被佈置為：從命令集線器520接收命令COMMAND_KERNEL以及接收對應于客戶VM 500_1的策略；根據命令COMMAND_KERNEL和策略，管理和配置客戶VM 500_1的安全設置(例如內核保護)；根據安全設置，管理和配置安全保護元件(例如MMU 590和/或MPU 591)。此外，主VM 540_1可以被佈置為通過傳輸介面560向管理程式580發送安全設置命令SAFETY_KERNEL_COMMAND(在第5圖中標記為“SKC”)。簡潔起見，在第5圖中標記的“內核保護”可以包括代理、內核保護管理器、保護管理器以及主VM 540_1的上述操作。

【0030】 主VM 540_2可以被佈置為：從命令集線器520接收命令COMMAND_DMA以及接收對應于客戶VM 500_1的策略；根據命令

第 12 頁，共 17 頁(發明說明書)

COMMAND_DMA 和策略，管理和配置客戶VM 500_1 的安全設置(例如 DMA 保護)；根據安全設置，管理和配置安全保護元件(例如MMU 590和/或MPU 591)。此外，主VM 540_2可以被佈置為通過傳輸介面560向管理程式580發送安全設置命令SAFETY_DMA_COMMAND(在第5圖中標記為“SDC”)。簡潔起見，在第5圖中標記的“DMA保護”可以包括代理、內核保護管理器、保護管理器以及主VM 540_2的上述操作。

【0031】 主 VM 540_3 可以被佈置為：從命令集線器 520 接收命令 COMMAND_IEE 以及接收對應于客戶 VM 500_2 的策略；根據命令 COMMAND_IEE和策略，管理和配置客戶VM 500_2的安全設置(例如隔離執行環境保護)；根據安全設置，管理和配置安全保護元件(例如MMU 590和/或MPU 591)。此外，主VM 540_3可以被佈置為通過傳輸介面560向管理程式580發送安全設置命令SAFETY_IEE_COMMAND(在第5圖中標記為“SIC”)。簡潔起見，在第5圖中標記的“IEE保護”可以包括代理、內核保護管理器、保護管理器以及主VM 540_3的上述操作。

【0032】 管理程式 580 可被佈置為接收基本規則和三個安全設置命令 SAFETY_KERNEL_COMMAND 、 SAFETY_DMA_COMMAND 和 SAFETY_IEE_COMMAND ， 並根據基本規則和三個安全設置命令 SAFETY_KERNEL_COMMAND 、 SAFETY_DMA_COMMAND 和 SAFETY_IEE_COMMAND，管理和配置安全保護元件(例如MMU 590和/或MPU 591)，在第5圖中標記的“KP”可以包括管理程式580的保護引擎和上述操作。需要注意的是，主VM 540_1的安全設置(即內核保護)、主VM 540_2的安全設置(即DMA保護)和主VM 540_3的安全設置(即隔離執行環境保護)相互獨立。

第 13 頁，共 17 頁(發明說明書)

【0033】 需要說明的是，在一些實施例中，根據設計需求可以通過同一個主VM來執行內核保護、DMA保護和隔離執行環境保護中的至少兩者。例如，處理器可以被佈置為僅執行一個主VM(例如，主VM 540_1)。主VM 540_1可以被佈置為：從命令集線器520接收命令COMMAND_KERNEL、COMMAND_DMA和COMMAND_IEE以及接收分別對應于客戶VM 500_1和客戶VM 500_2的策略；根據命令 COMMAND_KERNEL、COMMAND_DMA、COMMAND_IEE 和策略，管理和配置客戶VM 500_1和客戶VM500_2的安全設置(例如，內核保護、DMA 保護和隔離執行環境保護)；根據安全設置，管理和配置安全保護元件(例如MMU 590和/或MPU 591)。此外，主VM 500_1可以被佈置為通過傳輸介面560向管理程式 580 發送安全設置命令 SAFETY_KERNEL_COMMAND、SAFETY_DMA_COMMAND和SAFETY_IEE_COMMAND。再例如，處理器可以被佈置為執行兩個主VM(例如，主VM 540_1和VM 540_2)。主VM 540_1可以被佈置為從命令集線器 520 接收命令 COMMAND_KERNEL 和COMMAND_DMA以及接收對應于客戶VM 500_1的策略。主VM 540_2可以被佈置為從命令集線器520接收命令COMMAND_IEE以及接收對應于客戶VM 500_2的策略。簡潔起見，對於這些實施例的類似描述在此不再贅述。

【0034】 第6圖是例示根據本發明實施例的具有一個客戶VM和兩個主VM的用於兩個應用程式(APP)保護的系統60的示意圖。第6圖中所示的系統60可以由第2圖所示的系統20來實現。技術人員應該容易理解，也可以採用第3圖中所示的系統3來實現具有一個客戶VM和兩個主VM的系統用於兩個APP保護。系統60可以包括處理器(例如，第1圖中所示的處理器12)和傳輸介面660。處理器可以被佈置為執行客戶VM 600、命令集線器620、兩個主VM 640_1和640_2以及管理程

第 14 頁，共 17 頁(發明說明書)

式680。在本實施例中，命令集線器620是集成在管理程式680中的軟體模組，但本發明不限於此。如第6圖所示，客戶VM 600可以是具有Linux內核的Android VM，並且在客戶VM 600上運行有兩個APP(例如，APP A和APP B)，其中APP A可以向命令集線器620發送命令COMMAND_APPA用於APP A的APP保護，APP B可以向命令集線器620發送另一命令COMMAND_APPB用於APP B的APP保護。

【0035】 主VM 640_1可以被佈置為：從命令集線器620接收命令COMMAND_APPA以及接收對應于客戶VM 600的策略；根據命令COMMAND_APPA和策略，管理和配置客戶VM 600的安全設置（例如APP A的APP保護）；根據安全設置，管理和配置安全保護元件（例如MMU 690和/或MPU 691）。此外，主VM 640_1可以被佈置為通過傳輸介面660向管理程式680發送安全設置命令SAFETY_APPA_COMMAND(在第6圖中標記為“SAC”)。簡潔起見，在第6圖中標記的“APP A保護”可以包括代理、內核保護管理器、保護管理器以及主VM 640_1的上述操作。

【0036】 主VM 640_2可以被佈置為：接收來自命令集線器620的命令COMMAND_APPB以及接收對應于客戶VM 600的策略；根據命令COMMAND_APPB和策略，管理和配置客戶VM 600的安全設置（例如APP B的APP保護）；並根據安全設置，管理和配置安全保護元件（例如MMU 690和/或MPU 691）。此外，主VM 640_2可以被設置為通過傳輸介面660向管理程式680發送安全設置命令SAFETY_APPB_COMMAND(在第6圖中標記為“SBC”)。簡潔起見，在第6圖中標記的“APP B保護”可以包括代理、內核保護管理器、保護管理器以及主VM 640_2的上述操作。

【0037】 管理程式680可以被佈置為接收基本規則和兩個安全設置命令 SAFETY_APPA_COMMAND和SAFETY_APPB_COMMAND，並且根據基本規則和兩個安全設置命令 SAFETY_APPA_COMMAND 和 SAFETY_APPB_COMMAND，管理和配置安全保護元件（例如，MMU 690和/或MPU 691）。簡潔起見，在第6圖中標記的“KP”可以包括管理程式680的保護引擎和上述操作。在本實施例中，主VM 640_1的安全設置(例如APP A的APP保護)和主VM 640_2的安全設置(例如APP B的APP保護)彼此獨立。因此，APP A和APP B可以由不同的供應商提供。

以上所述僅為本發明之較佳實施例，凡依本發明申請專利範圍所做之均等變化與修飾，皆應屬本發明之涵蓋範圍。

【符號說明】

【0038】

10:電子設備

12:處理器

14:存放裝置

16:硬體電路

20, 30:內核保護系統

40:內核保護和DMA保護的系統

50:內核保護、DMA保護和隔離執行環境保護的系統

60:應用程式(APP)保護的系統

260, 360, 460, 560, 660:傳輸介面

第 16 頁，共 17 頁(發明說明書)

220, 320, 420, 520, 620:命令集線器

280, 380, 480, 580, 680:管理程式

200_1~200_N, 300_1~300_N, 400, 500_1, 500_2, 600:客VM

240_1~240_M, 340_1~340_M, 440_1, 440_2, 540_1~ 540_3, 640_1, 640_2:主VM

241, 341:代理

242, 342:內核保護管理器

243, 343:保護管理器

290, 390, 490, 590, 690: MMU 291, 391, 491, 591, 691: MPU 281, 381:保護引擎

【發明申請專利範圍】

【請求項1】 一種用於內核保護的系統，包括：

處理器，用於執行：

至少一個客戶虛擬機(VM)，其中所述至少一個客戶VM被設置為向命令集線器發送至少一個命令；

至少一個主VM，其中所述至少一個主VM用以接收從所述命令集線器發送的所述至少一個命令以及接收對應於所述至少一個客戶VM的至少一個策略，並根據所述至少一個命令以及所述至少一個策略，管理及配置安全設置；以及

管理程式，用於接收所述至少一個主VM發送的至少一個安全設置命令，並根據所述至少一個安全設置命令，管理和配置至少一個安全保護元件；

其中所述至少一個客戶VM、所述至少一個主VM以及所述管理程式為該處理器執行的軟體模組；

其中所述命令集線器是集成在所述管理程式中的軟體模組或所述命令集線器是在所述處理器上執行的所述管理程式外部的硬體元件；

所述系統還包括：

傳輸介面，用於將所述至少一個主VM綁定到所述管理程式，並執行所述至少一個主VM與所述管理程式之間的通信；

其中所述傳輸介面通過軟體或硬體實現。

【請求項2】 如請求項1之系統，其中，所述至少一個主VM包括多個主VM，並且所述多個主VM的安全設置彼此獨立。

【請求項3】 如請求項1之系統，其中，所述安全保護元件包括記憶體管理單元(MMU)或記憶體保護單元(MPU)。

【請求項4】 如請求項1之系統，其中，所述安全設置包括內核保護、直接記憶體存取(DMA)保護、隔離執行環境保護和應用程式保護中的至少一種。

【請求項5】 如請求項1之系統，其中所述管理程式還接收基本規則，所述基本規則由所述管理程式執行，並且所述至少一個主VM和所述管理程式遵循所述基本規則。

【請求項6】 如請求項1之系統，其中所述至少一個主VM包括第一主VM和第二主VM，由所述第一主VM配置的安全設置包括在所述至少一個客戶VM上運行的作業系統的內核保護，並且所述第二主VM配置的安全設置包括在所述至少一個客戶VM上運行的作業系統的直接記憶體存取(DMA)保護。

【請求項7】 如請求項1之系統，其中所述至少一個主VM包括第一主VM、第二主VM和第三主VM；所述至少一個客戶VM包括第一客戶VM和第二客戶VM；由所述第一主VM配置的安全設置包括在所述第一客戶VM上運行的作業系統的內核保護，由所述第二主VM配置的安全設置包括在所述第一客戶VM上運行的作業系統的DMA保護，並且由所述第三主VM配置的安全設置包括所述第二客戶VM上的隔離執行環境保護。

【請求項8】 如請求項1之系統，其中所述至少一個主VM包括第一主VM和第二主VM，由所述第一主VM配置的安全設置包括在所述至少一個客戶VM上運

行的第一應用程式的保護，由所述第二主VM配置的安全設置包括在所述至少一個客戶VM上運行的第二應用程式的保護。

【請求項9】 一種命令集線器，為運行在處理器上的軟體模組或者由純硬體實現，用於：

接收從至少一個客戶VM發送的至少一個命令；以及

將所述至少一個命令發送到至少一個主VM，

其中，從所述命令集線器發送的所述至少一個命令與對應於所述至少一個客戶VM的至少一個策略一起用於管理和配置所述至少一個客戶VM的安全設置，並且所述安全設置用於管理和配置安全保護元件。

【請求項10】 如請求項9之命令集線器，其中，所述安全保護元件包括記憶體管理單元(MMU)。

【請求項11】 如請求項9之命令集線器，其中，所述安全保護元件包括記憶體保護單元(MPU)。

【請求項12】 一種主虛擬機(VM)，為運行在處理器上的軟體模組，包括：

代理，用於接收從至少一個客戶VM發送的至少一個命令；

內核保護管理器，用於接收從所述代理發送的所述至少一個命令以及接收對應於所述至少一個客戶VM的至少一個策略，並根據所述至少一個命令和所述至少一個策略，管理和配置所述至少一個客戶VM的安全設置；以及

保護管理器，用於根據所述內核保護管理器提供的所述安全設置，管理和

配置安全保護元件。

【請求項13】 如請求項12之主VM，其中從所述至少一個客戶VM發送的所述至少一個命令首先由命令集線器接收，並且由所述命令集線器發送到所述主VM的所述代理。

【請求項14】 如請求項12之主VM，其中，所述主VM通過傳輸介面綁定到管理程式，並且所述傳輸介面用於執行所述主VM和所述管理程式之間的通信。

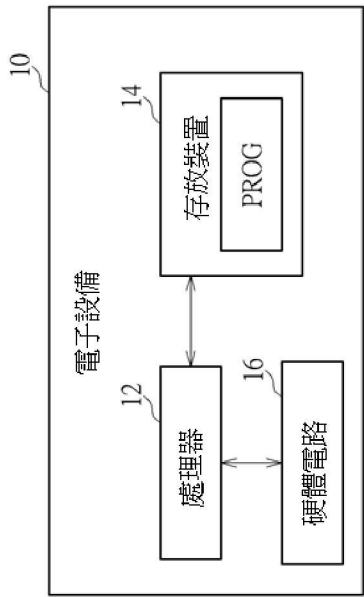
【請求項15】 如請求項12之主VM，其中，所述安全保護元件包括記憶體管理單元(MMU)。

【請求項16】 如請求項12之主VM，其中，所述安全保護元件包括記憶體保護單元(MPU)。

【請求項17】 如請求項12之主VM，其中，由所述主VM的所述內核保護管理器所配置的安全設置包括直接記憶體存取(DMA)保護。

【請求項18】 如請求項12之主VM，其中，由所述主VM的所述內核保護管理器所配置的安全設置包括內核保護。

【發明圖式】



第1圖

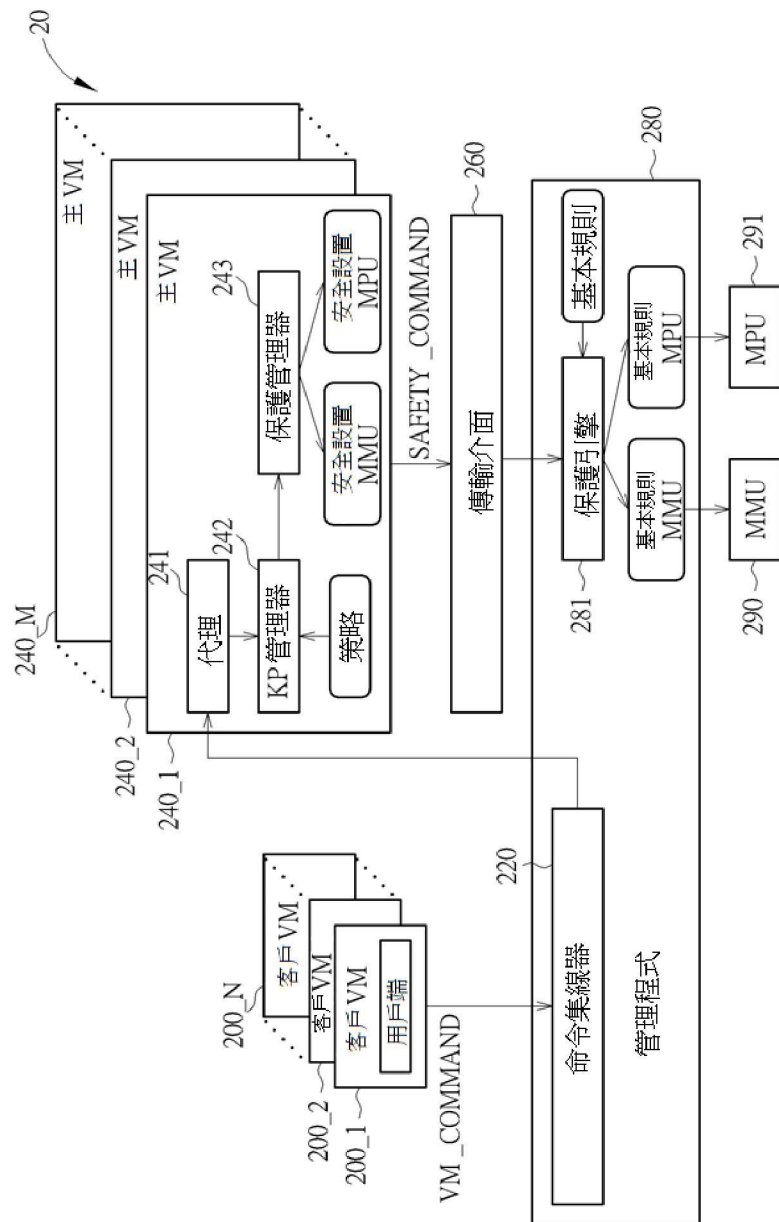
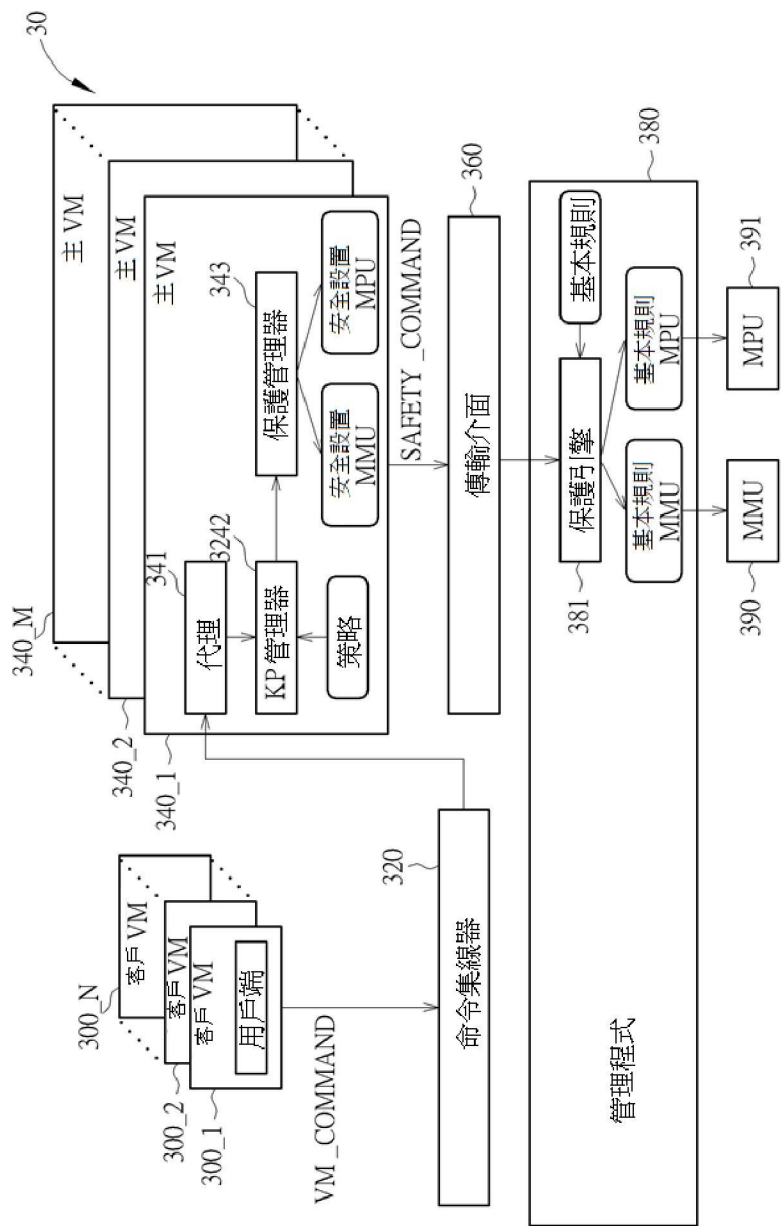
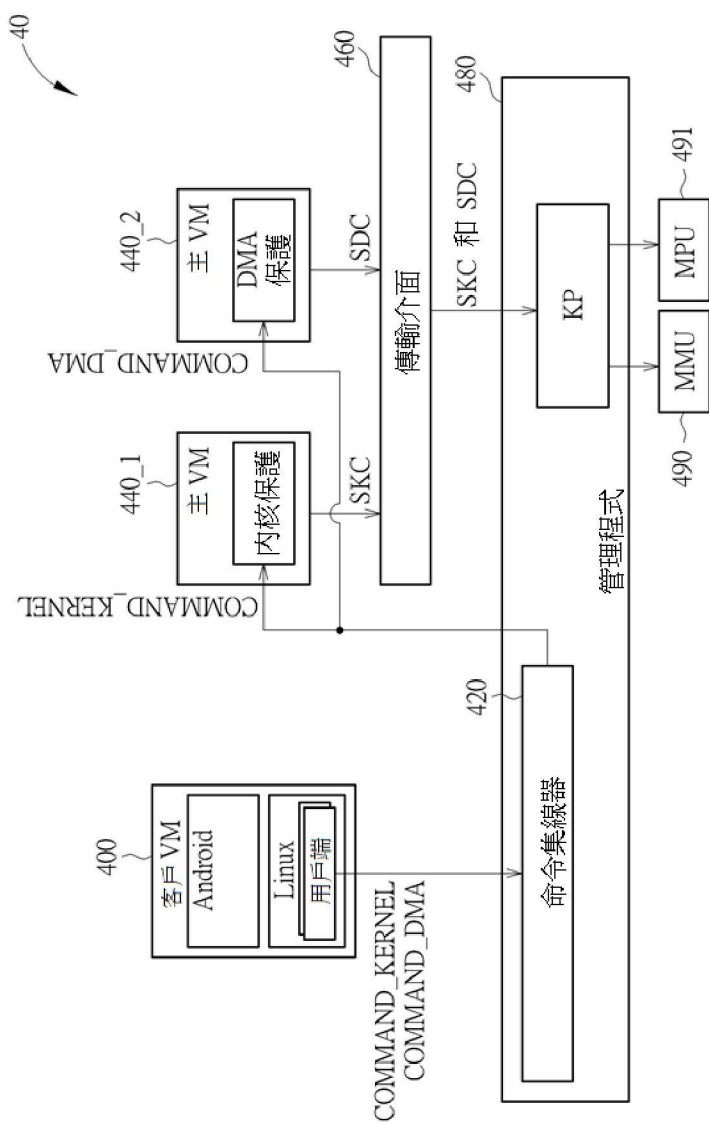


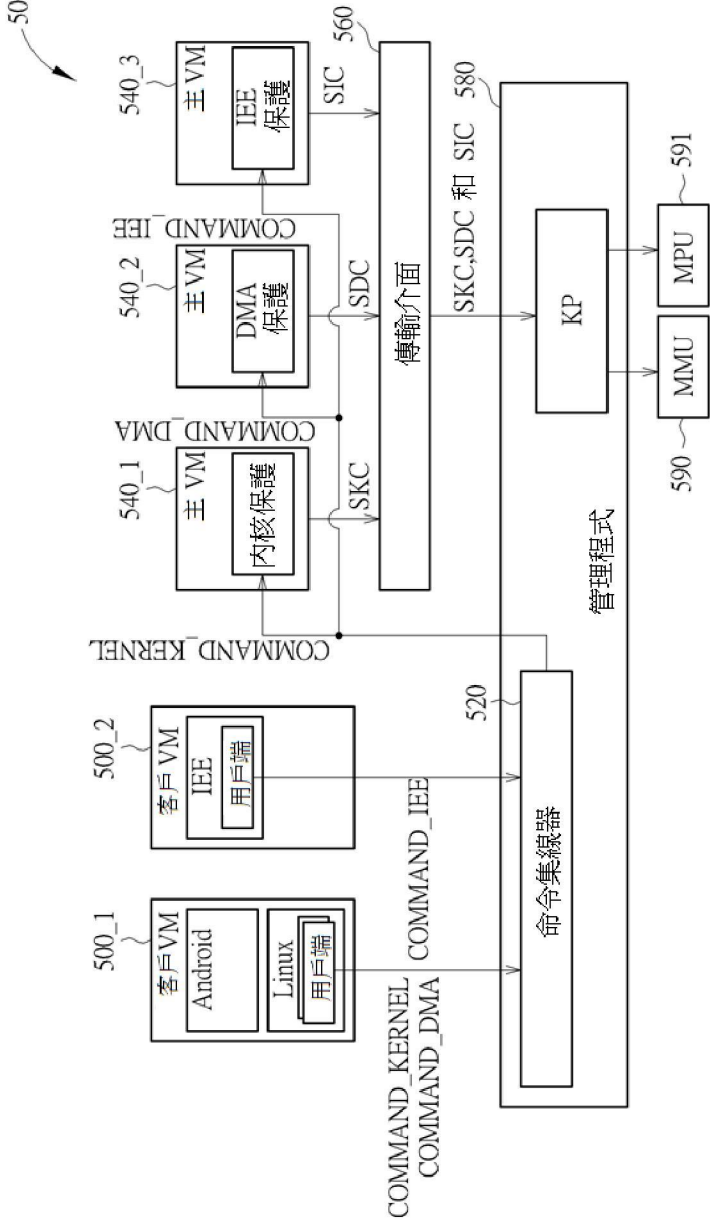
圖 2



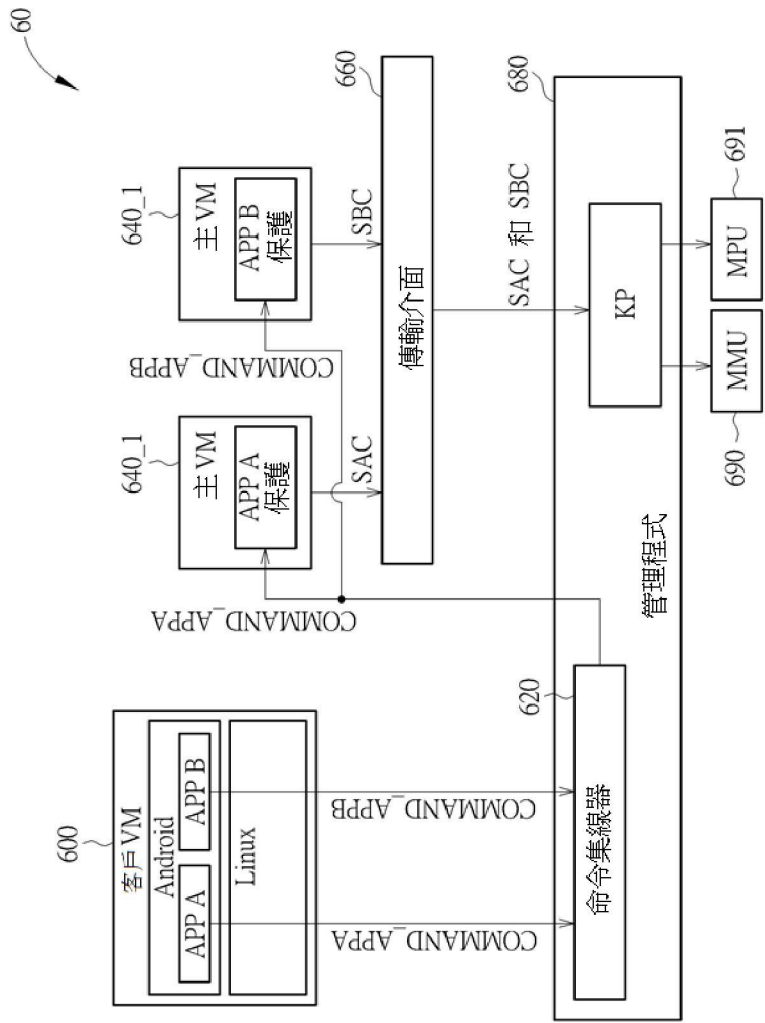
第3圖



第4圖



第5圖



第6圖