I527474

(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 I527474 B**

(45)公告日： 中華民國 105 (2016) 年 03 月 21 日

(21)申請案號：100140585 (22)申請日： 中華民國 100 (2011) 年 11 月 07 日

(51)Int. Cl.： ***H04W12/10 (2009.01)***

(30)優先權：2010/11/05 美國 61/410,781

(71)申請人：內數位專利控股公司 (美國) INTERDIGITAL PATENT HOLDINGS, INC. (US) 美國

(72)發明人：夏 尤根德拉 SHAH, YOGENDRA C. (GB)；卡斯 勞倫斯 CASE, LAWRENCE (US)；和利 多洛莉絲 HOWRY, DOLORES F. (US)；車 尹赫 CHA, INHYOK (US)；萊赫 安德魯斯 LEICHER, ANDREAS (DE)；史密特 安德魯斯 SCHMIDT, ANDREAS (DE)

(74)代理人：蔡清福

(56)參考文獻：

US 2007/0113120A1 US 2008/0046786A1

US 2009/0013210A1 WO 2010/102259A3

審查人員：易志孝

申請專利範圍項數：22 項 圖式數：10 共 114 頁

(54)名稱

裝置驗證、困擾指示及修復

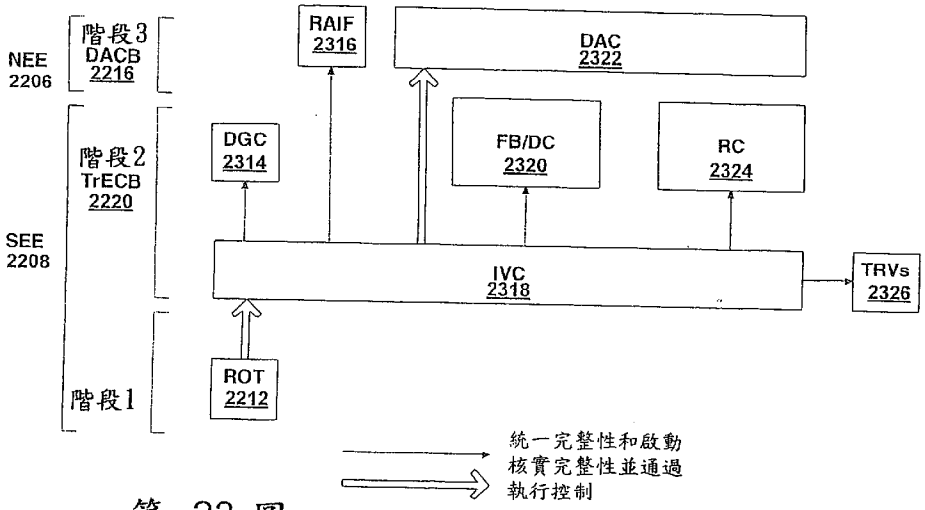
DEVICE VALIDATION, DISTRESS INDICATION, AND REMEDIATION

(57)摘要

一種無線通信裝置，其可以被配置用於執行完整性檢查並且向網路實體進行詢問來隔離無線通信裝置上的故障的元件的部分來進行修復。一旦確定了裝置的元件上的完整性故障，則裝置可以識別與該元件相關聯的功能，並且向網路實體指示該故障的功能。無線網路裝置和網路實體都可以使用元件至功能映射來識別故障的功能及/或故障的元件。在接收到裝置上的完整性故障的指示之後，網路實體可以確定在裝置上執行一個或多個附加的完整性檢查迭代，以窄化故障的元件上的完整性故障的範圍。一旦隔離了完整性故障，則網路實體可以修復無線通信裝置上的故障的元件的部分。

A wireless communications device may be configured to perform integrity checking and interrogation with a network entity to isolate a portion of a failed component on the wireless network device for remediation. Once an integrity failure is determined on a component of the device, the device may identify a functionality associated with the component and indicate the failed functionality to the network entity. Both the wireless network device and the network entity may identify the failed functionality and/or failed component using a component-to-functionality map. After receiving an indication of an integrity failure at the device, the network entity may determine that one or more additional iterations of integrity checking may be performed at the device to narrow the scope of the integrity failure on the failed component. Once the integrity failure is isolated, the network entity may remediate a portion of the failed component on the wireless communications device.

指定代表圖：



第 23 圖

符號簡單說明：

2206、NEE・・・正常執行環境

2208、SEE・・・安全的執行環境

2212、ROT・・・不可變硬體可信根

2216、DACB・・・裝置應用代碼庫

2220、TrECB・・・TrE 代碼庫

TrE・・・可信執行環境

2314、DGC・・・一般通信能力

RAIF、2316・・・修復應用 IF

IF・・・介面

2318、IVC・・・完整性驗證能力

2320、FB/DC・・・後降/困擾能力

2322、DAC・・・裝置應用能力

2324、RC・・・修復能力

2326、TRV・・・可信參考值

公告本

修正
年 月 日
103 年 11 月 3 日修正替換頁

發明摘要

※ 申請案號：100140585

※ 申請日：100.11.7

※IPC 分類：
H04W 12/10 (2009.01)

【發明名稱】(中文/英文)

裝置驗證、困擾指示及修復/DEVICE VALIDATION, DISTRESS INDICATION, AND REMEDIATION

【中文】

一種無線通信裝置，其可以被配置用於執行完整性檢查並且向網路實體進行詢問來隔離無線通信裝置上的故障的元件的部分來進行修復。一旦確定了裝置的元件上的完整性故障，則裝置可以識別與該元件相關聯的功能，並且向網路實體指示該故障的功能。無線網路裝置和網路實體都可以使用元件至功能映射來識別故障的功能及/或故障的元件。在接收到裝置上的完整性故障的指示之後，網路實體可以確定在裝置上執行一個或多個附加的完整性檢查迭代，以窄化故障的元件上的完整性故障的範圍。一旦隔離了完整性故障，則網路實體可以修復無線通信裝置上的故障的元件的部分。

【英文】

A wireless communications device may be configured to perform integrity checking and interrogation with a network entity to isolate a portion of a failed component on the wireless network device for remediation. Once an integrity failure is determined on a component of the device, the device may identify a functionality associated with the component and indicate the failed functionality

to the network entity. Both the wireless network device and the network entity may identify the failed functionality and/or failed component using a component-to-functionality map. After receiving an indication of an integrity failure at the device, the network entity may determine that one or more additional iterations of integrity checking may be performed at the device to narrow the scope of the integrity failure on the failed component. Once the integrity failure is isolated, the network entity may remediate a portion of the failed component on the wireless communications device.

【代表圖】

【本案指定代表圖】：第（ 23 ）圖。

【本代表圖之符號簡單說明】：

2206、NEE	正常執行環境
2208、SEE	安全的執行環境
2212、ROT	不可變硬體可信根
2216、DACB	裝置應用代碼庫
2220、TrECB	TrE 代碼庫
TrE	可信執行環境
2314、DGC	一般通信能力
RAIF、2316	修復應用 IF
IF	介面
2318、IVC	完整性驗證能力
2320、FB/DC	後降/困擾能力
2322、DAC	裝置應用能力
2324、RC	修復能力
2326、TRV	可信參考值

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

103 年 11 月 3 日修正替換頁

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】（中文/英文）

裝置驗證、困擾指示及修復/DEVICE VALIDATION, DISTRESS INDICATION, AND REMEDIATION

【技術領域】

【0001】 相關申請案的交叉引用

【0002】 本申請案要求於 2010 年 11 月 5 日提出的美國第 61/410,781 號臨時專利申請案的權益，其中該申請案的內容在這裏全部引入作爲參考。

【先前技術】

【0003】 無線通信系統可以使用多餘的資源來執行完整性檢查及/或修復該系統內部無線通信裝置上的完整性故障。目前的完整性檢查可以在大型單體碼塊上執行，以確定無線通信裝置的完整性是否已經受損。例如，經由完整性檢查，可以在無線通信裝置上偵測到未經授權的修改、篡改及/或受損軟體。一旦偵測到很大的碼塊的完整性故障，則網路可以採用大型單體碼塊的形式來將更新下載至無線通信裝置，以修復故障。這樣做有可能需要不必要的頻寬，並且在系統上增加了不需要的計算負擔。

【0004】 此外，多種類型及/或模型的無線通信裝置可以用於與網路通信或是在網路上通信，並且其中每一個裝置都具有不同的軟體和硬體形式。由於硬體和軟體發展實踐有可能會隨著公司而不同，因此，這些不同的裝置可能會導致難以使無線通信裝置上故障的元件的報告處理標準化。

【發明內容】

【0005】 本概述是以簡化形式引入在以下的詳細描述中被更進一步

描述的不同概念而被提供。

【0006】 在這裏描述的是用於對無線通信裝置的一個或多個元件執行完整性檢查的系統、方法和裝置實施例。這裏描述的第一完整性檢查可以在與無線通信裝置相關聯的元件上執行。該元件可被確定未通過第一完整性檢查。這時可以向網路實體發送關於與該故障的元件(即，未通過第一完整性檢查的元件)對應的功能的指示。可以從該網路實體接收在故障的元件上執行第二完整性檢查以確定故障的元件中導致該元件未通過第一完整性檢查的部分的請求。該第二完整性檢查可以在故障的元件上執行，以隔離該故障的元件的部分，以藉由網路實體來修復。

【0007】 根據一個例示實施例，載入器可以被配置用於在與無線通信裝置相關聯的元件上執行第一完整性檢查。該載入器還可以被配置用於確定元件未通過第一完整性檢查，並且在故障的元件上執行第二完整性檢查，以隔離故障的元件的部分，以藉由網路實體來修復。

【0008】 根據一個例示實施例，平臺完整性策略引擎（PIPE）可以被配置用於從載入器藉由關於故障的元件的指示、以及接收與故障的元件相對應的網路功能。該 PIPE 還可以被配置用於向網路實體報告關於與故障的元件相對應的功能的指示，並且從網路實體接收在故障的元件上執行第二完整性檢查以確定故障的元件中導致該元件未通過第一完整性檢查的部分的請求。

【0009】 根據一個例示實施例，裝置修復伺服器可以如這裏所述。該裝置修復伺服器可以駐留在無線通信網路上，並且被配置用於修復無線通信裝置上未通過完整性檢查的元件的部分。例如，裝置修復伺服器可以被配置用於從無線通信裝置接收關於與無線通信裝置上未通過完整性檢查的

元件相關聯的網路功能的指示。該故障的元件可以是基於接收到的關於網路功能的指示而被確定。裝置修復伺服器還可以被配置用於執行向無線通信裝置的詢問，以隔離故障的元件的部分來進行修復。該裝置修復伺服器還可以被配置爲基於一個或多個標準（criteria）來確定發送給無線通信裝置的關於故障的元件部分的修復或替換。一旦基於該標準確定了修復或替換，則裝置修復伺服器可以將用於故障的元件的部分的修復或替換發送到無線通信裝置。多種不同的標準可以用於確定故障的元件的修復或替換。例如，該標準可以基於故障的元件的大小或某個其他因素。在一個例示實施例中，修復伺服器可以基於 OS 軟體版本來替換特定元件。其他例示標準可以包括但不限於：版本號碼；每一個裝置/元件/代碼部分的最近更新或成功修復的日期/時間；代碼或元件的所有權；代碼許可的狀況（例如數字權利管理）；故障的元件、位元或位元組的數量；故障的代碼部分的大小；以及代碼部分或元件的所指定或計算的風險或損害影響值。

【0010】 本概述是爲了以簡化形式引入精選概念而被提供的，並且在以下的詳細描述中將會進一步描述這些概念。本概述既不是爲了確定所保護主題的關鍵特徵或必要特徵，也不是爲了限定所保護的主題的範圍。此外，所要保護的主題並不限於解決在本揭露的任何部分中指出的任何或所有缺陷的範圍。

【圖式簡單說明】

【0011】 更詳細的理解可以從以下結合附圖舉例給出的描述中得到，其中：

第 1A 圖示出的是可以實施所揭露的一個或多個實施例的例示通信系統；

第 1B 圖示出的是可以實施所揭露的一個或多個實施例的例示無線傳輸/接

收單元；

第 1C 圖示出的是可以實施所揭露的一個或多個實施例的例示系統無線電存取網路；

第 2 圖是示出了無線通信裝置上的引導序列的例示實施例的圖示；

第 3 圖是示出了物件檔與可執行映射之間的聯繫的圖示；

第 4 圖是示出了物件檔與可執行映射之間的聯繫的另一個圖示；

第 5 圖示出的是檔案的元件 TRV 區段的示例。

第 6 圖是示出了元件-網路功能映射的圖示；

第 7 圖示出的是檔案的元件-功能映射區段的示例；

第 8 圖是示出了在引導序列中使用的平臺能力及策略初啓（bring-up）的圖示；

第 9 圖是示出了這裏描述的在完整性檢查及/或報告期間使用表格或映射的圖示；

第 10 圖是示出了這裏描述的報告和修復處理的例示綜述的圖示；

第 11 圖示出的是在裝置上收集資訊來確定可以執行的操作的例示呼叫流程圖；

第 12 圖示出的是用於在裝置與網路實體之間執行詢問的例示呼叫流程圖；

第 13 圖示出的是在無線通信裝置的元件上執行的詢問的示例；

第 14 圖示出的是在無線通信裝置元件上執行的詢問的另一個示例；

第 15 圖示出的是與困擾警報以及單體代碼替換有關的例示呼叫流程圖；

第 16 圖示出的是與遠端軟體困擾/修復有關的例示呼叫流程圖；

第 17 圖示出的是與實施 SeGW 驗證嘗試的遠端軟體困擾/修復相關聯的例示呼叫流程圖；

第 18A 圖示出的是與遠端軟體困擾/修復有關的例示呼叫流程圖，其中網路可以禁止經由 SeGW 的驗證；

第 18B 圖示出的是與即時限制存取和精確存取控制的遠端軟體困擾/修復相關聯的例示呼叫流程圖；

第 19 圖示出的是將無線通信裝置軟體元件修復與 SeGW 存取相關聯的例示呼叫流程圖；

第 20 圖示出的是與中繼節點的能力自舉（bootstrap）有關的例示呼叫流程圖；

第 21 圖示出的是與具有經過驗證的管理能力的中繼節點修復有關的例示呼叫流程圖；

第 22 圖示出的是具有功能元件和代碼/資料儲存元件的例示系統；

第 23 圖示出的是引導序列的階段以及在每一個階段實施的不同實體間的交互作用的例示實施方式；

第 24A 圖示出的是被線性組合以創建 TRV 的量度序列的圖示；以及

第 24B 圖示出的是使用 Merkle 散列樹來創建 TRV 的值的組合的圖示。

【實施方式】

【0012】 第 1A-24B 圖涉及的是可以實施所揭露的系統、方法和手段的例示實施例。這裏描述的實施例是例示性而不是限制性的。雖然在這裏示出並描述了協定流程，但是這些流程的順序是可以改變的，及/或附加流程是可以添加的。

【0013】 第 1A、1B 和 1C 圖示出的是可以在這裏描述的實施例中使用的例示通信系統和裝置。第 1A 圖是可以實施一個或多個所揭露的實施例的例示通信系統 100 的圖示。通信系統 100 可以是爲多個無線用戶提供語

音、資料、視訊、訊息傳遞、廣播等內容的多重存取系統。該通信系統 100 經由共享包括無線頻寬在內的系統資源以使多個無線用戶能存取此類內容，舉例來說，通信系統 100 可以使用一種或多種頻道存取方法，如分碼多重存取（CDMA）、分時多重存取（TDMA）、分頻多重存取（FDMA）、正交 FDMA（OFDMA）、單載波 FDMA（SC-FDMA）等等。

【0014】 如第 1A 圖所示，通信系統 100 可以包括無線傳輸/接收單元（WTRU）102a、102b、102c、102d，無線電存取網路（RAN）104，核心網路 106，公共交換電話網路（PSTN）108，網際網路 110 以及其他網路 112，但是應該瞭解，所揭露的實施例設想了任一數量的 WTRU、基地台、網路及/或網路元件。WTRU102a、102b、102c、102d 中的每一者可以是被配置用於在無線環境中操作及/或通信的任何類型的裝置。例如，WTRU102a、102b、102c、102d 可以被配置用於傳輸及/或接收無線信號、並且可以包括用戶設備（UE）、行動站、固定或行動用戶單元、呼叫器、蜂巢式電話、個人數位助理（PDA）、智慧型電話、膝上型電腦、迷你筆記型電腦、個人電腦、無線感測器、消費類電子裝置等等。

【0015】 通信系統 100 還可以包括基地台 114a 和基地台 114b。基地台 114a、114b 中的每一者可以是被配置用於經由與 WTRU102a、102b、102c、102d 中的至少一者無線介面連接來促進對一個或多個通信網路(例如核心網路 106、網際網路 110 及/或網路 112)的存取。例如，基地台 114a、114b 可以是基地收發台（BTS）、節點 B、e 節點 B、家用節點 B、家用 e 節點 B、站點控制器、存取點（AP）、無線路由器等等。雖然每一個基地台 114a、114b 都被描述爲是單一元件，但是應該瞭解，基地台 114a、114b 可以包括任何數量的互連基地台及/或網路元件。

【0016】 基地台 114a 可以是 RAN104 的一部分，並且該 RAN 還可以包括其他基地台及/或網路元件（未顯示），例如基地台控制器（BSC）、無線電網路控制器（RNC）、中繼節點等等。基地台 114a 及/或基地台 114b 可以被配置用於在被稱之爲爲胞元（未顯示）的特定地理區域內部傳輸及/或接收無線信號。胞元可以進一步分成胞元扇區。例如，與基地台 114a 相關聯的胞元可以分成三個扇區。因此，在一個實施例中，基地台 114a 可以包括三個收發器，也就是說，每一個收發器對應於胞元的一個扇區。在另一個實施例中，基地台 114a 可以使用多輸入多輸出（MIMO）技術，由此可以爲胞元中的每個扇區使用多個收發器。

【0017】 基地台 114a、114b 可以經由空氣介面 116 來與 WTRU102a、102b、102c、102d 中的一個或多個進行通信，其中該空氣介面可以是任何適當的無線通信鏈路（例如射頻（RF）、微波、紅外線（IR）、紫外線（UV）、可見光等等）。空氣介面 216 可以採用任何適當的無線電存取技術（RAT）來建立。

【0018】 更具體地說，如上所述，通信系統 100 可以是多重存取系統、並且可以使用一種或多種頻道存取方案，如 CDMA、TDMA、FDMA、OFDMA、SC-FDMA 等等。舉例來說，RAN104 中的基地台 114a 和 WTRU102a、102b、102c 可以實施諸如通用行動電信系統（UMTS）陸地無線電存取（UTRA）之類的無線電技術，其中該技術可以使用寬頻 CDMA（WCDMA）來建立空氣介面 116。WCDMA 可以包括下列通信協定，如高速封包存取（HSPA）及/或演進型 HSPA（HSPA+）。HSPA 可以包括高速下行鏈路封包存取（HSDPA）及/或高速上行鏈路封包存取（HSUPA）。

【0019】 在另一個實施例中，基地台 114a 和 WTRU102a、102b、102c

可以實施諸如演進型 UMTS 陸地無線電存取（E-UTRA）之類的無線電技術，該技術可以使用長期演進（LTE）及/或高級 LTE（LTE-A）來建立空氣介面 116。

【0020】 在其他實施例中，基地台 114a 與 WTRU102a、102b、102c 可以實施 IEEE802.16（全球微波互通存取（WiMAX））、CDMA2000、CDMA2000 1X、CDMA2000 EV-DO、臨時標準 2000（IS-2000）、臨時標準 95（IS-95）、臨時標準 856（IS-856）、全球行動通信系統（GSM）、用於 GSM 演進的增強資料速率（EDGE）、GSM EDGE（GERAN）等無線電存取技術。

【0021】 第 1A 圖中的基地台 114b 可以是例如無線路由器、家用節點 B、家用 e 節點 B 或存取點，並且可以使用任何適當的 RAT 來促進例如營業場所、住宅、交通工具、校園等等局部區域中的無線連接。在一個實施例中，基地台 114b 和 WTRU102c、102d 可以實施諸如 IEEE802.11 之類的無線電技術來建立無線區域網路（WLAN）。在另一個實施例中，基地台 114b 和 WTRU102c、102d 可以實施諸如 IEEE802.15 之類的無線電技術來建立無線個人區域網路（WPAN）。在再一個實施例中，基地台 114b 和 WTRU102c、102d 可以通過使用基於蜂巢的 RAT（例如 WCDMA、CDMA2000、GSM、LTE、LTE-A 等等）來建立微微胞元或毫微微胞元。如第 1A 圖所示，基地台 114b 可以直接連接到網際網路 110。由此，基地台 114b 未必需要經由核心網路 106 來存取網際網路 110。

【0022】 RAN104 可以與核心網路 106 通信，該核心網路 106 可以是被配置用於向 WTRU102a、102b、102c、102d 中的一個或多個提供語音、資料、應用及/或網際網路協定語音（VoIP）服務的任何類型的網路。例如，核心網路 106 可以提供呼叫控制、記賬服務、基於移動位置的服務、預付

費呼叫、網際網路連接、視訊分發等等，及/或執行高階安全功能，例如用戶驗證。雖然在第 1A 圖中沒有顯示，但是應該瞭解，RAN104 及/或核心網路 106 可以直接或間接地和其他那些與 RAN104 使用相同 RAT 或不同 RAT 的 RAN 進行通信。例如，除了與可以使用 E-UTRA 無線電技術的 RAN104 相連之外，核心網路 106 還可以與使用 GSM 無線電技術的另一個 RAN（未顯示）通信。

【0023】 核心網路 106 還可以充當 WTRU102a、102b、102c、102d 存取 PSTN108、網際網路 110 及/或其他網路 112 的閘道。PSTN108 可以包括提供簡易老式電話服務（POTS）的電路交換電話網路。網際網路 110 可以包括使用公共通信協定的全球性互連電腦網路及裝置的系統，該協定可以是 TCP/IP 互連網協定族中的傳輸控制協定（TCP）、用戶資料報協定（UDP）和網際網路協定（IP）。網路 112 可以包括由其他服務提供者擁有及/或操作的有線或無線通信網路。例如，網路 112 可以包括與一個或多個 RAN 相連的另一個核心網路，其中所述一個或多個 RAN 可以與 RAN104 使用相同 RAT 或不同的 RAT。

【0024】 通信系統 100 中一些或所有 WTRU102a、102b、102c、102d 可以包括多模能力，換言之，WTRU102a、102b、102c、102d 可以包括在不同無線鏈路上與不同無線網路進行通信的多個收發器。例如，第 1A 圖所示的 WTRU102c 可以被配置用於與使用基於蜂巢的無線電技術的基地台 114a 通信，以及與可以使用 IEEE802 無線電技術的基地台 114b 通信。

【0025】 第 1B 圖是例示 WTRU102 的系統圖。如第 1B 圖所示，WTRU102 可以包括處理器 118、收發器 120、傳輸/接收元件 122、揚聲器/麥克風 124、鍵盤 126、顯示器/觸控板 128、不可拆卸記憶體 130、可拆卸

記憶體 132、電源 134、全球定位系統（GPS）碼片組 136 以及其他週邊裝置 138。應該瞭解的是，在保持符合實施例的同時，WTRU102 可以包括前述元件的任何子組合。

【0026】 處理器 118 可以是通用處理器、專用處理器、常規處理器、數位信號處理器（DSP）、多個微處理器、與 DSP 核心關聯的一或多個微處理器、控制器、微控制器、專用積體電路（ASIC）、現場可編程閘陣列（FPGA）電路、其他任何類型的積體電路（IC）、狀態機等等。處理器 118 可以執行信號編碼、資料處理、功率控制、輸入/輸出處理及/或其他任何能使 WTRU102 在無線環境中操作的功能。處理器 118 可以耦合至收發器 120，收發器 120 可以耦合至傳輸/接收元件 122。雖然第 1B 圖將處理器 118 和收發器 120 描述爲是獨立元件，但是應該瞭解，處理器 118 和收發器 120 可以一起集成在一個電子封裝或晶片中。

【0027】 傳輸/接收元件 122 可以被配置用於經由空氣介面 116 將信號傳輸至基地台（例如基地台 114a）或從基地台（例如基地台 114a）接收信號。例如，在一個實施例中，傳輸/接收元件 122 可以是被配置用於傳輸及/或接收 RF 信號的天線。在另一個實施例中，舉例來說，傳輸/接收元件 122 可以是被配置用於傳輸及/或接收 IR、UV 或可見光信號的發光體/偵測器。在再一個實施例中，傳輸/接收元件 122 可以被配置用於傳輸和接收 RF 和光信號。應該瞭解的是，傳輸/接收元件 122 可以被配置用於傳輸及/或接收無線信號的任何組合。

【0028】 此外，雖然在第 1B 圖中將傳輸/接收元件 122 描述爲是單一元件，但是 WTRU102 可以包括任何數量的傳輸/接收元件 122。更具體地說，WTRU102 可以使用 MIMO 技術。因此，在一個實施例中，WTRU102

可以包括兩個或更多個經由空氣介面 116 來傳輸和接收無線電信號的傳輸/接收元件 122（例如多個天線）。

【0029】 收發器 120 可以被配置用於對傳輸/接收元件 122 將要傳輸的信號進行調變，以及對傳輸/接收元件 122 接收的信號進行解調。如上所述，WTRU102 可以具有多模能力。因此，收發器 120 可以包括用於使 WTRU102 能經由 UTRA 和 IEEE802.11 之類的多種 RAT 來進行通信的多個收發器。

【0030】 WTRU102 的處理器 118 可以耦合至揚聲器/麥克風 124、鍵盤 126 及/或顯示器/觸控板 128（例如液晶顯示器（LCD）顯示單元或有機發光二極體（OLED）顯示單元），並且可以接收來自這些元件的用戶輸入資料。處理器 118 還可以向揚聲器/麥克風 124、鍵盤 126 及/或顯示器/觸控板 128 輸出用戶資料。此外，處理器 118 可以從任何適當的記憶體（例如不可拆卸記憶體 130 及/或可拆卸記憶體 132）中存取資訊，以及將資料存入這些記憶體。該不可拆卸記憶體 130 可以包括隨機存取記憶體（RAM）、唯讀記憶體（ROM）、硬碟或是其他任何類型的記憶儲存裝置。可拆卸記憶體 132 可以包括用戶身份模組（SIM）卡、記憶條、安全數位（SD）記憶卡等等。在其他實施例中，處理器 118 可以從那些並非實際位於 WTRU102 的記憶體存取資訊，以及將資料存入這些記憶體，其中舉例來說，該記憶體可以位於伺服器或家用電腦（未顯示）。

【0031】 處理器 118 可以接收來自電源 134 的電力，並且可以被配置用於分發及/或控制用於 WTRU102 中的其他元件的電力。電源 134 可以是爲 WTRU102 供電的任何適當的裝置。舉例來說，電源 134 可以包括一個或多個乾電池組（如鎳鎘（NiCd）、鎳鋅（NiZn）、鎳氫（NiMH）、鋰離子

（Li-ion）等等）、太陽能電池、燃料電池等等。

【0032】 處理器 118 還可以與 GPS 碼片組 136 耦合，該碼片組可以被配置用於提供與 WTRU102 的目前位置相關的位置資訊（例如經度和緯度）。作爲來自 GPS 碼片組 136 的資訊的補充或替代，WTRU102 可以經由空氣介面 116 接收來自基地台（例如基地台 114a、114b）的位置資訊、及/或根據從兩個或更多個附近基地台接收的信號的時序來確定其位置。應該瞭解的是，在保持符合實施例的同時，WTRU102 可以用任何適當的定位方法來獲取位置資訊。

【0033】 處理器 118 還可以耦合到其他週邊裝置 138，其他週邊裝置 138 可以包括提供附加特徵、功能及/或有線或無線連接的一個或多個軟體及/或硬體模組。例如，週邊裝置 138 可以包括加速度計、電子指南針、衛星收發器、數位相機（用於照片或視訊）、通用串列匯流排（USB）埠、振動裝置、電視收發器、免持耳機、藍芽®模組、調頻（FM）無線電單元、數位音樂播放器、媒體播放器、視訊遊戲播放器模組、網際網路瀏覽器等等。

【0034】 第 1C 圖是根據一個實施例的 RAN104 和核心網路 106 的系統圖示。如上所述，RAN104 可以使用 E-UTRA 無線電技術以經由空氣介面 116 來與 WTRU102a、102b、102c 進行通信。並且該 RAN104 還可以與核心網路 106 通信。

【0035】 RAN104 可以包括 e 節點 B140a、140b、140c，但是應該理解，在保持與實施例相符的同時，RAN104 可以包括任一數量的 e 節點 B。節點 B140a、140b、140c 中的每一者都可以包括一個或多個收發器，以經由空氣介面 116 來與 WTRU102a、102b、102c 進行通信。在一個實施例中，

e 節點 B140a、140b、140c 可以實施 MIMO 技術。因此，舉例來說，e 節點 B140a 可以使用多個天線來向 WTRU102a 傳輸無線信號以及接收來自 WTRU102a 的無線信號。

【0036】 e 節點 B140a、140b、140c 中的每一者都可以與特定的胞元（未顯示）相關聯，並且可以被配置用於處理無線電資源管理決策、切換決策、上行鏈路及/或下行鏈路中的用戶排程等等。如第 1C 圖所示，e 節點 B140a、140b、140c 彼此可以經由 X2 介面來進行通信。

【0037】 第 1C 圖所示的核心網路 106 可以包括移動性管理閘道（MME）142、服務閘道 144 以及封包資料網路（PDN）閘道 146。雖然在前的每一個元件都被描述爲是核心網路 106 的一部分，但是應該瞭解，這其中的任一元件都可以被核心網路操作者以外的實體擁有及/或操作。

【0038】 MME 142 可以經由 S1 介面來與 RAN104 中的每一個 e 節點 B140a、140b、140c 相連，並且可以充當控制節點。例如，MME 142 可以負責驗證 WTRU102a、102b、102c 的用戶、啓動/止動承載，在 WTRU102a、102b、102c 的初始連結過程中選擇特定服務閘道等等。MME 142 還可以提供控制平面功能，以在 RAN104 與使用了諸如 GSM 或 WCDMA 之類的其他無線電技術的其他 RAN（未顯示）之間進行切換。

【0039】 服務閘道 144 可以經由 S1 介面而與 RAN104 中的每一個 e 節點 B140a、140b、140c 相連。該服務閘道 144 通常可以路由用戶資料封包至 WTRU102a、102b、102c 和轉發來自 WTRU102a、102b、102c 的用戶資料封包。該服務閘道 144 還可以執行其他功能，例如在 e 節點 B 間的切換過程中錨定用戶面、在下行鏈路數據可供 WTRU102a、102b、102c 使用時觸發傳呼、管理和儲存 WTRU102a、102b、102c 的上下文等等。

【0040】 服務閘道 144 還可以連接到 PDN 閘道 146，該 PDN 閘道可以爲 WTRU102a、102b、102c 提供針對網際網路 110 之類的封包交換網路的存取，以促進 WTRU102a、102b、102c 與 IP 賦能的裝置之間的通信。

【0041】 核心網路 106 可以促進與其他網路的通信。例如，核心網路 106 可以爲 WTRU102a、102b、102c 提供針對 PSTN108 之類的電路交換網路的存取，以促進 WTRU102a、102b、102c 與傳統的陸線通信裝置之間的通信。例如，核心網路 106 可以包括 IP 閘道（例如 IP 多媒體子系統（IMS）伺服器）或與之通信，其中該 IP 閘道充當的是核心網路 106 與 PSTN108 之間的介面。此外，核心網路 106 可以爲 WTRU102a、102b、102c 提供針對網路 112 的存取，該網路可以包括其他服務提供者擁有及/或操作的其他有線或無線網路。

【0042】 這裏描述的通信系統和裝置可以用於管理通信裝置的軟體、管理通信裝置的配置、及/或提供軟體及/或配置資訊修復，以將裝置恢復到原始狀態。此外，在這裏還描述了使用軟體發展和代碼釋放工具的實施方式，其中該軟體發展和代碼釋放工具可以使用軟體工具、網路協定、裝置策略以及軟體管理及/或遠端除錯技術來自動產生和管理可信代碼庫（code base）的軟體方面的參考，從而在裝置中嵌入用於可證實報告和修復的機制和參考。更進一步，在這裏描述的是可以確保裝置實施的完整性檢查的故障指示的技術，其中包括對表明可以信任報告故障的裝置的指示所進行的描述。

【0043】 這裏描述的無線通信裝置可以被配置用於在具有多個階段的安全引導處理的每個階段執行完整性檢查。在多個階段的安全引導處理期間，每一個階段可以核實後續階段，由此創建信任鏈。在具有多個階段

的安全引導處理的每個階段中可以確定是否可以信任與該階段相關聯的元件。與元件相關聯的完整性量度可被確定。該元件可以具有相關聯的可信參考值。元件的可信賴度可以藉由將完整性量度與可信參考值進行比較來確定（例如測試）。如果完整性量度與可信參考值相匹配，則可以認爲該元件是可信賴的。如果完整性量度未能與可信參考值相匹配，則認爲該元件未必是可信賴的。雖然在這裏描述的是通過將完整性量度與可信參考值進行比較來執行完整性檢查，但是應該瞭解，完整性檢查是可以採用其他那些用於確定元件可信賴度的方式執行的。

【0044】 由於外部實體未必會辨認出元件，因此，舉例來說，在多個網路及/或裝置上可以定義及/或標準化功能，從而與標準規範及/或取決於實施的方式的一致。元件可以與功能相關聯。元件與功能之間的關係可以在元件-功能映射中給出。功能故障可以藉由將故障的元件與元件-功能映射進行比較來識別。

【0045】 裝置可以向外部實體發送與功能故障相關聯的警報。外部實體可以確定替換代碼，該替換代碼與可以用於修復或替換故障的元件的功能關聯。換言之，替換代碼可以是一個替換元件。裝置可以接收該替換元件、並且以該替換元件來替換故障的元件。

【0046】 安全引導處理可以提供驗證程序的基礎。由不可變硬體可信根（RoT）發起的信任鏈可以核實所載入的初始代碼的有效性。如第 2 圖所示，舉例來說，該引導處理可以在每一個階段經由信任鏈核實後續階段的時候繼續進行。

【0047】 在通電以及硬體初始化程序之後，裝置可以啓動例如第 2 圖所示的安全引導處理。初始的 RoT 可以由駐留於 ROM 中的安全記憶體

的引導載入器 202 表示。在一開始，ROM 引導載入器 202 可以執行一些初始化功能。該 ROM 引導載入器 202 可存取安全憑證（例如融合鍵控資訊），並且可以使用該資訊來核實第二階段的引導載入器 204（例如駐留在外部記憶體中）的完整性。第二階段的載入器 204 可以由硬體或軟體密碼加密裝置進行檢查，以確保其完整性。第二階段的載入器 204 的計算得到的散列（hash）量度可以與用安全憑證簽名並儲存在外部記憶體中的可信參考值（TRV）量度進行比較。如果計算得到的量度與經簽名的 TRV 相匹配，則第二階段的載入器 204 可被核實並載入到內部記憶體（例如 RAM）中。該引導 ROM 可以跳轉到第二階段的載入器 204 的開端，並且信任鏈可以繼續。所述核實處理中的初始階段的故障可以表明後續核實有可能受損（例如，初始階段的故障可以表明信任鏈發生了重大故障）。如果存在在核實處理的初始階段指示出的故障，則可以將裝置關閉。

【0048】 第二階段的引導載入器 204 可以包括可信執行環境（TrE）代碼以及可以檢查附加代碼並且將其載入到內部記憶體的代碼。TrE 可以建立能夠計算和儲存附加的完整性參考值的可信環境和安全儲存區域。該 TrE 完整性可以檢查、載入及/或啓動作業系統以及通信代碼。隨著每個階段被檢查和載入（例如，第 2 圖所示的方塊 202、204、206 和 208 中的每一者都可以表示一個階段），該信任鏈可以延續。例如，第二階段的載入器 204 可以核實 OS/通信（Comm）206 及/或裝置軟體 208 的完整性。作爲替代或補充，OS/通信 206 可以核實裝置軟體 208 的完整性。該 OS/通信 206 可以包括 OS 載入器。根據一個實施例，第 2 圖所示的實體可以按照執行順序而被核實及/或相互核實，以保持信任鏈。

【0049】 信任鏈可以由能夠安全核實後續處理的執行過程來保持。該

核實過程可以使用密碼加密計算及/或可信參考值。駐留在非安全記憶體中的代碼可能易受攻擊，並且可以在載入之前對其進行檢查。在沒有細粒度驗證的情況下，第二階段的引導載入器 204 可以驗證剩餘代碼，以此作爲成批（bulk）量度。如果測量得到的值不與單體塊的 TRV 匹配，那麼可以確定該代碼未必可信以及不可以載入該代碼。裝置未必能夠通信，並且結果有可能包括經由高成本的上門服務或是運回裝置進行修復來修復整個代碼庫。

【0050】 這裏描述的方法、系統和手段可以使得裝置能夠驗證已儲存代碼的較小元件，以及提供關於哪些元件已經故障以及哪些元件可以或者不可以被遠端修復的詳細描述。這種細粒度資訊可被提供給修復管理器。

【0051】 在這裏可以建立策略來確定哪些故障的元件是可以遠端修復的。舉個例子，如果裝置檢查並載入了 TrE 以及最小的通信代碼集合，那麼該裝置可以保持充當用於修復管理器的代理的功能，以識別以及向修復管理器報告故障的特定元件的資訊。如果修復能力存在且是裝置的代理功能的一部分，則可以發起後續的遠端修復程序，這樣做可以減少使用高成本的現場人員更新。

【0052】 根據一個實施例，可執行映射可被分區和驗證，以便能夠進行細粒度的報告。可執行映射的產生可以在幾個階段中進行。元件可以是指包含了副程式及/或參數/資料的檔案。開發人員可以編寫在元件來源和標頭檔案中捕獲的程式。從這些元件原始檔案中，編譯器和組譯器可以產生同時包含了機器二進位碼和程式資料的物件檔（例如*.o）。鏈結器可以將這些物件檔作爲輸入，並且產生能夠用於與其他物件檔附加鏈結的可執行映射或物件檔。鏈結器命令檔可以指示鏈結器如何組合物件檔，以及將二進

位碼和資料放置在目標嵌入式系統中的什麼位置。

【0053】 鏈結器的功能可以是將多個物件檔合併成較大的可重新定位的物件檔、共享的物件檔或是最終的可執行映射。總體變數和非靜態函數可被稱爲全局符號。在最終的可執行二進位映射中，符號可以是指記憶體中的位址位置。此記憶體位置的內容可以是用於變數的資料或是用於函數的可執行代碼。

【0054】 編譯器可以創建具有符號名稱-位址映射的符號表，以作爲其產生的物件檔的一部分。在創建可重新定位的輸出的時候，編譯器可以產生位址，其中對於每一個符號來說，該位址與所編譯的檔案是相關的。鏈結器執行的鏈結處理可以包括符號解析及/或符號重新定位。符號解析可以是鏈結器檢查每一個物件檔並且爲物件檔確定在哪個（哪些）（其他）物件檔中定義外部符號。符號重新定位可以是鏈結器將符號參考映射到其定義的處理。該鏈結器可以修改所鏈結的物件檔的機器碼，由此，對符號的代碼參考反映了指定給這些符號的實際位址。

【0055】 物件和可執行檔可以採用若干種格式，例如 ELF（可執行和鏈結格式）以及 COFF（公共物件-檔案格式）。物件檔可被劃分成區域或區段。這些區段可以保持下列各項中的一項或多項：例如可執行代碼、資料、動態鏈結資訊、除錯資料、符號表、重新定位資訊、註釋、字串表或註解。這些區段可以用於向二進位檔案提供指令，以及允許檢查。函數區段可以包括下列各項中的一項或多項：可以儲存系統函數位址的全局偏移表（GOT）、可以儲存間接鏈結至 GOT 的程序鏈結表（PLT）、可以用於內部初始化的.init/fini、以及可以用於建構器和破壞器的.shutdown或.ctors/.dtors。資料區段可以包括下列各項中的一項或多項：用於唯讀資料

的.rodata、用於已初始化資料的.data、或是用於未初始化資料的.bss。ELF區段可以包括下列各項中的一項或多項：用於啓動的.init、用於字串的.text、用於停機的.fini、用於唯讀資料的.rodata、用於已初始化資料的.data、用於已初始化的線程資料的.tdata、用於未初始化線程資料的.tbss、用於建構器的.ctors、用於破壞器的.dtors、用於全局偏移表的.got、或用於未初始化資料的.bss。

【0056】 一些區段可被載入到進程映射中。一些區段可以提供在建構進程映射中使用的資訊。一些區段可被限制爲在鏈結物件檔中使用。一些物件檔可以包括對位於其他物件檔中的符號的參考。該鏈結器可以創建符號表，該符號表可以包括符號名稱的列表及其在用於每一個物件檔的本文和資料分段中的相應偏移。在將物件檔鏈結在一起之後，鏈結器可以使用重新定位記錄來找出可能未被填充的未解析符號位址。在編譯了多個原始檔案（例如 C/C++和組譯檔）並將其組譯成 ELF 物件檔之後，鏈結器可以組合這些物件檔，並且將來自不同物件檔的區段併入如第 3 圖所示的程式分段。

【0057】 如第 3 圖所示，物件檔 302、304 和 306 的本文區段 308、316 和 324 分別可以併入可執行映射 338 的本文分段 332。作爲補充或替代，啓動區段 310、318 和 326 可以併入可執行映射 338 的本文分段 332。同樣，物件檔 302、304 和 306 的資料區段 312、320 和 328 分別可以併入可執行映射 338 的資料分段 334。最後，物件檔 302、304 和 306 的未初始化資料區段 314、322 和 330 分別可以併入可執行映射 338 的未初始化資料分段 336。雖然第 3 圖示出了可以併入可執行映射 338 的區段的物件檔 302、304 和 306 的多個區段，但是應該理解，任一數量及/或組合的區段都可以併入

可執行映射的區段。

【0058】 如第 3 圖所示，區段可以提供一種將相關區段分組的方式。每一個分段都可以包括相同或不同類型（例如本文、資料或動態區段）的一個或多個區段。作業系統在邏輯上可以依照在程式標頭表中提供的資訊來拷貝檔案分段。該可執行和唯讀資料區段可以組合爲單一本文區段。資料和未初始化的資料區段可以組合成資料分段或組合成其自己的單獨的分段。由於這些分段可以在創建過程的時候載入到記憶體中，因此，這些分段可被稱爲載入分段。諸如符號資訊和除錯區段之類的其他區段可以併入到其他的非載入分段。本文區段可以包括來源代碼以及已初始化的靜態變數。編譯器所定義的多個區段可被載入到鏈結器所定義的單一組合分段中。

【0059】 最終的可執行映射可以是使用控制鏈結器如何組合區段及/或將區段分配到目標系統記憶體映射的鏈結器命令（其可以是被叫鏈結器指令）產生的。鏈結器指令可以保持在鏈結器命令檔中。嵌入式開發人員可以使用該鏈結器命令檔來將可執行映射到目標系統。

【0060】 對故障的元件執行驗證和細粒度報告的能力可以使用可執行映射中可用的附加資訊，此外，開發和代碼釋放工具鏈是可以修改的。在可執行映射內部，每一個元件的參考量度以及識別該量度所關聯的元件的資訊元素都是可以識別的。

【0061】 對故障的元件所進行的修復可以取決於裝置報告標準的功能故障的能力。功能以及基於故障所採取的動作可以由網路操作者定義。軟體發展者可以確定如何能將操作者定義的功能映射到其系統中的軟體元件。在可執行映射中，功能映射是可見的，並且可以使用工具鏈增強。

【0062】 對開發階段期間使用的軟體工具鏈進行修改可以適應下列

各項中的一項或多項：元件區段產生、安全的 TRV 產生和嵌入、元件-功能定義的插入、或策略及策略配置檔的插入。

【0063】 對載入器的功能進行修改可以適應驗證及/或修復。載入器可被修改爲執行下列各項中的一項或多項：在載入元件時對元件執行完整性檢查、隔離或卸載故障的元件、管理策略、或在記憶體中儲存故障的元件 ID 以供策略管理器報告故障。

【0064】 在這裏描述了可被應用於這裏描述的軟體發展和代碼釋放工具鏈來闡明預期功能的例示實施例。然而，這裏的實施例並不限於這裏提供的示例。

【0065】 鏈結器的作用可以是取得輸入物件、以及將不同的區段組合成分段。由於可以在鏈結過程期間組合物件代碼，因此，在符號表資訊中可以保持用於識別物件檔中的函數或變數的能力。最終的合併代碼區段可不提供可以用於觸發這裏描述的驗證過程的驗證方案。

【0066】 爲了便於識別單一元件，載入器可以具有一種識別代碼起源的方式，其中可以包括定義元件或是產生可被載入器識別的單一元件的 TRV。例如，增強用於產生可執行映射的工具鏈，能夠識別出與載入器驗證功能的特定物件檔元件相關聯的代碼，從而識別特定的元件以及執行完整性檢查。代碼映射的重新排列可以改變輸入物件的 TRV（例如，如果修改一個輸入物件，那麼有可能導致改變其他輸入物件的 TRV）。此外還可以阻止工具鏈使用最佳化方法，以阻止 TRV 的變化。

【0067】 對於需要完整性檢查的元件來說，在這裏可以爲其產生特定區段名稱。例如，區段名稱可以出現在最終的 ELF 可執行檔包含的區段標頭表中。藉由將用戶定義的區段進行分組，載入器可以識別元件以及執行

完整性檢查。該載入器可以向策略管理器報告元件的通過與否的狀態。隔離那些通過/未通過完整性檢查的特定功能可以允許策略管理器以精細的粒度或詳細的等級來報告那些可能受到故障的元件影響的功能。

【0068】 第4圖示出了可以鏈結在一起形成單一可執行映射406的兩個物件檔402和404。物件檔402具有兩個不同的代碼分段，即元件檔區段408和本文區段410。物件檔404具有可以包括代碼及/或恆定資料的單一代碼分段，即元件檔區段416。對用戶定義的代碼區段(即元件檔區段408和元件檔區段416)來說，這些區段可以連同與其映射的分段類型相關的大小及/或儲存位置一起出現的區段標頭中。在第4圖中用箭頭描述了關於這種映射關係的示例。例如，物件檔402的元件檔區段408、本文區段410、資料區段412以及bss區段414分別可被映射到可執行映射406的元件檔區段420、本文區段424、資料區段426以及bss區段428。同樣，物件檔404的元件檔區段416和bss區段418分別可以被映射到可執行映射406的元件檔區段422以及bss區段428。可以鏈結可執行映射406以在可執行映射406開端的預定位置包含用戶定義的區段，由此可以按順序對其進行檢查。藉由驗證的完整性檢查可以僅限於代碼庫的一個子集。那些被分組到較大本文分段的剩餘代碼可以不被執行完整性檢查、及/或是可以載入的。

【0069】 用戶定義的區段的添加可以是可識別的，例如藉由在元件代碼中插入#_PRAGMA。仍舊參考第4圖的示例，在原始檔案的頂部可以插入指令#_PRAGMA區段（例如元件檔區段408）。可以用編譯器旗標來包含用戶定義的區段以增強編譯器。如果設定了特定的旗標，那麼可以增強編譯器來自動插入PRAGMA。此外，用戶定義的區段的概念可以擴展，以將用戶定義的區段限於那些可能被完整性檢查的元件內部的功能。可用於裝

置的可信執行的功能可被分區或隔離成在啓動過程中首先或者早期會被完整性檢查的元件。

【0070】 區段可以經由鏈結器命令檔而被映射到記憶體的特定分段。ELF 物件可以依照來源和目的地址來查看。在區段標頭表中識別的區段可以向載入器告知在哪兒發現所要移動的代碼及/或資料的開端。在分段標頭中識別的分段可以向載入器告知將元件拷貝至何處。在下文中示出了區段和程式標頭的格式。

區段標頭	程式標頭
typedef struct {	typedef struct {
Elf32_Word sh_name;	Elf32_Word p_type;
Elf32_Word sh_type;	Elf32_Off p_offset;
Elf32_Word sh_flags;	Elf32_Addr p_vaddr;
Elf32_Addr sh_addr;	Elf32_Addr p_paddr;
Elf32_Off sh_offset;	Elf32_Word p_filesz;
Elf32_Word sh_size;	Elf32_Word p_memsz;
Elf32_Word sh_link;	Elf32_Word p_flags;
Elf32_Word sh_info;	Elf32_Word p_align;
Elf32_Word sh_addralign;	} Elf32_Phdr;
Elf32_Word sh_entsize;	
} Elf32_Shdr;	

【0071】 sh_addr 是程式區段可以在目標記憶體中駐留的位址。p_addr 可以是程式分段在目標記憶體中駐留的位址。sh_addr 和 p_paddr 欄位可以是指載入位址。載入器可以使用來自區段標頭的載入位址欄位作爲

將映射從非揮發記憶體轉移到 RAM 的起始位址。

【0072】 元件區段識別碼的概念可被擴展至檔案內部包含的一個以上的特定元件。該擴展可以經由識別將被執行完整性檢查的特定子常式而不是整個檔案來允許策略管理器所實施的存取控制的進一步的粒度。

【0073】 TRV 可以是特定元件或物件檔的預期量度（例如以安全方式計算的元件的散列）。出於完整性核實的目的，舉例來說，驗證處理可以依靠將被檢查的存在於可執行映射中或是分別以安全方式載入的每一個元件的 TRV。該處理可以採用多種方式來實現。作爲例證，對建構可執行映射的工具鏈進行修改可以安全地計算元件或物件檔的散列值，並且安全地將計算得到的 TRV 插入同一物件檔的恰當區段。該計算可以作爲鏈結過程的一部分來執行。計算 TRV 散列的順序可以與要載入和量度的元件的順序匹配，否則有可能無法正確匹配量度值。該散列值可以被載入器得到或是包含在可執行映射內部。爲了維持信任鏈，可以安全地產生及/或儲存 TRV。舉例來說，藉由使用與諸如軟體/韌體製造者的公鑰之類的公鑰相對應的私鑰來對 TRV 值進行簽名，可以保護 TRV。

【0074】 元件物件檔可以包括單獨的用戶定義區段，以作爲如第 5 圖所示的與之關聯的 TRV 的占位符。舉個例子，如第 5 圖所示，元件物件檔 408 的 TRV 可被計算並儲存在元件 TRV 區段 502 中。區段標頭可以識別該區段的起始位址及/或尺寸，其中該區段包括這裏描述的用戶定義區段。在物件檔 402 上，鏈結器可以在符號解析階段結束時計算元件物件檔 408 的散列值，以及定位相應的元件 TRV 區段 502。該元件 TRV 可被插入到處於記憶體中的指定位置的可執行映射（例如元件 TRV 區段）。區段標頭可以允許載入器在驗證處理期間定位特定區段的 TRV。

【0075】 這裏描述的裝置驗證可以關注於元件的完整性狀態。由於軟體的開發實踐有可能會隨著公司的不同而不同，因此有可能很難使關於故障的軟體的報告處理標準化。

【0076】 在這裏揭露了用於將對照軟體執行的功能以分組元件的方式進行標準化的系統、方法和手段。將功能標準化可以使其與標準規範一致及/或採用與實施方式無關的方式。在這裏可以爲可被標準化的裝置功能預先定義一個功能列表。可以使用功能與元件之間的關聯以允許將完整性檢查期間發現的故障映射到特定功能以進行報告，並且在第 6 圖中描述了它的一個示例。

【0077】 如第 6 圖所示，信任域 602 可以包括相互映射的元件和功能。例如，可信任域 602 可以包括高階功能 604、中間功能 606 及/或可信環境（TrE）核心功能 608。高階功能 604 可以包括功能 610 和功能 612。中間功能 606 可以包括功能 614 和功能 616。TrE 核心功能 608 可以包括功能 618，例如 RoT。功能 612 可以映射到元件 620 及/或 622，其中舉例來說，該元件可以是軟體元件。功能 616 可以映射到元件 624，舉例來說，該元件同樣可以是軟體元件。功能 618 可以映射到元件 626，其中舉例來說，該元件可以是韌體元件。在對可信任域 602 執行完整性檢查期間，在元件 624 上可能會確定出故障。由於元件 624 映射到了功能 616，因此可以確定網路功能 616 同樣存在故障。由此，裝置可以向網路發送關於故障的功能 616 的指示，以進行修復。

【0078】 第 6 圖中的功能與元件之間的映射是作爲執行層映射而被示出的。作爲第 6 圖示出的實施例的替代或補充，元件與功能之間的映射可以具有一個以上的層。可以使用具有兩個以上的層的資料結構（例如，

其中一個層用於元件，另一個層用於功能）。在該結構中，元件可被映射到一組子功能，並且子功能可以被映射到一組更高階的子功能。中間映射可以持續進行，直至處於最終子功能層的子功能被映射至處於最終層的最終功能。樹或類似於樹的資料結構可以是能夠獲取這種多層元件-功能映射關係的結構的一個示例。

【0079】 開發者可以確定元件如何映射至標準化功能。根據一個實施例，可執行映射可以包括元件-功能映射。舉例來說，這種映射可以在編譯時經由一個圖形工具來實現，其中該圖形工具對經編譯的代碼或來源代碼進行解析，顯示了單一檔案佈局、檔案中的函數相互依存性中的一項或多項，以及允許將元件映射到功能。功能可以是本文欄位及/或縮寫 ID 號碼，其中該本文欄位及/或縮寫 ID 號碼可以由用戶輸入及/或手動映射到元件/檔案。開發工具可以創建引用了元件至功能映射表的區段。元件名稱、功能名稱以及 ID 連同交叉引用的互連一起可以作爲該表的元素而被包含。

【0080】 第 7 圖示出的是包含元件-功能映射的區段的一個示例。如第 7 圖所示，功能至元件映射區段 702 可以作爲諸如物件檔 402 之類的物件檔中的區段而被包含。此外，如這裏所述，功能-元件映射區段 702 還可以鏈結到可執行映射中的相應分段。

【0081】 載入器的功能可以是將代碼從外部記憶體引入內部記憶體。信任鏈可以依靠正由從 RoT 和引導載入器開始的先前階段所核實的每一個已載入階段的代碼。第二階段的載入器可以核實下一個階段，該下一個階段則可以包括可信環境核心以及 OS 載入器。一旦 OS 被初始化且正在運行，則剩餘的完整性檢查可以如這裏所述由標準的 OS 載入器執行。可執

行映射可以在沒有高速存取的情況下被載入到 RAM。這裏揭露的這些概念可以擴展成包含更多具有附加修改且可執行映射大於可用 ROM 的受限實施方式，例如使用快取記憶體以及直接從 ROM 執行代碼。

【0082】 將代碼從外部引入內部記憶體的載入器可以包括執行密碼加密的完整性檢查的能力。該完整性檢查回過來可以引用安全地保持在可信環境中的密碼加密功能。在正常的操作中，載入器可以將諸如本文區段 410 之類的組合本文區段以及諸如資料區段 412 之類的資料區段中的代碼和資料拷貝至鏈結器命令腳本和分段標頭資訊所定義的內部記憶體。與成批載入本文區段 410 和資料區段 412 不同，載入器可以識別用戶定義的代碼及/或資料區段。這其中的一些補充區段資訊可用於完整性檢查。載入器可以計算元件的完整性量度，然後將元件的 TRV 定位在與其關聯的區段。區段標頭可以提供區段的起始位址和大小。量度值可以與同一個元件的已儲存 TRV 進行比較。如果值是匹配的，則可以將代碼載入到內部記憶體。如果完整性量度不匹配，則不能載入代碼，並且可以爲元件記錄故障及/或將故障報告給策略管理器。

【0083】 每一個元件的載入器核實結果可以儲存在表明該元件已被檢查的位元欄位以及通過與否的位元欄位中。在將全部代碼移至內部記憶體時，策略管理器可以基於已完成的完整性檢查結果來確定授予裝置怎樣的存取。一種實現該處理的方式是規定載入器可以存取安全的記憶體位置來追蹤完整性結果。程序鏈結表（PLT）可以用附加資訊元素增強，以追蹤是否已經檢查並核實了元件完整性，並且在每次將經過檢查的元件載入到 RAM 的時候可以更新完整性檢查結果以及該資訊。

【0084】 在具有有限記憶體的嵌入式系統中，可以使用代碼調換。代

碼調換可以包括將那些可能用於執行的功能載入到 RAM 中。如果使用了子元件，那麼可以在 RAM 中未提供該子元件的情況下，使用 PLT 和 GOT 表來定位其位址。子元件可以是具有相關聯的 TRV 的較大元件中的小的部分。在載入子元件時對其進行動態檢查的系統中，在每次載入子元件的時候都可以使用關於整個元件的完整性檢查。這種需求有可能在系統上添加不必要的計算負擔。

【0085】 元件可以分成其子元件，並且可以計算中間 TRV，該中間 TRV 可以用於檢查每一個子元件的完整性。此外，實施最小塊尺寸可以計算出中間散列。這個產生子元件的 TRV 散列的過程可被稱爲 TRV 分解（digestion）。例如，小的子元件散列可以是基於記憶體頁面塊大小來計算。舉例來說，這種將元件拆分成子元件的處理可以在對元件執行作爲安裝或啓動過程的一部分的完整性檢查的時候進行。此外，將 GOT 增強以包含每一個子元件的中間 TRV。

【0086】 平臺完整性策略引擎（PIPE）可以是整個平臺的信任系統架構的一部分。例如，PIPE 可以防止下列各項中的一項或多項：網路受到攻擊、誤用裝置、在平臺上以未經授權的方式傳遞或操縱敏感資料。PIPE 可以依靠諸如引導載入器、策略管理器和虛擬化元件之類的不同作業系統功能來控制和創建安全可信賴的平臺。該 PIPE 可以控制不同的功能，該不同的功能包括安全引導處理流程、關於軟體元件的完整性檢查量度的處理、依照策略的後續強制動作、及/或後續的軟體負載控制流程。這些策略可以由外部的利益相關者定義，例如製造者或操作者，並且是可以在裝置上供應的。此外，這些策略可以經由遠端更新程序而在欄位中被更新。

【0087】 PIPE 可以通過下列各項中的一項或多項來減小載入受損軟

體功能的風險：受控軟體資料檢查和載入操作、漸進式地安裝更多的功能能力、或者在運行時保持元件的動態載入。依照載入操作的進度階段，該動作可以包括下列各項中的一項或多項：將平臺斷電；阻止載入一個或多個受損元件或是隔離一個或多個元件；觸發針對網路中的諸如安全閘道或修復管理器之類的外部實體的警報，以通告低階故障或是受損功能；禁止存取平臺上的安全資訊，例如驗證密鑰等等；禁止存取平臺上的安全功能，例如驗證演算法等等；執行成批代碼或資料重載/更新程序；替換受損的軟體元件及/或配置資料；或者進行更詳細的調查，包括以更高的細節粒度來對疑似受損的元件執行完整性檢查，以隔離元件中的故障位置。

【0088】 在一些情況中，故障有可能非常嚴重，以至於可信任環境由於核心 TrE 功能已經受損而不能保證平臺的信任度。低階故障有可能觸發諸如產生用可信根簽名的預設警報訊息之類的基本操作，其中可以包括完整性和重播保護以及機密性保護。換言之，一旦發生了嚴重的低階安全故障，則可以藉由一個或多個可用通信頻道來向網路釋放困擾訊息。

【0089】 由於所載入的功能已被建構並且變得日益複雜，裝置有可能執行更複雜的動作，例如充當代表網路實體的安全可信賴代理，這樣做可以促進用於診斷、報告及/或替換受損軟體或配置資料的詢問程序。

【0090】 依照成功核實的功能等級，可以（例如由 PIPE）提供針對平臺上的資源的不同存取。如果元件的完整性檢查失敗，那麼其可能不是可信的。偵測到的這種故障可以被安全標記並（顯性地或隱性地）指示給網路，並且引導流程有可能因爲這個故障的狀況而出現分支。這種完整性檢查故障可被稱爲執行流程故障，由此，經過檢查的元件可能不是可信賴的，並且啓動該元件有可能會導致執行惡意的、受損的、有故障的或是錯

誤配置的代碼，而這有可能導致裝置以非指定及/或非預期的方式執行網路功能。由此，新元件和可用功能的載入可能受到先前載入的元件的完整性的影響。

【0091】 結果，執行環境有可能根據控制執行過程及/或每一個引導階段以及每一個運行時間過程的存取許可權而改變。例如，在引導過程中的每一個階段，可以基於在該時間產生的完整性量度來做出決定。後續的階段和策略可以使用通過任何超越了執行階段的可用安全資訊運送或儲存手段而從先前階段傳遞的資訊（狀態、變數、參數、暫存器、檔案等等）來確定自己的操作。例如，上層應用驗證功能可以使用關於先前載入的元件的完整性的資訊來確定自己的操作，其中包括閘控釋放那些用於與例如外部實體進行成功驗證的密鑰。

【0092】 例示的 PIPE 功能流程可以採用這裏描述的方式執行。例如，在這裏可以對 RoT 執行完整性檢查、及/或其完整性可被核實。RoT 可以對基線 TrE 執行完整性檢查、及/或該基線 TrE 的完整性可被核實。如果在對基線 TrE 進行完整性檢查及/或核實中發生故障，那麼 PIPE 可以阻止用於連結於網路的密鑰的釋放、觸發針對網路的警報、及/或將裝置斷電。如果 PIPE 觸發針對網路的警報，則可以載入能向網路發送警報的後降代碼。該警報可以觸發遠端成批更新程序，以替換 TrE。

【0093】 如果在對基線 TrE 的完整性檢查及/或核實中沒有發生故障，那麼可以載入基本的通信連接代碼。這可以包括執行完整性檢查以及載入基線作業系統模組、執行完整性檢查以及載入基線管理用戶端、及/或執行完整性檢查以及載入通信模組。如果在檢查作業系統模組、基線管理用戶端及/或通信模組的完整性的同時識別出故障，那麼 PIPE 可以阻止用於

連結到網路的密鑰的釋放、觸發針對網路的警報、執行遠端成批程序來替換元件、執行遠端元件更新程序、及/或將裝置斷電。如果 PIPE 觸發遠端成批更新過程，那麼可以載入能夠向網路發送警報的後降代碼。該警報可以觸發遠端成批更新程序，以替換基本代碼。

【0094】 如果在對基本通信連接代碼的完整性檢查及/或核實中沒有出現故障，那麼可以對剩餘的作業系統及管理用戶端元件執行完整性檢查及/或載入這些元件。這可以包括執行完整性檢查及/或載入可重新定位及/或重新載入的功能模組。如果在完整性檢查期間識別出故障，那麼 PIPE 可以阻止釋放用於連結到網路的密鑰、向網路發送依照協定的故障報告、觸發警報及/或請求遠端元件更新程序、及/或將裝置斷電。該故障報告可以指示故障的元件，該元件例如可以由網路遠端更新。

【0095】 PIPE 的動作可以根據成功核實的引導鏈而改變。在引導過程的每一個階段都可以基於爲在該時間（或是該時間之前）被執行了完整性檢查的部分或全部底層平臺的經評定的完整性以及所應用的策略來做出決定。這些策略可以根據所實現的信任等級而適配或被其他策略替換。執行環境可以根據每一個引導階段的控制策略而改變。後續的階段及/或策略可以使用經由超越了執行階段的可用安全資訊運送或儲存手段而從先前階段傳遞的資訊（例如狀態、變數、參數、暫存器、檔案等等）。

【0096】 舉例來說，如這裏所述，PIPE 可以在平臺上規定策略，其中該策略可以根據如第 8 圖所示的平臺初啓和信任狀態的所實現等級而進行適配或改變。如第 8 圖所示，依照相應的策略 812，可以對 TrE802 執行完整性檢查、載入及/或執行該 TrE802。在將 TrE802 確定爲是可信實體並且執行該 TrE802 之後，裝置可以移動到引導序列的下一個階段。例如，可

以依照策略 814 來對能力 804 執行完整性檢查、載入及/或執行該能力 804。關於能力 804 的完整性檢查、載入或執行可以基於與 TrE802 的完整性檢查、載入及/或執行相關聯的資訊（例如信任狀態）。在引導序列先前階段中實施的策略 812 可以向在關於能力 904 的完整性檢查、載入及/或執行期間實施的策略 814 發出通知。在將能力 804 確定爲是可信實體並且執行了該能力 804 之後，該裝置可以移動到引導序列的下一個階段。該引導序列可以藉由依照相應的策略 816、818 和 820 分別檢查、載入及/或執行能力 806、808 和 810 而繼續進行。如這裏所述，引導序列的每一個階段可以由引導序列中的一個或多個先前階段通知。

【0097】 這裏描述的策略可以由諸如操作者之類的可信外部實體規定。所實現的平臺信任狀態的結果可被傳遞到外部實體，舉例來說，該外部實體有合法的興趣/權利來瞭解平臺的信任狀態，諸如敏感應用或服務的操作者或提供者。應該指出的是，對於可以在啓動或平臺操作循環中的不同階段評定的有關平臺可能的不同狀態的資訊來說，這些資訊可被傳遞到一個以上的外部實體。

【0098】 多層完整性檢查以及將這種完整性檢查綁定到平臺信任狀態的處理可以採用這裏描述的方式執行。例如，這種完整性檢查和綁定可以使用多層完整性檢查，以藉由策略和強制執行來確保裝置上的密鑰驗證裝置實現的能力（例如針對網路上的伺服器之類的外部核實器且執行修復任務的裝置修復功能）。如果某個用於實現預期能力的預先已知的軟體及/或配置檔集合通過了完整性檢查，那麼使用這種密鑰來進行驗證的安全敏感功能對於裝置而言將會是可用的。舉例來說，這種軟體及/或配置檔可以包括低階 OS 功能、驅動、配置檔及/或通信堆疊代碼的某個子集。

【0099】 多層完整性檢查以及完整性檢查綁定還可以包括用於保護驗證密鑰的策略，由此可以將密鑰限制爲只供已授權功能或過程使用。如果密鑰未受保護，那麼軟體有可能受損害以存取該密鑰。裝置可以提供可信功能以：對密鑰進行保護，使得其僅限於供有限集合的能力、功能或單一功能使用；保護對密鑰進行操作的功能/程式；及/或限制可以調用這其中的某個特許功能的物件（例如用戶、系統、腳本等等）。

【0100】 這裏描述的關於多層完整性檢查和綁定的實施例可以包括一組預先已知的軟體，這些軟體可以用於允許可能受損的裝置向外部實體驗證其部分能力（例如其報告故障以及與修復伺服器或是用於此類伺服器的 AAA 實體一起執行修復操作的能力）。外部實體（例如修復伺服器）可以是一個邏輯實體，並且可以由裝置管理伺服器託管，其中對於 H(e)NB 來說，該外部實體是 H(e)MS。

【0101】 爲了提供用於規定與特定平臺上的實際實施方式無關的策略的機制，在這裏可以藉由規定特定平臺能力所需要的功能來定義這些策略。由此，與特定能力相對應的策略也可以採用與這裏揭露的元件-功能映射相似的方式映射到功能。外部利益相關者可以將關於特定能力的策略規定給單一功能或若干個功能。而 PIPE 則可以在將能力映射到特定策略以及映射到平臺初啓階段中負責解釋策略需求。

【0102】 如果某個能力使用了某組功能，那麼可以爲指定給該特定能力的相應策略規定這些功能。舉個例子，如果希望將執行修復的能力映射到某個策略，那麼可以將用於執行修復的功能映射到相應的策略，例如，修補能力可以被功能 1、2 和 3 覆蓋，從而規定將相應的策略映射到功能 1、2 和 3。

【0103】 對於一些實施方式來說，在分層的平臺初啓與能力和功能之間存在著合理的相關等級。這些能力可以是隨著功能一層一層地漸進式初啓的。例如，在平臺初啓的較早階段即可初啓修復功能和能力。

【0104】 多層完整性檢查可不按順序確定不同功能的已檢查-未檢查狀態。這些功能可以是依照順序方式檢查的。然而，由於不同的功能可被映射到不同的元件（隨後可以在不同的階段載入這些元件），因此，依照功能的完整性確定處理有可能會以非順序方式執行、或者以一種可不與依照元件的完整性檢查的原子處理序列同步（在時間長度或時間順序方面）的順序方式執行。

【0105】 序列化可被用於策略實施。策略實施可以爲給定的平臺能力確定相應的功能是否已經通過了完整性檢查及/或是否應該應用策略。

【0106】 多範圍驗證可以允許平臺基於所實現的平臺信任等級來向一個或多個外部實體進行驗證。該驗證機制（例如驗證詢問回應機制）可被用作一種將最終得到的裝置完整性範圍傳達給外部實體的手段。該外部實體可以驗證並且同時獲得關於裝置完整性範疇/範圍的指示。

【0107】 在經歷多層完整性檢查的同時，裝置的 TrE 可以產生用於驗證詢問回應的不同參數或參數值，以用於不同的目的。根據成功的完整性檢查的範圍，這種參數產生可以基於或使用與外部驗證實體共享的相同的秘密證書。所使用的可以是常見的詢問-回應計算演算法。然而，根據完整性檢查的範圍及/或驗證目的，至這種演算法的輸入可能是不同的。舉個例子，如果 TrE 成功檢查了整個代碼庫，那麼可以使用諸如“已成功檢查整個代碼庫（entire code basis successfully checked）”之類的本文串作爲驗證詢問回應計算演算法的輸入。如果 TrE 成功檢查了用於實現困擾修復功能

的元件，但是未必檢查了整個代碼庫，那麼可以使用諸如“已成功檢查用於困擾修復的代碼庫（code base for distress remediation successfully checked）”之類的另一個字串。

【0108】 一旦向裝置發送了其驗證詢問請求，則外部驗證器還可以計算兩個版本的“預期”詢問回應。由於其可能不知道在計算裝置上計算詢問回應中已經使用的輸入，因此，其有可能必須同時計算所有這兩個版本的回應。藉由將從裝置接收到的回應與預期回應集合進行比較，外部驗證器可以隱性地成功測試出裝置完整性“範圍”。 藉由歸納，實體可以驗證及/或核實在裝置端已成功檢查了裝置完整性的某個“範圍”。在以上的示例中，可以使用相同或相似的實施方式來驗證裝置的另一個特定（例如部分）能力，這一點取決於對功能進而是用於實現該能力的元件所進行的完整性檢查。

【0109】 舉個例子，可被核實信任度的外部指示可以是在安全引導處理期間將代碼的完整性量度綁定到特定的引導循環執行和配置簽名的受保護的簽名證書版本。在這裏可以包括安全的時間戳、受保護的依照引導循環遞增的單調計數器、或引導循環秘密（在每個引導循環中產生或引入一次的隱藏隨機值，例如亂數（nonce））。當滿足前提條件時，驗證密鑰將會變得可用，並且目前的可信賴處理將會設定逐次引導的受保護一次性可編程“通過”旗標，該旗標可被限制爲在下一次重置之前恢復至發生故障的狀況（例如偵測到初始量度之後的故障的時候）。在釋放給外部實體之前，諸如 TrE 之類的永久性可信任環境（例如進入運行時間而不僅僅是引導時）可以使用驗證協定亂數來對狀態資訊進行簽名。該報告的區段可以由永久性核實的可信賴處理以臨時引導密鑰來簽名，由此，以後的處理可以將此

狀態呈現給外部實體，以進行驗證。

【0110】 在這裏可以使用在驗證協定中交換的一個或多個經過修改的隨機亂數，並且這種經過修改的亂數可被用作詢問回應以及所預期的詢問回應計算的輸入。換言之，在裝置本身，裝置的 TrE 可以嘗試以常規方式使用在回應計算輸入（例如在通過了完整性檢查的情況下）中從驗證伺服器接收的一個或多個隨機亂數來計算其驗證回應。如果關於整個裝置的完整性檢查失敗，但是裝置部分功能的完整性檢查成功，例如“困擾/修復功能”的完整性檢查成功，那麼 TrE 可以計算該回應的另一個值，此時使用的是所接收的亂數的修改版本。驗證伺服器可以知道在哪里/如何執行這種修改。這種修改的示例可以包括：改變初始亂數中的已知位置的一個或多個位元。這樣一來，除了計算初始的“裝置驗證”回應之外，裝置和驗證伺服器都可以使用經過修改的亂數輸入來計算回應。在接收器上（例如驗證伺服器），伺服器可以檢查其從裝置接收的回應是否與“裝置驗證”回應相匹配。如果它們不匹配，則與聲明驗證徹底失敗不同，驗證伺服器可以將接收到的回應與使用經過修改的亂數計算的另一個回應值進行比較。如果它們匹配，那麼驗證伺服器可以確定雖然裝置整體可能沒有通過驗證，但是某些功能是可以通過驗證的，例如本示例中的“困擾/修復功能”。

【0111】 在安全引導處理期間，藉由對照相應的 TRV 來比較每一個軟體元件，裝置可以獲悉元件的完整性故障，這樣做有助於確保元件的位元精度以及來源的真實性。

【0112】 偵測到的元件檢查故障可以在完整性檢查狀態資訊元素中獲取。出於安全性目的以及出於對報告和診斷效率的考慮，此狀態資料的

結構可以採用多種形式。該資訊可以被支援策略管理程序的目前和後續引導階段以及運行時間進程讀取。元件-功能映射可以用於確定元件與網路功能以及裝置的其他功能的依存關係。功能可以是諸如網路操作者之類的連接實體或是諸如移動支付之類的裝置支援的加值應用所依靠的功能。操作者及/或應用服務提供者可以定義哪些功能可被用於針對特定任務的可信裝置操作，例如承載訊務、修復、管理操作或加值應用特徵，並且可以在裝置上設定用於表明哪些功能可用於特定網路操作的策略。

【0113】 一組網路功能可以來自網路操作者及/或應用服務提供者所預期的標準能力集合。這些功能可以包括無線電技術、協定堆疊中的層、網路協定、管理能力、安全和信任機制、加值應用特徵等等。

【0114】 裝置的策略管理器可以使用顯示了依照裝置元件的網路功能依存關係的嵌入式元件-功能表或映射（如這裏所述）。在第 9 圖中顯示了在完整性檢查及/或報告期間使用這種元件-功能表或映射的處理。如第 9 圖所示，在 910，裝置可以藉由以相應的 TRV 904 檢查元件 902 的完整性量度來執行完整性檢查。在執行了完整性檢查之後，在 916，裝置策略管理實體 908 可以接收到已經經過了完整性檢查的一個或多個元件的元件識別符（例如元件位址），並且會在 918 接收到關於每一個元件是否通過或未通過完整性檢查的指示。該策略管理實體 908 可以確定與元件相關聯的相應功能，以發送至網路實體。舉例來說，需要修復的故障的功能可被發送，或者可以發送關於已被驗證的功能的指示。例如，策略管理實體 908 可以在 920 使用的元件位址在 922 檢索與所給出的元件相對應的元件識別符。如第 9 圖所示，元件識別符可以是從表 906 中檢索的，其中該表 906 包含了元件位址到元件識別符的映射。在 924，策略管理實體 908 可以使用元件識別符

以在 926 檢索與所給出的元件相對應的元件功能。這些元件功能可以是從表 912 中檢索的，其中該表 912 包含了元件識別符至元件功能的映射。在 932，策略管理實體 908 可以使用所確定的功能（例如已通過或未通過完整性檢查）來與網路實體進行交互作用。例如，策略管理實體可以執行完整性報告、接收裝置策略、或者接收與所確定的一個或多個功能相對應的動作及/或限制。每一功能可與一個或多個策略 930 相關聯。所收集的一個或多個功能可以一起啓用裝置內部的特定功能。這些能力可以是分層次的。例如，基礎層能力可以是下一個能力層的子集，該下一個能力層則是接下來的能力層的子集等等。將能力分層可以反映典型層或信任鏈爲基礎的安全引導序列。層可以是能夠實現特定能力的功能的任意組合、或者其也可以是分層的層次與特定功能組合的混合組合。策略管理實體 908 可以在 928 使用元件映射功能以在 930 檢索與給定能力相對應的一個或多個策略。這些策略可以是從表 914 中檢索的，其中該表 914 包括能力與不同策略的映射。如 932 所示，這些策略可以從網路實體接收的。

【0115】 故障的元件可能導致出現一個或多個故障的功能。軟體發展和建構工具嵌入的元件至功能映射資訊可以在確定功能的完整性檢查故障量度中爲策略管理器提供支援，並且由此支援以標準化的方式報告可能與裝置和製造者方面的實施方式無關的故障，例如驗證功能或基帶無線電協定堆疊故障。在裝置上，該資訊可以可被保護免於修改，這一點是由不可變的可信根（RoT）保證。

【0116】 策略管理進程可以在引導和運行時間環境中使用該資訊。使用完整性檢查處理的結果，裝置上的策略管理進程可以確定哪一個網路功能已經發生故障。在載入器檢查代碼的時候，元件可以用在引導時間期間

可用的參考（例如符號表或記憶體位址）來識別。在已核實了完整性和來源的真實性之前，被檢查的代碼可被隔離，以免在可執行記憶體中使用。同樣，從載入、檢查被檢查的代碼時起以及在執行期間，所述被檢查的代碼可以受到保護（例如藉由受保護的方式執行和儲存、硬體保護、密碼加密保護、虛擬化等等）。藉由修改記憶體映射、存取許可權等等，可以阻止執行。作爲在第 9 圖的表 906 和 912 中示出的示例，處於位址位置 x 的代碼可以對應於元件 A，該元件 A 可以映射到網路功能 F1、F5 和 F14。舉例來說，這個代碼可以是一個原始的散列函數，並且有若干個通信協定是依賴該函數的。完整性報告和修復有可能依賴於故障的基元。因此，在網路標準化列表中可以包含這些完整性報告和修復功能，以此作爲底層的支援功能。

【0117】 功能故障的標準化列表可以向網路提供關於裝置能力的細粒度資訊。對於遠端裝置來說，可靠地理解裝置所能實現的功能有助於應用資源來修復問題。在困擾情況下，如果有能力以安全和有保證的方式指示故障，從而使得網路可以驗證困擾指示本身（例如來源、時間和精度）的完整性，那麼可以防止在虛假警報的情況下不必要地使用昂貴的網路資源。

【0118】 第 10 圖提供的是包含了例示系統元件的報告和修復系統的例示綜述。如第 10 圖所示，在 1002，在裝置 1004 的元件上偵測到故障。該故障可被指示給網路。例如，在 1008，該故障可以被包含在報告給網路的裝置報告 1006 中。舉例來說，該故障可被指示爲是與故障的元件相關聯的故障的網路功能。在向網路報告故障時，網路可以做出關於存取控制的細粒度決定。例如，網路平臺驗證實體 1010 可以基於所報告的功能檢查報

告 1006 來允許禁止存取、局部存取或是完全存取。在 1016，裝置 1004 可以接收存取決定。如果在裝置報告 1006 中指示了故障，那麼網路平臺驗證實體可以將功能報告轉移給裝置管理伺服器 1012，該伺服器 1012 可以從功能至元件映射資訊 1014 中確定一個或多個故障的元件。此資訊可以用於修復裝置 1004、以及重新載入裝置 1004 中故障的軟體元件。例如，裝置管理伺服器 1012 可以在 1018 詢問裝置 1004，以窄化與故障的元件相關聯的故障的功能的範圍。在將完整性故障隔離到裝置 1004 的某個區段以便有效修復之後，裝置管理伺服器 1012 可以在 1020 請求軟體更新（例如替換元件），例如從代碼建構釋放實體 1022 請求。裝置管理伺服器 1012 可以在 1024 向裝置 1004 提供軟體更新，以修復故障的元件。製造者裝置上的特定故障代碼的這種抽象形式將會減小操作者緊密瞭解裝置（與之相連）的負擔，但是同時還可以允許基於故障的功能的粒狀存取控制及修復決定。

【0119】 執行流程故障有可能是在處理鏈中調用的元件的故障。元件的執行可以保持很高的確信等級，同時擴展裝置的能力。在目前已被核實的處理檢查下一個處理的代碼（並且有可能檢查裝置的配置）的完整性並且發現其出現故障的時候，這時有可能偵測到執行流程故障。後續引導代碼中的故障有可能意味著目前可信處理可以執行下列各項中的一項或多項：將目前狀態鎖定成最後一個已知的良好狀態；指示故障；將對於處理的控制保持在等待模式中；將控制權傳遞到困擾處理；及/或將控制權傳遞到不可信賴的處理。用於故障的階段的驗證和身份密鑰可被鎖定來避免進一步處理，以使不可信賴的處理無法通過報告（例如帶簽名的狀態）或是驗證技術（例如自主驗證）來向網路指示有效狀態。

【0120】 出於對效率的考慮，從裝置發送到網路的故障報告可以包括

用於提示來自操作者網路驗證功能的動作以執行細粒度閘道存取控制以及向網路裝置管理實體指示裝置故障的最低的資訊量。管理實體可以查看製造者專用資訊來確定故障的根本原因、以及確定哪些代碼可被修復。該管理實體可以向網路驗證功能反向提供進一步的資訊，以允許實體做出關於存取控制及/或修復的進一步策略決定。

【0121】 在下表 1 中描述了可以包含在故障報告中的故障的功能的例示集合。

故障的功能列表（代碼，資料，參數）
LTE
基帶域

表 1：用於故障的功能的例示完整性違例（由 TrE 簽名的故障報告）

【0122】 在這裏可以發送關於通過或未通過這樣的結果的功能報告。表 2 提供了關於這種列表的一個示例。

功能（代碼，資料，參數）	狀態（未通過或通過）
整體結果	
LTE	
UMTS	
核心閘道命令	
管理命令	
WiFi	
UICC/智慧卡頻道	
應用域	
基帶域	

表 2：用於功能的例示完整性違例（由 TrE 簽名的報告）

【0123】 在驗證期間，該功能報告可以備選頻道上的酬載中傳送，其中舉例來說，該頻道可以是用於閘道驗證的頻道，由此，即使閘道驗證失敗，該報告也可以作爲酬載而在驗證序列中被發送。該酬載可以由裝置的可信執行環境簽名。

【0124】 可信執行環境（TrE）可以具有自己的功能欄位（例如爲了方便起見或出於對冗餘度的考慮）。然而，如果功能或困擾酬載列表是由 TrE 簽名的，或者驗證密鑰是受 TrE 保護的，那麼在與網路取得聯繫的時候，TrE 的完整性是已知的。TrE 的一個或多個簽名密鑰可以用故障防護封閉方法來保護。換言之，如果 TrE 受損，那麼它的一個或多個密鑰是無法得到的（例如既無法被裝置或是其內部功能和介面得到，也不能被 I/O 和測試埠得到，並且不能被外部的網路實體得到）。

【0125】 如果發生故障或警報，那麼服務網路實體可以核實困擾裝置具有可靠報告故障的特徵，並且困擾裝置的機制並未發生故障。有兩種保證形式可以向網路指示報告機制可靠。一種機制可以採用靜態的可信第三方擔保的形式，例如特定類型的裝置與某一組可信賴的報告能力相符的證書。這種擔保可以提供關於處理和發送故障狀況的警報和訊息的裝置能力以及強健等級（或可信賴度）的資訊。網路操作者可以使用經過證實的能力來建立在發生故障警報的情況下恰當自動地做出回應的程序。

【0126】 另一種擔保形式可以是經由與裝置進行的線上事務。在發生故障事件的時候，裝置內部的機制可以提供關於報告機制完整性的指示。這種內部能力有可能涉及靜態的擔保形式，這是因爲它可以允許第三方提供符合證書。

【0127】 在這裏，關於裝置困擾和修復的不同協定流程可以在 H(e)NB 的上下文中描述。然而，這裏描述的概念並不限於這種實施例，而是可以應用於任何通信裝置。根據第 16 圖描述的例示實施例，裝置完整性資訊可從 H(e)NB 經由 SeGW 被發送到管理伺服器（H(e)MS）。根據第 17 圖描述的另一個實施例，H(e)NB 可以直接連接到管理伺服器（H(e)MS）。根據第 18A 和 18B 圖描述的另一個例示實施例，裝置完整性檢查可被加強，以在出現局部故障的情況下允許細粒度的存取控制。這些程序可以允許在 DRF 的控制下執行代碼或資料塊修復，其中該 DRF 可以使用從網路中的修復實體接收的修復資料來改變代碼或資料塊。如果系統架構允許軟體以及軟體或硬體配置資料的變化，那麼這其中可以包括這種變化。所示出的流程可以是針對軟體修復的，但是並不限於此。

【0128】 在網路管理實體與裝置本身之間可以執行詢問，在此期間，關於裝置的發生故障的完整性的詳細資訊可以用比初始報告更精細的粒度擷取。該資訊可以導致發現故障原因、指示元件的哪個部分發生故障、以及允許粒度更細的代碼修復及/或配置，以藉由減小軟體下載大小並且由此平衡網路頻寬需求以及代碼下載大小，實現有效裝置管理。根據一個例示實施例，使用 IP 網際網路協定的受管理網路裝置可以將 TR-069(CPE WAN) 用於裝置管理目的。該協定可以提供針對“自動配置伺服器”（ACS）的存取。ACS 應用可以在表 3 所示的協定堆疊中使用若干種能力。

ACS
RPC 方法
SOAP
HTTP

SSL/TLS
TCP/IP

【0129】 該堆疊可以被 RoT 處理存取，該 RoT 處理可以向連接 TR-069 的管理伺服器提供高保證的困擾指示。但是，在困擾狀況中可不使用每一個層的整個特徵列表，由此可以修整堆疊來執行這些用於安全地將裝置反向自舉至完整的管理和裝置功能的程序。

【0130】 第 11 圖示出的是在裝置上收集資訊來確定可以執行的動作的例示呼叫流程圖。當發生完整性故障時，這時可以在諸如 H(e)NB1102 之類的裝置（例如 TR-069 裝置）與諸如 H(e)MS1104 之類的網路實體之間執行第 11 圖所示的序列。在 1106，在 H(e)NB1102 與 H(e)MS1104 之間可以建立連接（例如 TR-069 連接）。例如，在 1106，H(e)NB1102 可以使用其 TrE 或 RoT 來建立連接。在 1108，H(e)NB1102 可以將一個或多個完整性故障報告給 H(e)MS1104，例如藉由使用資訊請求及/或警報來報告。在 1108，H(e)MS1104 可以接收警報，並且在 1110，它可以使用資訊回應訊息（例如 TR-069 通知回應）來對 H(e)NB1102 做出回應。

【0131】 粗略地說，裝置的每一個軟體元件都可以具有相應的 TRV。如這裏所述，當元件無法匹配參考的時候，該元件有可能具有完整性故障。一些元件有可能很大。例如，作業系統有可能是作爲具有單一 TRV 的單一單體碼塊遞送。

【0132】 第 12 圖示出的是通過詢問來隔離元件中的一個或多個故障的一個或多個位置的例示呼叫流程圖。在詢問過程期間，諸如 H(e)MS 之類的網路管理實體 1204 可以與諸如 H(e)NB 之類的裝置 1202 交互作用，以收集附加資訊來確定可被執行以修復偵測到的故障的動作。根據一個例示實

施例，裝置 1202 可以使用 TrE 或 RoT 來與網路管理實體 1204 交互作用。

【0133】 網路管理實體 1204 可以決定執行整個代碼映射的單體下載。該下載可以包括重新載入目前代碼映射以及經過更新的代碼映射。由於可以將整個映射下載至網路管理實體 1204，因此可以在已下載的映射中包含 TRV（初始或更新）。網路管理實體 1204 可以決定下載被報告爲故障的元件，而不是單體下載整個代碼映射。由於可以將包括更新時的 TRV 在內的整個元件下載到裝置 1202，因此，該映射可以是目前元件或經更新的元件的重新載入。對於經更新的元件來說，用戶端管理實體可以管理現有代碼映射，以確保整個映射的完整性和結構保持不變。

【0134】 如第 12 圖所示，在 1206 可以偵測到完整性故障。舉個例子，在裝置 1202 的元件中有可能偵測到完整性故障，並且可以像這裏描述的那樣向網路管理實體 1204 發送完整性檢查報告。在 1208，在裝置 1202 與網路管理實體 1204 之間可以建立連接（例如 TR-069 連接）。在 1210，網路管理實體 1204 可以向裝置 1202 發送關於參數的請求，其中該參數涉及的是與裝置 1202 上的完整性故障相關聯的警報。在 1212，裝置 1202 可以向網路管理實體 1204 發送包含警報細節的參數回應。在 1214，網路管理實體 1204 可以決定窄化一裝置上的元件的完整性故障，以進行修復。爲了窄化完整性故障，在 1216，網路管理實體 1204 可以向裝置 1202 發送參數請求，以獲取更細粒度的量度。在 1218，裝置 1202 可以對裝置 1202 上的元件進行量度。在 1220，網路管理實體 1204 可以對參考進行量度。例如，由於元件製造者可能沒有提供元件量度並且裝置 1202 可以使用動態粒度來產生元件量度，因此，網路管理實體 1204 可以即時產生參考值。舉例來說，網路實體 1204 產生的參考量度可以與裝置 1202 產生元件量度進行比較。裝置

1202 可以在 1222 發送一個向網路管理實體 1204 指示該裝置 1202 已經或者將要採用更細粒度的完整性量度的參數回應。

【0135】 在 1224，網路管理實體可以發送關於一個或多個第一節點（例如一個或多個元件）的完整性量度的參數請求。在 1226，裝置 1202 可以向網路管理實體 1204 發送指示了一個或多個第一節點的完整性量度的參數回應。網路管理實體 1204 可以在 1228 發送關於來自裝置 1202 的接下來的一個或多個節點（例如一個或多個元件）的量度的參數請求。舉例來說，關於接下來的一個或多個節點的量度可以是基於從裝置 1202 接收的一個或多個第一節點的量度請求的。此外，所述接下來的一個或多個節點可以是一個或多個第一節點的部分或子元件。在 1230，裝置 1202 可以向網路管理實體 1204 發送包含了所請求的接下來的一個或多個節點的量度的參數回應。舉例來說，如 1232 所示，來自網路管理實體 1204 的參數請求和來自裝置 1202 的參數回應可以重複進行，直至完整性故障與裝置 1202 的區段（例如元件、函數或是其部分）隔離，以實施有效的修復。在識別並隔離了完整性故障之後，在 1234，裝置 1202 與網路管理實體 1204 之間的連接（例如 TR-069 連接）可以關閉。

【0136】 即使在偵測到故障並且產生了單體塊或元件的多個量度之後，網路管理實體 1204 也可以決定進行詢問。裝置 1202 可以執行完整性量度及/或將完整性量度安排在二元樹之類的用於快速引用的資料結構中。網路管理實體 1204 可以執行相同的處理。這種結構可以揭示單一塊中的多個故障，由此網路管理實體 1204 可以快速確定哪些單體塊或元件未通過完整性檢查，這樣做可以窄化影響範圍，並且可以潛在地減小軟體下載訊務量。如第 12 和 13 圖所示，經過修改的塊的細節可被檢查，以便以比用於

元件或單體塊的 TRV 更精細的粒度來隔離其被損壞的位置。

【0137】 利用窄化元件故障範圍的細粒度資訊，網路管理實體可以爲代碼分段而不是整個碼塊創建下載映射。舉例來說，如第 13 圖所示，在支援若干種功能的大型單體元件 1302 中有可能發生故障。由於整個元件 1302 有可能無法通過完整性檢查，因此，整體量度值 1304 可以與整個元件 1302 相關聯。在 1306，經由裝置與網路管理實體之間的詢問，可以產生精細粒度的量度。該詢問有可能引起更精細粒度的完整性量度，以定位大型單體元件 1302 內部的分段的故障，例如分段 1308。例如，在詢問之後，從完整性檢查中得出的整體量度值 1310 可以包括分段 1308 的量度值 7，而不是與整個大型單體元件 1302 相關聯的量度值 1304。在識別了分段 1308 處的故障之後，這時可以將修復補丁定位到這個分段。該修復補丁可以包括使用大型單體元件 1302 內部通過完整性檢查的其他分段來修復分段 1308 上的故障的指令。

【0138】 所產生的完整性量度的數量可以基於裝置類型來限制。當子元件下載是目前元件的重新載入時，裝置不會使用附加資訊來執行重新載入。但是，如果子元件下載是對已有元件的更新時，那麼用於該子元件的經更新的 TRV 可以包含在該下載中。裝置用戶端和網路管理實體可以同步，以產生相同的更新元件映射，以使更新的 TRV 與經更新的元件映射的散列相匹配。裝置管理用戶端可以管理已有代碼映射，以確保整個映射的完整性不變。

【0139】 詢問處理有可能會修改網路所具有的所報告的故障的功能列表的版本，而這可以被回饋給網路驗證、驗證及/或閘道實體，以修改裝置上的網路存取控制。

【0140】 該詢問處理可以使用迭代量度方法來隔離元件故障，由此網路管理實體和裝置可以漸進式地產生量度，從而窄化指示故障的這些子區段上的映射的視野。該方法可以減小用於給定解析度的量度值的數量，由此允許記憶體受限裝置的量度與解析度之間的折衷。舉例來說，在第 14 圖中示出了這種詢問處理的一個例示實施例。如第 14 圖所示，在元件 1402 中有可能發現故障，並且整體量度值 1404 可以與整個元件 1402 相關聯。在發現元件 1402 中的故障之後，裝置和網路可以執行詢問，並且基於該詢問，裝置可以在元件 1402 上執行第一量度迭代。例如，在第一量度迭代中，裝置可以在元件 1402 的子區段 1406 和子區段 1408 上執行獨立的量度。由此，裝置可以確定子區段 1406 通過了完整性檢查，而子區段 1408 則包含完整性故障原因。這一點可以用關聯於子區段 1406 的量度值 1 以及關聯於子區段 1408 的量度值 2 來指示。由於子區段 1408 仍未通過完整性檢查，因此，整體量度值 1404 仍舊可以指示元件 1402 包含完整性故障。

【0141】 雖然將完整性故障窄化到了子區段 1408，但是裝置和網路可以執行附加詢問程序來漸進式地產生用於修復的粒度逐漸精細的量度。作爲詢問結果，裝置可以在元件 1402 上執行第二次量度迭代。如第 14 圖所示，第二次量度迭代可以在子區段 1408 上執行，這是因爲這個子區段是被確定爲完整性故障原因的子區段。裝置可以在第二次迭代中對子區段 1410 和 1412 執行獨立量度，這樣做分別可以產生量度值 3 和量度值 4。子區段 1410 和 1412 可以是子區段 1408 的子區段。量度值 3 可以指示子區段 1408 的子區段 1410 通過了完整性檢查。然而，量度值 4 可以指示子區段 1412 未通過完整性檢查，並且包含了元件 1402 的完整檢查故障的原因。

【0142】 雖然將完整性故障窄化到了子區段 1412，但是裝置和網路

可以執行附加詢問程序來漸進式地產生用於修復的粒度逐漸精細的量度。例如，裝置可以執行第三次量度迭代。第三次量度迭代可以在子區段 1412 上執行，這是因爲子區段 1412 是在第二次量度迭代之後被確定爲完整性故障原因的子區段。如第 14 圖所示，裝置可以在子區段 1414 和 1416 上執行獨立量度。該裝置可以確定子區段 1414 包含了完整性故障的原因。舉例來說，這一點可以用量度值 5 來指示。在第三次量度迭代之後，由於與包含完整性故障原因的元件 1402 的細粒度子區段相對應，與子區段 1414 相關聯的功能可被發送至網路。作爲詢問結果，網路可以確定能被定位至子區段 1414 的修復補丁（例如替換或修復子區段），並且將該修復補丁發送至裝置，以替換或修復子區段 1414。雖然第 14 圖示出了由於網路與裝置之間的詢問結果而在裝置上執行的三次量度迭代，但是任一數量的量度迭代都可以執行，以隔離包含完整性故障的元件部分。在一個例示實施例中，迭代次數是以服務提供者爲基礎的。在另一個例示實施例中，裝置管理伺服器保持了與不同標準相對應的故障資料庫，其中該標準包括裝置識別和軟體版本號碼。舉例來說，故障資訊可以允許裝置管理伺服器評定詢問策略。

【0143】 在對比諸如樹的完全產生之類的其他演算法來確定這種漸進式方法的值的過程中，關於網路通信成本、量度計算以及用於量度計算的值的負載之間的比較是可以加權的。

【0144】 在漸進式方法中，量度可以是在窄化故障欄位的時候取得。代碼/資料可以被重複量度。可以使用混合方法來減少有可能被再次量度的代碼/資料總量，其中舉例來說，該代碼/資料初始可以將映像分割爲某個最佳數量的子區段。藉由用某個因數對映射進行劃分，可以以漸進地方式進一步解析故障的一個或多個區段。該因數可以是依照迭代確定的，並且是

以其他時間延遲以及性能考慮因素爲基礎的，由此通過在網路上使用最小頻寬和最小功率消耗，最佳化故障隔離以及確定的速率。爲了加快故障隔離處理，網路可以在用於指定元件故障的散列樹之類的資料結構中預先產生一組預期散列，以及向裝置發送這個子 TRV 量度樹。這樣做可以允許裝置在這種漸進方法中進行比較，直至達到樹的最高解析度。網路可以確定是否需要更大的解析度來最佳化修復程序（例如基於需要被校正的裝置的數量）。如果需要更大的解析度，那麼網路可以產生和發送始於更精確的位置的新樹，或者可以交互執行該比較。

【0145】 對於軟體或資料更新來說，軟體管理伺服器可以對檔案中的簡單的二進位差異執行代碼/資料更新，以執行更新。裝置管理用戶端可以接收二進位更新，並且對完整的代碼映射進行修改來確保其完整性。相同的二進位差異原理可以擴展至包含用於軟體管理實體的詢問技術，從而減少軟體更新期間的訊務量。換言之，軟體更新程序可以包括這裏描述的很多相同的修復技術，其中包括二元樹搜尋。

【0146】 第 15 圖示出的是與困擾警報以及單體代碼替換有關的例示呼叫流程圖。雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。該呼叫流程序列可以包括這裏描述的一個或多個步驟。舉例來說，如第 15 圖所示，在 1512，H(e)NB1502 可以執行一個安全引導序列。在完整性檢查階段 1514，H(e)NB1502 有可能在用於操作的代碼中發現完整性故障，由此，H(e)NB1502 的 TrE 不會提供用於 SeGW1504 驗證的私鑰。然而，TrE 有可能認定 H(e)NB1502 通過了 H(e)MS1506 操作。例如，H(e)NB1502 能夠向 H(e)MS1506 發送警報、及/或可以將用於 H(e)MS1506 驗證的私鑰提供給 H(e)NB1502 能夠實施的程序。在 1516，H(e)MS1506 可

以與 H(e)NB1502 建立 IP 連接（例如 SSL/TLS 啓動）。在 1518，H(e)NB1502 可以向 H(e)MS1506 警告完整性故障。例如，H(e)MS1506 可以從 H(e)NB1502 接收困擾警報，並且在 1520 向軟體修復實體 1510 發送代碼修復請求（例如用於重新載入或更新）。在 1522，軟體修復實體 1510 可以執行軟體建構處理。在 1524，軟體修復實體 1510 可以向 H(e)MS1506 提供單體元件替換。例如，軟體修復實體 1510 可以向 H(e)MS1506 提供一個單體修復映射。H(e)MS1506 可以與 H(e)NB1502 建立安全連接。例如，在 1526，H(e)MS1506 可以與 H(e)NB1502 建立安全的 IP 連接（例如經由 SSL/TLS 啓動）。該 H(e)NB1502 和 H(e)MS1506 可以執行驗證來允許用於修復 H(e)NB1502 的軟體/韌體下載。在 1528，H(e)MS1506 可以更新 H(e)NB1502 的軟體/韌體、並且可以重新引導 H(e)NB1502。在 1530，H(e)NB1502 可以重新引導及/或重新啓動完整性檢查。

【0147】 第 16 圖示出的是與遠端軟體困擾/修復有關的例示呼叫流程圖，其中 H(e)NB1602 向 H(e)MS1606 告知困擾。該呼叫流程序列可以包括這裏描述的一個或多個步驟。此外，雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。如第 16 圖所示，在 1612，H(e)NB1602 可以執行一個安全引導序列。在 1614 的完整性檢查階段期間，H(e)NB1602 的 TrE 有可能在用於正常操作的代碼中發現了故障，由此，H(e)NB1602 的 TrE 不會提供用於 SeGW1604 驗證的私鑰。然而，TrE 有可能認定 H(e)NB1602 能夠安全地連接到 H(e)MS1606，因此，TrE 可以將用於 H(e)MS1606 驗證的私鑰提供給 H(e)NB1602 能夠實施的程序。H(e)NB1602 不能（或者在一些故障中不能）嘗試與 SeGW1604 進行驗證。在 1616，H(e)NB1602 可以與 H(e)MS1606 建立 IP 連接（例如安全的 SSL/TLS 會話）。

在 1618，H(e)NB1602 可以向 H(e)MS1606 警告 H(e)NB1602 的完整性檢查狀態（例如完整性故障）。例如，H(e)MS1606 可以藉由驗證或是藉由對帶有 TrE 簽名的完整性狀態酬載資訊的簽名核實來核實 H(e)NB1602 的完整性資訊的真實性。如果完整性檢查狀態表明在 H(e)NB1602 上存在完整性故障，那麼 H(e)MS1606 可以在 1620 確定用於所指示的故障的軟體修復。該軟體修復可以包括更進一步地詢問完整性故障。例如，在 1622，H(e)MS1606 可以診斷及/或詢問 H(e)NB1602。該 H(e)MS1606 可以詳細確定故障原因（例如位置），並且在 1624，H(e)MS1606 可以向軟體修復實體 1610 發送用於重新載入或更新的代碼修復請求。在 1626，軟體修復實體 1610 可以執行軟體建構，並且向 H(e)MS1606 發送軟體修復資訊。例如，該軟體修復資訊可以包括修復映射。在 1630，H(e)MS1606 可以與 H(e)NB1602 建立安全連接（例如經由 IP 連接）。H(e)NB1602 和 H(e)MS1606 可以進行驗證來允許用於修復 H(e)NB1602 的軟體/韌體下載。在 1632，H(e)MS1606 可以下載 H(e)NB1602 的軟體/韌體、及/或重新啓動 H(e)NB1602。在 1634，H(e)NB1602 可以執行安全的引導序列及/或重新啓動完整性檢查處理。在 1636 的完整性檢查階段期間，H(e)NB1602 的 TrE 有可能發現完整性檢查通過了用於 SeGW1604 的操作，並且可以提供用於 SeGW1604 驗證的私鑰。在 1638，H(e)NB1602 和 SeGW1604 可以相互驗證，並且在 1640，SeGW1604 可以向 H(e)NB1602 指示驗證成功。

【0148】 第 17 圖示出的是與結合 SeGW 驗證嘗試的遠端軟體困擾/修復有關的例示呼叫流程圖。該呼叫流程序列可以包括這裏描述的一個或多個步驟。此外，雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。如第 17 圖所示，在 1712，H(e)NB1702 可以執行安全引

導序列。在 1714 的完整性檢查階段期間，H(e)NB1702 有可能在用於 SeGW1704 操作的代碼中發現完整性故障，由此，H(e)NB1702 的 TrE 不會提供用於 SeGW1704 驗證的私鑰。然而，TrE 有可能認定 H(e)NB1702 能夠安全連接到 H(e)MS1706，並且可以將用於 H(e)MS1706 驗證的一個或多個私鑰提供給 H(e)NB1702 能夠實施的程序。例如，在 1716，H(e)NB1702 可以藉由使用 IKEv2 協定來嘗試向 SeGW1704 進行驗證，但是有可能會失敗（例如因爲私有驗證密鑰不可用）。在 1718，H(e)NB1702 可被提供一個表明與 SeGW1704 的驗證已經失敗的指示。在 1720，H(e)NB1702 可以與 H(e)MS1706 建立安全的 IP 連接（例如經由 SSL/TLS 啓動）。例如，該安全的 IP 連接可以基於 H(e)NB1702 與 SeGW1704 之間的失敗的驗證嘗試來建立。在 1722，H(e)NB1702 可以向 H(e)MS1706 警告 H(e)NB1702 的完整性檢查狀態（例如完整性成功或失敗）。H(e)MS1706 可以藉由驗證或者藉由對帶有 TrE 簽名的完整性狀態酬載資訊執行簽名核實來核實 H(e)NB1702 的完整性資訊的真實性。如果完整性檢查狀態指示在 H(e)NB1702 上存在元件的完整性故障，那麼在 1724，H(e)MS1706 可以確定用於所指示的故障的軟體修復。該軟體修復可以包括更進一步地詢問完整性故障。例如，在 1726，H(e)MS1706 可以診斷及/或詢問 H(e)NB1702。該 H(e)MS1706 可以詳細確定故障原因、並且在 1728 向軟體修復實體 1710 發送代碼修復請求（例如用於重新載入或更新）。軟體修復實體 1710 可以在 1730 執行軟體建構、並且在 1732 向 H(e)MS1706 提供軟體修復（例如修復映射）。在 1734，H(e)MS1706 可以與 H(e)NB1702 建立安全的 IP 連接(例如 SSL/TLS 啓動)。H(e)NB1702 和 H(e)MS1706 可以進行驗證來允許用於修復 H(e)NB1702 的軟體/韌體下載。在 1736，H(e)MS1706 可以下載 H(e)NB1702 的軟體/韌體、

並且重新啓動 H(e)NB1702。在 1738，H(e)NB1702 可以執行安全引導序列及/或重新啓動完整性檢查。在 1740 的完整性檢查階段期間，H(e)NB1702 可以發現通過了完整性檢查、並且提供用於 SeGW1704 驗證的私鑰。在 1742，H(e)NB1702 和 SeGW1704 可以相互驗證，並且在 1744，SeGW1704 可以指示驗證成功。

【0149】 第 18A 圖示出的是與遠端軟體困擾/修復有關的例示呼叫流程圖，其中網路可以禁止經由 SeGW 進行驗證。該呼叫流程序列可以包括這裏描述的一個或多個步驟。此外，雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。如第 18A 圖所示，在 1812，H(e)NB1802 可以執行安全的引導序列。在 1814 的完整性檢查階段期間，H(e)NB1802 可能發現用於操作的代碼中的故障，因此，H(e)NB1802 的 TrE 不會提供用於 SeGW1804 驗證的私鑰。然而，TrE 有可能認定 H(e)NB1802 能夠安全連接到 H(e)MS1806，由此將用於 H(e)MS1806 驗證的一個或多個密鑰提供給 H(e)NB1802 能夠實施的程序。在 1816，H(e)NB1802 可以嘗試向 SeGW1804 進行驗證（例如使用 IKEv2 協定），但是有可能失敗（例如因爲私鑰不可用）。H(e)NB1802 可以在驗證嘗試期間提供關於 H(e)NB1802 的完整性且帶有 TrE 簽名的資訊。在 1818，SeGW1804 可以將完整性資訊（例如故障報告）轉發給網路驗證實體 1808。網路驗證實體 1808 可以基於其接收的資訊來確定禁止一些通過 SeGW1804 的 H(e)NB1802 的訊務、並且可以在 1820 發送表明將一些或所有 H(e)NB1802 的訊務限制到於 H(e)MS1806 的細粒度存取決定。在 1822a，SeGW1804 可以發送一個關於驗證失敗的指示。在 1824，出於修復目的，網路驗證實體 1808 可以向 H(e)MS1806 發送 H(e)NB1802 的完整性資訊。在 1826，H(e)MS1806 可以與 H(e)NB1802 建

立安全 IP 連接(例如經由 SSL/TLS 啓動)。在 1828，舉例來說，H(e)MS1806 可以基於驗證失敗而確定執行軟體修復。在 1830，H(e)NB1802 和 H(e)MS1806 可以進行驗證來允許 H(e)MS1806 實施的診斷和詢問。在 1832，H(e)MS1806 可以詳細確定故障原因、並且向軟體修復實體 1810 發送代碼修復請求（例如用於重新載入或更新）。在 1834，軟體修復實體 810 可以執行軟體建構，以便爲 H(e)NB1802 建構替換軟體元件（或是其一部分）。在 1836，軟體修復實體 1810 可以向 H(e)MS1806 提供軟體修復資訊（例如修復映射）。在 1838，H(e)MS1806 可以與 H(e)NB1802 建立安全的 IP 連接（例如經由 SSL/TLS 啓動）。H(e)NB1802 和 H(e)MS1806 可以進行驗證來允許用於修復 H(e)NB1802 的軟體/韌體下載。在 1840，H(e)MS1806 可以下載 H(e)NB1802 的軟體/韌體。在 1842，H(e)NB1802 可以重新引導及/或載入並運行所下載的代碼。

【0150】 第 18B 圖示出的是涉及與即時受限存取及精細存取控制結合的遠端軟體困擾/修復的例示呼叫流程圖。雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。第 18B 圖的呼叫流程序列可以包括許多步驟，這些步驟與第 18A 圖示出的呼叫流程是相同或相似。然而如第 18B 圖所示，H(e)NB1802 與 SeGW1804 驗證可以成功，但是 SeGW1804 有可能限制存取 H(e)NB1802。例如，在 1814 的完整性檢查階段期間，H(e)NB1802 可能發現用於操作的代碼中的故障，因此，H(e)NB1802 的 TrE 不會提供用於 SeGW1804 驗證的私鑰。然而，TrE 有可能認定 H(e)NB1802 能夠安全連接到 H(e)MS1806，由此將用於 H(e)MS1806 驗證的一個或多個私鑰提供給 H(e)NB1802 能夠實施的程序。在 1816，H(e)NB1802 可以嘗試向 SeGW1804 進行驗證（例如使用 IKEv2 協定）。H(e)NB1802 可

以在驗證嘗試期間提供關於 H(e)NB1802 的完整性且帶有 TrE 簽名的資訊。在 1818，SeGW1804 可以將完整性資訊轉發給網路驗證實體 1808。網路驗證實體 1808 可以基於接收到的資訊來決定驗證 H(e)NB1802 的存取，並且可以將此發送給 SeGW1804。SeGW1804 可以以來自網路驗證實體 1808 的資訊爲基礎來驗證 H(e)NB1802，但是有可能限制 H(e)NB1802 的存取。在 1822b，SeGW1804 可以向 H(e)NB1802 發送表明驗證成功但是 SeGW1804 存取受限的指示。在第 18B 圖的協定流程中示出的剩餘步驟與第 18A 圖的協定中示出的步驟可以是相同或相似。

【0151】 第 19 圖示出的是涉及與 SeGW 存取結合的 H(e)NB 軟體元件修復的例示呼叫流程圖。該呼叫流程序列可以包括這裏描述的一個或多個步驟。此外，雖然該呼叫流程是用 H(e)NB 描述的，但是其他網路裝置也是可以使用的。如第 19 圖所示，在 1912，H(e)NB1902 可以執行安全引導序列。在 1914 的完整性檢查階段期間，H(e)NB1902 未能發現裝置代碼中的故障，但是有可能在映射中發現了故障、遺漏元件或配置缺失。H(e)NB1902 的 TrE 可以提供用於 SeGW1904 驗證的私鑰。例如，在 1916，H(e)NB1902 可以向 SeGW1904 發送包含該私鑰的狀態報告（例如使用 IKE）。在 1918，SeGW1904 可以將完整性資訊轉發給網路驗證實體 1908。網路驗證實體 1908 可以基於接收到的資訊來決定驗證 H(e)NB1902 的存取，並且可以將此發送給 SeGW1904。舉例來說，在 1920，網路驗證實體 1908 可以根據操作者策略而向 SeGW1904 發送細粒度的存取決定。基於網路驗證資訊，SeGW1904 可以驗證 H(e)NB1902、及/或根據操作者策略來設定存取許可。在 1922，SeGW1904 可以向 H(e)NB1902 發送驗證成功的指示。在 1924，網路驗證實體 1908 可以向 H(e)MS1906 發送 H(e)NB 完整性資訊。

例如，該完整性資訊可以是出於重新配置的目的而被發送的。在 1926，H(e)MS1906 可以確定可用於修復故障的修復資訊（例如軟體/參數），並且可以在 1928 向軟體修復實體 1910 發送修復請求（例如用於重新載入或更新）。在 1930，軟體修復實體 1910 可以執行軟體建構，以便爲 H(e)NB1802 建構替換軟體元件（例如，或其一部分）。在 1932，軟體修復實體 1910 可以向 H(e)MS1906 提供修復資訊（例如修復映射及/或軟體/配置更新）。在 1934，H(e)MS1906 可以將修復資訊轉發給 SeGW1904。在 1936，SeGW1904 和 H(e)NB1902 可以執行驗證並建立安全的 IP 連接（例如使用 IKEv2 或 IPsec）。在 1938，SeGW1904 可以將修復資訊（例如修復映射或軟體/韌體更新）下載到 H(e)NB1902。舉例來說，SeGW1904 可以發送關於故障的非重要軟體/參數的更新（例如 IKE 及/或 IPsec 更新）。

【0152】 裝置有可能同時具有舊有和先進能力。用於舊有能力的網路服務通常是可用的。用於先進能力的網路服務則有可能會很稀少及/或沒有得到全面支援。爲了減輕部署問題，操作者可以平衡舊有能力，以緩慢進入到先進能力。這種平衡可以採用這裏描述的方式使用。例如，裝置可以在某個位置作爲舊有裝置連結於網路。網路可以驗證裝置，並且在其訂閱中認定該裝置可能具有先進能力及/或能夠安全地支援先進能力。如果用於該位置的網路支援先進能力，那麼網路管理實體可以爲該裝置存取點提供針對更新伺服器的細粒度存取。裝置可以經由舊有存取點來存取更新伺服器。在一些實施方式中，裝置訂閱可以限制對高階特徵而不是舊有服務的存取，因此，存取點通常有可能限制裝置對於更新伺服器而不是舊有網路的存取。該更新伺服器和裝置可以相互驗證。更新伺服器可以（例如經由驗證隱性或顯性地）驗證裝置的先進能力，及/或爲裝置提供存取證書、配

置資訊、存取點位址及/或代碼，以允許裝置作爲新類型裝置來直接重連。裝置可能具有產生用於網路存取驗證的共享或非對稱密鑰對的能力。網路可以使用新的裝置證書來更新裝置訂閱資料庫。裝置可具有將用於先進網路位置的存取證書引入受保護區域的能力。線上證書產生可以允許未來針對先進網路且經過預先驗證的連接。網路可以向先進網路的存取點（這些支援先進能力）告知具有某些證書的裝置可連結在先進網路上。裝置可以使用經過更新的證書來存取先進網路。先進網路實體則可以將裝置作爲先進裝置來驗證。

【0153】 用於管理驗證的程序至少具有兩個階段。一個可以是用於配置，另一個則是用於修復。對於配置來說，網路管理實體可以驗證中繼節點作爲確信安裝用於與操作者的核心網路的後續驗證程序的操作者證書的裝置的能力。該中繼點可以經由使用了平臺驗證的自發平臺驗證手段來向網路實體提供隱性證明。管理實體可以經由驗證該裝置及/或核實 RN 製造者證書來瞭解 RN 完整性沒有受損（因爲自發驗證可在裝置完整性的內部核實成功的時候放出私有驗證密鑰）。

【0154】 對於修復來說，由於某些不重要的故障已經導致整個裝置的完整性檢查失敗，因此，RN 可以與管理實體執行遠端修復程序。在這種情況下，如果 RN 的管理能力無損，那麼 RN 可以向管理實體發送用於驗證目的的管理能力證書，而不是整個裝置的完整性證書。網路管理實體可以驗證裝置並核實證書。一旦成功，則網路管理實體可以執行遠端程序來自舉中繼點的能力。

【0155】 在初始範圍受限的情況下，可使用後一個程序來自舉 RN 的能力。在這種情況下，第一個證書可以代表與管理實體一起執行基本操作

的能力。第二個證書可以代表與管理實體一起執行更廣泛的操作的能力。在這種情況下，中繼點不能以功能提升的範圍來偵測完整性故障。完整性檢查範圍還可以藉由提供用以適應增強功能的附加更新策略來提升。這樣一來，裝置的能力可以與完整性檢查的程度一起增長。

【0156】 該技術通常可以應用於安全閘道驗證。在針對核心網路的閘道驗證中可以使用代表裝置受限範圍的證書，以使網路能在驗證期間確定驗證許可權。閘道（例如 H(e)NB 驗證中的 SeGW 或是用於 RN 驗證的 DeNB）可以驗證裝置並核實證書。基於證書資訊以及對於特定裝置身份的成功驗證，閘道可以限制那些出於修復或註冊目的而對網路管理實體進行的存取。一旦已成功配置、更新及/或修復了中繼點，則可以使驗證密鑰可用於基於驗證的增強。

【0157】 第 20 圖示出的是有關中繼節點能力自舉的例示呼叫流程圖。該呼叫流程序列可以包括這裏描述的一個或多個步驟。舉例來說，如第 20 圖所示，在 2014，中繼節點（RN）2002 可以執行安全引導序列。在 2016，RN2002 可以建立安全環境及/或執行自發驗證。在自發驗證期間，RN2002 沒能發現故障。在 2018，RN2002 可以例如作爲 UE 以經由 eNB 2004 連結於網路，例如連結在 MME/HSS 2012 上。在 2020，MME 2012 可以將 RN2002 的受限存取分派給註冊伺服器 2008。如第 20 圖所示，該受限存取可以是經由 eNB 2004 分派的。RN2002 和註冊伺服器 2008 可以相互驗證。在 2022，RN2002 可以向註冊伺服器 2008 發送註冊請求。在 2024，註冊伺服器可以驗證 RN2002、配置 RN2002 及/或向 RN2002 發行證書。註冊伺服器 2008 可以經由 RN2002 的私有註冊伺服器驗證密鑰的使用的 RN2002 安全環境釋放來隱性驗證 RN2002、或者註冊伺服器 2008 也可以藉由詢問 RN

報告來驗證 RN2002。註冊伺服器 2008 可以配置用於 DeNB 2006 連結的已驗證 RN2002，並且可以發行證書。註冊伺服器 2008 可以更新裝置上的 RN 策略，以繞過未來的重新引導中的註冊步驟，以及將註冊資訊包含在自發驗證處理中（例如添加涵蓋了註冊資訊的 TRV）。在 RN2002 上可以安裝新的私鑰，或者可以在此階段啓動新的私鑰。RN2002 可以具有密鑰產生能力，在這種情況下，在 RN2002 上可以產生密鑰對。RN2002 可以在其安全環境中安裝私鑰，並且可以將這個密鑰版本綁定到註冊配置以及低階安全引導階段。在 2026，註冊伺服器 2008 可以向中繼節點 2002 指示註冊已經完成。在 2028，RN2002 可以作爲 RN 以經由 DeNB 2006 連結於網路。在 2030，MME 2012 可以經由 DeNB 2006 來將 RN2002 的受限存取指定給配置伺服器 2010。在 2032，RN2002 可以向配置伺服器 2010 發送 RN 配置請求。在 2034，配置伺服器 2010 可以驗證 RN2002、配置 RN2002 及/或向 RN2002 發行證書。例如，配置伺服器 2010 可以配置用於操作的已驗證 RN2002，並且可以發行證書。配置伺服器 2010 可以更新裝置上的 RN 策略，以繞過未來的重新引導的配置步驟，以及將配置資訊包含在自發驗證處理中（例如添加涵蓋了配置資訊的 TRV）。在此階段可以安裝或者啓動用於 DeNB 2006 驗證的新私鑰。在 2036，配置伺服器 2010 可以向 RN2002 指示配置完成。在 2038，RN2002 可以與 DeNB 2006 發起 S1 建立。在 2040，RN2002 可以與 DeNB2006 發起 X2 建立。在 2042，RN2002 可以作爲中繼節點操作。

【0158】 在 2044，在 RN2002 上有可能發生重置。例如，此重置可由網路、裝置或停電引發的。在 2046，RN2002 可以執行安全的引導序列。在 2048，在建立安全環境及/或自發驗證期間，RN2002 未能發現故障。由

於註冊伺服器 2008 的資訊及/或配置伺服器 2010 的資訊可以包含在 2048 的自發驗證過程中，因此，RN2002 可以繼續在 2050 和 2052 分別建立 S1 和 X2 介面，而不需要與伺服器耦接。在 2054，RN2002 也可以作爲 RN 操作。如果註冊伺服器資訊或配置伺服器資訊出現故障，那麼策略可以或者不可以允許私有驗證密鑰釋放或是後續網路處理的執行，直至重新配置。

【0159】 第 21 圖示出的是與使用了已驗證管理能力的中繼節點修復有關的例示呼叫流程圖。該呼叫流程序列可以包括這裏描述的一個或多個步驟。舉例來說，如第 21 圖所示，在 2114，中繼節點（RN）2102 可以執行安全引導序列。在 2116，RN2102 可以建立安全環境及/或執行自發驗證。在 2116 的自發驗證期間，RN2102 可以發現裝置的非重要元件的故障。在 2118，RN2102 可以作爲 UE 以經由 eNB 2104 連結於網路（例如 MME/HSS 2112）。在 2120，MME 2112 可以將 RN2102 的受限存取分派給註冊伺服器 2106 及/或修復伺服器 2110。例如，MME 2112 可以經由 eNB 2104 來指定受限存取。RN2102 和修復伺服器 2110 可以相互驗證。在 2122，RN2102 可以向修復伺服器 2110 發送警報（例如修復請求）。在 2124，修復伺服器 2110 可以隱性地經由對 RN2102 的私有修復伺服器驗證密鑰的使用的 RN2102 安全環境釋放來驗證 RN 管理能力，及/或修復伺服器 2110 可以藉由詢問一個或多個 RN2102 完整性狀態報告來驗證 RN2102。在 2126，RN2102 和修復伺服器 2110 可以（可選地）執行關於 RN2102 的詢問。在 2128，修復伺服器 2110 可以修復（例如重新配置，修復或重新編程）RN2102，並且在 2130 向 RN2102 發送用於修復故障的修復資訊。

【0160】 在 2132，修復伺服器 2110 可以遠端命令 RN2102 安全地重新引導，或者由於 RN2102 已經執行了通電階段中的第一階段、並且用於平

臺驗證而不僅僅例如是管理驗證的裝置完整性檢查現在取得成功，RN2102 可以直接前進至 RN2102 通電序列中的下一個步驟。例如，在 2134，RN2102 可以建立安全環境及/或執行自發驗證。在 2136，RN2102 可以作爲 UE 以經由 eNB 2104 連結於網路（例如 MME/HSS 2112）。在 2138，MME 2112 可以將 RN2102 的受限存取指定給註冊伺服器 2106 及/或修復伺服器 2110。在 2140，RN2102 可以向註冊伺服器 2106 產生註冊請求。在 2142，註冊伺服器 2106 可以驗證 RN2102、配置 RN2102 及/或向 RN2102 發行證書。在 2144，該註冊伺服器 2106 可以向 RN2102 指示註冊完成。

【0161】 這裏描述的用於完整性檢查、報告和修復的程序、系統和手段未必限於這裏描述的軟體故障、TR-069，軟體修復、H(e)NB 等等。更進一步，所描述的動作是例示性的。應該理解的是，其他動作也是可以使用的，在不使用的情況下是可以省略的，及/或操作是可以添加的。

【0162】 在一些實施方式中，故障未必是針對軟體的，而是針對裝置上的配置資料或其他某些可量度的元件。在該實施方式中，舉例來說，管理實體接收的更新未必來自軟體修復實體，而是來自網路裝置配置資料庫。並且不是所有故障情景都可以使用詢問程序。在這些情況中，作爲來自裝置的警報或報告所發送的資訊起初足以確定故障原因，或者至少足以確定可以執行的某種動作，藉以管理實體可以在沒有詢問的情況下發起修復程序。舉個例子，管理實體可以從類似裝置的先前故障中識別出故障的元件量度，由此立即向裝置提交更新。詢問與更新之間的時間和訊務負載的折衷有可能是因爲很小的元件造成的，並且這種折衷可以觸發整個元件更新。

【0163】 在以下示例中描述了裝置架構和修復更新程序。該例示裝置

架構和修復更新程序可以與複雜度和資源有限的小型裝置一起使用。在這裏描述的是與本示例相關聯的限制。例如，就開發及/或部署生命週期以及其操作而言，裝置的應用代碼庫和可信代碼庫可以是獨立的。這兩個代碼庫可以是由獨立的各方開發及/或部署的。可以提供裝置的生產功能的裝置應用代碼庫可以作爲單一代碼和資料塊而被部署到裝置的非揮發記憶體的某個部分。在修復過程中可以最低限度地涉及應用代碼庫，及/或在完整性驗證中可不所述應用代碼庫。服務週期（例如裝置代碼庫一部分的更新之間可供裝置應用使用的可使用時間）有可能很長。舉例來說，這意味著不能在任何時間不加區別地強制執行用於修復的重新引導。裝置的正常操作不能因爲修復或裝置更新程序而被中斷。用於完整性驗證和修復的通信可以在裝置啓動的較早階段進行，在此期間可以應用關於裝置內部資源使用和通信頻寬的嚴格限制。從可以載入並且隨後逐一啓動元件（例如程式和資料）的典型的引導循環的意義上講，複雜的系統啓動未必是存在的。

【0164】 例示的系統模型可以被描述爲是在考慮了上述限制的情況下將系統拆分成 TrE 和正常元件的一般形式。系統架構的功能元件可以包括下列各項中的一項或多項：

【0165】 RoT（可信根），其可以是裝置完整性驗證在信任鏈中依靠的不變要素；

【0166】 SEE（安全的執行環境），其可以是對可執行代碼和資料進行硬體及/或軟體保護並且與系統的剩餘部分隔離的特殊的執行環境。一種可能的實現方式可以是處理器或是處理器中的單一核心的安全執行模式。對於 SEE 的限制可以包括對運行時間記憶體以及可用的（專爲 SEE 所有）非揮發記憶體（NVS）的限制；

【0167】 通信 IF（通信介面）元件，其可以將基本通信能力暴露給 SEE 及/或 NEE；及/或

【0168】 NEE（正常執行環境），其可以是裝置中的應用代碼的執行環境，其中舉例來說，該應用代碼可以是不屬於 TrE 的代碼。NEE 可以具有與 SEE 能力介面連接(例如與通信 IF 介面連接)的某些介面以重新使用此通信能力的介面。

【0169】 這些功能元件可以供包含裝置的能力和元件的若干代碼庫使用。該代碼庫可以分成 TrECB（TrE 代碼庫）和 DACB（裝置應用代碼庫）。TrECB 可被分配給 SEE，而 DACB 則可以被分配給 NEE。如果 DACB 元件將要存取 TrE 的能力，那麼該存取可以經由所述及的 NEE 與 SEE 之間的介面執行。在諸如安全啓動之後之類的從 SEE 到 NEE 的運行時間是沒有執行控制的，反之亦然。TrECB 和 DACB 可以儲存在 NVS 的單獨的部分。

【0170】 第 22 圖示出的是具有功能元件 2202（左手側）和代碼/資料儲存元件 2204（右手側）的例示系統。功能元件 2202 可以包括 NEE 2206 和 SEE 2208。SEE 2208 可以包括通信介面 2210 及/或 ROT 2212。代碼/資料儲存元件 2204 可以包括 NVS 元件。NVS 元件 TRV_tmp 2214 可以包括與 NEE 2206 相關聯的 TRV。NVS 元件 DACB 2216 可以包括 DACB。NVS 元件 TRV NVS 2218 可以包括與 SEE 2208 相關聯的 TRV。NVS 元件 TrECB NVS 2220 可以包括 TrECB。不同的安全措施可以單獨應用於 NVS 元件。這裏的箭頭可以指示第 22 圖所示實體之間的讀/寫存取。TrECB NVS 2220 可以提供不同的能力，例如完整性驗證能力（IVC）、裝置的一般通信能力（DGC）、後降/困擾能力（FB/DC）以及修復能力（RC）。在這裏對照第 22 圖和第 23 圖論述了這些能力。

【0171】 如第 22 圖所示，NEE 2206 可以與 SEE 2208 通信（例如從 SEE 2208 讀取及/或寫入 SEE 2208）。SEE 2208 可以使用通信介面 2210 來進行通信。該 SEE 2208 可以使用 ROT 2212 來與代碼/資料儲存元件一起執行完整性驗證。NEE 2206 可以寫入 NVS 元件 2214，以及讀取 NVS 元件 2216。SEE 2208 可以讀取 NVS 元件 2214。該 SEE 2208 還可以讀取和寫入 NVS 元件 2216、2218 和 2220。

【0172】 第 23 圖示出的是引導序列的階段以及在每個階段實施的不同實體間的交互作用的例示流程圖。如第 23 圖所示，在引導序列中可以實施 NEE 2206 和 SEE 2208。SEE 2208 可用於引導序列的第一和第二階段。第一階段可以合併 ROT 2212。第二階段可以合併 TrECB NVS 2220，該 TrECB NVS 2220 可以包括完整性驗證能力（IVC）2318、裝置的一般通信能力（DGC）2314、後降/困擾能力（FB/DC）2320、修復能力（RC）2324 及/或 TRV2326。IVC2318 可被指定獲取元件量度以及將元件量度與 TRV2326 之類的 TRV 中包含的參考值進行比較的任務。DGC2314 可以向 SEE 2208 提供基本的通信功能（該功能轉而可以暴露於 NEE 2206）。該 DGC2314 可用於 FB/DC2320 和 RC2324 實施的修復及/或困擾指示。DGC2314 同樣可以經由介面暴露於 DAC2322。FB/DC2320 可以在滿足某些條件的情況下被啓動，以執行相關功能，即分別使用後降代碼庫來替換 DACB 2216，由此向網路或裝置用戶指示困擾狀態。RC2324 可以是被指定了關於代碼庫的計畫變更及/或校正的任務的機構。RC2324 也可以是 TRV2326 的管理器，並且 RC2324 能檢查 TRV2326 的真實性。

【0173】 NEE 2206 可用於引導序列的第三階段。第三階段可以合併 DACB 2216，其中該 DACB 包括修復應用 IF（RAIF）2316 及/或裝置應用

能力（DAC）2322。RAIF 2316 可以是用於來自網路的到來的新 TRV 的傳遞介面。RAIF 2316 可以識別到來的通信中的 TRV，並且將其儲存在 TRV 臨時非揮發記憶體中。DAC2322 可以實現裝置的應用專用功能。如果 DAC 想要使用來自通信 IF 的通信能力，那麼對其進行的存取可以經由特定的 NEE-SEE IF 來傳達。

【0174】 TRV2326 可以儲存在系統中的兩個不同位置。TRV_tmp 2214 可以是用於 RAIF 2316 接收的新 TRV 的臨時記憶體，例如，TRV_tmp 2214 可從 NEE 2206 被寫入。TRV_tmp 可從 SEE 2208 被讀取，並且 RC2324 可以從中讀取新的 TRV，以及在對其進行了驗證之後將其置入 TRV NVS 2218。

【0175】 第 23 圖所示的啓動序列可以與簡化系統架構中帶有完整性檢查的正常啓動有關，例如，沒有出現有可能需要困擾/後降或修復動作的故障狀況的啓動處理。在安全啓動中的第一個階段，RoT 2212 可被啓動。與先前描述的安全啓動的第二階段不同，RoT 2212 可不核實並且啓動隨後可對已載入和啓動的元件執行進一步的完整性檢查的可信根載入器。這種載入器/執行控制器可能不能在簡化的系統架構中使用。取而代之的是，RoT 2212 可以在 TrECB NVS 2220 中檢查 IVC2318 的代碼和資料塊。在該架構中，由於 RoT 2212 不具有讀取 TRV2326 的能力，因此，IVC2318 的代碼有可能是不變的。由此，其可以對照固定的內置（在 RoT 2212 中）參考值來檢查 IVC2318。

【0176】 在一個實施例中，RoT2212 可以使用固定的根證書來檢查 IVC2318 的代碼和資料塊。爲此，TrECB NVS2220 的 IVC2318 部分可以與 TrECB NVS2220 中的後一個 IVC2318 部分上的簽名一起儲存。RoT2212 用

以檢查簽名的密鑰可以處於所述的固定根證書中。藉由下載新的 IVC2318 代碼以及使用相同固定密鑰的新代碼的新簽名，並且將後一個資料儲存在 TrECb NVS2220 中，可以實施 IVC2318 的代碼變化。IVC2318 可以在 SEE 2208 內部執行。IVC2318 可以檢查出 TRV_tmp NVS2214 爲空（這可以是爲簡化系統架構中帶有完整性檢查的正常啓動假設的）。IVC2318 可以從 TRV NVS 2218 中載入用於 DGC2314 的代碼的指定 TRV。

【0177】 IVC2318 可以藉由核實 TRV 參考值以及任何附加資料上的簽名來檢查 TRV2326 中的每一個被載入 TRV 的完整性。該簽名可以處於 TRV 中，而 IVC2318 用以檢查簽名的密鑰則處於 IVC2318 代碼/資料塊中。然後，IVC2318 可以量度從 TrECB NVS 2220 載入到 SEE 2208 的 DGC2314 代碼，並且將該量度與後一個 TRV 中的參考值進行比較。一旦成功，則可以啓動 DGC2314。啓動意味著 DGC2314 可用於執行，其中舉例來說，該 DGC 是在假設 SEE 2208 的處理器和 NEE2206 的處理器在檢查 NEE2206 代碼時會遵守在DGC2314所處的SEE2304的運行時間記憶體部分上設定的旗標“executable（可執行）”情況下藉由設定該旗標來執行的。

【0178】 IVC2318 可以從 TRV NVS2218 中載入爲 RAIF2316 的代碼指定的 TRV。IVC2318 對從 DACB NVS2216 載入到 NEE 2206 的 RAIF2316 的代碼進行量度，並且將該量度與後一個 TRV 中包含的參考值進行比較。一旦成功，則可以啓動 RAIF2316。

【0179】 IVC2318 可以載入與預定序列中的 DACB2216 的一些部分相關聯的每一個 TRV。IVC2318 可以量度由所載入的 TRV 指定並從 DACB NVS2216 載入到 NEE2306 的 DAC2322 的代碼和資料的某些部分，並且將該量度與後一個 TRV 中包含的參考值進行比較。

【0180】 當執行 DACB2216 中的檢查時（例如藉由窮舉可用於 DACB2216 代碼和資料的 TRV 序列），IVC2318 可以啓動 DAC2322，並且將執行傳遞到 NEE2206 的處理器（或者在 SEE 2208 和 NEE2206 的處理器可以同時運行的時候啓動該處理器）。如果在啓動程序中沒有出現特殊狀況（例如完整性檢查故障），那麼可以既不檢查也不啓動 FB/DC2320 和 RC2324 的代碼和資料塊。

【0181】 與諸如安全引導之類的更複雜系統中的安全啓動的差別可以包括：IVC2318 可以由 TRV 資料所驅動。換言之，TRV 可以具有關於不同代碼庫的哪些代碼段和資料將被檢查的資訊。TRV2326 可以由 IVC2318 依序讀取，其中該 IVC2318 可以對其進行評估，以發現應用了 TRV 參考完整性值的代碼段和資料，以及讀取及/或量度此資料，並且將經過校對的量度與參考值進行比較。

【0182】 由於單一 TRV 參考值可以對應於代碼庫中的多個代碼段和資料，因此，TRV 可以包括映射，例如關於代碼庫中的這些段的位置和長度的指示符，以及如何將這些段的量度合併爲混合量度值的規定。第 24A 和 24B 圖示出了將 TRV 映射至代碼庫中的代碼段及/或資料的例示實施方式。

【0183】 第 24A 圖是顯示了可被線性組合以創建 TRV 的部分量度序列的圖示。如第 24A 圖所示，DACB 的代碼量度 2402、2404、2406、2408 和 2410 可被線性組合，以創建 TRV2412。根據一個例示實施例，代碼量度 2402、2404、2406、2408 和 2410 可以藉由應用散列鏈來組合，其中該散列鏈是用 TCG 規定的可信平臺模組的 TPM 擴展命令實現的。

【0184】 第 24B 圖示出的是使用 Merkle 散列樹來創建 TRV 的值的組

合的圖示。如第 24B 圖所示，DACB 的代碼量度 2416、2418、2420、2422、2424 和 2426 可以使用 Merkle 散列樹來組合，以創建 TRV2414。

【0185】 在執行修復及/或更新的裝置與相應網路實體（例如 H(e)MS）之間的交互詢問程序可以使用這裏描述的 TRV-代碼/資料段映射。這裏描述的這些過程可以是這裏描述的通用裝置詢問程序的特例。

【0186】 每一個代碼段都可被量度，並且該量度可被逐一發送到網路實體，在那裏其會與例如代碼段參考值的順序列表中的相應代碼段參考值比較，其中該 TRV 參考值是先前已經通過諸如散列鏈之類的某種方法而從該列表中計算的。

【0187】 如果經由 Merkle 散列樹偵測到大量代碼段，那麼可以提高效率。這可以採用交互詢問程序以藉由遞減樹的等級來執行。在這裏，TRV 中包含的參考值以及從代碼/資料中取出的量度值均可表示相同二元樹的根（在圖表理論上）。如果它們不匹配，那麼裝置可以將這兩個子節點值發送到網路實體，該網路實體則可以決定哪一個存在故障，例如不與網路已使用以建構 TRV 參考值（其可爲該參考樹的根）的參考樹中的相同節點相匹配的子節點值。網路可以向裝置發送可以聲明哪個（些）分支不匹配的訊息。此程序可以重複進行，直至確定了存在參考（葉片）值不匹配的代碼段、構成量度樹葉片的量度值。

【0188】 回過來參考第 23 圖，在這裏可以執行那些以用於裝置修復的 TrECB 2220 的能力爲基礎的功能和程序。在一個實施例中，計畫代碼更新可以藉由在操作期間更新一個或多個 TRV2326 以及在下一次啓動時執行實際代碼更新來執行。

【0189】 以下涉及的是計畫進行的代碼更新。可以假設裝置已經執行

了這裏描述的啓動處理。例如，RAIF2316 可以經由通信 IF2210 及/或 DGC2314 接收來自 H(e)MS 之類的外部方的新 TRV。RAIF2316 可以將新接收的 TRV 儲存在 TRV_tmp NVS2214 中。在以後的時間，裝置可以重啓。IVC2318 可被執行完整性檢查，並且在這裏描述的 SEE 2208 內部啓動。IVC2318 可以檢查並發現 TRV_tmp NVS2214 非空，並且可以採用這裏描述的方式繼續前進。

【0190】 TRV_tmp2214 可以具有單一新 TRV。在第一個實施方式中，TRV_tmp 中的新 TRV 可以是指 DACB2216 中的代碼及/或資料。在第二個實施方式中，TRV_tmp 中的新 TRV 可以是指 TrECB 2220 中的代碼及/或資料，例如 DGC2314、FB/DC2320 或 RC2324 的代碼/資料。

【0191】 在第一實施方式中，IVC2318 可以採用上述方式來核實 TRV 的真實性。一旦成功，則 IVC2318 可以將新 TRV 儲存在 TRV NVS2218 中。IVC2318 可以刪除 TRV NVS2218 中的一個或多個舊 TRV，其中該舊 TRV 可以視爲被新 TRV 取代。如何確定這些棄用 TRV 可以取決於實施方式。唯一的識別符可以作爲 TRV 中的附加資料的一部分分派給 TRV。舉例來說，本段中描述的處理可被稱爲 TRV 攝入。

【0192】 IVC2318 可以量度從 TrECB 2220 NVS 載入到 SEE2208 的 DGC2314 的代碼，並且將該量度與後一個 TRV 中包含的參考值進行比較。一旦成功，則可以啓動 DGC2314。IVC2318 可以載入及/或核實來自 TRV NVS 的 TRV2326，並且可以爲這其中的每一個的指定代碼段或資料執行 IV；其中舉例來說，該 IV 是以 RAIF2316 爲開始並且前進至 DACB2216 的其他部分。當在 IV 序列中遭遇到新攝入的 TRV 時，在 DACB2216 的代碼和資料的指定部分上執行的 IV 必然失敗（例如，假設新 TRV 具有與被棄

用的一個或多個 TRV 不同的參考值）。

【0193】 IVC2318 可以從 TRV NVS2218 中載入用於 RC 代碼的指定 TRV。然後，IVC2318 可以量度從 TrECB 2220 NVS 載入到 SEE2208 的 DGC2314 代碼，並且可以將該量度與後一個 TRV 中包含的參考值進行比較。一旦成功，則可以啓動 RC。

【0194】 藉由與 H(e)MS 之類的相應網路實體一起實施的詢問程序，RC2324 可以確定諸如導致完整性量度故障的代碼段及/或資料之類的需要更新的代碼段及/或資料，以重新產生新攝入的 TRV 的參考值。舉例來說，該詢問程序可以採用這裏描述的方式執行。

【0195】 借助新的 TRV，裝置也可以接收哪些部分的代碼及/或資料需要替換的詳細資料。這樣做可以避免 RC2324 與網路之間的詢問程序。執行詢問可以將在裝置的正常操作期間下載用於裝置管理及/或修復的資料量減至最小。此外，執行詢問也可以允許裝置“遺漏”某些（一個，新的）TRV 及/或爲其指定的代碼段的某些中間更新的可能性。如果這種後續更新是累積的，那麼其往往會影響有可能在詢問程序中發現的更大數量的代碼段（但是不保證其處於僅限於最後一個 TRV 的更新所指定的代碼段列表，其中在對同一個 TRV 進行一系列更新之後，其可能已經被裝置遺漏）。

【0196】 RC2324 可以下載所確定的代碼段及/或從相應網路實體所確定的資料。根據一個示例，網路實體可以編譯用 TR-069 簽名的資料封包及/或將其發送至裝置。RC2324（或是 IVC2318）可以檢查接收資料的真實性，例如使用新攝入的 TRV 中的簽名證書、用於（例如由 IVC2318）檢查 TRV2326 的根證書或是用於修復目的的專用證書（例如在 RC2324 的代碼/資料庫中）來核實資料包簽名。

【0197】 在驗證了已下載的代碼段及/或資料之後，RC2324 可以將其寫入 DACB 2216 NVS 中的先前確定的片段位置。DGC2314 可以將執行返還給 IVC2318，該 IVC2318 可以在同一個 TRV 上重新開始 IV，舉例來說，該 TRV 可以是 TRV 序列中的新攝入的 TRV。

【0198】 上述程序可以是循環的。這種情況會因爲至少兩個原因中的一個原因而出現。首先，攻擊者可以將不與 TRV 參考值一致的自己的代碼插入更新過程。此外，舉例來說，由於網路側的代碼建構發生故障，TRV 參考值及/或下載的代碼有可能出現偶然的不匹配。在兩種實施方式中，這些狀態都是可以偵測並用信號通告給網路的。這可以由 IVC2318 使用關於 TRV 使用率的重複計數器來實現。爲了實現高保密性，這些計數器可以是藉由對 TRV NVS 的讀取存取而遞增的單調硬體計數器。如果偵測到 IV 在單一 TRV 上重複次數過多（其數量可以取決於策略），那麼 IVC2318 可以檢查並啓動 FB/DC2320、及/或將控制權傳遞給向網路發送一個相符信號的能力。

【0199】 與如上所述的第二實施方式（與參考 TrECB2220 中的代碼及/或資料的 TRV_tmp2214 中的新 TRV 相關）相比，在這裏未必使用第一實施方式（與參考 DACB2216 中的代碼及/或資料的 TRV_tmp2214 中的新的 TRV 相關），這是因爲該更新/修復有可能是爲更新/修復中包含和活動的元件本身請求的。在這種情況下，以下程序中的一個或多個步驟可以被應用。IVC2318 可以攝入新的 TRV，但是可以將相應的舊 TRV 保持在 TRV NVS2218 中。新的 TRV 可以用諸如字串“NEW_DGC_TRV”之類的某個資料旗標來進行標記，以表明其是新的。IVC2318 可以使用舊 TRV 來檢查及/或啓動 RC2324。RC2324 則可以執行 TrECB2220 的某些部分的更新，其

中該更新可以用與第一實施方式中的描述相同的方式使用，但在第二實施方式中，該更新可被寫入 TrECB 2220 NVS。IVC2318 可以使用新 TRV 來檢查 TrECB 2220 的更新部分。一旦成功，則可以從 TRV NVS2218 中刪除舊 TRV，並且可以移除連結於新 TRV 的標記。其中舉例來說，該處理可被延期至裝置下一次重啓之後。

【0200】 完整性檢查的第一種故障狀況有可能會在 RoT2212 檢查 IVC2318 的代碼的時候出現。如果未通過此檢查，則 RoT2212 可以停止系統，並且還可以向用戶發送信號（例如光信號）。

【0201】 根據一個實施例，RoT2212 可具有檢查 FB/DC2320 中的不變的部分（或是完整性受到如在用於 IC 代碼的類似變形中描述的簽名所保護的可變部分）、及/或調用困擾/後降程序的這些受限部分的能力，其中該受限部分可以經由受到自發檢查的這個代碼來得到，例如藉由將該代碼載入到 SEE2208 並且在 SEE2208 中執行該代碼。

【0202】 接下來的可能失敗的完整性檢查可以是關於 DGC2314 及/或 RAIF2316 的完整性檢查。前者可以是指裝置沒有可信賴的通信能力。在這種情況下，IVC2318 可以嘗試核實並啓動 FB/DC2320。FB/DC2320 在某種程度上能夠恢復可信賴的通信，並且能向網路發送困擾信號。如果不能的話，其可以用信號通告用戶並停止系統。如果 RC2324 的 IV 在上述修復程序中發生故障，那麼相同的程序也是可以應用的。

【0203】 在如上所述的第二實施方式中，如果 RAIF2316 的 IV 發生故障，則這可能意味著裝置有可能喪失了接收 TRV 更新的能力。然後，裝置首先可以嘗試如上所述那樣修復該狀況。如果失敗，則 IVC2318 可以核實及/或啓動 FB/DC2320，該 FB/DC2320 轉而可以採取特定操作，例如用某

個預設代碼替換 RAIF2316。

【0204】 從以上描述中可以看出，作爲在 NEE2206 中暴露的代碼的一部分以及正常代碼庫的一部分，RAIF2316 可能是裝置修復中的最薄弱環節。由於在完整性檢查中不會包含 RAIF2316，因此，這種狀況不會直接威脅裝置完整性，但是，其有可能會禁用更新/修復並且由此將裝置保持在棄用（例如故障）狀態，從而爲間接和拒絕服務攻擊開啓方便之門。根據一個實施例，RAIF2316 實現的功能可以作爲 TrECB2220 的一部分來提供，並且是在 SEE2208 中執行的。這樣做可以對系統架構施加提前配置，因爲這可能意味著 SEE2208 的一部分是活動的，並且預備接收新的 TRV。例如，SEE 的這種永久性活動可以在通信 IF2210 和 DGC2314 中實現。

【0205】 儘管以上以特定的組合描述了特徵和元素，但是一個本領域中具有通常知識者將理解，每個特徵或元素可以單獨地或與其它的特徵和元素任意組合地使用。此外，在此描述的方法可實施爲整合在由電腦或處理器執行的電腦可讀媒體中的電腦程式、軟體或韌體。電腦可讀媒體的示例包括電子信號（經由有線或無線連接發送）和電腦可讀儲存媒體。電腦可讀儲存媒體的示例包括但不限制爲唯讀記憶體（ROM）、隨機存取記憶體（RAM）、暫存器、緩衝記憶體、半導體記憶體裝置、諸如內部硬碟和可移式磁片這樣的磁性媒體、磁光媒體和諸如 CD-ROM 盤和數位通用盤（DVD）這樣的光學媒體。與軟體相關聯的處理器可用來實施在 WTRU、UE、終端、基地台、RNC 或任何主電腦中使用的射頻收發器。

【符號說明】

【0206】

2206、NEE	正常執行環境
2208、SEE	安全的執行環境
2212、ROT	不可變硬體可信根
2216、DACB	裝置應用代碼庫
2220、TrECB	TrE 代碼庫
TrE、802	可信執行環境
2314、DGC	一般通信能力
RAIF、2316	修復應用 IF
2210、IF	通信介面
IF	介面
2318、IVC	完整性驗證能力
2320、FB/DC	後降/困擾能力
2322、DAC	裝置應用能力
2324、RC	修復能力
904、2326、2412、2414、TRV	可信參考值
102a、102b、102c、102d、102、WTRU	無線傳輸/接收單元
104、RAN	無線電存取網路
106	核心網路
108、PSTN	公共交換電話網路
100	通信系統
110	網際網路
112	其他網路

114a、114b	基地台
116	空氣介面
118	處理器
120	收發器
122	傳輸/接收元件
124	揚聲器/麥克風
126	鍵盤
128	顯示器/觸控板
130	不可拆卸記憶體
132	可拆卸記憶體
134	電源
136、GPS	全球定位系統碼片組
138	週邊裝置
140a、140b、140c	e 節點 B
142、2012、2112、MME	移動性管理閘道
144	服務閘道
146、PDN	封包資料網路閘道
ROM	唯讀記憶體
302、304、306、402、404	物件檔
308、316、324、410、424、.text	本文區段
310、318、326、.init	啓動區段
312、320、328、412、426、.data	資料區段
314、322、330、414、418、428、.bss 區段	未初始化資料區段
.bss	未初始化資料

ELF	可執行和鏈結格式
332	本文分段
334	資料分段
336	未初始化資料分段
338、406	可執行映射
408、416、420、422	元件檔區段
502	元件 TRV 區段
602	可信任域
604	高階功能
606	中間功能
608	可信環境核心功能
610、612、614、616、618、928	功能
620、622、624、626、902、1402	元件
702	功能至元件映射區段
804、806、808、810	檢查、載入及/或執行能力
812、814、816、818、820	策略
906、912、914	表
908	策略管理實體
912	元件位址
914	完整性檢查
918	通過/未通過
920	位址
922、924	元件 ID
1004、1202	裝置

1006	裝置報告
1008	報告
1010	網路平臺驗證實體
1012	裝置管理伺服器
1016	存取決定
1018	詢問
1024	SW 更新
SW	軟體
1014	功能至元件映射資訊
1020	請求軟體更新
1022	代碼建構釋放實體
1102、1502	H(e)NB
1104、1506、1606、1706、1806、1906	H(e)MS
1204	網路管理實體
1302	大型單體元件
1304、1310、1404	整體量度值
1308	分段
1406、1408、1410、1412、1414、1416	子區段
1504、1604、1704、1804、1904	SeGW
1508、1608、1708、1808、1908	網路檢驗實體
1510、1610、1710、1810、1910	軟體修復實體
1514、1614、1636、1714、1814、1914	完整性檢查
1520、1624、1728、1832	代碼修復請求
1522、1626、1730、1834、1930	軟體建構

1524	單體元件替換
1628、1732、1836	軟體修復
2002、2102、RN	中繼節點
2004、2104	eNB
2006	DeNB
2008、2106	註冊伺服器
2010、2108	配置伺服器
2110	修復伺服器
2202	功能元件
2204	代碼/資料儲存元件
2214	NVS 元件
NVS	非揮發記憶體
2402、2404、2406、2408、2410、2416、2418、2420、2422、2424、2426	DACB 的代碼量度

【生物材料寄存】

國內寄存資訊【請依寄存機構、日期、號碼順序註記】

國外寄存資訊【請依寄存國家、機構、日期、號碼順序註記】

【序列表】(請換頁單獨記載)

申請專利範圍

1. 一種在一無線通信裝置中使用的方法，該方法包括：

對與該無線通信裝置相關聯的一元件執行一第一完整性檢查；

確定該元件未通過該第一完整性檢查；

確定對與該未通過的元件相對應的一功能；

向一網路實體發送對與該未通過的元件相對應的該功能的一指示；

從該網路實體接收對該未通過的元件執行一第二完整性檢查以確定該未通過的元件中導致該元件未通過該第一完整性檢查的一部分的一請求；以及

對該未通過的元件執行該第二完整性檢查，以隔離該未通過的元件的該部分，從而由該網路實體進行修復。

2. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，該方法更包括：

向該網路實體發送對與該未通過的元件中導致該元件未通過該第一完整性檢查的該部分相對應的一功能的一指示；

從該網路實體接收對該未通過的元件的該部分執行該第二完整性檢查的一次或多次迭代的一請求；以及

對該未通過的元件的該部分執行該第二完整性檢查的該一次或多次迭代，以進一步隔離該未通過的元件的該部分，以由該網路實體進行修復。

3. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該指示包括被配置用於觸發與該網路實體進行的一遠端更新程序，以替換該未通過的元件的該部分。

4. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，該方法更包括：基於儲存在該無線通信裝置處的一元件至功能映射來確定與該未

通過的元件相對應的該功能。

5. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該指示被安全地發送至該網路實體。

6. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中確定該元件未通過該第一次完整性檢查更包括：

確定與該元件相關聯的一完整性量度；

將該完整性量度與關聯於該元件的一可信參考值進行比較；以及

確定該完整性量度不與該可信參考值匹配。

7. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，該方法更包括：

接收與該未通過的元件的該部分相關聯的一替換元件；以及

用該替換元件來替換該未通過的元件的該部分。

8. 如申請專利範圍第 7 項所述的在一無線通信裝置中使用的方法，其中該未通過的元件的該部分是用使用了通過了該第一完整性檢查的與該網路裝置相關聯的其他元件的該替換元件來替換。

9. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，該方法更包括：在確定了該元件未通過該第一完整性檢查時，阻止釋放用於連結於該網路實體的一密鑰。

10. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該未通過的元件是在一多階段的安全引導處理期間被確定。

11. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該網路實體包括一裝置修復伺服器，並且其中該指示被直接地或者經由一網路發送到該裝置修復伺服器。

12. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該

第一完整性檢查和該第二完整性檢查是在一可信任環境中執行。

13. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該功能與將基於該第一完整性檢查的一結果來應用的一網路策略相關聯。

14. 如申請專利範圍第 1 項所述的在一無線通信裝置中使用的方法，其中該功能是藉由與至少一其他無線通信裝置上的至少一其他元件相關聯而在多個無線通信裝置上被標準化。

15. 一種無線通訊裝置，該無線通訊裝置包括：

一載入器，其駐留在該無線通訊裝置上，該載入器被配置用於：在與該無線通信裝置相關聯的一元件上執行一第一完整性檢查；確定該元件未通過該第一完整性檢查；以及對該未通過的元件的一部分執行一第二完整性檢查，以隔離該未通過的元件的一部分，從而由一網路實體進行修復；

一策略管理實體，駐留在該無線通訊裝置上，該策略管理實體被配置用於確定對與該未通過的元件相對應的一網路功能；以及

一平臺完整性策略引擎（PIPE），其與該載入器通訊且駐留在該無線通訊裝置上，該 PIPE 被配置用於：接收來自該載入器的對該未通過的元件的一指示；接收與該未通過的元件相對應的該網路功能；向一網路實體報告對與該未通過的元件相對應的該網路功能的一指示；以及從該網路實體接收對該未通過的元件執行一第二完整性檢查以確定該未通過的元件中導致該元件未通過該第一完整性檢查的該部分的一請求。

16. 如申請專利範圍第 15 項所述的無線通訊裝置，其中該載入器更被配置用於執行以下處理來確定該元件未通過該第一完整性檢查：

確定與該元件相關聯的一完整性量度；

將該完整性量度與關聯於該元件的一可信參考值進行比較；以及

確定該完整性量度不與該可信參考值匹配。

17. 如申請專利範圍第 15 項所述的無線通訊裝置，其中該 PIPE 更被配置用於在從該載入器接收到對該未通過的元件的該指示時執行下列各項中的一項或多項：將該系統斷電、阻止載入該未通過的元件、阻止存取用以向該網路實體驗證該無線通信裝置的一驗證密鑰、或者阻止存取一安全功能。

18. 如申請專利範圍第 15 項所述的無線通訊裝置，其中該 PIPE 更被配置用於核實一裝置管理功能，該裝置管理功能被配置用於：接收來自該網路實體的一替換元件；以及以該替換元件來替換該未通過的元件的該部分。

19. 如申請專利範圍第 15 項所述的無線通訊裝置，其中該 PIPE 更被配置用於接收來自一外部實體的多個策略，並且將該網路功能映射到該多個策略中的一者或多者，其中該多個策略被配置爲基於該第一完整性檢查的一結果來應用。

20. 一種駐留在一無線通信網路上的裝置修復伺服器，該裝置修復伺服器包括：

一處理器，適用以執行電腦可讀的指令；

一記憶體，與該處理器通信地耦合，該記憶體內已儲存一電腦可讀的指令，當由該處理器執行時，該電腦可讀的指令使該處理器執行一操作，該操作包括：

修復一無線通信裝置上的未通過一完整性檢查的一元件的一部分，其中該修復包括：

從該無線通信裝置接收對與該無線通信裝置上的未通過該完整性檢查的該元件相關聯的一網路功能的一指示；

基於對該網路功能的該接收到的指示來確定該未通過的元件；

執行向該無線通信裝置的一詢問，以隔離該未通過的元件的該部分來進行修復；

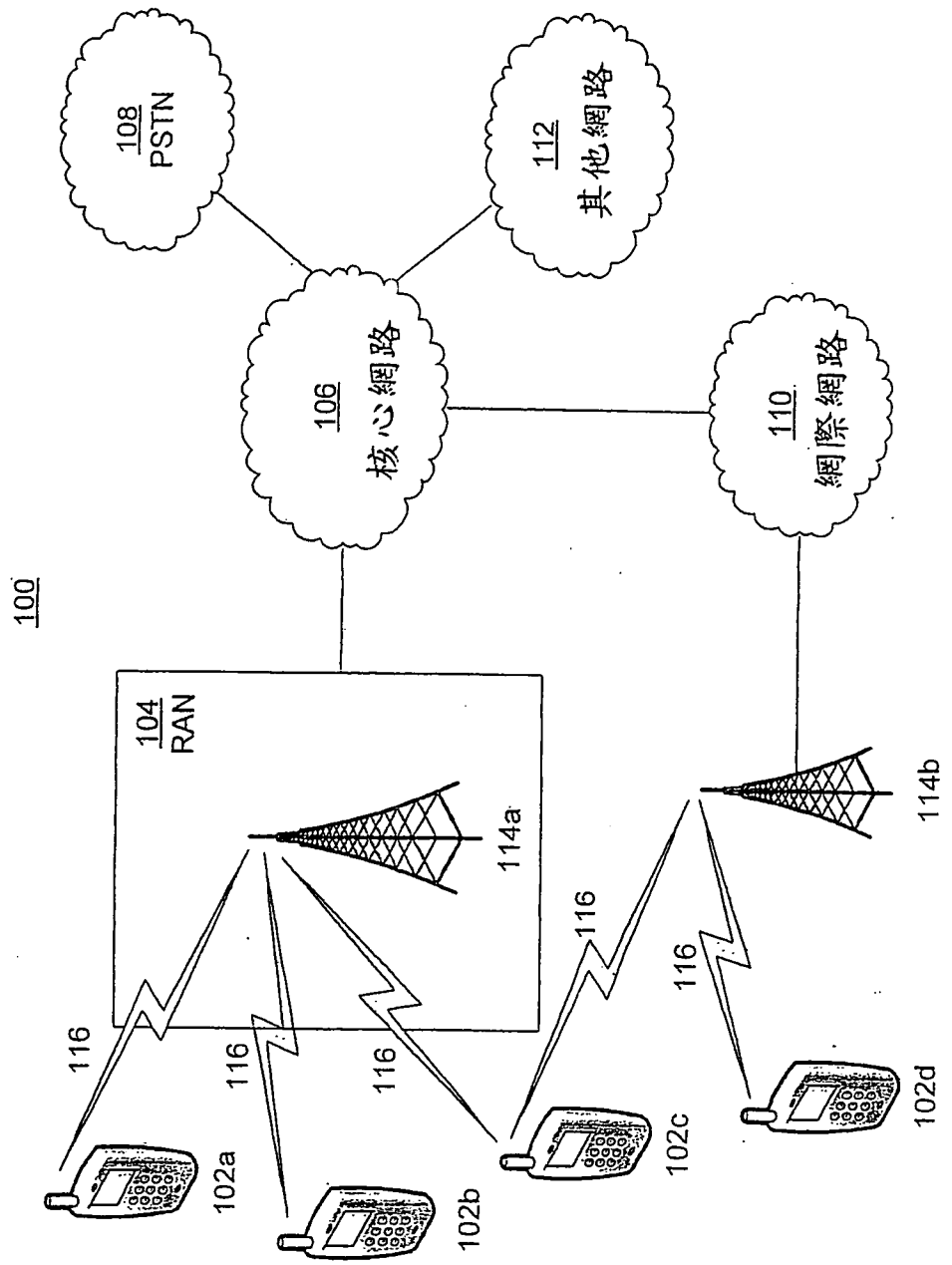
基於一個或多個標準來確定用於該未通過的元件的該部分的修復或替換；以及

將對該未通過的元件的該部分的修復或替換發送到該無線通信裝置。

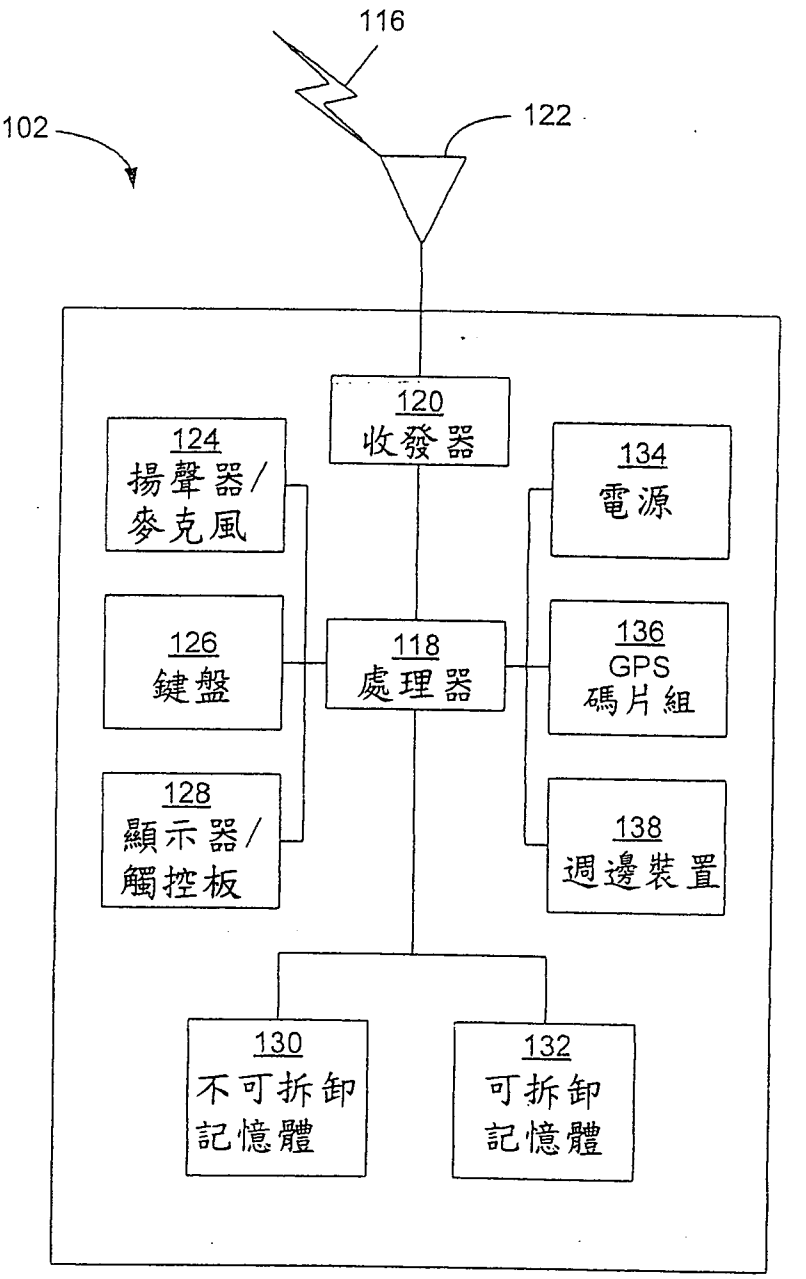
21. 如申請專利範圍第 20 項所述的裝置修復伺服器，其中對該未通過的元件的該部分的修復或替換包括一軟體代碼。

22. 如申請專利範圍第 20 項所述的裝置修復伺服器，其中該修復更包括接收表明與該完整性檢查相關聯的一資訊可靠的一指示。

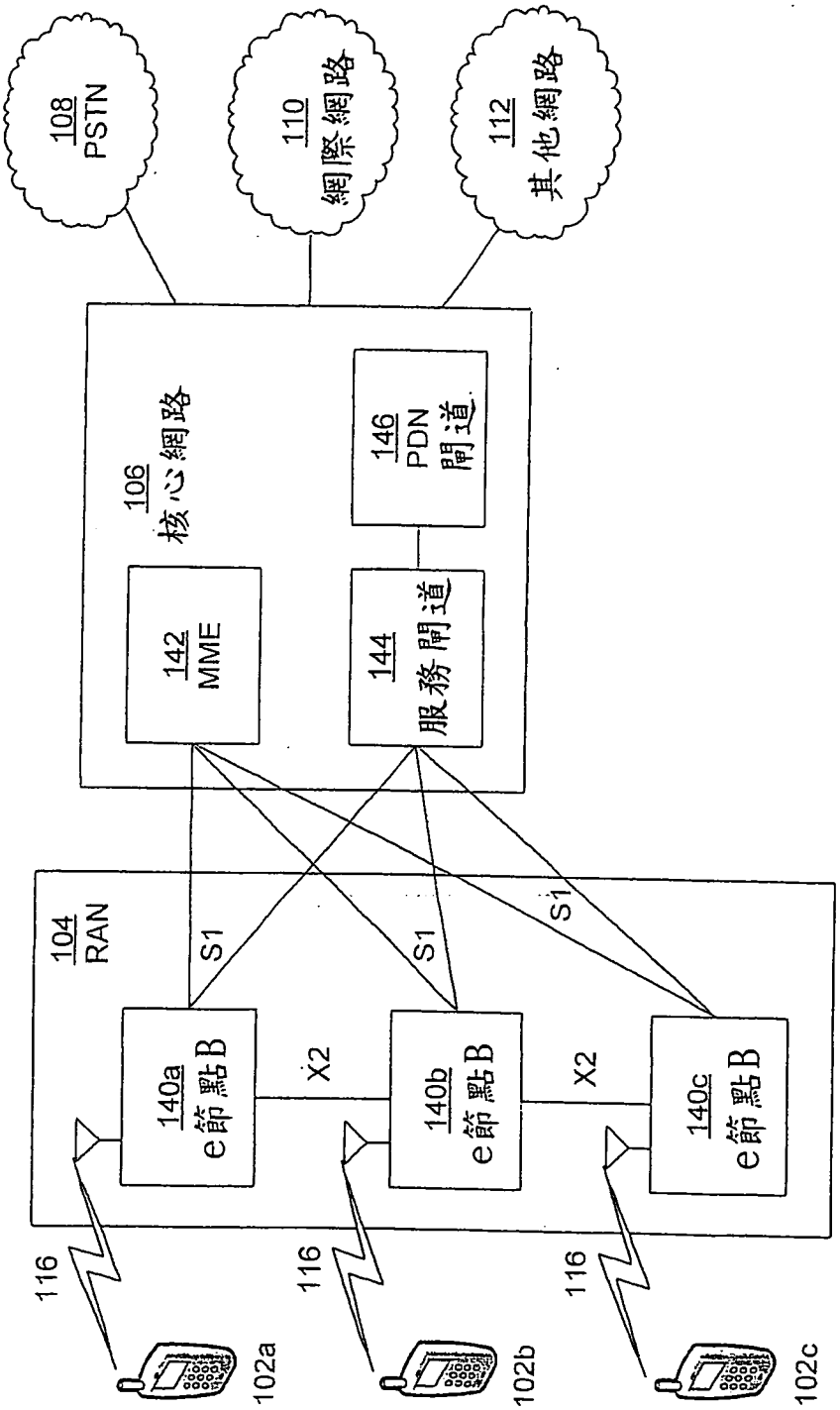
圖式


108
PSTN
112
其他網路
106
核心網路
110
網際網路
100
104
RAN
114a
114b
116
116
116
116
102a
102b
102c
102d

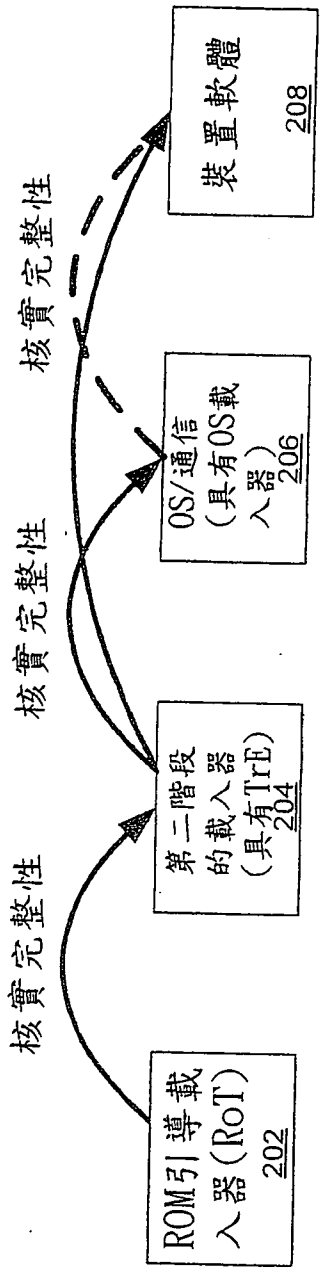
第 1A 圖


116
102
122
120
收發器
124
揚聲器/
麥克風
134
電源
126
鍵盤
118
處理器
136
GPS
碼片組
128
顯示器/
觸控板
138
週邊裝置
130
不可拆卸
記憶體
132
可拆卸
記憶體

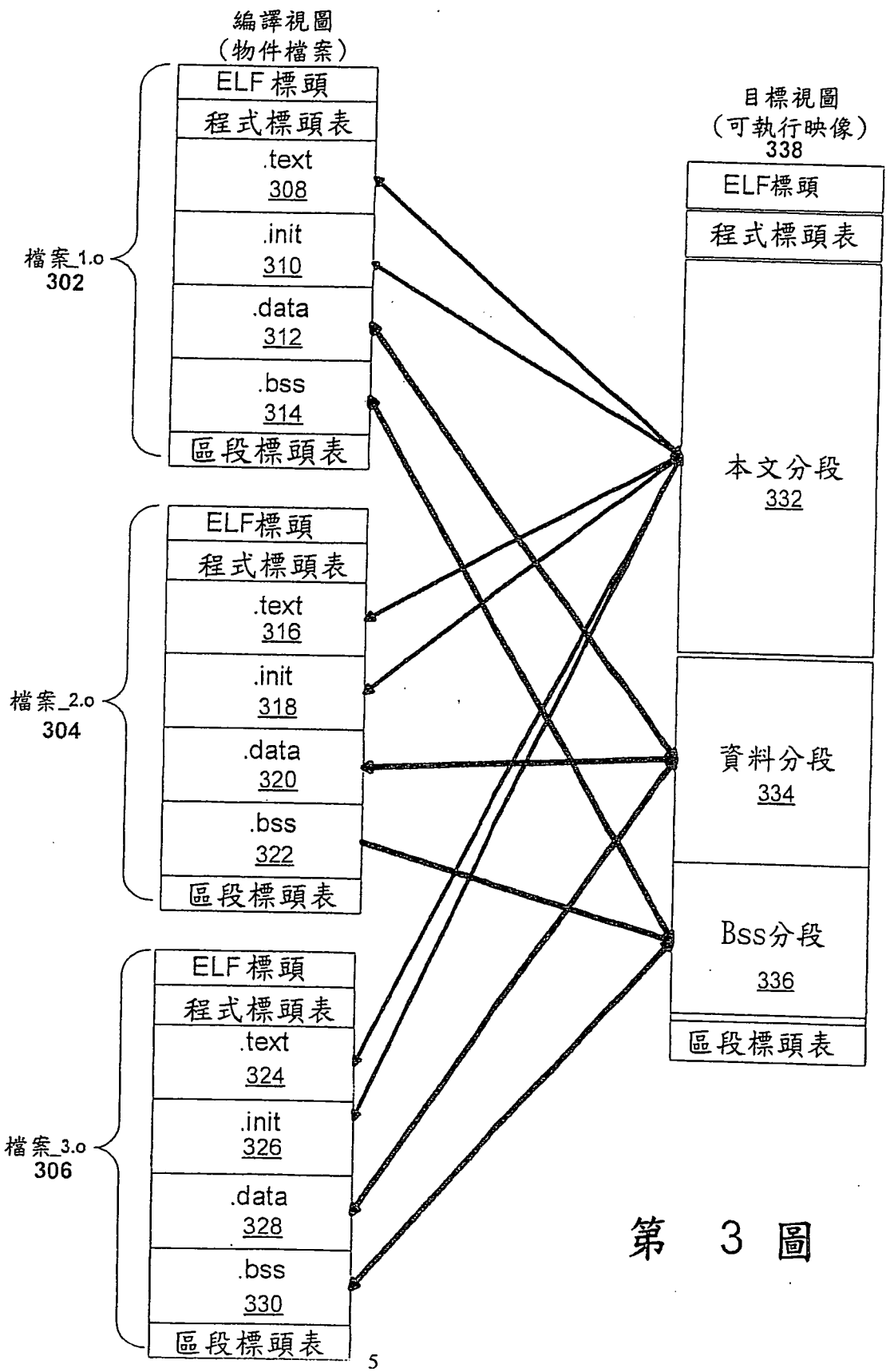
第 1B 圖


108
PSTN
110
網際網路
112
其他網路
106
核心網路
142
MME
144
服務閘道
146
PDN
閘道
104
RAN
S1
S1
S1
X2
X2
140a
e節點B
140b
e節點B
140c
e節點B
116
116
116
102a
102b
102c

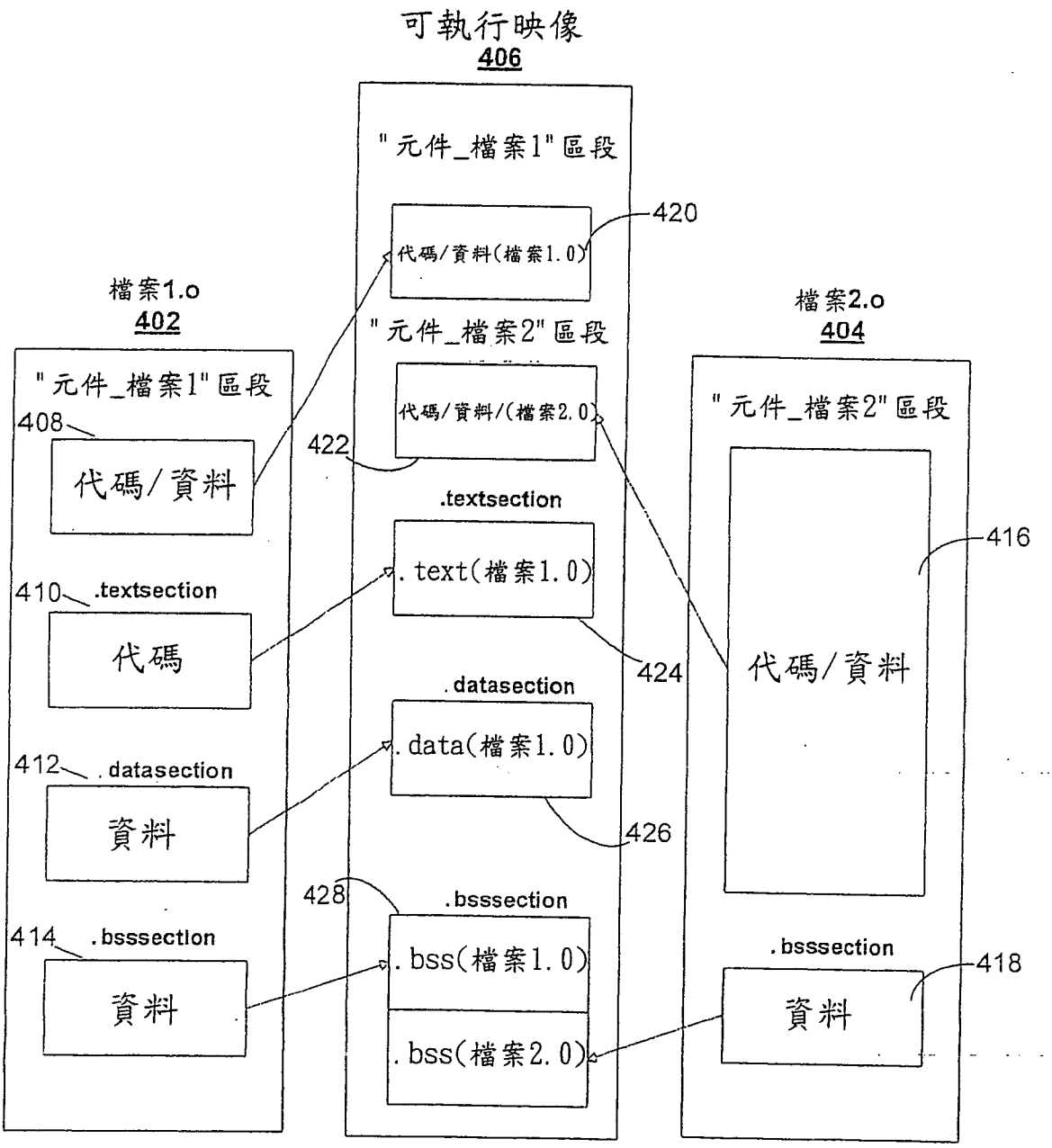
第 1C 圖


ROM引導載入器(RoT)
202
核實完整性
第二階段的載入器(具有TrE)
204
核實完整性
OS/通信(具有OS載入器)
206
核實完整性
裝置軟體
208

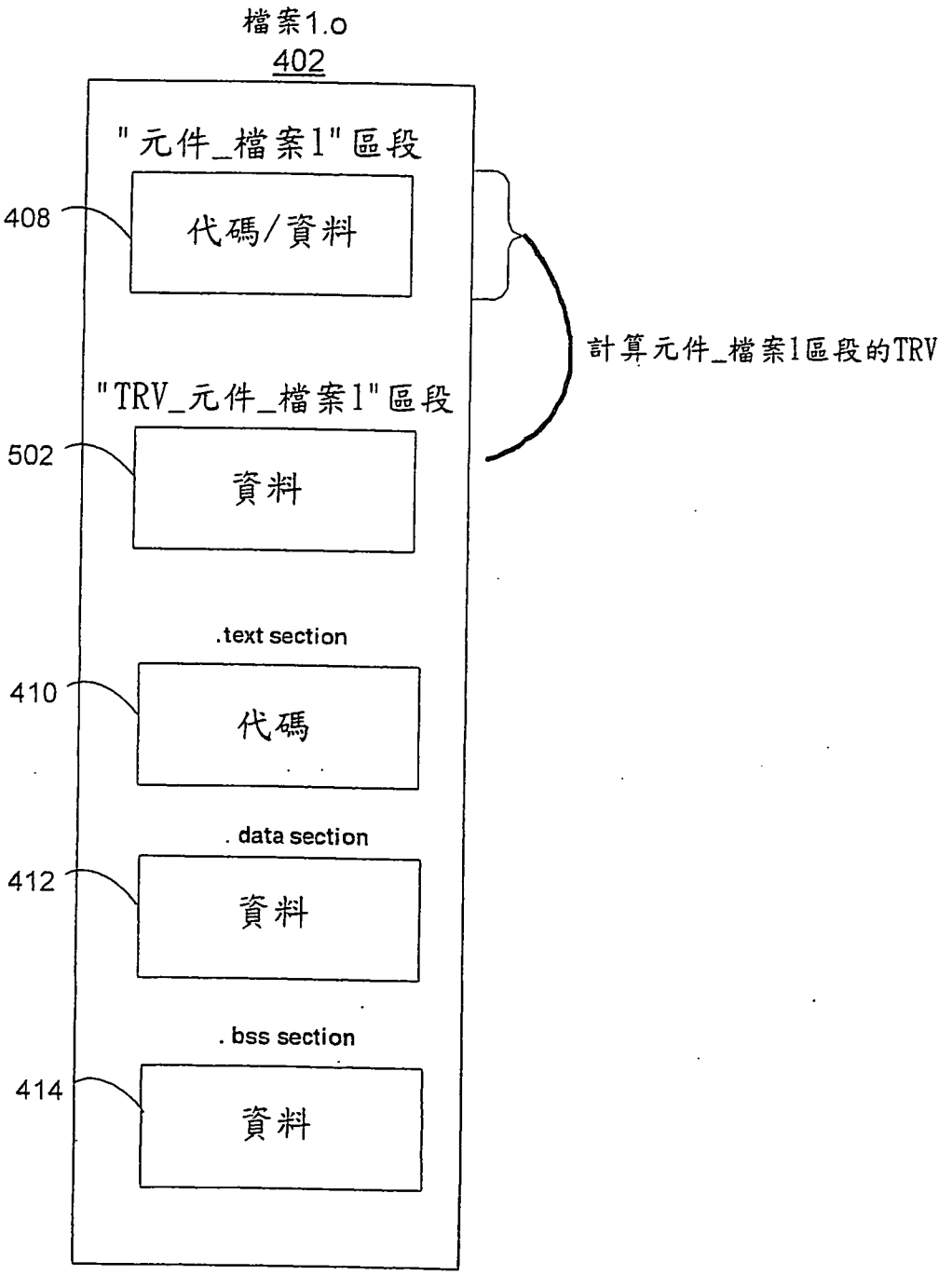
第 2 圖


編譯視圖
（物件檔案）
ELF 標頭
程式標頭表
.text
308
.init
310
.data
312
.bss
314
區段標頭表
檔案_1.o
302
ELF標頭
程式標頭表
.text
316
.init
318
.data
320
.bss
322
區段標頭表
檔案_2.o
304
ELF 標頭
程式標頭表
.text
324
.init
326
.data
328
.bss
330
區段標頭表
檔案_3.o
306
目標視圖
（可執行映像）
338
ELF標頭
程式標頭表
本文分段
332
資料分段
334
Bss分段
336
區段標頭表

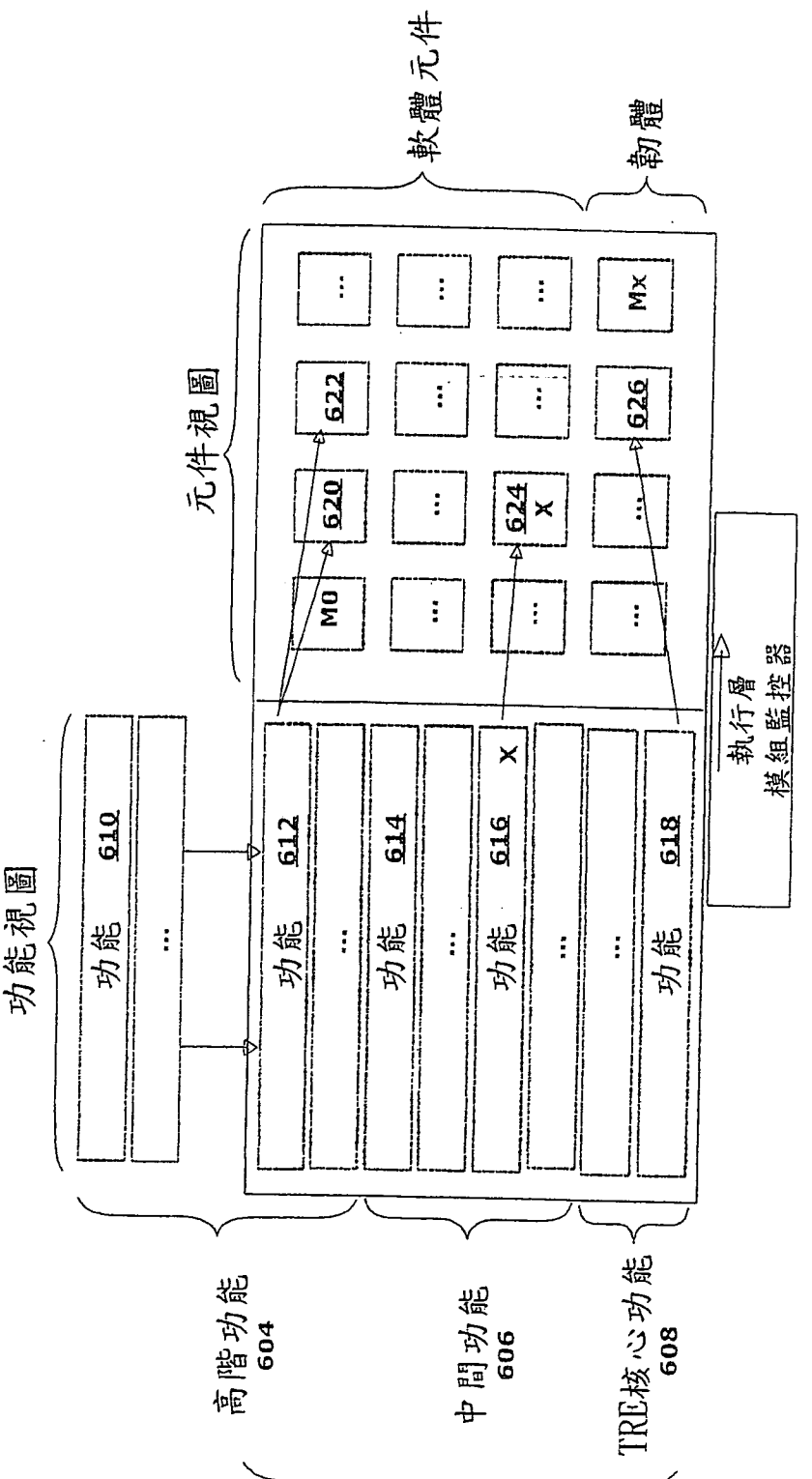
第 3 圖


可執行映像
406
"元件_檔案1"區段
代碼/資料(檔案1.0)
420
"元件_檔案2"區段
代碼/資料/(檔案2.0)
422
.textsection
.text(檔案1.0)
424
.datasection
.data(檔案1.0)
426
.bsssection
.bss(檔案1.0)
.bss(檔案2.0)
428
檔案1.o
402
"元件_檔案1"區段
408
代碼/資料
410
.textsection
代碼
412
.datasection
資料
414
.bsssection
資料
檔案2.o
404
"元件_檔案2"區段
代碼/資料
416
.bsssection
資料
418

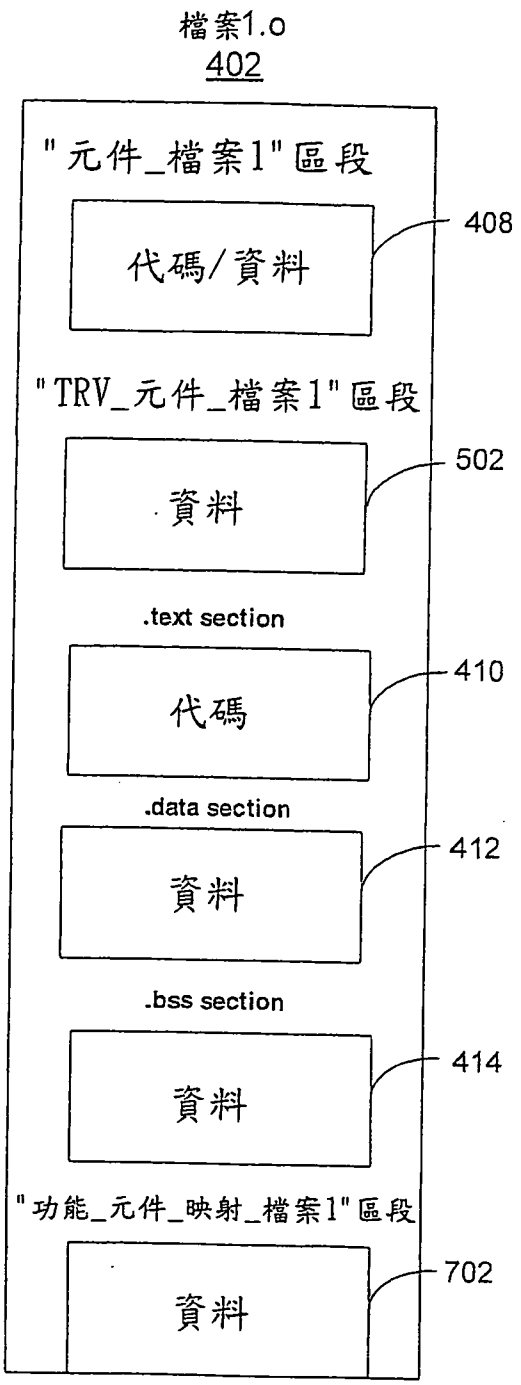
第 4 圖


檔案1.o
402
"元件_檔案1"區段
408
代碼/資料
計算元件_檔案1區段的TRV
"TRV_元件_檔案1"區段
502
資料
.text section
410
代碼
. data section
412
資料
. bss section
414
資料

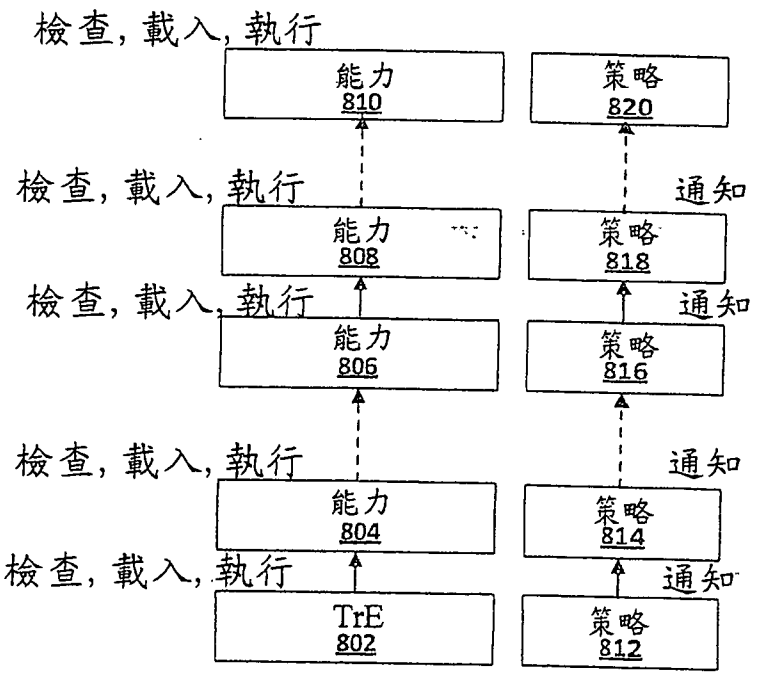
第 5 圖


功能視圖
功能 610
...
元件視圖
軟體元件
韌體
功能 612
功能 614
功能 616
X
功能 618
M0
620
622
624
X
626
Mx
執行層
模組監控器
高階功能
604
中間功能
606
TRE核心功能
608
可信任域
602

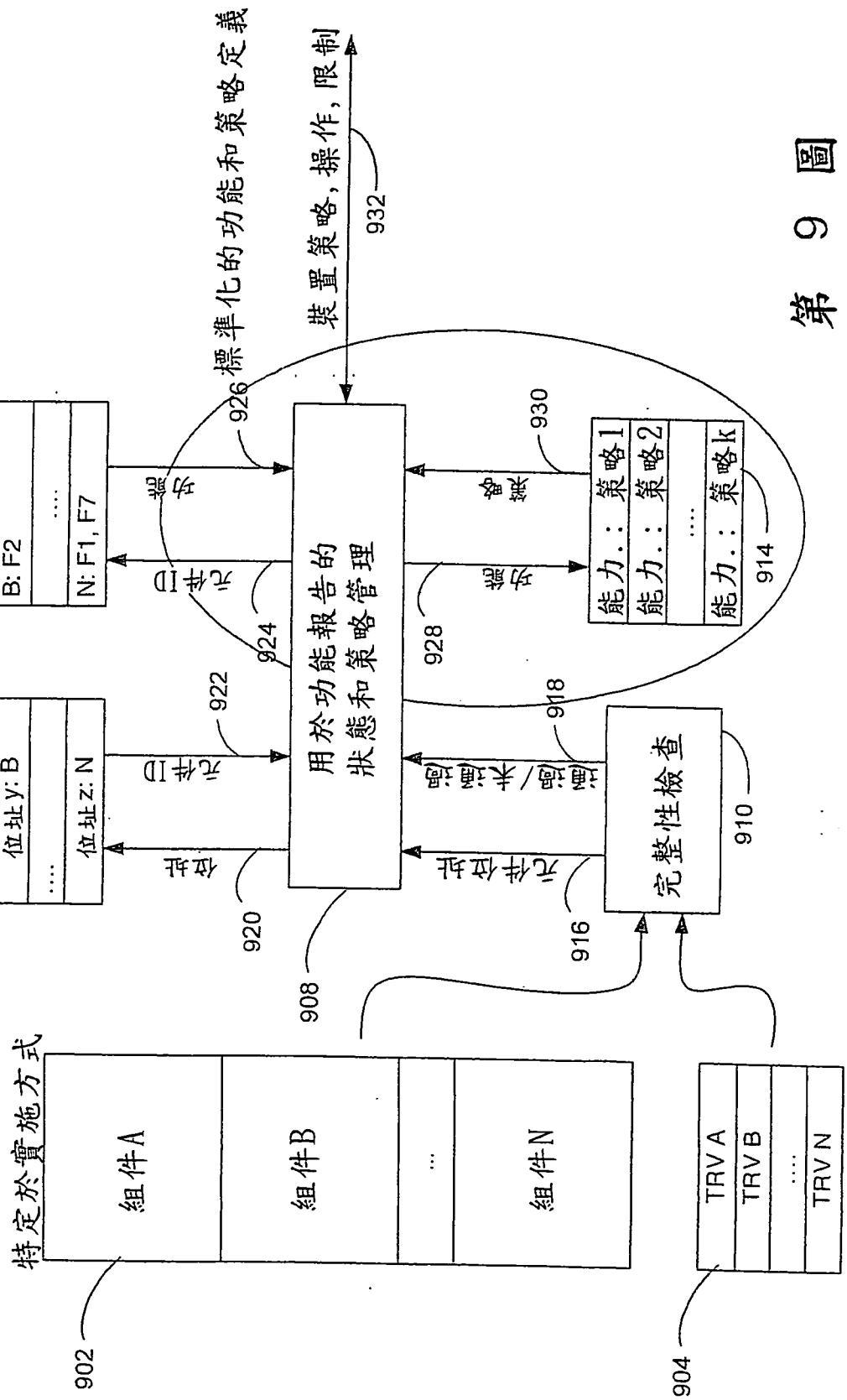
第 6 圖


檔案1.o
402
"元件_檔案1"區段
代碼/資料
408
"TRV_元件_檔案1"區段
資料
502
.text section
代碼
410
.data section
資料
412
.bss section
資料
414
"功能_元件_映射_檔案1"區段
資料
702

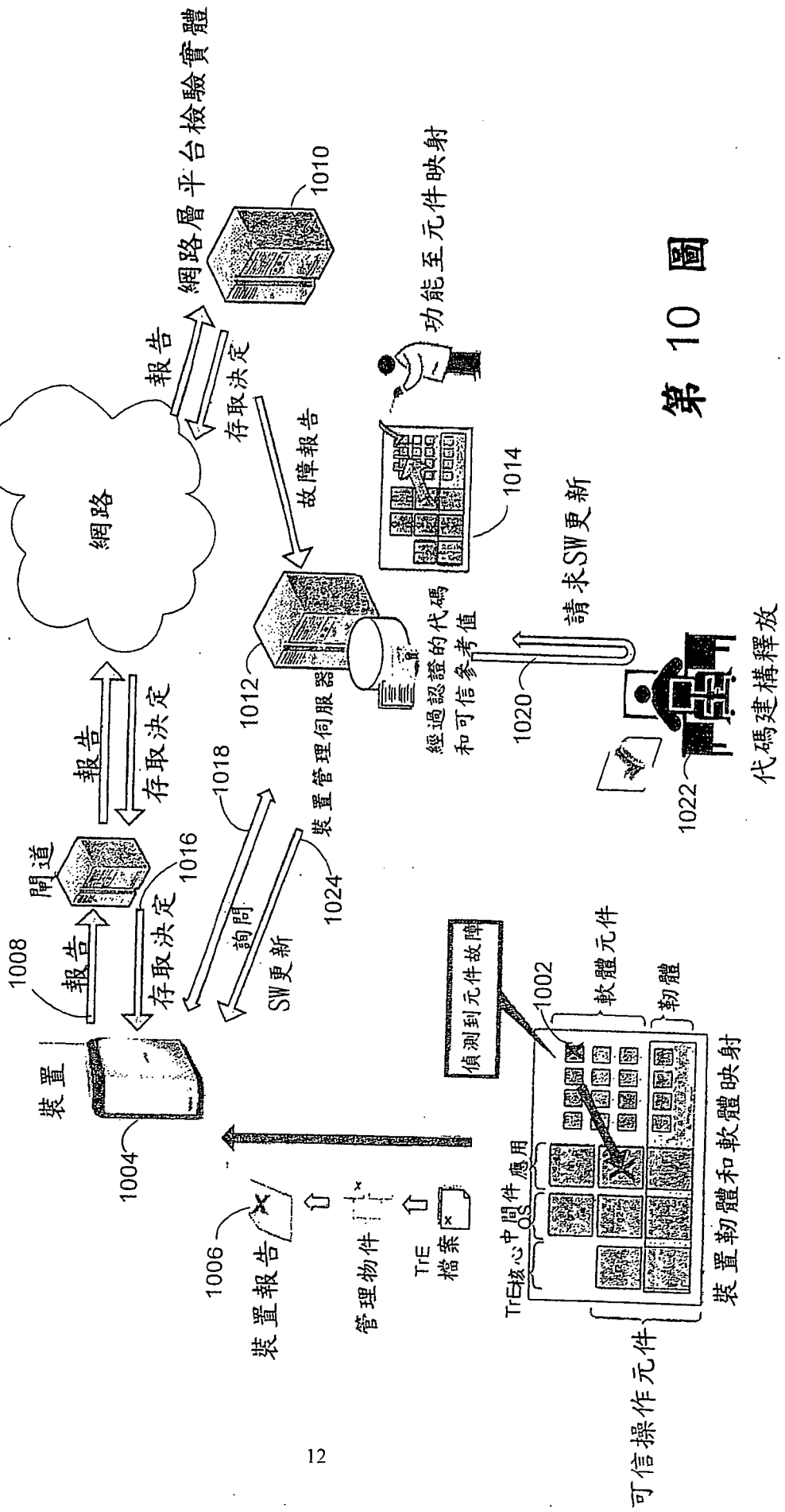
第 7 圖


檢查，載入，執行
能力
810
策略
820
檢查，載入，執行
通知
能力
808
策略
818
檢查，載入，執行
通知
能力
806
策略
816
檢查，載入，執行
通知
能力
804
策略
814
檢查，載入，執行
通知
TrE
802
策略
812

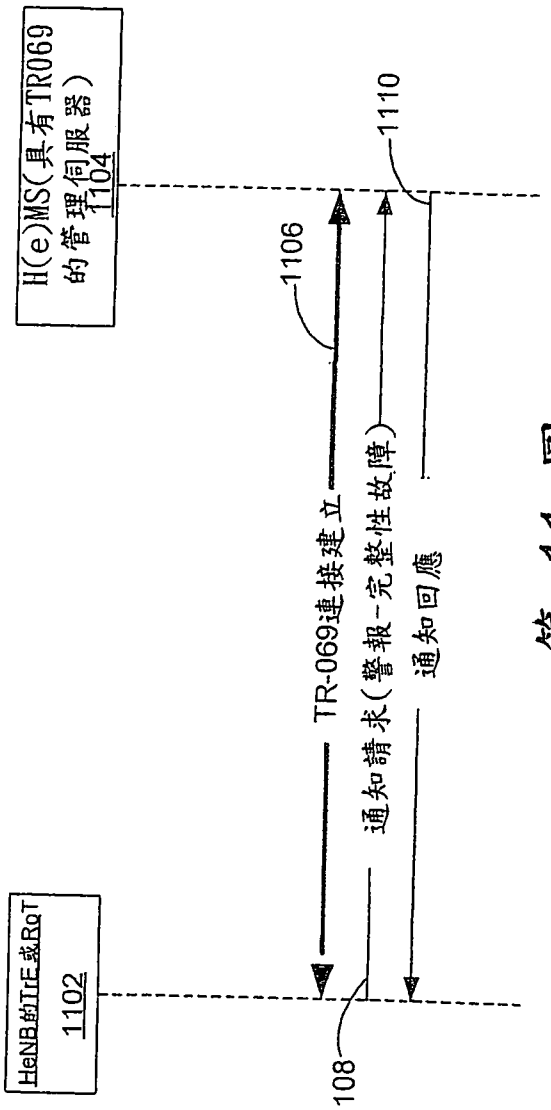
第 8 圖


特定於實施方式
組件A
組件B
...
組件N
902
TRV A
TRV B
....
TRV N
904
908
用於功能報告的
狀態和策略管理
920
916
完整性檢查
910
906
位址x: A
位址y: B
....
位址z: N
922
924
912
A: F1, F5, F14
B: F2
....
N: F1, F7
926
標準化的功能和策略定義
裝置策略，操作，限制
932
928
930
能力.: 策略1
能力.: 策略2
....
能力.: 策略k
914
918

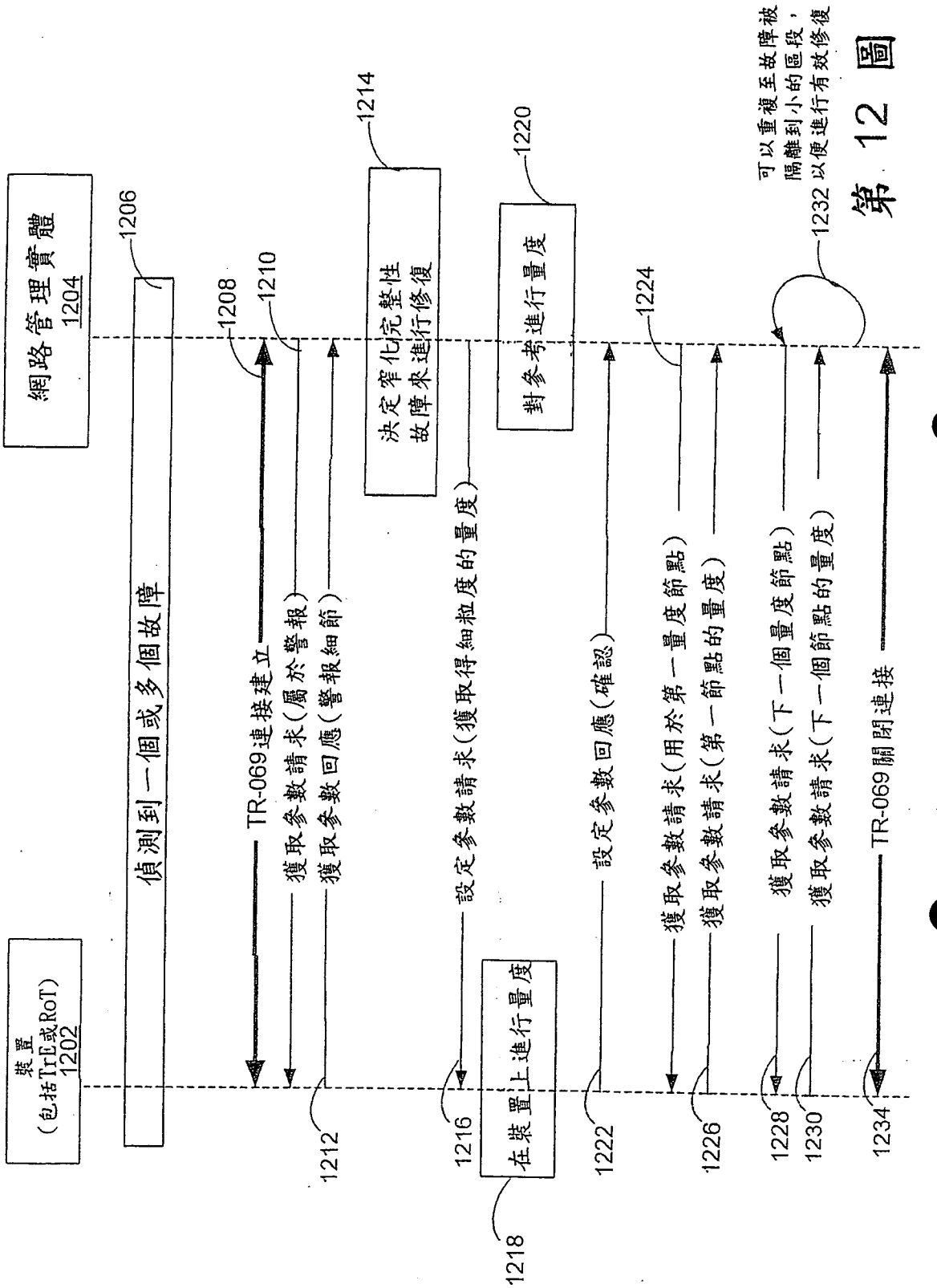
第 9 圖


網路層平台檢驗實體
1010
報告
存取決定
功能至元件映射
網路
故障報告
1014
1012
裝置管理伺服器
經過認證的代碼
和可信參考值
請求SW更新
1020
1018
詢問
SW更新
1024
閘道
1016
報告
存取決定
1008
裝置
1004
1022
代碼建構釋放
偵測到元件故障
1002
軟體元件
韌體
1006
裝置報告
管理物件
TrE
檔案
TrE核心
OS
中間件
應用
裝置韌體和軟體映射
可信操作元件

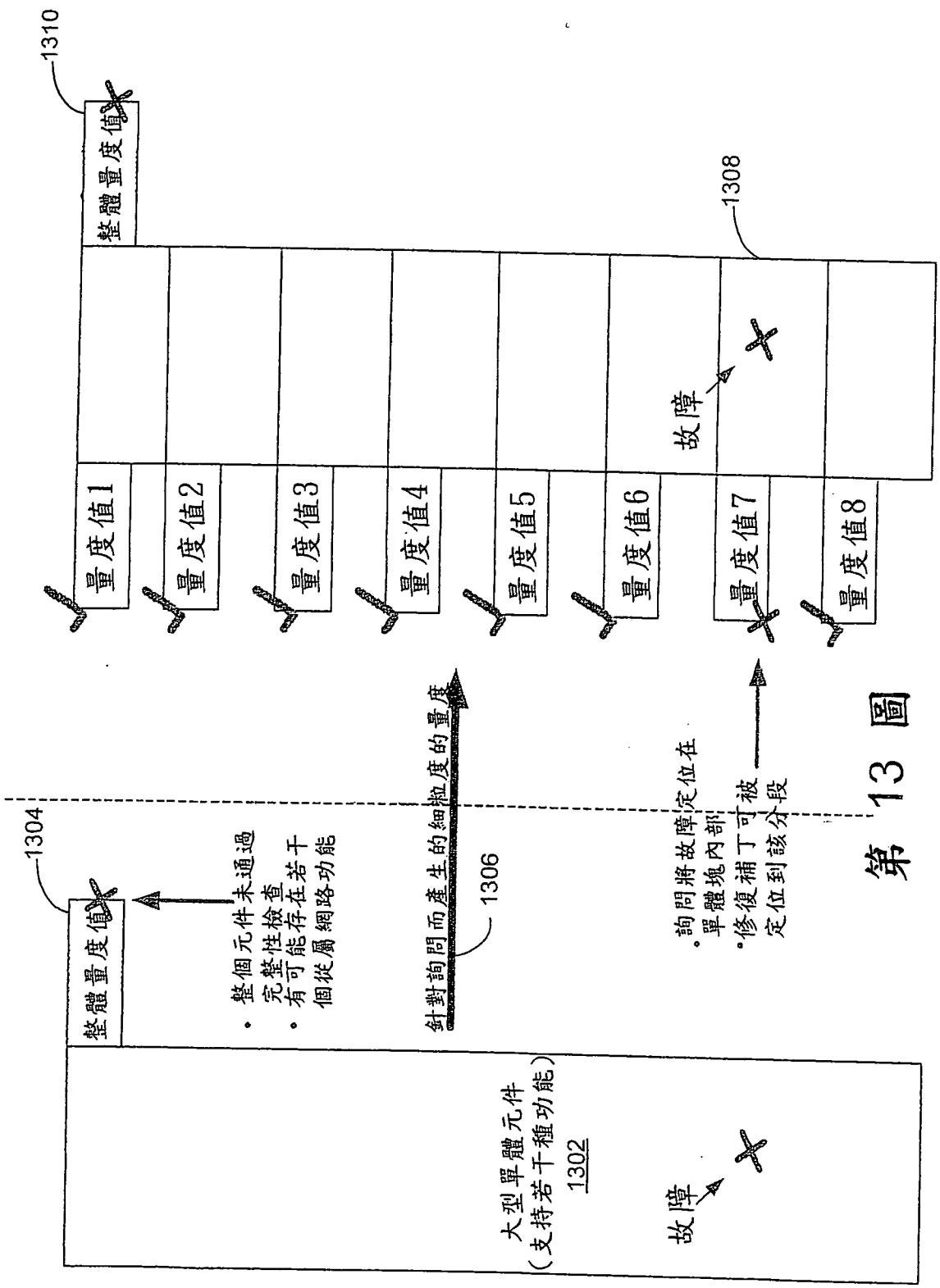
第 10 圖


H(e)MS(具有TR069的管理伺服器)
1104
HeNB的IrE或RoT
1102
1106
TR-069連接建立
1110
通知請求(警報-完整性故障)
通知回應
1108

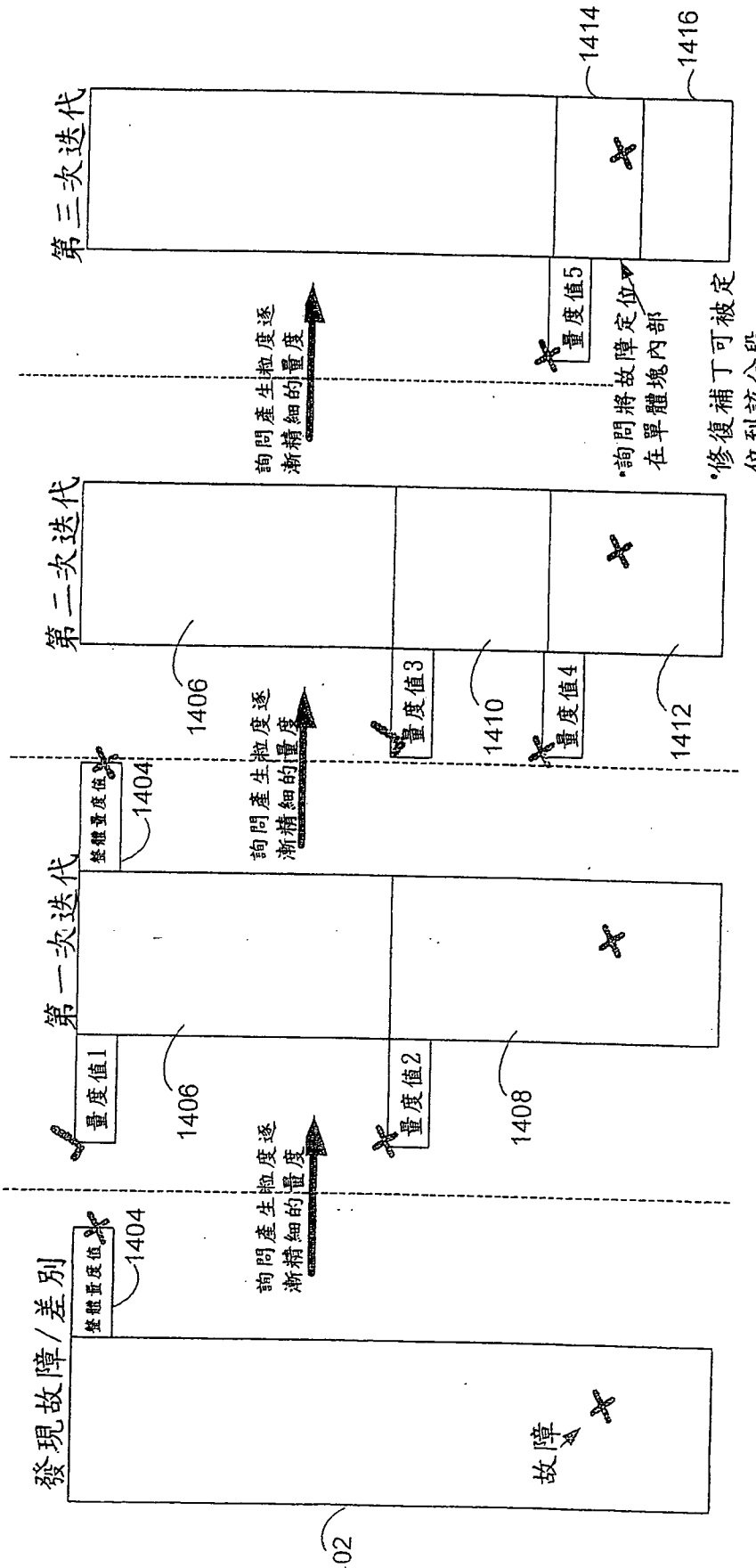
第 11 圖


裝置
（包括TrE或RoT）
1202
網路管理實體
1204
1206
偵測到一個或多個故障
1208
1210
TR-069連接建立
獲取參數請求（屬於警報）
獲取參數回應（警報細節）
1212
1214
決定窄化完整性
故障來進行修復
設定參數請求（獲取得細粒度的量度）
1216
在裝置上進行量度
1218
1220
對參考進行量度
設定參數回應（確認）
1222
1224
獲取參數請求（用於第一量度節點）
獲取參數請求（第一節點的量度）
1226
獲取參數請求（下一個量度節點）
獲取參數請求（下一個節點的量度）
1228
1230
可以重複至故障被
隔離到小的區段，
1232 以便進行有效修復
TR-069關閉連接
1234

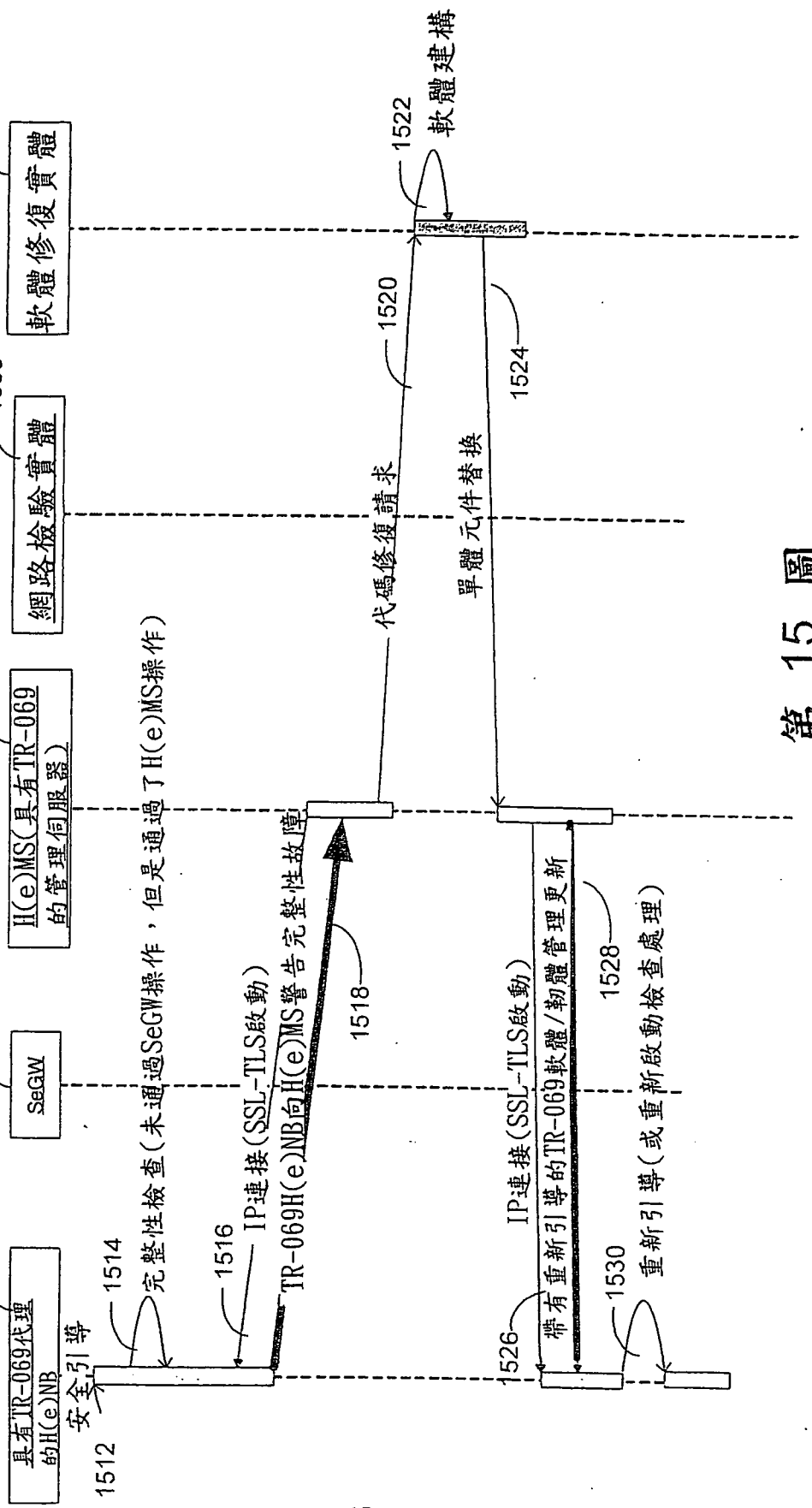
第 12 圖


1310
整體量度值
1308
故障
量度值1
量度值2
量度值3
量度值4
量度值5
量度值6
量度值7
量度值8
1304
整體量度值
• 整個元件未通過完整性檢查
• 有可能存在若干個從屬網路功能
針對詢問而產生的細粒度的量度
1306
• 詢問將故障定位在單體塊內部
• 修復補丁可被定位到該分段
大型單體元件
（支持若干種功能）
1302
故障

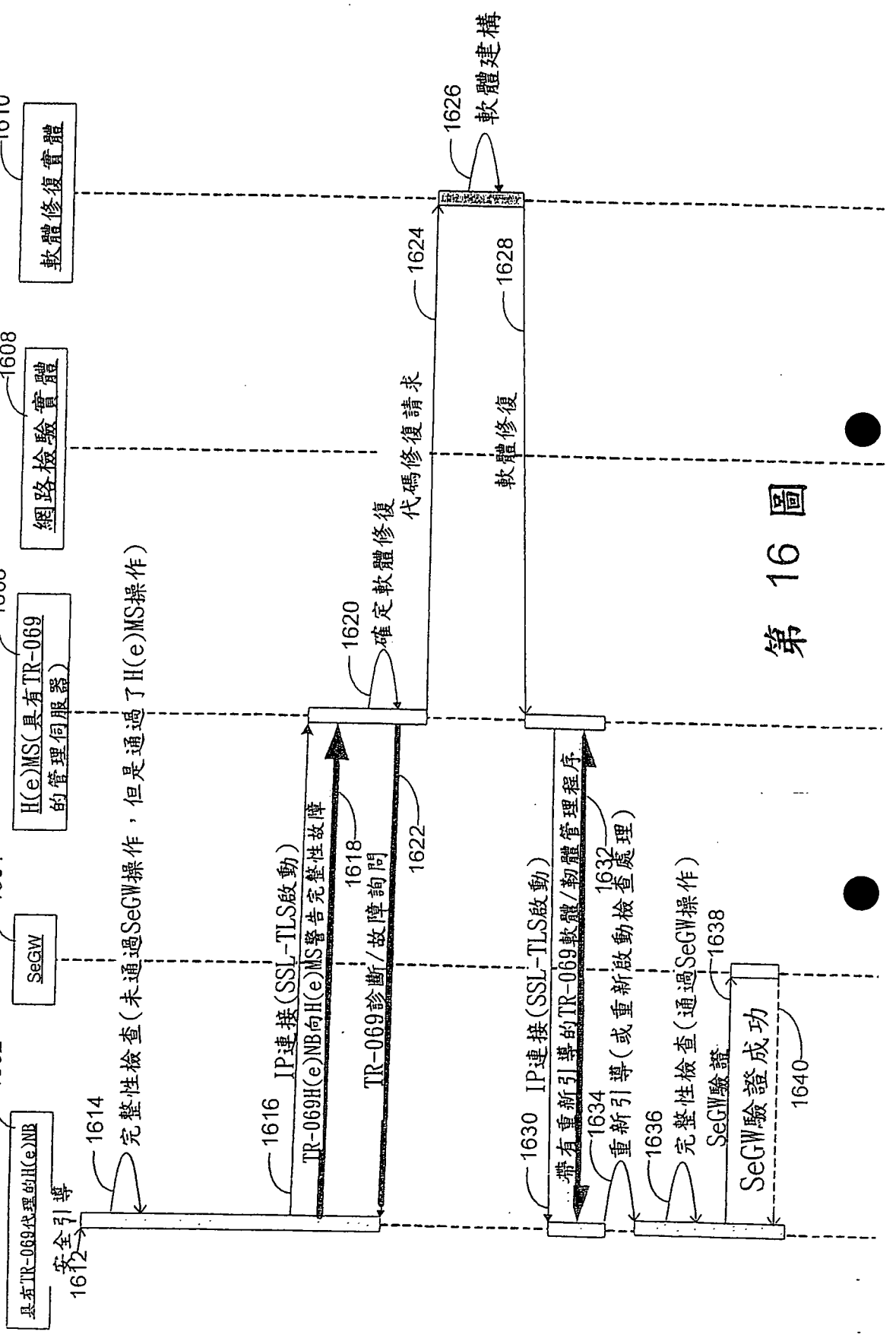
第 13 圖


發現故障/差別
1402
故障
1404
整體量度值
量度值1
1406
詢問產生粒度逐漸精細的量度
第一次迭代
1404
整體量度值
量度值2
1408
詢問產生粒度逐漸精細的量度
第二次迭代
1406
量度值3
1410
量度值4
1412
詢問產生粒度逐漸精細的量度
第三次迭代
1414
量度值5
1416
•詢問將故障定位在單體塊內部
•修復補丁可被定位到該分段

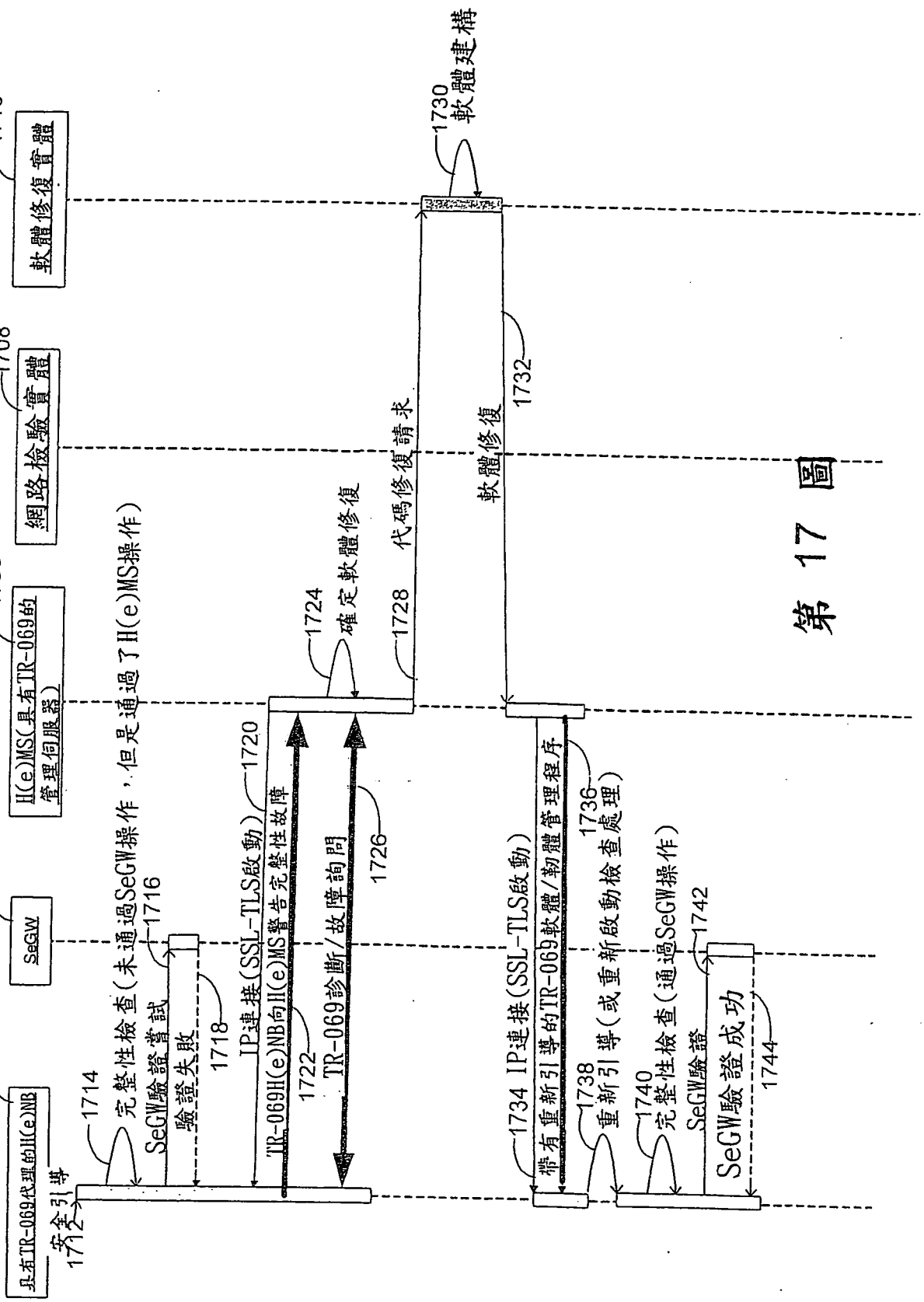
第 14 圖


具有TR-069代理的H(e)NB
1502
SeGW
1504
H(e)MS(具有TR-069的管理伺服器)
1506
網路檢驗實體
1508
軟體修復實體
1510
安全引導
1512
完整性檢查(未通過SeGW操作，但是通過了H(e)MS操作)
1514
IP連接(SSL-TLS啟動)
1516
TR-069H(e)NB向H(e)MS警告完整性故障
1518
代碼修復請求
1520
軟體建構
1522
單體元件替換
1524
IP連接(SSL-TLS啟動)
1526
帶有重新引導的TR-069軟體/韌體管理更新
1528
重新引導(或重新啟動檢查處理)
1530

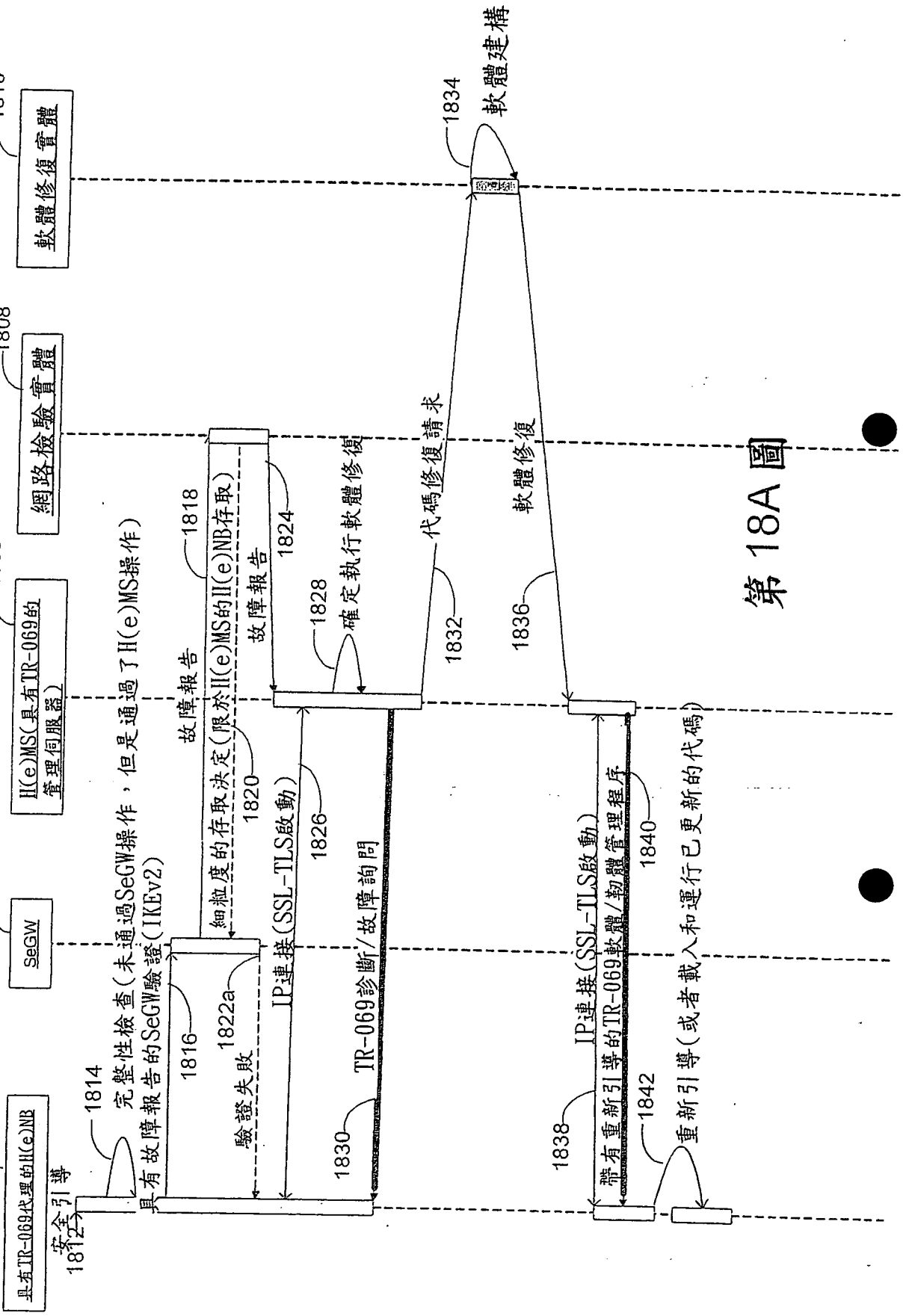
第 15 圖


具有TR-069代理的H(e)NB
1602
SeGW
1604
H(e)MS(具有TR-069的管理伺服器)
1606
網路檢驗實體
1608
軟體修復實體
1610
安全引導
1612
完整性檢查(未通過SeGW操作，但是通過了H(e)MS操作)
1614
IP連接(SSL-TLS啟動)
1616
TR-069H(e)NB向H(e)MS發告完整性故障
1618
TR-069診斷/故障詢問
1622
確定軟體修復
1620
代碼修復請求
1624
軟體修復
1628
軟體建構
1626
IP連接(SSL-TLS啟動)
1630
帶有重新引導的TR-069軟體/韌體管理程序
1632
重新引導(或重新啟動檢查處理)
1634
完整性檢查(通過SeGW操作)
1636
SeGW驗證
1638
SeGW驗證成功
1640

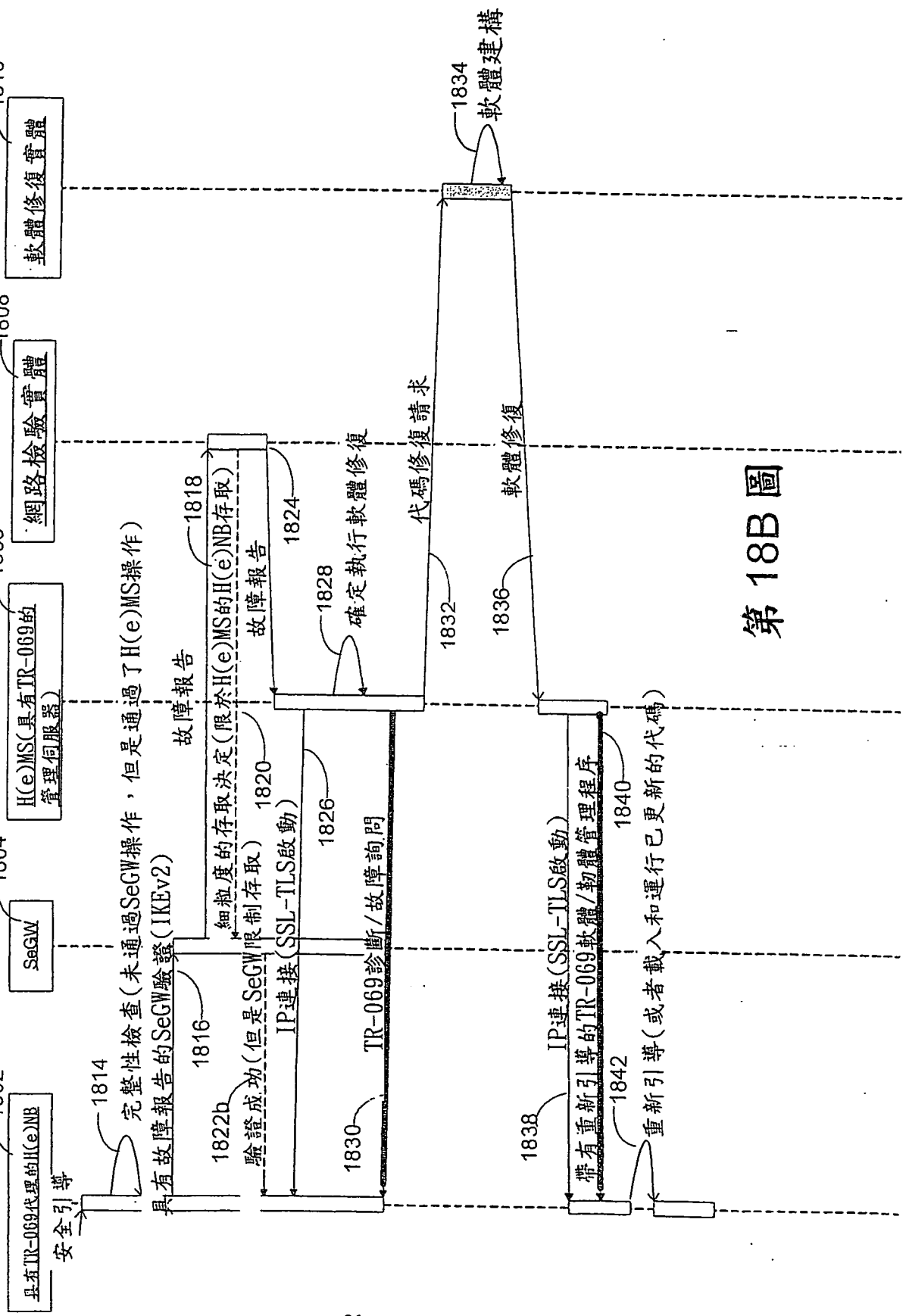
第16圖


1710
軟體修復實體
1730
軟體建構
1708
網路檢驗實體
1732
軟體修復
1706
H(e)MS(具有TR-069的管理伺服器)
1724
確定軟體修復
1728
代碼修復請求
1704
SeGW
1716
完整性檢查(未通過SeGW操作，但是通過了H(e)MS操作)
1714
SeGW驗證嘗試
1718
驗證失敗
1720
IP連接(SSL-TLS啟動)
TR-069H(e)NB向H(e)MS報告完整性故障
1722
TR-069診斷/故障詢問
1726
1734 IP連接(SSL-TLS啟動)
帶有重新引導的TR-069軟體/韌體管理程序
1736
1738
重新引導(或重新啟動檢查處理)
1740
完整性檢查(通過SeGW操作)
1742
SeGW驗證
SeGW驗證成功
1744
1702
具有TR-069代理的H(e)NB
1712
安全引導

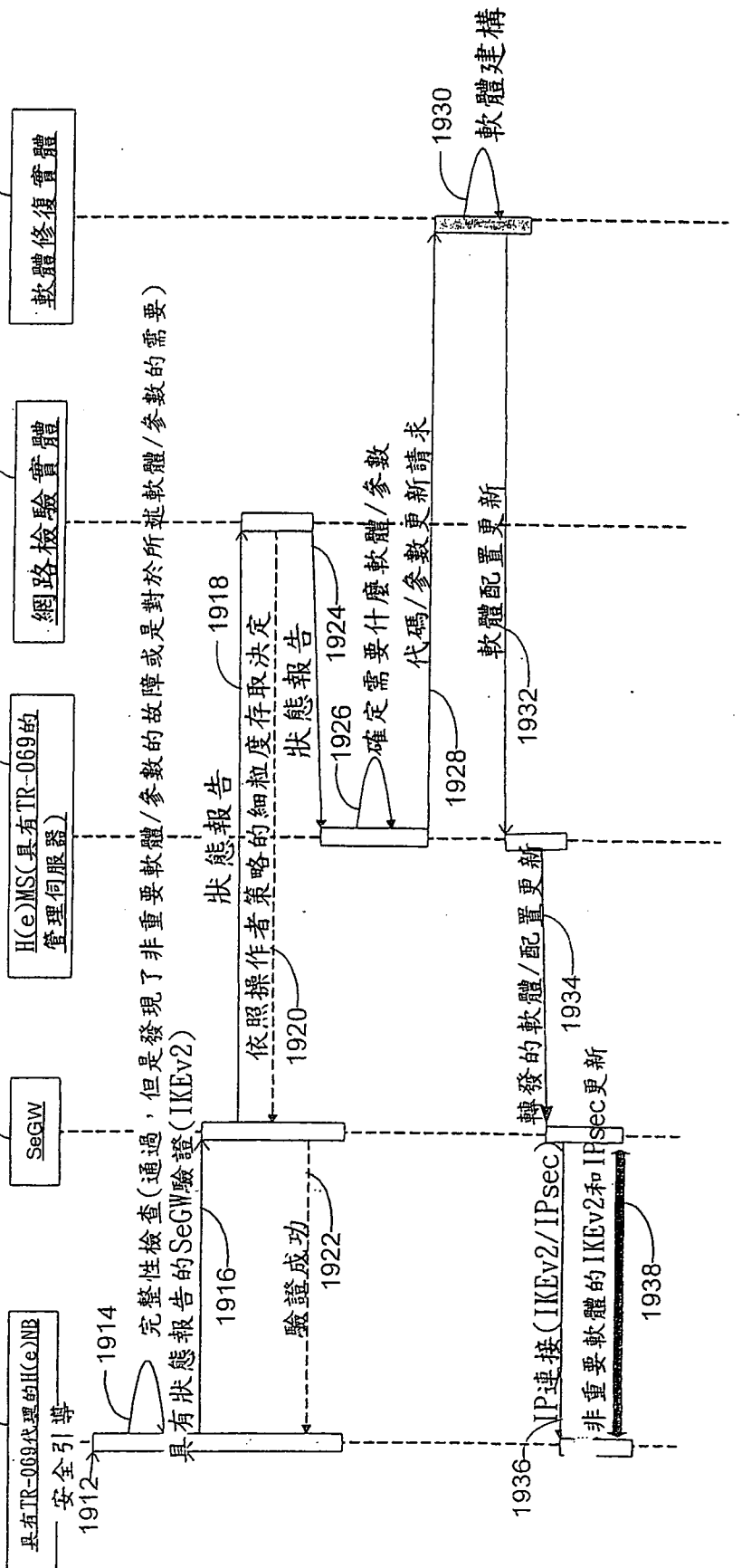
第17圖


1802
具有TR-069代理的H(e)NB
1804
SeGW
1806
H(e)MS(具有TR-069的管理伺服器)
1808
網路檢驗實體
1810
軟體修復實體
安全引導
1812
1814
完整性檢查(未通過SeGW操作，但是通過了H(e)MS操作)
具有故障報告的SeGW驗證(IKEv2)
1816
1818
故障報告
細粒度的存取決定(限於H(e)MS的H(e)NB存取)
1820
1822a
驗證失敗
IP連接(SSL-TLS啟動)
1824
故障報告
1826
TR-069診斷/故障詢問
1828
確定執行軟體修復
1830
1832
代碼修復請求
1834
軟體建構
1836
軟體修復
1838
IP連接(SSL-TLS啟動)
帶有重新引導的TR-069軟體/韌體管理程序
1840
1842
重新引導(或者載入和運行已更新的代碼)

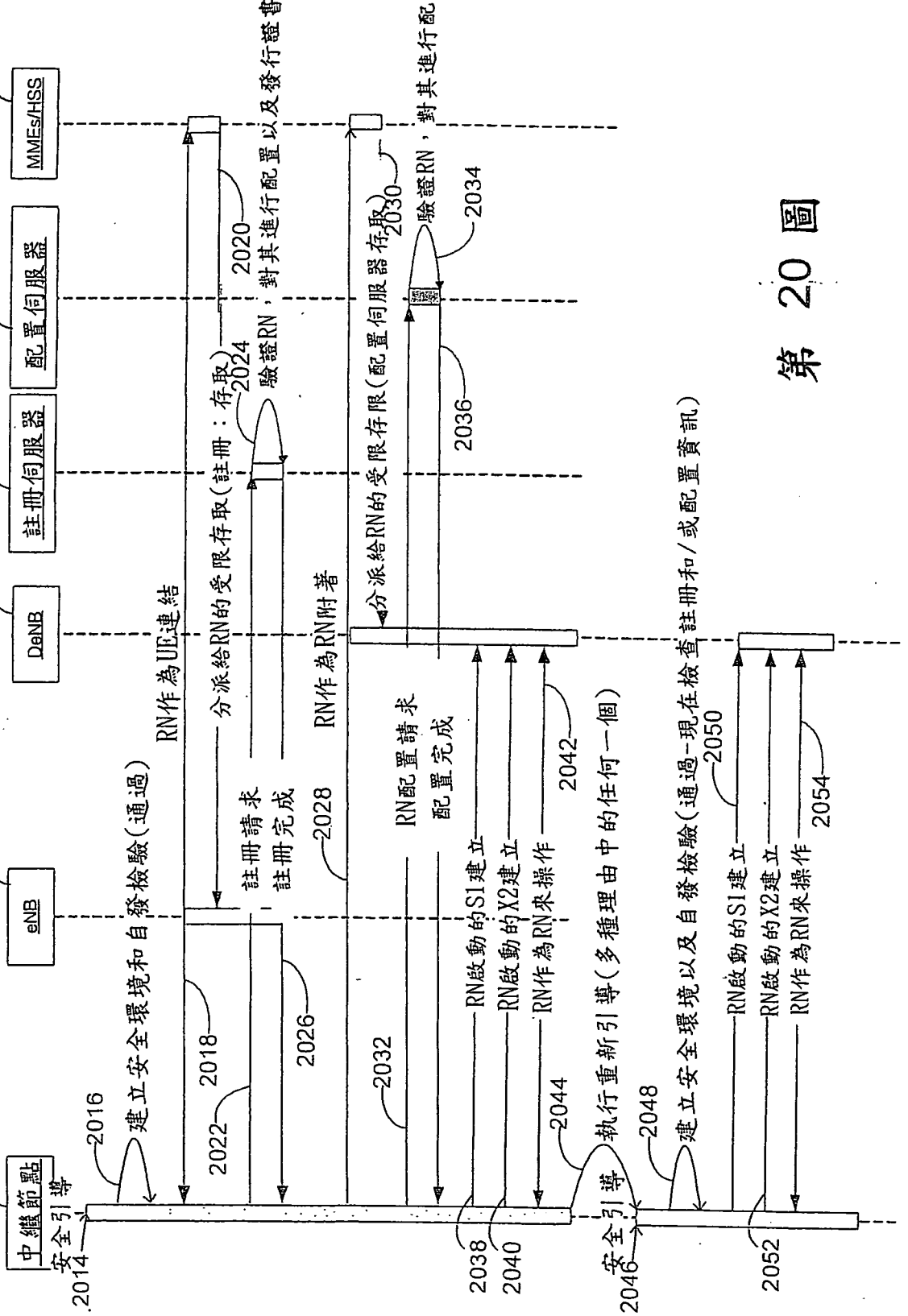
第 18A 圖


1802
具有TR-069代理的H(e)NB
1804
SeGW
1806
H(e)MS(具有TR-069的管理伺服器)
1808
網路檢驗實體
1810
軟體修復實體
安全引導
1814
完整性檢查(未通過SeGW操作，但是通過了H(e)MS操作)
具有故障報告的SeGW驗證(IKEv2)
1816
故障報告
1818
細粒度的存取決定(限於H(e)MS的H(e)NB存取)
1822b
驗證成功(但是SeGW限制存取)
1820
IP連接(SSL-TLS啟動)
1824
故障報告
1826
TR-069診斷/故障詢問
1828
確定執行軟體修復
代碼修復請求
1832
1834
軟體建構
1836
軟體修復
1838
IP連接(SSL-TLS啟動)
帶有重新引導的TR-069軟體/韌體管理程序
1840
1842
重新引導(或者載入和運行已更新的代碼)

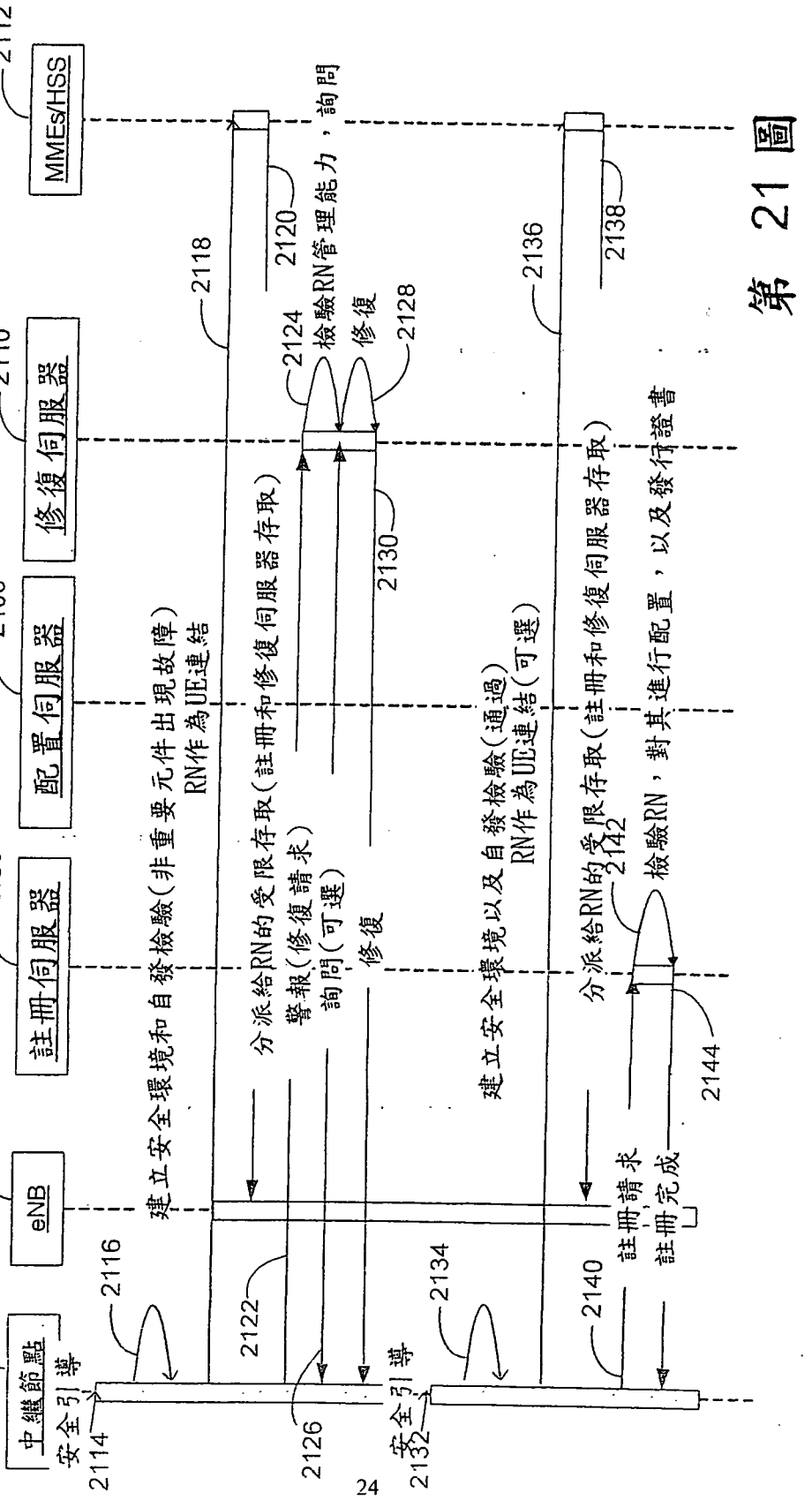
第 18B 圖


具有TR-069代理的H(e)NB
1902
SeGW
1904
H(e)MS(具有TR-069的管理伺服器)
1906
網路檢驗實體
1908
軟體修復實體
1910
安全引導
1912
完整性檢查(通過，但是發現了非重要軟體/參數的故障或是對於所述軟體/參數的需要)
1914
具有狀態報告的SeGW驗證(IKEv2)
1916
依照操作者策略的細粒度存取決定
1918
驗證成功
1922
狀態報告
1924
確定需要什麼軟體/參數
1926
代碼/參數更新請求
1928
軟體配置更新
1932
軟體建構
1930
轉發的軟體/配置更新
1934
IP連接(IKEv2/IPsec)
1936
非重要軟體的IKEv2和IPsec更新
1938

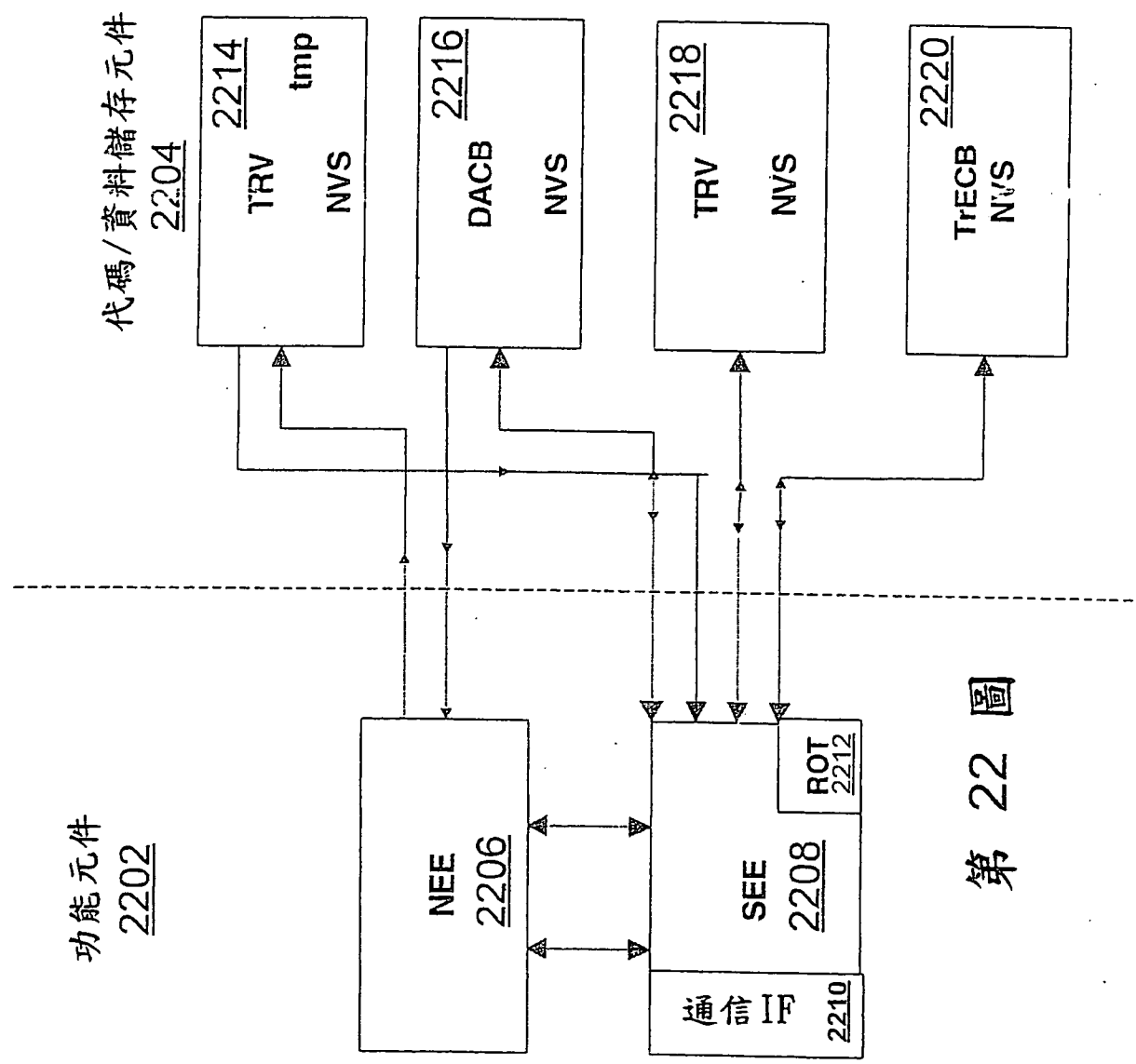
第 19 圖


中繼節點
eNB
DeNB
註冊伺服器
配置伺服器
MMEs/HSS
2002
2004
2006
2008
2010
2012
2014
安全引導
2016
建立安全環境和自發檢驗(通過)
2018
RN作為UE連結
2020
分派給RN的受限存取(註冊：存取)
2022
2024
驗證RN，對其進行配置以及發行證書
2026
註冊請求
註冊完成
2028
RN作為RN附著
2030
分派給RN的受限存取(配置伺服器存取)
2032
2034
驗證RN，對其進行配置以及發行證書
2036
RN配置請求
配置完成
2038
RN啟動的S1建立
2040
RN啟動的X2建立
2042
RN作為RN來操作
2044
執行重新引導(多種理由中的任何一個)
2046
安全引導
2048
建立安全環境以及自發檢驗(通過-現在檢查註冊和/或配置資訊)
2050
RN啟動的S1建立
2052
RN啟動的X2建立
2054
RN作為RN來操作

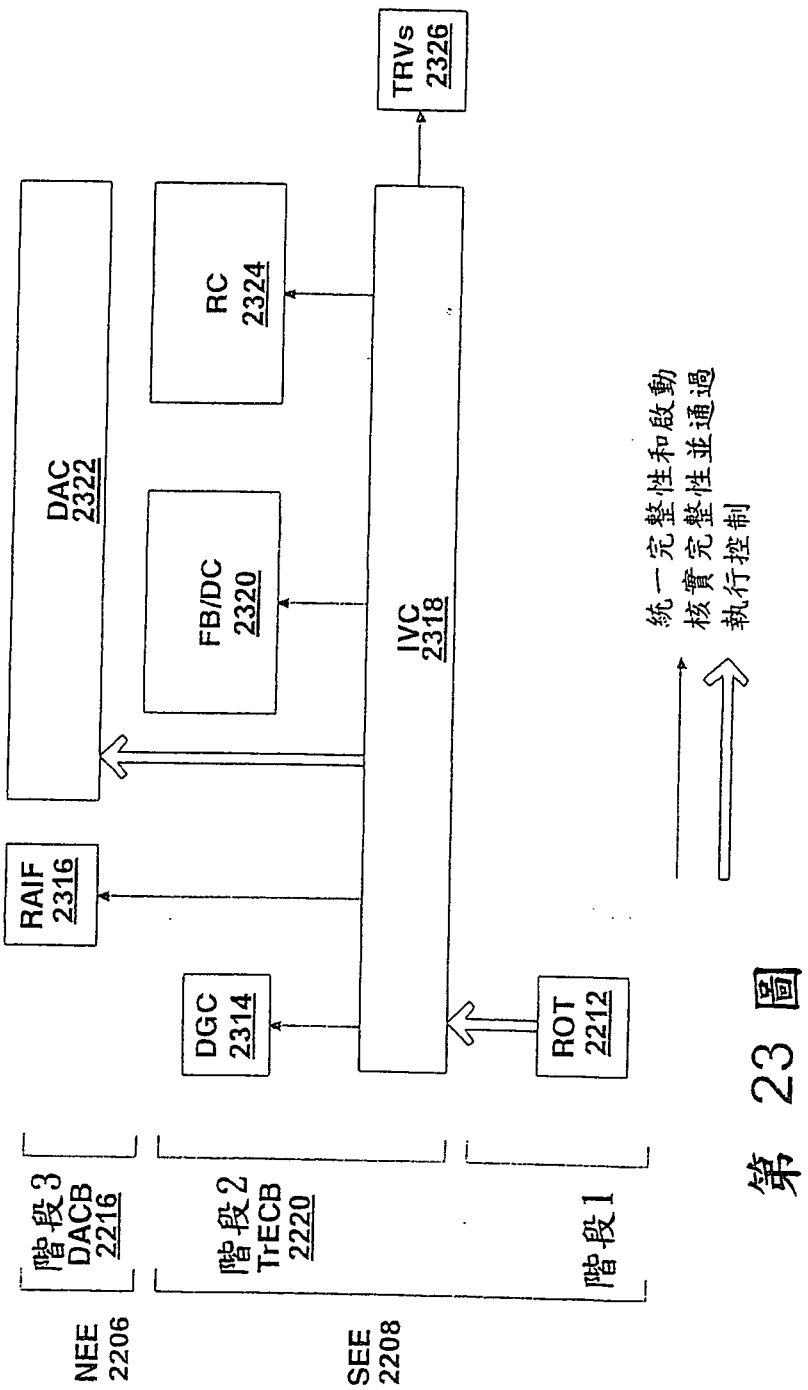
第 20 圖


中繼節點
2102
eNB
2104
註冊伺服器
2106
配置伺服器
2108
修復伺服器
2110
MMEs/HSS
2112
安全引導
2114
建立安全環境和自發檢驗(非重要元件出現故障)
RN作為UE連結
2116
2118
分派給RN的受限存取(註冊和修復伺服器存取)
警報(修復請求)
詢問(可選)
修復
2120
檢驗RN管理能力，詢問
2122
2124
修復
2126
2128
2130
安全引導
2132
建立安全環境以及自發檢驗(通過)
RN作為UE連結(可選)
2134
2136
分派給RN的受限存取(註冊和修復伺服器存取)
2138
2140
檢驗RN，對其進行配置，以及發行證書
2142
註冊請求
註冊完成
2144

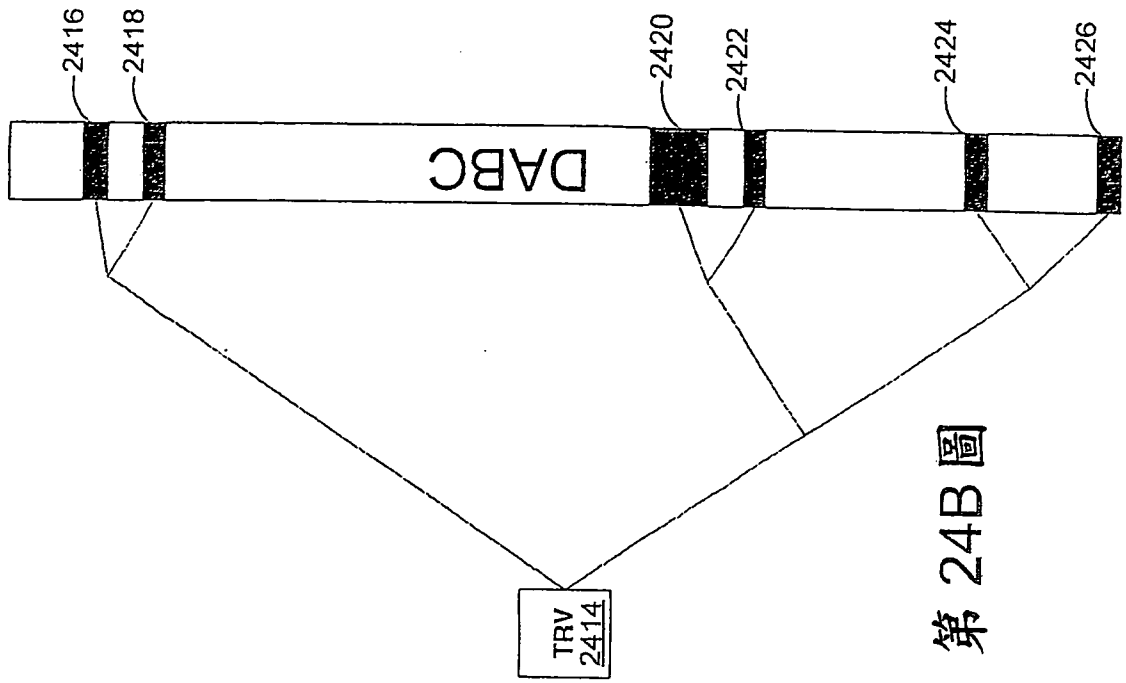
第 21 圖


代碼/資料儲存元件
2204
2214
TRV
tmp
NVS
2216
DACB
NVS
2218
TRV
NVS
2220
TrECB
NVS
功能元件
2202
NEE
2206
SEE
2208
ROT
2212
通信IF
2210

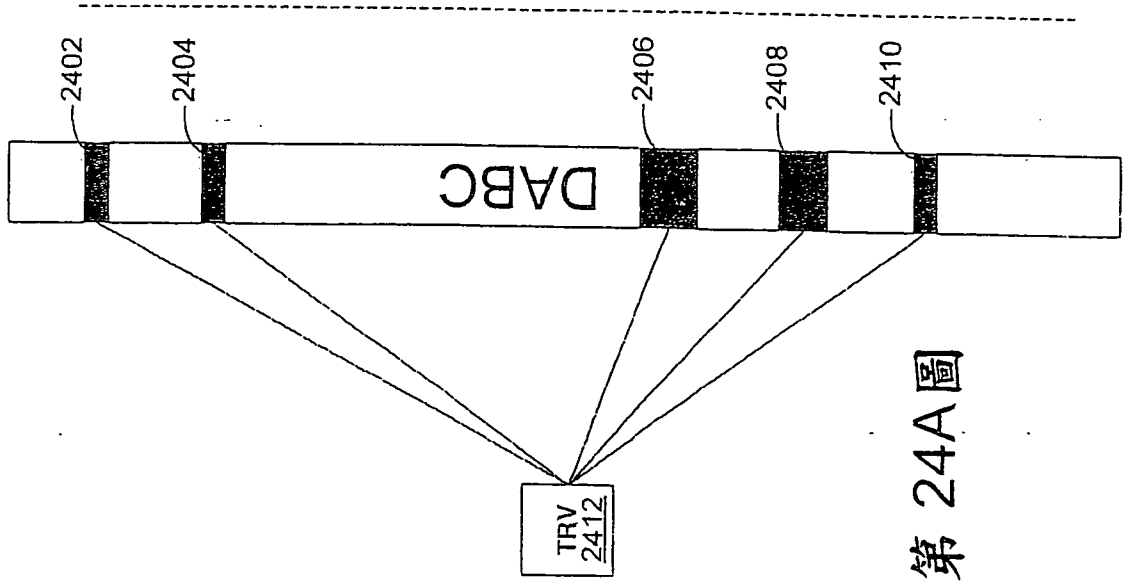
第 22 圖


TRVs 2326
RC 2324
DAC 2322
FB/DC 2320
IVC 2318
RAIF 2316
DGC 2314
ROT 2212
統一完整性和啟動
核實完整性並通過
執行控制
階段3 DACB 2216
階段2 TrECB 2220
階段1
NEE 2206
SEE 2208

第 23 圖


2416
2418
2420
2422
2424
2426
DABC
TRV
2414

第 24B 圖


2402
2404
2406
2408
2410
DABC
TRV
2412

第 24A 圖