I754219

(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 I754219 B**

(45)公告日： 中華民國 111 (2022) 年 02 月 01 日

(21)申請案號：109104523 (22)申請日： 中華民國 109 (2020) 年 02 月 13 日

(51)Int. Cl.： *G06F8/65 (2018.01)* *G06F21/57 (2013.01)*
G06F9/44 (2018.01)

(30)優先權：2019/05/15 世界智慧財產權組織 PCT/US19/32360

(71)申請人：美商惠普發展公司有限責任合夥企業 (美國) HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (US)
美國

(72)發明人：珍森納 傑佛瑞 K JEANSONNE, JEFFREY KEVIN (US)；劉 偉志 LIU, WEI ZE (US)；巴拉拉曼 瑟納斯 BALARAMAN, SRINATH (US)

(74)代理人：劉法正；尹重君

(56)參考文獻：

CN	105468978A	CN	106168899A
CN	107682159A	US	2017/0010875A1
US	2017/0220802A1	US	2019/0042229A1
WO	2018/039027A1		

審查人員：林剛煌

申請專利範圍項數：12 項 圖式數：4 共 31 頁

(54)名稱

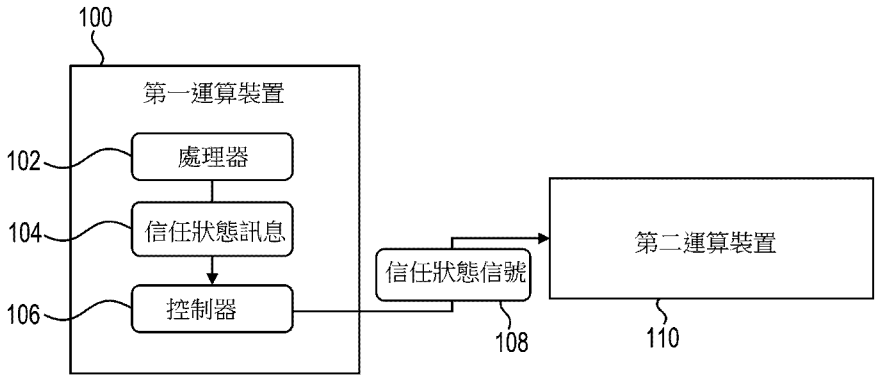
更新信號技術

(57)摘要

一種第一運算裝置的一實例可包括韌體、一控制器、以及一處理器。該處理器可將產生將被發送給該控制器的一信任狀態訊息，該信任狀態訊息指出該第一運算裝置的該韌體正操作一受信任的環境，並且利用該韌體在該受信任的環境中驗證一更新。該控制器回應於接收到該信任狀態訊息，可以向一第二運算裝置斷言一信任狀態信號指出該第一運算裝置的該韌體正操作該受信任的環境。該信任狀態信號的該斷言將致能該第二運算裝置安裝該經驗證的更新。

An example of a first computing device may include firmware, a controller, and a processor. The processor may be to generate a trust state message, to be sent to the controller, indicating the firmware of the first computing device is operating a trusted environment and utilize the firmware to validate an update within the trusted environment. The controller may be to assert, responsive to receiving the trust state message, a trust state signal to a second computing device indicating the firmware of the first computing device is operating the trusted environment. The assertion of the trust state signal may be to enable the second computing device to install the validated update.

指定代表圖：



【圖1】

符號簡單說明：

100:第一運算裝置

102:處理器

104:信任狀態訊息

106:控制器

108:信任狀態信號

110:第二運算裝置

I754219

公告本

【發明摘要】

【中文發明名稱】

更新信號技術

【英文發明名稱】

Update Signals

【中文】

一種第一運算裝置的一實例可包括韌體、一控制器、以及一處理器。該處理器可將產生將被發送給該控制器的一信任狀態訊息，該信任狀態訊息指出該第一運算裝置的該韌體正操作一受信任的環境，並且利用該韌體在該受信任的環境中驗證一更新。該控制器回應於接收到該信任狀態訊息，可以向一第二運算裝置斷言一信任狀態信號指出該第一運算裝置的該韌體正操作該受信任的環境。該信任狀態信號的該斷言將致能該第二運算裝置安裝該經驗證的更新。

【英文】

An example of a first computing device may include firmware, a controller, and a processor. The processor may be to generate a trust state message, to be sent to the controller, indicating the firmware of the first computing device is operating a trusted environment and utilize the firmware to validate an update within the trusted environment. The controller may be to assert, responsive to receiving the trust state message, a trust state signal to a second computing device indicating the firmware of the first computing device is operating the trusted environment. The assertion of the trust state signal may be to enable the second computing device to install the validated update.

【指定代表圖】　圖1

【代表圖之符號簡單說明】

100:第一運算裝置
102:處理器
104:信任狀態訊息
106:控制器
108:信任狀態信號
110:第二運算裝置

【特徵化學式】

(無)

【發明說明書】

【中文發明名稱】

更新信號技術

【英文發明名稱】

Update Signals

【技術領域】

發明領域

【0001】 本發明係有關於更新信號技術。

【先前技術】

發明背景

【0002】 一運算裝置可以包括可由一處理器執行以執行該運算裝置之各種功能的指令。該等指令可能會隨時更新。該等指令可以是惡意軟體的攻擊對象，該惡意軟體可能在該運算裝置中或來自其他的運算裝置。在一些實例中，該等攻擊可能在一更新期間或偽裝成更新被犯下。

【發明內容】

發明概要

【0003】 依據本發明之一實施例，係特地提出一種第一運算裝置，其包含有：韌體；一控制器；以及一處理器，其中該處理器將：產生將被發送給該控制器的一信任狀態訊息，該信任狀態訊息指出該第一運算裝置的該韌體正操作一受信任的環境，並且；利用該韌體在該受信任的環境中驗證一更新；並且其中該控制器回應於接收到該信任狀態訊息，向一第二運算裝置斷言一信任狀態信號指出該第一運算裝置的該韌體正操作該受信任的環境，其中該信任狀態信號的該斷言將致能該第二運算裝置安裝該經驗證的更新。

【圖式簡單說明】

【0004】 圖1圖示出利用與本發明一致之更新信號技術的一第一運算裝置的一實例。

【0005】 圖2圖示出利用與本發明一致之更新信號技術的一系統的一實例。

【0006】 圖3圖示出利用與本發明一致之更新信號技術的一非暫時性的機器可讀取記憶體及處理器的實例的一實例。

【0007】 圖4圖示出利用與本發明一致之更新信號技術的一非暫時性的機器可讀取記憶體及處理器的實例的一實例。

【實施方式】

【0008】 較佳實施例之詳細說明

一運算裝置可包括可由一處理資源執行以執行各種功能的指令。如此功能的一實例包括該運算系統的各種啟動功能。該等指令可以包括韌體指令。該等韌體指令可以包括開機韌體諸如基本輸入/輸出系統(BIOS)指令。該等BIOS指令可以包括統一可延伸韌體介面(UEFI)規範的指令。

【0009】 該等韌體指令可包括當被通電時由一運算裝置之一處理資源所執行的該等指令。該等韌體指令可被執行以執行該運算裝置的一啟動操作。例如，該等韌體指令可以識別、測試、及/或初始化與該運算裝置相關聯的硬體。該等韌體指令可把該運算裝置組配成為一特定的狀態，使得諸如一作業系統(OS)之類的其他指令可被載入並被執行以控制該運算裝置。

【0010】 針對被使用來執行一運算裝置之啟動功能的指令的惡意軟體攻擊，諸如對韌體指令的惡意軟體攻擊，可能會導致該運算裝置的完整性受到損害，從而可能會發生在該運算裝置中未經授權的存取及操作。受損的韌體指令可能包括已被損壞的指令，以致於該等韌體指令無法執行及/或已有些更改但仍可執行。例如，損害的韌體指令可能包括已經被一惡意實體以一種方式來修改的韌體指令使之可允許非所欲之遠程監控及/或控制一運算裝置、由一惡意軟體

未經授權地存取及/或修改與該運算裝置相關聯的資料、該運算裝置的禁用、等等。因此，在該等指令安裝在一運算裝置上之前，指令驗證可被執行。

【0011】該等指令的驗證可以包括一基於密碼的驗證技術。例如，該等指令的該驗證可以採用一種密碼學加密，其使用公鑰及私鑰的來驗證由該作者/發行者在該等指令中所包括的一數位簽名。如在本文中所使用的，一公鑰可以指多個實體已知的一把密鑰，而一私鑰可以指只由一單一實體或有限數量實體所知的一把密鑰。資料，諸如與指令相關聯的一數位簽名，用一把私鑰加密後，可以使用該對應的公鑰來解密。該基本的概念可被使用於數位簽名的產生及驗證中。例如，一數位簽名可被解密並且被驗證為真實的，以便認為該等相關聯的指令係有效的。

【0012】在一些實例中，運算裝置可以包括一密碼引擎及/或密碼加速器。如在本文中所使用的，一密碼引擎及/或密碼加速器可以包括被嵌入在運算裝置中並且可使用來在安裝之前以密碼方式驗證指令的指令及/或硬體。例如，一密碼引擎及/或密碼加速器可以包括專用資源，諸如專用於及/或保留用於執行基於密碼之指令驗證的指令或硬體。例如，一密碼引擎及/或密碼加速器可以包括一安全的密碼處理器，該安全的密碼處理器係用於執行我們的密碼操作的一專用處理器。該密碼引擎及/或密碼加速器可以是將安裝該等指令之一運算裝置的一組件、嵌入在該運算裝置中、及/或利用該運算裝置之資源。

【0013】然而，執行密碼操作之指令及/或硬體可能會對一運算裝置施加一運算成本及/或額外的金錢成本。也就是說，包括一密碼引擎及/或密碼加速器會增加一運算裝置的成本及/或降低該運算裝置的該運算量。然而，移除在一運算裝置上執行密碼操作的該等指令及/或硬體以可能會使該運算裝置容易受到攻擊。例如，因為該運算裝置無法驗證作為更新之一部分所接收到之安裝指令的真實性。

【0014】 形成對比的是，與本發明一致的實例可以包括一機制來安全化在一運算裝置上的更新，而無需要一種執行韌體指令更新驗證的功能。也就是說，與本發明一致的實例可以對沒有密碼引擎及/或密碼加速器的一運算裝置驗證韌體指令更新。例如，與本發明一致的實例可以包括一第一運算裝置。該第一運算裝置可以包括韌體、一控制器、及一處理器。該處理器可以是用於產生將被發送到該控制器之一信任狀態訊息的一處理器，該信任狀態訊息指出該第一運算裝置的韌體正操作一受信任的環境並且利用該韌體來驗證在該受信任環境內的一更新。該控制器可以是一控制器，其回應於接收到該信任狀態訊息，向一第二運算裝置斷言一信任狀態信號，該信任狀態信號指出該第一運算裝置的韌體正在運作該受信任的環境，其中該信任狀態信號的該斷言將致能該第二個運算裝置可安裝該經驗證的更新。

【0015】 圖1圖示出一第一運算裝置100的實例，其利用了與本發明一致的更新信號技術。該第一運算裝置100之該等所描述的組件及/或操作可以包括針對圖2-4所描述之該等描述的組件及/或操作及/或與其互換。

【0016】 該第一運算裝置100可以包括一處理器102。該處理器102可以包括一處理器102以執行機器可讀取指令來執行各種操作。該等指令可被儲存在一記憶體資源中，諸如用於儲存機器可讀取指令之非暫時性的電腦可讀取儲存媒體。在一些實例中，機器可讀取指令可被儲存在該第一運算裝置100之一母板上的一非依電性ROM晶片或快閃記憶體晶片上。

【0017】 可由該處理器102執行來執行操作的該機器可讀取指令可以包括韌體指令。例如，該韌體可能包括一基本輸入/輸出系統(BIOS)。該韌體可以包括在該第一運算裝置100啟動時要載入的指令，並且負責初始化及/或格式化該運算裝置100之該等各種硬體組件並確保它們可以正常地工作。該韌體可以執行一開機載入程式，其啟動被安裝在該第一運算裝置100上的一作業系統(OS)。

【0018】 在一些實例中，該韌體可以包括基於統一可延伸韌體介面(UEFI)的韌體。基於UEFI的韌體可以在製造時被安裝在該第一運算裝置100上，並且它可以是當該第一運算裝置100被通電時要被執行的該第一組指令。基於UEFI的韌體可以包括替代該標準BIOS功能的韌體。基於UEFI的韌體可做檢查以查看該運算裝置100具有哪些硬體組件、初始化及/或格式化這些組件、以及把它們移交給該OS。

【0019】 該基於UEFI的韌體可以包括一安全啟動功能。例如，該基於UEFI的韌體可以包括的一功能為在該第一運算裝置100之該啟動過程期間驗證所載入每一個組件。驗證每一個組件可以包括確保每一個組件被數位簽名及被驗證。以這種方式，可以確保該第一運算裝置100係利用由該第一運算裝置100的該製造商及/或由該第一運算裝置100的一使用者所信任的軟體來啟動。

【0020】 該等組件之每一個的該驗證可以針對存在於該基於UEFI之韌體中受信任的憑證或雜湊來進行。例如，這些憑證及/或雜湊可以使用密鑰來建立信任的層級結構。例如，一平台密鑰(PK)可以代表信任的一個根並且可被使用來保護一密鑰交換密鑰(KEK)資料庫。一供應商可以在製造期間釋放該PK的一公開部分進入到基於UEFI的韌體中。但是，該PK的一私有部分，可能還是保留在該供應商處。當更新該PK時，該新的PK憑證會用舊的哪一個被簽名。該KEK資料庫可以包含受信任的憑證，它們被允許來修改一允許的簽名資料庫(憑證或其雜湊的資料庫，憑證或其雜湊被使用來產生代碼簽名憑證，代碼簽名憑證被使用來簽署啟動載入程式及其他被允許執行之預先啟動組件)、不允許的簽名資料庫(已被破壞及/或被吊銷並且無法執行之憑證或其雜湊的資料庫)、或時戳簽名資料庫(包含有具時間戳記之憑證的資料庫，該時間戳記之憑證被使用在當簽屬啟動載入程式映像時)。該KEK資料庫可以包含作業系統供應商的憑證，並且可以由該PK來保全。

【0021】該處理器102可以執行韌體指令以驗證要被套用到該第一運算裝置100的一更新。例如，該第一運算裝置100的該處理器102可以執行該基於UEFI的韌體以便驗證一更新的數位簽名，該更新將被套用到載入到該第一運算裝置100之機器可讀取指令，包括有該等韌體指令。

【0022】該第一運算裝置100可以包括一主機裝置。一主機裝置可以包括一第一運算裝置100，其可以是在一網路或包括有複數個運算裝置之其他系統中的一運算裝置用以初始地接收要被套用到機器可讀取指令之一更新。例如，該主機裝置可以包括一個將把該機器可讀取指令更新分發到其他運算裝置的一第一運算裝置100。另外地或可替代地，該主機裝置可以包括一第一運算裝置100，該第一運算裝置100將授權把機器可讀指令更新分發給其他的運算裝置。因此，一第一運算裝置100可被通信地耦合到一第二運算裝置110。

【0023】一第二運算裝置110可包括從該第一運算裝置100接收該更新及/或接收該更新安裝許可的一種運算裝置。也就是說，該第二運算裝置110可以依賴該第一運算裝置100來向該第二運算裝置110提供對一更新的存取及/或對一更新存取的許可，以在該第二運算裝置110處進行安裝。該第一運算裝置100及該第二運算裝置110可以是一運算網路的成員或節點。在一實例中，該第一運算裝置100可包括在該網路中的一管理或控制節點，而該第二運算裝置110可包括在該網路中的一非管理或從屬節點。

【0024】該第二運算裝置110可以依賴該第一運算裝置100以代表該第二運算裝置110驗證一更新。也就是說，該第二運算裝置110可以根據以下該等描述的實例依賴該第一運算裝置100來驗證一更新的一數位簽名。

【0025】如以上所述，該第一運算裝置100可以包括一處理器102。該處理器102可以執行機器可讀取指令以執行各種操作。例如，該處理器102可以執行韌體指令。該處理器102可執行韌體指令來致使該第一運算裝置100操作一受信

任的環境。操作一受信任的環境可以包括初始化一開機自我檢測(POST)及載入一基於UEFI的韌體執行一安全的啟動。當在該可信任的環境中操作時，一信任鏈可被建立，並且機器可讀取指令可在由該第一運算裝置100執行之前被驗證。該處理器102可以藉由執行該第一運算裝置100的該韌體來打開一個可信任的窗口以在其中執行驗證，從而建立該信任鏈。在一可信任的環境內操作可使得該第一運算裝置100能夠驗證韌體及/或韌體升級，以藉由驗證它們各自的數位簽名來防止替換攻擊。

【0026】 該處理器102可以產生一信任狀態訊息104。如以上所述，該信任狀態訊息104可以包括指出該第一運算裝置100的該韌體正在操作一受信任的環境的一訊息。也就是說，回應於該第一運算裝置100經歷一重置並且安全地啟動到一受信任的環境中，該處理器102可以產生一信任狀態訊息104，其傳達該第一運算裝置100正在操作一受信任的環境。

【0027】 該信任狀態訊息104可以是一將被發送到該第一運算裝置100之一控制器106的訊息。該信任狀態訊息104可以經由一訊息通信通道被傳遞到該控制器106。例如，該控制器106可以經由一共享記憶體介面訊息通信通道被通信地耦合到該處理器102。該信任狀態訊息104可以經由在該處理器102與該控制器106之間的一共享記憶體介面被傳送到該控制器106。在一些實施例中，由該處理器102所產生的該信任狀態資訊104可以藉由把該信任狀態訊息104放置在該控制器106的一非依電性嵌入式控制器隨機存取記憶體(ECRAM)中來被傳送到該控制器106。該控制器106可以在一重置之後接受通過該共享記憶體介面所接收到的一初始訊息。也就是說，儘管這樣的通信通道可能被認為是不安全的，但是該通信通道可被安全化，方式係借助於該控制器106被限制於接受該第一信任狀態訊息104，該第一信任狀態訊息104係在該第一運算裝置100的一重置之後被接收。

【0028】該控制器106可以接收該信任狀態訊息104。該信任狀態訊息104可以是在該第一運算裝置100重置之後經由該通信通道所接收到的一第一訊息或初始訊息。回應於接收到該信任狀態訊息，該控制器106可以向該第二運算裝置110斷言一信任狀態信號108。該信任狀態信號108可包括通過一通用輸入/輸出(GPIO)引腳所斷言的一信號，該GPIO引腳可被通信連接到該第二運算裝置110。該第二運算裝置110通常可以位於諸如USB I2C等等之一特定的匯流排上，其可能係一主要通道。然而，可以經由不同於在該第一運算裝置100與該第二運算裝置110之間該主要介面，諸如一GPIO引腳的一頻外(OOB)通道來把該信任狀態信號108傳送到該第二運算裝置110。

【0029】該信任狀態信號108可以包括一信號向該第二運算裝置110指出該第一運算裝置100的該韌體正在由該處理器102執行使得該第一運算裝置100正操作在一受信任的環境中。也就是說，該信任狀態信號108可以包括通過一GPIO引腳被斷言的一信號以向一第二運算裝置指出該第一運算裝置100已經執行了一安全的啟動並正操作在一受信任的環境中。當該第一運算裝置的該韌體繼續操作在該受信任的環境中時，該信任狀態信號108可以持續性地及/或週期性地一直對該第二運算裝置110斷言。也就是說，只要該第一運算裝置100正操作該受信任的環境，那麼對該第二運算裝置做指示的該信任狀態信號就保持對該第二運算裝置110斷言，指出該情況。

【0030】如以上所述，該處理器102可在被建立在該第一運算裝置100之該受信任的環境中執行該韌體以驗證機器可讀取指令，諸如將被套用到該第一運算裝置100及/或第二運算裝置110的該韌體更新。例如，該處理器102可以執行該第一運算裝置100的該韌體以驗證在該第一運算裝置100處所接收到之一韌體更新套件的一數位簽名。一旦藉由該第一運算裝置100的該韌體驗證了該更新，則該處理器102可對該第一運算裝置100啟動該更新的安裝。一旦藉由該第一運算

裝置100的該韌體驗證了該更新，則該處理器102可信令該驗證給該第二運算裝置110。

【0031】有了該第一運算裝置100對該更新的驗證伴隨對該第二運算裝置110之該信任狀態信號108的斷言可以致能該第二運算裝置110安裝該經驗證的更新。例如，該第二運算裝置110可依賴被信號告知給該第二運算裝置110之該第一運算裝置100之該韌體的驗證，結合該信任狀態信號108的該斷言，該信任狀態信號108指出該驗證係在該第一運算裝置100所處之該受信任的環境內被執行的。因此，一旦由該第一運算裝置100的該韌體驗證，就可以在該第一運算裝置100及該第二運算裝置110處安裝一更新，只要該信任狀態信號108在該安裝過程中由該控制器106向該第二運算裝置110斷言即可。

【0032】一旦一更新已被安裝到該第一運算裝置100及/或該第二運算裝置110，該第一運算裝置100可以準備離開該受信任的環境及/或在該第一運算裝置100處啟動一OS。因此，該處理器102在離開該受信任的環境之前可以產生一第二信任狀態訊息。也就是說，該處理器102可在排定該第一運算裝置100的一重置以啟動該第一運算裝置100的一OS之前產生一第二信任狀態訊息。該第二信任狀態訊息可以包括一密切信任的更新訊息。該密切信任的更新訊息可被發送到該控制器106。該密切信任的更新訊息可向該控制器106指出該第一運算裝置100已經或將要離開該受信任的環境。也就是說，該密切信任的更新訊息可以向該控制器106指出該第一運算裝置100已經完成一驗證操作、已經安裝了一更新、及/或準備啟動該第一運算裝置100的一OS。

【0033】可經由與該控制器106相關聯之一共享記憶體介面及/或一ECRAM介面把該密切信任的更新訊息傳送到該控制器。該控制器106可以接收該密切信任的更新訊息。在離開該可信的環境之前，該密切信任的更新訊息可被排定要被發送並且可以以這樣的一種方式被發送使得在由該控制器106採取

重置行動之後該控制器106把該密切信任的更新訊息接受作為一初始訊息。

【0034】 回應於接收到該密切信任的更新訊息，該控制器106可解除斷言該信任狀態信號108。例如，回應於接收到該密切信任的更新訊息，該控制器106可致使該信任狀態信號108終止斷言及/或改變跨越該GPIO引腳之該信任狀態信號108的狀態。解除該信任狀態信號108的斷言可以禁止該第二運算裝置110安裝一更新套件。也就是說，由於該信任狀態信號108的斷言係充當該第一運算裝置100正在一受信任的環境中驗證一更新的指示，並且致能該第二運算裝置110安裝該經驗證的更新，取消斷言或改變該信任狀態信號108的狀態可達到防止更新安裝的作用，因為不能保證該第一運算裝置100係在該受信任的環境中驗證了該更新。

【0035】 圖2圖示出一種系統220的一實例，其利用了與本發明一致的更新信號技術。該系統220所描述的該等組件及/或操作可包括針對圖1及3-4所描述之該等描述的組件及/或操作及/或與其互換。

【0036】 該系統220可包括一韌體更新套件224。該韌體更新套件224可包括一組機器可讀取指令來修改及/或替換與該第一運算裝置222相關聯之一韌體的一部分。該韌體更新軟體套件224可以包括一份二進制文件，該二進制文件包含要安裝在該第一運算裝置222處的一系統韌體映像。

【0037】 該韌體更新套件224可由一第一運算裝置222來接收。該韌體更新套件224可以從另一運算裝置發送到該第一運算裝置222。該第一運算裝置222可以是一主機運算裝置。也就是說，該第一運算裝置222可以是複數個運算裝置中的一運算裝置，以在一運算網路中接收該韌體更新套件224。該第一運算裝置222可包括一運算裝置，該運算裝置可以負責驗證用於該運算網路的該韌體更新套件224及/或把該韌體更新套件224散佈到在該運算網路中的其他運算裝置。

【0038】 該第一運算裝置222可以包括一處理器及可由該處理器執行以執

行各種功能的機器可讀取指令。這些指令可以包括諸如韌體指令、OS指令、等等的指令。

【0039】該第一運算裝置222可以啟動一更新代理226。該更新代理226可包括一組機器可讀取指令，該組機器可讀取指令可由該第一運算裝置222的該處理器執行以自動觸發及/或支援更新傳送及安裝。該更新代理226可以掃描該第一運算裝置222以判定已經安裝了哪些更新，然後從製造商網站搜索並下載該韌體更新套件224。在一些實例中，回應於接收到該韌體更新套件224，該更新代理226可被啟動。該更新代理226可以檢測、下載、及/或安裝更新。該更新代理226可包括允許客戶端電腦連接到更新伺服器及/或更新網站的一應用程式介面。該更新代理226可以每天檢查並安裝更新。該更新代理226可以從一更新服務伺服器下載該韌體更新套件224。該更新代理226可把可用的更新從一更新服務伺服器安裝到該第一運算裝置222。

【0040】該更新代理226可以觸發該第一運算裝置222的一第一重置228。回應於接收或獲取該韌體更新套件224，該第一重置228可被觸發。在該第一重置228之後，該第一運算的一處理器裝置222可以執行指令以啟動一啟動載入程式230。該啟動載入程式230可以包括一組指令來啟動一安全的啟動並且是在該第一運算裝置222處建立一受信任環境的該過程。

【0041】該啟動載入程式230可以利用一UEFI更新封裝功能來處理該接收到的該韌體更新套件224，以把該韌體更新套件224之有效載荷移交給該第一運算裝置222的該韌體以進行處理。也就是說，該第一運算裝置222可在執行服務中把該韌體更新套件打包成為一更新套件包232。該更新套件包232可以是把該韌體更新套件224傳遞至該第一運算裝置222之該韌體的載具。該第一運算裝置222的該韌體可把一韌體更新套件224之有效載荷識別為該更新套件包232並且發起該更新過程。

【0042】該第一運算裝置222的該等韌體指令可執行來把該更新套件包232保存到一資料儲存分區236。例如，該更新套件包232可被保存到一可延伸韌體介面系統分區(ESP)，其可以是在該第一運算裝置222之一資料儲存裝置上之一系統分區。該資料儲存分區236可以以一具有基於一檔案配置表(FAT)檔案狀態規格的檔案系統被格式化並被保持為一UEFI規格的一部分。該資料儲存分區236可包括一資料儲存資源的一分區部分，其中用於該安裝之系統的EFI啟動載入程式及/或指令在啟動時由該第一運算裝置222的該韌體來使用。

【0043】在該更新套件包232被保存在該資料儲存分區236之後，該第一運算裝置222的該處理器可以觸發該第一運算裝置222的一第二重置234。該第二重置234可以充當一觸發器讓該UEFI韌體掌控該第一運算裝置222及建立並維持該第一運算裝置222的一安全邊界，在該安全邊界內來執行後續操作。該第二重置234可被認為是建立該安全環境的該事件。如以下詳細描述的，發生在該第二重置234之後並在該密切信任的更新訊息244之前之該第一運算裝置222的操作可被認為將被發生在由該第一運算裝置之該韌體所建立之該受信任環境的該等安全邊界內。

【0044】回應於該第二重置234及/或由在該第一運算裝置222處該韌體的執行所建立之該受信任的環境，可以產生一信任狀態資訊246。一信任狀態資訊246可以包括可傳送到一控制器250的一訊息。該控制器250可包括嵌入在該第一運算裝置222內的一控制器及/或在該第一運算裝置222外部但可被通信地耦合到該第一運算裝置222的一控制器。

【0045】該信任狀態訊息246可包括把該第一運算裝置是否正執行在一受信任的環境中的訊息傳達給該控制器250。例如，該信任狀態訊息246可以包括一訊息，該訊息確定了該第一運算裝置222的該韌體已經控制了該第一運算裝置222並且已建立了一安全受信任的環境，該安全受信任的環境建立了一信任的根

以驗證該韌體更新套件234。

【0046】 可經由把該信任狀態訊息246保存到一共享記憶體資源248來把該信任狀態訊息246傳送到該控制器250。該共享記憶體資源248可以包括在該第一運算裝置與該控制器250之間共享存取的一記憶體。在一些實例中，該共享記憶體248可以包括與該控制器250相關聯的ECRAM。

【0047】 回應於接收到指出該第一運算裝置222係操作在一受信任的環境中的該信任狀態訊息246，該控制器250可以使一信任狀態信號254將被斷言及/或改變通過一GPIO信號引腳252被斷言之該信任狀態信號的狀態254。一GPIO可包括在一積體電路或電子電路板上的一信號引腳。該信號引腳的該行為，其包括有該信號引腳是否作為輸入或輸出，可藉由指令或藉由在執行時之一使用者來控制。

【0048】 該GPIO信號引腳252可以包括介接及/或被通信地耦合到一第二運算裝置256的一信號引腳。因此，一信號，諸如該信任狀態信號254，可被斷言給該第二運算裝置256。該第二運算裝置256可以是與該第一運算裝置222位於同一運算網路中之非該第一運算裝置222的一裝置。該第二運算裝置256可包括一運算裝置，該運算裝置缺乏建立一受信任環境的能力及/或缺乏可獨立驗證一韌體更新套件224之硬體及/或指令的能力。也就是說，該第二運算裝置256可能缺乏在安裝一韌體更新套件到該第二運算裝置256之前驗證該韌體更新套件的一密碼引擎及/或密碼加速器。

【0049】 然而，藉由實現向該第二運算裝置256傳送該信任狀態信號254，操作在該第一運算裝置222處之該受信任環境的該等邊界可被延伸來包括該第二運算裝置256。也就是說，藉由該控制器250向該第二運算裝置256之一信任狀態信號254斷言可以在該第一運算裝置222與該第二運算裝置256之間建立與該韌體更新套件224之該驗證有關的一信任鏈。例如，該第二運算裝置256可確定

該第一運算裝置222係在一受信任環境中操作時執行一韌體更新套件224的一驗證操作，只要該信任狀態信號254向該第二運算裝置256指出該第一運算裝置222正操作在一受信任的環境中被斷言。以這種方式，指出該第一運算裝置222正操作在一受信任環境中之該信任狀態信號254的該斷言可以使該第二運算裝置256能夠依賴該第一運算裝置222對該韌體更新套件224的該驗證。因此，指出該第一運算裝置222正操作在一受信任環境中之該信任狀態信號254的該斷言可致能該第二運算裝置256在該第二運算裝置256處安裝該韌體更新套件224，而無需執行該韌體更新套件224之一獨立的驗證。

【0050】 返回到在該第二重置234之後該第一運算裝置222的功能，該第一運算裝置222之該裝置韌體的執行可以發起一更新處理程式238。該更新處理程式238可以從該資料儲存分區236檢索該更新套件包232。該更新處理程式238可以在一準備啟動前事件處從該資料儲存分區236檢索並載入該更新套件包232。一準備載入前事件可以指的是在該第一運算裝置222之該韌體達該第一運算裝置222的一驗證/安裝後狀態其中該第一運算裝置222準備要啟動之前所發生的一事件。

【0051】 當操作在該受信任的環境中時，該第一運算裝置222的該韌體可被執行來驗證該韌體更新套件。例如，該第一運算裝置222的該韌體可被執行以對檢索自該資料儲存分區236之該韌體更新套件包232執行一密碼數位簽名驗證240操作。

【0052】 一旦完成了對該韌體更新套件224的一成功驗證，該第一運算裝置222的該處理器就可以執行指令以執行該韌體更新242。執行該韌體更新242可以包括在第一運算裝置222處安裝該韌體更新套件224。另外，執行該韌體更新242可以包括把一訊息及/或其他信號發送到該第二運算裝置256指出該韌體更新套件224的驗證已經完成及/或成功。在一些實例中，執行該韌體更新242可以包括

在該第二運算裝置256處安裝該韌體更新242。在該第二運算裝置256處接收到指出該韌體更新套件224驗證已完成及/或成功的該訊息及/或其他信號、及/或指出該第一運算裝置222正操作在該受信任的環境中之該信任狀態信號254被斷言給該第二運算裝置256，在這些情況下，該第二運算裝置256可以允許安裝該韌體更新套件224。

【0053】 在該韌體簽名240的該驗證及/或該韌體更新242的該執行之後，該第一運算裝置222的該處理器可以執行指令以產生另一信任狀態訊息246。然而，在這樣的例子中，將被產生及/或被發送到該控制器250之該信任狀態訊息246可以是一密切信任的更新訊息244。該密切信任的更新訊息244可以在一準備要啟動事件時被產生及/或被發送。也就是說，當該第一運算裝置222的該韌體已經驗證該韌體簽名240及/或完成一韌體更新242安裝並且準備要啟動例如該第一運算裝置222的一OS時，該密切信任的更新訊息244可被產生及/或被發送。當該第一運算裝置正準備要啟動而導致該第一運算裝置離開及/或停止操作在該受信任的信環境中時，該密切信任的更新訊息244可被產生及/或被排定將被發送。

【0054】 因此，一信任狀態訊息246，諸如一密切信任的更新訊息244，可被傳送到該控制器250。例如，可以藉由把該密切信任的更新訊息244放置在一共享記憶體248中來把該密切信任的更新訊息244傳送給該控制器250。該密切信任的更新訊息244可以向該控制器250指出該第一運算裝置222正在離開及/或已經離開該受信任的環境。

【0055】 回應於接收到包括有該密切信任的更新訊息244的該信任狀態訊息246，該控制器250可以解除斷言或修改跨越該GPIO信號引腳252正被斷言給該第二運算裝置256之該信任狀態信號的狀態。該信任狀態信號254之該狀態的該解除斷言及/或修改可向該第二運算裝置256指出該第一運算裝置222正在離開及/或已經離開了該受信任的環境。因此，對該信任狀態信號254之該狀態的解除斷

言及/或修改可在當該後續的韌體更新套件係在該信任狀態信號254被解除斷言或被斷言在該經修改的狀態中被接收時，會禁止該第二運算裝置256安裝該隨後的韌體更新套件。也就是說，當該信任狀態信號254被解除斷言或被斷言在該經修改的狀態中時，該第二運算裝置256可不允許安裝該韌體更新套件。在該信任狀態信號254被再次斷言或再次修改該信任狀態信號254的狀態之前，該第二運算裝置256可不允許安裝該韌體更新套件。以這種方式，藉由把一韌體更新安裝到該第二運算裝置256的可否取決於在驗證期間由該第一運算裝置222進行韌體驗證及/或對該第二運算裝置256之該信任狀態信號254的斷言，由該第一運算裝置222所建立之該受信任的環境的該信任邊界被擴展到該第二運算裝置256，以用於該韌體驗證的目的。

【0056】 圖3圖示出使用與本發明一致之更新信號技術之一非暫時性的機器可讀取記憶體362及處理器360的一實例。諸如該非暫時性記憶體362之類的一記憶體資源可被使用來儲存由該處理器360所執行的指令(例如364、366、等等)以執行在本文所描述的該等操作。該等操作不侷限於在本文所描述之一特定的實施例，並且可以包括針對圖1-2與圖4所描述之該等描述的組件及/或操作及/或與其互換。

【0057】 該處理器360可以包括與一控制器相關聯及/或被併入到一控制器中的一處理器及/或特定應用積體電路。在一些實例中，該控制器可以是嵌入到該第一運算裝置中及/或可被通信地耦合到該第一運算裝置的一控制器。該第一運算裝置可以包括一主機裝置用於驗證將被套用到一第二運算裝置的韌體更新。

【0058】 該非暫時性的記憶體362可以儲存可由該處理器360執行的指令364，以致使該控制器從該第一運算裝置接收及/或檢索一信任狀態訊息。在實例中，該第一運算裝置可以包括一運算裝置，其將把一更新提供給一第二運算裝

置。例如，一第一運算裝置可以包括一管理裝置，該管理裝置接收一韌體更新並且為與該第一運算裝置相關聯之各種其他運算裝置驗證更新及/或把該等更新分發給其他的運算裝置。

【0059】該信任狀態訊息可以包括由該第一運算裝置之一處理器所產生的一訊息，該訊息向該控制器指出該第一運算裝置已經進入及/或正在利用一受信任的環境來驗證其已經接收到的一更新。該更新可以是適用於及/或可安裝在被通信地耦合到該控制器之一第二運算裝置的一種更新。

【0060】該信任狀態訊息可經由在該兩者之間的一共享記憶體介面從該第一運算裝置發送到該控制器。也就是說，可以把該信任狀態訊息儲存到在該第一運算裝置與該第二運算裝置之間之可共同存取之共享記憶體資源或分區，諸如一ECRAM。

【0061】給該控制器之該信任狀態訊息的該產生、發送、接收、及/或檢索可由在該第一運算裝置處的一重置及/或一重置之排定來被觸發。例如，給該控制器之該信任狀態訊息的該發送及/或檢索可由一重置來觸發，該重置標記了由在該第一運算裝置處韌體的執行而導致之該第一運算裝置進入一受信任環境的一轉變。

【0062】在一些實例中，該信任狀態訊息可以包括一密切信任的更新信任狀態訊息。該密切信任的更新信任狀態訊息可由該第一運算裝置的一處理器來產生，並可以向該控制器指出該第一運算裝置正在離開及/或已經離開一受信任的環境。在一些實例中，該密切信任的更新信任狀態訊息可以包括由該第一運算裝置之一處理器所產生的一訊息，該訊息向該控制器指出該第一運算裝置正準備要離開一受信任的環境以啟動該第一運算裝置的一OS。

【0063】該密切信任的更新信任狀態訊息可從該第一運算裝置發送至該控制器，方式係經由在該等兩者之間的一共享記憶體介面。也就是說，該密切信

任的更新信任狀態訊息可被儲存到在該第一運算裝置與該第二運算裝置之間之可共同存取之一共享記憶體資源或分區中，諸如一ECRAM。

【0064】給該控制器之該密切信任的更新信任狀態訊息的該產生、發送、接收、及/或檢索可由在該第一運算裝置處的一重置及/或一重置之排定來被觸發。例如，給該控制器之該密切信任的更新信任狀態訊息的該發送及/或檢索可藉由排定及/或執行一重置以啟動作業系統來被觸發。因此，給該控制器之該密切信任的更新信任狀態訊息的發送及/或檢索可藉由排定及/或執行一重置來觸發，該重置標記了該第一運算裝置離開一受信任的環境的一轉變。

【0065】該非暫時性的記憶體362可以儲存可由該處理器360執行的指令366，以致使該控制器指定被斷言給一第二運算裝置之一GPIO信任狀態信號的信號狀態。該GPIO信任狀態信號及/或甚至係被斷言之該信任狀態信號的信號狀態可以基礎於該控制器所接收到的該信任狀態訊息。

【0066】因此，基於對該控制器指出該第一運算裝置是否操作在一受信任的環境中的該信任狀態訊息，該控制器可指定一信任狀態信號之一對應的狀態，其可跨越該GPIO引腳被斷言給該第二運算裝置。因此，跨越該GPIO引腳被斷言該第二運算裝置之該信號的狀態可以向該第二運算裝置指出該第一運算裝置是否正在利用一受信任的環境來驗證該更新。

【0067】例如，在重置該第一運算裝置之後，該控制器可以接收從該第一運算裝置所發出之一第一信任狀態訊息，該第一信任狀態訊息指出該第一運算裝置操作在一受信任的環境中。回應於接收該第一信任狀態訊息，該控制器可致使在被通信耦合到該第二運算裝置之一GPIO引腳處把一信任狀態信號的一狀態修改成一第一狀態。把該信任狀態信號修改成該第一狀態可以致能該第二運算裝置安裝可由操作在一受信任環境中該第一運算裝置所驗證之一經驗證的韌體套件。

【0068】 在另一個實例中，該控制器可以在該第一運算裝置重置以啟動一OS之前接收從該第一運算裝置所發出之一第二信任狀態訊息，該訊息指出該第一運算裝置正在離開或已經離開了一受信任的環境。回應於接收到該第二信任狀態訊息，該控制器可在被通信耦合到該第二運算裝置之一GPIO引腳處把一信任狀態信號的一狀態修改為一第二狀態。把該信任狀態信號修改成該第二狀態可以禁止該第二運算裝置安裝該韌體套件，因為雖然該韌體套件係被認定為經驗證的或係其他情況，但是該信任狀態信號不在是該第一狀態中。

【0069】 圖4圖示出使用與本發明一致之更新信號技術之一非暫時性的機器可讀取記憶體472及處理器470的一實例。諸如該非暫時性記憶體472之類的一記憶體資源可被使用來儲存由該處理器470所執行的指令(例如，474、476、478、等等)以執行在本文所描述的該等操作。該等操作不侷限於在本文所描述之一特定的實施例，並且可以包括針對圖1-3所描述之該等描述的組件及/或操作及/或與其互換。

【0070】 該處理器470可包括與一控制器相關聯及/或被併入到一第一運算裝置中的一處理器及/或特定應用積體電路。在一些實例中，該第一運算裝置可被通信地耦合到一控制器及/或具有嵌入在該第一運算裝置內的一控制器。該第一運算裝置可以包括一主機裝置用於驗證將被套用到一第二運算裝置的韌體更新。

【0071】 該非暫時性的記憶體472可以儲存可由該處理器470執行的指令474，以致使該第一運算裝置重置該第一運算裝置。該重置可以是一重置以提示該第一運算裝置的韌體在該第一運算裝置處載入一受信任的環境。該重置可以包括一重置，其在把由一韌體更新套件所產生之一更新套件包儲存到與該第一運算裝置相關聯之可延伸韌體介面系統(ESP)分區之後被產生及/或被觸發。

【0072】 該非暫時性記憶體472可以儲存可由該處理器470執行的指令

474，以致使該第一運算裝置利用操作在受信任的環境中該第一運算裝置的該韌體來驗證該韌體更新套件的一數位簽名。驗證該韌體更新套件的該數位簽名可以包括利用執行在該受信任的環境中該第一運算裝置的該韌體從該ESP分區檢索該更新套件包。可在該檢索到之更新套件包上執行一簽名驗證操作，以驗證該韌體更新套件的該簽名。例如，可以在該更新套件包上利用公鑰及/或私鑰來對該韌體更新套件之該數位簽名的執行一種密碼式的驗證。

【0073】該非暫時性的記憶體472可以儲存可由該處理器470執行的指令476，以致使該第一運算裝置產生將被傳遞至一GPIO信號引腳之一控制器的一信任狀態訊息。該信任狀態訊息可被產生並且經由一共享記憶體介面被傳送給該控制器。該信任狀態訊息可以包括一指令來信令該控制器經由該GPIO引腳向一第二運算裝置斷言一信任狀態信號。通過該GPIO引腳對該第二運算裝置之該信任狀態信號的該斷言可致能該第二運算裝置安裝由該第一運算裝置驗證之該經驗證的韌體更新套件。

【0074】一旦該第一運算裝置已完成一驗證操作及/或安裝一經驗證的韌體更新套件，該第一運算裝置可達到一準備要啟動事件。一準備啟動事件可以包括由該第一運算裝置之基於UEFI韌體的執行所指定之一事件序列中的一事件，該事件指使一重置而該重置標記了該第一運算裝置離開該受信任的環境。例如，該準備啟動事件可以是該第一運算裝置準備退出該受信任的環境並啟動一OS的事件。

【0075】回應於到達該準備啟動事件，該第一運算裝置可以產生一密切信任的更新訊息。該密切信任的更新訊息可以是經由一共享記憶體介面被傳送到一控制器的一信任狀態訊息。該密切信任的更新訊息可以包括給該控制器的指令，以解除對該第二運算裝置之該信任狀態信號的斷言。該信任狀態信號的解除斷言可禁止該第二運算裝置安裝一第二韌體更新套件。也就是說，在沒有一

被斷言之信任狀態信號的情況下，該第二運算裝置可以不允許安裝該韌體更新套件。

【0076】在本發明前述的詳細描述中，參考了構成本發明之一部分的該等附圖，並且在該等附圖中藉由說明的方式圖示出如何可以實踐本發明的實例。對這些實例已進行了足夠詳細的描述，以使得本領域的普通技術人員能夠實踐本發明的實例，並且應被理解的是其他的實例也可被利用，並且可以在不脫離本發明之範圍的情況下進行在工序、電氣及/或結構上的改變。此外，如在本文中所使用的，「複數個」元件及/或特徵可以指多於一個之如此的元件及/或特徵。

【0077】在本文中的該等附圖遵循一種編號的慣例，其中第一個數字對應於該附圖編號，其餘的數字標識在該等附圖中的元件或組件。在本文之各個圖中所圖示出的元件可被添加、交換、及/或移除，以便提供本發明之多數個額外的實例。另外，在附圖中所提供元件之比例以及相對大小旨在說明本發明的實例，而不應被認為係限制性的。

【符號說明】

【0078】

100、222:第一運算裝置

102、360、470:處理器

104: 信任狀態訊息

106、250:控制器

108: 信任狀態信號

110、256:第二運算裝置

220: 系統

224:韌體更新套件

226: 更新代理

228、234: 重置

230:啟動載入程式

232:更新套件包；韌體更新套件包

236:資料儲存分區

238:在準備啟動之前事件處的更新處理程式

240:驗證韌體簽名

242:執行韌體更新

244:在準備啟動事件處之密切信任的更新訊息

246:信任狀態訊息

248:共享記憶體

252:GPIO信號引腳

254:信任狀態信號

362、472:非暫時性的記憶體

364、366、474～478:方塊

【發明申請專利範圍】

【請求項1】 一種第一運算裝置，其包含有：

韌體；

一控制器；以及

一處理器，其中該處理器將進行下列動作：

產生將發送給該控制器的一信任狀態訊息，該信任狀態訊息指出該第一運算裝置的該韌體正操作一受信任的環境，以及

利用該韌體在該受信任的環境中驗證一更新；以及

其中該控制器回應於接收到該信任狀態訊息，向一第二運算裝置宣告一信任狀態信號，其指出該第一運算裝置的該韌體正操作該受信任的環境，其中該信任狀態信號的該宣告將致能該第二運算裝置安裝該經驗證的更新，及

其中該控制器回應於接收到由該處理器所產生的一第二信任狀態訊息而將該信任狀態信號的宣告解除，該第二信任狀態訊息指出該第一運算裝置已準備好要啟動該第一運算裝置之一作業系統(OS)。

【請求項2】 如請求項1之第一運算裝置，其中該第一運算裝置的該韌體係一基於統一可延伸韌體介面(UEFI)的韌體。

【請求項3】 如請求項1之第一運算裝置，其中當該第一運算裝置的該韌體正操作該受信任的環境時，該信任狀態信號維持由該控制器宣告的狀態。

【請求項4】 如請求項1之第一運算裝置，其中該處理器將執行該第一運算裝置的該韌體以藉由驗證與該更新相關聯的一數位簽名來驗證該更新。

【請求項5】 如請求項1之第一運算裝置，其中該控制器經由一共享記憶體介面通訊式地耦合到該處理器，其中該控制器將在一重置之後接受通過該共享記憶體介面所接收到的一初始訊息。

【請求項6】 如請求項1之第一運算裝置，其中該信任狀態信號係經由一通用輸入/輸出(GPIO)信號引腳向該第二運算裝置宣告。

【請求項7】 一種包括有指令之非暫時性機器可讀媒體，該等指令執行時，會致使一控制器進行下列動作：

從一第一運算裝置接收一信任狀態訊息以把一更新提供給一第二運算裝置；

基於該信任狀態訊息，指定向該第二運算裝置宣告之一通用輸入/輸出(GPIO)信任狀態信號的一信號狀態，其中該GPIO信任狀態信號的該信號狀態向該第二運算裝置指出該第一運算裝置是否正利用一受信任的環境來驗證該更新；以及

回應於接收到一密切信任的更新信任狀態訊息，修改該GPIO信任狀態信號的該狀態，其中該密切信任的更新信任狀態訊息係經由一非依電性嵌入式控制器隨機存取記憶體(ECRAM)從該第一運算裝置發出，該密切信任的更新信任狀態訊息指出該第一運算裝置已準備好要啟動一作業系統。

【請求項8】 如請求項7之非暫時性機器可讀媒體，其更包括有數個指令，該等指令執行時，致使該控制器回應於接收到在一重置後從該第一運算裝置所發出之一第二信任狀態訊息，而修改該GPIO信任狀態信號的該狀態，該第二信任狀態訊息指出該第一運算裝置正操作在該受信任的環境中。

【請求項9】 一種包括有指令之非暫時性機器可讀媒體，該等指令執行時，會致使一第一運算裝置進行下列動作：

重置該第一運算裝置以提示該第一運算裝置的韌體在該第一運算裝置載入一受信任環境；

以操作在該受信任環境中之該第一運算裝置的該韌體來驗證一韌體更新套件的一簽名；

產生將要傳遞至一通用輸入/輸出(GPIO)信號引腳之一控制器的一信任狀態訊息，以指示該控制器經由該GPIO信號引腳向一第二運算裝置宣告一信任狀態信號，其中該信任狀態信號的該宣告將致能該第二運算裝置安裝該經驗證的韌體更新套件；以及

回應於該第一運算裝置達到一準備啟動事件而產生一密切信任的更新訊息，該訊息將被傳遞給該控制器以指示該控制器解除對該第二運算裝置之該信任狀態信號的宣告。

【請求項10】如請求項9之非暫時性機器可讀媒體，其更包括有數個指令，該等指令執行時，致使該第一運算裝置的該處理器把從該韌體更新套件所產生的一更新套件包儲存到與該第一運算裝置相關聯的一可延伸韌體介面系統(ESP)分區。

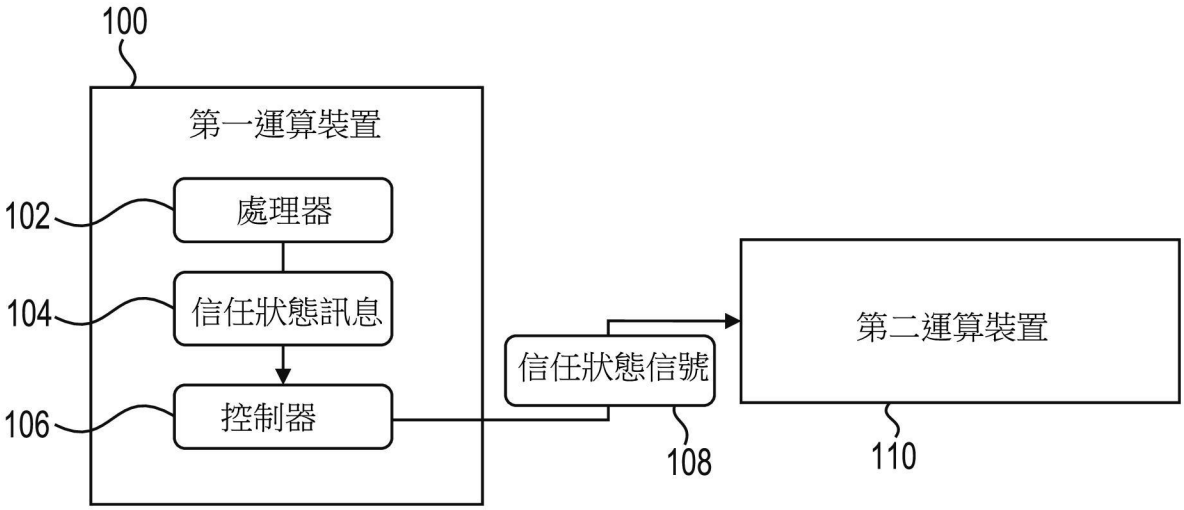
【請求項11】如請求項10之非暫時性機器可讀媒體，其更包括有數個指令，該等指令執行時，致使該第一運算裝置的該處理器進行下列動作：

以在該受信任環境中執行之該第一運算裝置的該韌體，從該ESP分區檢索該更新套件包；以及

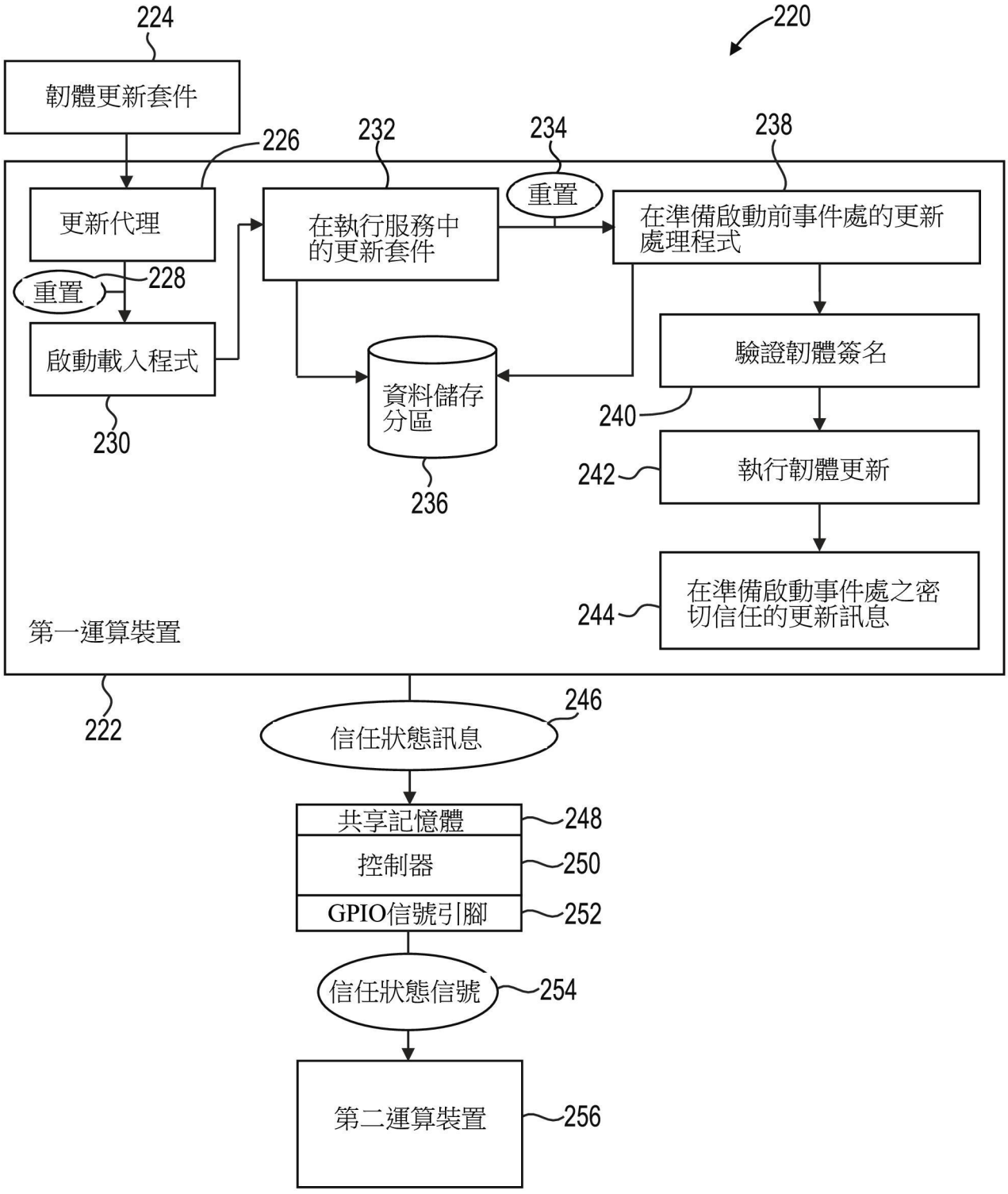
對該檢索到的更新套件包執行一簽名驗證操作來驗證該韌體更新套件的該簽名。

【請求項12】如請求項9之非暫時性機器可讀媒體，其中解除該信任狀態信號的宣告將禁止該第二運算裝置安裝一第二韌體更新套件。

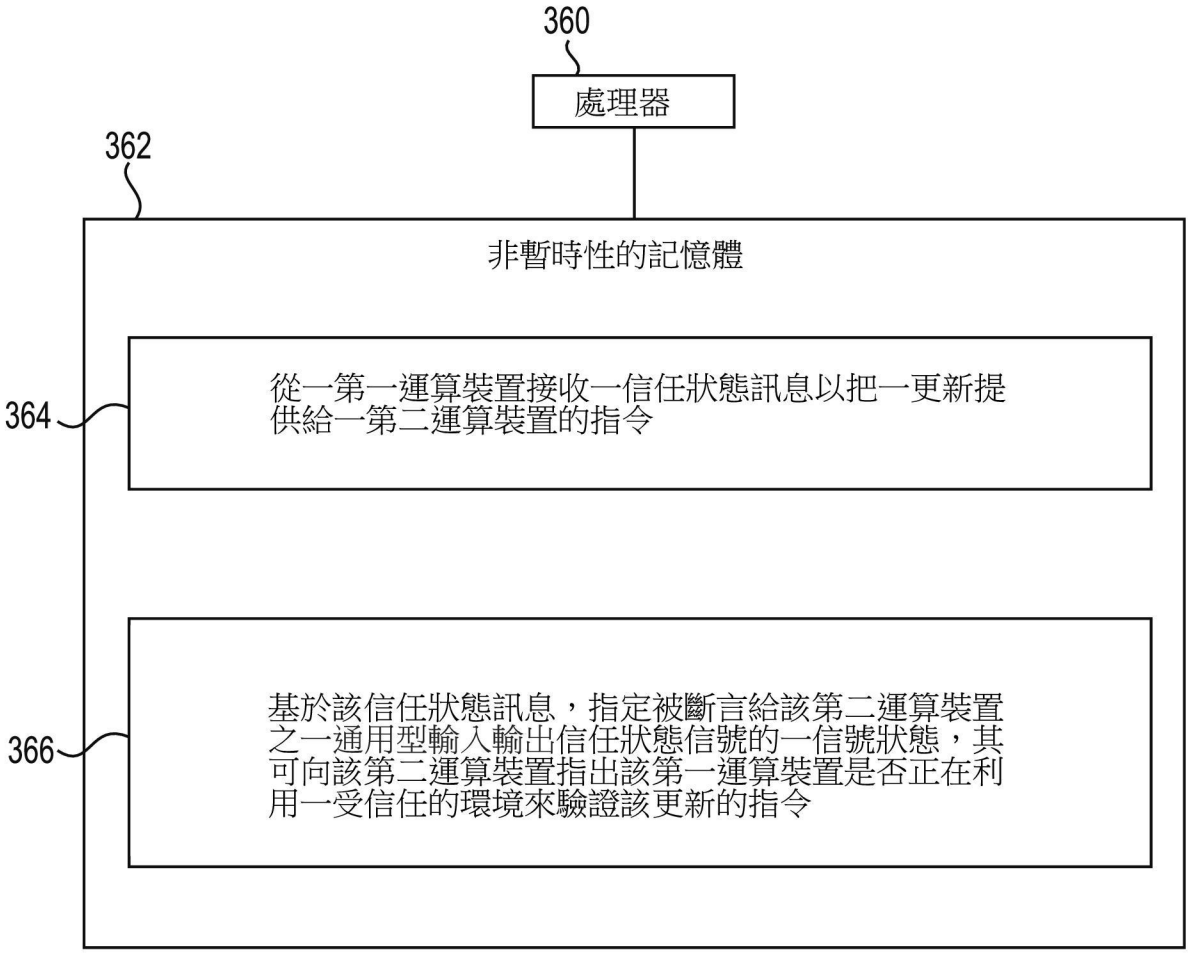
【發明圖式】



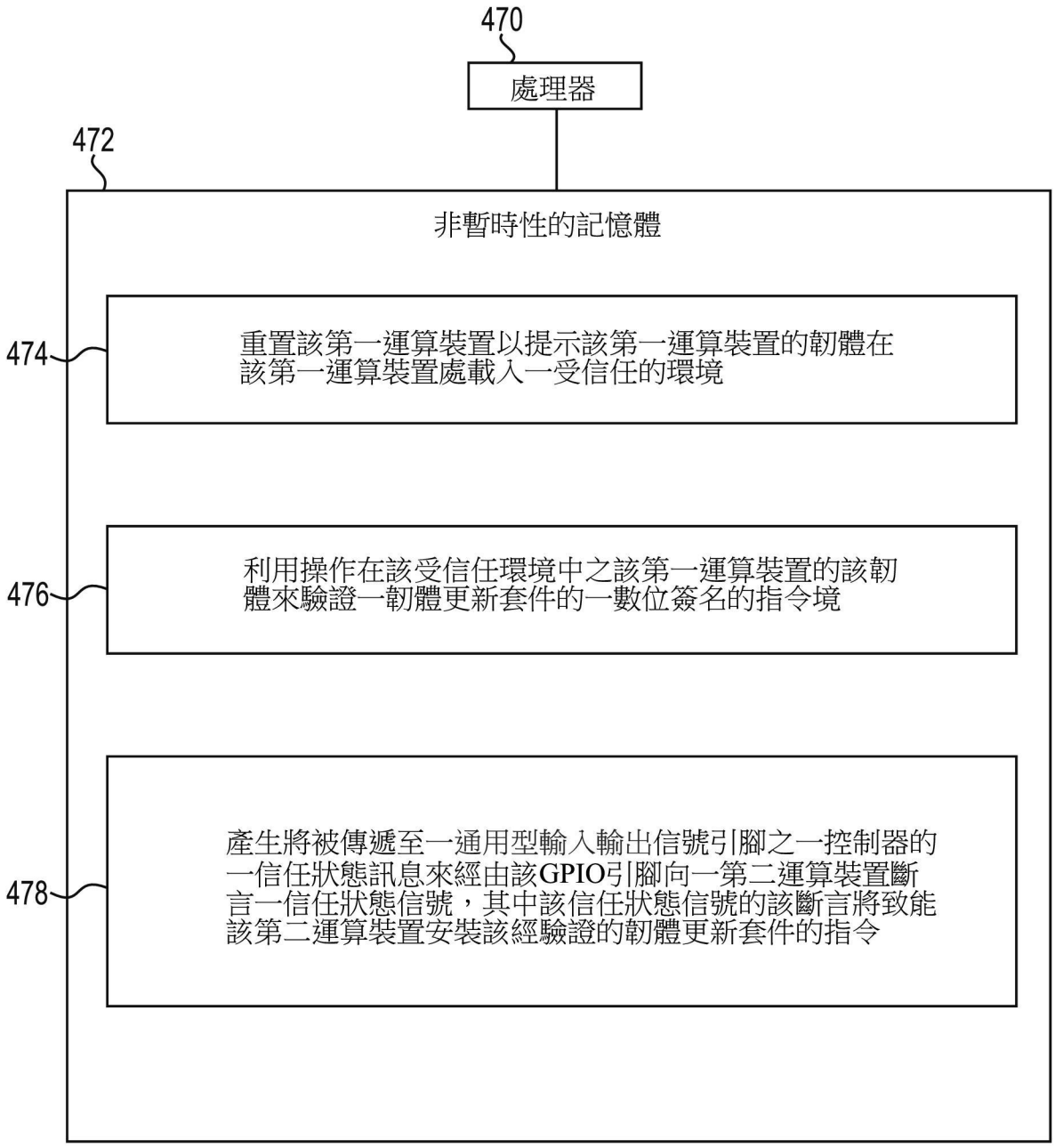
【圖1】


224
韌體更新套件
220
226
232
234
238
更新代理
在執行服務中的更新套件
重置
在準備啟動前事件處的更新處理程式
重置
228
啟動載入程式
230
資料儲存分區
236
驗證韌體簽名
240
執行韌體更新
242
在準備啟動事件處之密切信任的更新訊息
244
第一運算裝置
222
246
信任狀態訊息
共享記憶體
248
控制器
250
GPIO信號引腳
252
信任狀態信號
254
第二運算裝置
256

【圖2】


360
處理器
362
非暫時性的記憶體
364
從一第一運算裝置接收一信任狀態訊息以把一更新提供給一第二運算裝置的指令
366
基於該信任狀態訊息，指定被斷言給該第二運算裝置之一通用型輸入輸出信任狀態信號的一信號狀態，其可向該第二運算裝置指出該第一運算裝置是否正在利用一受信任的環境來驗證該更新的指令

【圖3】


470
處理器
472
非暫時性的記憶體
474
重置該第一運算裝置以提示該第一運算裝置的韌體在該第一運算裝置處載入一受信任的環境
476
利用操作在該受信任環境中之該第一運算裝置的該韌體來驗證一韌體更新套件的一數位簽名的指令境
478
產生將被傳遞至一通用型輸入輸出信號引腳之一控制器的一信任狀態訊息來經由該GPIO引腳向一第二運算裝置斷言一信任狀態信號，其中該信任狀態信號的該斷言將致能該第二運算裝置安裝該經驗證的韌體更新套件的指令

【圖4】