



(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 201324155 A1

(43)公開日：中華民國 102 (2013) 年 06 月 16 日

(21)申請案號：100145324

(22)申請日：中華民國 100 (2011) 年 12 月 08 日

(51)Int. Cl. : **G06F12/16 (2006.01)**

(71)申請人：聯陽半導體股份有限公司 (中華民國) ITE TECH. INC. (TW)

新竹市新竹科學工業園區創新一路 13 號 3 樓

(72)發明人：周家源 CHOU, CHIA YUAN (TW)；侯慶敏 HOU, CHING MIN (TW)

(74)代理人：詹銘文

申請實體審查：有 申請專利範圍項數：10 項 圖式數：4 共 18 頁

(54)名稱

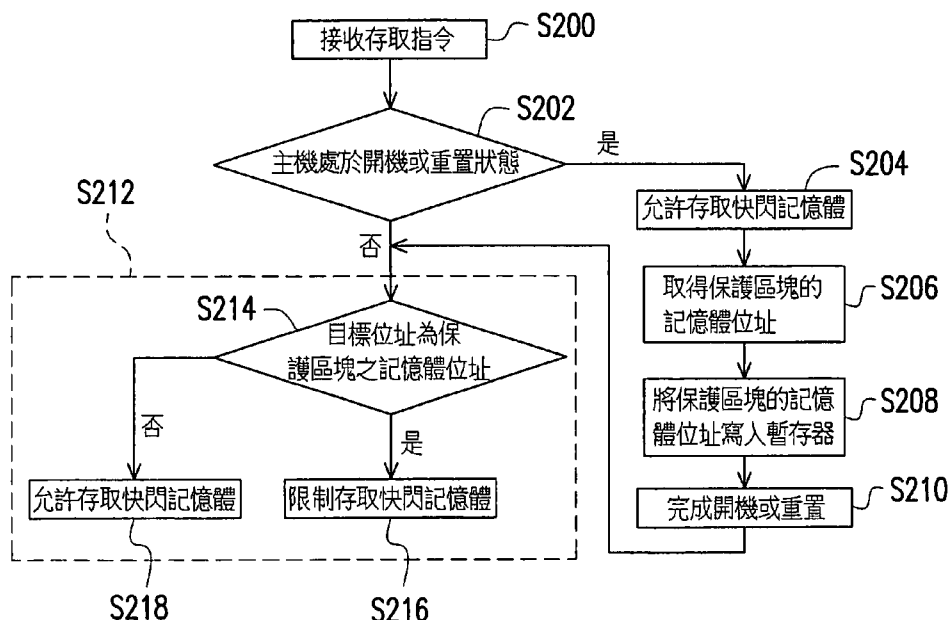
快閃記憶體儲存系統及其資料保護方法

FLASH MEMORY STORAGE SYSTEM AND DATA PROTECTION METHOD THEREOF

(57)摘要

一種快閃記憶體儲存系統，包括快閃記憶體、主機以及控制器。控制器耦接主機與快閃記憶體，依據主機的狀態，限制主機存取快閃記憶體。其中當主機處於開機或重置狀態時，控制器允許主機存取快閃記憶體，當主機完成開機或重置動作後，控制器限制主機存取快閃記憶體，以保護快閃記憶體所儲存的資料。另外，本發明也提出了一個應用於上述儲存系統的資料保護方法。

S200~S218：資料保護方法的步驟



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：100/45324

※申請日：100.12.08

※IPC 分類：

G06F 12/16 2006.01

一、發明名稱：(中文/英文)

快閃記憶體儲存系統及其資料保護方法 / FLASH
MEMORY STORAGE SYSTEM AND DATA
PROTECTION METHOD THEREOF

二、中文發明摘要：

一種快閃記憶體儲存系統，包括快閃記憶體、主機以及控制器。控制器耦接主機與快閃記憶體，依據主機的狀態，限制主機存取快閃記憶體。其中當主機處於開機或重置狀態時，控制器允許主機存取快閃記憶體，當主機完成開機或重置動作後，控制器限制主機存取快閃記憶體，以保護快閃記憶體所儲存的資料。另外，本發明也提出了一個應用於上述儲存系統的資料保護方法。

三、英文發明摘要：

A flash memory storage system includes a flash memory, a computer and a controller. Controller couple to the computer and the flash memory, and restricts the computer to access the flash memory according to the status of the computer. When the computer is booting or resetting, the controller allow the

computer access the flash memory. After the computer completes the boot or reset procedure, controller restricts the computer to access the flash memory in order to protect the data stored by the flash memory. Besides, a data protection method for which applied to the above-mentioned storage system is also provided in the present invention.

四、指定代表圖：

(一) 本案之指定代表圖：圖 2

(二) 本代表圖之元件符號簡單說明：

S200~S218：資料保護方法的步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

computer access the flash memory. After the computer completes the boot or reset procedure, controller restricts the computer to access the flash memory in order to protect the data stored by the flash memory. Besides, a data protection method for which applied to the above-mentioned storage system is also provided in the present invention.

四、指定代表圖：

(一) 本案之指定代表圖：圖 2

(二) 本代表圖之元件符號簡單說明：

S200~S218：資料保護方法的步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種儲存系統及其資料保護方法，且特別是有關於一種避免快閃記憶體的资料被惡意存取的保護方法以及包含此方法的快閃記憶體儲存系統。

【先前技術】

在一般的電腦系統中，系統藉由執行儲存於快閃記憶體(flash memory)中的基本輸入輸出系統(Basic Input and Output System, BIOS)程式進行開機程序，並載入作業系統。在開機程序完成之後，電腦系統的控制權便交由作業系統所控制並完成開機狀態，亦即進入一般使用者所可以控制的狀態，使用者可以對電腦系統進行指令的輸入與系統資料的存取。

在開機完成之後，使用者便可以以下指令至控制器以讀取或寫入快閃記憶體內的資料。然而，一旦有使用者想要經由控制器對快閃記憶體內的重要資料(如 BIOS)做惡意的修改、竊取或是破壞，在一般的電腦系統中卻是無法加以防範的。因此，如何保護快閃記憶體中所儲存的資料，便是一個相當重要的問題。

【發明內容】

本發明提供一種快閃記憶體儲存系統，其可限制主機在開機完成後存取快閃記憶體內之特定資料，防止特定資

料遭到惡意的篡改或破壞。

本發明提供一種資料保護方法，其可針對特定資料的記憶體位址進行保護，使其在開機程序完成後無法被讀取或寫入。

本發明提出一種快閃記憶體儲存系統，包括快閃記憶體、主機以及控制器。控制器耦接主機與快閃記憶體，依據主機的狀態，限制主機存取快閃記憶體。其中當主機處於開機或重置狀態時，控制器允許主機存取快閃記憶體，當主機完成開機或重置動作後，控制器限制主機存取快閃記憶體。

在本發明之一實施例中，快閃記憶體儲存系統更包括開關。開關耦接於主電源與主機之間，控制器更依據暫停電源而導通開關，以將主電源提供至主機。

在本發明之一實施例中，當控制器被關閉時，控制器斷開快閃記憶體儲存系統的開關，以停止供應主電源至主機。

在本發明之一實施例中，當主機受控於重置訊號而處於重置狀態時，控制器依據重置訊號而允許主機存取快閃記憶體。

在本發明之一實施例中，快閃記憶體儲存系統更包括時脈產生器。時脈產生器耦接主機，提供主機運作所依據之時脈訊號，當控制器被關閉時，時脈產生器停止供給時脈訊號至主機。

在本發明之一實施例中，控制器包括至少一暫存器。

暫存器儲存快閃記憶體之保護區塊的記憶體位址，控制器更自快閃記憶體取得保護區塊的記憶體位址，並將保護區塊的記憶體位址寫入暫存器。

在本發明之一實施例中，控制器更判斷主機欲存取的目標記憶體位址是否為保護區塊的記憶體位址，若為保護區塊的記憶體位址則拒絕主機存取目標記憶體位址。

本發明提出一種快閃記憶體儲存系統的資料保護方法，其中快閃記憶體儲存系統包括主機以及快閃記憶體，資料保護方法包括下列步驟：判斷主機是否處於開機或重置狀態；若主機處於開機或重置狀態，允許主機存取快閃記憶體；以及若主機非處於開機或重置狀態，限制主機存取快閃記憶體。

在本發明之一實施例中，限制主機存取快閃記憶體的步驟更包括以下步驟：判斷主機欲存取的目標記憶體位址是否為保護區塊的記憶體位址；若為保護區塊的記憶體位址，拒絕主機存取目標記憶體位址；以及若非為保護區塊的記憶體位址，則允許主機存取目標記憶體位址。

在本發明之一實施例中，快閃記憶體儲存系統更包括暫存器，主機處於開機或重置狀態時的步驟更包括以下步驟：取得保護區塊的記憶體位址；以及將保護區塊的記憶體位址寫入暫存器。

基於上述，本發明實施例之快閃記憶體儲存系統利用將快閃記憶體內特定資料區域設為保護區塊，使得控制器針對保護區塊的記憶體位址寫入暫存器並進行存取限制。

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如下。

【實施方式】

在本發明之實施例中，提出了多個具有資料保護功能的快閃記憶體儲存系統以及應用於上述快閃記憶體儲存系統的資料保護方法，其不僅可以避免一般使用者無意間存取快閃記憶體內的特定資料造成系統損毀，更可以防止惡意使用者破壞系統或是竊取快閃記憶體內特定資料。詳細的實施方式將完整揭露如下。

圖 1 繪示為本發明一實施例之快閃記憶體儲存系統的示意圖。請參照圖 1，快閃記憶體儲存系統 100 包括快閃記憶體 110、主機 120 以及具有暫存器 140 的控制器 130。本發明的快閃記憶體儲存系統可適用於各種電腦裝置，如桌上型電腦或是筆記型電腦等等。

在快閃記憶體儲存系統 100 中，控制器 130 耦接快閃記憶體 110 與主機 120，以控制主機 120 對快閃記憶體 110 的資料存取，其中快閃記憶體儲存系統 100 可預先定義快閃記憶體 110 中的特定資料存放區域為保護區塊；而主電源 M_P 與暫停電源 S_P 分別耦接於主機 120 與控制器 130 上，並提供其運作所需的電力。在一些實施例中，控制器可為內嵌控制器(Embedded Controller, EC)，快閃記憶體可為 NAND 結構的快閃記憶體，而主機可為南橋晶片(South Bridge Chip)，並且主機 120 可透過低針腳數匯流排(Low

Pin Count Bus, LPC Bus) 與控制器 130 進行指令的傳送，然而本發明並不僅限於此。

當快閃記憶體儲存系統 100 啟動時，主電源 M_P 以及暫停電源 S_P 供給主機 120 以及控制器 130 電源，使系統處於開機狀態。在開機狀態下，主機 120 會發送指令至控制器 130，要求讀取儲存於快閃記憶體 110 中的開機程式(如 BIOS)，以進行開機程序。此時控制器 130 自快閃記憶體 110 取得保護區塊的記憶體位址(如 BIOS 的記憶體位址)，並將保護區塊的記憶體位址寫入暫存器 140。當開機完成後，控制器 130 將快閃記憶體儲存系統 100 的主控權交還給使用者以進行正常使用程序，其中由於保護區塊的記憶體位址已經被控制器 130 寫入暫存器 140 中，控制器 130 將會依據暫存器所儲存的記憶體位址，限制快閃記憶體 110 的存取。舉例來說，在本實施例中，當使用者發出控制訊號 CTL_S 控制主機發出指令要求控制器 130 對快閃記憶體 110 的 BIOS 程式進行存取時，控制器 130 將會判斷此指令所要求存取的記憶體位址為保護區塊的記憶體位址，並且拒絕進行存取。換句話說，當控制器 130 判斷主機 110 欲存取的目標記憶體位址為保護區塊的記憶體位址時，則拒絕主機 120 存取目標記憶體位址。

圖 2 繪示為依據圖 1 實施例之資料保護方法的流程圖。請同時參照圖 1 與圖 2，在快閃記憶體儲存系統 100 接收到一個存取指令時，如步驟 S200。快閃記憶體儲存系統 100 首先在步驟 S202 中判斷主機 120 是否處於開機或

重置狀態，若主機 120 處於開機或重置狀態，則允許主機 120 存取快閃記憶體(步驟 S204)；反之，則限制主機 120 存取該快閃記憶體(步驟 S212)。

進一步來說，主機 120 在步驟 S204 中取得存取快閃記憶體 110 的權限後，便可接著取得快閃記憶體 110 中預設的保護區塊的記憶體位址(步驟 206)，然後再將保護區塊的記憶體位址寫入暫存器 140 中(步驟 S208)。最後，主機 120 完成後續開機或重置程序，如步驟 S210 所示。

在步驟 S210 後，由於主機 120 已完成開機或重置的狀態，因此流程跳至步驟 S212。在步驟 S212 中，控制器 130 判斷所接收的存取指令之目標記憶體位址是否為保護區塊的記憶體位址(步驟 S214)；若是，則拒絕主機 120 存取快閃記憶體 110(步驟 S216)，亦即拒絕存取指令；若否，則允許主機 120 存取快閃記憶體(步驟 S218)，亦即接受存取指令並進行後續存取動作。

在一些特定的情況下，例如惡意使用者使用特定方法關閉控制器 130，並且藉由其他控制手段以規避控制器 130 的保護機制時，系統可能就會出現漏洞。因此本發明提出多個具有系統保護機制的快閃記憶體儲存系統 100 實施例以解決惡意使用者侵入系統衍伸出的問題。

圖 3 繪示為本發明另一實施例之快閃記憶體儲存系統的示意圖。請參照圖 3，快閃記憶體儲存系統 300 與圖 1 實施例之快閃記憶體儲存系統 100 的不同之處在於，快閃記憶體儲存系統 300 加入一個耦接於主電源 M_P 與主機

120 之間的開關 SW，其導通狀態由控制器 130 所控制。

當快閃記憶體儲存系統 300 被啟動時，控制器 130 會先被暫停電源 S_P 開啟，之後控制器 130 才控制開關 SW 導通，使得主機 120 得以被主電源 M_P 啟動以進入開機狀態。接著主機 120 便可向控制器 130 發出讀取快閃記憶體 110 的請求指令，控制器 130 則將預設保護區塊的記憶體位址寫入暫存器 140，並進行後續開機程序，其詳細作動已於圖 1 實施例中描述，因此不再贅述。

在本實施例中，控制器 130 會先被暫停電源 S_P 所啟動，然後控制器 130 才會透過導通開關 SW，使得主電源 M_P 得以啟動主機 120。若控制器 130 被關閉時，則控制器 130 將會使開關 SW 回復至不導通的狀態，使得主機 120 無法啟動。因此一旦控制器 130 被關閉，主機 120 也將關機而快閃記憶體儲存系統 300 將無法再繼續運作，藉由此方式使得快閃記憶體 110 內保護區塊的特定資料能夠在任何時間下皆受到控制器 130 的保護機制所保護。

另外，在主機 120 開機完成後，若使用者欲利用給予主機 120 一個重置訊號 RST_S，以對主機 120 進行重置，控制器 130 此時將依據重置訊號 RST_S 而允許主機 120 存取快閃記憶體 110，以使主機 120 可執行重置程序。在重置狀態中，相似於開機狀態，主機 120 再度將快閃記憶體儲存系統 300 的控制權取回，並透過控制器 130 對快閃記憶體 110 進行 BIOS 的存取，並且如上述的實施例所述，控制器 130 再次將預設保護區塊的記憶體位址寫入暫存器

140 中。

圖 4 繪示為本發明又一實施例之快閃記憶體儲存系統的示意圖。本實施例利用控制器 130 控制時脈產生器 150 的方法以防止控制器 130 被關閉時，無法對快閃記憶體 110 進行保護的情況。

在本實施例之快閃記憶體儲存系統 400 中，時脈產生器 150 耦接主機 120，並提供主機 120 運作所依據之時脈訊號 CLK_S。請參照圖 3，本實施例與圖 1 之實施例的不同之處在於，當控制器 130 被以任何手段關閉時，此時控制器 130 將會使時脈產生器 150 同時停止供給時脈訊號 CLK_S 至主機 120。一旦主機 120 無法接收到時脈訊號 CLK_S，主機 120 將立即關機(shut down)。

更確切地說，當惡意使用者意圖關閉控制器 130 時，控制器 130 會控制時脈產生器 150 停止傳送時脈訊號 CLK_S 至主機 120，主機 120 將無法繼續運行。因此，在本實施例中，一旦控制器 130 被關閉，主機 120 也將關機而快閃記憶體儲存系統 400 將無法再繼續運作，藉由此方式使得快閃記憶體 110 內保護區塊的特定資料能夠在任何時間下皆受到控制器 130 的保護機制所保護。

上述之多個實施例，其相同之處在於一旦控制器 130 被以任何方式關閉時，主機 120 也必將停止運作，因此得以使快閃記憶體儲存系統必定得經由所述之控制器 130 而存取快閃記憶體 110，使得快閃記憶體 110 內的特定資料得以被保護。然而，上述之實施例僅為表示快閃記憶體儲

存系統 100 無法運作在控制器 130 關閉的情況下的數個實施方式，本發明並不以此為限。

綜上所述，本發明實施例之快閃記憶體儲存系統利用將快閃記憶體內特定資料區域設為保護區塊，使得控制器針對保護區塊的記憶體位址寫入暫存器並進行存取限制，其中快閃記憶體儲存系統在本發明之實施例中，只能運作在控制器啟動的狀態下，只要控制器被關閉，主機也會隨之停止運作，因此系統得以在任何操作時間下，皆可受到控制器的存取限制所保護。

雖然本發明已以實施例揭露如上，然其並非用以限定本發明，任何所屬技術領域中具有通常知識者，在不脫離本發明之精神和範圍內，當可作些許之更動與潤飾，故本發明之保護範圍當視後附之申請專利範圍所界定者為準。

【圖式簡單說明】

圖 1 繪示為本發明一實施例之快閃記憶體儲存系統的示意圖。

圖 2 繪示為依據圖 1 實施例之資料保護方法的流程圖。

圖 3 繪示為本發明另一實施例之快閃記憶體儲存系統的示意圖。

圖 4 繪示為本發明又一實施例之快閃記憶體儲存系統的示意圖。

【主要元件符號說明】

100、300、400：快閃記憶體儲存系統

110：快閃記憶體

120：主機

130：控制器

140：暫存器

150：時脈產生器

S200~S218：資料保護方法的步驟

M_P：主電源

S_P：暫停電源

CTL_S：控制訊號

RST_S：重置訊號

CLK_S：時脈訊號

SW：開關

七、申請專利範圍：

1. 一種快閃記憶體儲存系統，包括：

一快閃記憶體；

一主機；以及

一控制器，耦接該主機與該快閃記憶體，依據該主機之狀態限制該主機存取該快閃記憶體；其中當該主機處於開機或重置狀態時，該控制器允許該主機存取該快閃記憶體，當該主機完成開機或重置動作後，該控制器限制該主機存取該快閃記憶體。

2. 如申請專利範圍第 1 項所述之快閃記憶體儲存系統，更包括：

一開關，耦接於一主電源與該主機之間，該控制器更依據一暫停電源而導通該開關，以將該主電源提供至該主機。

3. 如申請專利範圍第 2 項所述之快閃記憶體儲存系統，其中當該控制器被關閉時，該控制器斷開該開關以停止供應該主電源至該主機。

4. 如申請專利範圍第 3 項所述之快閃記憶體儲存系統，其中當該主機受控於一重置訊號而處於重置狀態時，該控制器依據該重置訊號而允許該主機存取該快閃記憶體。

5. 如申請專利範圍第 1 項所述之快閃記憶體儲存系統，更包括：

一時脈產生器，耦接該主機，提供該主機運作所依據

之一時脈訊號，當該控制器被關閉時，該時脈產生器停止供給該時脈訊號至該主機。

6. 如申請專利範圍第 1 項所述之快閃記憶體儲存系統，其中該控制器包括：

至少一暫存器，儲存該快閃記憶體之保護區塊的記憶體位址，該控制器更自該快閃記憶體取得該保護區塊的記憶體位址，並將該保護區塊的記憶體位址寫入該暫存器。

7. 如申請專利範圍第 6 項所述之快閃記憶體儲存系統，其中該控制器更判斷該主機欲存取的一目標記憶體位址是否為該保護區塊的記憶體位址，若為該保護區塊的記憶體位址則拒絕該主機存取該目標記憶體位址。

8. 一種快閃記憶體儲存系統的資料保護方法，其中該快閃記憶體儲存系統包括一主機以及一快閃記憶體，該資料保護方法包括：

判斷該主機是否處於開機或重置狀態；

若該主機處於開機或重置狀態，允許該主機存取該快閃記憶體；以及

若該主機非處於開機或重置狀態，限制該主機存取該快閃記憶體。

9. 如申請專利範圍第 8 項所述之快閃記憶體儲存系統的資料保護方法，其中限制該主機存取該快閃記憶體的步驟更包括：

判斷該主機欲存取的一目標記憶體位址是否為該保護區塊的記憶體位址；

若為該保護區塊的記憶體位址，拒絕該主機存取該目標記憶體位址；以及

若非為該保護區塊的記憶體位址，則允許該主機存取該目標記憶體位址。

10. 如申請專利範圍第 8 項所述之快閃記憶體儲存系統的資料保護方法，其中該快閃記憶體儲存系統更包括一暫存器，該主機處於開機或重置狀態時的步驟更包括：

取得該保護區塊的記憶體位址；以及

將該保護區塊的記憶體位址寫入該暫存器。

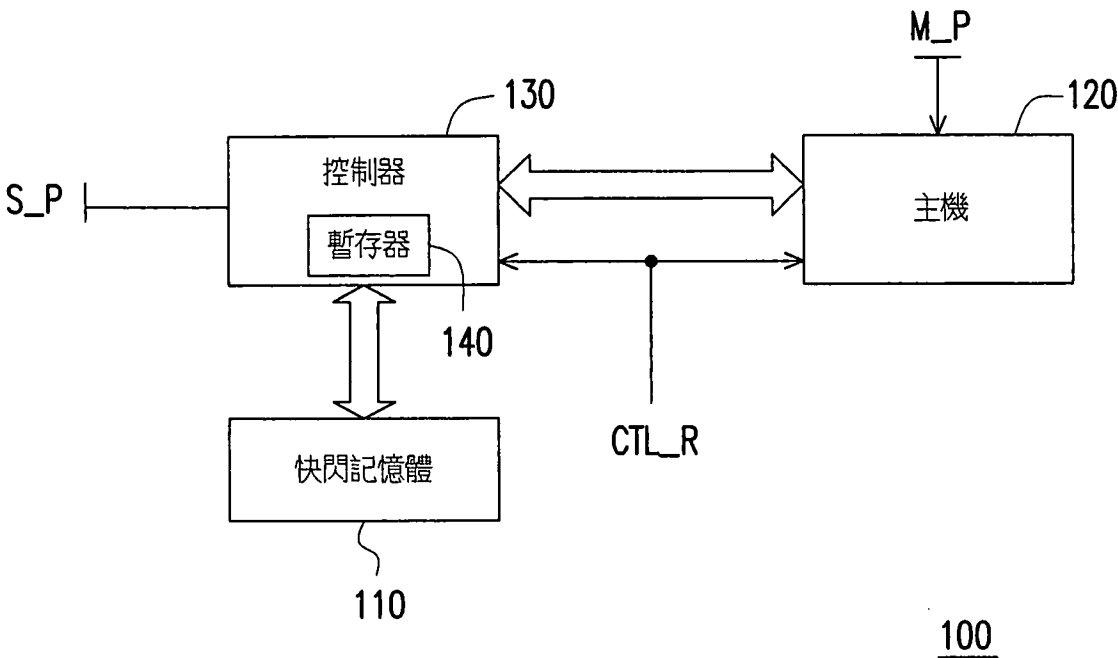


圖 1

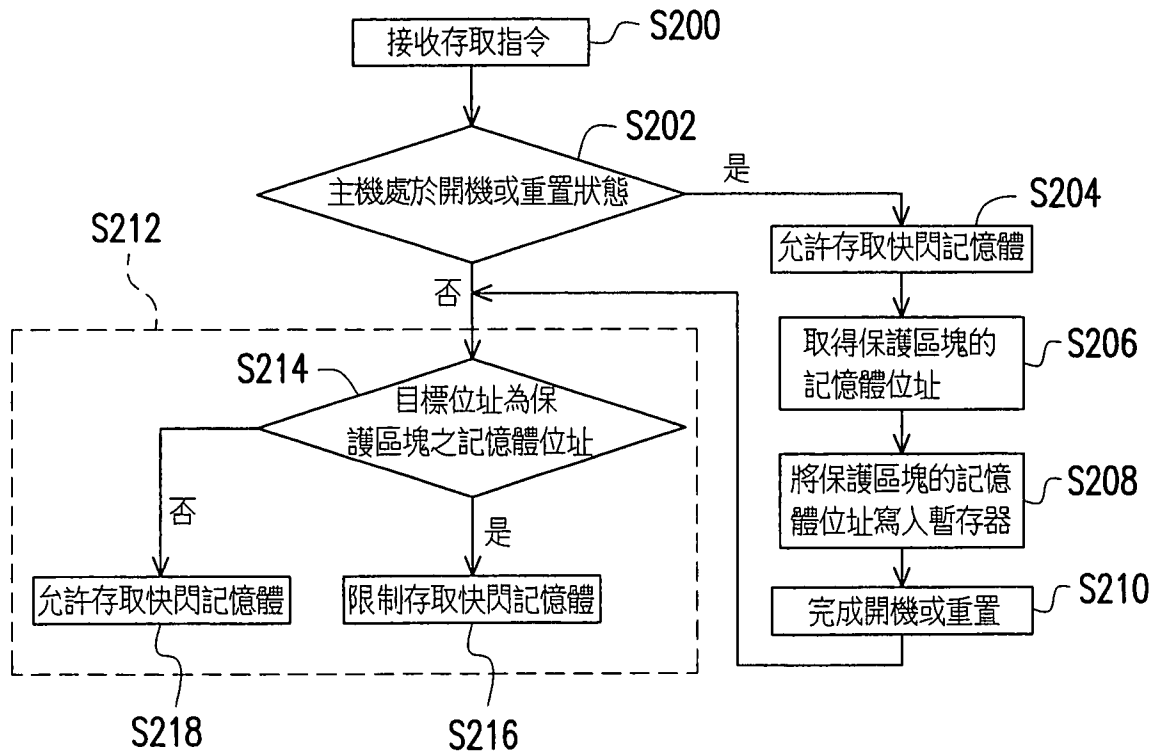


圖 2

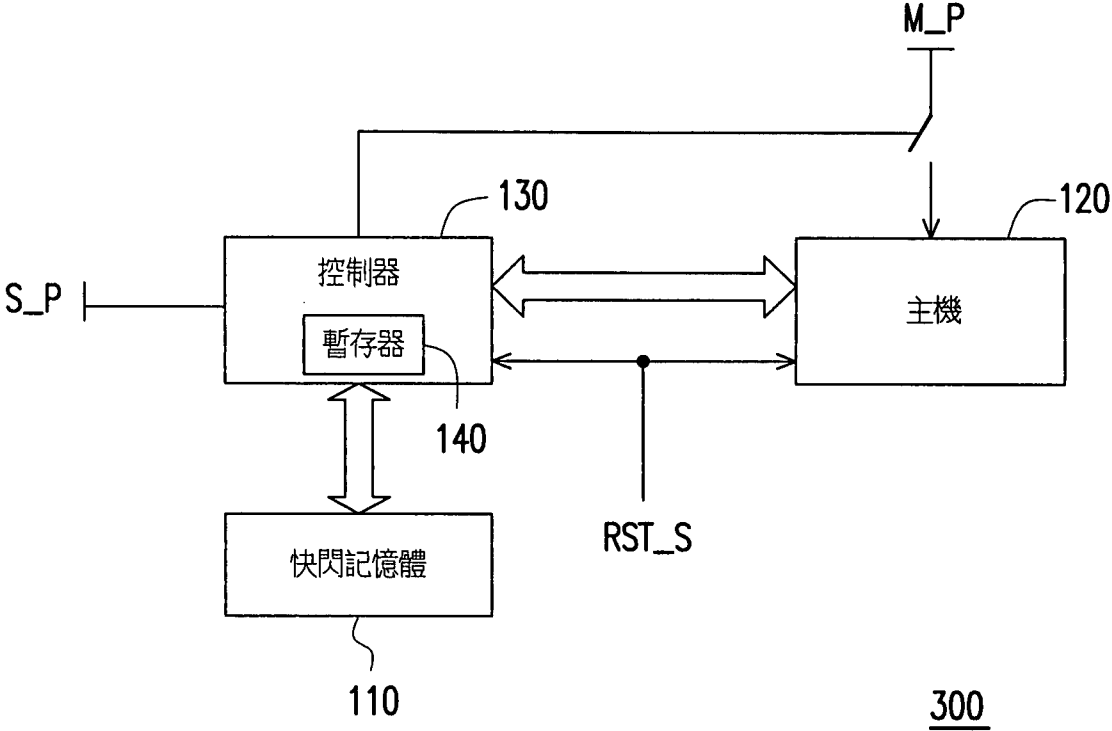


圖 3

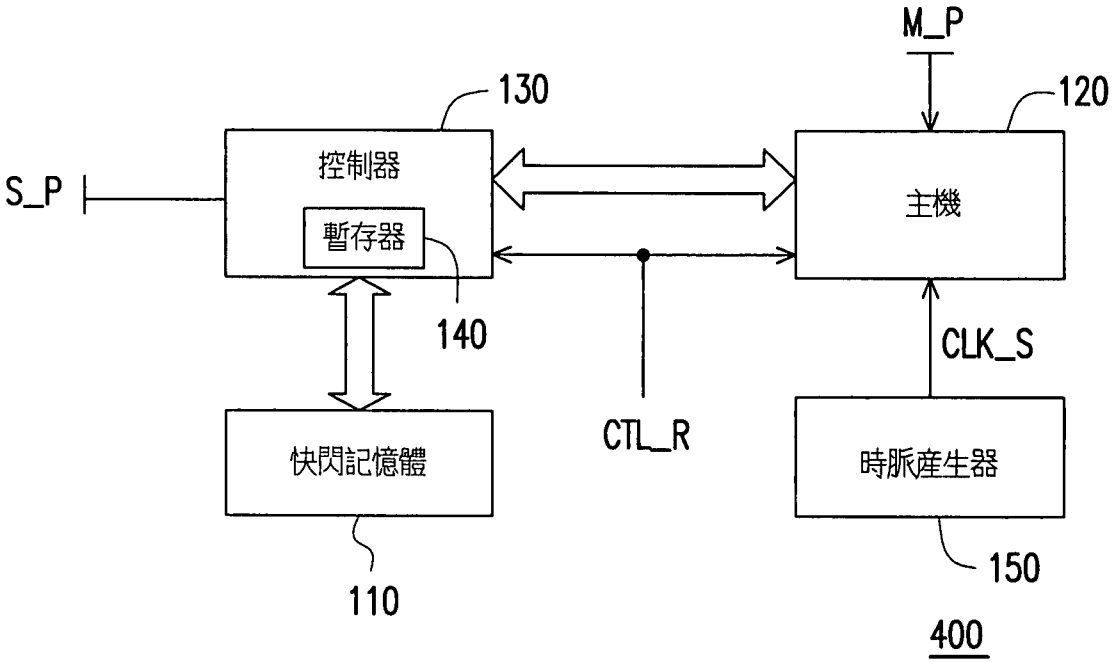


圖 4