202226016

(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 202226016 A

(43)公開日： 中華民國 111 (2022) 年 07 月 01 日

(21)申請案號：110135161 (22)申請日： 中華民國 110 (2021) 年 09 月 22 日

(51)Int. Cl.： *G06F21/32 (2013.01)* *G06F11/22 (2006.01)*
G06F13/14 (2006.01) *G06F21/81 (2013.01)*

(30)優先權：2020/12/23 美國 17/132,844

(71)申請人：美商英特爾公司 (美國) INTEL CORPORATION (US)
美國

(72)發明人：帕瓦爾 薩加爾 C PAWAR, SAGAR C. (IN)；拉賈戈帕爾 潘納庫馬爾 RAJAGOPAL, PANNERKUMAR (IN)；N 拉格文卓拉 N, RAGHAVENDRA (IN)；皮萊 普拉卡什 PILLAI, PRAKASH (IN)；皮爾 歐威斯 PIR, OVAIS (IN)

(74)代理人：劉法正；尹重君

申請實體審查：無 申請專利範圍項數：20 項 圖式數：4 共 52 頁

(54)名稱

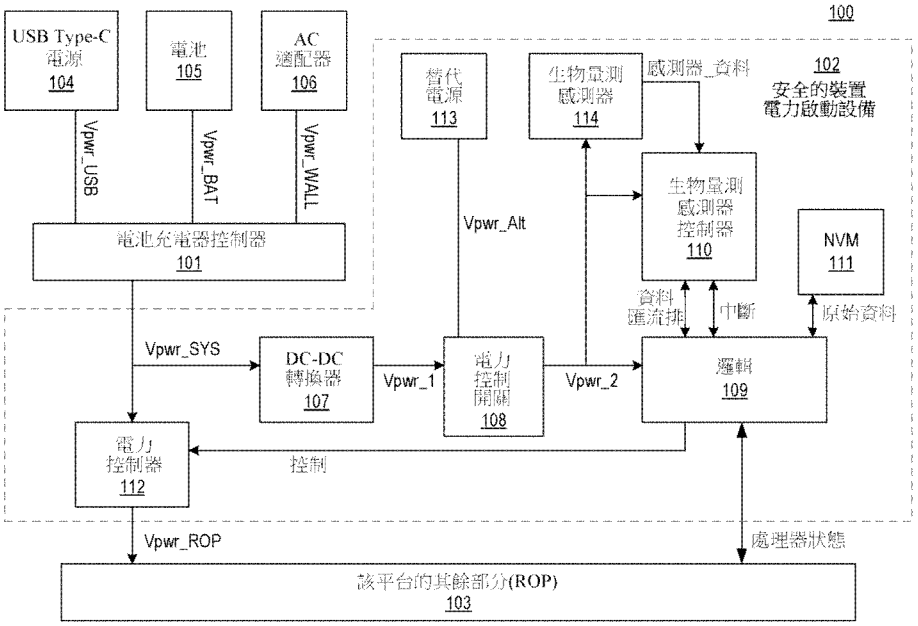
安全的裝置電力啟動設備及方法

(57)摘要

一種用於一運算系統的電力啟動方案，該方案運用一生物量測感測器(例如，一指紋感測器、眼感測器、等等)來在啟用該運算系統的電力啟動之前驗證一使用者或以恢復轉移到一電力狀態(例如，由該先進組配與電力介面(ACPI)所定義的該等電力狀態之一)。把該生物量測感測器的輸出與一註冊使用者的資料進行比較以進行一匹配。該資料可包括被保存在一非依電性記憶體(例如，串列週邊介面(SPI)快閃裝置)中之該生物量測感測器一輸出的一原始副本。如果存在一匹配，則在該運算系統中的一邏輯將允許該運算系統的電力啟動。在沒有匹配的情況下，該運算系統不會被電力啟動。在一些實施例中，如果未找到匹配，則電池的充電也會被禁用。

A power-up scheme for a computing system that applies a biometric sensor (e.g., a fingerprint sensor, eye sensor, etc.) to authenticate a user before enabling power-up of the computing system or to resume transition to a power state (e.g., one of the power states defined by the Advance Configuration and Power Interface (ACPI)). Output of the biometric sensor is compared against data of a registered user for a match. The data may include an original copy of an output of the biometric sensor saved in a non-volatile memory (e.g., serial peripheral interface (SPI) flash device). If a match exists, a logic in the computing system will allow the computing system to power-up. In the absence of a match, the computing system will not be powered up. In some examples, battery charging is also disabled if the match is not found.

指定代表圖：



【圖1】

符號簡單說明：

100:運算系統

101:電池充電器控制器

102:安全的裝置電力啟動設備

103:該平台的其餘部分(ROP)

104:USB Type-C 電源

105:電池

106:AC 適配器

107:DC-DC 轉換器

108:電力控制開關

109:邏輯

110:生物量測感測器控制器

111:NVM

112:電力控制器

113:替代電源

114:生物量測感測器

【發明摘要】

【中文發明名稱】

安全的裝置電力啟動設備及方法

【英文發明名稱】

SECURE DEVICE POWER-UP APPARATUS AND METHOD

【中文】

一種用於一運算系統的電力啟動方案，該方案運用一生物量測感測器(例如，一指紋感測器、眼感測器、等等)來在啟用該運算系統的電力啟動之前驗證一使用者或以恢復轉移到一電力狀態(例如，由該先進組配與電力介面(ACPI)所定義的該等電力狀態之一)。把該生物量測感測器的輸出與一註冊使用者的資料進行比較以進行一匹配。該資料可包括被保存在一非依電性記憶體(例如，串列週邊介面(SPI)快閃裝置)中之該生物量測感測器一輸出的一原始副本。如果存在一匹配，則在該運算系統中的一邏輯將允許該運算系統的電力啟動。在沒有匹配的情況下，該運算系統不會被電力啟動。在一些實施例中，如果未找到匹配，則電池的充電也會被禁用。

【英文】

A power-up scheme for a computing system that applies a biometric sensor (e.g., a fingerprint sensor, eye sensor, etc.) to authenticate a user before enabling power-up of the computing system or to resume transition to a power state (e.g., one of the power states defined by the Advance Configuration and Power Interface (ACPI)). Output of the biometric sensor is compared against data of a registered user for a match. The data may include an original copy of an output of the biometric sensor saved in a non-volatile memory (e.g., serial peripheral interface (SPI) flash device). If a match exists, a logic in the computing system will allow the computing system to power-up. In the absence of a match, the computing system will not be powered up. In some examples, battery charging is also disabled if the match is not found.

【指定代表圖】　圖1

【代表圖之符號簡單說明】

100:運算系統
101:電池充電器控制器
102:安全的裝置電力啟動設備
103:該平台的其餘部分(ROP)
104:USB Type-C電源
105:電池
106:AC適配器
107:DC-DC轉換器
108:電力控制開關
109:邏輯
110:生物量測感測器控制器
111:NVM
112:電力控制器
113:替代電源
114:生物量測感測器

【特徵化學式】

無

【發明說明書】

【中文發明名稱】

安全的裝置電力啟動設備及方法

【英文發明名稱】

SECURE DEVICE POWER-UP APPARATUS AND METHOD

【技術領域】

發明領域

【0001】 本發明係有關於安全的裝置電力啟動設備及方法。

【先前技術】

發明背景

【0002】 通常，諸如智慧型手機、膝上型電腦、等等之類的運算裝置面臨失敗之未授權存取時，該運算裝置可被重置成為出廠設定並重新使用相同或新的記憶體。例如，一被偷的運算裝置可藉由完成該運算裝置的一出廠重置過程來在黑市或灰市中轉售。因此，當前的裝置不能防盜。

【發明內容】

發明概要

【0003】 依據本發明之一實施例，係特地提出一種設備，其包含有：可由一控制信號來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到一運算平台；以及邏輯，其用以根據在被儲存於記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。

【圖式簡單說明】

【0004】 從以下所給出的詳細描述以及本發明之各個實施例的附圖，本發明的該等實施例將被更全面地理解，然而，該等附圖不應把本發明限制為該等

特定的實施例，而是只用於解釋及理解而已。

【0005】 **圖1**根據一些實施例圖示出具有安全裝置電力啟動的一運算系統。

【0006】 **圖2**根據一些實施例圖示出具有安全生物感測器資料區域的一串列週邊介面(SPI)快閃軟體堆疊。

【0007】 **圖3**根據一些實施例圖示出一安全裝置電力啟動的一狀態圖。

【0008】 **圖4**根據一些實施例圖示出具有安全裝置電力啟動的一智慧型裝置或一電腦系統或一SoC(系統單晶片)。

【實施方式】

【0009】 較佳實施例之詳細說明

一些實施例描述了用於一運算系統的一電力啟動方案，其應用生物量測感測器(例如，一指紋感測器、眼感測器、等等)來在啟用該運算系統的電力啟動之前驗證一使用者或以恢復轉移到一電力狀態(例如，由該先進組配與電力介面(ACPI)所定義的該等電力狀態之一)。在一些實施例中，把該生物量測感測器的輸出與一註冊使用者的資料進行比較以進行一匹配。該資料可包括被保存在一非依電性記憶體(例如，串列週邊介面(SPI)快閃裝置)中之該生物量測感測器一輸出的一原始副本。如果存在一匹配，則在該運算系統中的一邏輯將允許該運算系統的電力啟動。在沒有匹配的情況下，該運算系統不會被電力啟動。在一些實施例中，如果未找到匹配，則電池充電也會被禁用。

【0010】 在一些實施例中，該電力啟動方案包括一設備，該設備包含可由一控制器來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到一運算平台。在各種實施例中的該設備包括一邏輯以根據在儲存在記憶體中的一第一生物量測資料與由一生物量測感測器所感測的第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。在一些實施例中，當該第一生物量測資料與該第二生物量測資料不匹配時，

該邏輯關閉該電力閘以切斷在該第二電源軌上的一第二電源。在一些實施例中，當該第一生物量測資料與該第二生物量測資料實質上匹配時，該邏輯開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。在一些實施例中，該記憶體係一非依電性記憶體。在一些實施例中，該生物量測感測器係以下中之一個：一指紋感測器、一眼睛系統、一臉部識別設備。在一些實施例中，該第一電源軌被耦合到一電池充電器控制器，該電池充電器控制器被耦合到複數個電源。在一些實施例中，該等複數個電源包括：一USB Type-C電源、一電池、以及一AC適配器。

【0011】 在一些實施例中，該設備包含一生物量測控制器以在當該生物量測感測器產生該第二生物量測資料時向該邏輯發出一中斷。在一些實施例中，該設備包括一DC-DC轉換器以在該第一電源軌上接收一第一電力並且在一第三電源軌上產生一第三電力。在一些實施例中，該設備包含一電力控制開關，以把該第三電源或在一第四電源軌上的一第四電力中之一個提供給一第五電源軌。在一些實施例中，該第四電源軌被耦合到一替代的電源。在一些實施例中，該替代的電源包括一硬幣型電池。在一些實施例中，該第五電源軌用於向該生物量測感測器、該生物量測控制器、該邏輯、以及該記憶體供電。在一些實施例中，該電力控制開關包含一多工器，其當該第三電力低於一臨界值時向該第五電源軌提供該第四電力。

【0012】 各種實施例的技術效果有很多。例如，該安全的電力啟動設備及方法藉由使該運算系統對隨後未經授權所有者變得無法操作來保護在該運算系統中的使用者資料。當一裝置被電力啟動時，現有的身份驗證方案運行時因執行出廠重置而使惡意得逞。從各種附圖及實施例，其他的技術效果將會是顯而易見的。

【0013】 在以下的描述中，許多的細節被討論以對本發明的實施例提供更

為全面的解釋。然而，對於本領域的習知技藝者顯而易見的是，可以在沒有這些具體細節的情況下實踐本發明的實施例。在其他的情況下，眾所周知的結構及裝置係以方塊圖的形式示出而不被詳細地示出，以避免混淆本發明的實施例。

【0014】 請注意，在實施例對應的附圖中，信號係以線來被表示。一些線可能較粗，以指出更多的組成信號路徑，及/或在一或多個末端具有箭頭，以指出主要的資訊流方向。此類的指出並非旨在進行限制。相反的是，這些線與一或多個示例性的實施例結合來使用以促進對一電路或一邏輯單元之更容易的理解。任何表示的信號，如設計所需要的或偏好所指定的，實際上可以包括一或多個可以沿著任一方向進行傳播的信號，並且可以用任何合適類型的信號方案來被實現。

【0015】 **圖1**根據一些實施例圖示出一種具有安全的裝置電力啟動的運算系統100。運算系統100包含電池充電器控制器101、安全的裝置電力啟動設備102(在此為設備102)、該平台的其餘部分(ROP)103、以及數個電源，諸如通用串列匯流排(USB)Type-C(USB Type-C)104、電池105、以及AC適配器106。來自各種電源的該電源係由電池充電器控制器101來處理或管理。例如，來自USB Type-C電源104的Vpwr_USB、來自電池105的Vpwe_BAT、及/或Vpwr_WALL係由電池充電器控制器101分別從USB Type-C 104、電池105、以及AC適配器106來接收。在這裡，ROP 103可以包括**圖4**的電腦系統組件。在一些實施例中，設備102包含DC-DC轉換器107、電力控制開關108、邏輯109、生物量測感測器控制器110、非依電性記憶體(NVM)111、電力控制器112、替代電源113、以及生物量測感測器114。

【0016】 在一些實施例中，DC-DC轉換器107接收Vpwr_SYS作為來自電池充電器控制器101的輸入並產生一經調整的輸出電源Vpwr_1(例如，3.3V)。任何合適的DC-DC轉換器可被使用來實現轉換器107。例如，降壓轉換器、升壓轉換

器、降壓-升壓轉換器、等等，可被使用來實現轉換器107。在一些實施例中，Vpwr_1向電力控制開關108提供電力，其傳遞Vpwr_1作為Vpwr_2以當作邏輯109、生物量測感測器控制器110、NVM 111、以及生物量測感測器114的電源。在一些實施例中，電力控制開關108包含一電力多工器，其提供Vpwr_Alt(備用電源)或Vpwr1其中之一個作為給節點Vpwr_2的電源。在一些實施例中，從一替代電源113接收Vpwr_Alt。電源113的實例包括硬幣式電池及/或其他的長期電池電源。

【0017】 在一些實施例中，電力控制開關108包含檢測Vpwr_1存不存在的一邏輯，並根據該邏輯向邏輯109、生物量測感測器控制器110、NVM記憶體111、以及生物量測感測器114供電。在一個實例中，當控制器101檢測到沒有電源時(例如，當電池105沒電而其他的電源沒被連接時)，Vpwr_1被放電到地面。當Vpwr_1被放電到地面時，電力控制開關可以檢測到該輸出Vpwr_Alt作為用於Vpwr_2的電源。在一種實現方式中，用於電力控制開關108之一多工器的一選擇信號係由Vpwr_1來控制。當控制器101檢測到在Vpwr_1上的電源供應時，電力控制開關108的多工器選擇Vpwr_1並將其傳遞給Vpwr_2。因此，設備102能夠在沒有(臨時或永久)典型電源104、105、以及106的情況下執行裝置認證。

【0018】 在一些實施例中，生物量測控制器110處理來自生物量測感測器114的感測器資料。生物量測感測器114可以是一或多個感測器以建立一個人的身份。這些感測器包括指紋感測器、臉部識別、眼睛感測器、等等。在一些實施例中，生物量測控制器110包括邏輯(硬體及/或軟體)以處理感測器資料的種類、把其儲存在NVM 111中、與在NVM 111中一預先儲存的感測器資料執行一匹配分析。在一些實施例中，該匹配分析係由邏輯109來執行。在一些實施例中，控制器110在接收到感測器資料(sensor_data)時發出用於邏輯109的一中斷。

【0019】 在一些實施例中，NVM 110包含一串列週邊介面(SPI)快閃。SPI

符合用於短距離通訊(例如，在一嵌入式系統中)的一同步串列通訊介面規範。SPI快閃通常是一低功耗及低速度的記憶體(例如，133 MHz的速度)。可以使用像是I2C的介面來存取它。在一些實施例中，該快閃記憶體包括NAND及/或NOR記憶體。在一些實施例中，NVM 110包含以下中之一個：鐵電記憶體、相變記憶體(PCM)、電阻式記憶體(ReRAM)、或磁性RAM(MRAM)。在各種實施例中，NVM儲存該原始生物量測感測器資料(也被稱為黃金資料)，其與由一生物量測感測器114所接收到的輸入進行比較。雖然各種實施例僅圖示出了一個生物量測感測器114，但可以使用多個生物量測感測器。在一些實施例中，NVM 111包括在NVM 111中的該原始真實使用者生物量測感測器資料。

【0020】 在一些實施例中，邏輯109包含一有限狀態機，其基於是否確定有一匹配及/或基於處理器狀態(例如，睡眠狀態、效能狀態、等等)產生用於電力控制器113的一控制信號。根據該系統狀態或處理器狀態，邏輯109可以檢測及/或解讀該生物量測輸入資料，然後驗證該使用者。邏輯109然後釋放該主控制控制器112以把該系統從該相應狀態引導至正常的開啟狀態。在各種實施例中，電力控制器112基於來自邏輯109之該控制信號的一邏輯值把該電源供應Vpwr_ROP選通到ROP 103。該控制信號的該邏輯值取決於邏輯109判定一使用者的一生物量測是否被認證。如果邏輯109判定該使用者的該生物量測被認證，則電力控制器112允許Vpwr_SYS被傳遞到Vpwr_ROP。此處，節點名稱及信號名稱可被互換地使用。例如，取決於該句子的上下文，Vpwr_ROP可以指電源供應電壓及/或電流或節點Vpwr_ROP。在沒有向Vpwr_ROP提供Vpwr_SYS的情況下，ROP 103維持係斷電的。在一些實施例中，電力控制器112包含一電力開關或電力閘，其閘極受控制(control)來控制且源極端被耦合到Vpwr_SYS以及汲極端被耦合到Vpwr_ROP。

【0021】 **圖2**根據一些實施例圖示出具有安全生物感測器資料區域的一串

列週邊介面(SPI)快閃軟體堆疊200。在一些實施例中，軟體堆疊200被儲存在NVM 111中。在一些實施例中，堆疊200包含BIOS 201、MRC訓練資料202、GOP 203、WiFi及/或藍牙韌體(FW)204、微碼(uCode)及電力管理單元(p-單元)補丁205、安全的生物量測(例如指紋)資料區域206、平台實體(PHY) FW 207、CSE FW 208、ISH FW 209、嵌入式控制器FW 210、電力管理控制器(PMC) FE 211，以及軟體帶212。

【0022】 BIOS 201係一基本輸入/輸出系統，負責啟動ROP 103。MRC訓練資料202係指記憶體參考代碼，其包含有關於一記憶體控制器之記憶體設置、頻率、時序、驅動及詳細操作等等的資訊。GOP 203指的是圖形輸出協定，其提供有限的運行時服務支援。GOP係UEFI的一種標準，可以在其中查詢節點及設置模式。GOP係一種可擴展韌體介面(EFI)啟動時間服務，其在一啟動退出服務之後不會被存取。統一可擴展韌體介面(UEFI)係用於把一電腦的韌體連接到其作業系統(OS)之軟體程式的一種規範。UEFI係在製造時被安裝的，係當一電腦開機時所運行的第一個程式。實體FW 207、CSE FW 208、ISH FW 209、嵌入式控制器FW 210係用於IA平台啟動/安全性的基本韌體區域。

【0023】 **圖3**根據一些實施例圖示出一安全的設備電力啟動的狀態圖300。在一些實施例中，狀態圖300以硬體、軟體或它們的組合來被實現。在一些實施例中，狀態圖300係由邏輯109來實現。狀態301係當系統處於睡眠狀態並且沒有輸入被檢測到時的一預設狀態。在一些實施例中，一系統可以處於先進組配及電力介面(ACPI)規範所定義的S3、S4或S5狀態中之一個。在一些實施例中，只要沒有按下電源按鈕、沒有打開顯示器上蓋、並且沒有使用生物量測感測器114，由邏輯109所執行的該程序就保持在狀態301中。在本文中參考作為一指紋感測器的一生物量測感測器114來描述各種實施例。然而，狀態圖300適用於包括有一生物量測感測器之任何的感測器。

【0024】 如果設備 102 檢測到一使用者輸入正被接收，則該程序從狀態 301 移動到狀態 302。例如，當一使用者按下該電源按鈕以開啟系統100時、顯示器上蓋被打開時、及/或手指在該指紋掃描其上被掃過時，然後該程序進行到狀態302。在一些實施例中，在檢測到使用者輸入之後，如果系統100或使用者沒有採取任何的動作，則該程序返回到狀態301。例如，一定時器在一使用者按下該開機按鈕但未嘗試在該掃描器上掃描手指之後啟動，然後在該計時器到期時(例如，一預先規劃或可規劃的計數值)，該程序返回到狀態301。一旦進入狀態302，系統還不會啟動或打開。電池充電器控制器101檢查諸如USB Type-C電源104、電池105、或AC適配器106的電力輸入。如果該等電源的任意一項存在(如由Vpwr_USB、Vpwr_BAT、或Vpwr_WALL之任一個所檢測到)，電池充電器控制器101產生該適當的系統電源Vpwr_SYS。該Vpwr_SYS被提供給DC-DC轉換器107作為輸入以產生用於設備102之其餘部分的Vpwr_1 。在各種實施例中，Vpwr_SYS(一非閘控電源)係由電力控制器112所閘控，直到邏輯109另有指示為止。在一些實施例中，Vpwr_SYS可以被提供給ROP 103的一些邏輯。例如，ROP 103也可以具有一傳統的認證方案，並且該方案可以由Vpwr_SYS提供電力。在各種實施例中，給ROP 103之處理器的電力係由電力控制器112所閘控，直到邏輯109經由一控制信號另有指示為止。

【0025】 在狀態303，邏輯109判定沒有電源處於活動狀態或者電池電力Vpwr_BAT低於一臨界值(例如，太低而無法開啟系統100)，則該程序回到狀態301。如果使用者在生物量測感測器114上掃過他/她的手指，生物量測控制器110向邏輯109發出一中斷，因此邏輯109可以開始處理該使用者的該認證。在一些實施例中，邏輯109讀取儲存在NVM 111中的該原始感測器資料並把其與由控制器110所接收到的感測器資料(sensor_data)進行比較。在各種實施例中，該比較係一數位比較。例如，使用一類比到數位轉換器(ADC)把指紋資料或任何的生物量

測資料從類比形式轉換為數位形式。在一些實施例中，該比較係一種逐一位元比較。在一些實施例中，當該儲存的資料實質上等於該感測器資料(sensor_data)時，該比較被認為係匹配的。

【0026】 在狀態304，如果在該儲存的資料與該感測器資料(sensor_data)之間確定匹配，則邏輯109產生不會對Vpwr_SYS進行閘控的一控制，從而把Vpwr_SYS提供給ROP 103作為Vpwr_ROP。ROP 103然後會甦醒。在一些實施例中，ROP 103從其先前狀態甦醒。在狀態305，如果該等以下使用者輸入的任一被接收到，則該程序前進到狀態301。例如，如果按下電源按鈕來關閉系統100、如果使用者經由一作業系統啟動一系統關閉、顯示螢幕上蓋被關閉、及/或該系統根據OS電源管理策略判定為閒置的，系統100進入睡眠狀態(例如，S3、S4狀態)。

【0027】 實施例的元素(例如，參考**圖3**的流程圖)也被提供為用於儲存電腦可執行指令(例如，實現本文所討論之任何其他程序的指令)的一機器可讀取媒體(例如，NVM 111)。在一些實施例中，運算平台包含被耦合在一起的記憶體、處理器、機器可讀取儲存媒體(也稱為有形的機器可讀取媒體)、通訊介面(例如，無線或有線介面)及網路匯流排。

【0028】 在一些實施例中，邏輯109包含一處理器，其係一數位信號處理器(DSP)、專用積體電路(ASIC)、通用中央處理單元(CPU)、或實現一簡單有限狀態機的低功率邏輯，以執行參照**圖3**的該方法及/或各種的實施例、等等。

【0029】 在一些實施例中，邏輯109的各種邏輯區塊經由一網路匯流排被耦合在一起。可以使用任何合適的協定來實現網路匯流排。在一些實施例中，機器可讀取儲存媒體包括用於計算或測量一裝置相對於另一裝置的距離及相對方向的指令(也被稱為程式軟體代碼/指令)，正如參考各種實施例及流程圖所描述的。

【0030】 與參考**圖3**(及/或各種實施例)的流程圖相關聯並被執行以實現該揭露技術主題之實施例的程式軟體代碼/指令可以被實現為一作業系統的一部分或為一特定的應用程式、組件、程式、物件、模組、程序、或其他的指令序列或指令序列的組織，被稱為「程式軟體代碼/指令」、「作業系統程式軟體代碼/指令」、「應用程式軟體代碼/指令」、或簡稱「軟體」或嵌入在處理器中的韌體。在一些實施例中，與參照**圖3**之流程圖 (及/或各種實施例)相關聯的程式軟體代碼/指令係由系統來執行。

【0031】 在一些實施例中，與參照**圖3**之流程圖(及/或各種實施例)相關聯的程式軟體代碼/指令被儲存在一電腦可執行儲存媒體中並且由該處理器來執行。在本文中，電腦可執行儲存媒體係一種有形的機器可讀取媒體，其可被使用來儲存程式軟體代碼/指令及資料，當由一運算裝置執行時，致使一或多個處理器執行如針對所揭露技術主題在一或多個所附請求項中所陳述一或多種方法。

【0032】 該有形的機器可讀取媒體可包括把該可執行軟體程式代碼/指令及資料儲存在各種的有形位置中，該等有形位置包括有例如ROM、依電性RAM、非依電性記憶體及/或快取及/或其他有形記憶體，如在本申請中所參照的。該程式軟體代碼/指令及/或資料的一部分可被儲存在這些儲存器及記憶體裝置中的任何一個中。此外，該程式軟體代碼/指令可以從其他儲存器獲得，包括有，例如透過集中式伺服器或對等網路等等，包括有網際網路。該軟體程式代碼/指令及資料的不同部分可以在不同的時間及不同的通訊會談中或在同一通訊會談中獲得。

【0033】 該軟體程式代碼/指令(與參考**圖3**及其他實施例相關聯)及資料可以在由該運算裝置執行一相應軟體程式或應用程式之前被整體地獲得。或者，該軟體程式代碼/指令及資料的部分可被動態地獲得，例如，在需要執行時即時地獲得。或者，舉例來說，例如對於不同的應用程式、組件、程式、物件、模

組、程序或其他指令序列或指令序列的組織，可以用獲得軟體程式代碼/指令及資料之上述方式的某種組合來獲得。因此，並不要求資料及指令在特定時間實例上要完整地位於一有形的機器可讀取媒體上。

【0034】 有形電腦可讀取媒體的實例包括但不侷限於可記錄及不可記錄類型的媒體，例如依電性及非依電性記憶體裝置、唯讀記憶體(ROM)、隨機存取記憶體(RAM)、快閃記憶體裝置、軟碟及其他可移動磁碟、磁性儲存媒體、光學儲存媒體(例如，光碟唯讀記憶體(CD ROM)、數位多功能碟(DVD)、等等)、鐵電記憶體、電阻式RAM、相變記憶體(PCM)、磁性RAM(MRAM)、等等。該軟體程式代碼/指令可被暫時地儲存在數位有形的通訊鏈路中，透過這種有形的通訊鏈路同時實現電氣、光學、聲音或其他形式的傳播信號，諸如載波、紅外線信號、數位信號、等等。

【0035】 一般而言，有形的機器可讀取媒體包含任何有形的機制，其提供可由一機器(即，一運算裝置)存取的形式(即，以數位形式儲存及/或傳輸，例如，資料封包)的資訊，其可被包括，例如，在一通訊裝置、一運算裝置、一網路裝置、一個人數位助理、一製造工具、一行動通訊裝置(無論是否能夠從諸如網際網路之類的通訊網路下載及運行應用程式及補貼應用程式，例如，一iPhone®、Galaxy®、等等)、或包括有一運算裝置之任何其他裝置中。在一個實施例中，基於處理器的系統係以一PDA(個人數位助理)、一蜂巢式電話、一筆記型電腦、一平板電腦、一遊戲機、一機上盒、一嵌入式系統、一TV(電視)、一個人桌上型電腦、等等形式出現，或被包括在一PDA、一蜂巢式電話、一筆記型電腦、一平板電腦、一遊戲機、一機上盒、一嵌入式系統、一TV、一個人桌上型電腦、等等之中。或者，該等傳統的通訊應用程式及補貼應用程式可被使用在本揭露技術主題的一些實施例中。

【0036】 在一些實施例中，該機器可讀取儲存媒體包括儲存在其上的機器

可讀取指令，當執行該等指令時，致使一或多個機器執行一方法，該方法包含有根據一控制信號控制被耦合到一第一電源軌及一第二電源軌的一電力閘，其中該第二電源軌被耦合到一運算平台。在一些實施例中，該方法更包含根據在儲存在一記憶體中的一第一生物量測資料與由一生物量測感測器所感測到的第二生物量測資料之間的一匹配來產生該控制信號。在一些實施例中，該方法更包含當該第一生物量測資料與該第二生物量測資料不匹配時，關閉該電力閘以切斷在該第二電源軌上的一第二電源。在一些實施例中，該方法包含當該第一生物量測資料與該第二生物量測資料實質上匹配時開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。在一些實施例中，該方法包含當該生物量測感測器產生該第二生物量測資料時發出一中斷。

【0037】 **圖4**根據一些實施例圖示出具有安全的裝置電力啟動的一智慧型裝置或電腦系統或一SoC(系統單晶片)。需要指出的是，**圖4**的那些具有與任何其他圖示之元件有相同參考號碼(或名稱)的元件可以以與所描述類似之任何方式來操作或起作用，但不侷限於此。在該智慧型裝置中的任何方塊都可以具有用於動態最佳化電池充電電壓的該設備。

【0038】 在一些實施例中，裝置 5500表示一適當的運算裝置，諸如一運算平板電腦、一行動電話或智慧型手機、一膝上型電腦、一桌上型電腦、一物聯網(IOT)裝置、一伺服器、一可穿戴式裝置、一機上盒、一無線電子閱讀器、等等。將被理解的是，某些組件被概括性地示出，且並非如此一裝置之所有的組件都在裝置5500中被示出。

【0039】 在一個實例中，該裝置5500包含一SoC(系統單晶片)5501。在**圖4** 中使用了虛線來示出該SoC 5501的一示例性邊界，其中一些實例組件被圖示為被包含在SoC 5501中--然而，SoC 5501可能包含裝置 5500之任何適當的組件。

【0040】 在一些實施例中，裝置5500包含一處理器5504。處理器5504可以

包括一或多個實體裝置，諸如微處理器、應用處理器、微控制器、可規劃邏輯裝置、處理核心、或其他的處理實現方式諸如多個運算、圖形、加速器、I/O及/或其他處理晶片的分解組合。由處理器5504所執行的該等處理操作包括一作業平台或作業系統的該執行，應用程式及/或裝置功能被執行在該作業平台或作業系統上。該等處理操作包含與人類使用者或與其他裝置I/O(輸入/輸出)相關的操作、與電力管理相關的操作、與把運算裝置5500連接到另一裝置相關的操作、等等。該等處理操作還可包含與音訊I/O及/或顯示I/O相關的操作。

【0041】 在一些實施例中，處理器5504包括多個處理核心(也被稱為核心)5508a、5508b、5508c。儘管在**圖4**中僅展示出了三個核心5508a、5508b、5508c，但是處理器5504可包含任何其他適當數量的處理核心，例如，數十個或甚至數百個處理核心。處理器核心5508a、5508b、5508c可被實現在一單一積體電路(IC)晶片上。此外，該晶片可以包含一或多個共享及/或私有的快取、匯流排或互連、圖形及/或記憶體控制器、或其他的組件。

【0042】 在一些實施例中，處理器5504包含快取5506。在一實例中，快取5506的部分可被專用於各個核心5508(例如，快取5506的一第一部分被專用於核心5508a、快取5506的一第二部分被專用於核心5508b、等等)。在一實例中，快取5506的一或多個部分可以在兩個或更多個核心5508之間共享。快取5506可以分為不同級別，例如，1級(L1)快取、2級(L2)快取、3級(L3)快取、等等。

【0043】 在一些實施例中，處理器核心5504可以包括一提取單元以提取指令(包括有具有條件分支的指令)以供該核心5504執行。該等指令可以從諸如記憶體5530的任何儲存裝置被提取。處理器核心5504還可以包括一解碼單元，用以對該提取的指令進行解碼。例如，該解碼單元可以把該提取出的指令解碼為複數個微運算。處理器核心5504可以包含一排程單元以執行與儲存之經解碼指令相關聯的各種操作。例如，該排程單元可以保有來自該解碼單元的資料直到該

等指令準備好分派為止，例如，直到一經解碼指令之所有的來源值變得可用為止。在一個實施例中，該排程單元可以排程及/或發布(或分派)經解碼的指令到給一執行單元來執行。

【0044】 該執行單元可以在指令被解碼(例如，由該解碼單元)及被分派(例如，由該排程單元)之後執行該等被分派的指令。在一實施例中，該執行單元可以包含一個以上的執行單元(諸如一成像運算單元、一圖形運算單元、一通用運算單元、等等)。該執行單元還可以執行各種算術運算，例如加法、減法、乘法、及/或除法，並且可以包含一或多個算術邏輯單元(ALU)。在一實施例中，一協同處理器(圖中未示出)可結合該執行單元來執行各種算術運算。

【0045】 此外，執行單元可以亂序執行指令。因此，在一個實施例中，處理器核心5504可以是一亂序處理器核心。處理器核心5504還可包含一退出單元。該退出單元可以在指令被達成之後退出已執行的指令。在一實施例中，該等已執行指令的退出可導致處理器狀態為該等指令該執行被達成、由該等指令所使用的實體暫存器被解除分配、等等。處理器核心5504還可包含一匯流排單元以實現經由一或多個匯流排在處理器核心5504的組件與其他組件之間的通訊。處理器核心5504還可以包含一或多個暫存器以儲存由該核心5504之各種組件所存取的資料(諸如與分配的應用優先級及/或子系統狀態(模式)關聯相關的值)。

【0046】 在一些實施例中，裝置5500包含連接電路5531。例如，連接電路5531包括硬體裝置(例如，無線及/或有線連接器及通訊硬體)及/或軟體組件(例如，驅動程式、協定堆疊)，例如，以使裝置5500能夠與外部裝置進行通訊。裝置5500可以與諸如其他運算裝置、無線接入點或基站、等等之類的外部裝置分離。

【0047】 在一實例中，連接電路5531可以包含多種不同類型的連接。概括

地說，該等連接電路5531可以包含蜂巢式連接電路、無線連接電路、等等。連接電路5531的蜂巢式連接電路一般係指由無線運營商提供的蜂巢式網路連接，諸如經過GSM(全球移動通訊系統)或變型或衍生物、CDMA(分碼多重存取)或變型或衍生物、TDM(分時多工)或變型或衍生物、第三代合作夥伴計劃(3GPP)通用移動電信系統(UMTS)系統或變型或衍生物、3GPP長期演進技術(LTE)系統或變型或衍生物、3GPP先進長期演進技術(LTE-A)系統或變型或衍生物、第五代 (5G)無線系統或變型或衍生物、5G行動網路系統或變型或衍生物、5G新無線電(NR)系統或變型或衍生物、或其他蜂巢式服務標準。連接電路5531的無線連接電路(或無線介面)係指非蜂巢式的無線連接，可包含個人區域網路(諸如藍牙、近場、等等)、區域網路(諸如Wi-Fi)及/或廣域網路(例如WiMax)及/或其他的無線通訊。在一實例中，連接電路5531可包括一網路介面，諸如一有線或無線介面，例如，使得一系統實施例可被併入到一無線裝置中，例如一手機或個人數位助理。

【0048】 在一些實施例中，裝置5500包含控制集線器5532，其代表與一或多個I/O裝置互動相關的硬體裝置及/或軟體組件。例如，處理器5504可以經由控制集線器5532與顯示器5522、一或多個週邊裝置5524、儲存裝置5528、一或多個其他外部裝置5529等等中的一或多個進行通訊。控制集線器5532可以是一晶片組、一平台控制集線器(PCH)、等等。

【0049】 例如，控制集線器5532圖示了用於連接到裝置5500之附加裝置的一或多個連接點，例如，使用者可以通過這些連接點與該系統互動。例如，可被連接到裝置5500的裝置(例如，裝置5529)包括麥克風裝置、揚聲器或立體聲系統、音訊裝置、視訊系統或其他顯示器裝置、鍵盤或小鍵盤裝置、或用於特定應用使用的其他I/O裝置諸如讀卡器或其他的裝置。

【0050】 如以上所述，控制集線器5532可以與音訊裝置、顯示器5522、等等互動。例如，透過一麥克風或其他音訊裝置的輸入可以為裝置5500的一或多

個應用程式或功能提供輸入或命令。此外，音訊輸出可被提供來代替顯示器輸出或作為顯示器輸出的補充。在另一實例中，如果顯示器5522包括一觸控螢幕，則顯示器5522還充當一輸入裝置，其可至少部分地由控制集線器5532來管理。在運算裝置5500上還可以存在附加的按鈕或開關以提供I/O由控制集線器5532所管理的功能。在一個實施例中，控制集線器5532管理諸如加速度計、相機、光感測器或其他環境感測器之類的裝置、或可被包括在裝置5500中的其他硬體。該輸入可以是直接使用者互動的一部分，以及為該系統提供環境輸入以影響其操作(例如過濾雜訊、調整顯示以進行亮度檢測、為相機施加一閃光燈、或其他的功能)。

【0051】 在一些實施例中，控制集線器5532可以使用任何適當的通訊協定耦合到各種裝置，例如PCIe(快速週邊組件互連)、USB(通用串列匯流排)、Thunderbolt、高解析度多媒體介面(HDMI)、火線、等等。

【0052】 在一些實施例中，顯示器5522 表示為使用者提供視覺及/或觸覺顯示器以與裝置5500互動的硬體(例如，顯示器裝置)及軟體(例如，驅動程式)組件。顯示器5522可以包括一顯示器介面、一顯示器螢幕、及/或用於向使用者提供一顯示器的硬體裝置。在一些實施例中，顯示器5522包括同時向使用者提供輸出及輸入兩者的一觸控螢幕(或觸控板)裝置。在一實例中，顯示器5522可以直接與該處理器5504通訊。顯示器5522可以是一個或多個內部顯示器裝置，如在一行動電子裝置或一膝上型裝置或經由一顯示器介面(例如，DisplayPort、等等)所附接的一外部顯示器裝置中。在一個實施例中，顯示器5522可以是一頭戴式顯示器(HMD)諸如用於虛擬實境(VR)應用中或擴增實境(AR)應用中的一立體顯示器裝置。

【0053】 在一些實施例中，儘管在圖中未被示出，除了(或代替)處理器5504之外，裝置5500可以包括圖形處理單元(GPU)，該圖形處理單元包含有一或多個

圖形處理核心，其可以控制在該顯示器5522上顯示內容的一或多個方面。

【0054】 控制集線器5532(或平台控制器集線器)可以包含硬體介面及連接器，以及軟體組件(例如，驅動程式、協定堆疊)以進行週邊連接，例如到週邊裝置5524。

【0055】 應被理解的是，裝置5500既可以是其他運算裝置的一週邊裝置，也可以具有連接到它的週邊裝置。裝置5500可以具有一「對接」連接器以連接到其他運算裝置，用於諸如管理(例如，下載及/或上傳、更改、同步)在裝置5500上的內容。此外，一對接連接器可允許裝置5500連接到可允許運算裝置5500控制內容輸出至例如視聽或其他系統的某些週邊裝置。

【0056】 除了專有的對接連接器或其他專有的連接硬體之外，裝置5500還可以經由共用或基於標準的連接器進行週邊連接。常見類型可包括通用串列匯流排(USB)連接器(其可包括多種不同硬體介面中的任何一種)、包括有MiniDisplayPort (MDP)的DisplayPort、高解析度多媒體介面(HDMI)、火線、或其他的類型。

【0057】 在一些實施例中，連接電路5531可被耦合到控制集線器5532，例如在除了被直接耦合到該處理器5504之外，或取代被直接耦合到該處理器5504。在一些實施例中，顯示器5522可被耦合到控制集線器5532，例如在除了被直接耦合到該處理器5504之外，或取代被直接耦合到該處理器5504。

【0058】 在一些實施例中，裝置5500包含經由記憶體介面5534被耦合到處理器5504的記憶體5530。記憶體5530包括用於在裝置5500中儲存資訊的記憶體裝置。

【0059】 在一些實施例中，記憶體5530包括如參考各種實施例所描述之用於保持穩定時脈信號的設備。記憶體可以包含非依電性(如果該記憶體裝置的電源被中斷，狀態不會改變)及/或依電性(如果該記憶體裝置的電源被中斷，狀態

係不確定的)記憶體裝置。記憶體裝置5530可以是一動態隨機存取記憶體(DRAM)裝置、一靜態隨機存取記憶體(SRAM)裝置、快閃記憶體裝置、相變記憶體裝置、或具有合適性能用作為處理記憶體的一些其他記憶體裝置。在一個實施例中，記憶體5530可以操作為用於裝置5500的系統記憶體，用以儲存當該等一或多個處理器5504執行一應用程式或程序時所使用的資料及指令。記憶體5530可以儲存應用程式資料、使用者資料、音樂、照片、文件檔、或其他的資料，以及與裝置5500之該等應用程式及功能執行相關的系統資料(無論是長期的還是暫時的)。

【0060】 各種實施例及實例的元件也被提供做為用於儲存該等電腦可執行指令(例如，實現本文討論之任何其他程序的指令)的一機器可讀取媒體(例如，記憶體5530)。該機器可讀取媒體(例如，記憶體5530)可以包括但不侷限於快閃記憶體、光碟、CD-ROM、DVD ROM、RAM、EPROM、EEPROM、磁卡或光卡、相變記憶體(PCM)、或適合儲存電子或電腦可執行指令之其他類型的機器可讀取媒體。例如，本發明的實施例可被下載作為一電腦程式(例如，BIOS)，該電腦程式可以經由一通訊鏈接(例如，一調變解調器或網路連接)藉由資料信號的方式從一遠端電腦(例如，一伺服器)傳送到一請求的電腦(例如，一客戶端)。

【0061】 在一些實施例中，裝置5500包含溫度測量電路5540，例如，用於測量裝置5500之各種組件的溫度。在一實例中，溫度測量電路5540可被嵌入、或被耦合或被附接到各種組件，其溫度將被測量並被監控。例如，溫度測量電路5540可以測量核心5508a、5508b、5508c、電壓調節器5514、記憶體5530、SoC 5501的一母板、及/或裝置5500之任何適當組件中的一或多個的(或其內部的)溫度。在某些實施例中，溫度測量電路系統5540包括一低功率混合反向(LPHR)帶隙基準(BGR)及數位溫度感測器(DTS)，其利用次臨界金屬氧化物半導體(MOS)電晶體及該PNP寄生雙極性接面電晶體(BJT)裝置以形成一反向BGR，其作為可

組配BGR或DTS操作模式的該基礎。該LPHR架構使用低成本MOS電晶體及該標準的寄生PNP裝置。基於一反向帶隙電壓，該LPHR可工作為一可組配的BGR。藉由把該可組配的BGR與該經縮放的基極-射極電壓進行比較，該電路還可以執行作為一DTS，該DTS具有一線性轉移函數具有實現高精確度用的單一溫度微調。

【0062】 在一些實施例中，裝置5500包含電力測量電路5542，例如，用於測量由裝置5500之一或多個組件所消耗的功率。在一實例中，除了測量電力之外，或取代測量電力，電力測量電路5542可以測量電壓及/或電流。在一實例中，該電力測量電路5542可被嵌入、或被耦合或被附接到各種組件，其功率、電壓、及/或電流消耗將被測量及監測。例如，電力測量電路5542可以測量由一或多個電壓調節器5514所提供的功率、電流及/或電壓、提供給SoC 5501的功率、提供給裝置5500的功率、由裝置5500的處理器5504(或任何其他組件)所消耗的功率、等等。

【0063】 在一些實施例中，裝置5500包含一或多個電壓調節器電路，通常被稱為電壓調節器(VR)5514。VR 5514產生處於適當電壓位準的信號，其可以被提供來操作裝置5500之任何適當的組件。僅作為一實例，VR 5514被圖示為向裝置5500的處理器5504提供信號。在一些實施例中，VR 5514接收一或多個電壓識別(VID)信號，並基於該等VID信號產生在一適當位準的該電壓信號。該VR 5514可以使用各種類型的VR。例如，VR 5514 可能包含一「降壓」VR、一「升壓」VR、降壓及升壓VR的一組合、低壓差(LDO)調節器、開關DC- DC調節器、基於恆定導通時間控制器的DC-DC調節器、等等。降壓VR通常被使用在需要把一輸入電壓以小於一的比率轉換為輸出電壓的供電應用中。升壓VR通常被使用在需要把一輸入電壓以大於一的比率轉換為輸出電壓的供電應用中。在一些實施例中，每一個處理器核心具有其自己的VR，其由PCU 5510a/b及/或PMIC 5512來控

制。在一些實施例中，每一個核心具有一分散式的LDO網路以提供對電力管理有效的控制。該等LDO可以是數位、類比、或數位或類比LDO的一組合。在一些實施例中，VR 5514包括電流追踪設備以測量通過電源軌的電流。

【0064】 在一些實施例中，VR 5514包括一數位控制方案以管理比例積分微分(PID)濾波器(也被稱為一數位III型補償器)的狀態。該數位控制方案控制該PID濾波器的該積分器以實現飽和該工作週期的非線性控制，在此期間，PID的比例及微分項被設置為0，而該積分器及其內部狀態(以前的值或記憶)被設置為一工作週期，即當前名目工作週期加上一deltaD的該總和。該deltaD係該最大的工作週期增量，其被使用來把一電壓調節器從ICCmin調整到ICCmax，並且是可以在矽後被設置的一組配暫存器。一狀態機從非線性全導通狀態(其把該輸出電壓Vout帶回一調節窗口)轉變為一開迴路工作週期，從而保持該輸出電壓略高於該所需的參考電壓Vref。在該命令的工作週期下在此開迴路狀態經過一特定時間段之後，該狀態機會逐漸降低該開迴路工作週期值，直到該輸出電壓接近該所命令的Vref為止。因此，來自VR 5514該輸出電源上的輸出顫動被完全地消除(或實質上被消除)，並且只有單一一個下沖轉移，這可導致一保證的Vmin，其係基於一比較器延遲以及具有該可用輸出去耦電容之該負載的該di/dt。

【0065】 在一些實施例中，VR 5514包含一單獨的自啟動控制器，其在沒有熔線及/或調整資訊的情況下起作用。該自啟動控制器保護VR 5514 免於受大浪湧電流及電壓過衝的影響，同時能夠跟隨由該系統所施加之一可變的VID(電壓識別)參考斜坡。在一些實施例中，該自啟動控制器使用內置於該控制器中的一張弛振盪器來設置該降壓轉換器的該開關頻率。該振盪器可以使用一時脈或電流參考來進行初始化，以接近一所需的工作頻率。VR 5514的該輸出被弱耦合到該振盪器，以設置用於閉迴路操作的該工作週期。該控制器被自然地偏置，使得該輸出電壓始終略高於該設定點，從而無需對任何工序、電壓、及/或溫度

(PVT)施加微調。

【0066】 在一些實施例中，裝置5500包含一或多個時脈產生器電路，一般被稱為時脈產生器5516。時脈產生器5516在適當的頻率位準產生時脈信號，其可被提供給裝置5500之任何適當的組件。僅作為一實例，時脈產生器5516被圖示為向裝置5500的處理器5504提供時脈信號。在一些實施例中，時脈產生器5516接收一或多個頻率識別(FID)信號，並基於該等FID信號以一適當的頻率產生該等時脈信號。

【0067】 在一些實施例中，裝置5500包含向裝置5500的各種組件供電的電池5518。僅作為一實例，電池5518被圖示為向處理器5504供電。雖然在圖中未被示出，但裝置5500可以包含一充電電路，例如，基於從一AC適配器所接收的交流(AC)電源為該電池充電。

【0068】 在一些實施例中，電池5518以充電至一預設的電壓(例如，4.1V)周期性地檢查一實際的電池容量或能量。然後該電池確定該電池容量或能量。如果該容量或能量不足，則在該電池中或與該電池相關聯的一設備將稍微把充電電壓增加到該容量為足夠的一個點(例如從4.1V到4.11V)。週期性地檢查並略微增加充電電壓的該程序被執行，直到充電電壓達到規格限制(例如，4.2V)為止。這裡所描述的方案具有一些優點，諸如可以延長電池壽命、可以降低能量儲備不足的風險、可盡可能長時間地使用突發電力、及/或可以使用甚至更高的突發電力。

【0069】 在一些實施例中，該充電電路(例如，5518)包含一降壓-升壓轉換器。該降壓-升壓轉換器包含DrMOS或DrGaN裝置，被使用來代替用於傳統降壓-升壓轉換器的半橋。本文的各種實施例係參考DrMOS來被描述的。然而，該等實施例亦適用於DrGaN。由於減少的寄生及最佳化的MOSFET封裝，該等DrMOS裝置可實現更佳的電力轉換效率。由於該空檔時間管理係內部於該DrMOS，該

空檔時間管理比傳統降壓-升壓轉換器更為準確，從而實現更高的轉換效率。更高的工作頻率允許較小的電感器大小，這反過來又降低了包含有基於該DrMOS降壓-升壓轉換器之該充電器的z高度。各種實施例的降壓-升壓轉換器包含用於DrMOS裝置的雙折疊自我啟動。在一些實施例中，除了該等傳統的自我啟動電容器之外，還添加了折疊的自我啟動電容器，其把電感器節點交互耦合到該等兩組DrMOS開關。

【0070】 在一些實施例中，裝置5500包含電力控制單元(PCU)5510(也被稱為電力管理單元(PMU)、電力管理控制器(PMC)、電力單元(p-單元)、等等)。在一實例中，PCU 5510的一些部分可由一或多個處理核心5508來實現，並且PCU 5510的這些部分使用一虛線框被象徵性地圖示出，並被標記為PCU 5510a。在一實例中，PCU 5510的一些其他部分可以在該等處理核心5508之外面來被實現，並且PCU 5510的這些部分使用一虛線框被象徵性地圖示出並且被標記為PCU 5510b。PCU 5510可以為裝置5500實現各種電力管理操作。PCU 5510可以包含硬體介面、硬體電路、連接器、暫存器、等等，以及軟體組件(例如，驅動程式、協定堆疊)，以實現用於裝置5500的各種電力管理操作。

【0071】 在各種實施例中，PCU或PMU 5510以一分層的方式被組織，形成一分層電力管理(HPM)。各種實施例的HPM構建出可用於該平台之封裝級別管理的一能力及基礎架構，同時仍然迎合可能存於遍及在該封裝中該組成晶粒的自治孤立區。HPM並不假定實體分區到域的一預定映射。一HPM域可以與被整合在一小晶粒內部的一功能、一小晶粒邊界、一或多個小晶粒、一伴隨晶粒、或甚至一分立的CXL裝置對齊。HPM解決了在同一晶粒上多個實例的整合、與整合在同一晶粒上或分開晶粒上的專有功能或第三方功能混合、並且甚至係經由CXL(例如 Flexbus)所連接的加速器，其可能位於該封裝內部，或在一分立的形狀因子中。

【0072】 HPM使設計人員能夠滿足可擴展性、模組化及後期綁定的該等目標。HPM還允許利用可能已經存在於其他晶粒上的PMU功能，而不是在該扁平型方案中被禁用。HPM啟用功能之任意隨意集合的管理，而與其整合的級別無關。各種實施例的HPM係可擴展的、模組化的、與對稱多晶片處理器(MCP)一起工作、並且與非對稱MCP一起工作。例如，HPM不需要一信號PM控制器及封裝基礎架構來成長超出合理的擴展限制。HPM支援在一封裝中後期添加一晶粒，而無需要在該基礎晶粒架構中做出更改。HPM解決了把具有不同工序技術節點的晶粒耦合在一單一封裝中的分解解決方案的需求。HPM還解決了配套晶粒整合解決方案的該等需求—在封裝的內外。

【0073】 在各種實施例中，每一個晶粒(或小晶粒)包含一電力管理單元(PMU)或p-單元。例如，處理器晶粒可以有一監督者p-單元、受監督者p-單元或一雙重角色監督者/受監督者p-單元。在一些實施例中，一I/O晶粒具有其自身的雙重角色p-單元，諸如監督者及/或受監督者p-單元。在每一個晶粒中的該等p-單元可以是一通用p-單元的實例。在一個這樣的實例中，所有的p-單元具有相同的能力及電路，但被組配成(動態地或靜態地)扮演監督者、受監督者、及/或兩者都有的角色。在一些實施例中，用於運算晶粒的該等p-單元是係一運算p-單元的實例，而用於IO晶粒的p-單元係不同於該運算p-單元之一IO p-單元的實例。取決於該角色，p-單元獲得特定的職責以管理該多晶片模組及/或運算平台的電力。雖然係針對在一多晶片模組或系統單晶片中的晶粒描述了各種p-單元，但一p-單元也可以是一外部裝置諸如I/O裝置的一部分。

【0074】 在這裡，各種p-單元不一定相同。該HPM架構可以操作非常不同類型的p-單元。該等p-單元的一個共同特徵是它們被期望要接收HPM訊息並期望要能夠對其解讀。在一些實施例中，IO晶粒的該p-單元可以不同於該等運算晶粒的該p-單元。例如，在該IO p-單元中每一類暫存器的暫存器實例數量與在該等

運算晶粒的該等p-單元中的暫存器實例數量不同。一IO晶粒具有作為CXL連接裝置之 HPM監督者的能力，但運算晶粒可能不需具有該功能。該IO及運算晶粒也有不同的韌體流程及可能有不同的韌體映像。這些是一實現方式可以做出的選擇。一HPM架構可以選擇擁有一個超集韌體映像，並有選擇性地執行與該韌體相關聯之該晶粒類型有關的流程。或者，對於每一種p-單元類型都可以有一個顧客韌體；它可允許更為流線型的調整用於每一種p-單元類型的該韌體儲存需求。

【0075】 在每一個晶粒中的該p-單元可被組配為一監督者p-單元、受監督者p-單元或具有一監督者/受監督者雙重角色。因此，p-單元可以在不同的領域扮演監督者或受監督者的角色。在各種實施例中，p-單元的每一個實例能夠自主地管理本地專用的資源並且包含用以聚合資料及在實例之間通訊的結構，以藉由被組配為該共享資源監督者的該實例來實現共享的資源管理。一種基於訊息及線路的基礎架構被提供，其可被複製及組配以促進在多個p-單元之間的管理及流動。

【0076】 在一些實施例中，電力及熱臨界值由一監督者p-單元傳達給受監督p-單元。例如，一監督者p-單元了解每一個晶粒的工作負載(當前及未來)、每一個晶粒的電力測量值、以及其他參數(例如平台級別的電力邊界)，並確定用於每一個晶粒的新電力限制。這些電力限制然後由監督者p-單元經由一或多個互連及結構傳達給該受監督者p-單元。在一些實施例中，一結構表示包含一第一結構、一第二結構、以及一快速響應互連的一組結構及互連。在一些實施例中，該第一結構被使用於在一監督者p-單元與一受監督者p-單元之間的常見通訊。這些常見的通訊包含在一晶粒之電壓、頻率、及/或電力狀態中的變化，其基於多個因素(例如，未來工作量、使用者行為、等等)而被計劃。在一些實施例中，該第二結構被使用於在監督者p-單元與受監督者p-單元之間較高優先級的通訊。較高優先級通訊的實例包括由於可能的熱失控狀況、可靠性問題、等等而要進行

節流的一訊息。在一些實施例中，一快速響應互連被使用來傳達所有晶粒的快速或硬節流。在這種情況下，例如，一監督者p-單元可以向所有其他的p-單元發送一快速節流訊息。在一些實施例中，一快速響應互連係其功能可由該第二結構所執行的一種傳統互連。

【0077】 各種實施例的該HPM架構實現對稱及/或非對稱晶粒的可擴展性、模組化、以及後期綁定。在本文中，對稱晶粒係具有相同尺寸、類型、及/或功能的晶粒，而非對稱晶粒係具有不同尺寸、類型、及/或功能的晶粒。分層的方法還允許利用可能已經存在於其他晶粒上的 PMU功能，而不是在該傳統的扁平型電力管理方案中被禁用。HPM並不假定實體分區到域的一預定映射。一HPM域可以與被整合在一小晶粒內部的一功能、一小晶粒邊界、一或多個小晶粒、一伴隨晶粒、或甚至一分立的CXL裝置對齊。HPM啟用功能之任意隨意集合的管理，而與它們的整合的級別無關。在一些實施例中，基於一或多個因子，一p-單元被宣稱為一監督者p-單元。這些因子包括記憶體大小、實體限制(例如，引腳的數量)、及感測器(例如，溫度、功耗、等等感測器)的位置以確定該處理器的實體限制。

【0078】 各種實施例的該HPM架構，提供了一種擴展電力管理的一構件，使得一單一p-單元實例不需要知道該處理器整體。這可以實現更小粒度的電力管理，並提高響應時間及效率。分層結構為該使用者保持一整體視圖。例如，在一作業系統(OS)級別，即使該PMU被實體地分佈在一或多個監督者-受監督者組配中，HPM體系結構也為該OS提供了一單一PMU視圖。

【0079】 在一些實施例中，該HPM架構係集中式的，其中一個監督者控制所有的受監督者。在一些實施例中，該HPM架構是去中心化的，其中在各個晶粒中的各個-單元通過對等通訊來控制整體電力管理。在一些實施例中，該HPM架構是分散式的，其中對於不同的域有不同的監督者。一分散式架構的一個實

例係一樹狀架構。

【0080】 在一些實施例中，裝置5500包含電力管理積體電路(PMIC)5512，例如，以實現用於裝置5500的各種電力管理作業。在一些實施例中，PMIC 5512係一可組配電力管理IC(RPMIC)及/或IMVP(Intel®移動電壓定位)。在一實例中，該PMIC位於與處理器5504分離的一IC晶粒內。它可以實現用於裝置5500的各種電力管理操作。PMIC 5512可以包含硬體介面、硬體電路、連接器、暫存器、等等，以及軟體組件(例如，驅動程式、協定堆疊)，以實現用於裝置5500的各種電力管理操作。

【0081】 在一實例中，裝置5500包含PCU 5510或PMIC 5512之一或兩者。在一實例中，PCU 5510或PMIC 5512中的任何一個可以不存在於裝置5500中，因此，使用虛線來圖示出這些組件。

【0082】 裝置5500的各種電力管理操作可由PCU 5510、PMIC 5512、或PCU 5510及PMIC 5512的一組合來執行。例如，PCU 5510及/或 PMIC 5512可為裝置5500的各種組件選擇一電力狀態(例如，P-狀態)。例如，PCU 5510及/或 PMIC 5512可以為裝置5500的各種組件選擇一電力狀態(例如，根據該ACPI(先進組配及電力介面)規範)。僅作為一實例，PCU 5510及/或PMIC 5512可致使該裝置5500 的各種組件轉移到一睡眠狀態、到一活動狀態、到一適當的C狀態(例如，C0狀態或另一個適當的C狀態，根據該ACPI規範)、等等。在一實例中，PCU 5510及/或PMIC 5512可以控制由VR 5514所輸出的一電壓及/或由該時脈產生器輸出之一時脈信號的一頻率，例如分別藉由輸出該VID信號及/或該FID信號。在一實例中，PCU 5510及/或PMIC 5512可以控制電池電力的使用、電池5518的充電、以及與省電操作相關的特徵。

【0083】 該時脈產生器5516可以包含一鎖相迴路(PLL)、鎖頻迴路(FLL)、或任何合適的時脈源。在一些實施例中，處理器5504的每一個核心具有其自己

的時脈源。因此，每一個核心可以在獨立於另一個核心的該操作頻率的一頻率下操作。在一些實施例中，PCU 5510及/或PMIC 5512執行自適應或動態的頻率縮放或調整。例如，如果該核心未在其最大功耗臨界值或限制下運行，則可以增加一處理器核心的時脈頻率。在一些實施例中，PCU 5510及/或PMIC 5512確定一處理器之每一個核心的該操作條件，並且當該PCU 5510及/或 PMIC 5512判定該核心正在一目標效能位準以下運行時，在該核心時脈源(例如，該核心的PLL)不失鎖的情況下，機會性地調整該核心的頻率及/或電源電壓。例如，如果一核心從一電源軌所汲取的電流小於分配給該核心或處理器5504的一總電流，則PCU 5510及/或PMIC 5512可以暫時地增加該核心或處理器5504的該電力汲取(例如，藉由增加時脈頻率及/或電源電壓位準)，使得該核心或處理器5504可以在更高的效能位準上執行。因此，可以在不違反產品可靠性的情況下為處理器5504臨時地增電壓及/或頻率。

【0084】 在一實例中，PCU 5510及/或PMIC 5512可以執行電力管理操作，例如，至少部分地基於從電力測量電路5542、溫度測量電路5540、電池5518的充電位準接收的測量、及/或任何其他適當可被使用來用於電力管理的資訊。為此，PMIC 5512被通訊地耦合到一或多個感測器以感測/檢測對該系統/平台的電力/熱行為有一影響之一或多個因子中各種數值/變化。該等一或多個因子的實例包括電流、電壓降、溫度、工作頻率、工作電壓、功耗、核心之間通訊活動、等等。這些感測器中的一或多個可以與一運算系統的一或多個組件或邏輯/IP區塊實體接近地(及/或熱接觸/耦合)。此外，在至少一個實施例中，感測器可被直接地耦合到PCU 5510及/或PMIC 5512，以允許PCU 5510及/或PMIC 5512至少部分地基於由該等感測器之一或多個所檢測到的值來管理處理器核心能量。

【0085】 也被圖示出的係裝置5500的一實例軟體堆疊(儘管未圖示出該軟體堆疊的所有元素)。僅作為一實例，處理器5504可以執行應用程式5550、作業

系統5552、一或多個電力管理(PM)特定應用程式(例如，一般被稱為PM應用程式5558)、等等。PM應用5558也可由該PCU 5510及/或PMIC 5512來執行。OS 5552還可包括一或多個PM應用5556a、5556b、5556c。該OS 5552還可以包括各種驅動程式5554a、5554b、5554c、等等，其中一些可以專用於電力管理目的。在一些實施例中，裝置5500更可包含一基本輸入/輸出系統(BIOS)5520。BIOS 5520可以與OS 5552進行通訊(例如，經由一或多個驅動程式5554)、與處理器5504進行通訊、等等。

【0086】 例如，PM應用程式5558、5556、驅動程式5554、BIOS 5520、等等中的一或多個可被使用來實現電力管理特定任務，例如控制裝置5500之各種組件的電壓及/或頻率，以控制喚醒啟動狀態、睡眠狀態、及/或裝置5500之各種組件的任何其他適當的電力狀態、控制電池電力使用、該電池5518的充電、與省電操作相關的特徵、等等。

【0087】 在一些實施例中，電池5518係具有一壓力室的鋰金屬電池以允許在一電池上施加均勻的壓力。該壓力室由金屬板(諸如均壓板)來支撐的，被使用來為該電池提供均勻的壓力。該壓力室可以包括加壓的氣體、彈性材料、彈簧板、等等。該壓力室的該外板可以自由地彎曲，在其邊緣受到(金屬)板的限制，但仍然對正在壓縮該電池胞元的該板施加一均勻的壓力。該壓力室為電池提供均勻的壓力，其被使用來實現高能量密度電池，例如，電池壽命延長20%。

【0088】 在一些實施例中，在PCU 5510a/b上執行的pCode具有為該pCode運行時支援啟用額外的運算及遙測資源的能力。這裡的pCode 係指由PCU 5510a/b所執行用以管理該5501效能的一韌體。例如，pCode可以為該處理器設置頻率及適當的電壓。該pCode的一部分可經由OS 5552來存取。在各種實施例中，提供了基於工作負載、使用者行為、及/或系統條件來動態地改變能量效能偏好(EPP)值的機制及方法。在OS 5552與該pCode之間可能有一明確定義的介面。該

介面可以允許或促進數個參數的該軟體組配及/或可以向該pCode提供提示。作為一實例，一EPP參數可以告知一pCode演算法是效能還是電池壽命更為重要。

【0089】 該OS 5552也可藉由把機器學習支援作為OS 5552的一部分來完成這種支援，並且藉由機器學習預測調整該OS向該硬體(例如，SoC 5501的各種組件)提示的該EPP值，或是以類似於一動態調整技術(DTT)驅動程式所做的方式向該pCode提供該機器學習預測。在此模型中，OS 5552可能對一DTT可用之同一組遙測具有可見性。作為一DTT機器學習提示設置的結果，根據該啟動類型的機器學習預測，pCode可能會調整其內部演算法以實現最佳電力及效能結果。例如，該pCode可能會增加針對該處理器利用率變化的責任以實現對使用者活動的快速響應，或者可能藉由減少對該處理器利用率的責任或藉由調整該節能最佳化來節省更多的電力並增加效能損失來增加對節能的傾向。這種方法可以有助於節省更多的電池壽命，以防所啟用的該等活動類型失去該系統可以啟用的某些效能位準。該pCode可包括用於動態EPP的演算法，該演算法可採用兩個輸入，一個來自OS 5552，另一個來自諸如DTT之類的軟體，並且可以選擇性地選擇以提供更高的效能及/或響應性。作為該方法的一部分，該pCode可以在該DTT中啟用一選項以針對不同類型的活動調整其對該DTT的反應。

【0090】 在一些實施例中，pCode提高了在電池模式下該SoC的該效能。在一些實施例中，pCode在電池模式下允許顯著更高的SoC峰值電力限制位準(並因此更高的Turbo效能)。在一些實施例中，pCode實現了電力節流並且是英特爾動態調整技術(DTT)的一部分。在各種實施例中，該峰值電力限制被稱為PL4。然而，該等實施例適用於其他的峰值電力限制。在一些實施例中，pCode以一種防止該系統意外關閉(或黑螢幕)如此的方式設置*Vth*臨界值電壓(該平台將會節流該SoC的該電壓位準)。在一些實施例中，pCode根據臨界值電壓(*Vth*)計算該*Psoc,pk* SoC峰值電力限制(例如，PL4)。這是兩個相依的參數，如果設置了一個，

則可以計算出另一個。pCode被使用來基於該系統參數及該操作的歷史最佳地設置一個參數(*Vth*)。在一些實施例中，pCode提供了一種基於該可用電池電力(其緩慢地變化)來動態地計算該節流的位準(*Psoc,th*)並設置該SoC節流峰值電力(*Psoc,th*)的方案。在一些實施例中，pCode基於*Psoc,th*決定該等頻率及電壓。在這種情況下，節流事件在該SoC效能上的負面影響較小。各種實施例提供一種允許最大效能(Pmax)框架來操作的方案。

【0091】 在一些實施例中，VR 5514包括一電流感測器以感測及/或測量通過VR 5514之一高側開關的電流。在一些實施例中，該電流感測器使用在反饋中具有被電容耦合輸入的一放大器，以感測該放大器的該輸入偏移，其可以在測量期間進行補償。在一些實施例中，在反饋中具有被電容耦合輸入的該放大器被使用來在該輸入共模規範被放寬的一區域中操作放大器，使得該反饋迴路增益及/或頻寬會更高。在一些實施例中，在反饋中具有被電容耦合輸入的該放大器被使用來從該轉換器輸入電壓操作感測器，方式係藉由採用高PSRR(電源抑制比)調節器來創建一本地、乾淨的電源電壓，從而減少對在該開關區域中該電力網的干擾。在一些實施例中，該設計的一變型可被使用來對在該輸入電壓與該控制器電源之間的該差異進行採樣，並在該電力及複製開關的該等汲極電壓之間重新創建該差異。這允許該感測器不會被暴露於該電源電壓。在一些實施例中，在反饋中具有被電容耦合輸入的該放大器被使用來補償在電流感測期間在該輸入電壓中與電力輸送網路相關(PDN相關)的變化。

【0092】 一些實施例使用三個組件來基於USB TYPE-C裝置5529的該等狀態來調整SoC 5501該的峰值電力。這些組件包括OS峰值電力管理器(OS 5552的一部分)、USB TYPE-C連接器管理器(OS 5552的一部分))以及USB TYPE-C協定裝置驅動程式(例如，驅動程式5554a、5554b、5554c中之一個)。在一些實施例中，當一USB TYPE-C電槽裝置從SoC 5501被連接或分離時，該USB TYPE-C連

接器管理器向該OS峰值電力管理器發送一同步請求；並且當該電槽轉換裝置狀態時，該USB TYPE-C協定裝置驅動程式發送一同步請求給該峰值電力管理器。在一些實施例中，當該USB TYPE-C連接器被附接到一電槽並且處於活動狀態(例如，高電力裝置狀態)時，該峰值電力管理器從該CPU獲取電力預算。在一些實施例中，當該USB TYPE-C連接器被分離或被附接並且電槽係閒置(最低裝置狀態)時，該峰值電力管理器會把該電力預算返還給該CPU以提高效能。

【0093】 在一些實施例中，邏輯被提供以動態地選擇用於BIOS電力啟動流程及睡眠退出流程(例如，S3、S4及/或S5)的該最佳操作處理核心。該自我啟動處理器(BSP)的該選擇被移至一早期電力啟動時間，而不是在任何時候之一固定的硬體選擇。為了獲得最大的啟動效能，該邏輯在一早期電力啟動時選擇該速度最快的核心作為該BSP。此外，為了最大程度地節省功耗，該邏輯選擇最具功率效率的核心作為該BSP。用於選擇該BSP的該處理器或切換發生在該啟動以及電力啟動流程(例如，S3、S4、及/或S5流程)期間。

【0094】 在一些實施例中，本文中的該等記憶體被組織成多級記憶體架構並且它們的效能由一去中心化的方案來掌控。該去中心化的方案包含p-單元5510及記憶體控制器。在一些實施例中，該方案基於應用程式如何使用遠離處理器核心的記憶體級別，動態地平衡了與在該平台5500中該處理器越來越遠之記憶體級別的數個參數諸如功率、熱度、成本、延遲及效能。在一些實例中，針對該遠處記憶體(FM)該狀態的該決策係分散的。例如，一處理器電力管理單元(p-單元)、近處記憶體控制器(NMC)、及/或遠處記憶體主機控制器(FMHC)在它們各自的級別做出有關於該FM之該電力及/或效能狀態的決定。這些決定被協調以提供針對一給定時間點之該FM的最佳電力及/或效能狀態。即使當該(等)處理器處於一特定的電力狀態時，該等記憶體的該電力及/或效能狀態也會自適應地改變以改變工作負載及其他參數。

【0095】 在一些實施例中，設備102被提供，其為系統5500執行一電力啟動方案。在一些實施例中，設備102運用一生物量測感測器(例如，一指紋感測器、眼感測器、等等)來在啟用運算系統5500的電力啟動之前驗證一使用者或以恢復轉移到一電力狀態(例如，由該先進組配與電力介面(ACPI)所定義的該等電力狀態之一)。把該生物量測感測器的輸出與一註冊使用者的資料進行比較以進行一匹配。該資料可包括被保存在一非依電性記憶體(例如，串列週邊介面(SPI)快閃裝置)中之該生物量測感測器一輸出的一原始副本。如果存在一匹配，則在該運算系統中的一邏輯將允許該運算系統的電力啟動。在沒有匹配的情況下，該運算系統不會被電力啟動。在一些實施例中，如果未找到匹配，則電池5518的充電也會被禁用。

【0096】 在本說明書中對「一實施例」、「一個實施例」、「一些實施例」、或「其他實施例」的引用意味著結合該等實施例所描述之一特定的特徵、結構、或特性被包括在至少一些實施例中，但是不一定是所有的實施例。「一實施例」、「一個實施例」、或「一些實施例」的各種出現不一定都是指相同的實施例。如果本說明書陳述「可能」、「有可能」、或「可以」包括某個組件、特徵、結構、或特性，則該特定組件、特徵、結構、或特性不一定要被包括。如果本說明書或請求項提及「一」或「一個」元素，並不意味著只有該等元素中的一個。如果本說明書或請求項提及「一附加」元素，並不排除存在多於一個的該等附加元素。

【0097】 在整個說明書及請求項中，術語「連接的」係指被連接的事物之間的一直接連接，諸如電氣、機械的、或磁性的連接，沒有任何中間的裝置。

【0098】 術語「被耦合的」係指透過一或多個被動或主動中間裝置的一直接或間接連接，諸如被連接的該等事物之間的直接電氣、機械、或磁性的連接或一間接連接。

【0099】 本文中的術語「相鄰」通常係指一物的位置，該位置緊鄰(例如，以在其之間有一或多個事物的方式來緊鄰或靠近)或鄰接另一物(例如，接觸它)。

【0100】 術語「電路」或「模組」可以指一或多個被動及/或主動組件，這些組件被安排為彼此相互協作以提供一所需的功能。

【0101】 術語「信號」可以指至少一種電流信號、電壓信號、磁性信號、或資料/時脈信號。「一」、「一個」、以及「該」的含義包含複數個的引用。「在」的含義包含「在...之內」及「在...之上」。

【0102】 術語「類比信號」係任何的連續信號，其中該信號的該時變特徵(變量)係某個其他時變量的一表示，即，類似於另一個時變信號。

【0103】 術語「數位信號」是係一種實體信號，它表示一離散值序列(一經量化的離散時間信號)，例如一任意位元流，或一經數位化的(採樣及類比到數位轉換的)類比信號。

【0104】 術語「縮放」通常係指把一設計(原理圖及佈局)從一種工序技術轉換為另一種工序技術，隨後可能會縮小佈局面積。在某些情況下，縮放還指把一設計從一種工序技術放大到另一種工序技術，並可能隨後增加佈局面積。術語「縮放」通常也指縮小或放大在同一技術節點內的佈局及裝置。術語「縮放」還可以指相對於另一個參數(例如，電源位準，來調整(例如，減慢或加速—即分別按比例縮小或按比例放大)一信號頻率。

【0105】 術語「實質上」、「接近」、「大約」、「靠近」、及「約為」通常係指在一目標值的+/- 10%以內。

【0106】 除非另有說明，使用序數形容詞「第一」、「第二」、以及「第三」、等等來描述一共同的物件，僅表示引用了相似物件的不同實例，並且並非意在暗示該等如此描述的物件必須在時間、空間、在排名中、或任何其他方式上處於一給定的順序。

【0107】 出於本發明的目的，短語「A及/或B」及「A或B」表示(A)、(B)、或(A及B)。出於本發明的目的，短語「A、B及/或C」係指(A)、(B)、(C)、(A及B)、(A及C)、(B及C)、或(A、B及C)。

【0108】 在本說明書及請求項中的術語「左」、「右」、「前」、「後」、「上」、「下」、「在...之上」、「在...之下」及類似用語，如果有的話，係被使用於描述的目的，並不一定用於描述永久的相對位置。

【0109】 需被指出的是，與任何其他圖示之該等元件具有相同參考號碼(或名稱)之該等圖示的那些元件可以以與所描述方式類似的任何方式操作或起作用，但不侷限於此。

【0110】 出於該等實施例的目的，在本文所描述的各種電路及邏輯區塊中的該等電晶體係金屬氧化物半導體(MOS)電晶體或其衍生物，其中該等MOS電晶體包含汲極、源極、閘極、以基極。該等電晶體及/或 MOS電晶體衍生物還包含三閘極及FinFET電晶體、閘極環繞圓柱形電晶體、穿隧FET(TFET)、方形導線、或矩形帶狀電晶體、鐵電 FET(FeFET)、或實現電晶體功能的其他裝置如碳奈米管或自旋電子裝置。MOSFET對稱的源極及汲極端子，係相同的端子，在本文中可被互換使用。在另一方面，一TFET裝置具有不對稱的源極及汲極端子。本領域的習知技藝者將理解的是，在不脫離本發明範圍的情況下，可以使用其他電晶體，例如雙極性接面電晶體(BJT PNP/NPN)、BiCMOS、CMOS、等等。

【0111】 本文中的術語「監督者」通常係指一電力控制器，或電力管理，單元(「p-單元」)，其單獨地或與一或多個其他p-單元合作地針對一或多個相關聯電力域中監視及管理與電力及效能相關的參數。電力/效能相關的參數可包括但不侷限於域電力、平台電力、電壓、電壓域電流、晶粒電流、負載線、溫度、裝置延遲、利用率、時脈頻率、處理效率、當前/未來工作負載資訊、以及其他參數。它可為該等一或多個域確定新的電力或效能參數(限制、平均操作、等等)。

然後可以把這些參數經由一或多個結構及/或互連傳遞給受監督者p-單元，或直接傳遞給受控或受監視的實體諸如VR或時脈節流控制暫存器。一監督者獲悉一或多個晶粒的該工作負載(當前及未來)、該等一或多個晶粒的電力測量值、以及其他參數(例如，平台級別的電力邊界)並確定用於該等一或多個晶粒的新電力限制。這些電力限制然後由監督者p-單元經由一或多個結構及/或互連被傳送到該等受監督者p-單元。在一晶粒具有一個p-單元的實例中，一監督者(Svor)p-單元也被稱為一監督者晶粒。

【0112】 本文中的術語「受監督者」通常係指一電力控制器，或電力管理，單元(一「p-單元」)，其單獨地或與一或多個其他p-單元合作地針對一或多個相關聯電力域中監視及管理與電力及效能相關的參數，並且接收來自一監督者的指令，以便為其相關聯的電力域設置電力及/或效能參數(例如，電源電壓、工作頻率、最大電流、節流臨界值、等等)。在一晶粒具有一個p-單元的實例中，一受監督者(Svee)p-單元也可被稱為一受監督者晶粒。請注意，一p-單元可以作為一Svor、一Svee、或同時作為一Svor/Svee p-單元。

【0113】 在本文中，術語「處理器核心」一般係指一獨立的執行單元，它可以與其他的核心並行地一次運行一程式執行續。一處理器核心可以包括一專用的電力控制器或電力控制單元(p-單元)，其可以動態地或靜態地被組配為一監督者或受監督者。在一些實例中，該專用的p-單元也被稱為一自主p-單元。在一些實例中，所有的處理器核心都具有相同的大小及功能，即對稱核心。但是，處理器核心也可以是不對稱的。例如，一些處理器核心與其他的處理器核心具有不同的大小及/或功能。一處理器核心可以是一虛擬處理器核心或一實體處理器核心。

【0114】 在本文中術語「晶粒」通常係指單一一塊連續的半導體材料(例如矽)，電晶體或其他構成一處理器核心的組件可能位於其中。多核心處理器可以

在在一單一晶粒上具有兩個或更多個處理器，但是備選地是，該等兩個或更多個處理器可被提供在兩個或更多個相應的晶粒上。每一個晶粒都有一專用的電力控制器或電力控制單元(p-單元)其可被動態地或靜態地被組配為一監督者或受監督者。在一些實例中，晶粒具有相同的大小及功能，即對稱核心。然而，晶粒也可以是不對稱的。例如，一些晶粒與其他的晶粒具有不同的大小及/或功能。

【0115】 在本文中，術語「互連」係指在兩個或多個點或節點之間的一通訊鏈路或通道。它可以包含一或多個單獨的傳導路徑，諸如導線、通孔、波導、被動組件、及/或主動組件。它還可以包含一結構。

【0116】 在本文中，術語「介面」通常係指被使用來與一互連進行通訊的軟體及/或硬體。一介面可以包括邏輯及I/O驅動程式/接收器，以通過該互連或一或多條導線來發送及接收資料。

【0117】 在本文中，術語「結構」通常係指具有一組已知的來源、目的地、路由安排規則、拓撲及其他屬性的通訊機制。該等來源及目的地可以是任何類型的資料處理功能單元，諸如電力管理單元。結構可以是沿著一晶粒的一xy平面二維展開及/或沿著一垂直及水平定位之晶粒堆疊的一xyz平面三維(3D)展開。一單一結構可以跨距多個晶粒。一結構可以採用任何拓撲，諸如網狀拓撲、星形拓撲、菊花鏈拓撲。一結構可能是具有多個代理之一網路單晶片(NoC)的一部分。這些代理可以是任何的功能單元。

【0118】 在本文中，術語「小晶粒」或「小晶片」通常係指一實體上不同的半導體晶粒，通常係以某一種方式被連接到一相鄰的晶粒，該種方式允許該結構跨越一晶粒邊界以像是一單一結構一樣來起作用，而不是兩個不同的結構來起作用。因此至少一些晶粒可以是小晶粒。每一個小晶粒可以包括一或多個p-單元，這些p-單元可被動態地或靜態地組配為監督者、受監督者或兩者。

【0119】 在本文中，術語「域」通常係指具有相似屬性(例如，電源電壓、工作頻率、電路或邏輯類型、及/或工作負載類型)及/或由一特定代理控制的邏輯或實體邊界。例如，一域可以是一組由一特定監督者控制的邏輯單元或功能單元。一域也可以被稱為一自治邊界(AP)。一域可以是整個系統單晶片(SoC)或該SoC的一部分，並由一p-單元來管理。

【0120】 此外，該等特定的特徵、結構、功能、或特性可以在一或多個實施例中以任何合適的方式被結合。例如，一第一實施例可以與一第二實施例結合，可以在與該等兩個實施例相關聯之該等特定特徵、結構、功能、或特性不相互排斥的任何地方相結合。

【0121】 雖然已經結合了特定的實施例描述了本發明，但是受到前述描述的啟發，這些實施例的許多替代、修改及變化對於本領域的普通技術人員來說將會是顯而易見的。本發明的實施例旨在包含落入所附請求項之廣泛範圍內的所有此類替代、修改、以及變化。

【0122】 此外，為了說明及討論的簡單性，並且為了不混淆本發明的內容，在該等所呈現的圖示中可能或可能不圖示出與積體電路(IC)晶粒及其他組件之眾所周知的電力/接地連接。此外，可以以方塊圖的形式展示出佈置以避免混淆本發明，並且還考慮到如此方塊圖佈置之實現方式細節高度依賴於本發明將在其中該平台被實現的該事實(即，這些細節應該在本領域習知技藝者的能力範圍內)。在為了描述本發明之實例實施例而闡述之特定細節(例如，電路)的情況下，對於本領域習知技藝者而言將顯而易見的是，可以在沒有這些特定細節或這些特定細節變化的情況下實踐本發明。因此，該描述應被認為是說明性的而不是限制性的。

【0123】 以下的實例涉及進一步的實施例。在該等實例中的細節可被使用來在一或多個實施例中的任何地方。在此所描述之該設備的所有可選特徵也可

以相對於一方法或程序來被實現。該等實例可以以任何的結合方式來結合。例如，實例4可以與實例2結合。

【0124】 實例1：一種設備，其包含有可由一控制信號來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到一運算平台；以及邏輯以根據在被儲存在記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。

【0125】 實例2：如實例1之設備，當該第一生物量測資料與該第二生物量測資料不匹配時，該邏輯關閉該電力閘以切斷在該第二電源軌上的一第二電源。

【0126】 實例3：如實例1之設備，當該第一生物量測資料與該第二生物量測資料實質上匹配時，該邏輯開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

【0127】 實例4：如實例1之設備，其包含有一生物量測控制器以當該生物量測感測器產生該第二生物量測資料時向該邏輯發出一中斷。

【0128】 實例5：如實例4之設備，其包含有一DC-DC轉換器以在該第一電源軌上接收一第一電力並且在一第三電源軌上產生一第三電力。

【0129】 實例6：如實例5之設備，其包含有一電力控制開關，以把該第三電源或在一第四電源軌上的一第四電力中之一個提供給一第五電源軌。

【0130】 實例7：如實例6之設備，其中該第四電源軌被耦合到一替代的電源。

【0131】 實例8：如實例7之設備，其中該替代的電源包含一硬幣型電池。

【0132】 實例9：如實例6之設備，其中該第五電源軌用以向該生物量測感測器、該生物量測控制器、該邏輯、以及該記憶體供電。

【0133】 實例10：如實例6之設備，其中該電力控制開關包含一多工器，其

當該第三電力低於一臨界值時向該第五電源軌提供該第四電力。

【0134】 實例11：如實例1之設備，其中該記憶體係一非依電性記憶體。

【0135】 實例12：如實例1之設備，其中該生物量測感測器係以下中之一個：一指紋感測器、一眼睛系統、一臉部識別設備。

【0136】 實例13：如實例1之設備，其中該第一電源軌被耦合到一電池充電器控制器，該電池充電器控制器被耦合到複數個電源。

【0137】 實例14：如實例13之設備，其中該等複數個電源包括：一USB Type-C電源、一電池、以及一AC適配器。

【0138】 實例15：一種機器可讀取儲存媒體，其具有機器可讀取指令儲存在其上，當執行該等指令時，致使一或多個機器執行一種方法，該方法包含有：根據一控制信號控制被耦合到一第一電源軌及一第二電源軌的一電源閘，其中該第二電源軌被耦合到一運算平台；以及根據在被儲存在記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號。

【0139】 實例16：如實例15之機器可讀取儲存媒體，其具有機器可讀取指令儲存在其上，當執行該等指令時，致使一或多個機器執行該方法，該方法包含有：當該第一生物量測資料與該第二生物量測資料不匹配時，關閉該電力閘以切斷在該第二電源軌上的一第二電源；或當該第一生物量測資料與該第二生物量測資料實質上匹配時，開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

【0140】 實例17：如實例15之機器可讀取儲存媒體，其具有機器可讀取指令儲存在其上，當執行該等指令時，致使一或多個機器執行該方法，該方法包含有：當該生物量測感測器產生該第二生物量測資料時發出一中斷。

【0141】 實例18：一種系統，其包含有：一電池充電器控制器以從一或多

個電源接收電力；被耦合到該電池充電器的一電力啟動設備；被耦合到該電力啟動設備的一處理器系統，其中該處理器系統包含具有一或多個處理核心的系統單晶片(SoC)，其中該電力啟動設備包含：可由一控制信號來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到該處理器系統；以及邏輯以根據在被儲存在記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。

【0142】 實例19：如實例18之系統，當該第一生物量測資料與該第二生物量測資料不匹配時，該邏輯關閉該電力閘以切斷在該第二電源軌上的一第二電源。

【0143】 實例20：如實例18之系統，當該第一生物量測資料與該第二生物量測資料實質上匹配時，該邏輯開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

【0144】 一摘要被提供，其將允許讀者確定本技術發明的該性質及要點。本發明人對該摘要被提交的理解為它將不會被使用來限制該等請求項的該範圍或含義。該等以下請求項特此被併入到該詳細說明中，其中每一個請求項自己獨立地作為一單獨的實施例。

【符號說明】

【0145】

100:運算系統

101:電池充電器控制器

102:安全的裝置電力啟動設備

103:該平台的其餘部分(ROP)

104:USB Type-C電源

105:電池

106:AC適配器

107:DC-DC轉換器

108:電力控制開關

109:邏輯

110:生物量測感測器控制器

111:NVM

112:電力控制器

113:替代電源

114:生物量測感測器

200:軟體堆疊

201:BIOS

202:MRC訓練資料

203:GOP

204:WiFi、藍牙韌體

205:uCode及p-單元補丁

206:安全的指紋資料區域

207:平台PHY韌體

208:CSE韌體

209:ISH韌體

210:嵌入式控制器韌體

211:PMC韌體

212:軟體帶

300:狀態圖

301～305:狀態

5500:裝置

5501:SoC

5504:處理器

5506:快取

5508a、5508b、5508c:核心

5510a、5510b:PCU

5512:PMIC

5514:電壓調節器

5516:時脈產生器

5518:電池

5520:BIOS

5522:顯示器

5524:週邊裝置

5528:儲存裝置

5529:其他外部裝置

5530:記憶體

5531:連接電路

5532:控制集線器

5534:記憶體介面

5540:溫度測量電路

5542:電力測量電路

5550:應用程式

5552:OS

5554a、5554b、5554c:驅動程式

5556a、5556b、5556c、5558:PM應用程式

【發明申請專利範圍】

【請求項1】 一種設備，其包含有：

可由一控制信號來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到一運算平台；以及

邏輯，其用以根據在被儲存於記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。

【請求項2】 如請求項1之設備，其中當該第一生物量測資料與該第二生物量測資料不匹配時，該邏輯要關閉該電力閘以切斷在該第二電源軌上的一第二電力。

【請求項3】 如請求項1之設備，其中當該第一生物量測資料與該第二生物量測資料實質上匹配時，該邏輯要開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

【請求項4】 如請求項1之設備，其更包含有一生物量測控制器以當該生物量測感測器產生該第二生物量測資料時向該邏輯發出一中斷。

【請求項5】 如請求項4之設備，其更包含有一DC-DC轉換器用以在該第一電源軌上接收一第一電力以及在一第三電源軌上產生一第三電力。

【請求項6】 如請求項5之設備，其更包含有一電力控制開關用以把該第三電力或在一第四電源軌上的一第四電力中之一者提供給一第五電源軌。

【請求項7】 如請求項6之設備，其中該第四電源軌被耦合到一替代的電源。

【請求項8】 如請求項7之設備，其中該替代的電源包含一硬幣型電池。

【請求項9】 如請求項6之設備，其中該第五電源軌要向該生物量測感測器、該生物量測控制器、該邏輯、以及該記憶體供電。

【請求項10】如請求項6之設備，其中該電力控制開關包含一多工器，當該第三電力低於一臨界值時，該多工器要向該第五電源軌提供該第四電力。

【請求項11】如請求項1-10中任一項之設備，其中該記憶體係一非依電性記憶體。

【請求項12】如請求項1-10中任一項之設備，其中該生物量測感測器係以下中之一者：一指紋感測器、一眼睛系統、或一臉部識別設備。

【請求項13】如請求項1-10中任一項之設備，其中該第一電源軌被耦合到一電池充電器控制器，該電池充電器控制器被耦合到複數個電源。

【請求項14】如請求項13之設備，其中該等複數個電源包括：一USB Type-C電源、一電池、以及一AC適配器。

【請求項15】一種機器可讀取儲存媒體，其具有機器可讀取指令儲存在其上，當該等指令被執行時，致使一或多個機器執行一種方法，該方法包含有：

根據一控制信號，控制被耦合到一第一電源軌及一第二電源軌的一電力閘，其中該第二電源軌被耦合到一運算平台；以及

根據在被儲存於記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號。

【請求項16】如請求項15之機器可讀取儲存媒體，其具有機器可讀取指令儲存在其上，當該等指令被執行時，致使該等一或多個機器執行該方法，該方法包含有：

當該第一生物量測資料與該第二生物量測資料不匹配時，關閉該電力閘以切斷在該第二電源軌上的一第二電力；或

當該第一生物量測資料與該第二生物量測資料實質上匹配時，開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

【請求項17】如請求項15或請求項16之機器可讀取儲存媒體，其具有機器

可讀取指令儲存在其上，當該等指令被執行時，致使該等一或多個機器執行該方法，該方法包含有：

當該生物量測感測器產生該第二生物量測資料時發出一中斷。

【請求項18】一種系統，其包含有：

一電池充電器控制器，其用以從一或多個電源接收電力；

被耦合到該電池充電器的一電力啟動設備；

被耦合到該電力啟動設備的一處理器系統，其中該處理器系統包含具有一或多個處理核心的一系統單晶片(SoC)，其中該電力啟動設備包含：

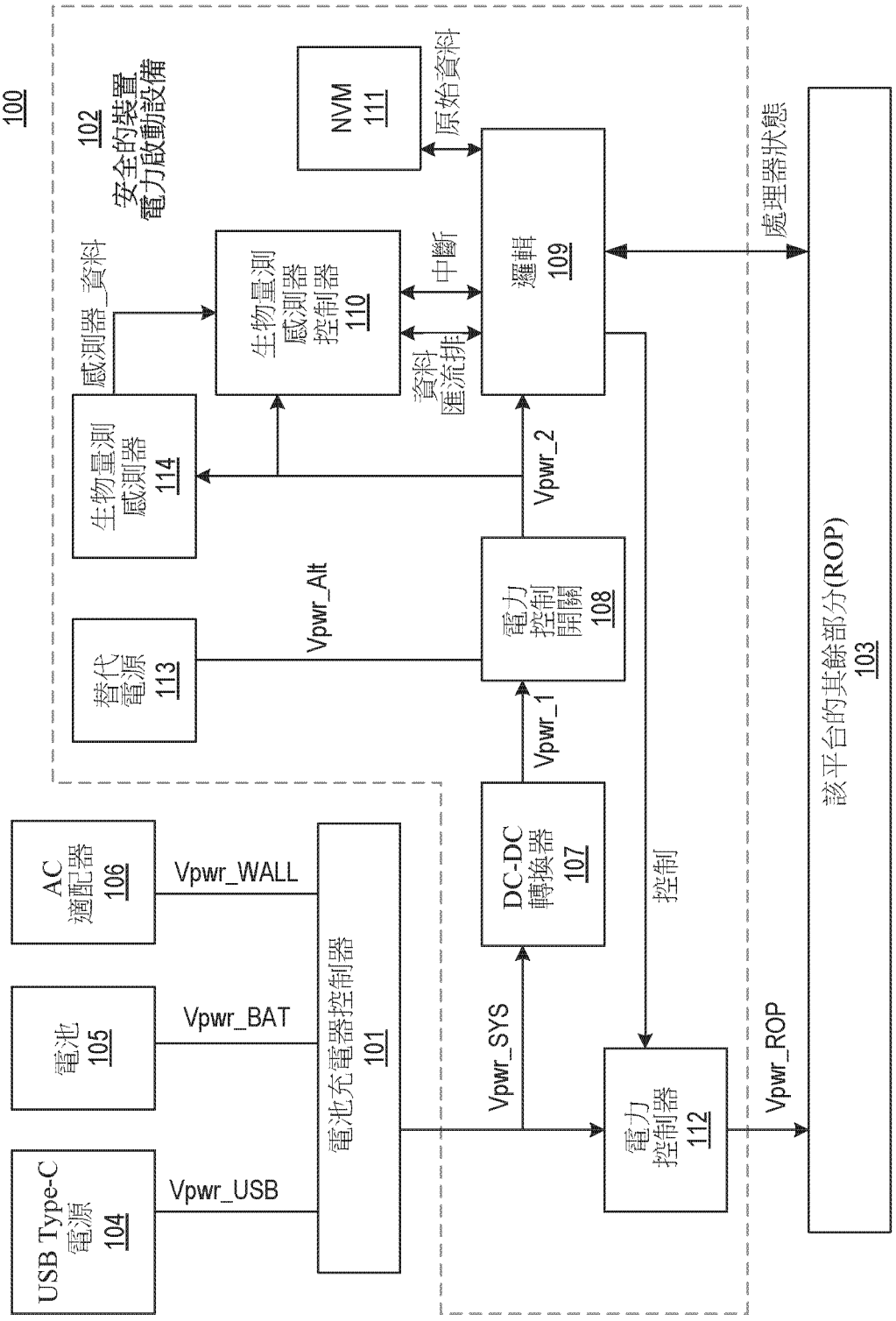
可由一控制信號來控制的一電力閘，該電力閘被耦合到一第一電源軌及一第二電源軌，其中該第二電源軌被耦合到該處理器系統；以及

邏輯，其用以根據在被儲存於記憶體中的一第一生物量測資料與由一生物量測感測器所感測的一第二生物量測資料之間的一匹配來產生該控制信號以開啟或關閉該電力閘。

【請求項19】如請求項18之系統，其中當該第一生物量測資料與該第二生物量測資料不匹配時，該邏輯要關閉該電力閘以切斷在該第二電源軌上的一第二電力。

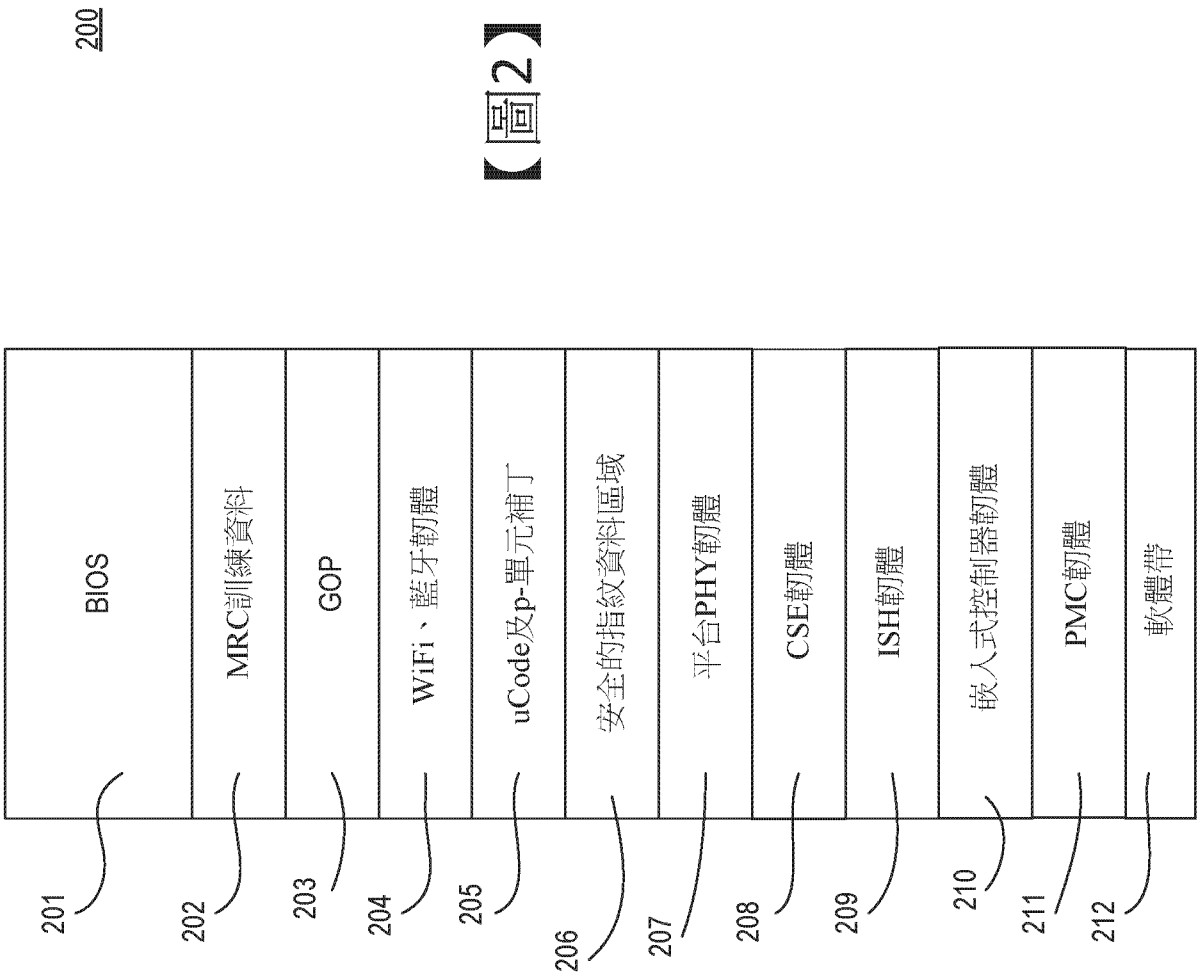
【請求項20】如請求項18或請求項19之系統，其中當該第一生物量測資料與該第二生物量測資料實質上匹配時，該邏輯要開啟該電力閘以提供該第一電力作為在該第二電源軌上的一第二電力。

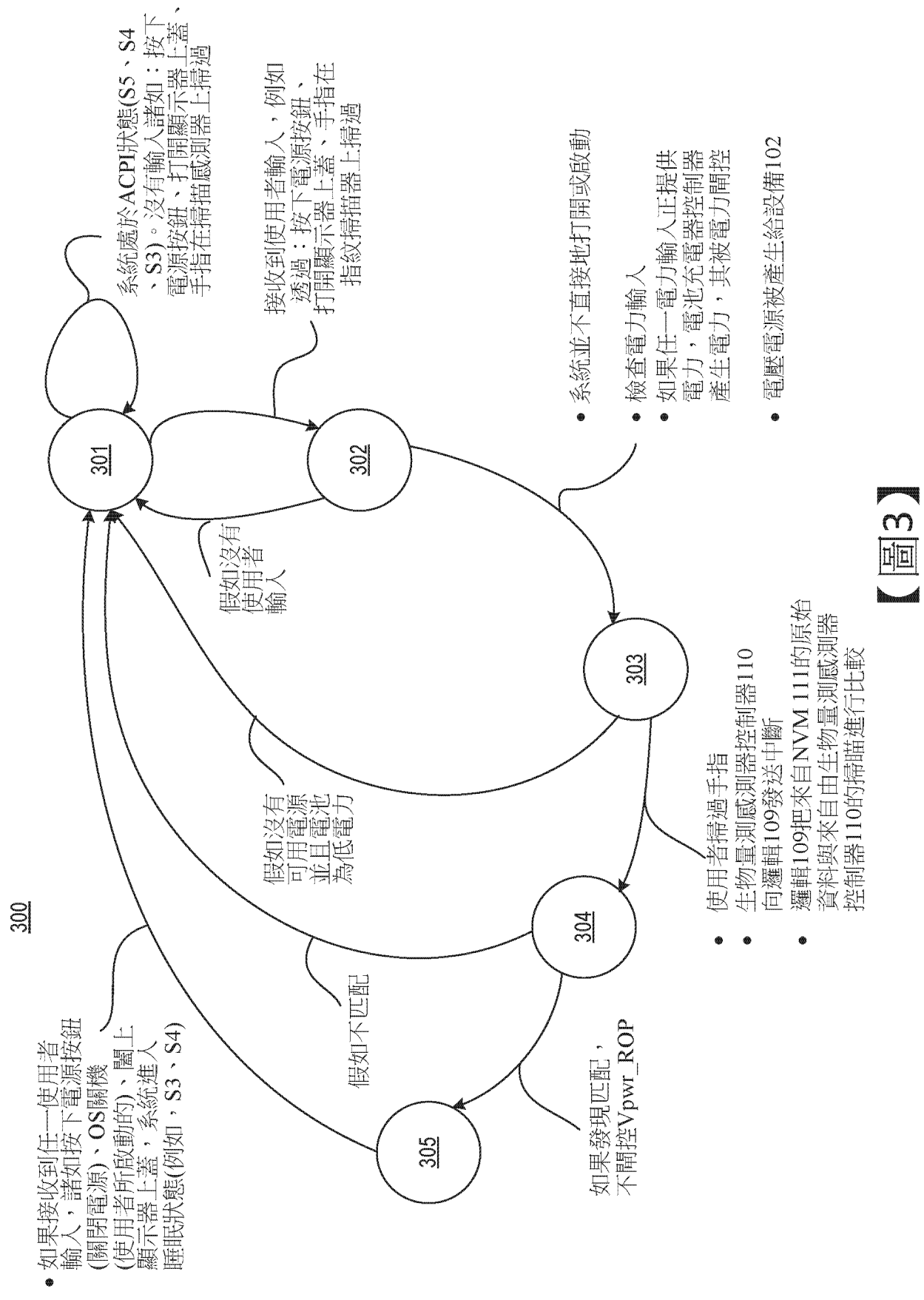
【發明圖式】


100
102
安全的裝置
電力啟動設備
NVM
111
原始資料
感測器_資料
生物量測
感測器
控制器
110
中斷
資料
匯流排
邏輯
109
處理器狀態
生物量測
感測器
114
Vpwr_2
替代
電源
113
Vpwr_Alt
電力
控制
開關
108
該平台的其餘部分(ROP)
103
Vpwr_1
AC
適配器
106
Vpwr_WALL
DC-DC
轉換器
107
控制
電池
105
Vpwr_BAT
電池充電器控制器
101
Vpwr_SYS
電力
控制器
112
Vpwr_ROP
USB Type-C
電源
104
Vpwr_USB

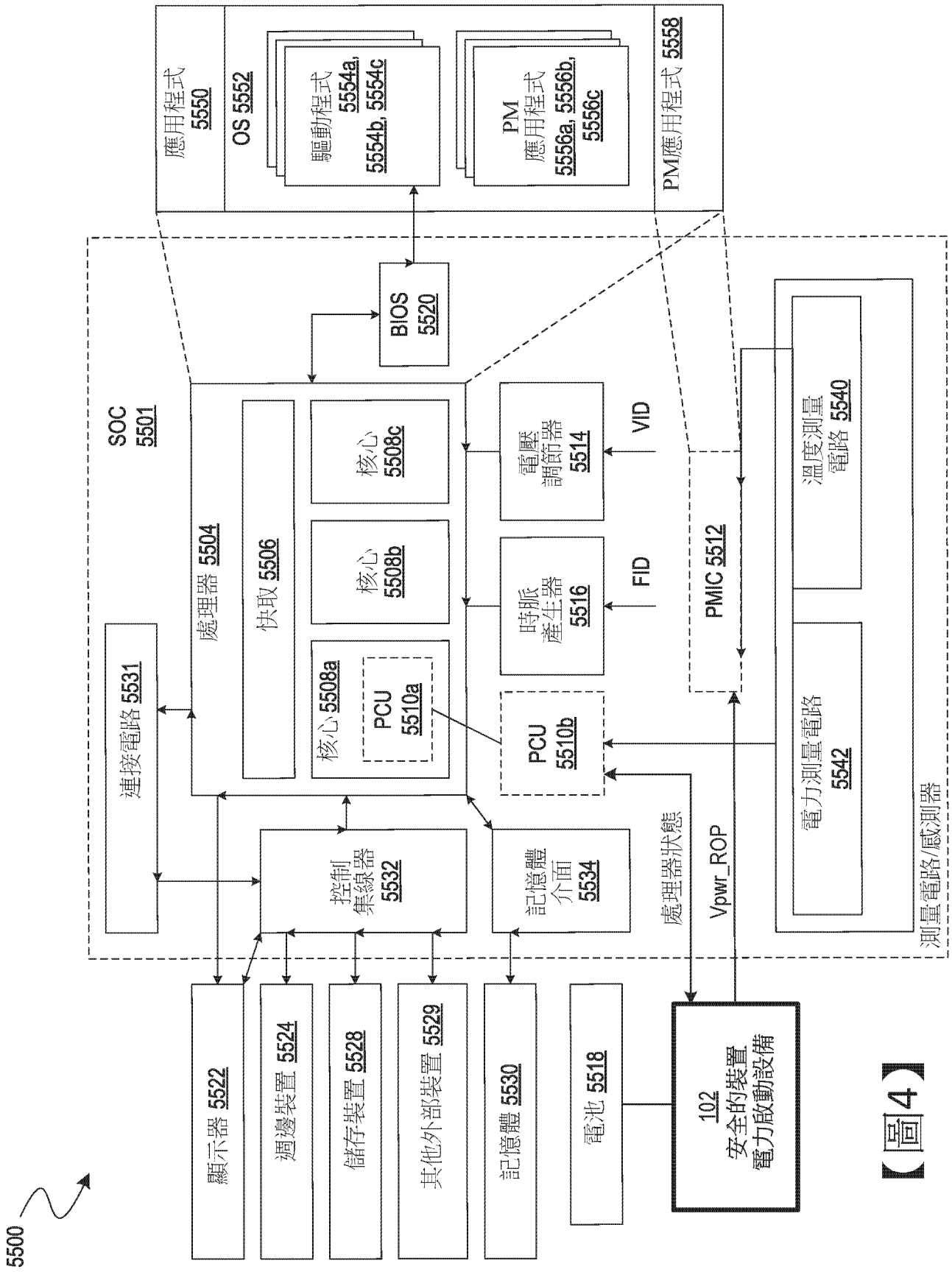
【圖1】

【圖2】


200
BIOS
MRC訓練資料
GOP
WiFi、藍牙韌體
uCode及p-單元補丁
安全的指紋資料區域
平台PHY韌體
CSE韌體
ISH韌體
嵌入式控制器韌體
PMC韌體
軟體帶
201
202
203
204
205
206
207
208
209
210
211
212


300
301
302
303
304
305
• 如果接收到任一使用者輸入，諸如按下電源按鈕(關閉電源)、OS關機(使用者所啟動的)、蓋上顯示器上蓋，系統進入睡眠狀態(例如，S3、S4)
系統處於ACPI狀態(S5、S4、S3)。沒有輸入諸如：按下電源按鈕、打開顯示器上蓋、手指在掃描感測器上掃過
接收到使用者輸入，例如透過：按下電源按鈕、打開顯示器上蓋、手指在指紋掃描器上掃過
假如沒有使用者輸入
假如沒有可用電源並且電池為低電力
假如不匹配
如果發現匹配，不闡控Vpwr_ROP
• 系統並不直接地打開或啟動
• 檢查電力輸入
• 如果任一電力輸入正提供電力，電池充電器控制器產生電力，其被電力閘控
• 電壓電源被產生給設備102
• 使用者掃過手指
• 生物量測感測器控制器110向邏輯109發送中斷
• 邏輯109把來自NVM 111的原始資料與來自由生物量測感測器控制器110的掃瞄進行比較

【圖3】


5500
應用程式 5550
OS 5552
驅動程式 5554a, 5554b, 5554c
PM 應用程式 5556a, 5556b, 5556c
PM/應用程式 5558
BIOS 5520
SOC 5501
處理器 5504
快取 5506
核心 5508a
核心 5508b
核心 5508c
PCU 5510a
PCU 5510b
電壓調節器 5514
時脈產生器 5516
PMIC 5512
VID
FID
連接電路 5531
控制集線器 5532
記憶體介面 5534
處理器狀態
Vpwr_ROP
溫度測量電路 5540
電力測量電路 5542
測量電路/感測器
顯示器 5522
週邊裝置 5524
儲存裝置 5528
其他外部裝置 5529
記憶體 5530
電池 5518
102 安全的裝置電力啟動設備

【圖4】