



(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 201937366 A

(43)公開日：中華民國 108 (2019) 年 09 月 16 日

(21)申請案號：107106581

(22)申請日：中華民國 107 (2018) 年 02 月 27 日

(51)Int. Cl.：

G06F9/06 (2006.01)

G06F21/44 (2013.01)

(71)申請人：其陽科技股份有限公司 (中華民國) AEWIN TECHNOLOGIES CO., LTD. (TW)

新北市汐止區大同路 2 段 133 號 9 樓

(72)發明人：陳志強 CHEN, CHIH CHIANG (TW)

(74)代理人：陳孚竹；張家彬

申請實體審查：有 申請專利範圍項數：20 項 圖式數：2 共 27 頁

(54)名稱

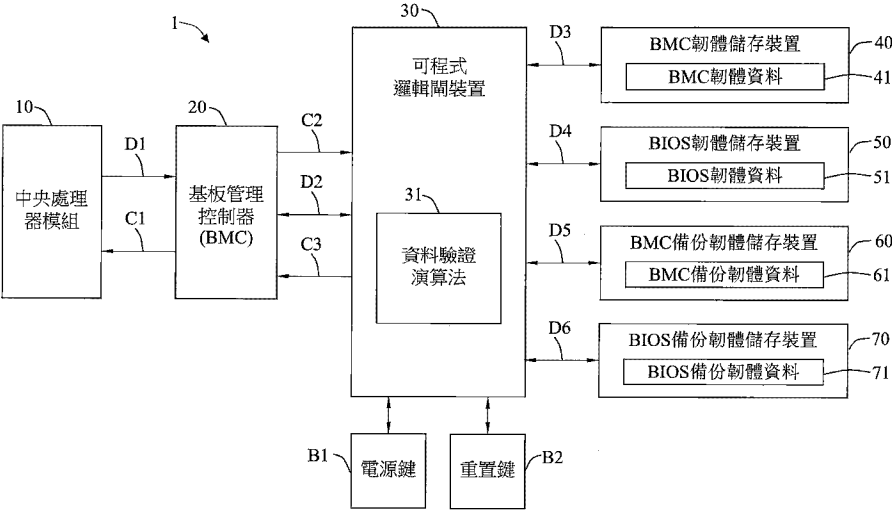
具開機之可信驗證與容錯移轉之計算機系統及方法

(57)摘要

本發明揭露一種具開機之可信驗證與容錯移轉之計算機系統及方法。該方法包括：提供一包括基板管理控制器(BMC)、BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置、BIOS 備份韌體儲存裝置與可程式邏輯閘裝置之計算機系統；當計算機系統進行開機時，由可程式邏輯閘裝置對 BMC 韌體資料與 BIOS 韌體資料執行可信驗證；以及當 BMC 韌體資料或 BIOS 韌體資料未通過可信驗證時，由可程式邏輯閘裝置將保證可信之 BMC 備份韌體資料或 BIOS 備份韌體資料對應覆蓋 BMC 韌體資料或 BIOS 韌體資料以達到容錯移轉。

A computer system and method with credible verification and fault tolerant transfer of boot-up are disclosed. The method includes: provide a computer system having a baseboard management controller (BMC), a BMC firmware storage apparatus, a BIOS firmware storage apparatus, a BMC backup firmware storage apparatus, a BIOS backup firmware storage apparatus and a programmable logic gate apparatus; when the computer system is boot-up, the programmable logic gate apparatus performs a trusted verification of the BMC firmware data and the BIOS firmware data; and when the BMC firmware data or BIOS firmware data fails to pass the trusted verification, the programmable logic gate apparatus writes the guaranteed credible BMC backup firmware data or BIOS backup firmware data to cover the BMC firmware data or BIOS firmware data to achieve fault tolerant transfer.

指定代表圖：



【第1圖】

符號簡單說明：

- 1 . . . 計算機系統
- 10 . . . 中央處理器模組
- 20 . . . 基板管理控制器
- 30 . . . 可程式邏輯閘裝置
- 31 . . . 資料驗證演算法
- 40 . . . BMC 韌體儲存裝置
- 41 . . . BMC 韌體資料
- 50 . . . BIOS 韌體儲存裝置
- 51 . . . BIOS 韌體資料
- 60 . . . BMC 備份韌體儲存裝置
- 61 . . . BMC 備份韌體資料
- 70 . . . BIOS 備份韌體儲存裝置
- 71 . . . BIOS 備份韌體資料
- B1 . . . 電源鍵
- B2 . . . 重置鍵
- C1 至 C3 . . . 控制匯流排
- D1 至 D6 . . . 資料匯流排

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

具開機之可信驗證與容錯移轉之計算機系統及方法

COMPUTER SYSTEM AND METHOD WITH
CREDIBLE VERIFICATION AND FAULT TOLERANT
TRANSFER OF BOOT-UP

【技術領域】

本發明係關於一種計算機系統，特別是指一種具開機之可信驗證與容錯移轉之計算機系統及方法。

【先前技術】

在現有技術之伺服器、個人電腦(PC)、筆記型電腦(NB)、或其他手持裝置(如智慧型手機)等計算機系統中，僅伺服器之內部有 TPM(Trusted Platform Module; 可信平台模組)卡能單純地驗證作業系統(Operating System; OS)之儲存裝置是否可信而沒有被變更過，更遑論個人電腦(PC)、筆記型電腦(NB)、或其他手持裝置是無驗證裝置的。

以伺服器而言，伺服器之基板管理控制器(Baseboard Management Controller; BMC)與基本輸入輸出系統(Basic Input/Output System; BIOS)通常無可信驗證與容錯移轉機制，一旦伺服器開機至作業系統(OS)之前的韌體有被植入後門或被竄改過，TPM 卡並無法偵測出來。

因此，現有技術實缺乏一種對計算機系統之開機程序

提供可信驗證與容錯移轉之保護機制。所以，如何解決上述現有技術之缺點，實已成為本領域技術人員之一大課題。

【發明內容】

本發明提供一種具開機之可信驗證與容錯移轉之計算機系統及方法，其能對計算機系統之開機程序提供可信驗證與容錯移轉之保護機制。

本發明中具開機之可信驗證與容錯移轉之計算機系統包括：一基板管理控制器(BMC)；一 BMC 韌體儲存裝置，其儲存有 BMC 韌體資料；一 BIOS(基本輸入輸出系統)韌體儲存裝置，其儲存有 BIOS 韌體資料；一 BMC 備份韌體儲存裝置，其儲存有無法被修改及保證可信之 BMC 備份韌體資料；一 BIOS 備份韌體儲存裝置，其儲存有無法被修改及保證可信之 BIOS 備份韌體資料；以及一可程式邏輯閘裝置，其將基板管理控制器物理隔離 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置，其中，當計算機系統進行開機時，由可程式邏輯閘裝置對 BMC 韌體儲存裝置之 BMC 韌體資料與 BIOS 韌體儲存裝置之 BIOS 韌體資料執行可信驗證，並在 BMC 韌體資料或 BIOS 韌體資料未通過可信驗證時，由可程式邏輯閘裝置將無法被修改及保證可信之 BMC 備份韌體儲存裝置之 BMC 備份韌體資料或 BIOS 備份韌體儲存裝置之 BIOS 備份韌體資料對應覆蓋未通過可信驗證之 BMC 韌體資料或 BIOS 韌體資料以達到容錯移轉。

本發明中具開機之可信驗證與容錯移轉之方法包括：

提供一包括基板管理控制器(BMC)、BMC 韌體儲存裝置、BIOS(基本輸入輸出系統)韌體儲存裝置、BMC 備份韌體儲存裝置、BIOS 備份韌體儲存裝置與可程式邏輯閘裝置之計算機系統，且可程式邏輯閘裝置將基板管理控制器物理隔離 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置；當計算機系統進行開機時，由可程式邏輯閘裝置對 BMC 韌體儲存裝置之 BMC 韌體資料與 BIOS 韌體儲存裝置之 BIOS 韌體資料執行可信驗證；以及當 BMC 韌體資料或 BIOS 韌體資料未通過可信驗證時，由可程式邏輯閘裝置將無法被修改及保證可信之 BMC 備份韌體儲存裝置之 BMC 備份韌體資料或 BIOS 備份韌體儲存裝置之 BIOS 備份韌體資料對應覆蓋未通過可信驗證之 BMC 韌體資料或 BIOS 韌體資料以達到容錯移轉。

為讓本發明之上述特徵和優點能更明顯易懂，下文特舉實施例，並配合所附圖式作詳細說明。在以下描述內容中將部分闡述本發明之額外特徵及優點，且此等特徵及優點將部分自所述描述內容顯而易見，或可藉由對本發明之實踐習得。本發明之特徵及優點借助於在申請專利範圍中特別指出的元件及組合來認識到並達到。應理解，前文一般描述與以下詳細描述兩者均僅為例示性及解釋性的，且不欲約束本發明所主張之範圍。

【圖式簡單說明】

第 1 圖係繪示本發明中具開機之可信驗證與容錯移轉

之計算機系統之方塊示意圖；以及

第 2 圖係繪示本發明中具開機之可信驗證與容錯移轉之方法之示意流程圖。

【實施方式】

以下藉由特定的具體實施形態說明本發明之實施方式，熟悉此技術之人士可由本說明書所揭示之內容輕易地了解本發明之其他優點與功效，亦可藉由其他不同的具體實施形態加以施行或應用。

第 1 圖係繪示本發明之具開機之可信驗證與容錯移轉之計算機系統 1 之方塊示意圖。如圖所示，計算機系統 1 包括一中央處理器模組 10、一基板管理控制器(BMC)20、一可程式邏輯閘裝置 30、一 BMC 韌體儲存裝置 40、一 BIOS(基本輸入輸出系統)韌體儲存裝置 50、一 BMC 備份韌體儲存裝置 60 與一 BIOS 備份韌體儲存裝置 70。

計算機系統 1 可應用於伺服器、個人電腦、筆記型電腦、平板電腦或智慧型手機等。中央處理器模組 10 可包括中央處理器(CPU)與南橋晶片組(Platform Controller Hub; PCH)等。可程式邏輯閘裝置 30 可為場域可程式閘陣列(Field-Programmable Gate Array, FPGA)、複雜可程式邏輯閘元件(Complex Programmable Logic Device, CPLD)、可程式邏輯閘元件(Programmable Logic Device, PLD)、或通用陣列邏輯(Generic Array Logic, GAL)。但是，本發明並不以此為限。

BMC 韌體儲存裝置 40 儲存有 BMC 韌體資料 41，BIOS

韌體儲存裝置 50 儲存有 BIOS 韌體資料 51，BMC 備份韌體儲存裝置 60 儲存有無法被修改及保證可信之 BMC 備份韌體資料 61，BIOS 備份韌體儲存裝置 70 儲存有無法被修改及保證可信之 BIOS 備份韌體資料 71。

可程式邏輯閘裝置 30 在計算機系統 1 中具有最高之主導權，並可將基板管理控制器 20 物理隔離 BMC 韌體儲存裝置 40、BIOS 韌體儲存裝置 50、BMC 備份韌體儲存裝置 60 與 BIOS 備份韌體儲存裝置 70，使基板管理控制器 20 無法直接讀取或寫入 BMC 韌體儲存裝置 40、BIOS 韌體儲存裝置 50、BMC 備份韌體儲存裝置 60 或 BIOS 備份韌體儲存裝置 70 等之韌體資料，即 BMC 韌體資料 41、BIOS 韌體資料 51、BMC 備份韌體資料 61 或 BIOS 備份韌體資料 71，以達到物理隔離保護該些韌體資料之效果。

當計算機系統 1 進行開機時，由可程式邏輯閘裝置 30 對 BMC 韌體儲存裝置 40 之 BMC 韌體資料 41 與 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51 執行可信驗證，並在 BMC 韌體資料 41 或 BIOS 韌體資料 51 未通過可信驗證時，由可程式邏輯閘裝置 30 將無法被修改及保證可信之 BMC 備份韌體儲存裝置 60 之 BMC 備份韌體資料 61 或 BIOS 備份韌體儲存裝置 70 之 BIOS 備份韌體資料 71 對應覆蓋未通過可信驗證之 BMC 韌體資料 41 或 BIOS 韌體資料 51 以達到容錯移轉。

詳言之，可程式邏輯閘裝置 30 具有一資料驗證演算法 31，以透過資料驗證演算法 31 對 BMC 韌體資料 41 或 BIOS

韌體資料 51 執行可信驗證，使可程式邏輯閘裝置 30 能安全讀取或寫入 BMC 韌體資料 41 或 BIOS 韌體資料 51。

可程式邏輯閘裝置 30 接上電源時會主動讀取 BMC 韌體儲存裝置 40 之 BMC 韌體資料 41，並在 BMC 韌體資料 41 通過資料驗證演算法 31 之可信驗證時，由可程式邏輯閘裝置 30 控制基板管理控制器 20 開始運行，使基板管理控制器 20 藉由可程式邏輯閘裝置 30 讀取 BMC 韌體資料 41。

中央處理器模組 10 係連接基板管理控制器 20，且可程式邏輯閘裝置 30 可將中央處理器模組 10 與基板管理控制器 20 物理隔離 BMC 韌體儲存裝置 40、BIOS 韌體儲存裝置 50、BMC 備份韌體儲存裝置 60 與 BIOS 備份韌體儲存裝置 70，使中央處理器模組 10 與基板管理控制器 20 皆無法直接讀取或寫入 BMC 韌體儲存裝置 40、BIOS 韌體儲存裝置 50、BMC 備份韌體儲存裝置 60 或 BIOS 備份韌體儲存裝置 70 等之韌體資料，以達到物理隔離保護該些韌體資料之效果。

計算機系統 1 可包括連接可程式邏輯閘裝置 30 之電源鍵 B1，且可程式邏輯閘裝置 30 會隨時監控電源鍵 B1 之訊號。當計算機系統 1 處於關機狀態時，可程式邏輯閘裝置 30 接收到電源鍵 B1 之訊號後才會讀取 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51，並由可程式邏輯閘裝置 30 之資料驗證演算法 31 對 BIOS 韌體資料 51 執行可信驗證。可程式邏輯閘裝置 30 將 BIOS 韌體資料 51 之可信驗證之

結果傳送至基板管理控制器 20，並在 BIOS 韌體資料 51 之可信驗證之結果為通過或可信時，由基板管理控制器 20 控制中央處理器模組 10 開始運行，使中央處理器模組 10 依序透過基板管理控制器 20 與可程式邏輯閘裝置 30 讀取 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51 以進行開機。

計算機系統 1 可包括連接可程式邏輯閘裝置 30 之重置鍵 B2，且可程式邏輯閘裝置 30 會隨時監控重置鍵 B2 之訊號。當計算機系統 1 處於開機狀態時，可程式邏輯閘裝置 30 接收到重置鍵 B2 之訊號後將其傳送至基板管理控制器 20，並由基板管理控制器 20 將重置鍵 B2 之訊號傳送至中央處理器模組 10，而中央處理器模組 10 在完成重置或關機後會送出通知訊號予基板管理控制器 20，以供基板管理控制器 20 控制中央處理器模組 10，使中央處理器模組 10 處於重置狀態而無法運作。

計算機系統 1 可包括一控制匯流排 C1，其分別連接中央處理器模組 10 與基板管理控制器 20，以供基板管理控制器 20 透過控制匯流排 C1 控制中央處理器模組 10。

計算機系統 1 可包括連接基板管理控制器 20 與可程式邏輯閘裝置 30 之控制匯流排 C2 及控制匯流排 C3，以使可程式邏輯閘裝置 30 透過控制匯流排 C3 控制基板管理控制器 20，或使基板管理控制器 20 經由控制匯流排 C2 傳送重置通知信號予可程式邏輯閘裝置 30。

計算機系統 1 可包括資料匯流排 D1 及資料匯流排 D2，資料匯流排 D1 分別連接中央處理器模組 10 與基板管

理控制器 20，而資料匯流排 D2 分別連接基板管理控制器 20 與可程式邏輯閘裝置 30，以進行資料之傳送。

計算機系統 1 可包括四資料匯流排，即資料匯流排 D3、資料匯流排 D4、資料匯流排 D5 及資料匯流排 D6，其分別連接可程式邏輯閘裝置 30 與 BMC 韌體儲存裝置 40、可程式邏輯閘裝置 30 與 BIOS 韌體儲存裝置 50、可程式邏輯閘裝置 30 與 BMC 備份韌體儲存裝置 60 以及可程式邏輯閘裝置 30 與 BIOS 備份韌體儲存裝置 70，以供可程式邏輯閘裝置 30 透過資料匯流排 D3、資料匯流排 D4、資料匯流排 D5 及資料匯流排 D6 分別讀取或寫入 BMC 韌體資料 41、BIOS 韌體資料 51、BMC 備份韌體資料 61 與 BIOS 備份韌體資料 71。

第 2 圖係繪示本發明之具開機之可信驗證與容錯移轉之方法之示意流程圖，並參閱第 1 圖加以說明。

本發明之具開機之可信驗證與容錯移轉之方法係提供一包括基板管理控制器(BMC)20、BMC 韌體儲存裝置 40、BIOS(基本輸入輸出系統)韌體儲存裝置 50、BMC 備份韌體儲存裝置 60、BIOS 備份韌體儲存裝置 70 與可程式邏輯閘裝置 30 之計算機系統 1，且可程式邏輯閘裝置 30 將基板管理控制器 20 物理隔離 BMC 韌體儲存裝置 40、BIOS 韌體儲存裝置 50、BMC 備份韌體儲存裝置 60 與 BIOS 備份韌體儲存裝置 70。當計算機系統 1 進行開機時，由可程式邏輯閘裝置 30 對 BMC 韌體儲存裝置 40 之 BMC 韌體資料 41 與 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51 執行

可信驗證。而且，當 BMC 韌體資料 41 或 BIOS 韌體資料 51 未通過可信驗證時，由可程式邏輯閘裝置 30 將無法被修改及保證可信之 BMC 備份韌體儲存裝置 60 之 BMC 備份韌體資料 61 或 BIOS 備份韌體儲存裝置 70 之 BIOS 備份韌體資料 71 對應覆蓋未通過可信驗證之 BMC 韌體資料 41 或 BIOS 韌體資料 51 以達到容錯移轉。

詳言之，在第 2 圖之步驟 S01 中，在計算機系統 1 接上電源並啟動計算機系統 1 之電源鍵 B1 之情況下，基板管理控制器 20 與可程式邏輯閘裝置 30 均有電且開始運作。

在第 2 圖之步驟 S02 中，由可程式邏輯閘裝置 30 控制計算機系統 1 之控制匯流排 C3，以使基板管理控制器 20 處於重置狀態而無法運行。接著，由可程式邏輯閘裝置 30 經由計算機系統 1 之資料匯流排 D3 讀取 BMC 韌體儲存裝置 40 之 BMC 韌體資料 41，並透過可程式邏輯閘裝置 30 之資料驗證演算法 31 對 BMC 韌體資料 41 執行可信驗證。

在第 2 圖之步驟 S03 中，由可程式邏輯閘裝置 30 之資料驗證演算法 31 判斷 BMC 韌體資料 41 是否通過可信驗證。若否，則進入步驟 S04；若是，則進入步驟 S05。

在第 2 圖之步驟 S04 中，若 BMC 韌體資料 41 未通過資料驗證演算法 31 之可信驗證，則可程式邏輯閘裝置 30 控制計算機系統 1 之資料匯流排 D5 以讀取 BMC 備份韌體儲存裝置 60 中無法被修改及保證可信之 BMC 備份韌體資料 61，並將無法被修改及保證可信之 BMC 備份韌體資料

61 經由資料匯流排 D3 寫入覆蓋 BMC 韌體儲存裝置 40 中未通過可信驗證之 BMC 韌體資料 41。

在第 2 圖之步驟 S05 中，若 BMC 韌體資料 41 通過資料驗證演算法 31 之可信驗證，則可程式邏輯閘裝置 30 控制計算機系統 1 之控制匯流排 C3 以釋放基板管理控制器 20 而開始運行，使基板管理控制器 20 依序透過計算機系統 1 之資料匯流排 D2 與可程式邏輯閘裝置 30 讀取 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51 以執行運作。

在第 2 圖之步驟 S06 中，判斷計算機系統 1 是否處於關機狀態。若否，則進入步驟 S15；若是，則進入步驟 S07。

在第 2 圖之步驟 S07 中，若計算機系統 1 處於關機狀態，則基板管理控制器 20 控制計算機系統 1 之控制匯流排 C1，以使計算機系統 1 之中央處理器模組 10 處於重置狀態而無法運作。

在第 2 圖之步驟 S08 中，由可程式邏輯閘裝置 30 持續監控計算機系統 1 之電源鍵 B1 是否被啟動而送出開機訊號。若否，則進入步驟 S09；若是，則進入步驟 S11。

在第 2 圖之步驟 S09 中，由可程式邏輯閘裝置 30 持續監控基板管理控制器 20 是否發生內部或非預期之外力重置。若否，則返回步驟 S08；若是，則進入步驟 S10。

在第 2 圖之步驟 S10 中，由基板管理控制器 20 透過控制匯流排 C2 傳送重置通知信號予可程式邏輯閘裝置 30，並返回步驟 S02。

在第 2 圖之步驟 S11 中，若可程式邏輯閘裝置 30 收

到電源鍵 B1 被啟動而送出之開機訊號，則可程式邏輯閘裝置 30 透過資料匯流排 D4 讀取 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51，並由可程式邏輯閘裝置 30 之資料驗證演算法 31 對 BIOS 韌體資料 51 執行可信驗證。

在第 2 圖之步驟 S12 中，由可程式邏輯閘裝置 30 之資料驗證演算法 31 判斷 BIOS 韌體資料 51 是否通過可信驗證。若否，則進入步驟 S13；若是，則進入步驟 S14。

在第 2 圖之步驟 S13 中，若 BIOS 韌體資料 51 未通過可信驗證，則可程式邏輯閘裝置 30 控制計算機系統 1 之資料匯流排 D6 以讀取 BIOS 備份韌體儲存裝置 70 中無法被修改及保證可信之 BIOS 備份韌體資料 71，並將無法被修改及保證可信之 BIOS 備份韌體資料 71 經由計算機系統 1 之資料匯流排 D4 寫入覆蓋 BIOS 韌體儲存裝置 50 中未通過可信驗證之 BIOS 韌體資料 51。

在第 2 圖之步驟 S14 中，若 BIOS 韌體資料 51 通過可信驗證，則可程式邏輯閘裝置 30 控制計算機系統 1 之控制匯流排 C3 以通知基板管理控制器 20 有關 BIOS 韌體資料 51 已通過可信驗證，使基板管理控制器 20 控制計算機系統之控制匯流排 C1 以釋放計算機系統 1 之中央處理器模組 10 而開始運作。中央處理器模組 10 開始運作後會控制資料匯流排 D1，並依序透過基板管理控制器 20、資料匯流排 D2、可程式邏輯閘裝置 30、資料匯流排 D4 去讀取 BIOS 韌體儲存裝置 50 之 BIOS 韌體資料 51 以執行計算機系統 1 之開機，此時計算機系統 1 已安全開機。

在第 2 圖之步驟 S15 中，由可程式邏輯閘裝置 30 持續監控電源鍵 B1 或重置鍵 B2 是否被啟動而送出相應之關機訊號或重置訊號。若否，則進入步驟 S16；若是，則進入步驟 S17。

在第 2 圖之步驟 S16 中，由可程式邏輯閘裝置 30 持續監控基板管理控制器 20 是否發生內部或非預期之外力重置。若否，則返回步驟 S15；若是，則進入步驟 S10。

在第 2 圖之步驟 S17 中，若可程式邏輯閘裝置 30 收到電源鍵 B1 之關機訊號或重置鍵 B2 之重置訊號，則可程式邏輯閘裝置 30 會控制該控制匯流排 C3 通知基板管理控制器 20，使基板管理控制器 20 透過控制匯流排 C1 傳送關機訊號或重置訊號至中央處理器模組 10，而中央處理器模組 10 會依據關機訊號或重置訊號執行相應之關機或重置動作，並經由資料匯流排 D1 送出重置訊號予基板管理控制器 20，此時返回步驟 S07。

由上可知，本發明之具開機之可信驗證與容錯移轉之計算機系統及方法中，當計算機系統進行開機時，經由可程式邏輯閘裝置對 BMC 韌體資料與 BIOS 韌體資料執行可信驗證，並在 BMC 韌體資料或 BIOS 韌體資料未通過可信驗證時，將無法被修改及保證可信之 BMC 備份韌體資料或 BIOS 備份韌體資料寫入覆蓋未通過可信驗證之 BMC 韌體資料或 BIOS 韌體資料，藉以達到容錯移轉，據此提供對計算機系統之開機程序具有可信驗證與容錯移轉之保護機制。

同時，本發明之可程式邏輯閘裝置可將基板管理控制器（或中央處理器模組）物理隔離 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置，使基板管理控制器（或中央處理器模組）無法直接讀取或寫入 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置或 BIOS 備份韌體儲存裝置等之韌體資料，以達到物理隔離保護該些韌體資料之效果。

再者，本發明之基板管理控制器(BMC)需透過可程式邏輯閘裝置才能讀取其開機之 BMC 韌體資料以達成第一層之分層保護，而中央處理器模組需透過基板管理控制器與可程式邏輯閘裝置才能讀取其開機之 BIOS 韌體資料以達成第二層之分層保護，藉此提供雙層之保護機制。

上述實施形態僅例示性說明本發明之原理、特點及其功效，並非用以限制本發明之可實施範疇，任何熟習此項技藝之人士均可在不違背本發明之精神及範疇下，對上述實施形態進行修飾與改變。任何運用本發明所揭示內容而完成之等效改變及修飾，均仍應為申請專利範圍所涵蓋。因此，本發明之權利保護範圍，應如申請專利範圍所列。

【符號說明】

- 1 計算機系統
- 10 中央處理器模組
- 20 基板管理控制器
- 30 可程式邏輯閘裝置
- 31 資料驗證演算法

40	BMC 韌體儲存裝置
41	BMC 韌體資料
50	BIOS 韌體儲存裝置
51	BIOS 韌體資料
60	BMC 備份韌體儲存裝置
61	BMC 備份韌體資料
70	BIOS 備份韌體儲存裝置
71	BIOS 備份韌體資料
B1	電源鍵
B2	重置鍵
C1 至 C3	控制匯流排
D1 至 D6	資料匯流排
S01 至 S17	步驟

發明摘要

【發明名稱】(中文/英文)

具開機之可信驗證與容錯移轉之計算機系統及方法

COMPUTER SYSTEM AND METHOD WITH
CREDIBLE VERIFICATION AND FAULT TOLERANT
TRANSFER OF BOOT-UP

【中文】

本發明揭露一種具開機之可信驗證與容錯移轉之計算機系統及方法。該方法包括：提供一包括基板管理控制器(BMC)、BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置、BIOS 備份韌體儲存裝置與可程式邏輯閘裝置之計算機系統；當計算機系統進行開機時，由可程式邏輯閘裝置對 BMC 韌體資料與 BIOS 韌體資料執行可信驗證；以及當 BMC 韌體資料或 BIOS 韌體資料未通過可信驗證時，由可程式邏輯閘裝置將保證可信之 BMC 備份韌體資料或 BIOS 備份韌體資料對應覆蓋 BMC 韌體資料或 BIOS 韌體資料以達到容錯移轉。

【英文】

A computer system and method with credible verification and fault tolerant transfer of boot-up are disclosed. The method includes: provide a computer system having a baseboard management controller (BMC), a BMC firmware storage apparatus, a BIOS firmware storage apparatus, a BMC backup firmware storage apparatus, a BIOS backup firmware storage apparatus and a programmable logic gate apparatus; when the computer system is boot-up, the programmable logic gate apparatus performs a trusted verification of the BMC firmware data and the BIOS firmware data; and when the BMC firmware data or BIOS firmware data fails to pass the trusted verification, the programmable logic gate apparatus writes the guaranteed credible BMC backup firmware data or BIOS backup firmware data to cover the BMC firmware data or BIOS firmware data to achieve fault tolerant transfer.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

1	計算機系統
10	中央處理器模組
20	基板管理控制器
30	可程式邏輯閘裝置
31	資料驗證演算法
40	BMC 韌體儲存裝置
41	BMC 韌體資料
50	BIOS 韌體儲存裝置
51	BIOS 韌體資料
60	BMC 備份韌體儲存裝置
61	BMC 備份韌體資料
70	BIOS 備份韌體儲存裝置
71	BIOS 備份韌體資料
B1	電源鍵
B2	重置鍵
C1 至 C3	控制匯流排
D1 至 D6	資料匯流排

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

本案無化學式。

申請專利範圍

1. 一種具開機之可信驗證與容錯移轉之計算機系統，包括：

- 一基板管理控制器(BMC)；

- 一 BMC 韌體儲存裝置，係儲存有 BMC 韌體資料；

- 一 BIOS(基本輸入輸出系統)韌體儲存裝置，係儲存有 BIOS 韌體資料；

- 一 BMC 備份韌體儲存裝置，係儲存有無法被修改及保證可信之 BMC 備份韌體資料；

- 一 BIOS 備份韌體儲存裝置，係儲存有無法被修改及保證可信之 BIOS 備份韌體資料；以及

- 一可程式邏輯閘裝置，係將該基板管理控制器物理隔離該 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置，

其中，當該計算機系統進行開機時，由該可程式邏輯閘裝置對該 BMC 韌體儲存裝置之 BMC 韌體資料與該 BIOS 韌體儲存裝置之 BIOS 韌體資料執行可信驗證，並在該 BMC 韌體資料或該 BIOS 韌體資料未通過該可信驗證時，由該可程式邏輯閘裝置將無法被修改及保證可信之該 BMC 備份韌體儲存裝置之 BMC 備份韌體資料或該 BIOS 備份韌體儲存裝置之 BIOS 備份韌體資料對應覆蓋未通過該可信驗證之該 BMC 韌體資料或該 BIOS 韌體資料。

2. 如申請專利範圍第 1 項所述之計算機系統，其中，該

計算機系統係應用於伺服器、個人電腦、筆記型電腦、平板電腦或智慧型手機，該可程式邏輯閘裝置為場域可程式閘陣列 (FPGA)、複雜可程式邏輯閘元件 (CPLD)、可程式邏輯閘元件 (PLD)、或通用陣列邏輯 (GAL)。

3. 如申請專利範圍第 1 項所述之計算機系統，其中，該可程式邏輯閘裝置透過資料驗證演算法對該 BMC 韌體資料或該 BIOS 韌體資料執行該可信驗證，使該可程式邏輯閘裝置安全讀取或寫入該 BMC 韌體資料或該 BIOS 韌體資料。
4. 如申請專利範圍第 3 項所述之計算機系統，其中，該可程式邏輯閘裝置接上電源時主動讀取該 BMC 韌體儲存裝置之 BMC 韌體資料，並在該 BMC 韌體資料通過該資料驗證演算法之該可信驗證時，由該可程式邏輯閘裝置控制該基板管理控制器開始運行，使該基板管理控制器讀取該 BMC 韌體資料。
5. 如申請專利範圍第 1 項所述之計算機系統，更包括一連接該基板管理控制器之中央處理器模組，且該可程式邏輯閘裝置將該中央處理器模組與該基板管理控制器物理隔離該 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置。
6. 如申請專利範圍第 5 項所述之計算機系統，更包括一連接該可程式邏輯閘裝置之電源鍵，該可程式邏輯閘

裝置隨時監控該電源鍵之訊號，當該計算機系統處於關機狀態時，該可程式邏輯閘裝置接收到該電源鍵之訊號後才讀取該 BIOS 韌體儲存裝置之 BIOS 韌體資料，並由該可程式邏輯閘裝置之資料驗證演算法對該 BIOS 韌體資料執行該可信驗證。

7. 如申請專利範圍第 6 項所述之計算機系統，其中，該可程式邏輯閘裝置將該 BIOS 韌體資料之可信驗證之結果傳送至該基板管理控制器，並在該 BIOS 韌體資料之可信驗證之結果為通過或可信時，由該基板管理控制器控制該中央處理器模組開始運行，使該中央處理器模組依序透過該基板管理控制器與該可程式邏輯閘裝置讀取該 BIOS 韌體儲存裝置之 BIOS 韌體資料以進行開機。
8. 如申請專利範圍第 5 項所述之計算機系統，更包括一連接該可程式邏輯閘裝置之重置鍵，該可程式邏輯閘裝置隨時監控該重置鍵之訊號，當該計算機系統處於開機狀態時，該可程式邏輯閘裝置接收到該重置鍵之訊號後將其傳送至該基板管理控制器，並由該基板管理控制器將該重置鍵之訊號傳送至該中央處理器模組，而該中央處理器模組在完成重置或關機後送出通知訊號予該基板管理控制器，以供該基板管理控制器控制該中央處理器模組，使該中央處理器模組處於重置狀態而無法運作。
9. 如申請專利範圍第 1 項所述之計算機系統，更包括至

少一控制匯流排，係連接該基板管理控制器與該可程式邏輯閘裝置，以供該可程式邏輯閘裝置透過該控制匯流排控制該基板管理控制器。

10. 如申請專利範圍第 1 項所述之計算機系統，更包括四資料匯流排，係分別連接該可程式邏輯閘裝置與該 BMC 韌體儲存裝置、該可程式邏輯閘裝置與該 BIOS 韌體儲存裝置、該可程式邏輯閘裝置與該 BMC 備份韌體儲存裝置以及該可程式邏輯閘裝置與該 BIOS 備份韌體儲存裝置，以供該可程式邏輯閘裝置透過該四資料匯流排分別讀取或寫入該 BMC 韌體資料、BIOS 韌體資料、BMC 備份韌體資料與 BIOS 備份韌體資料。

11. 一種具開機之可信驗證與容錯移轉之方法，包括：

提供一包括基板管理控制器(BMC)、BMC 韌體儲存裝置、BIOS(基本輸入輸出系統)韌體儲存裝置、BMC 備份韌體儲存裝置、BIOS 備份韌體儲存裝置與可程式邏輯閘裝置之計算機系統，且該可程式邏輯閘裝置將該基板管理控制器物理隔離該 BMC 韌體儲存裝置、BIOS 韌體儲存裝置、BMC 備份韌體儲存裝置與 BIOS 備份韌體儲存裝置；

當該計算機系統進行開機時，由該可程式邏輯閘裝置對該 BMC 韌體儲存裝置之 BMC 韌體資料與該 BIOS 韌體儲存裝置之 BIOS 韌體資料執行可信驗證；
以及

當該 BMC 韌體資料或該 BIOS 韌體資料未通過該

可信驗證時，由該可程式邏輯閘裝置將無法被修改及保證可信之該 BMC 備份韌體儲存裝置之 BMC 備份韌體資料或該 BIOS 備份韌體儲存裝置之 BIOS 備份韌體資料對應覆蓋未通過該可信驗證之該 BMC 韌體資料或該 BIOS 韌體資料。

12. 如申請專利範圍第 11 項所述之方法，更包括當該計算機系統接上電源且啟動該計算機系統之電源鍵時，該可程式邏輯閘裝置控制該計算機系統之一控制匯流排以使該基板管理控制器處於重置狀態而無法運行。
13. 如申請專利範圍第 11 項所述之方法，更包括由該可程式邏輯閘裝置經由該計算機系統之一資料匯流排讀取該 BMC 韌體儲存裝置之 BMC 韌體資料，以透過該可程式邏輯閘裝置之資料驗證演算法對該 BMC 韌體資料執行該可信驗證。
14. 如申請專利範圍第 13 項所述之方法，其中，若該 BMC 韌體資料未通過該可信驗證，該可程式邏輯閘裝置控制該計算機系統之另一資料匯流排以讀取該 BMC 備份韌體儲存裝置之 BMC 備份韌體資料，並將 BMC 備份韌體資料經由該資料匯流排寫入覆蓋該 BMC 韌體資料。
15. 如申請專利範圍第 13 項所述之方法，其中，若該 BMC 韌體資料通過該可信驗證，該可程式邏輯閘裝置控制該計算機系統之控制匯流排以釋放該基板管理控制器而開始運行，使該基板管理控制器透過該計算機系統

之又一資料匯流排藉由該可程式邏輯閘裝置讀取該 BMC 韌體儲存裝置之 BMC 韌體資料以執行運作。

16. 如申請專利範圍第 11 項所述之方法，更包括若該計算機系統處於關機狀態，該基板管理控制器控制該計算機系統之一控制匯流排，以使該計算機系統之中央處理器模組處於重置狀態而無法運作。
17. 如申請專利範圍第 11 項所述之方法，更包括由該可程式邏輯閘裝置持續監控該基板管理控制器是否發生內部或非預期之外力重置。
18. 如申請專利範圍第 11 項所述之方法，更包括由該可程式邏輯閘裝置持續監控該計算機系統之電源鍵是否被啟動，若該可程式邏輯閘裝置收到該電源鍵被啟動而送出之開機訊號，該可程式邏輯閘裝置讀取該 BIOS 韌體儲存裝置之 BIOS 韌體資料，並由該可程式邏輯閘裝置之資料驗證演算法對該 BIOS 韌體資料執行該可信驗證。
19. 如申請專利範圍第 18 項所述之方法，更包括若該 BIOS 韌體資料未通過該可信驗證，該可程式邏輯閘裝置控制該計算機系統之一資料匯流排以讀取該 BIOS 備份韌體儲存裝置中保證可信之該 BIOS 備份韌體資料，並將該 BIOS 備份韌體資料經由該計算機系統之另一資料匯流排寫入覆蓋該 BIOS 韌體資料。
20. 如申請專利範圍第 18 項所述之方法，其中，若該 BIOS 韌體資料通過該可信驗證，該可程式邏輯閘裝置控制

該計算機系統之一控制匯流排以通知該基板管理控制器有關該 BIOS 韌體資料已通過該可信驗證，使該基板管理控制器控制該計算機系統之另一控制匯流排以釋放該計算機系統之中央處理器模組而開始運作。

