I879999

(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 I879999 B**

(45)公告日： 中華民國 114 (2025) 年 04 月 11 日

(21)申請案號：110126422 (22)申請日： 中華民國 110 (2021) 年 07 月 19 日

(51)Int. Cl.： ***G06F9/312 (2006.01)*** ***G06F12/02 (2006.01)***

G06F21/46 (2013.01)

(30)優先權：2020/07/24 美國 16/937,907

(71)申請人：美商高通公司 (美國) QUALCOMM INCORPORATED (US)

美國

(72)發明人：李 燕如 LI, YANRU (US)；千 德斯特塔密歐 CHUN, DEXTER TAMIO (US)

(74)代理人：李世章

(56)參考文獻：

TW 201939341A US 8893267B1

US 2014/0089617A1 US 2018/0121125A1

審查人員：林剛煌

申請專利範圍項數：14 項 圖式數：15 共 78 頁

(54)名稱

記憶體設備與用於向片上系統（ＳＯＣ）指示存取通過/違規回饋作為記憶體設備的讀/寫事務序列的一部分的方法

(57)摘要

各種實施例可以包括用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法和系統。各種方法可以包括：從 SOC 接收用於配置記憶體設備的記憶體存取控制的配置訊息，基於配置訊息來配置記憶體存取控制。各種實施例可以包括：從 SOC 接收請求存取記憶體設備的記憶體單元陣列的記憶體基底位址和記憶體存取範圍的存取請求訊息，其中存取請求訊息包括讀/寫操作。各種實施例可以包括：將存取請求訊息與配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的。各種實施例亦可以包括：回應於決定存取請求訊息是可允許的，執行讀/寫操作。

Various embodiments may include methods and systems for providing secure in-memory device access of a memory device by a system-on-a-chip (SOC). Various methods may include receiving a configuration message from the SOC for configuring a memory access control of the memory device, and configuring the memory access control based on the configuration message. Various embodiments may include receiving an access request message from the SOC requesting access to a memory base address and a memory access range of a memory cell array of the memory device, wherein the access request message includes a read/write operation. Various embodiments may include comparing the access request message with the configured memory access control to determine whether the access request message is allowable. Various embodiments may further include performing the read/write operation in response to determining that the access request message is allowable.

指定代表圖：

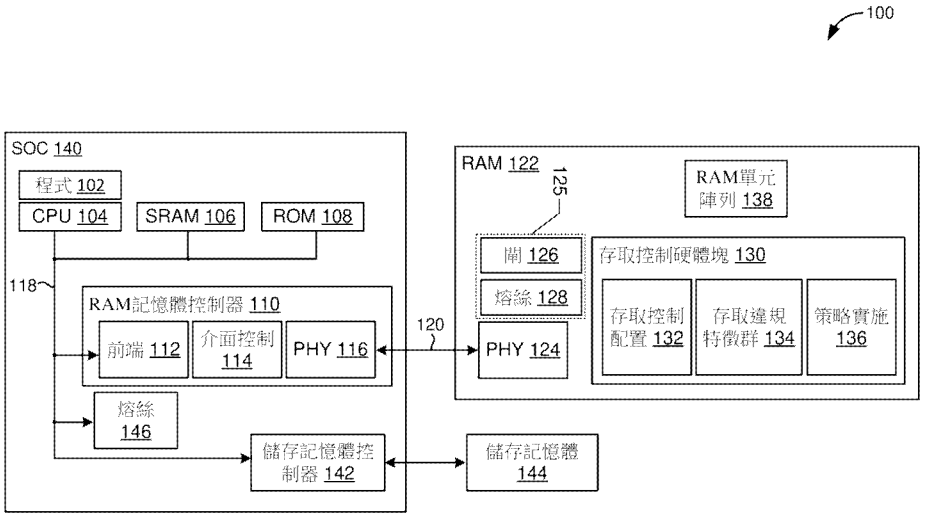

圖1

符號簡單說明：

100:計算系統

102:可信程式

104:中央處理單元（CPU）

106:靜態 RAM（SRAM）

108:唯讀記憶體（ROM）

110:RAM 記憶體控制器

112:前端

114:介面控制

116:實體介面（PHY）

118:匯流排

120:外部匯流排

122:RAM

124:PHY

125:信任硬體塊

126:閘

128:熔絲

130:存取控制硬體塊

132:存取控制配置塊

134:存取違規特徵群塊

136:策略實施塊

138:RAM 單元陣列

140:SOC

142:儲存記憶體控制器

144:存取儲存記憶體

146:熔絲

I879999

【發明摘要】

【中文發明名稱】記憶體設備與用於向片上系統（SOC）指示存取通過/違規回饋作為記憶體設備的讀/寫事務序列的一部分的方法

【英文發明名稱】MEMORY DEVICE, AND METHOD FOR INDICATING ACCESS PASS/VIOLATION FEEDBACK TO A SYSTEM ON CHIP, (SOC), AS PART OF A READ/WRITE TRANSACTION SEQUENCE OF THE MEMORY DEVICE

【中文】

各種實施例可以包括用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法和系統。各種方法可以包括：從SOC接收用於配置記憶體設備的記憶體存取控制的配置訊息，基於配置訊息來配置記憶體存取控制。各種實施例可以包括：從SOC接收請求存取記憶體設備的記憶體單元陣列的記憶體基底位址和記憶體存取範圍的存取請求訊息，其中存取請求訊息包括讀/寫操作。各種實施例可以包括：將存取請求訊息與配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的。各種實施例亦可以包括：回應於決定存取請求訊息是可允許的，執行讀/寫操作。

【英文】

Various embodiments may include methods and systems for providing secure in-memory device access of a memory device by a system-on-a-chip (SOC). Various methods may include receiving a configuration message from the SOC for configuring a memory access control of the memory device, and configuring the memory access

control based on the configuration message. Various embodiments may include receiving an access request message from the SOC requesting access to a memory base address and a memory access range of a memory cell array of the memory device, wherein the access request message includes a read/write operation. Various embodiments may include comparing the access request message with the configured memory access control to determine whether the access request message is allowable. Various embodiments may further include performing the read/write operation in response to determining that the access request message is allowable.

【指定代表圖】第（ 1 ）圖。

【代表圖之符號簡單說明】

100：計 算 系 統

102：可 信 程 式

104：中 央 處 理 單 元 （ CPU ）

106：靜 態 RAM （ SRAM ）

108：唯 讀 記 憶 體 （ ROM ）

110：RAM 記 憶 體 控 制 器

112：前 端

114：介 面 控 制

116：實 體 介 面 （ PHY ）

118：匯 流 排

120：外 部 匯 流 排

122：RAM

124：PHY

125：信 任 硬 體 塊

126：閘

128：熔絲

130：存取控制硬體塊

132：存取控制配置塊

134：存取違規特徵群塊

136：策略實施塊

138：RAM單元陣列

140：SOC

142：儲存記憶體控制器

144：存取儲存記憶體

146：熔絲

【特徵化學式】

無

【發明說明書】

【中文發明名稱】記憶體設備與用於向片上系統（SOC）指示存取通過/違規回饋作為記憶體設備的讀/寫事務序列的一部分的方法

【英文發明名稱】MEMORY DEVICE, AND METHOD FOR INDICATING ACCESS PASS/VIOLATION FEEDBACK TO A SYSTEM ON CHIP, (SOC), AS PART OF A READ/WRITE TRANSACTION SEQUENCE OF THE MEMORY DEVICE

【技術領域】

【0001】 本案係關於用於在記憶體設備內的存取控制的方法和裝置。

【先前技術】

【0002】 傳統上，系統記憶體存取控制已經被實現為在應用處理器（AP）或片上系統（SOC）內的專有功能，或者由主側（諸如經由記憶體管理單元（MMU）、輸入/輸出MMU或系統MMU的實現方式）來實現，或者經由從側（諸如經由在雙倍資料速率（DDR）子系統前面的記憶體保護單元（MPU）的實現方式）來實現。為了實現由SOC對記憶體的安全配置和存取，SOC可以包括硬體和軟體，來監督和保護記憶體存取，確保記憶體存取控制程序不妨礙或降低系統效能，並且提供保護以防止程序間損壞、洩漏、損害及/或安全攻擊。

【0003】 正在開發新的SOC以發展用例，諸如物聯網路（IoT）、可穿戴設備、以及其他小形狀因數設備。這樣的用例可以有利於將硬體及/或軟體的一些部分從SOC卸載

到外部裝置及/或硬體，以減小SOC的實體大小、成本和功耗。然而，將硬體和軟體卸載到已經按慣例在SOC內本端實現的外部裝置可能引入安全風險和效能降級。

【發明內容】

【0004】 各個態樣包括用於以下操作的方法和實現方法的記憶體設備：向SOC指示存取通過/違規回饋作為經由SOC進行的記憶體設備的讀/寫事務序列的一部分。各個態樣可以包括：從SOC接收用於配置記憶體設備的記憶體存取控制的配置訊息；基於配置訊息來配置記憶體存取控制；從SOC接收請求存取記憶體設備的記憶體單元陣列的記憶體基底位址和記憶體存取範圍的存取請求訊息，其中存取請求訊息可以包括讀/寫操作；將存取請求訊息與所配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的；及回應於決定存取請求訊息是可允許的，執行讀/寫操作。

【0005】 在一些態樣中，配置訊息可以包括配置安全域ID，並且存取請求訊息可以包括請求的安全域ID。在一些態樣中，配置訊息可以是包括配置安全域ID的經編碼的JEDEC訊息，並且存取請求訊息可以是包括請求的安全域ID的經編碼的JEDEC訊息。在一些態樣中，將存取請求訊息與配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的可以包括：決定配置安全域ID與請求的安全域ID是否匹配，以及回應於決定配置安全域ID與請求的安全域ID匹配，決定存取請求訊息是可允許的，並且向

SOC發送指示存取請求訊息是可允許的通知。這樣的態樣亦可以包括：回應於決定配置安全域ID與請求的安全域ID不匹配，決定存取請求訊息是不可允許的，儲存包括記憶體基底位址、記憶體存取範圍和請求的安全域ID的錯誤資訊，向SOC發送指示存取請求訊息是不可允許的通知，以及回應於從SOC接收錯誤插斷要求，向SOC發送錯誤資訊。

【0006】 一些態樣亦可以包括：從SOC接收解鎖密碼，決定所接收的解鎖密碼與被儲存在記憶體設備中的可接受密碼集合內的密碼是否匹配；及回應於決定所接收的解鎖密碼與在可接受密碼集合內的密碼匹配，解鎖記憶體設備閘邏輯以允許記憶體存取控制來接收配置訊息。一些態樣亦可以包括：從SOC接收鎖定命令，該鎖定命令被配置為設置在記憶體設備的暫存器內的鎖定位元，並且設置鎖定位元以防止對所配置的記憶體存取控制的配置改變。

【0007】 另外的態樣包括具有處理器的記憶體設備，處理器被配置為執行上文概述的方法中的任何方法的操作。另外的態樣包括記憶體設備，記憶體設備具有用於執行上文概述的方法中的任何方法的功能的單元。

【圖式簡單說明】

【0008】 併入本文中並且構成本說明書的一部分的附圖示出示例性實施例，並且連同上文提供的整體概述和下文提供的具體實施方式一起用以解釋各種實施例的特徵。

【0009】 圖1是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的實例計算系統100的部件方塊圖。

【0010】 圖2是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的包括閘的實例計算系統200的部件方塊圖。

【0011】 圖3是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的實例計算系統300的部件方塊圖。

【0012】 圖4是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的方法400的程序流程圖。

【0013】 圖5是示出根據一些實施例的包括用於提供安全的在記憶體設備內的存取控制的資料和配置事務路徑的實例計算系統500的部件方塊圖。

【0014】 圖6是示出根據一些實施例的用於監視安全的記憶體設備內的存取違規的方法600的程序流程圖。

【0015】 圖7示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的系統記憶體映射700。

【0016】 圖8是示出根據一些實施例的用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的程序流程圖。

【0017】 圖9是示出根據一些實施例的可以由記憶體設備執行的作為用於經由片上系統（SOC）提供對記憶體設備

的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。

【0018】 圖10是示出根據一些實施例的可以由記憶體設備執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。

【0019】 圖11是示出根據一些實施例的可以由記憶體設備執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。

【0020】 圖12是示出根據一些實施例的可以由記憶體設備執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。

【0021】 圖13示出根據一些實施例的以智慧手錶1300的形式的實例可穿戴計算設備。

【0022】 圖14是根據一些實施例的可以經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的網路計算設備1400的實例的部件方塊圖。

【0023】 圖15是適於實現一些實施例的以智慧型電話1500的形式的實例無線設備的部件方塊圖。

【實施方式】

【0024】 將參照附圖詳細描述各種實施例。在可能的情況下，在貫穿附圖使用相同的元件符號來指代相同或相似的

組件。對特定實例和實施例所做出的參考是出於說明性目的，以及不意欲限制各種實施例或請求項的範疇。

【0025】 各種實施例提供用於提供安全的在記憶體設備內的存取控制的解決方案，以實現硬體及/或軟體的一些部分到外部裝置的卸載，以減小SOC大小、成本和功耗，而不引入安全風險和效能降級。

【0026】 本文使用術語「無線設備」來指代蜂巢式電話、智慧型電話、可攜式計算設備、個人或行動多媒體播放機、自主車輛、在自主和半自主車輛內的無線通訊部件、附接到或併入到各種行動平臺中的無線設備、支援多媒體網際網路的蜂巢式電話、和包括記憶體、無線通訊部件和可程式設計處理器的類似電子設備中的任何一項或全部。

【0027】 術語「片上系統」（SOC）在本文中用於指代包含集成在單個襯底上的多個資源或處理器的單個積體電路（IC）晶片。單個SOC可以包含用於數位、類比、混合訊號和射頻功能的電路。單個SOC亦可以包括任何數量的通用或專用處理器（數位訊號處理器、數據機處理器、視訊處理器等）、記憶體塊（諸如ROM、RAM、快閃記憶體等）和資源（諸如計時器、電壓調節器、振盪器等）。SOC亦可以包括用於控制集成的資源和處理器以及用於控制周邊設備的軟體。

【0028】 術語「系統級封裝」（SIP）在本文中用於指代在兩個或更多IC晶片、襯底或SOC上包含多個資源、計算單元、核心或處理器的單個模組或封裝。例如，SIP可以包

括在其上以垂直配置堆疊多個IC晶片或半導體晶粒的單個襯底。類似地，SIP可以包括在其上多個IC或半導體晶粒被封裝到統一的襯底中的一或多個多晶片模組（MCM）。SIP亦可以包括經由高速通訊電路耦合在一起並且密集地封裝的多個獨立SOC，諸如在單個主機板上或者在單個無線設備中。SOC的接近性促進高速通訊以及記憶體和資源的共享。

【0029】 在一般計算設備中，記憶體存取控制部件和電路實體上位於那些計算設備內。例如，為了存取外部隨機存取記憶體（RAM），SOC將在SOC的實體佈局內包括用於記憶體存取控制的部件和電路，使得對RAM的存取是由SOC控制的。

【0030】 各種實施例在記憶體設備內而不是在SOC內實現安全記憶體存取控制。各種實施例可以包括：實現在記憶體設備內的存取控制，將在每個事務中的啟動程式的安全域傳送到記憶體，在記憶體設備中施行存取控制，包括配置、策略施行和錯誤指示，檢查存取錯誤指示作為讀/寫序列的一部分，以及建立對記憶體設備的存取控制作為系統初始化序列的一部分。

【0031】 各種實施例在SOC內包括安全機制，諸如閘和熔絲，該等安全機制允許SOC配設定於在SOC的實體佈局之外但是與SOC電通訊的記憶體設備內的記憶體存取控制。經由將記憶體存取控制從SOC卸載到一或多個記憶體設備，可以減少SOC實體大小、成本和功耗。在記憶體設備

內而不是在SOC內實現記憶體存取控制的額外益處包括：消除跨越廣泛範圍的SOC供應商對專有存取控制方案的需要並且因此增加標準化和通訊性，允許在安全記憶體系統中使用低或中等複雜度微處理器晶片，跨越大量微處理器、應用處理器（AP）或SOC重複使用存取控制韌體/軟體，以及開發能夠包括諸如計算和存取控制的功的新的更複雜記憶體設備（例如，記憶體計算裝置中/附近）。

【0032】 圖1是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制（而不是在SOC內）的實例計算系統100的部件方塊圖。各種實施例包括：在記憶體設備（諸如RAM 122）內實現記憶體存取控制硬體塊，該記憶體可以是在與處理設備（例如，AP、SOC、SIP等）進行電通訊的系統內實現的。各種實施例可以是以記憶體設備的形式來實現的，諸如動態RAM（DRAM）、儲存記憶體、非揮發性RAM（NVRAM）或者可以與在系統內的SOC 140進行電通訊的任何其他類型的記憶體設備或模組。

【0033】 SOC可以在具有一或多個安全RAM裝置的系統內實現。因此，可以執行額外的交握協定或程序以在不安全的SOC與安全的RAM之間建立安全級別。例如，可以執行額外的程序以經由匯流排120（例如，高速匯流排、RAM匯流排等）在SOC 140與RAM 122之間建立信任。SOC可以包括可信程式102、中央處理單元（CPU）104、靜態RAM（SRAM）106、唯讀記憶體（ROM）108、包括前端112、介面控制114和實體介面（PHY）116的RAM

記憶體控制器110、存取儲存記憶體144的儲存記憶體控制器142以及熔絲146。RAM 122可以包括PHY 124和RAM單元陣列138。RAM 122亦可以包括信任硬體塊125，信任硬體塊125包括閘126和熔絲128。RAM 122亦可以包括存取控制硬體塊130，存取控制硬體塊130包括存取控制配置塊132、存取違規特徵群塊134和策略實施塊136。SOC 140可以經由PHY 116電耦合到RAM 122的PHY 124，以發送交握協定，從而允許SOC 140配置存取控制硬體塊130。RAM 122的包括閘126和熔絲128的信任硬體塊125可以被實現以在SOC 140與RAM 122之間建立信任。一旦建立信任，SOC 140就可以接著配置存取控制硬體塊130以根據各種實施例提供記憶體保護。

【0034】 在一些實施例中，在RAM 122內的存取控制硬體塊130在功能上可以類似於實體上在SOC內的一般存取控制，並且可以執行程序，該程序包括：檢查發起程式、安全域、實體位址和存取類型以決定其是讀存取還是寫存取，以及隨後針對授權的事務允許對RAM單元陣列138進行記憶體存取。在可以經由存取控制配置塊132來初始化存取控制硬體塊130之前，可以解鎖閘126。當在CPU 104上執行的可信程式102向RAM 122發送解鎖密碼時，可發生解鎖，其中對照存在於熔斷器128中的值來檢查密碼。密碼可以是秘密的，並且可以被預先提供到RAM熔絲128中。若密碼解鎖成功，則閘126可以打開對存取控制配置塊132的讀/寫存取，並且可信程式102可以初始化存取控

制配置塊132，就像其是根據一般方法被包含在SOC內的一樣。在完成初始化之後，閘126可以返回到鎖定狀態。對存取控制配置塊132的額外改變可以一直遵循該解鎖/改變/鎖定程序。一旦存取控制硬體塊130被初始化，策略實施塊136就可以監視和調節在SOC 140與RAM單元陣列138之間的任務模式傳輸量。

【0035】 圖2是示出根據一些實施例的實例計算系統200的部件方塊圖，其示出在被配置用於提供安全的在記憶體設備內的存取控制的信任硬體塊125中耦合到邏輯204的閘126的細節。

【0036】 參考圖1和2，閘126可以包括一或多個通過閘202和控制邏輯204。通過閘202可以包括將PHY 124與存取控制硬體塊130連接/斷開的一或多個直列式開關，存取控制硬體塊130可以提供對RAM單元陣列138的存取。如上文所提及的，PHY 124可以提供與匯流排120相關聯的連接。連接120d對應於資料訊號，以及連接120c對應於位址/控制訊號。PHY 124可以經由連接214d將與連接120d相關聯的資料訊號提供給信任硬體塊125的通過閘202和控制邏輯204。PHY 124可以經由連接214c將與連接120c相關聯的位址/控制訊號提供給信任硬體塊125的通過閘202和控制邏輯204。

【0037】 如在圖2中進一步所示出的，每個通過閘202可以包括第一觸點和第二觸點。第一觸點可以電耦合到相應的資料連接214d和位址/控制連接214c，以及在閘或開關的

另一側的第二觸點可以電耦合到相應的閘控資料連接216d和閘控位址/控制連接216c。控制邏輯204可以經由連接218電耦合到每個通過閘202，經由該連接218可以提供閘控制訊號以斷開和封閉各個開關。在這點上，信任硬體塊125的「鎖定狀態」可以對應於其中斷開通過閘202以防止對閘控連接216d和216c的存取的操作狀態。

【0038】 通過閘202功能的替代實施例可以包括具有由閘控制218控制的輸出使能的雙向收發機、可以在閘控制218的控制下經由電源軌來通電/斷電的雙向收發機、或可以具有在閘控制218的控制下的輸出使能或電源軌的雙向鎖存器/暫存器。所採用的電路可以被有目的地設計用於雙向訊號傳輸，或者可以包括用於處理對應於寫和讀資料傳輸量的每個（例如，前向和反向）方向的兩個單獨的電路。

【0039】 在一些實施例中，當記憶體設備122斷電時，控制邏輯204可從SOC 140的電源管理器控制器接收對應命令，並且作為回應，經由連接218向通過閘202發送「鎖定」閘控制訊號。閘極控制訊號可以包括單獨的訊號（例如，用於一個通過閘的一條閘控制線）或單個訊號（例如，用於所有通過閘的一個閘控制）。在一些實施例中，通過閘202可以由電源開關代替，該電源開關對RAM單元陣列138的存取控制硬體塊130進行加電或斷電。回應於「鎖定」閘控制訊號，可以斷開通過閘202以阻止對閘控連接216d和216c的存取。以這種方式，當啟動記憶體設備時，閘機

制126處於「鎖定狀態」，其中通過閘202處於斷開位置，以首先防止讀/寫操作存取RAM記憶體單元陣列138。

【0040】 如參考圖1所描述的，當系統200被啟動並且可信程式102開始在CPU 104上執行時，儲存在SOC 140上的熔絲146中的解鎖密碼可以被取出並且提供給RAM記憶體控制器110，該RAM記憶體控制器110經由PHY116將值發送到PHY 124。在信任硬體塊125中的控制邏輯204可以經由例如在信任硬體塊125中的熔絲資料匯流排220和熔絲控制匯流排222來取出在熔絲128中提供的通過閘值。如在圖2中所示出的，信任硬體塊125及/或熔絲128可以包括控制器212以促進與控制邏輯204的通訊。控制邏輯204可以將通過閘值與從SOC 140接收的解鎖密碼進行比較。若解鎖密碼與通過閘值匹配，則控制邏輯204可以經由連接218向通過閘202發送「解鎖」閘控制訊號。回應於「解鎖」閘控制訊號，通過閘202可以被封閉，從而將資料連接214d和位址/控制連接214c分別連接到閘控連接216d和閘控位址/控制連接216c。在該「解鎖狀態」中，閘機制126可以經由資料匯流排224d和控制匯流排224c提供對存取控制硬體塊130的無限制存取。

【0041】 如上文所提及的，在SOC 140及閘控RAM 122之間的密碼交換可以以各種方式來實現。在一些實施例中，可以經由熔絲146、128來實現簡單的未加密的密碼交換。在一些實施例中，安全密碼交換可以採用任何期望的加密演算法以經由更複雜或額外的交握協定或程序來改善

安全級別。如在圖2中所示出的，當安全密碼交換採用加密時，在信任硬體塊125中的控制邏輯204可以包括用於支援解碼功能（方塊206）、雜湊（hash）函數（方塊208）和校驗功能（方塊210）的邏輯模組。

【0042】 在信任硬體塊125中的解碼邏輯206可以經由匯流排214c接收控制和位址資訊，並且經由匯流排214d接收資料。在一些實施例中，可以實現預先決定的及/或標準化的協定，以控制控制邏輯204、交換資訊（諸如金鑰和密碼）、或者對部件（諸如熔絲128）進行初始化和程式設計。例如，在控制與位址匯流排214d上可存在特定命令，該特定命令可以由解碼邏輯206解碼並且接著可以啟動特定命令功能。一些實施例可以包括與每種類型的功能相關聯的獨有的命令和資料，諸如重定閘邏輯、在多個位置中的程式熔絲資料、程式私密金鑰、程式密碼、程式自毀失敗嘗試、使能篡改機制、輸入金鑰模數p、輸入金鑰基數g、檢索散列、解鎖未加密密碼、解鎖加密密碼等。

【0043】 在信任硬體塊125中的解碼邏輯206可以負責回應於進入的控制、位址和資料來解析和觸發適當的操作。如在圖2中所示出的，控制與位址214c和資料214d連接到達通過閘202，並且若已解鎖，則可以傳播到存取控制硬體塊130，該存取控制硬體塊130可以執行類似的預先決定的及/或標準化的任務模式操作，諸如RAM單元陣列讀取、RAM單元陣列寫入、RAM單元陣列頁選擇、RAM單

元陣列修復、RAM裝置配置、PHY高級配置、以及與防竄改功能無關的任何其他功能性。

【0044】 雜湊函數208可以執行用於秘密金鑰交換程序的模算數運算，並且可以包括查閱資料表及/或模加法順序和平行計算邏輯。檢查功能210可以被包括在信任硬體塊125的控制邏輯204中，用於將從SOC 140發送的密碼與先前程式設計到信任硬體塊125中的本端熔絲128中的本機複本進行比較。解密邏輯（未圖示）可以被包括在信任硬體塊125的校驗功能210內，以允許SOC 140發送使用加密的密碼，以防止當密碼經過外部匯流排120時窺探者查看密碼。若SOC 140已經對密碼進行加密，則解密邏輯可以首先使用在安全交換程序（諸如Diffie-Hellman方法）期間推導的共享秘密金鑰來對密碼進行解密。

【0045】 在一些實施例中，在已經發生多個不成功的解鎖事件的情況下，可以啟動在信任硬體塊125中的熔絲128以永久地禁用控制邏輯204，從而防止對記憶體的未來存取。

【0046】 圖3是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的實例計算系統300的部件方塊圖。參考圖1-3，SOC 140可以包括實現除了由CPU 104實現的可信程式102之外的各種可信程式的處理單元。例如，SOC 140可以包括實現可信程式306的網路處理單元（NPU）308，其中NPU 308電連接到匯流排118。

【0047】 與RAM 122電通訊的SOC 140可以在每次SOC執行對RAM單元陣列138的新的存取嘗試時配置存取控制硬體塊130。在配置存取控制硬體塊130之前，可以初始化SOC 140和RAM 122以配置任務模式記憶體存取過濾。例如，可以在SOC 140配置和初始化存取控制硬體塊130之前執行金鑰交換和建立秘密頻道。SOC 140的安全實體或部件可以包括用於打開閘126的金鑰或密碼。如上文所描述的，SOC 140可以將金鑰發送到RAM 122以打開閘126，以隨後允許SOC 140配置存取控制硬體塊130，以初始化RAM單元陣列138的適當存取。在存取控制硬體塊130的配置之後，SOC 140可以設置在RAM 122內的鎖定位元，以防止對存取控制硬體塊130的進一步修改。SOC 140的安全實體亦可以向存取控制硬體塊130發佈命令，以在經由所建立的秘密頻道交換記憶體資訊之後再次改變配置，以進行隨後的未來記憶體存取嘗試。換句話說，SOC 140可使用儲存在SOC 140的安全實體中的金鑰或密碼/密碼來解鎖閘126，利用適當的記憶體存取資訊來配置存取控制硬體塊130，鎖定配置以防止在對RAM單元陣列138的存取正在進行時修改秘密頻道，並且在已經配置並且鎖定秘密頻道之後使存取控制硬體塊130能夠開始存取RAM單元陣列138。

【0048】 RAM 122可以提供用於由SOC 140進行的側控制的暫存器介面。RAM 122可以包括用於在RAM單元陣列138內的每個存取區域的鎖定位元以防止對配置的進一

步修改。在SOC到RAM初始化之後，可以設置、啟用或以其他方式配置鎖定位元，以在存取控制硬體塊130的最近配置中進行鎖定。RAM 122可以包括用於在RAM單元陣列138的每個存取區域的啟用位元，使得設置啟用位元允許（例如，經由策略實施塊136）實施所配置的存取控制硬體塊130。

【0049】 SOC 140可配置存取控制硬體塊130，以經由將存取資訊編碼在發送到RAM 122的命令內來存取RAM單元陣列138的特定部分或域。例如，SOC 140可以將關於記憶體基底位址（例如，位址32）、記憶體資料大小及/或範圍（例如，資料34）及存取域ID（例如，ID 36）的資訊編碼到經由資料和存取/控制通道（例如，連接120d、120c、214d、214c、216d、216c）發送到RAM 122的命令內。針對每個存取區域的基底位址和大小資訊可以根據記憶體設備存取方案來表達，諸如以RAM單元陣列138的記憶體單元行的細微性來表達。在一些實例中，可以跨越與資料和存取/控制通道分離的匯流排將存取域ID/安全域ID發送到RAM 122。例如，RAM記憶體控制器110可以經由連接302i和304i將安全域ID發送到PHY 124並且隨後發送到存取控制硬體塊130。

【0050】 經編碼的命令可以包括用於存取針對每個存取區域或域的正確配置的資訊。經編碼的命令可以包括安全ID或域ID，並且策略實施塊136可以檢查安全ID以驗證SOC 140正在嘗試存取哪個域。經編碼的命令亦可以包括用以

指定針對RAM單元陣列138的每個所支援安全域的讀取和寫入存取許可的資訊。換句話說，經編碼的命令可以指定是從安全域讀取記憶體資訊、向安全域寫入記憶體資訊、還是從安全域讀取和向安全域寫入兩者。例如，RAM 122可以支援四個安全域，其可以被映射到四個SOC 140側安全域，例如AP、圖形、數位訊號處理（DSP）和安全處理器。對於每個存取控制區域，可以存在用於指示針對每個安全域的讀取許可的四個位元，以及用於指示針對每個安全域的寫入許可的四個位元。SOC 140可以配置安全域ID是如何映射到SOC 140安全域的。例如，SOC 140可以定義或以其他方式將安全ID值0歸於AP高級作業系統（HLOS），將1歸於AP安全實體，將2歸於圖形，並將3歸於安全處理器。可在經編碼的命令中指定針對在RAM單元陣列138內的每個特定安全域的讀/寫存取許可。

【0051】 在一些實施例中，存取控制硬體塊130的存取違規特徵群塊134可以監視和報告在存取控制配置之前和期間以及在配置存取控制硬體塊130之後跨域建立的秘密頻道的記憶體交換期間發生的任何錯誤。RAM 122可以包括錯誤中斷引腳，當存取違規特徵群塊134已經觀察到錯誤時，該錯誤中斷引腳可以向SOC 140發送中斷訊號。例如，存取違規特徵群塊可以觀察到在存取控制硬體塊130已經被適當配置之後在記憶體存取（例如，從在RAM單元陣列138內的安全域讀取及/或向其寫入）期間已發生一或多個錯誤。回應於觀察並且記錄錯誤，存取控制可以接著經由

連接304e和302e從PHY 124向SOC 140的RAM記憶體控制器110發送錯誤中斷訊號。在執行讀取或寫入命令之後的至少一個時鐘週期，SOC 140可以感測錯誤指示/中斷訊號/引腳（例如，連接302e）。對於讀取錯誤，錯誤指示可以是讀取回應的一部分，使得讀取回應可以包括在資料匯流排（例如，連接120d）上的未定義值。對於寫入錯誤，可能需要額外的時鐘週期來感測錯誤中斷引腳，使得存取違規特徵群塊134可以分析寫入命令是被不正確地執行還是不能被適當地執行，並且隨後產生指示以發送到SOC 140，指示寫入命令導致一或多個錯誤。由存取違規特徵群塊134產生的錯誤指示可以包括錯誤類型（例如，讀/寫錯誤）、與RAM單元陣列138對應的錯誤位址、以及錯誤與哪個安全域ID對應。例如，在錯誤中斷訊號中報告的安全域ID可以標識在發生錯誤時SOC 140的安全域（例如，AP HLOS、AP安全實體、圖形、安全處理器等）中的哪個安全域正在嘗試存取RAM單元陣列138。

【0052】 錯誤指示可以包括針對由於單個讀或寫操作而發生的一或多個錯誤的這種資訊。例如，存取違規特徵群塊134可以儲存在SOC 140已經被計時以感測發生的錯誤中的至少一個錯誤之前可能已經發生的一系列錯誤。因此，經由存取違規特徵群塊134建立錯誤緩衝器可以允許SOC 140在一個時鐘循環中接收綜合的錯誤報告，而不遺漏可能在最近觀察到的錯誤之前的一或多個時鐘循環已經發生的任何錯誤。在一些實施例中，報告給SOC 140的錯誤指

示可以包括關於沿著在存取控制配置塊132、策略實施塊136和RAM單元陣列138處的資料及/或控制連接記憶體存取命令可能已經在何處被拒絕的指示。在一些實例中，存取違規特徵群塊134可以包括計數器，該計數器對由於一或多個記憶體存取命令已經發生的錯誤的數量進行計數。

【0053】 圖4是示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的方法400的程序流程圖。參考圖1-4，方法400的操作可由SOC（例如，SOC 140）的配置外部記憶體設備（例如，RAM 122）的處理器（例如，CPU 104、NPU 308）來執行。

【0054】 在方塊402-418中執行的操作的順序僅僅是說明性的，並且在一些實施例中，方塊402-418的操作可以以任何循序執行並且部分地同時執行。在一些實施例中，方法400可以由設備的處理器獨立於外部記憶體設備但與外部記憶體設備結合地執行。例如，方法400可以被實現為在SOC的處理器內執行的軟體模組，或者在SOC內的專用硬體中實現，其發佈命令以建立安全記憶體通道並且存取外部記憶體設備的記憶體，並且另外被配置為採取動作和儲存資料，如所描述的。

【0055】 在方塊402中，可以禁止對記憶體設備的存取。預設地，被設計為具有在記憶體內的安全存取控制的記憶體設備可以處於禁用狀態，其中記憶體設備可以是由外部處理設備（諸如SOC）可配置的。例如，如參考圖1-3所

描述的，記憶體設備可以是RAM 122，其可以具有處於斷開狀態的通過閘202，使得任何處理設備（例如，SOC 140）在與RAM 122電耦合/配對時將不能存取記憶體（例如，RAM單元陣列138）。記憶體設備的初始狀況亦可具有針對未初始化的或以其他方式未程式設計的金鑰/密碼碼/密碼的預設值，使得私密金鑰可具有空的/未程式設計的預設狀態或為0的預設值。例如，RAM 122的熔絲128可以具有為0的預設私密金鑰值。

【0056】 在方塊404中，SOC和記憶體設備可以配對。在包括SOC和外部記憶體設備的系統的現場實現之前工廠初始化可以發生，使得SOC和記憶體設備被程式設計有或被發佈有特定金鑰/密碼/密碼，以允許在SOC與記憶體設備之間建立安全存取通道。初始化可以包括在將SOC從記憶體設備鎖定之前燒制私密金鑰、密碼和最大存取嘗試的數量。例如，在由SOC進行的一數量的失敗存取嘗試之後，記憶體設備可以禁用存取控制（例如，經由防止閘的狀態改變/將閘保持在解鎖狀態），防止由與記憶體設備進行電通訊的未授權SOC的潛在駭客攻擊。

【0057】 在方塊406中，可以啟動包括SOC和配對外部記憶體設備的系統。系統啟動可以包括：將SOC和記憶體設備實體地配對（亦即，在硬佈線系統中），以及隨後給系統通電。例如，SOC 140可以硬佈線到RAM 122，使得SOC 140和RAM 122實體地位於並且耦合在單個系統外殼內。

【0058】 在方塊408中，一旦SOC和記憶體設備被供電和啟動，SOC就可以與記憶體設備的信任硬體塊125交換金鑰/密碼資訊，如參考圖2所描述的。記憶體設備處於預設鎖定狀態，信任硬體塊125可以從SOC接收金鑰/密碼資訊，並且邏輯204可以將所接收的金鑰/密碼資訊與被儲存在熔絲記憶體128中的資訊進行比較，以驗證SOC是否有權配置記憶體設備的存取控制硬體塊130的存取控制策略。若邏輯204驗證了SOC許可權，則信任硬體塊125可以解鎖閘126以供SOC配置存取控制硬體塊130的存取控制。SOC可以從公共秘鑰集合中隨機選擇以發送到記憶體設備，以允許記憶體設備決定是否應當准許存取。公共秘鑰集合可以是由SOC配置並且儲存的，如在方塊404中所述的。

【0059】 在決定方塊410中，信任硬體方塊125的邏輯204可以決定由SOC提供的金鑰資訊是否有效。在一些實施例中，信任硬體塊125的邏輯204可以在決定方塊410中根據塊在404中描述的程序經由與在記憶體設備中初始化的私密金鑰資訊進行比較來決定金鑰是否有效。如參考圖2所描述的，如由信任硬體塊125的控制邏輯204所決定的，若由SOC發送的金鑰無效，則記憶體設備將保持在鎖定狀態（亦即，閘斷開），或者若金鑰有效，則記憶體設備將改變到解鎖狀態（亦即，閘封閉）。

【0060】 回應於決定由SOC所提供的金鑰無效（亦即，決定方塊410 =「否」），SOC可以經由選擇如在方塊408

中所描述的其他公共秘鑰來嘗試進一步的存取嘗試，直到可以發生某個數量的存取嘗試並且記憶體設備保持在鎖定狀態為止。

【0061】 回應於決定由SOC所提供的金鑰有效（亦即，決定方塊410 = 「是」），在方塊412中信任硬體塊125可以解鎖以建立與SOC的安全連接，並且允許SOC向記憶體（例如，RAM單元陣列138）發佈讀/寫命令之前出於配置目的而存取控制硬體塊130。該程序可以由參照圖2描述的SOC和配對的記憶體設備執行。在一些實施例中，准許由SOC進行的存取可以包括解鎖記憶體設備的暫存器以配置存取控制。

【0062】 在方塊414中，SOC可以向記憶體設備發送命令，以配置並且隨後鎖定存取控制硬體塊130的記憶體存取控制。如參考圖3所描述的，SOC可以向記憶體設備發佈經編碼的命令以配置存取控制硬體塊130的存取控制，以準備跨越秘密頻道執行讀/寫記憶體操作。由SOC發送並且由記憶體設備的存取控制配置塊接收的經編碼的命令可以包括存取配置參數，該存取配置參數包括基底位址、大小或位址範圍以及安全域ID，以決定SOC的哪些安全實體正在嘗試存取記憶體的特定部分以及在記憶體設備內的哪個記憶體以及多少記憶體將被存取。SOC的處理器可以向在存取控制硬體塊130中的存取控制配置塊132發佈讀/寫操作，以準備用於交換記憶體資訊的秘密頻道。

【0063】 在一些實施例中，可以根據JEDEC記憶體標準從SOC向記憶體設備發送讀/寫命令。例如，實現JEDEC標準可以包括：經由JEDEC CMD和DATA匯流排發送讀/寫命令，其中cmd操作碼*指定操作是讀取還是寫入。例如，表1和表2示出使用JEDEC標準來配置存取控制配置塊的位址空間以定義存取配置參數（例如，基底位址、位址範圍、安全域ID）的寫入命令，其中讀取、寫入、Cas-2、MRW-1和MRW-2（模式暫存器寫入）是現有JEDEC命令。寫入專用和Cas-2專用可以是作為用於對記憶體設備的存取控制配置塊的暫存器空間進行程式設計的經修改的JEDEC協定命令的命令。

表1

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
寫入專用		*cmd**	*cmd**	*cmd**					1
									2

表2

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2專用		*cmd**	*cmd**	*cmd**					1
									2

【0064】 由於SOC執行如在表1和2中所示的命令，存取控制配置的32位元組的暫存器空間被配置為定義存取配置參

數。在表1和2中所示的命令可以在必要時重複多次，以針對每個安全域配置在存取控制配置塊內的額外位址空間。

【0065】 在一些實施例中，可根據包括SOC和記憶體設備的系統的應用來以各種格式使用JEDEC協定，使得記憶體設備可以是標準化的或是特定於應用的。例如，表3和4示出使用現有JEDEC命令來配置存取控制配置塊的位址空間以定義存取配置參數的一系列命令。

表3

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
寫入		*cmd**	*cmd**	*cmd**					1
									2

表4

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		*cmd**	*cmd**	*cmd**					1
									2

【0066】 除了在表3和4中所示的命令之外，SOC可以向在記憶體設備的存取控制硬體塊130內的存取控制配置塊發送指令，該等指令指定要修改的存取配置位址。例如，SOC可以發送32位元組命令，其包括定義存取配置位址的8位元組資料和定義存取配置參數的24位元組資料。該指令可以與SOC執行Cas-2命令一起、同時或基本上同時發送，使得在記憶體設備的存取控制硬體塊130內的存取控制配置塊可以將寫入和Cas-2命令與所接收的存取配置位址和參數資訊相關聯。這樣，在存取控制硬體塊130內的存取

控制配置塊可以被配置為當跨越一個匯流排介面接收Cas-2命令時，跨越另一個匯流排介面專閘監測對包括存取配置位址和參數資訊的指令的接收。在表3和4中所示的命令可以在必要時重複多次，以針對每個安全域配置在存取控制配置塊內的額外位址空間。

【0067】 表1-4僅僅是允許SOC向存取控制配置塊的位址空間寫入存取配置參數的實例的說明。可以執行讀取命令，以便以與寫入命令類似的方式從在存取控制硬體塊130內的存取控制配置塊的暫存器空間中讀取存取配置參數資訊（亦即，利用在表1-4中的JEDEC命令中的「讀取」代替「寫入」）。

【0068】 如上文所描述的，SOC可以經由向在記憶體設備的存取控制硬體塊130內的存取控制配置塊內的特定位址空間進行寫入來配置存取配置參數。存取配置參數可以定義在建立並鎖定存取控制配置以在SOC與記憶體設備之間建立秘密頻道之後由SOC執行的可允許的存取類型。例如，SOC可以執行與先前配置在存取控制硬體塊130的存取控制內的基底位址、位址範圍和安全域ID相對應的讀取和寫入操作。若SOC嘗試向例如在配置存取配置參數時沒有定義的安全域請求讀取或寫入資料，則存取控制硬體塊130將記錄錯誤，並且向SOC發送包括與錯誤有關的資訊的中斷（亦即，如參考圖3的存取違規特徵群塊134所描述的）。

【0069】 一旦存取控制硬體塊130的存取控制已經根據SOC發佈的命令進行配置，SOC亦可以向記憶體設備的存取控制硬體塊130發佈命令，以設置鎖定位元來在當前存取控制配置中進行鎖定，從而防止對配置的修改。在一些實施例中，SOC可以向記憶體發佈命令以復位鎖定位元，以允許在存取控制配置中的改變，諸如實現新的策略改變或記憶體改變。SOC亦可以向記憶體設備發佈命令以設置啟用位元以允許實施當前配置的存取控制（亦即，根據配置的存取控制配置塊在SOC與記憶體設備之間建立秘密頻道）。

【0070】 在方塊416中，SOC可存取記憶體設備的記憶體陣列。例如，在配置存取控制硬體塊130之後，SOC 140可以存取RAM單元陣列138以執行讀/寫操作。由SOC發送並且由記憶體設備接收的經編碼的命令可以包括包含安全域ID的額外資訊，以決定SOC的哪些安全實體正在嘗試存取在記憶體設備內的記憶體的特定部分。SOC的處理器可以發佈不具有存取保護的頁打開/關閉操作，並且可以發佈具有存取保護的讀/寫操作。

【0071】 在一些實施例中，可以根據JEDEC記憶體標準從SOC向記憶體設備發送讀/寫命令。例如，實現JEDEC標準可以包括：經由JEDEC CMD和DATA匯流排發送讀/寫命令，其中cmd操作碼*指定操作類型（例如，讀取、寫入或列位址選通）。JEDEC標準可被調整、修改、利用或以其他方式實現為包括指定安全域的存取控制ID**。例

如，表5-7示出根據JEDEC標準的讀取命令，其中Cas-3是新的額外JEDEC命令，其包括指定安全域的存取控制ID。讀取、寫入、Cas-2、MRW-1和MRW-2（模式暫存器寫入）是現有JEDEC命令。

表5

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
讀取		*cmd**	*cmd**	*cmd**					1
									2

表6

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

表7

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-3		cmd*	cmd*	cmd*					1
					ID**	ID**	ID**	ID**	2

【0072】 由SOC對記憶體設備的存取控制執行經編碼的命令讀取、Cas-2和Cas-3的結果是從與在Cas-3命令中指定的安全域ID相對應的記憶體位置讀取32位元組的資料。表5-7僅僅是允許SOC從記憶體設備讀取32位元組的實例的說明。可以執行寫入命令，以便以與讀取命令類似的方式將32位元組寫入到與安全域ID相對應的記憶體位置（亦即，利用在JEDEC命令中的「寫入」代替「讀取」）。

【0073】 在一些實施例中，可以根據包括SOC和記憶體設備的系統的應用來以各種格式使用JEDEC協定，使得記憶體設備可以是標準化的或是特定於應用的。例如，表8-11示出從記憶體設備讀取32位元組資料的一系列命令。

表8

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
寫入		*cmd**	*cmd**	*cmd**					1
									2

表9

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

表10

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
讀取		cmd*	cmd*	cmd*					1
									2

表11

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
Cas-2		cmd*	cmd*	cmd*					1
									2

【0074】 SOC可以向記憶體設備的存取控制發送指定安全域ID的指令。例如，SOC可以發送32位元組命令，其包括用於指定安全域ID的1位元組資料，並且其中其他31位元

組被忽略、不相關或包含用於除了標識安全域之外的目的的資訊。該指令可以與SOC執行Cas-2命令一起、同時或基本上同時發送，使得記憶體設備的存取控制可以將寫入和Cas-2命令與指定的安全域ID相關聯。這樣，存取控制可以被配置為當跨越一個匯流排介面接收Cas-2命令時，跨越另一個匯流排介面專閘監視對包括安全域ID的指令的接收。例如，如參考圖3所描述的，存取控制硬體塊130可以跨越連接216d、216接收Cas-2命令，並且可以跨越連接304i接收安全域ID。表8-11僅僅是允許SOC從記憶體設備讀取32位元組的實例的說明。可以執行寫入命令，以便以與讀取命令類似的方式將32個位元組寫入到與安全域ID相對應的記憶體位置(亦即，利用在JEDEC命令中的「寫入」代替「讀取」)。為了減少管理負擔，額外的操作模式是：一旦安全域ID已經由存取控制硬體塊130接收，則可以成功地接收與最近的安全域ID相對應的後續讀取或寫入命令，而不需要重新發送新的安全域ID。SOC 140可以經由向RAM 122發送全部屬於相同安全域ID的複數個讀取或寫入事務，來利用該機會，例如存取控制硬體塊130將保留當前安全域ID並將其應用於後續的讀取或寫入事務，直到接收到新的安全域ID為止。將具有相同ID的事務進行附隨可以因此消除在表5、6和7中的不必要的安全域ID設置。

【0075】 表12-14示出實現JEDEC協定以指定安全域ID的另一實例格式。

表12

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
MRW-1		cmd*	cmd*	cmd*				ID**	1
		Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	Mode addr	2

表13

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
MRW-2		cmd*	cmd*	cmd*				ID**	1
							ID**	ID**	2

表14

Cmd	CS	CA0	CA1	CA2	CA3	CA4	CA5	CA6	CK
讀取		cmd*	cmd*	cmd*					1
									2

【0076】 表12-14僅僅是允許SOC從記憶體設備讀取32位元組的實例的說明。可以執行寫入命令，以便以與讀取命令類似的方式將32個位元組寫入到與安全域ID相對應的記憶體位置（亦即，利用在JEDEC命令中的「寫入」代替「讀取」）。再次，最近的安全域ID可以仍然是活躍的，並且SOC 140可以附隨（發佈連續的）與相同安全域ID相對應的讀取或寫入事務，並且減少在表12和13中花費的管理負擔。

【0077】 返回參照圖4，在方塊418中，SOC可以實現新的存取控制策略、程式，或可能已經使記憶體緩衝器分配更新，並且因此可能需要基於更新的SOC記憶體緩衝器分配

來重新配置記憶體設備存取控制。當決定已經重新配置或更新SOC記憶體緩衝器分配時，可以重複在方塊408-416中所描述的程序以重新配置記憶體設備的存取控制。利用未反映到記憶體設備存取控制的經更新的記憶體來實現SOC將導致錯誤，並且因此需要重新配置記憶體設備以適應針對SOC側用例的經更新的記憶體分配。

【0078】 圖5是示出根據一些實施例的包括用於提供安全的在記憶體設備內的存取控制的資料和配置事務路徑的實例計算系統500的部件方塊圖。參考圖1-5，系統500可以包括CPU 104，CPU 104可以包括安全實體（例如，熔絲、信任區）502和HLOS 504。系統500可以包括RAM 122，RAM 122可以包括策略資料結構506。系統可以包括各種硬體塊和路徑以實現配置模式事務和任務模式資料事務，其中兩組事務是經由相同的介面PHY 124中繼的。

【0079】 配置模式事務可以由PHY 124中繼到存取控制配置塊132，其中路徑508包括用於中繼位址和資料資訊的連接，以及用於中繼存取域資訊的連接514i。經由路徑508中繼的資料可以包括用於配置存取控制配置塊132的基底位址、大小或位址範圍以及安全域ID，以準備任務模式資料事務。跨越路徑508中繼的配置事務可以如參考方法400（圖4）的方塊414所描述的來執行。

【0080】 任務模式資料事務可以由PHY 124中繼到策略實施塊136，其中路徑510包括用於中繼位址和資料資訊的連接，以及用於中繼存取域資訊的連接512i。經由路徑510

中繼的資訊可以包括位址資訊和資料，以從RAM單元陣列138內的特定位置進行讀取或向其進行寫入。經由路徑510中繼的任務模式資料事務可以如參考方法400（圖4）的方塊416所描述的來執行。

【0081】 圖6是示出根據一些實施例的用於監視安全的在記憶體設備內的存取違規的方法600的程序流程圖。參考圖1-6，方法600的操作可以由SOC（例如，SOC 140）的處理器（例如，CPU 104、NPU 308）和外部記憶體設備（例如，RAM 122）的存取控制硬體塊（例如，130）來執行。

【0082】 在方塊602-620中執行的操作的順序僅僅是說明性的，並且在一些實施例中，方塊602-620的操作可以以任何循序執行並且部分地同時執行。在一些實施例中，方法600可以由設備的處理器獨立於外部記憶體設備但與外部記憶體設備結合地執行。例如，方法600可以被實現為在SOC的處理器內執行的軟體模組，或者在SOC內的專用硬體中實現，該SOC發佈命令以嘗試存取外部記憶體設備的記憶體，並且另外被配置為採取動作和儲存資料，如所描述的。

【0083】 在方塊602中，記憶體設備的存取控制可以由存取控制硬體塊來配置和啟用。這可以如參考方法400（圖4）的方塊402-414所描述的來執行，使得SOC配置記憶體設備的存取控制硬體塊的存取控制以允許SOC從在記憶體設備單元陣列內的記憶體進行讀取及/或向其進行寫入。

【0084】 在方塊604中，SOC處理器可以將存取請求連同存取控制ID一起發送到SOC記憶體控制器。例如，如參考圖3所描述的，CPU 104可產生記憶體存取請求以存取在RAM單元陣列138內的特定記憶體。存取請求可以由CPU 104跨越匯流排118發送到RAM記憶體控制器110。存取請求可以包括存取控制ID（例如，安全域ID）以標識CPU 104是請求源。作為另一實例，NPU 308可以向RAM記憶體控制器110發送包括存取控制ID的存取請求，其中NPU 308的存取控制ID不同於CPU 104的存取控制ID。

【0085】 在方塊606中，SOC記憶體控制器可以回應於從SOC處理器接收存取請求，向記憶體設備發送包括存取控制ID的讀/寫命令。這可以如參考方法400（圖4）的方塊416所描述的來執行。

【0086】 在方塊608中，存取控制硬體塊可以將存取請求與存取控制配置進行比較。例如，如參考圖3所描述的，在存取控制硬體塊130內的策略實施塊136可以從PHY 124接收存取請求，並且基於在方塊602中配置的存取控制配置來決定包括讀/寫命令的存取請求是否是可允許的。在存取控制硬體塊130內的策略實施塊136可以分析存取請求以決定基底位址、位址範圍和安全域ID，並且接著將記憶體資訊和安全域ID與記憶體存取控制配置進行比較（例如，如由存取控制配置塊132所定義的）。所標識的記憶體位置和範圍可以用於標識在RAM記憶體單元陣列138內的記憶體資訊。安全ID可以標識SOC的初始化存取請求的

安全域，使得該安全域ID與在所標識的記憶體位址和範圍處請求讀/寫操作的安全域相對應。

【0087】 在決定方塊610中，記憶體設備的存取控制硬體塊130可以基於存取請求和存取控制配置，來決定是否應當准許SOC對記憶體設備記憶體單元陣列的存取。存取控制硬體塊130可以被配置為允許（例如實施策略實施塊136）基於特定的安全域ID和對應的記憶體位址位置和範圍的對記憶體單元陣列的存取請求，同時拒絕指定未包括在記憶體存取控制的配置中的其他安全域ID的存取請求。

【0088】 例如，圖7示出根據一些實施例的用於提供安全的在記憶體設備內的存取控制的系統記憶體映射700。對於該實例，可假定SOC的CPU歸於安全域ID 0，且同一SOC的NPU歸於安全域ID 1。在記憶體存取控制的配置期間，記憶體設備可以接收包括與CPU和NPU相對應的安全域ID 0和1的配置訊息。配置訊息可以包括記憶體設備基於對應的安全域ID應當允許對其的存取的記憶體位址位置和範圍。例如，如在方法400（圖4）中所描述的，記憶體設備可能已經接收到配置訊息以配置存取控制，以允許由NPU和CPU針對記憶體位址範圍704請求的讀/寫操作，並且允許由CPU對記憶體位址範圍702的讀/寫操作，而不允許由NPU對記憶體位址範圍702的讀/寫操作。作為另一實例，存取控制可能已經被配置為允許對除了CPU以外對記憶體位址範圍702的讀取操作而不允許寫入操作，使得除了CPU以外的包括NPU安全域的所有其他安全域不可以

對記憶體位址範圍702進行寫入。因此，若NPU執行操作706以請求寫入到記憶體位址範圍702，則記憶體設備的策略實施可檢查請求包括安全域ID 1，決定僅允許包括安全域ID 0的請求寫入到記憶體位址範圍702，並且可以拒絕請求。

【0089】 返回參考圖6，回應於基於存取控制配置決定存取請求的記憶體位址位置和範圍以及安全域ID是不允許的（亦即，決定方塊610 =「否」），則可以不執行存取請求的讀/寫，可以記錄包括存取請求資訊的錯誤（例如，經由存取違規特徵群塊134），並且可以在方塊604中執行新的存取請求。

【0090】 回應於基於存取控制配置決定存取請求的記憶體位址位置和範圍以及安全域ID是允許的（亦即，決定方塊610 =「是」），則可以在方塊612中執行存取請求的讀/寫。方塊608、610和612可以允許複數個讀及/或寫事務在不必在方塊604和606中重新發送存取控制ID的情況下進行。若這樣，則所有事務將如同屬於已經在方塊604和606中提供的當前安全域ID一樣進行處理，並且各個讀或寫事務之每一者讀或寫事務將對照當前安全域ID進行評估，並且單獨地准許或拒絕存取。

【0091】 在方塊614中，SOC記憶體控制器鎖存回應資料並分析錯誤指示訊號。例如，如參考圖3所描述的，在發送到策略實施塊136的存取請求期間，或者在對RAM單元陣列138的讀/寫操作期間，可能已經發生一或多個錯誤。存

取違規特徵群可以記錄任何錯誤，並且隨後在SOC發送取回錯誤資訊的命令請求時跨越連接304e和302e將錯誤資訊發送到SOC。RAM記憶體控制器110隨後可以在執行讀/寫操作之後鎖存回應資料（例如，在連接120d處），並且可以檢查連接302e以決定是否存在指示在存取請求及/或讀/寫操作期間是否發生任何錯誤的錯誤訊號。

【0092】 在決定方塊616中，SOC可以基於從記憶體設備接收的錯誤訊號來決定是否發生錯誤。回應於決定沒有發生錯誤（亦即，決定方塊410 =「否」），不向SOC報告錯誤中斷，並可根據方塊604執行新的存取請求。

【0093】 回應於決定發生錯誤（亦即，決定方塊410 =「是」），SOC記憶體控制器可在方塊618中從記憶體設備請求錯誤資訊。由存取違規特徵群擷取的錯誤資訊可以由記憶體設備發送到SOC。

【0094】 在方塊620中，SOC記憶體控制器可以保存並且在本機存放區錯誤資訊，並且接著對SOC主控制器觸發中斷以執行任何必要操作來記錄及/或修復存取及/或讀/寫錯誤。

【0095】 圖8是示出根據一些實施例的用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的程序流程圖。參考圖1-8，方法800的操作可以由在與SOC（例如，SOC 140）的外部處理器（例如，CPU 104、NPU 308）進行電通訊的記憶體設備（例如，RAM 122）中的存取控制硬體塊（例如，130）來執行。

【0096】 在方塊802-810中執行的操作的順序僅僅是說明性的，並且在一些實施例中，方塊802-810的操作可以以任何循序執行並且部分地同時執行。在一些實施例中，方法800可以由在記憶體設備內的存取控制硬體塊獨立於SOC的外部處理器但與SOC的外部處理器結合地執行。例如，方法800可以被實現為存取控制硬體塊，該存取控制硬體塊可以是在記憶體設備內的執行從SOC的處理器接收的記憶體存取控制配置和任務模式命令的專用硬體。

【0097】 在方塊802中，存取控制硬體塊可以執行包括以下操作的操作：從SOC接收用於配置記憶體設備的記憶體存取控制的配置訊息。在一些實施例中，配置訊息可以包括由記憶體設備的存取控制硬體塊用於配置存取控制的配置安全域ID。在一些實施例中，配置訊息可以是包括配置安全域ID的經編碼的JEDEC訊息。

【0098】 在方塊804中，存取控制硬體塊可以執行包括以下操作的操作：基於配置訊息來配置記憶體存取控制。

【0099】 在方塊806中，存取控制硬體塊可以執行包括以下操作的操作：從SOC接收請求存取記憶體設備的記憶體單元陣列的記憶體基底位址和記憶體存取範圍的存取請求訊息。在一些實施例中，存取請求訊息可以包括讀/寫操作。在一些實施例中，存取請求訊息可以包括用於標識請求SOC的哪個安全域進行讀/寫操作的請求的安全域ID。在一些實施例中，存取請求訊息可以是包括請求的安全域ID的經編碼的JEDEC訊息。

【0100】 在方塊808中，存取控制硬體塊可以執行包括以下操作的操作：將存取請求訊息與所配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的。

【0101】 在方塊810中，存取控制硬體塊可以執行包括以下操作的操作：回應於決定存取請求訊息是可允許的，允許讀/寫操作。

【0102】 圖9是示出根據一些實施例的可以由存取控制硬體塊執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。參考圖1-9，方法900的操作可以由在與SOC（例如，SOC 140）的外部處理器（例如，CPU 104、NPU 308）進行電通訊的記憶體設備（例如，RAM 122）中的存取控制硬體塊（例如，130）來執行。

【0103】 在執行方法800的方塊808的操作（圖8）之後，在方塊902中，記憶體設備的存取控制硬體塊可以執行包括以下操作的操作：決定配置安全域ID與請求的安全域ID是否匹配。這可以作為在方法800（圖8）的方塊808中描述的操作的一部分來執行。

【0104】 在方塊904中，存取控制硬體塊可以執行包括以下操作的操作：回應於決定配置安全域ID與請求的安全域ID匹配，決定存取請求訊息是可允許的。

【0105】 存取控制硬體塊隨後可以執行如所描述的方法800（圖8）的方塊810的操作。

【0106】 圖10是示出根據一些實施例的可以由記憶體設備的存取控制硬體塊執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。參考圖1-10，方法1000的操作可以由與SOC（例如，SOC 140）的外部處理器（例如，CPU 104、NPU 308）進行電通訊的記憶體設備（例如，RAM 122）的存取控制硬體塊（例如，130）來執行。

【0107】 在執行方法800（圖8）的方塊808的操作之後，在方塊1002中，記憶體設備的存取控制硬體塊可以執行包括以下操作的操作：回應於決定配置安全域ID與請求的安全域ID不匹配，決定存取請求訊息是不可允許的。這可以作為在方法800（圖8）的方塊808中描述的程序的一部分來執行。

【0108】 在方塊1004中，存取控制硬體塊可以執行包括以下操作的操作：儲存包括記憶體基底位址、記憶體存取範圍和請求的安全域ID的錯誤資訊。

【0109】 在方塊1006中，存取控制硬體塊可以執行包括以下操作的操作：將錯誤資訊發送到SOC。

【0110】 圖11是示出根據一些實施例的可以由記憶體設備的信任硬體塊執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。參考圖1-11，方法1100的操作可以由與SOC（例如，SOC 140）的外部

處理器（例如，CPU 104、NPU 308）進行電通訊的記憶體設備（例如，RAM 122）的信任硬體塊（例如，125）來執行。

【0111】 在方塊1102中，記憶體設備的信任硬體塊可以執行包括以下操作的操作：從SOC接收解鎖密碼。

【0112】 在方塊1104中，信任硬體塊可以執行包括以下操作的操作：決定所接收的解鎖密碼與在被儲存在記憶體設備中的可接受密碼集合內的密碼是否匹配。

【0113】 在方塊1106中，信任硬體塊可以執行包括以下操作的操作：回應於決定所接收的解鎖密碼與在可接受密碼集合內的密碼相匹配，解鎖記憶體設備閘邏輯以允許存取控制硬體塊來接收配置訊息。

【0114】 存取控制硬體塊隨後可以執行如所描述的方法800（圖8）的方塊802的操作。

【0115】 圖12是示出根據一些實施例的可以由記憶體設備執行的作為用於經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的方法800的一部分的替代操作的程序流程圖。參考圖1-12，方法1200的操作可以由與SOC（例如，SOC 140）的外部處理器（例如，CPU 104、NPU 308）進行電通訊的記憶體設備（例如，RAM 122）的存取控制硬體塊（例如，130）來執行。

【0116】 在執行方法800（圖8）的方塊804的操作之後，在方塊1202中，記憶體設備的存取控制硬體塊可以執行包

括以下操作的操作：從SOC接收被配置為設置在記憶體設備的暫存器內的鎖定位元的鎖定命令。

【0117】 在方塊1204中，存取控制硬體塊可以執行包括以下操作的操作：設置鎖定位元以防止對所配置的記憶體存取控制的配置改變。

【0118】 存取控制硬體塊隨後可以執行如所描述的方法800（圖8）的方塊806的操作。

【0119】 各種實施例可以在諸如可穿戴計算設備之類的各種計算設備內實現。圖13示出根據一些實施例的以智慧手錶1300的形式的實例可穿戴計算設備。智慧手錶1300可以包括耦合到內部記憶體1304和1306的處理器1302。內部記憶體1304、1306可以是揮發性或非揮發性記憶體，並且亦可以是安全及/或加密的記憶體，或不安全及/或未加密的記憶體，或其任何組合。處理器1302亦可耦合到觸控式螢幕顯示器1320，諸如電阻式感測觸控式螢幕、電容式感測觸控式螢幕、紅外感測觸控式螢幕等。另外，智慧手錶1300可具有可以連接到一或多個無線資料連結1312的用於發送和接收電磁輻射的一或多個天線1308，諸如一或多個藍芽®收發機、Peanut收發機、Wi-Fi收發機、ANT+收發機等，其可耦合到處理器1302。智慧手錶1300亦可以包括用於接收使用者輸入的實體虛擬按鈕1322和1310以及用於接收使用者輸入的滑動感測器1316。

【0120】 無線資料連結1312和所連接的收發機可以用於與外部記憶體設備（諸如耦合到回應無線收發機的

RAM/NVRAM）進行電配對和通訊。例如，如參考圖3所描述的，智慧手錶1300可以與外部記憶體設備（例如，RAM 122）臨時配對，使得處理器（例如，CPU 104）可以配置存取控制配置塊132，以準備發佈存取記憶體設備的記憶體（例如，RAM單元陣列138）的命令。

【0121】 觸控式螢幕顯示器1320可以耦合到觸控式螢幕介面模組，該觸控式螢幕介面模組被配置為從觸控式螢幕顯示器1320接收指示在螢幕上的使用者的指尖或觸筆正在觸摸表面的位置的訊號，並且將關於觸摸事件的座標的資訊輸出到處理器1302。此外，處理器1302可以配置有處理器可執行指令以將呈現在觸控式螢幕顯示器1320上的圖像與從觸控式螢幕介面模組接收的觸摸事件的位置相關聯，以便偵測使用者何時與圖形介面圖示（例如，虛擬按鈕）互動。

【0122】 處理器1302可以是可以由軟體指令（應用程式）配置以執行各種功能（包括各種實施例的功能）的任何可程式設計微處理器、微型電腦或一或多個多處理器晶片。在一些設備中，可以提供多個處理器，諸如專用於無線通訊功能的一個處理器以及專用於執行其他應用程式的一個處理器。通常，軟體應用程式可在其被存取並載入到處理器1302中之前儲存在內部記憶體中。處理器1302可以包括足以儲存應用程式軟體指令的內部記憶體。在許多設備中，內部記憶體可以是揮發性或非揮發性記憶體（諸如快閃記憶體），或者是兩者的混合。出於本描述的目的，對

記憶體的一般引用是指可由處理器1302存取的記憶體，包括內部記憶體或插入到行動裝置中的可移除記憶體以及在處理器1302自身內的記憶體。

【0123】 圖14是根據一些實施例的可以經由片上系統（SOC）提供對記憶體設備的安全的在記憶體設備內的存取的網路計算設備1400的實例的部件方塊圖。參考圖1-14，網路計算設備1400可以用作通訊網路的網路元件，諸如基地台。網路計算設備1400可以包括耦合到揮發性記憶體1402和大容量非揮發性記憶體1408（例如，RAM 122）的處理器1410（例如，CPU 104、NPU 308）。網路計算設備1400亦可以包括耦合到處理器1410的周邊記憶體存取設備，諸如軟碟機、壓縮磁碟（CD）或數位視訊盤（DVD）驅動器1406。網路計算設備1400亦可以包括耦合到處理器1410的用於建立與網路的資料連接的網路存取埠1404（或介面），該網路諸如耦合到其他系統電腦和伺服器的網際網路或區域網路。網路計算設備1400可以包括可以連接到無線通訊鏈路的用於發送和接收電磁輻射的一或多個天線1404。網路計算設備1400可以包括用於耦合到周邊設備、外部記憶體或其他設備的額外的存取埠，諸如USB、火線、Thunderbolt等。

【0124】 圖15是適於實現一些實施例的以智慧型電話1500的形式的實例無線設備的部件方塊圖。參考圖1-15，智慧型電話1500可以包括耦合到第二SOC 1502（例如，具有5G能力的SOC）的第一SOC 140（例如，

SOC-CPU）。第一SOC 140和第二SOC 1502可以耦合到內部記憶體1516（例如SRAM 106）、顯示器1512和揚聲器1514。另外，智慧型電話1500可以包括用於發送和接收電磁輻射的天線1504，該天線1504可以連接到無線資料連結或耦合到在第一SOC 140或第二SOC 1502中的一或多個處理器的蜂巢式電話收發機1508。例如，天線1504可以用於電連接到外部記憶體設備（例如，RAM 122）並且向外部記憶體設備發佈配置和任務模式記憶體存取命令。智慧型電話1500通常亦包括用於接收使用者輸入的功能表選擇按鈕或搖臂開關1520。

【0125】 典型的智慧型電話1500亦包括聲音編碼/解碼（CODEC）電路1510，其將從麥克風接收的聲音數位化為適合於無線傳輸的資料封包，並且解碼所接收的聲音資料封包以產生類比訊號，該類比訊號被提供給揚聲器以產生聲音。而且，在第一SOC 140和第二SOC 1502中的一或多個處理器、無線收發機1508和CODEC 1510可以包括數位訊號處理器（DSP）電路（未單獨示出）。

【0126】 智慧手錶1300、無線網路計算設備1400和智慧型電話1500的處理器可以是可由處理器可執行指令配置以執行各種功能的任何可程式設計微處理器、微型電腦或一或多個多處理器晶片，包括本文描述的各種實施例的功能。在一些無線設備中，可提供多個處理器，諸如在SOC 1502內的專用於無線通訊功能的一個處理器和在SOC 140內的專用於執行其他應用程式的一個處理器。通常，

軟體應用（例如，可信程式102、306）可在其被存取並載入到處理器中之前儲存在記憶體1506、1516中。處理器可以包括足以儲存應用軟體指令的內部記憶體。

【0127】 如在本案中所使用的，術語「部件」、「模組」、「系統」等意欲包括電腦相關實體，諸如但不限於被配置為執行特定操作或功能的硬體、韌體、硬體和軟體的組合、軟體、或執行中的軟體。例如，部件可以是，但不限於，在處理器上執行的程序、處理器、物件、可執行檔、執行執行緒、程式或電腦。經由實例的方式，在無線設備上執行的應用程式和無線設備兩者皆可稱為部件。一或多個部件可以位元在程序或執行的執行緒內，並且部件可以位於一個處理器或核心上，或者分佈在兩個或兩個以上處理器或核心之間。另外，這些部件可從具有在其上儲存的各種指令或資料結構的各種非暫時性電腦可讀取媒體執行。部件可以經由本端或遠端程序、函數或程式撥叫、電子訊號、資料封包、記憶體讀/寫、以及其他已知的網路、電腦、處理器或程序相關的通訊方法來進行通訊。

【0128】 所示出和描述的各種實施例僅是作為實例而提供的，以說明請求項的各種特徵。然而，關於任何給定實施例示出和描述的特徵不一定限於相關聯的實施例，並且可以與示出和描述的其他實施例一起使用或組合。此外，請求項不意欲受任何一個實例實施例的限制。例如，本文揭示的方法的一或多個操作可以替代本文揭示的方法的一或多個操作或與其組合。

【0129】 前述方法描述和程序流程圖僅是作為說明性實例而提供的，並且不意欲要求或暗示各種實施例的方塊可以以所呈現的循序執行。如本發明所屬領域中具有通常知識者將理解的，在前述實施例中的方塊的順序可以以任何循序執行。諸如「其後」、「隨後」、「接下來」等詞語不意欲限制方塊的順序；這些詞語僅用於引導讀者通讀對方法的描述。此外，任何對單數形式的請求項元素的引用，例如使用冠詞「一」、「一個」或「該」不應被解釋為將該元素限制為單數。

【0130】 如本文所使用的，提及項目列表中的「至少一個」的短語是指那些項目的任何組合，包括單個成員。作為實例，「a、b或c中的至少一個」意欲涵蓋：a、b、c、a-b、a-c、b-c和a-b-c。

【0131】 結合本文所揭示的實施例而描述的各種說明性邏輯方塊、模組、電路和演算法方塊可以被實現為電子硬體、電腦軟體或兩者的組合。為了清楚地說明硬體與軟體的這種可互換性，上文已經大體上在其功能性態樣描述了各種說明性部件、方塊、模組、電路和方塊。這樣的功能是實現為硬體還是軟體取決於特定應用和施加於整個系統的設計約束。本發明所屬領域中具有通常知識者可以針對每個特定應用以不同方式實施所描述的功能性，但此類實施例決策不應被解釋為導致脫離各種實施例的範疇。

【0132】 用於實現結合本文所揭示的各態樣描述的各種說明性邏輯、邏輯方塊、模組和電路的硬體和資料處理裝置

可以利用被設計為執行本文所描述的功能的通用單晶片或多晶片處理器、數位訊號處理器（DSP）、特殊應用積體電路（ASIC）、現場可程式設計閘陣列（FPGA）或其他可程式設計邏輯裝置、個別閘閘或電晶體邏輯、個別硬體部件或其任何組合來實現或執行。通用處理器可以是微處理器，或任何一般處理器、控制器、微控制器或狀態機。處理器亦可以被實現為組合，諸如DSP和微處理器的組合、複數個微處理器、一或多個微處理器與DSP核心的結合、或者任何其他這樣的配置。在一些實施例中，特定的程序和方法可以由特定於給定功能的電路來執行。

【0133】 在一或多個態樣中，所描述的功能可以以硬體、數位電子電路、電腦軟體、韌體來實現，包括在本說明書中揭示的結構及其結構等同方案，或者以其任何組合實現。在本說明書中描述的主題的實施例亦可以被實現為一或多個電腦程式，亦即，一或多個電腦程式指令的模組，其被編碼在電腦儲存媒體上以供資料處理裝置執行或控制資料處理裝置的操作。

【0134】 用於在可程式設計處理器上執行以執行各種實施例的操作的電腦程式代碼或「程式碼」可以用高級程式設計語言來編寫（諸如C、C++、C#、Smalltalk、Java、JavaScript、Visual Basic、結構化查詢語言（例如，Transact-SQL）、Perl）或用各種其他程式設計語言來編寫。如本案中所使用的儲存在電腦可讀取儲存媒體上的

程式碼或程式可以指代其格式可由處理器理解的機器語言代碼（諸如目標代碼）。

【0135】 若以軟體實施，則所述功能可以作為一或多個指令或代碼儲存在電腦可讀取媒體上或經由電腦可讀取媒體進行傳輸。本文所揭示的方法或演算法的程序可以在可以駐存在電腦可讀取媒體上的處理器可執行軟體模組中實現。電腦可讀取媒體包括電腦儲存媒體與通訊媒體兩者，該通訊媒體包括可以被啟用以將電腦程式從一個地方傳送到另一地方的任何媒體。儲存媒體可以是可以由電腦存取的任何可用媒體。經由實例而非限制的方式，這樣的電腦可讀取媒體可以包括RAM、ROM、EEPROM、CD-ROM或其他光碟儲存、磁碟儲存或其他磁性存放裝置，或可以用於以指令或資料結構的形式儲存期望的程式碼並且可以由電腦存取的任何其他媒體。而且，任何連接可適當地稱為電腦可讀取媒體。如本文所使用的，磁碟和光碟包括壓縮光碟（CD）、鐳射光碟、光學光碟、數位多功能光碟（DVD）、軟碟和藍光光碟，其中磁碟通常磁性地複製資料，而光碟用鐳射光學地複製資料。以上的組合亦應當被包括在電腦可讀取媒體的範疇內。另外，方法或演算法的操作可以作為代碼和指令中的一個或任何組合或集合駐存在機器可讀取媒體和電腦可讀取媒體上，該機器可讀取媒體和電腦可讀取媒體可併入到電腦程式產品中。

【0136】 對本案中描述的實施例的各種修改對於本發明所屬領域中具有通常知識者可以是顯而易見的，並且本文定

義的一般原理可以在不脫離請求項的範疇的情況下應用於其他實施例。因此，請求項不意欲限於本文所示的實施例，而是要被賦予與本案內容、本文揭示的原理和新穎特徵一致的最廣範疇。

【符號說明】

【0137】

100：計算系統

102：可信程式

104：中央處理單元（CPU）

106：靜態RAM（SRAM）

108：唯讀記憶體（ROM）

110：RAM記憶體控制器

112：前端

114：介面控制

116：實體介面（PHY）

118：匯流排

120：外部匯流排

120c：連接

120d：連接

122：RAM

124：PHY

125：信任硬體塊

126：閘

128：熔絲

130：存取控制硬體塊

132：存取控制配置塊

134：存取違規特徵群塊

136：策略實施塊

138：RAM單元陣列

140：SOC

142：儲存記憶體控制器

144：存取儲存記憶體

146：熔絲

200：系統

202：通過閘

204：控制邏輯

206：方塊

208：方塊

210：方塊

212：控制器

214c：位址/控制連接

214d：資料連接

216c：閘控位址/控制連接

216d：閘控連接

218：連接

220：熔絲資料匯流排

222：熔絲控制匯流排

224c：控制匯流排

224d:資料匯流排

300:計算系統

302e:連接

302i:連接

304e:連接

304i:連接

400:方法

402:方塊

404:方塊

406:方塊

408:方塊

410:方塊

412:方塊

414:方塊

416:方塊

418:方塊

500:系統

502:安全實體

504:HLOS

506:策略資料結構

508:路徑

510:路徑

512i:連接

514i:連接

600：方 法

602：方 塊

604：方 塊

606：方 塊

608：方 塊

610：方 塊

612：方 塊

614：方 塊

616：方 塊

618：方 塊

620：方 塊

700：系 統 記 憶 體 映 射

702：記 憶 體 位 址 範 圍

704：記 憶 體 位 址 範 圍

706：操 作

800：方 法

802：方 塊

804：方 塊

806：方 塊

808：方 塊

810：方 塊

900：方 法

902：方 塊

904：方 塊

1000：方法

1002：方塊

1004：方塊

1006：方塊

1100：方法

1102：方塊

1104：方塊

1106：方塊

1200：方法

1202：方塊

1204：方塊

1300：智慧手錶

1302：處理器

1304：內部記憶體

1306：內部記憶體

1308：天線

1310：實體虛擬按鈕

1312：無線資料連結

1316：滑動感測器

1320：觸控式螢幕顯示器

1322：實體虛擬按鈕

1400：網路計算設備

1402：揮發性記憶體

1404：網路存取埠

1406:數位視訊盤（DVD）驅動器

1408:大容量非揮發性記憶體

1500:智慧型電話

1502:第二SOC

1504:天線

1506:記憶體

1508:蜂巢式電話收發機

1510:聲音編碼/解碼（CODEC）電路

1512:顯示器

1514:揚聲器1

1516:內部記憶體

1520:功能表選擇按鈕或搖臂開關

【發明申請專利範圍】

【請求項1】 一種用於向一片上系統（SOC）指示存取通過/違規回饋作為一記憶體設備的讀/寫事務序列的一部分的方法，其特徵在於包括以下步驟：

從該 SOC 接收一解鎖密碼；

決定所接收的解鎖密碼與被儲存在該記憶體設備中的一可接受密碼集合內的一密碼是否匹配；及

回應於決定所接收的解鎖密碼與在該可接受密碼集合內的一密碼匹配，解鎖記憶體設備閘邏輯以允許一記憶體存取控制來接收一配置訊息；

從該 SOC 接收用於配置該記憶體設備的該記憶體存取控制的該配置訊息；

基於該配置訊息來配置該記憶體存取控制；

從該 SOC 接收請求存取該記憶體設備的一記憶體單元陣列的一記憶體基底位址和一記憶體存取範圍的一存取請求訊息，其中該存取請求訊息包括一讀/寫操作；

將該存取請求訊息與所配置的記憶體存取控制進行比較以決定該存取請求訊息是否是可允許的；及

回應於決定該存取請求訊息是可允許的，執行該讀/寫操作。

【請求項2】 根據請求項 1 之方法，其特徵在於：

該配置訊息包括一配置安全域 ID；及

該存取請求訊息包括一請求的安全域 ID。

【請求項3】 根據請求項 2 之方法，其特徵在於將該存取

請求訊息與所配置的記憶體存取控制進行比較以決定該存取請求訊息是否是可允許的包括：

決定該配置安全域ID與該請求的安全域ID是否匹配；及

回應於決定該配置安全域ID與該請求的安全域ID匹配：

決定該存取請求訊息是可允許的；及

向該SOC發送指示該存取請求訊息是可允許的一通知。

【請求項4】 根據請求項3之方法，進一步其特徵在於包括以下步驟：

回應於決定該配置安全域ID與該請求的安全域ID不匹配：

決定該存取請求訊息是不可允許的；

儲存包括該記憶體基底位址、該記憶體存取範圍和該請求的安全域ID的錯誤資訊；

向該SOC發送指示該存取請求訊息是不可允許的一通知；及

回應於從該SOC接收一錯誤插斷要求，向該SOC發送該錯誤資訊。

【請求項5】 根據請求項2之方法，其特徵在於：

該配置訊息是包括該配置安全域ID的一經編碼的JEDEC訊息；及

該存取請求訊息是包括該請求的安全域ID的一經編

碼的JEDEC訊息。

【請求項6】 根據請求項1之方法，進一步其特徵在於包括以下步驟：

從該SOC接收一鎖定命令，該鎖定命令被配置為設置在該記憶體設備的一暫存器內的一鎖定位元；及

設置該鎖定位元以防止對所配置的記憶體存取控制的配置改變。

【請求項7】 一種記憶體設備，其特徵在於包括：

一記憶體單元陣列；

記憶體設備閘邏輯；

一信任硬體塊，其中該信任硬體塊被配置為執行進一步包括以下操作之操作：

從一片上系統（SOC）接收一解鎖密碼；

決定所接收的解鎖密碼與被儲存在該記憶體設備中的一可接受密碼集合內的一密碼是否匹配；及

回應於決定所接收的解鎖密碼與在該可接受密碼集合內的一密碼匹配，解鎖該記憶體設備閘邏輯以允許一存取控制硬體塊來接收一配置訊息；及

其中該存取控制硬體塊，被配置為執行包括以下操作的操作：

從該SOC接收用於配置該記憶體設備的記憶體存取控制的該配置訊息；

基於該配置訊息來配置該記憶體存取控制；

從該SOC接收請求存取該記憶體單元陣列的一記憶

體基底位址和一記憶體存取範圍的一存取請求訊息，其中該存取請求訊息包括一讀/寫操作；

將該存取請求訊息與所配置的記憶體存取控制進行比較以決定該存取請求訊息是否是可允許的；及

回應於決定該存取請求訊息是可允許的，執行該讀/寫操作。

【請求項8】 根據請求項7之記憶體設備，其特徵在於該存取控制硬體塊被配置為執行操作，使得：

從該SOC接收該配置訊息包括：接收包括一配置安全域ID的一配置訊息；及

從該SOC接收一存取請求訊息包括：接收包括一請求的安全域ID的一存取請求訊息。

【請求項9】 根據請求項8之記憶體設備，其特徵在於該存取控制硬體塊被配置為執行操作，使得將該存取請求訊息與所配置的記憶體存取控制進行比較以決定該存取請求訊息是否是可允許的包括：

決定該配置安全域ID與該請求的安全域ID是否匹配；及

回應於決定該配置安全域ID與該請求的安全域ID匹配：

決定該存取請求訊息是可允許的；及

向該SOC發送指示該存取請求訊息是可允許的一通知。

【請求項10】根據請求項9之記憶體設備，其特徵在於該

存取控制硬體塊被配置為執行亦包括以下操作的操作：

回應於決定該配置安全域ID與該請求的安全域ID不匹配：

決定該存取請求訊息是不可允許的；

儲存包括該記憶體基底位址、該記憶體存取範圍和該請求的安全域ID的錯誤資訊；

向該SOC發送指示該存取請求訊息是不可允許的一通知；及

回應於從該SOC接收一錯誤插斷要求，向該SOC發送該錯誤資訊。

【請求項11】根據請求項8之記憶體設備，其特徵在於該存取控制硬體塊被配置為執行操作，使得：

從該SOC接收該配置訊息包括：接收包括該配置安全域ID的一經編碼的JEDEC訊息；及

從該SOC接收一存取請求訊息包括：接收包括該請求的安全域ID的一經編碼的JEDEC訊息。

【請求項12】根據請求項7之記憶體設備，其特徵在於該存取控制硬體塊被配置為執行亦包括以下操作的操作：

從該SOC接收一鎖定命令，該鎖定命令被配置為設置在該記憶體設備的一暫存器內的一鎖定位元；及

設置該鎖定位元以防止對所配置的記憶體存取控制的配置改變。

【請求項13】根據請求項7之記憶體設備，其特徵在於該信任硬體塊包括：

一熔絲記憶體，其被配置為儲存一可接受密碼集合；

一通過閘，其包括該記憶體設備閘邏輯；及

一邏輯區塊，其耦合到該熔絲記憶體和該通過閘並且被配置為：

決定所接收的解鎖密碼與被儲存在該熔絲記憶體中的該可接受密碼集合內的該密碼是否匹配；及

回應於決定所接收的解鎖密碼與被儲存在該熔絲記憶體中的該可接受密碼集合內的該密碼匹配，向該通過閘發訊號以解鎖該記憶體設備閘邏輯。

【請求項14】根據請求項7之記憶體設備，其特徵在於該存取控制硬體塊包括：

一存取控制配置塊；

一存取違規特徵群；及

一策略實施塊。

【發明圖式】

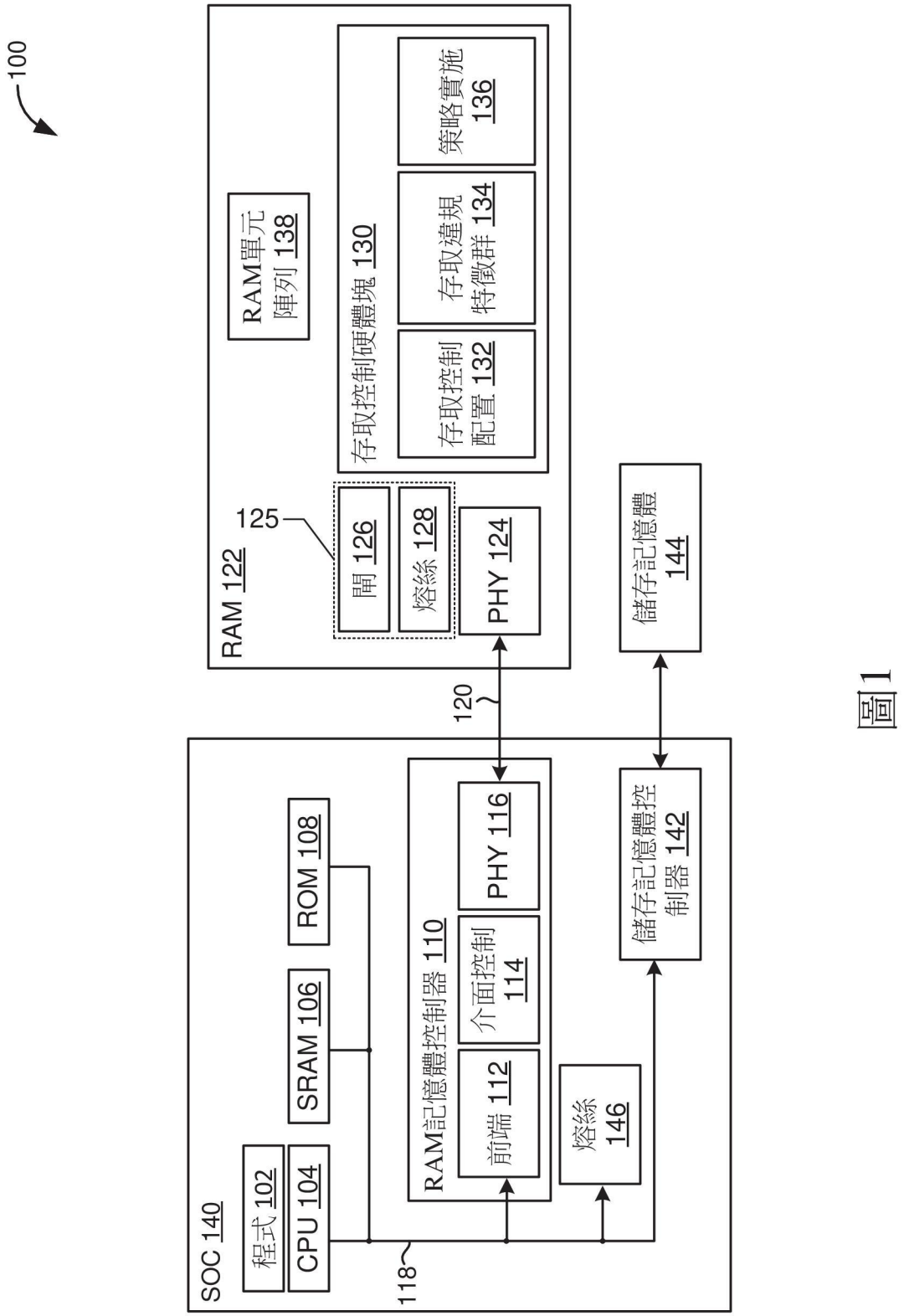
100
RAM 122
125
閘 126
熔絲 128
PHY 124
RAM單元陣列 138
存取控制硬體塊 130
存取控制配置 132
存取違規特徵群 134
策略實施 136
120
儲存記憶體 144
SOC 140
程式 102
CPU 104
SRAM 106
ROM 108
RAM記憶體控制器 110
前端 112
介面控制 114
PHY 116
118
熔絲 146
儲存記憶體控制器 142

圖1

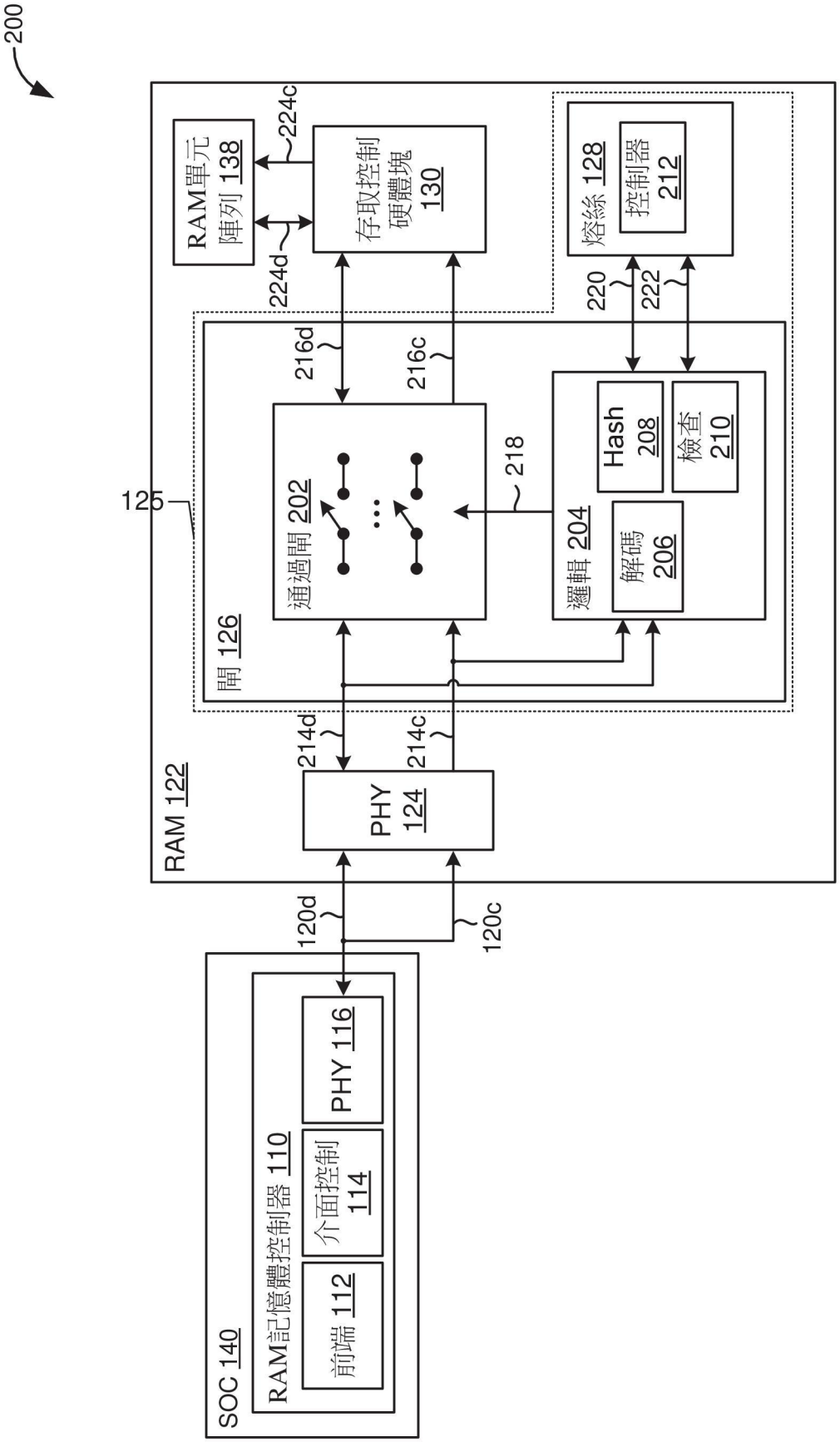
200
RAM 122
PHY 124
214d
214c
120d
120c
SOC 140
RAM記憶體控制器 110
前端 112
介面控制 114
PHY 116
125
閘 126
通過閘 202
216d
216c
218
邏輯 204
解碼 206
Hash 208
檢查 210
RAM單元陣列 138
224c
224d
存取控制硬體塊 130
熔絲 128
控制器 212
220
222

圖2

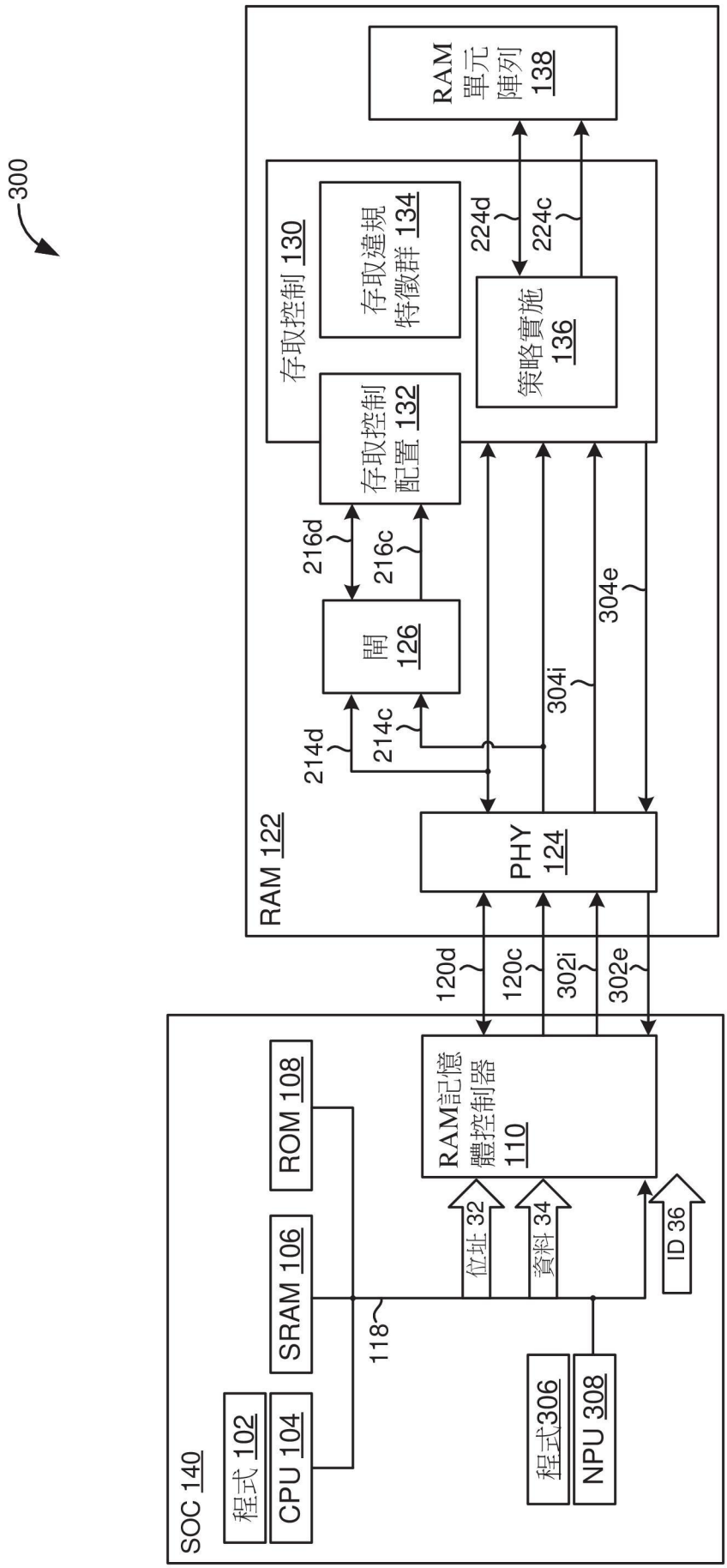
300
SOC 140
程式 102
CPU 104
SRAM 106
ROM 108
118
RAM記憶體控制器 110
位址 32
資料 34
ID 36
程式306
NPU 308
120d
120c
302i
302e
RAM 122
PHY 124
214d
214c
閘 126
216d
216c
存取控制配置 132
存取控制 130
存取違規特徵群 134
策略實施 136
224d
224c
304i
304e
RAM 單元陣列 138

圖3

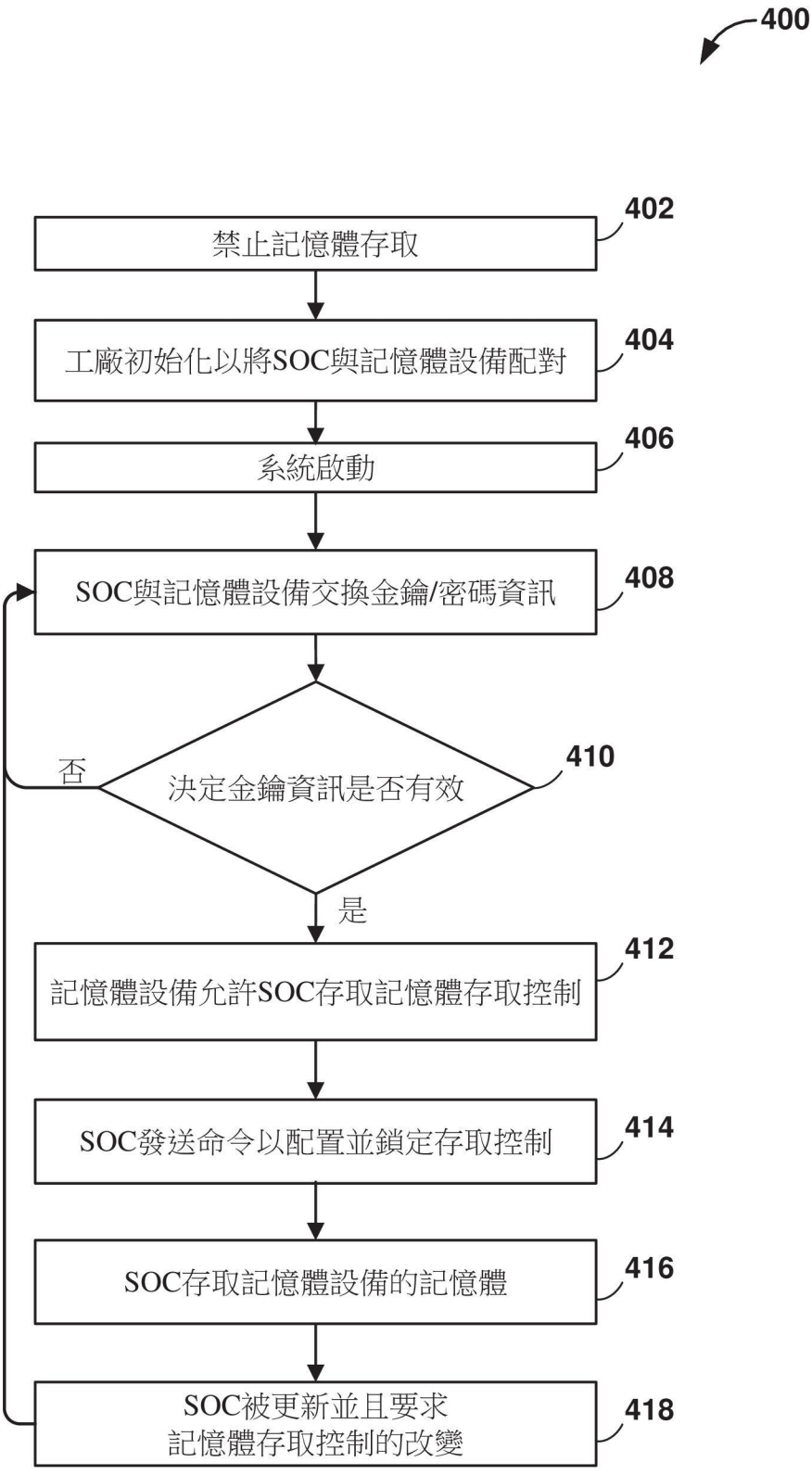
400
402
禁止記憶體存取
404
工廠初始化以將SOC與記憶體設備配對
406
系統啟動
408
SOC與記憶體設備交換金鑰/密碼資訊
410
決定金鑰資訊是否有效
否
是
412
記憶體設備允許SOC存取記憶體存取控制
414
SOC發送命令以配置並鎖定存取控制
416
SOC存取記憶體設備的記憶體
418
SOC被更新並且要求
記憶體存取控制的改變

圖4

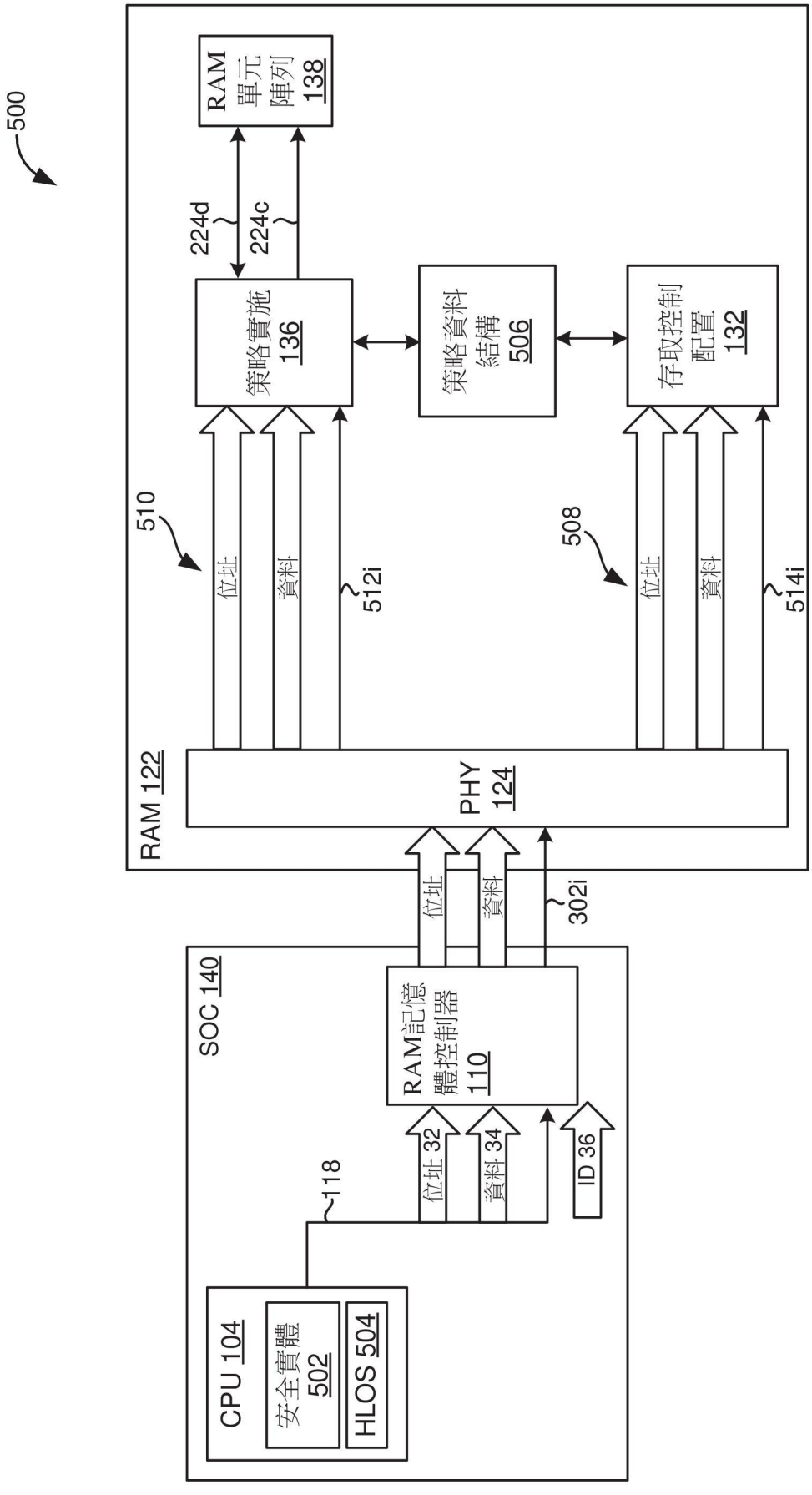
500
RAM 單元陣列 138
224d
224c
策略實施 136
策略資料結構 506
存取控制配置 132
510
位址
資料
512i
508
位址
資料
514i
RAM 122
PHY 124
位址
資料
302i
SOC 140
RAM記憶體控制器 110
位址 32
資料 34
ID 36
118
CPU 104
安全實體 502
HLOS 504

圖5

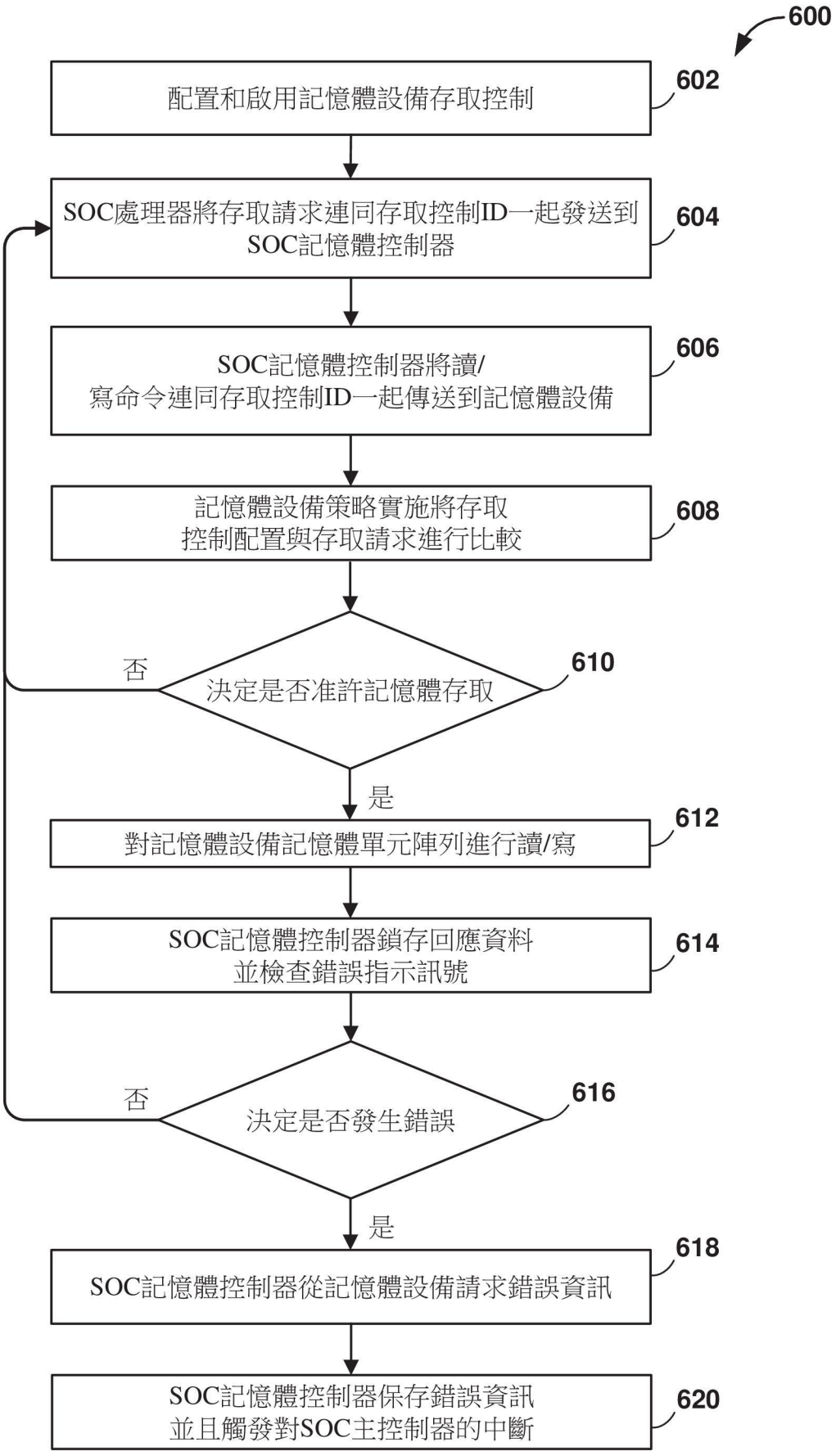
600
配置和啟用記憶體設備存取控制
602
SOC處理器將存取請求連同存取控制ID一起發送到SOC記憶體控制器
604
SOC記憶體控制器將讀/寫命令連同存取控制ID一起傳送到記憶體設備
606
記憶體設備策略實施將存取控制配置與存取請求進行比較
608
決定是否准許記憶體存取
610
否
是
對記憶體設備記憶體單元陣列進行讀/寫
612
SOC記憶體控制器鎖存回應資料並檢查錯誤指示訊號
614
決定是否發生錯誤
616
否
是
SOC記憶體控制器從記憶體設備請求錯誤資訊
618
SOC記憶體控制器保存錯誤資訊並且觸發對SOC主控制器的中斷
620

圖6

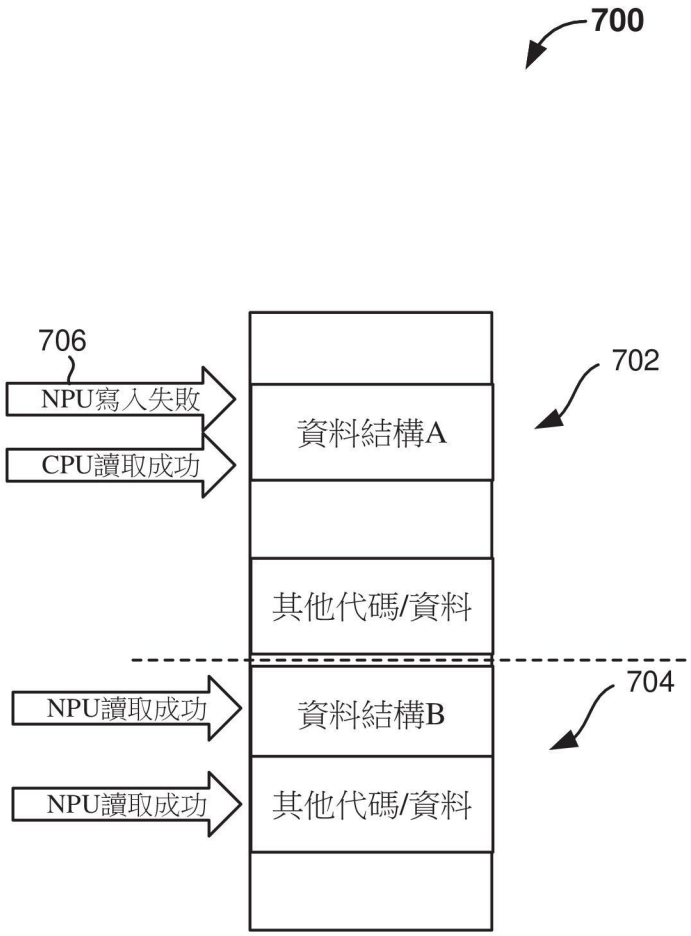
700
706
NPU寫入失敗
CPU讀取成功
資料結構A
702
其他代碼/資料
NPU讀取成功
資料結構B
704
NPU讀取成功
其他代碼/資料

圖7

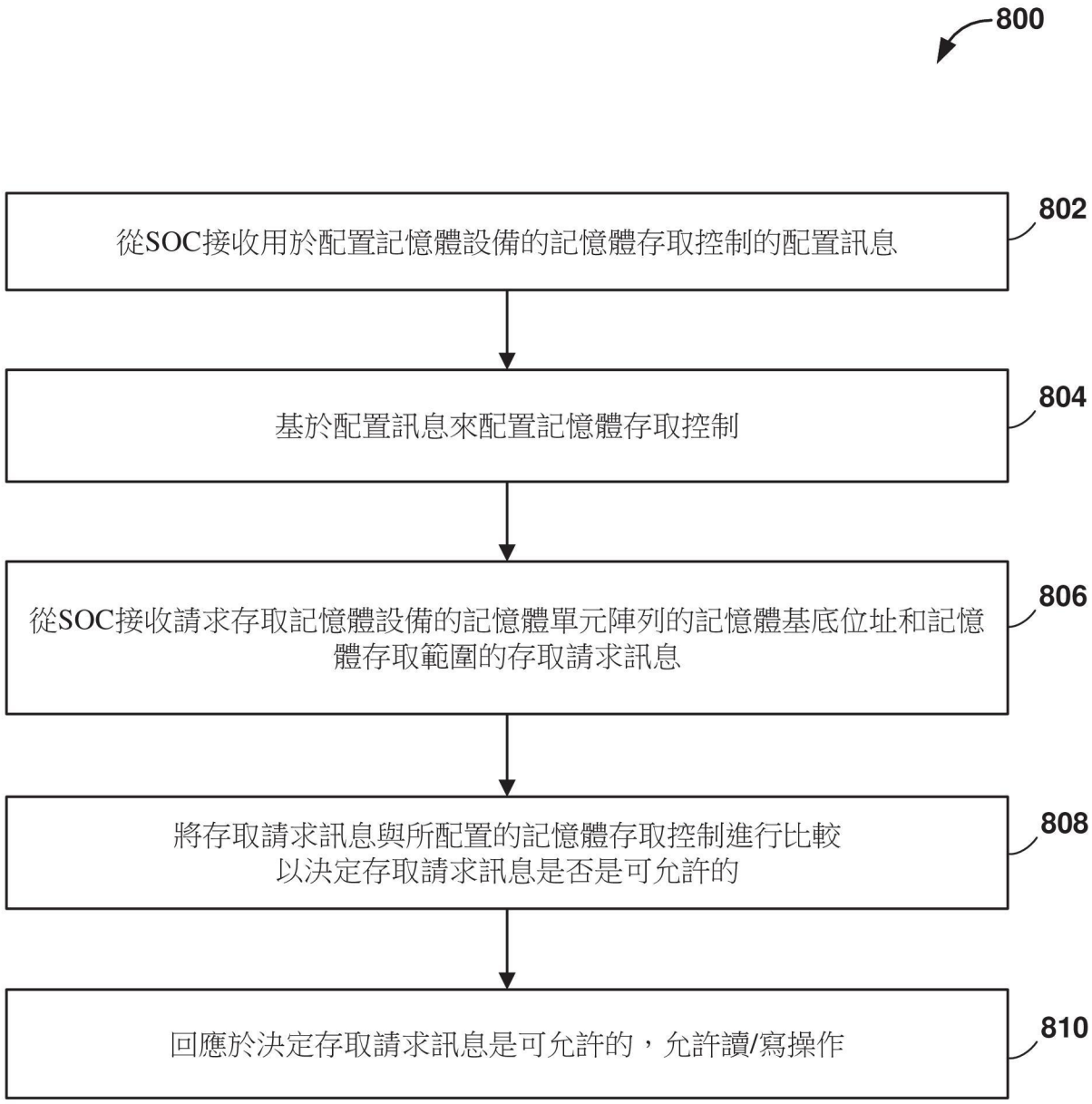
800
從SOC接收用於配置記憶體設備的記憶體存取控制的配置訊息
802
基於配置訊息來配置記憶體存取控制
804
從SOC接收請求存取記憶體設備的記憶體單元陣列的記憶體基底位址和記憶體存取範圍的存取請求訊息
806
將存取請求訊息與所配置的記憶體存取控制進行比較以決定存取請求訊息是否是可允許的
808
回應於決定存取請求訊息是可允許的，允許讀/寫操作
810

圖8

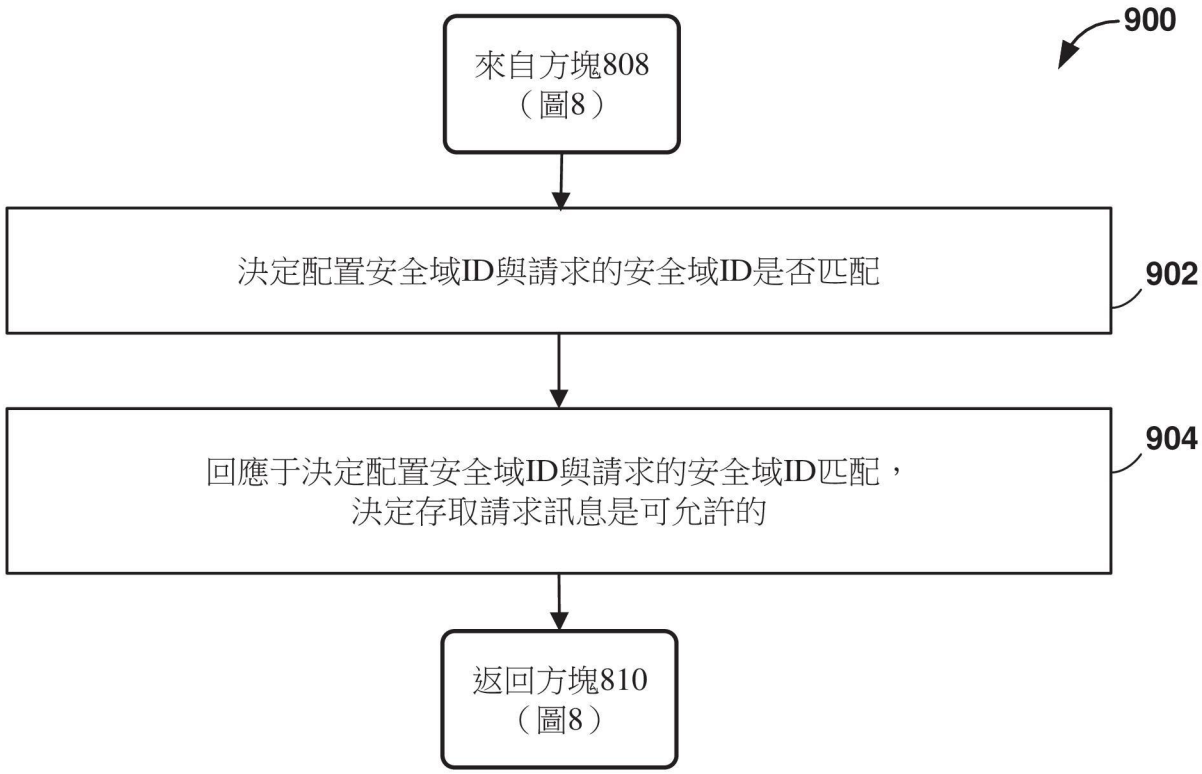
900
來自方塊808
（圖8）
決定配置安全域ID與請求的安全域ID是否匹配
902
回應于決定配置安全域ID與請求的安全域ID匹配，
決定存取請求訊息是可允許的
904
返回方塊810
（圖8）

圖9

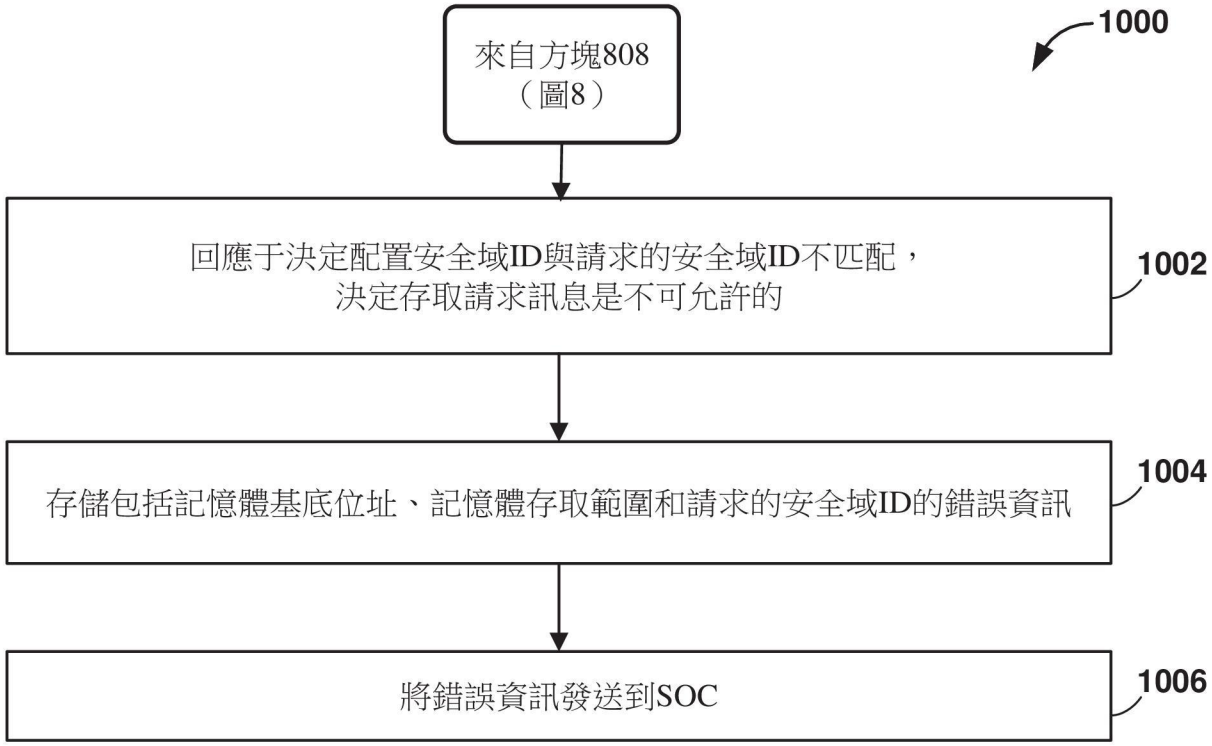
1000
來自方塊808
（圖8）
回應于決定配置安全域ID與請求的安全域ID不匹配，
決定存取請求訊息是不可允許的
1002
存儲包括記憶體基底位址、記憶體存取範圍和請求的安全域ID的錯誤資訊
1004
將錯誤資訊發送到SOC
1006

圖10

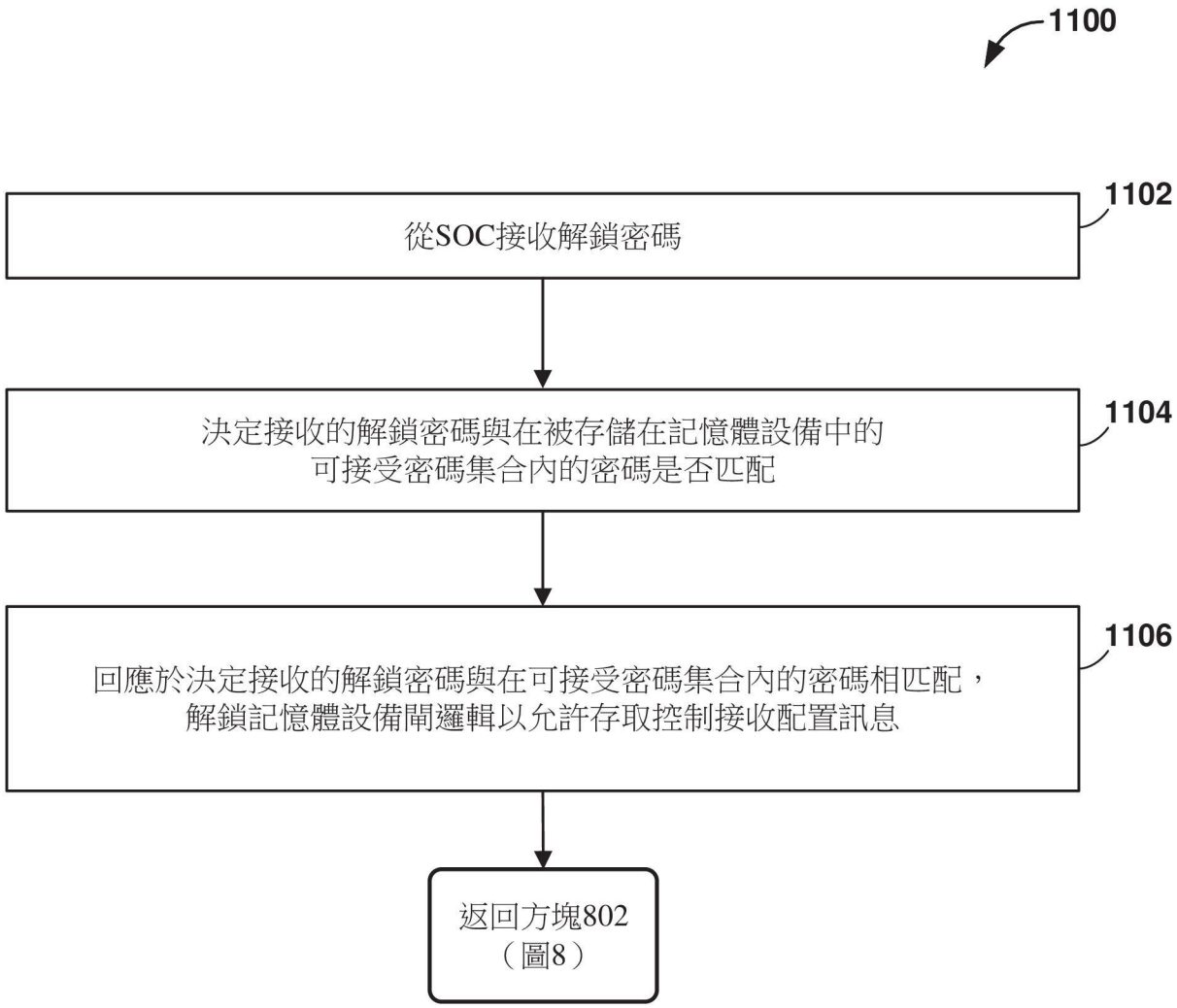
1100
1102
從SOC接收解鎖密碼
1104
決定接收的解鎖密碼與在被存儲在記憶體設備中的
可接受密碼集合內的密碼是否匹配
1106
回應於決定接收的解鎖密碼與在可接受密碼集合內的密碼相匹配，
解鎖記憶體設備閘邏輯以允許存取控制接收配置訊息
返回方塊802
（圖8）

圖11

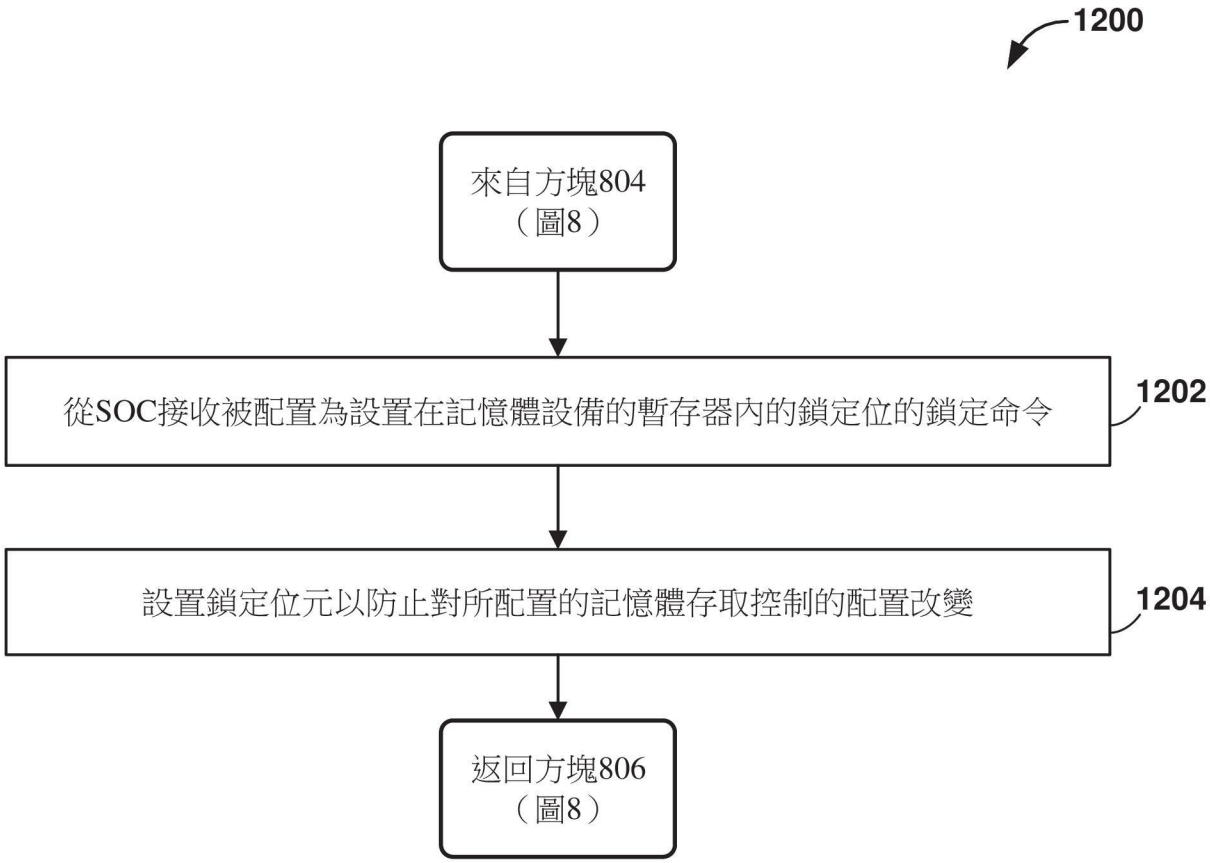
1200
來自方塊804
（圖8）
從SOC接收被配置為設置在記憶體設備的暫存器內的鎖定位的鎖定命令
1202
設置鎖定位元以防止對所配置的記憶體存取控制的配置改變
1204
返回方塊806
（圖8）

圖12

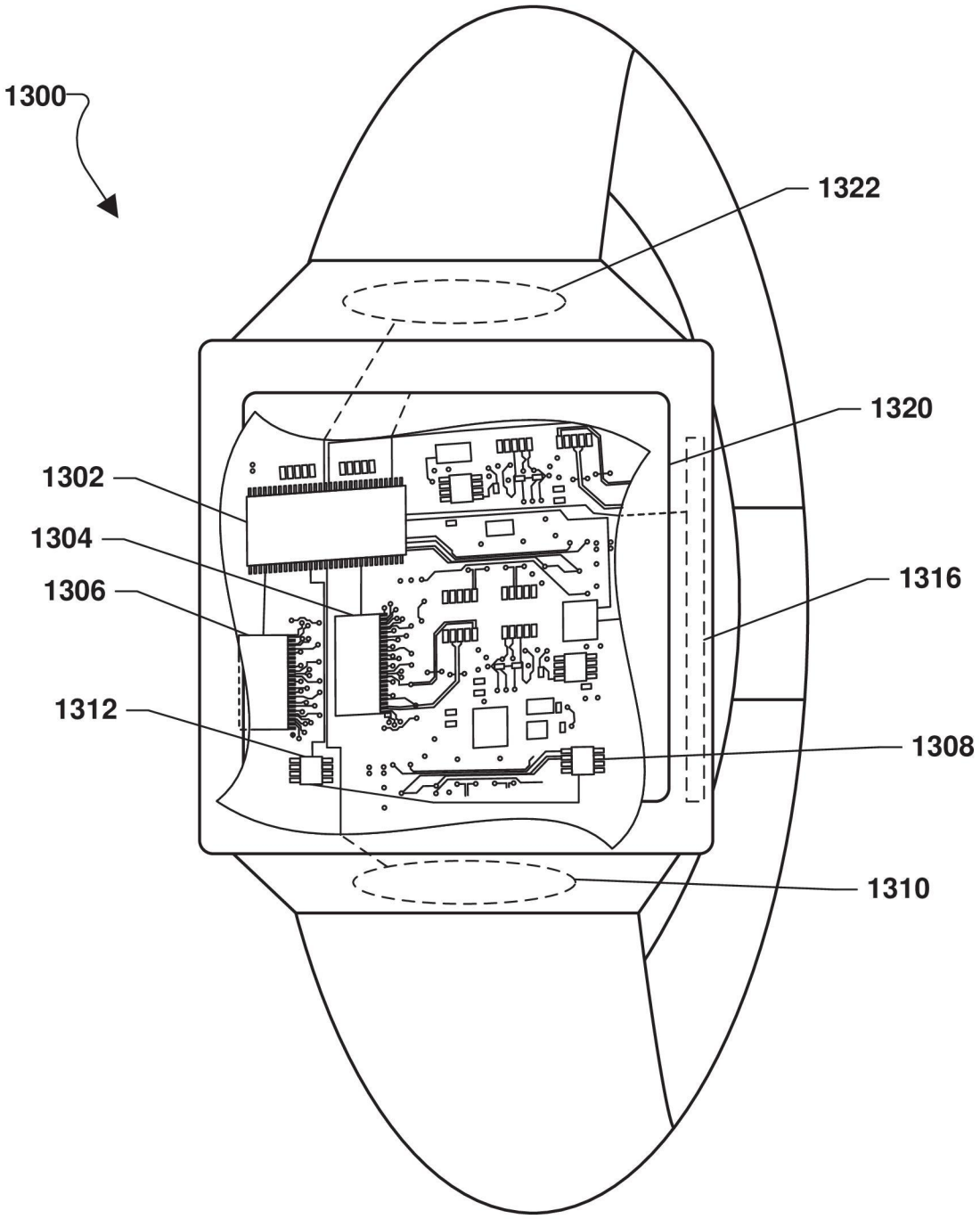

圖13

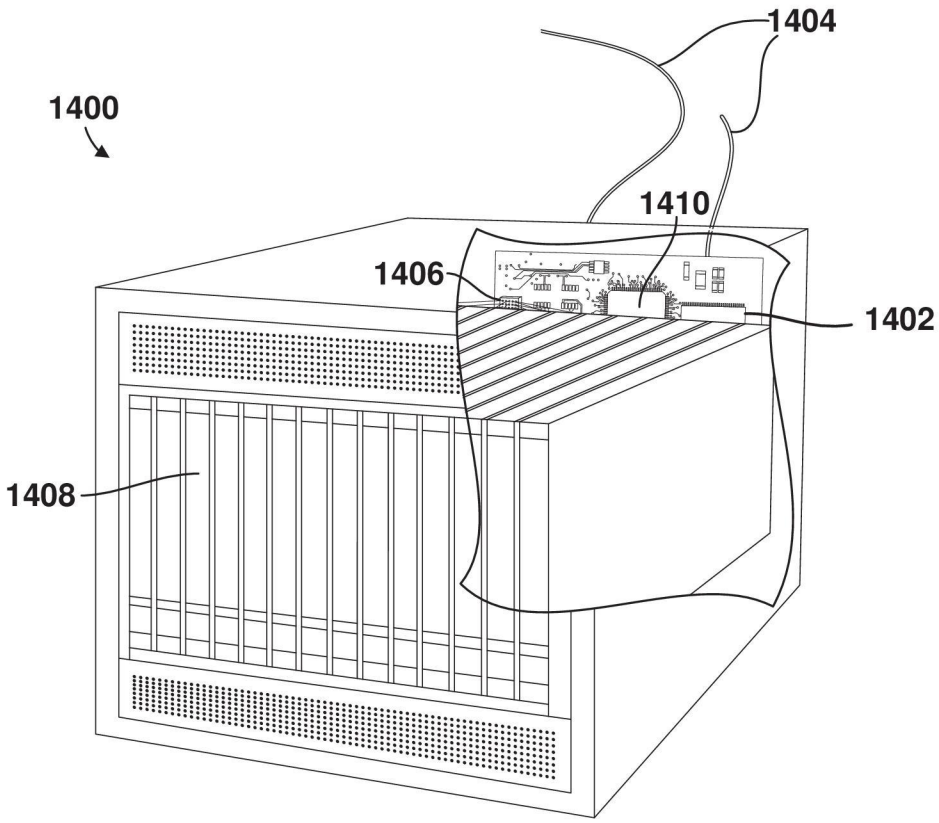

圖14

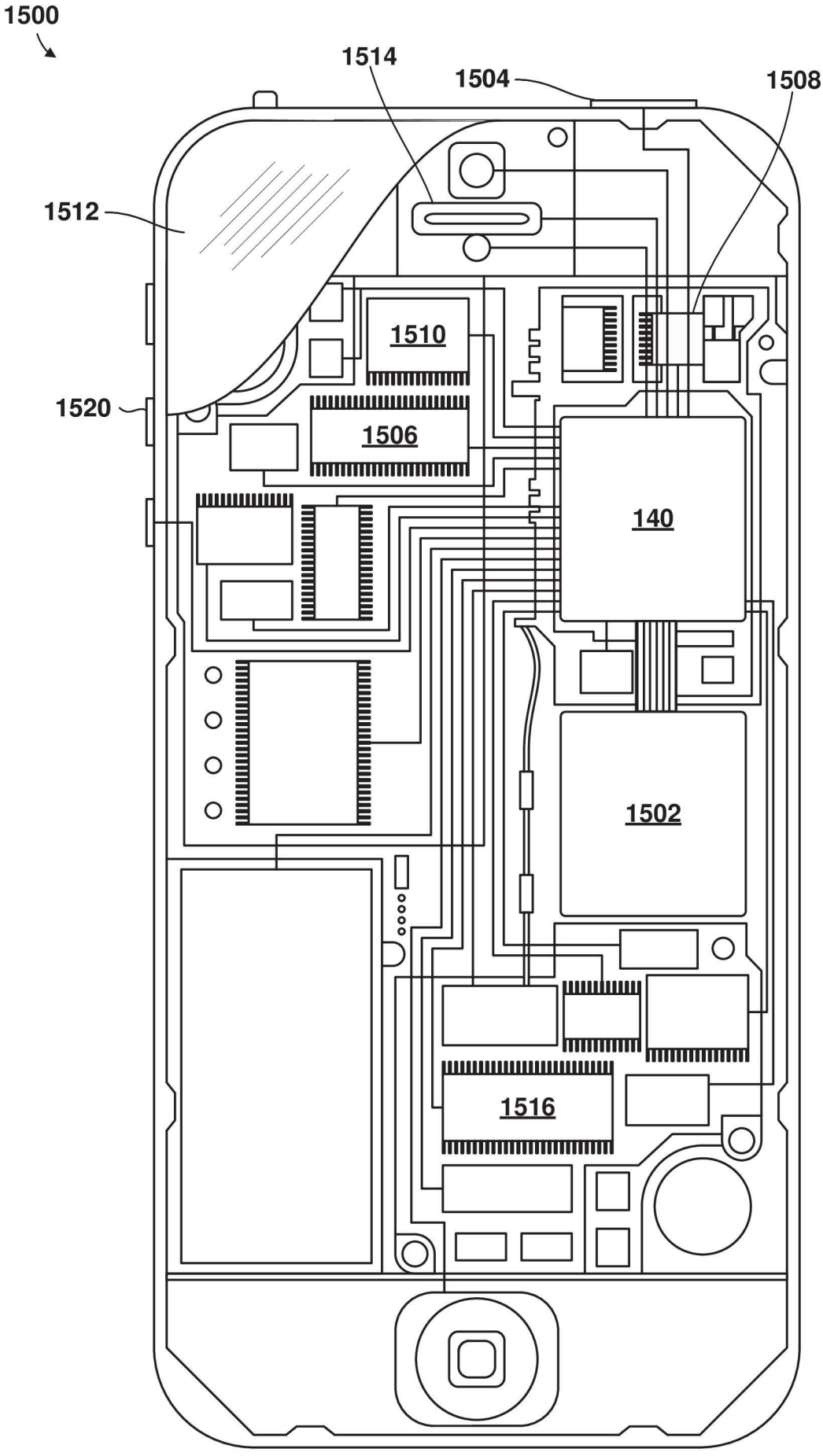

圖15