



(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 I522838 B

(45)公告日：中華民國 105 (2016) 年 02 月 21 日

(21)申請案號：103106570

(22)申請日：中華民國 103 (2014) 年 02 月 26 日

(51)Int. Cl. : G06F21/57 (2013.01)

G06F9/445 (2006.01)

(30)優先權：2013/04/23 世界智慧財產權組織 PCT/US13/37727

(71)申請人：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)；尼西諺 馬瑞特 NERSISYAN, MARAT (US)；巴米迪帕提 阿尤創姆 BHAMIDIPATY, ACHYUTRAM (US)；史考特 杰尼 E SCOTT, JAYNE E. (US)

(74)代理人：憚軼群；陳文郎

(56)參考文獻：

TW 200941344A

TW 201020785A

CN 1534685A

US 7908470B1

US 20080086629A1

US 20090150598A1

US 2009/0049293A1

審查人員：王鵬翔

申請專利範圍項數：15 項 圖式數：4 共 38 頁

(54)名稱

組配系統之技術

CONFIGURING A SYSTEM

(57)摘要

回應啟動包含一包括系統啟動碼之第一非依電性記憶體及一第二非依電性記憶體之一系統，執行該第二非依電性記憶體之配設。該配設包含檢查該第二非依電性記憶體係未初始化，以及回應判定該第二非依電性記憶體係未初始化，該系統啟動碼係由該第一非依電性記憶體複製至該第二非依電性記憶體。

In response to starting a system including a first non-volatile memory containing system boot code, and a second non-volatile memory, provisioning of the second non-volatile memory is performed. The provisioning includes checking that the second non-volatile memory is uninitialized, and in response to determining that the second non-volatile memory is uninitialized, the system boot code is copied from the first non-volatile memory to the second non-volatile memory.

指定代表圖：

符號簡單說明：
102-106 . . . 作業步驟

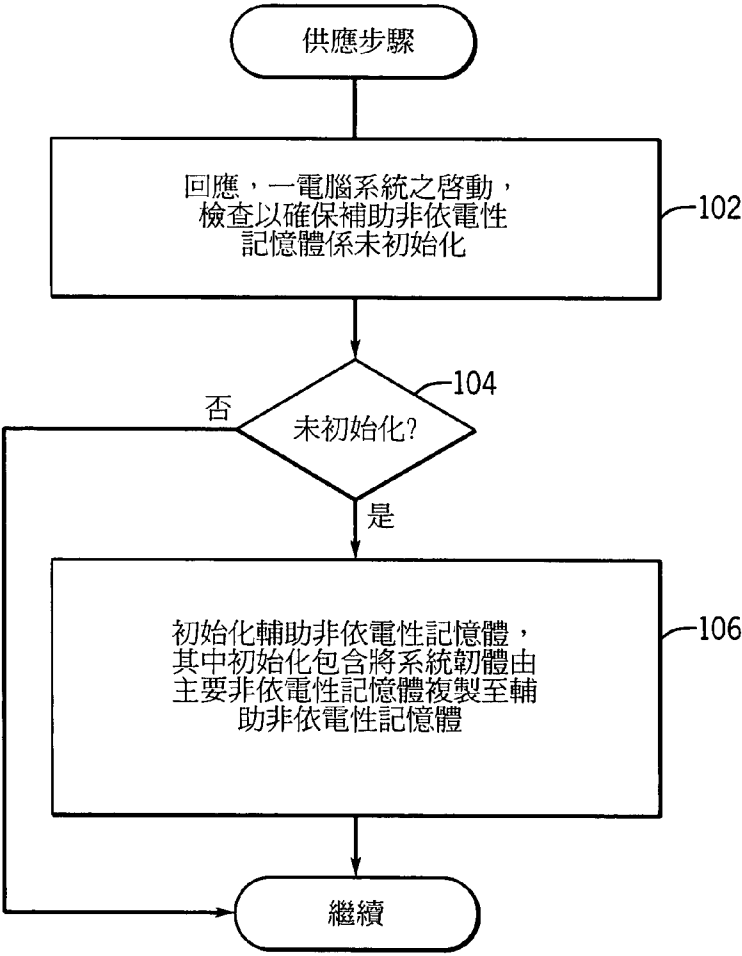


圖1

發明摘要

公告本

※ 申請案號：103106570

※ 申請日：103.2.26

※ IPC 分類：

G06F 21/57 (2013.01)

【發明名稱】(中文/英文)

9/445 (2006.01)

組配系統之技術

CONFIGURING A SYSTEM

【中文】

回應啟動包含一包括系統啟動碼之第一非依電性記憶體及一第二非依電性記憶體之一系統，執行該第二非依電性記憶體之配設。該配設包含檢查該第二非依電性記憶體係未初始化，以及回應判定該第二非依電性記憶體係未初始化，該系統啟動碼係由該第一非依電性記憶體複製至該第二非依電性記憶體。

【英文】

In response to starting a system including a first non-volatile memory containing system boot code, and a second non-volatile memory, provisioning of the second non-volatile memory is performed. The provisioning includes checking that the second non-volatile memory is uninitialized, and in response to determining that the second non-volatile memory is uninitialized, the system boot code is copied from the first non-volatile memory to the second non-volatile memory.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

102-106...作業步驟

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

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)

組配系統之技術

CONFIGURING A SYSTEM

【技術領域】

發明領域

[0001]本發明係有關於組配系統之技術。

【先前技術】

發明背景

[0002]一種電腦系統可包含碼以執行該電腦系統之各種啓動功能。此碼可包含基本輸入/輸出系統(BIOS)碼。BIOS碼可為受到電腦系統中或來自一項外部服務之有毒軟體之攻擊主體。由於一項攻擊，該BIOS碼可能變成受到危害。

【發明內容】

發明概要

[0003]依據本發明之實施例，係特別提出一種組配一系統之方法，包含：回應啓動包含一包括系統啓動碼之第一非依電性記憶體以及一第二非依電性記憶體之一系統，藉由一控制器執行該第二非依電性記憶體之配設，該配設包含：檢查該第二非依電性記憶體係未初始化，以及回應判定該第二非依電性記憶體係未初始化，將該系統啓動碼由該第一非依電性記憶體複製至該第二非依電性記憶體。

【圖式簡單說明】

[0004]相關於下列圖式以說明某些實施例：

圖1係依據某些建置之一配設步驟之一流程圖；

圖2係一結合某些建置之例示性電腦系統之一方塊圖；

圖3係依據某些建置之一利用系統資料之程序之一流程圖；以及

圖4係依據某些建置之有關一製造程式化模式之各種狀態之一狀態圖。

【實施方式】

詳細說明

[0005]對用以執行一電腦系統啟動之系統碼之有毒軟體攻擊可能導致該電腦系統之完整性受到危害，使得電腦系統中未經授權之存取及作業可能發生。例如，受危害之系統碼可能容許一惡意實體之隱蔽式遠端監視及/或電腦系統之控制、藉由有毒軟體而在電腦系統中之未經授權之存取及/或資料修改、電腦系統之失效、等。受危害之系統碼可能指已被毀壞且因此系統碼無法再使用之系統碼、或替代地，受危害之系統碼可能指已被某種方式改變但系統碼仍可執行之系統碼。注意系統碼亦可能受到意外地或故意地危害。

[0006]雖然一保護機制可設於一電腦系統中以保護系統碼，然而此種保護機制可能在某些情況下變成受到危害，而前述狀況可使該系統碼遭受有毒軟體攻擊。

[0007]用以執行一電腦系統啟動之系統碼可包含系統

韌體，而該系統韌體可為在該電腦系統之一處理器(或多數處理器)上可執行之機器可讀取式指令之型式。”系統韌體”可涵蓋能夠執行一電腦系統之啟動之任何機器可讀取式指令。電腦系統之實例包含桌上型電腦、筆記型電腦、平板電腦、個人數位助理器(PDAs)、智慧手機、遊戲裝置、伺服器電腦、儲存節點、網路通訊節點、等。

[0008]系統韌體可包含基本輸入/輸出系統(BIOS)碼，而該BIOS碼可初始化電腦系統之各種組件，以及載入電腦系統之一作業程式(OS)。BIOS碼可執行硬體組件之檢查以確保該等硬體組件係現存的以及適當地運行。舉例而言，此可為一開啓電源自我測試(POST)步驟。POST步驟之後，BIOS碼可進行一啟動序列之其餘部分，前述作業之後，BIOS碼可載入以及傳送控制至OS。BIOS碼可包含傳統BIOS碼或統一可延伸韌體介面(UEFI)碼。某些實例中，BIOS碼可包含一運行時間部分而該運行時間部分可在OS載入之後加以執行。

[0009]現行討論中，雖然係提及”系統韌體”，然而要注意的是技術或機制可適用於其他型式之系統啟動碼，其中系統啟動碼可指重新啟動一電腦系統後能夠啟動該電腦系統或能夠自一低電力狀態回復該電腦系統之任何碼。

[0010]一電腦系統亦可包含一嵌入式控制器，自電腦系統之處理器分離，俾執行各種所指定之工作。型式為嵌入式控制器(EC)韌體之控制碼可在嵌入式控制器上執行俾執行所指定之工作。EC韌體係為機器可讀取式指令之型

式。雖然提供保護機制以保護EC韌體免於受到危害，然而EC韌體亦有可能在某些情況下變成受到危害。

[0011]隨後之討論中，係涉及可於一嵌入式控制器中執行之EC韌體。某些實例中，依據某些建置之技術或機制可適用於可在一嵌入式控制器或其他型式之控制器中執行之其他型式之控制器碼。

[0012]另，隨後之討論中，係假設EC韌體係系統韌體之部分。其他建置中，EC韌體可自系統韌體分離。

[0013]為保護系統韌體免於，因為一有毒軟體攻擊或非故意之危害，受到危害，除了用以儲存系統韌體之一主要非依電性記憶體以外，可提供一輔助非依電性記憶體。輔助非依電性記憶體可用以儲存系統韌體之一複本。輔助非依電性記憶體上之系統韌體複本可為主要非依電性記憶體中之系統韌體之複本。替代地，輔助非依電性記憶體中之系統韌體複本可為與主要非依電性記憶體中之系統韌體不同之版本(較近之版本或較早之版本)。

[0014]提供多數非依電性記憶體而每一非依電性記憶體均儲存系統韌體之個別複本的作法可能會增加一包含多數非依電性記憶體之電腦系統之製造費用。某些情況下，一供一電腦系統用之製造程序期間，在主要非依電性記憶體安置於電腦系統內之前，主要非依電性記憶體可以系統韌體及關連之系統資料預先程式化。假設輔助非依電性記憶體亦需受到相同之預先程式化程序，則一額外步驟將增加至製造程序中，而此舉會增加關聯於電腦系統之製造費

用。

[0015]依據某些建置，輔助非依電性記憶體可猶如一空空白部分(該空白部分未包含一系統韌體複本)般安置於電腦系統中，而非在「輔助非依電性記憶體安置於電腦系統中」之前即預先程式化該輔助非依電性記憶體。例如，輔助非依電性記憶體可安裝至電腦系統之一電路板上而並未先行程式化該輔助非依電性記憶體。輔助非依電性記憶體之安裝可藉由將輔助非依電性記憶體焊接至電路板，或藉由某些其他之附接技術而完成。

[0016]在第一次開啓包含輔助非依電性記憶體及連接至該輔助非依電性記憶體之一嵌入式控制器之電路板的電源時，一配設步驟可加以執行以程式化該輔助非依電性記憶體。電路板之第一次開啓電源可指在製造期間電路板第一次開啓電源。更一般性地，配設步驟可回應一電腦系統之啓動而執行。啓動電腦系統可指回應開啓電源、系統重設、等而啓動電腦系統，或自一關閉狀態而初始化電腦系統。

[0017]如圖1所示，一配設步驟在某些建置中可藉由嵌入式控制器，以及更特定地，藉由嵌入式控制器可執行之控制器碼加以執行。嵌入式控制器碼可由主要非依電性記憶體載入，其中前述載入可藉由一初始載入器執行而該初始載入器可在執行控制器碼之前先檢查該控制器碼之有效性。

[0018]回應電腦系統之啓動，配設程序檢查(作業步驟

102)以確保輔助非依電性記憶體係未初始化。假設(1)輔助非依電性記憶體先前並未程式化，或(2)輔助非依電性記憶體先前曾初始化但後來已被抹除，則輔助非依電性記憶體可為未初始化。

[0019]嵌入式控制器可以幾種不同方式之一來判定輔助非依電性記憶體係未完成初始化。例如，輔助非依電性記憶體可包含一特定區域，以及一散列、核對和、或其他數值可依據該特定區域中之內容而計算。某些實例中，特定區域係一策略倉庫以用來儲存策略資訊(下文將進一步討論)。替代性實例中，特定區域可為輔助非依電性記憶體中之另一區域。假設輔助非依電性記憶體先前已完成程式化，則此特定區域將包含有效內容以及一儲存之散列、核對和、或其他數值。假設計算之散列、核對和、或其他數值匹配於儲存之散列、核對和、或其他數值，則對嵌入式控制器而言即為輔助非依電性記憶體先前已完成儲存之一項指示。另一方面，假設未匹配，則即為輔助非依電性記憶體係未初始化之一項指示。

[0020]替代地，或額外地，檢查(作業步驟102)包含在輔助非依電性記憶體中之一特定位置處尋找一簽名(例如，一特定已知數值或一標記)。假設該簽名出現在特定位置，則即為輔助非依電性記憶體已完成初始化之一項指示。然而，假設該簽名未出現在特定位置，則即為輔助非依電性記憶體係未初始化之一項指示。

[0021]回應判定(作業步驟104)輔助非依電性記憶體係

未初始化，嵌入式控制器即初始化(作業步驟106)輔助非依電性記憶體，其中初始化包含將系統韌體(以及嵌入式控制器之控制器碼)由主要非依電性記憶體複製至輔助非依電性記憶體。然而，假設嵌入式控制器判定(作業步驟104)輔助非依電性記憶體係初始化，則繞過作業步驟106。

[0022]注意，嵌入式控制器在其他情況下，諸如當嵌入式控制器檢測到主要與輔助非依電性記憶體中之系統韌體版本不同時，可將系統韌體由主要非依電性記憶體複製至輔助非依電性記憶體。

[0023]作為作業步驟106之初始化之部分，配設步驟亦可將一簽名寫入至輔助非依電性記憶體中之一特定位置以指示輔助非依電性記憶體已完成初始化。某些實例中，簽名之寫入可為作業步驟106之初始化之一最後步驟。

[0024]此外，配設步驟可產生策略倉庫而該策略倉庫將策略資訊儲存至輔助非依電性記憶體中，以及初始化一稽核資料結構(例如，稽核日誌)。策略資訊可關於與EC韌體執行有關之策略。例如，至少策略之一可有關當檢測到系統韌體已受到危害時之系統韌體之修復。另一例示性策略可指明是否一積極作業模式即將使用，其中積極模式在每次處理器將執行系統韌體之一啟動塊之情況下可促成系統韌體之驗證(以檢查是否系統韌體已受到危害)。另一例示性策略指明是否一手動或自動回復模式即將使用，其中一手動回復模式包含容許執行一受危害系統韌體之回復前之一使用者動作。又一例示性策略指示是否一鎖定或未鎖

定模式即將使用，其中鎖定模式導致系統韌體鎖定至一特定版本，諸如輔助非依電性記憶體中之版本。

[0025]某些建置中，配設步驟可初始化策略資訊以預設數值。

[0026]稽核日誌可儲存有關EC韌體事件之紀錄。稽核日誌之初始化係準備稽核日誌以接受有關EC韌體事件之資訊。

[0027]圖1之配設步驟可在電腦系統之製造程序期間，諸如在一工廠處，執行。配設步驟可在一包含輔助非依電性記憶體之電路板首先插入至電腦系統內之後執行，其中該輔助非依電性記憶體在此階段係空白者。藉著在製造程序期間執行配設步驟，可確保電腦系統係處於一安全環境因此輔助非依電性記憶體之內容的配設可以一安全方式執行。

[0028]圖2係一例示性電腦系統200之一方塊圖而該電腦系統包含一嵌入式控制器202、一主要非依電性記憶體204、一處理器206、以及一輔助非依電性記憶體216。主要非依電性記憶體204係一共用式非依電性記憶體而該主要非依電性記憶體可藉由多數實體，包含嵌入式控制器202以及至少一其他實體(包含處理器206)，存取。輔助非依電性記憶體216係藉由嵌入式控制器202存取，但無法由處理器206或電腦系統200中之其他組件存取(有效地，輔助非依電性記憶體216係與嵌入式控制器202以外的實體電性式隔離)。使輔助非依電性記憶體216無法由處理器206

以及其他組件存取係保護輔助非依電性記憶體216之內容免受未經授權之竄改。輔助非依電性記憶體216可一直藉由嵌入式控制器202存取。

[0029]雖然並未顯示於圖1中，然而一輸入/輸出(I/O)控制器可設於處理器206與主要非依電性記憶體204之間。

[0030]輔助非依電性記憶體216可與主要非依電性記憶體204實質地分離(諸如以不同之實體記憶體裝置執行)。替代地，輔助非依電性記憶體216以及主要非依電性記憶體204可實質地駐留在一共用記憶體裝置上，但主要非依電性記憶體204以及輔助非依電性記憶體216係在實體記憶體裝置之不同區段內，其中包含輔助非依電性記憶體216之實體記憶體裝置之區段係僅藉由嵌入式控制器202存取。換言之，包含輔助非依電性記憶體216之區段係在嵌入式控制器202之專有控制之下，以及此區段係鎖定而無法藉由處理器206或另一實體存取。

[0031]主要非依電性記憶體204係藉著嵌入式控制器202或藉著另一實體而經由一共用式匯流排220存取。某些建置中，任何既定時間僅有單一實體可存取共用式匯流排220，因此每一次僅有單一實體可存取主要非依電性記憶體204。某些實例中，共用式匯流排220係一共用式串列週邊介面(SPI)匯流排。一SPI匯流排係一同步串列資料鏈接其中SPI匯流排上之裝置係以一主從模式運作。其他實例中，可使用另一型式之共用式匯流排。替代實例中，可提供一仲裁機制以容許，在電腦系統之各種狀態中包含一低

電力狀態以及一正常運行時間狀態，匯流排220之共用式存取。

[0032] 主要非依電性記憶體204可儲存系統韌體207，而系統韌體207可包含BIOS碼。系統韌體(BIOS碼)207可包含EC韌體208而該EC韌體208係藉由嵌入式控制器202執行，以及一啟動塊210而該啟動塊210係藉由處理器206執行。

[0033] 依據圖2之實例中，EC韌體208係內含於系統韌體207之啟動塊210內。將EC韌體208內含於啟動塊210內側可提供一項指示而該項指示係EC韌體208已由提供系統韌體207之實體簽名，而該實體可為電腦系統200之供應商，或另一實體。其他實例中，EC韌體208可與啟動塊210分離。

[0034] 啟動塊210係BIOS碼之一部分，以及當電腦系統200啟動時係首先加以執行。啟動塊210在BIOS碼之其餘部分受允許在處理器206上執行之前即首先加以執行。啟動塊210可用以檢查BIOS碼之完整性以及執行其他初始功能。假設啟動塊210確認BIOS碼之完整性，則啟動塊210可將控制傳送至BIOS碼之主要部分俾初始化關聯於BIOS碼之其餘作業。

[0035] 某些建置中，啟動塊210可包含測量用核心信賴根(CRTM)邏輯，該邏輯係由一產業標準工作組群之信賴電腦運算組群(TCG)所指定之邏輯。電腦系統200之一電源開啓步驟期間，CRTM邏輯可執行特定初始化作業以及可

進行一些測量而該等測量可儲存供稍後使用。接著CRTM邏輯可在將控制傳送給BIOS碼之主要部分之前先行檢查BIOS碼。一旦BIOS碼完成執行以及將控制傳送至OS時，OS可依據CRTM邏輯所進行之測量來驗證電腦系統200之可信賴性。

[0036] 嵌入式控制器202係與電腦系統200之處理器206實質地分離。處理器206係用以執行OS、應用程式碼、以及電腦系統200中其他之碼。另一方面，嵌入式控制器202可用以執行程式化至EC韌體208內之特定預先界定之作業。可藉著嵌入式控制器202執行之作業實例包含下列任何一種或某種組合：電腦系統200中之電源控制(用以控制一電源供應器而該電源供應器係供應電源電壓至電腦系統200中之各種組件)、充電及控制電腦系統200中之一電池、溫度監控(以監控電腦系統200中之一溫度)、風扇控制(以控制電腦系統200中之一風扇)、以及與一使用者輸入裝置交互作用(諸如執行電腦系統200之一鍵盤之一掃描或與一指標裝置諸如一滑鼠、觸控板、觸控螢幕、等交互作用)。嵌入式控制器202可以一微控器、一特定應用積體電路(ASIC)、一可程式閘列(PGA)、或任何其他型式之可程式電路執行。

[0037] 輔助非依電性記憶體216儲存一系統韌體冗餘複本214，其中系統韌體冗餘複本214包含一啟動塊232以及一EC韌體230。輔助非依電性記憶體216中之系統韌體冗餘複本214可為主要非依電性記憶體204中之系統韌體207之

一複本。替代地，系統韌體冗餘複本214可為一與系統韌體207不同之版本(較近版本或較早版本)。

[0038]某些建置中，系統韌體冗餘複本214僅包含啟動塊232，但未包含BIOS碼之主要部分。其他建置中，系統韌體冗餘複本214可包含BIOS碼之全部。進一步實例中，輔助非依電性記憶體216亦可儲存其他碼，諸如作業系統或應用程式碼、處理器206之碼 等。

[0039]某些建置中，製造程序期間之某個時點或在一不同時間，嵌入式控制器202可接收來自系統韌體207之命令 (在處理器206上執行)而該等命令觸發輔助非依電性記憶體之額外配設。例如，來自系統韌體207之命令可指示嵌入式控制器202以藉著將系統資料240複製至輔助非依電性記憶體216而將系統資料240由主要非依電性記憶體204交託給輔助非依電性記憶體216，俾儲存作為一系統資料複本242。系統資料240可包含機器唯一資料，而該機器唯一資料可指對每一特定電腦系統為唯一之任何組態資料或設定值。機器唯一資料之實例可包含下列任何一種或某一組合：產品名稱、產品型號、庫存保持單元(SKU)號碼(用以辨識銷售之個別電腦系統)、電腦系統之一序號、一系統或商品追蹤號碼(用以辨識電腦系統之一系統板)、一系統組態辨識碼(用以辨識電腦系統之一組態)、保證資料(用以說明關聯於電腦系統之一保證)、一通用式唯一辨識碼(UUID)、一BIOS碼之預設設定 等。前述說明係提供作為機器唯一資料之實例；其他實例中，可提供其他或額外

型式之機器唯一資料。

[0040]某些實例中，當系統資料複本242保存至輔助非依電性記憶體216時，嵌入式控制器202可依據系統資料240之內容而計算一散列、核對和、或其他數值。此散列、核對和、或其他數值可保存至輔助非依電性記憶體216以及關聯於系統資料複本242。

[0041]系統韌體207更可提供其他指令而該等指令可導致嵌入式控制器202自主要非依電性記憶體204讀取更多系統資料，以及將此更多系統資料保存至輔助非依電性記憶體216。

[0042]此更多系統資料可包含，舉例而言，電腦系統200之一網路控制器之組態資料。網路控制器可用以依據一網路協定，諸如一乙太網路協定(例如，十億位元乙太網路協定或其他型式之乙太網路協定)、或另一型式之協定而經由一網路進行通訊。在網路控制器所支援之網路協定係十億位元乙太網路(GbE)之實例中，網路控制器之組態資料可包含主要非依電性記憶體204之一GbE區域中之資料。GbE區域係一包含網路控制器用之可程式設定值之資料結構而該網路控制器可為電腦系統之部分。可程式設定值在網路控制器所連接之一匯流排上之一匯流排重設信號未判定時係藉由該網路控制器讀取。

[0043]其他實例中，可由主要非依電性記憶體204複製至輔助非依電性記憶體216之更多系統資料額外地包含一描述符號區域。描述符號區域係一包含資訊之資料結構而

該資訊係描述主要非依電性記憶體204之一佈局，以及一輸入/輸出(I/O)控制器，諸如來自Intel公司之平台控制器集線器(PCH)，或另一型式之(I/O)控制器用之組態參數。PCH可包含各種功能，包含面對一圖形子系統之一顯示器介面、面對一系統匯流排之一系統匯流排介面而各種I/O裝置可連接至該系統匯流排、等。I/O控制器在該I/O控制器由重設退出時可讀取描述符號區域中之資料。

[0044]其他實例中，額外或替代之系統資料可由主要非依電性記憶體204複製至輔助非依電性記憶體216。

[0045]藉著將資料由GbE區域及描述符號區域複製至輔助非依電性記憶體216，可產生GbE區域資料及描述符號區域資料之一備援。

[0046]作為將每一GbE區域資料及描述符號區域資料複製至輔助非依電性記憶體216之部分，嵌入式控制器202可分別依據每一GbE區域資料及描述符號區域資料而計算一對應之散列、核對和、或其他數值。此類散列、核對和、或其他數值可保存至關聯於個別之GbE區域資料複本及描述符號區域資料複本之輔助非依電性記憶體216。

[0047]關聯於輔助非依電性記憶體216中之各個部份之系統資料之散列、核對和、或其他數值可稍後用以驗證此種系統資料之內容並未改變，因此輔助非依電性記憶體216中之系統資料之備援複本的完整性可得到驗證。

[0048]輔助非依電性記憶體216更儲存一策略倉庫244以儲存策略資訊，以及稽核日誌246以儲存有關關聯於嵌

入式控制器202之多數事件之事件資料。

[0049]輔助非依電性記憶體216(藉由執行圖1之配設步驟以及複製各種系統資料至輔助非依電性記憶體216)組配之後，嵌入式控制器202可監控輔助非依電性記憶體中所儲存之內容(碼及資料)之完整性以確保該內容未因有毒軟體、一項碼錯誤、或其他原因而受到危害。輔助非依電性記憶體216中之內容之完整性檢查可在每次嵌入式控制器202退出重設、電腦系統之一低電力狀態期間、或擷取碼及系統資料之備援複本以執行一回復作業之任何其他時間加以執行。

[0050]如上所註解者，輔助非依電性記憶體216中可有各種型式之備援系統資料，包含下列之某些或全部：機器唯一資料、GbE區域資料、描述符號區域資料、稽核日誌資料、以及策略倉庫資料。某些實例中，機器唯一資料、GbE區域資料、以及描述符號區域資料係期望在，諸如工廠中或藉由一服務設施，完成輔助非依電性記憶體216之配設後，於電腦系統200中保持靜態。假設即將使用輔助非依電性記憶體216中任何前述部分之系統資料，諸如回復主要非依電性記憶體204中個別受危害之系統資料，時，則圖3中所描述之一程序可加以執行。

[0051]圖3之程序中，嵌入式控制器202可驗證(作業步驟302)即將使用之輔助非依電性記憶體216中之每一部分之系統資料之完整性。

[0052]為驗證輔助非依電性記憶體216中所儲存之每一

前述部分之資料之完整性，嵌入式控制器202可以個別部分之系統資料計算一散列或其他數值，以及將計算之散列或其他數值與輔助非依電性記憶體中所儲存之散列或其他數值作比較。一匹配係指示個別部分之系統資料係有效的。一非匹配係指示個別部分之系統資料已改變，而此情況係該個別部分之系統資料受到危害之一項指示。

[0053] 稽核日誌246之完整性之驗證可包含驗證稽核日誌之實體結構係正確的以及準備接收稽核日誌事件。為驗證策略倉庫中之策略資訊之完整性，嵌入式控制器202可在每次策略資訊更新時將策略倉庫之一測量值儲存至輔助非依電性記憶體216中。該測量值之型式依據策略倉庫中所儲存之策略資訊可為一散列、核對和、或其他數值。嵌入式控制器202可計算該測量值以及確認該測量值匹配於策略倉庫測量值以驗證策略倉庫之完整性。假設未匹配時，即為策略倉庫244已受危害之一項指示。

[0054] 嵌入式控制器202判定(作業步驟304)是否部分之系統資料之完整性已完成驗證。假設如此，則圖3之程序結束。然而，假設該部分之系統資料之完整性未完成驗證，則進一步之處理可視該部分之系統資料之型態而定(如作業步驟306判定)。某些建置中，係假設機器唯一資料、GbE區域資料、以及描述符號區域資料將在一安全環境諸如一工廠或一服務設施中加以擷取。因此，某些實例中，輔助非依電性記憶體216中之此類型式之系統資料在現場是無法回復的。一旦遭遇到一資料完整性問題，嵌入

式控制器202可設定(作業步驟308)一對應狀態指示器以指示個別部分之系統資料係無效的。例如，每一個機器唯一資料、GbE區域資料、以及描述符號區域資料均可關聯於一個別狀態指示器而該個別狀態指示器可設定為一第一數值以指示個別系統資料係無效的。假設對應狀態指示器設定為一第二數值，則指示該個別系統資料係有效的。

[0055]當一個別部分之系統資料用之狀態指示器設定為第一數值以指示該個別部分之系統資料係無效者時，自該狀態指示器設定為該第一數值時起，嵌入式控制器202將停止執行該個別部分之系統資料之一完整性檢查。此外，當設定該狀態指示器為該第一數值時，嵌入式控制器202可增加(作業步驟310)一個別事件至稽核日誌以指示一錯誤已經發生。

[0056]狀態指示器，當設定為第一數值時，係通知系統韌體207該輔助非依電性記憶體216中之個別部分之系統資料(例如，機器唯一資料、GbE區域資料、或描述符號區域資料)之複本將不會用以回復主要非依電性記憶體204中之個別部分之系統資料。因此，對應於無效部分之系統資料之個別特徵可為失效(或不宜用)者。例如，機器唯一資料、GbE區域資料、以及描述符號區域資料之使用可為不宜用者。

[0057]為修改關聯於狀態指示器(而該狀態指示器係指示部分之系統資料為無效者)之個別部分之系統資料，電腦系統200可置放於一製造程式化模式內以補救該問題，

如下文將進一步討論者。注意製造程式化模式係一可在一工廠處或一服務設施處進入之模式，而且並非在一使用者場所之現場。

[0058] 假設嵌入式控制器202判定(作業步驟306)輔助非依電性記憶體216中之稽核日誌以如此之方式受到損害使得嵌入式控制器202將不再能夠增加新事件至該稽核日誌時，則嵌入式控制器202可修復(作業步驟312)該稽核日誌之結構。當修復該稽核日誌結構時，嵌入式控制器202可增加(作業步驟)一事件至稽核日誌以指示該稽核日誌之一結構問題已受檢測並修復。

[0059] 假設嵌入式控制器202判定(作業步驟306)資料完整性問題係在輔助非依電性記憶體216中之策略倉庫內，嵌入式控制器202可將策略資訊(例如，可為使用者控制之策略資訊)回復(作業步驟316)為預設數值以及將該等預設數值交託回輔助非依電性記憶體216。此外，有關策略倉庫之輔助非依電性記憶體216中之完整性測量值可加以更新(作業步驟318)。將策略資訊設定為預設數值可包含將一參數EC_MPM(圖2中之252)設定為一失效狀態。EC_MPM參數252係有關製造程式化模式之輔助非依電性記憶體216中所儲存之一數值，以及將於下文中進一步討論。其他實例中，策略資訊之其他參數可設定為預設數值。

[0060] 當策略資訊回復為預設狀態時，嵌入式控制器202可為次一啟動週期設定(作業步驟320)一狀態警示

指示器以指示嵌入式控制器策略已回復為預設數值。一警示訊息可回應受到設定之狀態警示指示器而藉著系統韌體顯示給一使用者。回應此顯示訊息，假設期望不同之設定值，則一使用者可重新組配系統韌體配置中之設定值(例如，BIOS配置)。此外，一事件可增加(作業步驟322)至稽核日誌以指示在策略倉庫中已檢測到一資料完整性問題，以及策略已回復為預設數值。

[0061]如圖2進一步描繪者，一MPM參數250(有關製造程式化模式)係儲存於主要非依電性記憶體204中，以及MPM參數之一複本係儲存於輔助非依電性記憶體216中之策略倉庫內，如同EC_MPM參數252一般。一供EC_MPM 252參數用之預設設定值係一失效之設定值(該失效設定值指示製造程式化模式係失效者)。更普遍地，MPM及EC_MPM參數係儲存於主要及輔助非依電性記憶體中之指示器俾用以轉換為關聯於製造程式化模式之各種狀態。

[0062]一電腦系統可置放於一工廠或服務設施處之一製造程式化模式中。在製造程式化模式中，服務人員可設定或改變主要非依電性記憶體204中之系統韌體內容及系統資料。例如，系統資料(諸如機器唯一資料、GbE區域資料、以及描述符號區域資料)可加以修改。

[0063]某些實例中，當電腦系統200處於製造程式

化模式中時，服務人員，使用一應用程式，可利用一介面，諸如Windows管理儀表(WMI)介面，或其他型式之介面來存取特定系統韌體設定值。製造程式化模式可在執行電腦系統之修復或其他服務之一工廠處或一服務設施處獲得。製造程式化模式中，各種系統資料，諸如機器唯一資料、GbE區域資料、以及描述符號區域資料，可在輔助非依電性記憶體216中清除。此可容許機器唯一資料、GbE區域資料、以及描述符號區域資料之新的備援複本由主要非依電性記憶體204複製，前述複製可加以執行以修復，例如，輔助非依電性記憶體216中之受危害系統資料。

[0064]圖4係一狀態圖以揭示有關製造程式化模式之一狀態機器之各種狀態。一工廠第一啟動狀態402代表當製造電腦系統200時之該工廠處之一狀態。工廠第一啟動狀態402可為電腦系統200在工廠處第一次啟動之該電腦系統200之狀態。工廠第一啟動狀態402至少係依據下列而指示：主要非依電性記憶體204中之MPM參數250(圖2)係處於生效狀態，以及輔助非依電性記憶體216中之EC_MPM參數252係處於失效狀態。

[0065]在主要非依電性記憶體204附接至電腦系統200之電路板之前，主要非依電性記憶體204中之預設狀態MPM參數250係經由外部程式化而設定為生效狀態。藉由嵌入式控制器202執行之輔助非依電性記憶體216之初始化期間，輔助非依電性記憶體216中之

EC_MPM參數252，例如，係配設至失效狀態，以作為圖1中所執行之初始化步驟之部分。

[0066]此外，某些建置中，工廠第一啟動狀態402係藉著下列具有錯誤狀態之指示器而進一步指示：擷取之有效MUD、擷取之有效GbE、以及擷取之有效描述符號。設定為錯誤狀態之此類指示器係指示機器唯一資料、GbE區域資料、以及描述符號區域資料之複本，分別地，未提供給輔助非依電性記憶體216。一旦個別之機器唯一資料、GbE區域資料、以及描述符號區域資料之複本已在輔助非依電性記憶體216中擷取完成，則擷取之有效MUD指示器、擷取之有效GbE指示器、以及擷取之有效描述符號指示器即可設定為正確狀態。

[0067]電腦系統200在工廠處第一次啟動時，系統韌體207可傳送一命令至嵌入式控制器202以將(輔助非依電性記憶體216中之)EC_MPM參數252設定為生效狀態，以導致由狀態402至狀態404之一項轉換。藉由MPM參數250及EC_MPM參數252兩者皆處於生效狀態所代表之狀態404對應於電腦系統200之製造程式化模式。

[0068]在狀態404中之製造程式化模式下，服務人員可依期望修改主要非依電性記憶體204中之系統資料。在某時點時，系統韌體207可退出狀態404之製造程式化模式。系統韌體207藉著將MPM參數250設定為

失效狀態而觸發由製造程式化模式之退出。此舉導致MPM參數250設定為失效狀態，而EC_MPM參數252仍為生效狀態。前述組合觸發由狀態404至狀態406之一項轉換。

[0069]注意假設檢測到至少一種預先界定之情況，則可發生由狀態404回到工廠第一啟動狀態402之一項轉換。舉例言之，該至少一種預先界定之狀況包含：
(1)利用一使用者輸入之一預先界定之關鍵順序使輔助非依電性記憶體216遭到抹除；或(2)策略倉庫244受到危害之一項檢測。

[0070]狀態406中，系統韌體207可傳送一命令至嵌入式控制器202以將機器唯一資料由主要非依電性記憶體204複製至輔助非依電性記憶體216。此外，系統韌體207可傳送一命令至嵌入式控制器202以將EC_MPM參數252設定為失效狀態，而此舉導致由狀態406至狀態408之一項轉換。

[0071]作為由狀態406至狀態408之轉換之部分，系統韌體207導致電腦系統200之一冷啟動之執行。此外，嵌入式控制器202對電腦系統200中之核心邏輯(例如，I/O控制器諸如Intel PCH)主張一重設信號(例如，RSMRST#)以確保嵌入式控制器202存取主要非依電式記憶體204。另，由狀態406至狀態408之轉換中，嵌入式控制器202自主要非依電性記憶體204讀取GbE區域資料及描述符號區域資料以及在輔助非依電性記憶體

216中產生一備援複本。某些實例中，假設輔助非依電性記憶體216中之啓動塊232與主要非依電式記憶體204中之啓動塊210不同時，嵌入式控制器202亦可更新輔助非依電性記憶體216中之啓動塊232之複本。

[0072]注意狀態408，對應於MPM參數250及EC_MPM參數252兩者皆為失效狀態，係現場之電腦系統200藉由一使用者之正常作業之狀態。

[0073]作為進入狀態408之程序之部分，嵌入式控制器202可執行下列程序：確認狀態指示器指示啓動塊232、機器唯一資料、GbE區域資料、以及描述符號區域資料係集結於輔助非依電性記憶體216中。另，嵌入式控制器202可執行如下之散列、核對和、或其他數值之一項比較：確認輔助非依電性記憶體216中之啓動塊232之一散列、核對和、或其他數值匹配主要非依電性記憶體204中之啓動塊210之散列、核對和、或其他數值；確認輔助非依電性記憶體216中之機器唯一資料之散列、核對和、或其他數值匹配主要非依電性記憶體204中之機器唯一資料之散列、核對和、或其他數值；確認輔助非依電性記憶體216中之GbE區域資料之散列、核對和、或其他數值匹配主要非依電性記憶體204中之GbE區域資料之散列、核對和、或其他數值；以及確認輔助非依電性記憶體216中之描述符號區域資料之散列、核對和、或其他數值匹配主要非依電性記憶體204中之描述符號區域資料之散列、核對和、或其他

數值。

[0074]接著，電腦系統200，基於某種理由諸如因爲偵測到電腦系統200受到危害，而可返回工廠或服務設施。在工廠或服務設施處，可由服務人員利用一應用程式以發出一安全命令至系統韌體207以將MPM參數250及EC_MPM參數252之狀態改變爲生效狀態(以導致重新進入製造程式化模式)。安全命令可爲一管理命令而該管理命令係以一加密鍵，諸如一私用鍵加以簽名。系統韌體207可利用一對應加密鍵，諸如一公用鍵或私用鍵來解密該簽名命令。

[0075]某些實例中，簽名命令可利用一可移除式儲存媒介，諸如一通用串列匯流排(USB)儲存媒介或其他型式之儲存媒介，而呈現給電腦系統。某些情況下，係期望在傳送簽名命令之前先將電力自嵌入式控制器202移除，此舉確保在啓動塊210執行之前嵌入式控制器202先驗證該啓動塊210，以及促使接界於嵌入式控制器202之一介面(例如，應用程式之程式化界面或API)生效。

[0076]一旦系統韌體207接受一促使製造程式化模式重新生效之簽名命令，以及回應MPM參數250及EC_MPM參數252兩者皆設定爲生效狀態，狀態機器即由狀態408轉換爲狀態404。在由狀態408至狀態404之轉換中，嵌入式控制器202可抹除特定備援系統資料，包含輔助非依電性記憶體216中之，機器唯一資料、

GbE區域資料、以及描述符號區域資料，以及可將下列指示器設定為錯誤狀態：擷取之有效MUD、擷取之有效GbE、以及擷取之有效描述符號。

[0077]用於重新進入製造程式化模式之另一機制(並非上文討論之傳送簽名命令)係執行其上安裝有主要非依電性記憶體204之電路板之一實體重工。某些實例中，主要非依電性記憶體204可自電路板實質移除以及離線式程式化至一預設系統韌體影像處，其中MPM參數250係設定為生效狀態。

[0078]一旦重新程式化之主要非依電性記憶體204放置回電腦系統200內時，系統韌體207即檢測到MPM參數250具有生效狀態，以及EC_MPM參數252具有失效狀態。此導致由狀態408至狀態410之一項轉換。當進入因主要非依電性記憶體204之重工所發生之製造程式化模式時，系統韌體207可檢查以確保系統韌體(包含啟動塊)已對現行啟動期間完成驗證。此舉可以檢查一關聯於系統韌體207之指示器為依據。假設系統韌體207未對現行啟動期間完成驗證，則系統韌體207可傳送一命令以強制系統韌體207之一項檢查，以及電腦系統200可重新啟動。

[0079]當由狀態408轉換至狀態410時，系統韌體207可提供(決策菱形塊412)一提示符號俾供服務人員輸入一項輸入。假設所接收之輸入係一特殊預先界定之關鍵順序，則系統韌體207傳送一命令至嵌入式控制器

202以將EC_MPM參數252設定為生效狀態。此舉導致MPM及EC_MPM參數250與252兩者皆設定為生效狀態，而此導致成為狀態404之一項轉換。

[0080]基於特殊預先界定之關鍵順序而由決策菱形塊412至狀態404之轉換中，嵌入式控制器202，在某些實例中，可清除下列已備援至輔助非依電性記憶體216之系統資料：機器唯一資料、GbE區域資料、以及描述符號區域資料。

[0081]然而，假設回應決策菱形塊412所呈現之提示符號而未接收到一特殊預先界定之關鍵順序時，則系統韌體207將MPM參數250設定為失效狀態，以導致由決策菱形塊412至狀態408之一項轉換。在此轉換中，輔助非依電性記憶體216中之內容仍然未改變以及假設主要與輔助複本之間有任何差異時，藉著以輔助非依電性記憶體216中之對應系統資料替換主要非依電性記憶體204中之個別系統資料，系統韌體207或EC韌體208可將機器唯一資料、GbE區域資料、以及描述符號區域資料由輔助非依電性記憶體216重新儲存至主要非依電性記憶體204。

[0082]藉著使用依據某些建置之技術及機制，一具有主要及輔助非依電性記憶體之電腦系統之一製造程序可藉著在輔助非依電性記憶體安裝至一裝設於該電腦系統中之電路板上之前無需先行程式化該輔助非依電性記憶體而得到簡化。另，萬一關聯於功能之資料

變成受危害時，各種功能可個別地受到否決。此外，技術或機制係提供用以容許進入一製造程式化模式而容許清除或回復輔助非依電性記憶體之內容。

[0083]上述各種模組之機器可讀取式指令係載入以供在一處理電路(例如，嵌入式控制器202或處理器206)上執行。一處理電路可包含一微處理器、微控制器、處理器模組或子系統、可程式積體電路、可程式開列、或另一控制或電腦裝置。

[0084]資料及指令係儲存於個別儲存裝置內，而該等儲存裝置係建置為一或多個電腦可讀取式或機器可讀取式儲存媒介。儲存媒介包含不同型式之記憶體而該等不同型式之記憶體包含半導體記憶體裝置諸如動態或靜態隨機存取記憶體(DRAMs或SRAMs)、可抹除及可程式唯讀記憶體(EPROMs)、電子式可抹除及可程式唯讀記憶體(EEPROMs)及快閃記憶體；磁碟諸如固定式、軟式及可移除式碟片；其他磁性媒介包含磁帶；光學媒介諸如緊密碟片(CDs)或數位視訊碟片(DVDs)；或其他形式之儲存裝置。注意上文討論之指令可提供至單一電腦可讀取式或機器可讀取式儲存媒介上，或替代地，可提供至一可能具有多數節點之大型系統中所分佈之多數電腦可讀取式或機器可讀取式儲存媒介上。此類電腦可讀取式或機器可讀取式單一儲存媒介或多數儲存媒介係視為一物品(或製造品)之部

分。一物品或製造品可指任何製成之單一組件或多數組件。儲存單一媒介或多數媒介可安置於運行機器可讀取式指令之機器中，或安置於一遠端場所處而機器可讀取式指令可經由一網路而自該遠端場所下載以供執行之用。

[0085]前述說明中，各種細節均加以陳述以提供對此處所揭示主題之一項理解。然而，建置可加以實踐而無需此類細節之某些或全部。其他建置可包含來自上文所討論細節之修改及變化。隨附請求項有意涵蓋此類修改及變化。

【符號說明】

102-106...作業步驟	230...EC韌體
200...電腦系統	232...啟動塊
202...嵌入式控制器	240...系統資料
204...主要非依電性記憶體	242...系統資料複本
206...處理器	244...策略倉庫
207...系統韌體	246...稽核日誌
208...EC韌體	250...MPM參數
210...啟動塊	252...EC_MPM參數
214...系統韌體冗餘複本	302-322...作業步驟
216...輔助非依電性記憶體	402-410...狀態
220...匯流排	412...決策菱形塊

申請專利範圍

1. 一種組配系統之方法，包含：

回應於啓動包含有包括系統啓動碼之一第一非依電性記憶體以及一第二非依電性記憶體之一系統，藉由一控制器執行該第二非依電性記憶體之配設，該配設包含：

檢查該第二非依電性記憶體係未初始化，以及
回應於判定該第二非依電性記憶體係未初始化，將該系統啓動碼由該第一非依電性記憶體複製至該第二非依電性記憶體。

2. 如請求項1之方法，其中該配設更包含在該第二非依電性記憶體中產生一策略倉庫，該策略倉庫儲存有關相關於該控制器之執行之至少一策略之資訊。
3. 如請求項2之方法，其中該至少一策略係有關當檢測到該系統啓動碼受到危害時更新該系統啓動碼，或檢查該系統啓動碼是否受到危害。
4. 如請求項1之方法，其中該配設更包含初始化該第二非依電性記憶體中之一稽核資料結構，該稽核資料結構係接收有關該控制器之事件之資訊。
5. 如請求項1之方法，其中執行該配設係回應於在製造該系統之一工廠處檢測到包含該控制器及該第二非依電性記憶體之一電路板之一第一次電源開啓。
6. 如請求項1之方法，更包含：

在一工廠處或在一服務設施處之一程式化程序期間，藉由該控制器接收來自該系統啟動碼之一命令；以及

回應於該命令，擷取來自該第一非依電性記憶體之系統資料以及將該系統資料複製至該第二非依電性記憶體。

7. 如請求項6之方法，其中該系統包含多數型式之系統資料，該方法更包含：

檢測到該等多數型式之系統資料之一者受到危害；以及

為該系統資料之受到危害的型式設定一指示符，以指示所檢測到之危害。

8. 如請求項7之方法，其中該等多數型式之系統資料係由以下所組成之組群中選出：包含該系統唯一之組態資料之機器唯一資料、一網路控制器之組態資料、以及說明該第一非依電性記憶體之一佈局之資料。

9. 一種系統，包含：

一處理器；

一控制器；

一第一非依電性記憶體係儲存有關該系統之一程式化模式之一第一指示符；

一第二非依電性記憶體係連接至該控制器以及係儲存有關該程式化模式之一第二指示符；以及

系統啟動碼係可在該處理器上執行以判定是否該

系統將依據該第一及第二指示符之數值進入該程式化模式，其中該系統啓動碼在該系統處於該程式化模式時係可組配者。

10. 如請求項9之系統，其中該第二非依電性記憶體可由該控制器存取但與該處理器電性式隔離，其中該第一非依電性記憶體可藉由該控制器及該處理器兩者存取，以及其中該系統啓動碼可執行以進一步：

回應於判定該系統將進入該程式化模式，傳送一命令至該控制器以使該控制器將該第二指示符由一第一數值改變為一第二數值。

11. 如請求項9之系統，其中該第一及第二指示符之該等數值之不同組合導致轉換為不同狀態，其中該等轉換包含由一工廠第一啓動狀態至對應於該程式化模式之一狀態之一轉換。

12. 如請求項11之系統，其中該等轉換更包含由對應於該程式化模式之該狀態至另一狀態之一轉換，以退出該程式化模式。

13. 如請求項12之系統，其中該等轉換更包含由該另一狀態回到對應於該程式化模式之該狀態之一轉換。

14. 一種物品，包含儲存指令之至少一機器可讀取式儲存媒介，該等指令於執行時使一系統：

回應於啓動包含有包括系統啓動碼之一第一非依電性記憶體以及一第二非依電性記憶體之該系統，藉由該系統之一控制器執行該第二非依電性記憶體之配

設，該配設包含；

檢查該第二非依電性記憶體係未初始化，以及
回應於判定該第二非依電性記憶體係未初始化，將該系統啟動碼由該第一非依電性記憶體複製至該第二非依電性記憶體，以及將有關該系統之組態以及該系統之至少一組件之組態之系統資料由該第一非依電性記憶體複製至該第二非依電性記憶體。

15. 如請求項14之物品，其中該第二非依電性記憶體可藉由該控制器存取但無法藉由該系統之一處理器存取，以及其中該第一非依電性記憶體係由該控制器及該處理器共用以及可藉由該控制器及該處理器存取。

圖式

1 / 4

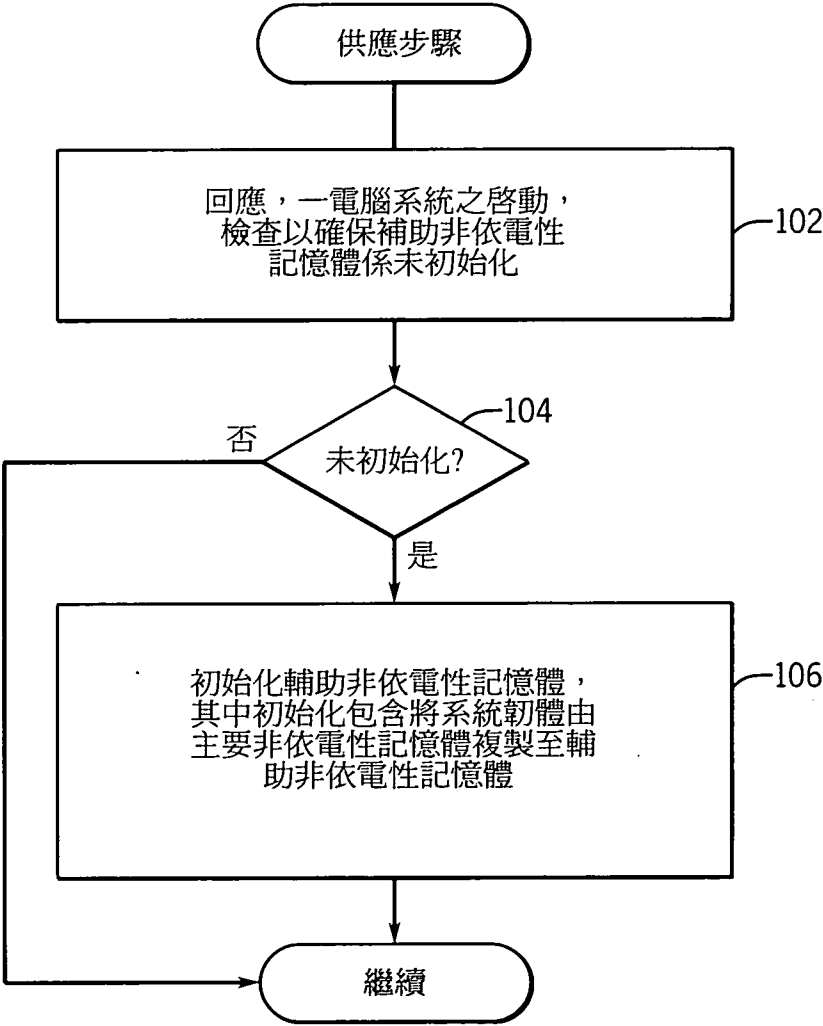


圖1

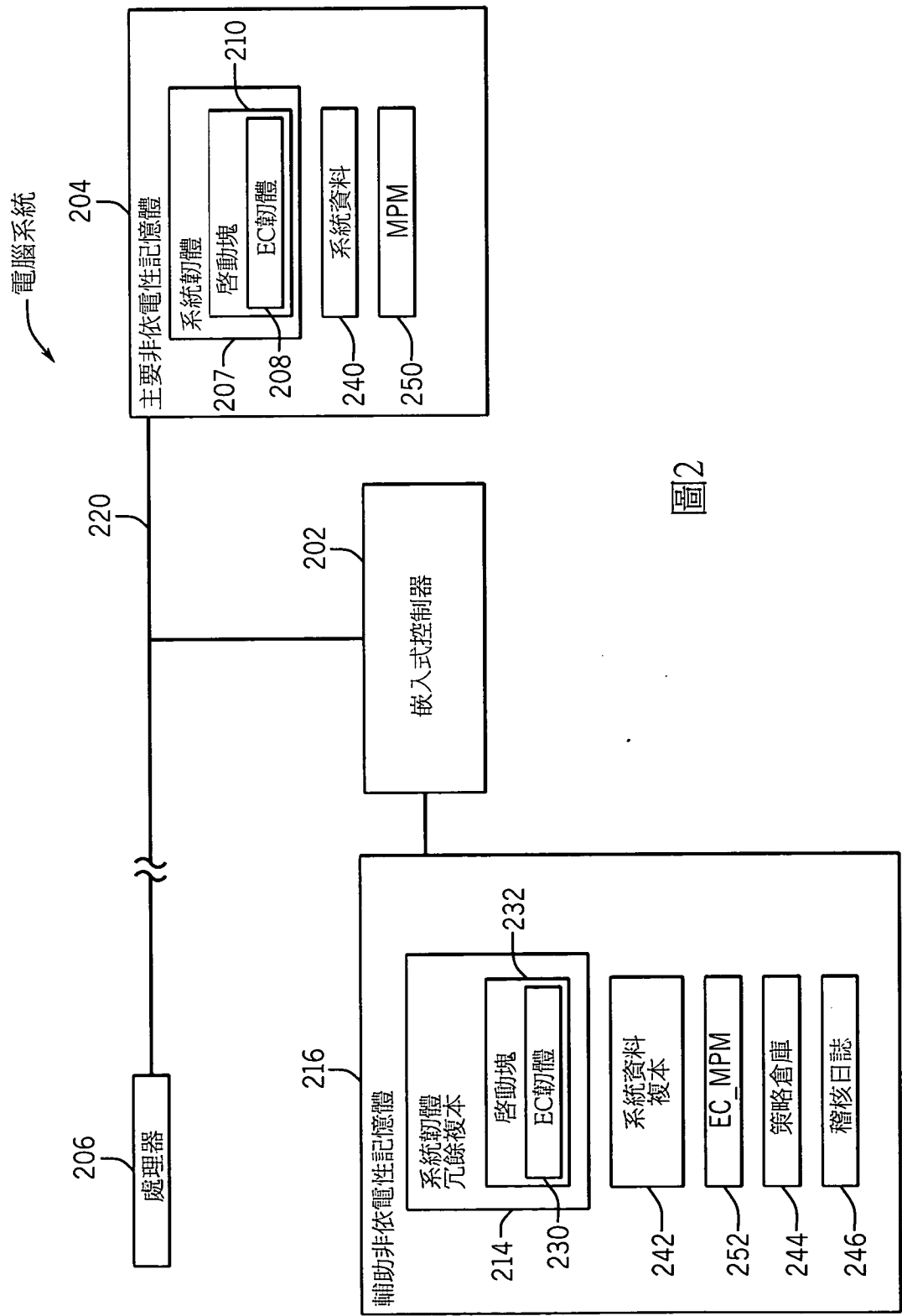


圖2

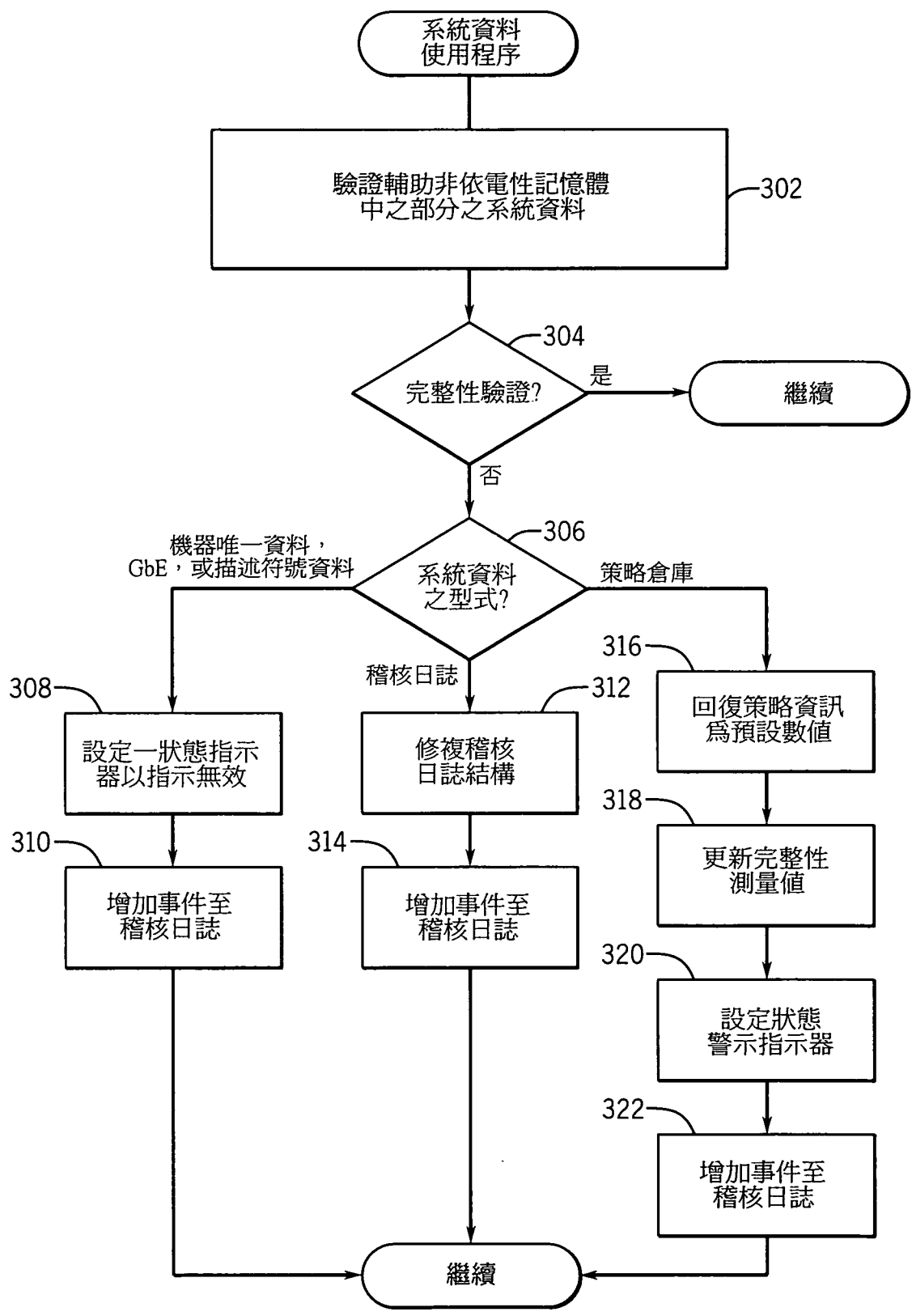


圖3

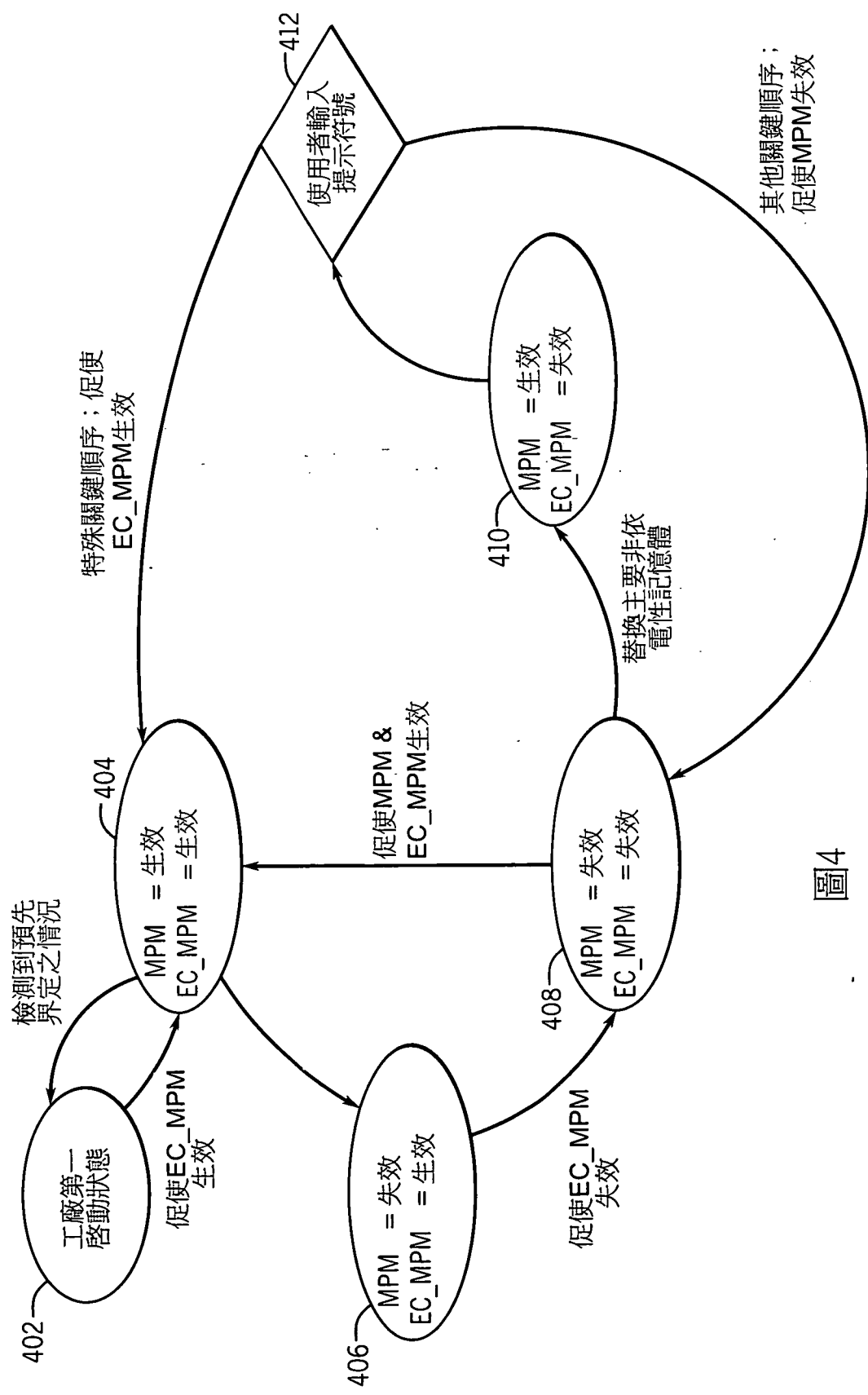


圖4