



(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 I690173 B

(45)公告日：中華民國 109 (2020) 年 04 月 01 日

(21)申請案號：105112018

(22)申請日：中華民國 105 (2016) 年 04 月 18 日

(51)Int. Cl. : *H04L12/851 (2013.01)**H04L29/06 (2006.01)*

(30)優先權：2015/06/16 美國

62/180,433

2015/09/25 美國

14/866,565

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

美國

(72)發明人：索德 卡皮爾 SOOD, KAPIL (US)；奈德伯 曼紐爾 NEDBAL, MANUEL (AT)

(74)代理人：惲軼群；劉法正

(56)參考文獻：

CN 103458003A

US 2008/0005791A1

US 2010/0005504A1

US 2014/0053226A1

WO 2010/059893A1

審查人員：賴文能

申請專利範圍項數：29 項 圖式數：14 共 99 頁

(54)名稱

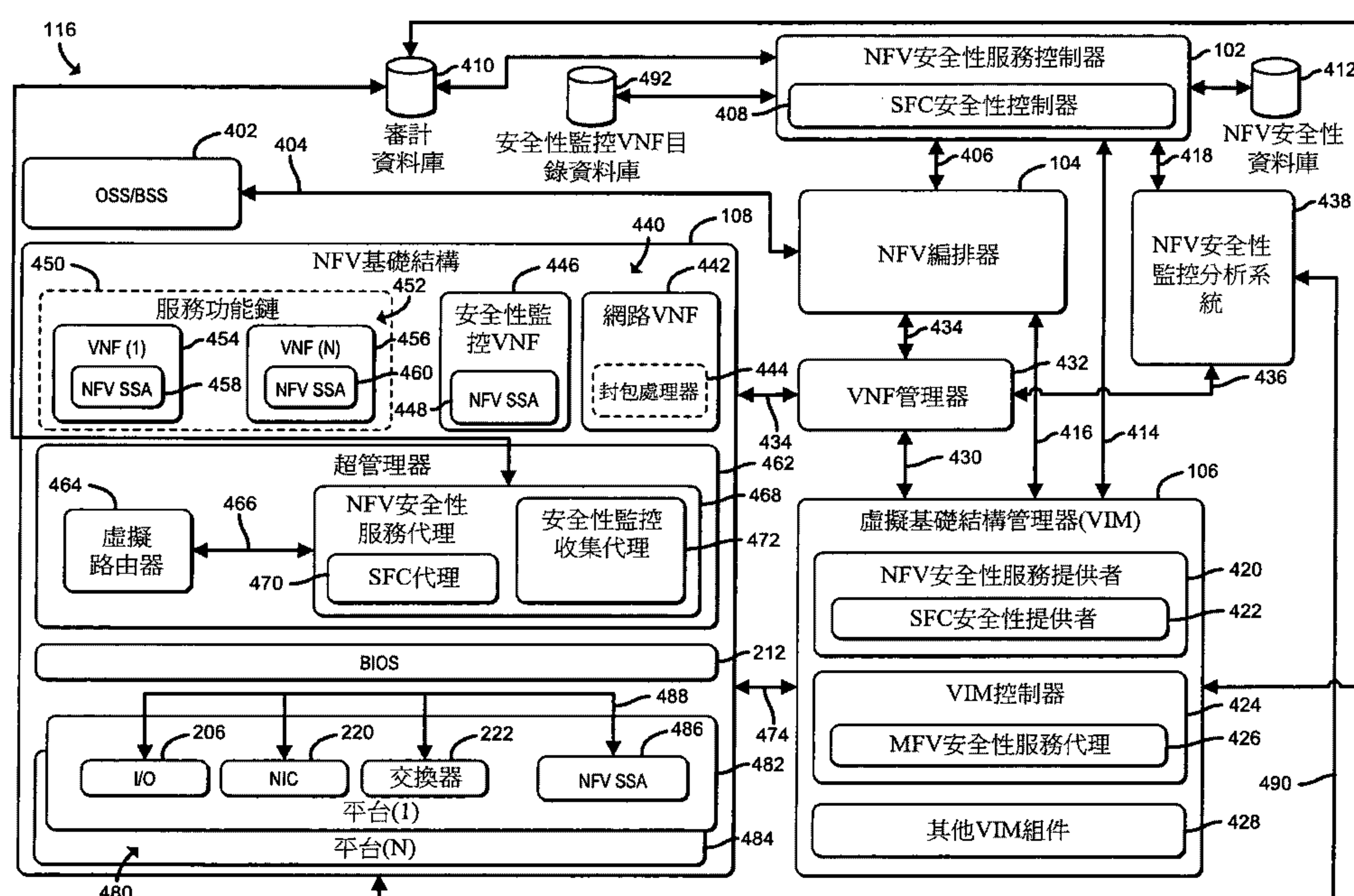
供安全性監控虛擬網路功能用的安全個人化之技術

(57)摘要

供一網路功能虛擬化(NFV)架構中之安全性監控虛擬網路功能(VNF)用的安全個人化之技術包括各種安全性監控組件，該等安全性監控組件包括一 NFV 安全性服務控制器、一 VNF 管理器及一安全性監控 VNF。該安全性監控 VNF 經組配以自該 NFV 安全性服務控制器接收佈建資料且使用該佈建資料之至少一部分執行一相互鑑別密鑰交換程序以建立該安全性監控 VNF 與一 VNF 管理器之間的一安全通訊路徑。該安全性監控 VNF 經進一步組配以經由該安全通訊路徑自該 VNF 管理器接收個人化資料且執行一個人化操作以基於該個人化資料來組配該安全性監控 VNF 之一或多個功能。描述並主張其他實施例。

Technologies for secure personalization of a security monitoring virtual network function (VNF) in a network functions virtualization (NFV) architecture include various security monitoring components, including a NFV security services controller, a VNF manager, and a security monitoring VNF. The security monitoring VNF is configured to receive provisioning data from the NFV security services controller and perform a mutually authenticated key exchange procedure using at least a portion of the provisioning data to establish a secure communication path between the security monitoring VNF and a VNF manager. The security monitoring VNF is further configured to receive personalization data from the VNF manager via the secure communication path and perform a personalization operation to configure one or more functions of the security monitoring VNF based on the personalization data. Other embodiments are described and claimed.

指定代表圖：



符號簡單說明：

102 · · · NFV 安全
性服務控制器

104 · · · NFV 編排
器

106 · · · 虛擬基礎結構管理器(VIM)

108 · · · NFV 基礎
結構

116 · · · 網路功能虛
擬化(NFV)安全性架構206 · · · 輸入/輸出
(I/O)子系統

212 · · · 基本輸入/輸出系統(BIOS)

220 · · · 網路介面卡 (NIC)

222 · · · 交換器

402 · · · 操作支援系
統及商務支援系統

(OSS/BSS)

404 · · · 通訊頻道

406、414、416、

418、430、434、

436、466、474、

488、490 · · · 491

通訊頻道

408 · · · SFC 安全性
控制器

410 . . . 審計資料庫

412 . . . NFV 安全

性資料庫

420 · · · NFV 安全
性服務提供者

422 · · · SFC 安全性
提供者

424 · · · VIM 控制
器

426、448、458、

460、468、

486 . . . NFV 安全性服務代理

428 . . . VIM 組件

432 . . . VNF 管理器

438 . . . NFV 安全性監控分析系統

440 . . . NFVI

442 . . . 網路 VNF

444 . . . 封包處理器

446 . . . 安全性監控 VNF

450 . . . 服務功能鏈

452 . . . 服務功能鏈 VNF

454、456 . . . VNF

462 . . . 超管理器

464 . . . 虛擬路由器

470 . . . SFC 代理

472 . . . 安全性監控收集代理

480、482、

484 . . . 平台

492 . . . VSF 目錄資料庫

發明摘要

I690173※申請案號：105112018

※申請日：105.04.18

※IPC 分類：

【發明名稱】(中文/英文)

供安全性監控虛擬網路功能用的安全個人化之技術

TECHNOLOGIES FOR SECURE PERSONALIZATION OF A
SECURITY MONITORING VIRTUAL NETWORK FUNCTION

【中文】

供一網路功能虛擬化(NFV)架構中之安全性監控虛擬網路功能(VNF)用的安全個人化之技術包括各種安全性監控組件，該等安全性監控組件包括一NFV安全性服務控制器、一VNF管理器及一安全性監控VNF。該安全性監控VNF經組配以自該NFV安全性服務控制器接收佈建資料且使用該佈建資料之至少一部分執行一相互鑑別密鑰交換程序以建立該安全性監控VNF與一VNF管理器之間的一安全通訊路徑。該安全性監控VNF經進一步組配以經由該安全通訊路徑自該VNF管理器接收個人化資料且執行一個人化操作以基於該個人化資料來組配該安全性監控VNF之一或多個功能。描述並主張其他實施例。

【英文】

Technologies for secure personalization of a security monitoring virtual network function (VNF) in a network functions virtualization (NFV) architecture include various security monitoring components, including a NFV security services controller, a VNF manager, and a security monitoring VNF. The security monitoring VNF is configured to receive provisioning data from the NFV security services controller and perform a mutually authenticated key exchange procedure using at least a portion of the provisioning data to establish a secure communication path between the security monitoring VNF and a VNF manager. The security monitoring VNF is further configured to receive personalization data from the VNF manager via the secure communication path and perform a personalization operation to configure one or more functions of the security monitoring VNF based on the personalization data. Other embodiments are described and claimed.

【代表圖】

【本案指定代表圖】：第（4）圖。

【本代表圖之符號簡單說明】：

102...NFV安全性服務控制器	422..SFC安全性提供者
104...NFV編排器	424...VIM控制器
106...虛擬基礎結構管理器(VIM)	426 、 448 、 458 、 460 、 468 、
108.....NFV基礎結構	486...NFV安全性服務代理
116...網路功能虛擬化(NFV)安全性 架構	428...VIM組件
206...輸入/輸出(I/O)子系統	432...VNF管理器
212...基本輸入/輸出系統(BIOS)	438...NFV安全性監控分析系統
220...網路介面卡(NIC)	440...NFVI
222...交換器	442...網路VNF
402...操作支援系統及商務支援系統 (OSS/BSS)	444...封包處理器
404...通訊頻道	446...安全性監控VNF
406、414、416、418、430、434、436、454、456...VNF	450...服務功能鏈
466、474、488、490...安全通訊 頻道	452...服務功能鏈VNF
408...SFC安全性控制器	462...超管理器
410...審計資料庫	464...虛擬路由器
412...NFV安全性資料庫	470...SFC代理
420...NFV安全性服務提供者	472...安全性監控收集代理
	480、482、484...平台
	492...VSF目錄資料庫

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

(無)

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)

供安全性監控虛擬網路功能用的安全個人化之技術

TECHNOLOGIES FOR SECURE PERSONALIZATION OF A
SECURITY MONITORING VIRTUAL NETWORK
FUNCTION

【技術領域】

[0001]本發明係有關於供安全性監控虛擬網路功能用的安全個人化之技術。

【先前技術】

發明背景

[0002]網路業者及服務提供者通常依賴於各種網路虛擬化技術來管理複雜的大規模計算環境，諸如高效能計算(high-performance computing，HPC)及雲端計算環境。舉例而言，網路業者及服務提供者網路可依賴於網路功能虛擬化(NFV)部署來部署網路服務(例如，防火牆服務、網路位址轉譯(network address translation，NAT)服務、負載平衡服務、深度封包檢測(deep packet inspection，DPI)服務、傳輸控制協定(transmission control protocol，TCP)最佳化服務等)。此等NFV部署通常使用NFV基礎結構來編排各種虛擬機器(virtual machine，VM)，以對網路訊務執行虛擬化網路服務(通常被稱作虛擬化網路功能(VNF))且跨各種VM管理網路訊務。

[0003]不同於傳統的非虛擬化部署，虛擬化部署將網路功能與基礎硬體解耦，此產生高度動態且大體上能夠在具有通用處理器之現成伺服器上執行之網路功能及服務。因而，VNF可基於將對網路訊務執行之特定功能或網路服務而視需要相應縮小/相應放大。然而，存取監控傳統的非虛擬化部署之功能組件之間的網路訊務之處理的曝露介面(例如，經由探測器之存取介面)之傳統手段就VNF部署中之存取而言並無不同。舉例而言，歐洲電信標準協會(European Standards Institute, ETSI)的NFV產業規範群組已公佈許多虛擬化模型，其中此等存取/監控介面可能不明確。此外，於各種部署中(例如，在VNF內、在VNF之間等)可獲得的不同存取介面之數目可使得難以探查關於VNF之所要資訊。舉例而言，某些部署可實施供應商專屬的非標準化介面以便最佳化處理能力且減小可能限制存取可用性的由發信引起之潛時。

【發明內容】

[0004]依據本發明之一實施例，係特地提出一種用於執行一網路功能虛擬化(NFV)架構中之安全性監控的安全性監控虛擬網路功能(VNF)，該安全性監控VNF包含：一或多個處理器；及一或多個記憶體裝置，其中儲存有多個指令，該多個指令在由該一或多個處理器執行時使該安全性監控VNF用以：接收來自與該安全性監控VNF網路通訊的該NFV架構之一NFV安全性服務控制器的佈建資料；使用該佈建資料之至少一部分執行與該NFV架構之一VNF管理器

之一相互鑑別密鑰交換程序，以建立在該安全性監控VNF與該VNF管理器之間的一安全通訊路徑；經由該安全通訊路徑接收來自該VNF管理器之個人化資料，其中該個人化資料包括可用以組配該安全性監控VNF之一或多個安全性功能的資料；以及執行一個人化操作以基於該個人化資料來組配該安全性監控VNF。

【圖式簡單說明】

[0005]在隨附諸圖中藉由實例而非限制來說明本文中所描述之概念。為說明簡單及清晰起見，諸圖中所說明之元件未必按比例繪製。在認為適當之處，已在諸圖當中重複參考標號以指示對應或類似元件。

圖1為用於監控網路功能虛擬化(NFV)安全性架構處所處理的網路通訊之安全性的系統之至少一個實施例的簡化方塊圖，NFV安全性架構包括NFV基礎結構之一或多個計算節點；

圖2為圖1之系統之NFV基礎結構的計算節點中之一者之至少一個實施例的簡化方塊圖；

圖3為圖1之系統之端點裝置之至少一個實施例的簡化方塊圖；

圖4為圖1之系統之NFV安全性架構之至少一個實施例的簡化方塊圖；

圖5為圖1及圖4之NFV安全性架構之NFV安全性服務控制器的環境之至少一個實施例的簡化方塊圖；

圖6為圖4之NFV安全性架構之NFV安全性服務代理的

環境之至少一個實施例的簡化方塊圖；

圖7為可由圖5之NFV安全性服務控制器執行的用於管理安全性監控服務之方法之至少一個實施例的簡化流程圖；

圖8為可由圖5之NFV安全性服務控制器執行的用於更新安全性監控策略之方法之至少一個實施例的簡化流程圖；

圖9為用於初始化圖4之NFV安全性服務代理中之一者的通訊流程之至少一個實施例的簡化流程圖；

圖10為可由圖4之NFV安全性服務代理中之一或多者執行的用於監控圖1之NFV網路架構之安全性的方法之至少一個實施例的簡化流程圖；

圖11為用於監控圖1之NFV網路架構之服務功能鏈接(SFC)之安全性的通訊流程之至少一個實施例的簡化流程圖；

圖12為圖1及圖4之NFV安全性架構之安全性監控VNF的環境之至少一個實施例的簡化方塊圖；

圖13為用於佈建圖1之NFV網路架構之安全VNF個人化及策略協定的通訊流程之至少一個實施例的簡化流程圖；
且

圖14為用於更新圖12之安全VNF個人化及策略協定的通訊流程之至少一個實施例的簡化流程圖。

【實施方式】

較佳實施例之詳細說明

[0006]雖然本發明之概念易受各種修改及替代形式影響，但該等概念之特定實施例已在圖式中藉由實例展示，且將在本文中加以詳細描述。然而，應理解，不欲將本發明之概念限於所揭示的特定形式，而是相反，意欲涵蓋與本發明及所附申請專利範圍一致的所有修改、等效物及替代物。

[0007]本說明書中對「一個實施例」、「一實施例」、「一示例性實施例」等之引用指示所描述實施例可包括一特定特徵、結構或特性，但每一實施例可以或可能未必包括該特定特徵、結構或特性。此外，此等短語未必指相同實施例。此外，當結合一實施例來描述一特定特徵、結構或特性時，應主張，無論是否予以明確描述，結合其他實施例來實現此特徵、結構或特性在熟習此項技術者之認識範圍內。另外，應瞭解，以「A、B及C中之至少一者」之形式包括於清單中之項目可意謂(A)；(B)；(C)；(A及B)；(A及C)；(B及C)；或(A、B及C)。類似地，以「A、B或C中之至少一者」之形式列出的項目可意謂(A)；(B)；(C)；(A及B)；(B及C)；(A及C)；或(A、B及C)。

[0008]在某些狀況下，所揭示實施例可以硬體、軟體、軟體或其任何組合來實施。所揭示實施例亦可實施為由一或多個暫時或非暫時性機器可讀(例如，電腦可讀)儲存媒體攜載或儲存於一或多個暫時或非暫時性機器可讀(例如，電腦可讀)儲存媒體上的指令，該等指令可由一或多個處理器讀取並執行。機器可讀儲存媒體可體現為用於儲存或傳輸

呈機器可讀之形式之資訊的任何儲存裝置、機構或其他實體結構(例如，依電性或非依電性記憶體、媒體光碟或其他媒體裝置)。

[0009]在圖式中，一些結構或方法特徵可以特定安排及/或次序來展示。然而，應瞭解，可能不需要此等特定安排及/或次序。確切而言，在一些實施例中，此等特徵可以不同於例示性諸圖中所展示之方式及/或次序的方式及/或次序安排。另外，特定圖中包括結構或方法特徵不意謂，暗示此特徵為所有實施例中所需的，且在一些實施例中，可不包括此特徵或此特徵可與其他特徵組合。

[0010]現參看圖1，在一例示性實施例中，用於監控網路通訊之安全性的系統100包括網路功能虛擬化(NFV)安全性架構116以處理一端點裝置118與另一端點裝置120之間的網路通訊。NFV安全性架構116包括許多網路處理組件，包括NFV編排器104、虛擬基礎結構管理器(virtual infrastructure manager, VIM) 106及NFV基礎結構108。應瞭解，在一些實施例中，NFV安全性架構116可包含額外及/或替代網路處理組件(實體的及/或虛擬的)以對網路訊務資料(例如，網路訊務有效負載、網路封包標頭等)執行處理功能(例如，分析、網路功能等)。

[0011]另外，NFV安全性架構116包括許多安全性監控組件，包括NFV安全性服務控制器102。在使用中，NFV安全性服務控制器102管理NFV安全性架構116中的各種安全性監控組件，該等安全性監控組件執行遙測資料之主動式

及/或被動式監控。為進行管理，NFV安全性服務控制器102執行個體化許多NFV安全性服務代理(參見，例如，圖4之NVF安全性服務代理468)以基於藉由NFV安全性服務控制器102(參見，例如，圖4之超管理器462)管理之安全性策略進行監控。該等NFV安全性服務代理另外經組配以收集、封裝且安全地傳輸遙測資料以用於分析。

[0012]藉由NFV安全性服務代理中之每一者收集的遙測資料可體現為或以其他方式包括可加以執行安全性分析的任何類型之資料。舉例而言，例示性遙測資料包括NFV安全性服務代理駐留所在之組件各自的組件層級組配、操作及策略資料及關於彼組件的經處理之網路訊務資料。如下文所更詳細論述，該等NFV安全性服務代理經組配以封裝資訊且將經封裝資訊安全地傳傳送至NFV安全性監控分析系統(參見，例如，圖4之NFV安全性監控分析系統438)。在使用中，NFV安全性監控分析系統判定是否任何威脅及/或異常存在於遙測資料中。NFV安全性監控分析系統另外為NFV安全性服務控制器102提供修復安全性策略以解決任何偵測到之威脅及/或異常。作為回應，NFV安全性服務控制器102基於修復安全性策略來更新用於NFV安全性服務代理之安全性策略且在NFV安全性服務代理中施行經更新的安全性策略。

[0013]如下文將更詳細地描述，NFV基礎結構108包括能夠管理(例如，建立、移動、破壞等)經組配以作為虛擬化網路功能(VNF)執行個體而操作之許多虛擬機(VM)的一或

多個計算節點110。VNF執行個體或VNF中之每一者通常依賴於一或多個VM，VM可執行不同軟體及/或處理程序以對網路訊務執行網路服務(例如，防火牆服務、網路位址轉譯(NAT)服務、負載平衡服務、深度封包檢測(DPI)服務、傳輸控制協定(TCP)最佳化服務、入侵偵測服務等)。此外，為提供某些網路服務，多個VNF可建立為服務功能鏈或VNF轉遞圖(亦即，以有序序列執行以實施所要網路服務的一系列VNF)。

[0014]NFV安全性架構116之網路及安全性監控組件可以各種虛擬化網路架構(諸如，虛擬演進型封包核心(virtual Evolved Packet Core，vEPC)基礎結構、虛擬化用戶端設備(virtualized Customer Premise Equipment，vCPE)基礎結構或任何其他類型之操作員可視化基礎結構)來部署。應瞭解，視NFV安全性架構116部署所在之網路架構而定，NFV安全性架構116可包括一或多個NFV安全性服務控制器102、一或多個NFV編排器104、一或多個VIM 106及/或一或多個NFV基礎結構108。

[0015]NFV安全性服務控制器102可體現為或另外包括能夠執行本文中所描述之功能(諸如，管理NFV安全性架構116之安全性監控組件)的任何類型之硬體、軟體及/或韌體。如下文將更詳細地描述，NFV安全性服務控制器102經組配以充當安全性監控編排器。為此，NFV安全性服務控制器102經組配以傳輸包括各種監控規則之安全性監控策略，其可包括安全性監控策略、安全通訊路徑策略、組配

參數及功能描述符以向遍佈NFV安全性架構116中之安全性監控組件(例如，圖4之NFV安全性服務代理)指示要監控何種遙測資料及如何組配安全性監控組件。NFV安全性服務控制器102另外經組配以施行遍佈NFV安全性架構116傳輸之安全性監控策略。各種安全性功能可包括(但不限於)保全服務功能鏈接(service function chaining, SFC)佈建、施行SFC安全性組配及監控、提供機密性受保護符記、管理受保護策略傳輸及提供VNF間SFC路徑保護。

[0016]爲了擷取及/或更新安全性監控策略，NFV安全性服務控制器102可經組配以與一或多個外部安全性系統(例如，Intel®安全性控制器)、安全性資料庫(參見圖4之NFV安全性資料庫412)及/或安全性策略引擎介接。爲了與外部安全性系統通訊，NFV安全性服務控制器102可將應用程式設計介面(application programming interface, API)及/或安全性策略傳遞至外部安全性服務編排系統。在一些實施例中，NFV安全性服務控制器102可充當受信任第三方以跨NFV安全性架構116之各種網路及安全性監控組件鑑認訊息。

[0017]此外，NFV安全性服務控制器102經組配以管理一或多個安全性監控VNF或虛擬安全性功能(VSF) VNF、部署至虛擬化環境中從而建立一組虛擬安全性裝置。因此，NFV安全性服務控制器102可經組配以根據前述安全性策略而在NFV安全性架構116中維持始終如一的狀態。安全性監控VNF (參見，例如，下文所更詳細描述的圖4之安全性

監控VNF 446)為特製(purpose-built)的安全性虛擬器具，其能夠與NFV安全性服務控制器102互動。

[0018]舉例而言，安全性監控VNF可為防火牆、入侵偵測/阻止系統、反惡意程式碼、沙箱、安全性識別碼管理器、資料損失預防或用以部署NFV安全性架構116之組件的任何其他安全性功能。因此，NFV安全性服務控制器102可經組配以曝露可藉由NFV安全性服務控制器102編排的安全性功能之目錄、在VIM 106登記安全性監控VNF、管理安全性監控VNF之執行個體、配對安全性監控VNF與其各別VNF管理器(例如，圖4之VNF管理器432)、個人化安全性監控VNF、管理安全性策略，以及執行完整性確證(integrity assertion)、憑證管理，促進多個安全性監控VNF至分散式器具中之集群，以及針對故障及修復來監控安全性監控VNF。應瞭解，由於安全性監控VNF為VNF，因此每一安全性監控VNF與特定VNF管理器相關聯，安全性監控VNF可連接至特定VNF管理器以在安全具現化(例如，安全性監控VNF之安全啟動)後接收策略及其他資料(例如，惡意程式碼之簽章等)。

[0019]在一些實施例中，安全性監控VNF可被視為均勻叢集。因而，與哪個安全性監控VNF執行個體看到某一類型之工作負載訊務無關，可在VNF管理器上定義均勻結果。因此，經更新策略可傳播至個別安全性監控VNF。在此等實施例中，NFV安全性服務控制器102可確證安全性監控VNF之完整性且管理安全性監控VNF執行個體之間的其

他通用性，包括憑證、裝置設定及/或其他操作態樣。在一些實施例中，此完整性確證及管理可以自動方式執行。因此，NFV安全性服務控制器102可管理跨NFVI（例如，圖4之NFVI 440）內之多個實體主機或跨分散式NFVI部署的多個安全性監控VNF執行個體。

[0020]應瞭解，在採用動態佈建之此等實施例中，安全性監控VNF執行個體可以相應縮小/相應放大之方式藉由VIM 106部署。替代地，在採用預先佈建安全性監控之此等實施例中，安全性監控VNF執行個體可靜態地部署至NFV基礎結構108中。另外，部署策略可用以判定什麼類型之安全性監控VNF執行個體、多少安全性監控VNF執行個體等將動態地部署或預先部署至NFV基礎結構108中。因此，NFV安全性服務控制器102經組配以確保安全性監控VNF執行個體係根據部署策略來部署。

[0021]NFV安全性服務控制器102可經進一步組配以監控安全性監控VNF之健康，且在判定安全性監控VNF之健康可能有損NFV安全性架構116之一或多個組件的安全性完整性後立即採取校正動作（例如，建立新的安全性監控VNF、終止現有VNF、更新安全性策略等）。因此，NFV安全性服務控制器102可經組配以自安全性監控VNF接收故障偵測及校正選項。因而，NFV安全性服務控制器102可組配將自動採用之動作。

[0022]應瞭解，在一些實施例中，NFV安全性服務控制器102可與NFV編排器104共置，諸如在NFV管理及編排

(management and orchestration, MANO)架構性架構中。應進一步瞭解，在一些實施例中，NFV安全性服務控制器102可具有高於NFV安全性架構116之其他網路及安全性監控組件的安全性特權，以確保NFV安全性服務控制器102之完整性及安全性。

[0023]NFV編排器104可體現為能夠執行本文中所描述之功能的任何類型之電路系統及/或硬體、軟體及/或韌體組件，該等功能諸如經由VNF管理器(參見圖4)來管理VNF之生命週期(例如，具現化、相應縮小/相應放大、效能量測結果、事件相關、終止等)、管理全域資源、驗證及授權NFV基礎結構108之資源請求、裝載新VNF及/或管理用於VNF之各種策略及封裝。舉例而言，NFV編排器104可經組配以接收來自影響特定VNF之操作員的資源請求。在使用中，NFV編排器104基於操作員請求來管理任何可應用處理、儲存及/或網路組配調整，以使VNF開始操作或遵守資源請求。一旦在操作中，NFV編排器104可針對可藉由NFV編排器104容量及利用率來監控VNF，容量及利用率可藉由NFV編排器104視需要調整。

[0024]VIM 106可體現為或以其他方式包括能夠執行本文中所描述之功能(諸如，控制及管理一個操作員之基礎結構子域內的NFV基礎結構108計算、儲存及網路資源(例如，實體的及虛擬的)，以及收集及轉遞效能量測結果及事件)的任何類型之硬體、軟體及/或韌體。應瞭解，在一些實施例中，NFV編排器104可與VIM 106共置，諸如在NFV架

構性架構中。

[0025]NFV基礎結構108可體現為或以其他方式包括任何類型之虛擬及/或實體處理及儲存資源，諸如一或多個伺服器或其他計算節點，以及虛擬化軟體。舉例而言，例示性NFV基礎結構108包括一或多個計算節點110。例示性計算節點110包括指明為計算節點(1) 112之第一計算節點，及指明為計算節點(N) 114之第二計算節點(亦即，計算節點110之「第N」計算節點，其中「N」為正整數且指明一或多個額外計算節點110)。

[0026]計算節點110可體現為能夠執行本文中所描述之功能的任何類型之計算或電腦裝置，包括(但不限於)伺服器(例如，獨立伺服器、機架式伺服器、刀鋒伺服器等)、網路器具(例如，實體的或虛擬的)、高效能計算裝置、網站器具、分散式計算系統、電腦、基於處理器之系統、多處理器系統、智慧型電話、平板電腦、膝上型電腦、筆記型電腦及/或行動計算裝置。如圖2中所示，在一實施例中，計算節點110中之每一者例示性地包括處理器202、輸入/輸出(I/O)子系統206、記憶體208、資料儲存裝置214、安全時鐘216及通訊電路系統218。當然，在其他實施例中，計算節點110可包括其他或額外組件，諸如通常存在於伺服器中之彼等組件(例如，各種輸入/輸出裝置)。另外，在一些實施例中，例示性組件其中之一或多者可併入於另一組件中或以其他方式形成另一組件之一部分。舉例而言，在一些實施例中，記憶體208或其部分可併入於處理器202中。

[0027]處理器202可體現為能夠執行本文中所描述之功能的任何類型之處理器。舉例而言，處理器202可體現為單個或多核心處理器、數位信號處理器、微控制器，或其他處理器或處理/控制電路。例示性處理器202包括一或多個受信任執行環境(trusted execution environment，TEE)支援204，或安全包體(secure enclave)支援(該等支援可由計算節點110在建立受信任執行環境時使用)。應瞭解，在一些實施例中，TEE支援204為受信任執行環境提供硬體加強型安全性，執行碼可在受信任執行環境中進行量測、驗證或以其他方式判定為可靠的。舉例而言，TEE支援204可體現為Intel®軟體保護擴充(Software Guard Extension，SGX)技術。儘管TEE支援204經例示性地展示於處理器202中，但應瞭解，在一些實施例中，計算節點110的其他組件中之一或多者可包括TEE支援204。此外，在一些實施例中，計算節點110之處理器202可包括安全性引擎(例如，下文所論述之安全性引擎224)、可管理性引擎，或經組配以利用TEE支援204來建立受信任執行環境的安全性共處理器。

[0028]記憶體208可體現為能夠執行本文中所描述之功能的任何類型之依電性或非依電性記憶體或資料儲存器。在操作中，記憶體208可儲存在計算節點110之操作期間所使用的各種資料及軟體，諸如作業系統、應用程式、程式、程式庫及驅動程式。記憶體208經由I/O子系統206通訊地耦接至處理器202，該I/O子系統可體現為電路系統及/或組件以藉由計算節點110之處理器202、記憶體208及其他組件來

促進輸入/輸出操作。舉例而言，I/O子系統206可體現為或以其他方式包括記憶體控制器集線器、輸入/輸出控制集線器、韌體裝置、通訊連結(亦即，點對點連結、匯流排連結、電線、纜線、光導、印刷電路板跡線等)及/或其他組件及子系統以促進輸入/輸出操作。

[0029]例示性記憶體208包括安全記憶體210。<0> 在一些實施例中，安全記憶體210可體現為記憶體208之安全分區；而，在其他實施例中，安全記憶體210可體現於或包括於計算節點110之單獨硬體組件上。<0>如本文中所描述，安全記憶體210可儲存供應至計算節點110之各種資料。舉例而言，安全記憶體210可儲存計算節點110之安全密鑰(例如，證明密鑰、專用直接匿名證明(direct anonymous attestation，DAA)密鑰、增強型隱私識別(Enhanced Privacy Identification，EPID)密鑰，或任何其他類型之安全/密碼編譯密鑰)，該安全密鑰可由晶片組及/或受信任執行環境之製造商供應。安全記憶體210亦可儲存(例如)藉由計算節點110之(original equipment manufacturer，OEM)供應於其中的計算節點110之密碼、PIN或其他唯一識別符。當然，應瞭解，安全記憶體210可視特定實施例而儲存各種其他資料(例如，群組名稱、裝置識別符、白名單、期望PIN值等)。在一些實施例中，供應之資料可儲存於安全記憶體210之唯讀記憶體中。

[0030]例示性記憶體208另外包括基本輸入/輸出系統(basic input / output system，BIOS) 212。BIOS 212包括用以

在開機過程期間初始化計算節點110的指令(例如，計算節點110之開機期間所使用的BIOS驅動程式)。在一些實施例中，計算節點110可經由主平台韌體或預開機韌體(諸如，Intel®平台晶片組之擴充，或基於統一可延伸韌體介面(Unified Extensible Firmware Interface，「UEFI」)規範之平台BIOS 212)來促進VNF之編排，UEFI規範具有藉由統一EFI論壇公佈之若干版本。

[0031]資料儲存裝置214可體現為經組配以用於短期或長期資料儲存的任何類型之一或多個裝置，諸如記憶體裝置及電路、記憶卡、硬碟機、固態磁碟機或其他資料儲存裝置。在使用中，如下所述，資料儲存裝置214及/或記憶體208可儲存安全性監控策略、組配策略或其他類似資料。

[0032]安全時鐘216可體現為能夠提供安全時序信號且另外執行本文中所描述之功能的任何硬體組件或電路系統。舉例而言，在例示性實施例中，安全時鐘216可產生獨立的且功能上與計算節點110之其他時脈源無關的時序信號。因此，在此等實施例中，安全時鐘216可不受藉由其他實體(諸如，在計算節點110上執行之軟體)作出之更改影響或抵制該更改。應瞭解，在一些實施例中，安全時鐘216可體現為獨立組件或電路系統，而在其他實施例中，安全時鐘216可與另一組件(例如，處理器202)之安全部分整合或形成另一組件(例如，處理器202)之安全部分。舉例而言，在一些實施例中，安全時鐘216可經由晶片上振盪器來實施及/或體現為可管理性引擎(manageability engine，ME)之安全

時鐘。應進一步瞭解，安全時鐘216可同步至其他計算節點110之安全時鐘，且粒度可具有可區分相異訊息時序之次序。

[0033]計算節點110之通訊電路系統218可體現為能夠視訊計算節點110與另一計算節點110、NFV編排器104、VIM 106、端點裝置118、120及/或其他已連接的具網路能力之計算節點之間的通訊的任何通訊電路、裝置或其集合。通訊電路系統218可經組配以使用任何一或多個通訊技術(例如，有線或無線通訊)及相關聯協定(例如，乙太網路、Bluetooth®、Wi-Fi®、WiMAX、GSM、LTE等)來實行此通訊。例示性通訊電路系統218包括網路介面卡(network interface card，NIC) 220及交換器222。NIC 220可體現為一或多個附加板、子卡、網路介面卡、控制器晶片、晶片組或可由計算節點110使用之其他裝置。舉例而言，NIC 220可體現為經由擴充匯流排(諸如，快速PCI)耦接至I/O子系統206之擴充卡。交換器222可體現為能夠執行網路交換器操作且另外執行本文中所描述之功能的任何硬體組件或電路系統，諸如乙太網路交換器晶片、快速PCI交換晶片等。

[0034]如上文所論述，計算節點110亦可包括安全性引擎224，其可體現為能夠在計算節點110上建立受信任執行環境(TEE)的任何硬體組件或電路系統。詳言之，安全性引擎224可支援執行碼及/或存取獨立的且不受藉由計算節點110執行之其他碼影響的資料。安全性引擎224可體現為受信任平台模組(Trusted Platform Module，TPM) (例如，實體

的或虛擬的)、可管理性引擎、帶外(out-of-band, OOB)處理器或其他安全性引擎裝置或裝置集合。在一些實施例中，安全性引擎224可體現為併入於計算節點110之系統單晶片(system-on-a-chip, SoC)中的聚合安全性及可管理性引擎(converged security and manageability engine, CSME)。

[0035]再次參看圖1，例示性NFV安全性架構116以通訊方式耦接在兩個端點裝置118、120之間。在例示性系統100中，第一端點裝置經指明為端點裝置(1) 118，且第二端點裝置經指明為端點裝置(2) 120。然而，應瞭解，經由NFV安全性架構116可連接任意數目之端點裝置。端點裝置118、120使用有線或無線技術經由網路(圖中未示)以通訊方式與NFV安全性架構116耦接，以形成端對端通訊系統，其中端點裝置(1)可與端點裝置(2)通訊，反之亦然。因此，NFV安全性架構116可監控並處理在端點裝置118、120之間傳輸的網路通訊訊務(亦即，網路封包)。

[0036]端點裝置118、120通訊所經由的網路可體現為任何類型之有線或無線通訊網路，包括蜂巢式網路(諸如全球行動通訊系統(GSM)或長期演進(LTE))、電話網路、數位用戶線(DSL)網路、電纜網路、區域或廣域網路、全球網路(例如，網際網路)或其任何組合。舉例而言，在一些實施例中，網路可體現為具有vEPC架構的基於NFV之長期演進(LTE)網路。應瞭解，網路可充當集中式網路，且在一些實施例中，可以通訊方式耦接至另一網路(例如，網際網路)。因此，網路可按需要包括多種網路裝置(虛擬的及實體的，諸如路

由器、交換器、網路集線器、伺服器、儲存裝置、計算裝置等)，以促進端點裝置118、120與NFV安全性架構116之間的通訊。

[0037]端點裝置118、120可體現為能夠執行本文中所描述之功能的任何類型之計算或電腦裝置，包括(但不限於)智慧型電話、行動計算裝置、平板電腦、膝上型電腦、筆記型電腦、電腦、伺服器(例如，獨立伺服器、機架式伺服器、刀鋒伺服器等)、網路器具(例如，實體的或虛擬的)、網絡器具、分散式計算系統、基於處理器之系統及/或多處理器系統。如圖3中所示，類似於圖2之計算節點110，例示性端點裝置(例如，圖1之端點裝置118、120中之一者)包括處理器302、輸入/輸出(I/O)子系統304、記憶體306、資料儲存裝置308、一或多個周邊裝置310及通訊電路系統312。因而，出於描述清楚起見，本文中不重複類似組件之另外描述，條件為上文關於計算節點110所提供之對應組件之描述同樣適用於端點裝置118、120之對應組件。

[0038]當然，端點裝置118、120可包括其他或額外組件，諸如通常存在於能夠在其他實施例中以電信基礎結構操作之行動計算裝置中之彼等組件(例如，各種輸入/輸出裝置)。另外，在一些實施例中，例示性組件中之一或多者可併入於另一組件中或以其他方式形成另一組件之一部分。周邊裝置310可包括任意數目之輸入/輸出裝置、介面裝置及/或其他周邊裝置。舉例而言，在一些實施例中，周邊裝置310可包括顯示器、觸控螢幕、圖形電路系統、鍵盤、滑

鼠、揚聲器系統及/或其他輸入/輸出裝置、介面裝置及/或周邊裝置。

[0039]現參看圖4，圖1的用於監控NFV安全性架構116之安全性的NFV安全性架構116之例示性實施例包括圖1之NFV安全性服務控制器102、NFV編排器104、VIM 106及NFV基礎結構108。例示性實施例116之每一安全性監控組件包括唯一地識別對應安全性監控組件之全域唯一安全性識別符。全域唯一安全性識別符可基於(例如)安全性監控組件之媒體存取控制(MAC)位址、指派給安全性監控組件之網際網路協定(IP)位址、嵌入至安全性監控組件之安全記憶體210中的識別符(例如，BIOS 212 (UEFI)識別符、安全性監控組件之作業系統的識別符等)。全域唯一安全性識別符可保護在實體TPM或基於軟體之受信任模組(諸如，安全性引擎224上之韌體TPM (例如，ME、聚合安全性及可管理性引擎(CSME)、創新引擎)、安全分區、安全性共處理器或獨立處理器核心等))內，及/或儲存於安全位置(例如，安全記憶體210)中。安全性監控組件中之任一者或其功能性可在安全環境(例如，處理器202之TEE支援204)中具現化。因而，每個具現化可藉由全域唯一安全性識別符來識別。此外，在一些實施例中，全域唯一安全性識別符可在具現化後立即結合至使用情況傳訊。

[0040]另外，每一唯一使用執行個體包括唯一使用識別符。因此，可唯一地識別NFV安全性架構116內之多個使用及流程，諸如用於審計、鑑認、控制、除錯等。如先前所

描述，在一些實施例中，NFV安全性架構116可包括NFV安全性服務控制器102、NFV編排器104及VIM 106之一或多個執行個體。在此等實施例中，組件之多個執行個體可成鏡像以使用相同外部識別符，且另外包括唯一內部識別符(例如，執行個體安全性識別符)以區分鏡像組件。

[0041]此外，NFV安全性架構116之每一邏輯組件可分隔成一個以上實體及/或邏輯組件以解決特定使用，諸如SFC策略、VNF間通訊密鑰、VIM控制器424策略等。在此等實施例中，實體及/或邏輯組件可與藉由操作員或雲端提供者提供之全域唯一識別符(GUID)一起標記，全域唯一識別符可在安裝之前驗證。該標記可使用私密密鑰來執行，其公用密鑰(例如，憑證密鑰、熔斷密鑰、裝置特定密鑰等)可嵌入至NFV基礎結構108中且可由NFV安全性服務代理存取。因此，驗證可在嚴格控制實體及/或邏輯組件之環境的情況下由NFV安全性服務代理執行。

[0042]NFV安全性服務控制器102係經由安全通訊頻道406以通訊方式耦接至NFV編排器104。如上文所論述，在一些實施例中，NFV安全性服務控制器102及NFV編排器104可共置，諸如在MANO架構性架構中。此外，NFV安全性服務控制器102係經由安全通訊頻道414以通訊方式耦接至VIM 106，且NFV編排器104係經由安全通訊頻道416以通訊方式耦接至VIM 106。NFV安全性架構116之安全通訊頻道406、414、416以及其他安全通訊頻道可用由NFV安全性服務控制器102使用以建立根信任(root of trust, RoT)之安

全密鑰(例如，工作階段密鑰及/或其他密碼編譯密鑰)來保護，以建立NFV安全性架構116之通訊頻道(例如，安全通訊頻道406、414、416)。在一些實施例中，安全密鑰可體現為可定期再新之成對工作階段密鑰。因而，NFV安全性服務控制器102可經組配以充當鑑認伺服器。

[0043]NFV安全性架構116另外包括操作支援系統及商務支援系統(OSS/BSS) 402，其經由通訊頻道404以通訊方式耦接至NFV編排器104。OSS/BSS 402可體現為能夠執行本文中所描述之功能(諸如，支援電話網路中之各種端對端電信服務)的任何類型之計算或計算節點。在一些實施例中，OSS/BSS 402可經組配以支援管理功能(諸如，網路清查、服務佈建、網路組配及故障管理)，以及用以支援可由OSS/BSS 402支援之端對端電信服務的各種商業功能(諸如，產品管理、客戶管理、收入管理、訂單管理等)。

[0044]如先前所描述，在使用中，NFV安全性服務控制器102跨NFV安全性架構116之各種安全性監控組件提供並施行安全性監控策略。為此，NFV安全性服務控制器102跨各別安全通訊頻道將安全性監控策略傳輸至NFV編排器104及VIM 106。NFV安全性服務控制器102係經由安全通訊頻道418另外以通訊方式耦接至NFV安全性監控分析系統438。

[0045]NFV安全性監控分析系統438 (其將在下文加以進一步描述)基於NFV安全性監控分析系統438在根據目前施行之安全性監控策略所接收的遙測資料之分析中是否已

偵測到安全性威脅(諸如攻擊(例如，拒絕服務(DoS)攻擊、攔截式攻擊、竊聽、資料修改攻擊等)或異常)而為NFV安全性服務控制器102提供修復策略(亦即，經更新的安全性監控策略)。因此，NFV安全性服務控制器102經組配以基於修復策略施行對安全性監控策略之任何更新，諸如藉由可採取以解決威脅或驗證異常之校正動作。舉例而言，校正動作可包括阻擋某一網路訊務(亦即，某些網路封包)、將某一網路訊務串流傳輸至深度封包檢測(DPI)VNF執行個體、速率限制或節制網路訊務等。因此，NFV安全性服務控制器102接著可將安全性策略更新傳輸至VIM 106之NFV安全性服務提供者420。

[0046]另外，例示性NFV安全性服務控制器102與如下三個邏輯安全資料庫介接：審計資料庫410、NFV安全性資料庫412及VSF目錄資料庫。審計資料庫410體現為安全資料庫，其包括關於NFV安全性架構116之各種安全性監控組件之安全性審計資訊。安全性審計資訊可包括組配改變記錄檔、網路軌跡、除錯軌跡、應用軌跡等。在例示性NFV安全性架構116中，審計資料庫410另外經組配以與NFV安全性架構116之其他網路及安全性監控組件介接，諸如VIM 106及跨NFV安全性架構116分佈之各種NFV安全性服務代理，該等組件將在下文加以更詳細論述。在一些實施例中，例示性NFV安全性架構116的與審計資料庫410介接之各種安全性監控組件可使用安全時鐘(例如，圖2之安全時鐘216)對接收於審計資料庫410處之遙測資料加時間戳記以達成

安全儲存。因此，NFV安全性服務控制器102可基於遙測資料之時間戳記來審計遙測資料(亦即，驗證遙測資料且對遙測資料排序)。

[0047]NFV安全性資料庫412體現為用於跨NFV安全性架構116 (亦即，跨NFV安全性架構116)部署安全性監控的安全資料庫。因此，NFV安全性資料庫412可包括安全性資料結構，諸如NFV用戶/租戶、SFC策略、SFC路徑保護策略、用於VIM 106 (例如，VIM控制器424)之控制器策略、NFV安全性監控策略及組配、NFV安全性佈建憑證(例如，用於保護SFC)服務功能鏈、VNF間策略、一或多個雲端作業系統安全性策略及/或租戶特定安全性策略。

[0048]VSF目錄資料庫492體現為安全資料庫，其包括用以添加及移除安全性監控VNF之指令的目錄，以及關於安全性監控VNF的元資料及資訊。換言之，VSF目錄資料庫492可充當安全性監控VNF之儲存庫。應瞭解，VSF目錄資料庫492可在安全性監控VNF「登記」至VSF目錄資料庫492後立即變得可用於編排。

[0049]如先前所描述，在使用中，NFV編排器104管理NFV基礎結構108中之VNF之生命週期，包括具現化、相應放大/縮小、量測效能、關聯事件、終止等。為進行管理，NFV編排器104經組配以經由安全通訊頻道434將指令提供至VNF管理器432，以基於NFV基礎結構108之資源來管理NFV基礎結構108之VNF (參見VNF執行個體440)之初始化及組配(亦即，按比例縮放及部署)。VNF管理器432經進一

步組配以執行總體協調及調適以用於NFV基礎結構108之組配及事件報告。VNF管理器432另外經組配以更新及確保VNF之完整性。為此，VNF管理器432經組配以經由安全通訊頻道430與VIM 106協商，以判定特定VNF執行個體進行執行個體化所在的可用實體資源。應瞭解，VIM 106可使用任何合適的技術、演算法及/或機制來作出此判定。應進一步瞭解，在一些實施例中，單一VNF管理器432可負責管理一或多個VNF執行個體。換言之，在一些實施例中，VNF管理器432可針對VNF執行個體中之每一者具現化。

[0050]亦如先前所描述，在使用中，VIM 106經由安全地經由安全通訊頻道474傳輸之訊息來控制且管理NFV基礎結構108之虛擬及硬體計算、儲存及網路資源的分配。另外，VIM 106可經組配以收集NFV基礎結構108之計算、儲存及網路資源(例如，實體的及虛擬的)之效能量測結果及事件且將該等效能量測結果及事件安全地轉遞至審計資料庫410。例示性VIM 106包括NFV安全性服務提供者420、VIM控制器424及許多VIM組件428。NFV安全性服務提供商420經組配以：經由安全通訊頻道414自NFV安全性服務控制器102接收安全性監控策略；跨NFV基礎結構108之各種安全性監控組件實施安全性監控策略；且基於接收自NFV安全性服務控制器102之安全性監控策略來佈建VNF執行個體(例如，VNF執行個體440之服務功能鏈VNF 452)。

[0051]另外，NFV安全性服務提供者420經組配以安全地與VIM 106及NFV基礎結構108之NFV安全性服務代理中

之一或多者通訊。舉例而言，VIM控制器424經組配以充當網路策略控制器或網路連接服務控制器，諸如軟體定義網路連接(SDN)控制器或開放式堆疊中子星(OpenStack Neutron)。VIM組件428可包括如安裝VNF執行個體及/或啟動服務可能需要的VIM 106之任何額外實體及/或虛擬計算、儲存及網路資源，諸如VNF影像管理控制器(例如，用於安裝及佈建VNF執行個體440之開放式堆疊新星(OpenStack Nova))。例示性VIM控制器424包括NFV安全性服務代理426，其經組配以收集VIM控制器424之遙測資料，諸如基於策略之資訊，以及自其他VIM組件428收集遙測資料。

[0052]NFV基礎結構108包括計算節點110之所有硬體及軟體組件(亦即，虛擬計算、儲存及網路資源、虛擬化軟體、硬體計算、儲存及網路資源等)，VNF可自該等計算節點部署。應瞭解，NFV基礎結構108之實體及/或虛擬組件可跨越不同位置、資料中心、地理、提供者等。另外，應進一步瞭解，NFV基礎結構108之組件用來通訊及介接的網路可被視為包括於NFV基礎結構108中。

[0053]例示性NFV基礎結構108包括一或多個平台480、圖2之BIOS 212、超管理器462及一或多個VNF執行個體440。例示性平台480包括指明為平台(1) 482之第一平台，及指明為平台(N) 482之第二平台(亦即，「第N」平台，其中「N」為正整數且指明一或多個額外平台)。平台480中之每一者包括圖2之I/O子系統206、NIC 220及/或交換器

222。例示性平台(1) 482另外包括NFV安全性服務代理486。NFV安全性服務代理486經組配以經由安全通訊頻道488在硬體層級(亦即，自I/O子系統206、NIC 220及/或交換器222)收集遙測資料。因此，藉由NFV安全性服務代理486收集之遙測資料可包括NIC組配資訊、各種硬體缺陷、錯誤及/或異常，及網路封包行為(例如，丟棄之封包)。在收集後，遙測資料立即安全地傳輸至NFV安全性監控分析系統438，諸如經由安全通訊頻道490。

[0054]在使用中，超管理器462或虛擬機監控器(VMM)執行VNF執行個體440，通常經由用於執行VNF執行個體440中之每一者的一或多個虛擬機(VM)及/或容器應用程式(container)。在一些實施例中，VNF執行個體440可包括虛擬交換器(vSwitch)、虛擬路由器(vRouter)、防火牆、網路位址轉譯(NAT)、DPI、演進型封包核心(EPC)、行動性管理實體(MME)、封包資料網路閘道器(PGW)、服務閘道器(SGW)、計費功能及/或其他虛擬網路功能。在一些實施例中，特定VNF執行個體440可具有多個子執行個體，該等子執行個體可在單一平台(例如，平台482)上或跨不同平台(例如，平台482及平台484)而執行。換言之，當虛擬化時，傳統上藉由與特定平台共置之實體硬體處置的網路功能可分散為跨平台480中之一或多者的許多執行個體440。VNF執行個體440中之每一者可包括任意數目之VNF，其中之每一者可包括一或多個VNF組件(VNFC)(圖中未示)。應瞭解，VNF執行個體440可體現為任何合適之虛擬網路功能；類似

地，VNFC可體現為任何合適之VNF組件。VNFC為合作以傳遞一或多個VNF執行個體440之功能性的處理程序及/或執行個體。舉例而言，在一些實施例中，VNFC可為VNF執行個體440之子模組。

[0055]類似於VNF執行個體440，應瞭解，VNFC可跨一或多個平台480分佈。此外，應瞭解，特定VNF執行個體440可跨多個平台480分佈且仍形成建立於平台480中之一者上的VNF執行個體440之一部分。在一些實施例中，VNF執行個體440及/或VNFC可在同一平台(例如，平台482或平台484)上執行或在同一資料中心內，但在不同平台480上。此外，在一些實施例中，VNF執行個體440及/或VNFC可跨不同資料中心執行。

[0056]超管理器462經組配以建立及/或利用NFV基礎結構108之各種虛擬化硬體資源(例如，虛擬記憶體、虛擬作業系統、虛擬網路連接組件等)。另外，超管理器462可促進跨VNF執行個體440及/或VNFC之通訊。例示性超管理器462包括經由安全通訊頻道466以通訊方式耦接至NFV安全性服務代理468之虛擬路由器464。NFV安全性服務代理468經組配以經由NFV安全性服務提供者420自NFV安全性服務控制器102接收安全性監控策略且實施該安全性監控策略。換言之，NFV安全性服務代理468經組配以基於安全性監控策略而執行主動式及/或被動式安全性監控。此外，NFV安全性服務代理468經組配以在NFV安全性服務代理468啟動後立即將監控及/或收集之網路訊務映射至安全性

監控策略。

[0057] 例示性NFV安全性服務代理468包括SFC代理程式(其將在下文另外描述)及安全性監控收集代理472。安全性監控收集代理472經組配以收集用於NFV安全性架構116之組件之遙測資訊，NFV安全性服務代理駐留於該組件處。在例示性NFV安全性服務代理468中，該組件為超管理器462，而對於NFV安全性服務代理486，該組件為平台482。應瞭解，儘管僅一個NFV安全性服務代理468展示安全性監控收集代理472及SFC代理470，但跨NFV安全性架構116分散的NFV安全性服務代理(例如，NFV安全性服務代理426、NFV安全性服務代理448、NFV安全性服務代理458、NFV安全性服務代理460及NFV安全性服務代理486)中之每一者可包括安全性監控收集代理及/或SFC代理之執行個體。NFV安全性服務代理468之安全性監控收集代理472經組配以在BIOS層級(亦即，在BIOS 212及/或超管理器462處)收集遙測資料。藉由安全性監控收集代理472收集之遙測資料被安全地傳輸至NFV安全性監控分析系統438，諸如經由安全通訊頻道490。

[0058] 例示性VNF執行個體440包括：網路VNF 442，其經組配以作為虛擬網路連接裝置(例如，vSwitch、vRouter、防火牆、NAT、DPI、EPC、MME、PGW、SGW等)而執行；安全性監控VNF 446，其經組配以充當專用監控代理；及服務功能鏈450，其包括能夠執行特定虛擬功能或服務之一或多個服務功能鏈VNF 452。應瞭解，在其他實

施例中，可部署額外及/或替代VNF執行個體。因而，應瞭解，儘管圖4之例示性NFV安全性架構116僅展示單一安全性監控VNF 446，但在其他實施例中可部署多個單一安全性監控VNF 446。

[0059]服務功能鏈450之例示性服務功能鏈VNF 452包括指明為VNF (1) 454之第一服務功能鏈VNF，及指明為VNF (N) 456之第二服務功能鏈VNF(亦即，「第N」服務功能鏈VNF，其中「N」為正整數且指明一或多個額外服務功能鏈VNF執行個體)。此外，例示性服務功能鏈VNF 452中之每一者包括NFV安全性服務代理之執行個體(亦即，VNF (1) 454之NFV安全性服務代理458及VNF (N) 456之NFV安全性服務代理460)。NFV安全性服務代理458、460中之每一者經組配以在虛擬環境層級收集遙測資料(亦即，自NFV安全性服務代理駐留所在的服務功能鏈VNF 452中之每一者收集VNF遙測資料)。儘管服務功能鏈450之例示性服務功能鏈VNF 452中之每一者包括NFV安全性服務代理458、460，但應瞭解，一些實施例，單一NFV安全性服務代理(例如，安全性監控VNF 446之NFV安全性服務代理448)可用以監控及收集遙測資料。

[0060]網路VNF 442可包括封包處理器444，其用以在使用者資料平面(諸如Intel®資料平面開發套件(Intel® DPDK))處理網路訊務。安全性監控VNF 446可包括NFV安全性服務代理(SSA) 448，其經組配以在虛擬環境層級收集遙測資料(亦即，自VNF執行個體440中之每一者收集VNF

遙測資料)。藉由NFV安全性服務代理448之安全性監控收集代理(圖中未示)收集之遙測資料被安全地傳輸至NFV安全性監控分析系統438，諸如經由安全通訊頻道490。

[0061]NFV安全性監控分析系統438經組配以經由安全通訊頻道490自各種NFV安全性服務代理安全地獲取關於NFV基礎結構108之遙測資料且經由安全通訊頻道436安全地獲取關於VNF管理器432之VNF組配資料。VNF組配資料可包括藉由每一NFV提供的具現化NFV之數目、已啟動NFV之數目、功能或服務或功能或服務之部分等。因此，NFV安全性監控分析系統438可分析遙測資料及VNF組配資料以偵測是否存在任何威脅及/或異常。在一些實施例中，NFV安全性監控分析系統438可分析遙測資料及VNF組配資料以產生遙測圖案，安全性威脅可自該等遙測圖案識別。NFV安全性監控分析系統438經進一步組配以將修復策略(亦即，經更新的安全性監控策略)傳遞至安全性監控組件以供回應於已偵測到安全性威脅而施行。

[0062]例示性NFV安全性架構116包括經特定組配以監控NFV基礎結構108內所執行之服務功能鏈之安全性的許多安全性監控組件。該等服務功能鏈接(SFC)安全性監控組件包括NFV安全性服務控制器102之SFC安全性控制器408、VIM 106之NFV安全性服務提供者420之SFC安全性提供者422，及遍佈NFV基礎結構108分佈的許多SFC代理。NFV安全性架構116之SFC安全性監控組件經相互鑑認以用於安全通訊，且可在安全之經驗證開機後建置。因此，NFV

安全性架構116之SFC安全性監控組件可跨不同地理、跨不同代管資料中心及/或在不可信網路中部署。此外，NFV安全性架構116之SFC安全性監控組件可安全地佈建在NFV安全性架構116內。

[0063]舉例而言，該等SFC安全性監控組件可在於頂上執行各種VNF的控制平面、管理平面及/或資料平面上執行，諸如在vEPC架構內。在一些實施例中，執行階段SFC特定安全性監控策略可藉由發生在一個平面上之事件觸發，而基於安全性監控策略所執行之安全性監控可在彼平面上及/或其他平面中之一個或兩個平面上起始。舉例而言，事件可在控制平面中(諸如，藉由惡意或畸形網路封包)觸發，且修復策略可包括SFC監控及網路資料封包收集以用於跨控制平面、管理平面及資料平面匹配事件觸發網路封包。

[0064]SFC安全性控制器408經組配以跨NFV基礎結構108編排SFC安全性策略。為此，SFC安全性控制器408經組配以與NFV安全性資料庫412通訊以存取SFC安全性策略及憑證。SFC安全性策略及憑證可包括任何類型之安全性策略，諸如輸送策略(亦即，用於訊息、安全性密鑰等之安全輸送)及針對在安全佈建VNF及/或安裝於NFV基礎結構108之各種節點處時的安全性監控態樣之策略。SFC安全性策略及憑證可另外包括用於跨SFC及/或在SFC之VNF內部的通訊之策略，諸如該等通訊是否將經由軟體之硬體(亦即，虛擬的)、網路介面卡、交換器及/或路由器來傳輸。SFC安全

性策略及憑證可基於流識別符、租戶識別符、用戶識別符(例如，國際行動用戶識別碼(IMSII))、地理位置、法規適用地區等。

[0065]在一些實施例中，特定策略可經由OSS/BSS 402及/或現有安全性基礎結構(諸如，第3代合作夥伴計劃(3GPP)安全性基礎結構)而組配至SFC安全性控制器408中。應瞭解，在一些實施例中，對於執行階段策略(例如，監控某些訂戶流、租戶、應用程式標籤等)，該等策略可使用現有安全性基礎結構來傳遞。如先前所描述，NFV安全性架構116之安全性監控組件可相互鑑認。在其他實施例中，SFC安全性控制器408可在SFC代理及/或其他遙測搜集組件之間傳遞安全性密鑰。另外或替代地，在一些實施例中，現有安全性基礎結構亦可傳遞可用於各種VNF間或按照SFC之通訊或策略施行之安全性密鑰。另外，SFC安全性控制器408經進一步組配以經由安全通訊頻道414安全地將SFC安全性策略提供至一或多個SFC安全性提供者422。

[0066]類似於NFV安全性服務控制器102，SFC安全性控制器408經組配以基於在NFV安全性監控分析系統438處所接收的經分析遙測資料而安全地接收來自NFV安全性監控分析系統438之修復安全性監控策略，用於接收之過程將在下文另外描述。亦類似於藉由NFV安全性服務控制器102接收之修復策略，藉由SFC安全性控制器408接收之修復安全性監控策略可包括一校正動作以基於藉由NFV安全性監控分析系統438執行的對遙測資料之分析而採用受NFV安

全性監控分析系統438懷疑之網路訊務。該校正動作可包括阻擋某一網路訊務、將某一網路訊務串流傳輸至深度封包檢測(DPI)VNF執行個體、速率限制或節制網路訊務，或可對受懷疑網路訊務採用以另外識別根本原因或驗證安全性威脅之任何其他動作。

[0067] SFC安全性控制器408經進一步組配以將安全性監控策略更新傳遞至例示性NFV安全性服務提供者420的以通訊方式耦接至SFC安全性控制器408之一或多個SFC安全性提供者422。SFC安全性提供者422經組配以跨VIM 106之各種網路及安全性監控組件(包括VIM控制器424)傳輸安全性監控策略更新。SFC安全性提供者422另外經組配以跨遍佈NFV基礎結構108分佈之NFV安全性服務代理內之各種SFC代理傳輸安全性監控策略更新(包括任何適當安全性監控動作)。

[0068] 儘管例示性NFV基礎結構108僅包括NFV安全性服務代理468之SFC代理470，但應瞭解，SFC代理可在遍佈NFV基礎結構108分佈之NFV安全性服務代理中的任何一或多者內具現化。SFC代理(例如，SFC代理470)經組配以與NFV基礎結構108之各種安全性監控組件通訊，以執行遙測資料之提取且基於安全性監控策略而安全地傳遞所提取之遙測資料。遙測資料提取(亦即，收集)可使用NFV基礎結構108內之適當鉤來起始，諸如在與SFC代理連接的開放式vSwitch、開放式vRouter、DPDK、硬體NIC(例如，NIC 220)、硬體交換器(例如，交換器222或硬體路由器等處。

[0069]應瞭解，類似於例示性NFV安全性服務代理468之安全性監控收集代理472，SFC代理中之每一者可另外包括特定於SFC代理之收集代理(圖中未示)及/或依賴於SFC代理駐留所在之NFV安全性服務代理之安全性監控收集代理，未展示該等收集代理以保留說明之清晰性。換言之，在被動式及/或主動式安全性監控期間藉由SFC代理提取之遙測資料可藉由執行於NFV基礎結構108上之SFC代理(例如，經修改s流(sFlow)等)之收集代理來收集。

[0070]如上文所論述，遙測資料可體現為可對予以執行安全性分析的任何類型之資料。舉例而言，遙測資料可包括安全性統計資料，以及來自NFV基礎結構108內之各種硬體資源(例如，計算、儲存及網路資源)、虛擬化軟體及虛擬資源(例如，計算、儲存及網路資源)的組配及健康資料。另外或替代地，遙測資料可包括特定流(亦即，藉由待監控之特定流之識別符判定的及/或為了用於封包及傳輸而收集的)、裝置、節點、管理網域、地理及/或任何管理上經組配之流等的完整或部分(例如，標頭、有效負載等)網路封包。為此，SFC代理可具備唯一地識別網路封包、裝置、節點、地理等之識別符。此外，遙測資料可特定於(例如)特定SFC，合併SFC流，或隧道傳輸SFC流。另外或替代地，遙測資料可包括全SFC訊務封包流或SFC訊務封包流之子集，諸如虛擬區域網路(VLAN)及層二(L2)或層三(L3)穿隧封包。

[0071]SFC代理可自NFV基礎結構108之任何安全性監

控組件及/或通訊頻道(諸如，安全VM、實體層NIC、交換器、路由器及/或網狀架構)提取遙測資料。舉例而言，在一些實施例中，在VNF執行個體440中之一者之NFV安全性服務代理(例如，NFV安全性服務代理448、NFV安全性服務代理458或NFV安全性服務代理460)內具現化且經啟動的SFC代理可與Intel®DPDK使用者平面應用程式(例如，vSwitch、vRouter、EPC系統等)通訊以提取遙測資料。在另一實施例中，在一些實施例中，SFC代理470可與虛擬路由器464(例如，虛擬路由器464之開放式vSwitch)通訊以提取遙測資料。

[0072]在使用中，SFC代理將遙測資料封裝且經由安全通訊頻道490將遙測資料安全地傳遞至NFV安全性監控分析系統438。SFC安全性控制器408提供且組配接收自各種SFC代理及NFV安全性監控分析系統438且在各種SFC代理與NFV安全性監控分析系統438之間組配的保護憑證。為此，SFC代理可使用人工密鑰佈建、預共用密鑰及/或使用SFC安全性控制器408之另一相互鑑認功能的啟動。此外，通訊頻道490可由一或多個安全密鑰(諸如，具有經合理組配之有限密鑰壽命的唯一成對隨機密鑰工作階段)來保護。

[0073]現參看圖5，在使用中，NFV安全性服務控制器102在操作期間建立環境500。NFV安全性服務控制器102之例示性環境500包括安全通訊模組510、安全性監控策略管理模組520、受保護傳輸控制模組530、NFV安全性服務代理控制模組540及遙測資料審計模組550。例示性環境500以

通訊方式耦接至圖4的審計資料庫410（其儲存安全性審計資訊）及NFV安全性資料庫412（其儲存安全性監控策略）。環境500之模組、邏輯及其他組件中之每一者可體現為硬體、軟體、韌體或其組合。舉例而言，環境500之各種模組、邏輯及其他組件可形成NFV安全性服務控制器102之硬體組件之一部分或以其他方式藉由NFV安全性服務控制器102之硬體組件建立。因而，在一些實施例中，環境500之模組中之任何一或多者可體現為電氣裝置之電路或集合（例如，安全通訊電路、安全性管理電路、受保護傳輸控制電路、NFV安全性服務代理控制電路及遙測資料審計電路等）。另外或替代地，在一些實施例中，例示性模組中之一或多者可形成另一模組之一部分及/或例示性模組及/或子模組中之一或多者，該等模組可體現為獨立或非依賴性模組。

[0074]安全通訊模組510經組配以促進資料（例如，訊息、安全性監控策略等）至及自NFV安全性服務控制器102之安全傳輸。為此，安全通訊模組510經組配以安全地接收來自外部安全性系統（例如，來自外部安全性控制器、圖4之OSS/BSS 402等）之安全性策略資訊。另外，安全通訊模組510經組配以經由安全通訊頻道418自NFV安全性監控分析系統438接收修復安全性策略。

[0075]安全通訊模組510經進一步組配以經由安全通訊頻道414將經更新的安全性策略安全地傳輸至NFV安全性服務提供者420。類似地，安全通訊模組510經組配以促進

資料在NFV安全性服務控制器102與NFV安全性資料庫412之間以及在NFV安全性服務控制器102與審計資料庫410之間的安全傳輸。對於藉由安全通訊模組510傳輸之所有安全訊息，安全通訊模組510包括正在執行傳輸之NFV安全性服務控制器102之執行個體的唯一識別符，以及鑑認密鑰。為此，安全通訊模組510可執行各種密鑰管理功能、密碼編譯功能、安全通訊頻道管理及/或其他安全性功能，諸如使用定期再新之成對工作階段密鑰。因此，接收訊息之安全性監控組件可經由NFV安全性服務控制器102來鑑認訊息。

[0076]安全性監控策略管理模組520經組配以基於接收之安全性監控策略而跨NFV安全性架構116編排安全性監控策略之管理。為此，安全性監控策略管理模組520包括安全性監控策略發佈模組522及安全性監控策略施行模組524。安全性監控策略發佈模組522經組配以將安全性監控策略(其包括安全性監控組件策略、組配及功能)傳輸至遍佈NFV安全性架構116之各種安全性監控組件，諸如傳輸至跨NFV安全性架構116分佈之NFV安全性服務代理。

[0077]安全性監控策略施行模組524經組配施行傳輸至NFV安全性架構116之各種安全性監控組件的安全性監控策略。為此，安全性監控策略施行模組524經組配以藉由驗證NFV安全性服務代理係根據安全性監控策略組配，以及根據安全性監控策略而監控及收集遙測資料來施行安全性監控策略。舉例而言，安全性監控策略施行模組524可經組配以NFV基礎結構108之VNF執行個體處(諸如，在VNF執行

階段或在裝置NFV基礎結構108處之VNF時)驗證安全性監控策略，以確保VNF執行個體經正確地組配且當前執行於執行個體上的NFV安全性服務代理正在監控且收集符合安全性監控策略之遙測資料。另外，安全性監控策略施行模組524可基於安全性監控策略來驗證服務功能鏈(例如，圖4之服務功能鏈450)之拓撲，該服務功能鏈包括多個VNF執行個體(例如，服務功能鏈450之服務功能鏈VNF 452)。

[0078]受保護傳輸控制模組530經組配以設置用於VNF(諸如，服務功能鏈450之服務功能鏈VNF 452)之受保護傳輸策略(例如，應用用於安全通訊頻道保護之安全性)。如先前所描述，NFV安全性服務控制器102可經組配以充當鑑認伺服器以保護安全通訊頻道。因此，受保護傳輸控制模組530可另外包括訊息鑑認模組534，該訊息鑑認模組經組配以執行鑑認伺服器之功用(亦即，對NFV安全性架構116之安全通訊頻道所有傳輸及所接收之訊息執行鑑認。舉例而言，受保護傳輸控制模組530可利用一或多個安全密鑰(例如，熔斷密鑰、工作階段密鑰或任何類型之密碼編譯密鑰)來建立根信任(RoT)以保全通訊頻道(例如，經由共用記憶體)。在一些實施例中，安全密鑰可體現為可定期再新之成對工作階段密鑰。類似地，受保護傳輸控制模組530經組配以保護安全性監控組件與審計資料庫410之間的安全通訊頻道。

[0079]NFV安全性服務代理控制模組540經組配以管理NFV安全性服務代理(參見圖4)，該等NFV安全性服務代理

經組配以遍佈VIM 106及NFV基礎結構108傳遞各種安全性功能。爲此，在NFV安全性服務代理開機之前，NFV安全性服務代理控制模組540播種適當安全性及策略組配資訊(其可在執行階段藉由NFV安全性服務代理提取)，以執行特定任務(諸如連接至適當VNF管理器)。舉例而言，在NFV安全性架構116包括服務功能鏈之許多具現化VNF (例如，服務功能鏈450之服務功能鏈VNF 452)之一實施例中，NFV安全性服務代理控制模組540經組配以啓動服務功能鏈之VNF，藉由在服務功能鏈之VNF中之一或多者上執行NFV安全性服務代理之啓動來起始NFV安全性服務代理之部署(亦即，加快旋轉及具現化)，且接收啓動資訊(例如，可由啓動使用以執行個體化NFV安全性服務代理的啓動組配參數，用於特定NFV安全性服務代理執行個體之個人化資訊，及/或NFV安全性服務代理執行個體之使用權資訊等)。

[0080]NFV安全性服務代理控制模組540經進一步組配以告知具現化NFV安全性服務代理的對應VNF管理器432。NFV安全性服務代理可經組配以執行相互鑑別密鑰交換以用於建立與受保護傳輸控制模組530之安全通訊頻道，NFV安全性服務代理控制模組540可使用安全通訊頻道來個人化NFV安全性服務代理(例如，集合姓名、安全性策略群組、每租戶策略、分配密鑰材料以用於與特定NFV安全性服務代理駐留所在之VNF執行個體之VNF管理器432的安全工作階段建立等)。

[0081]遙測資料審計模組550經組配以對儲存於審計資

料庫410處之遙測資料執行審計。爲此，遙測資料審計模組550經組配以分析與遙測資料相關聯之時間戳記。如先前所描述，遙測資料在經傳輸至審計資料庫410之前藉由安全時鐘(例如，圖2之安全時鐘216)加時間戳記。因此，遙測資料審計模組550經進一步組配以作爲審計之部分而驗證及序列遙測資料。

[0082]現參看圖6，在使用中，每一NFV安全性服務代理(例如，圖4之NFV安全性服務代理426、448、458、460、468、486)在操作期間建立環境600。對應安全性服務代理之例示性環境600包括安全通訊模組610、遙測資料監控模組620、遙測資料封包模組630及啓動執行模組640。例示性環境600另外包括安全性策略資料庫602 (其中儲存NFV安全性服務代理處之安全性監控策略)及遙測資料庫604 (其中儲存NFV安全性服務代理處之遙測資料)。應瞭解，在一些實施例中，安全性監控策略及/或遙測資料可在NFV安全性服務代理外部儲存，諸如儲存於NFV安全性資料庫412及/或審計資料庫410中。

[0083]環境600之模組、邏輯及其他組件中之每一者可體現爲硬體、軟體、韌體或其組合。舉例而言，環境600之各種模組、邏輯及其他組件可形成NFV安全性服務代理之硬體組件之一部分或以其他方式藉由NFV安全性服務代理之硬體組件建立。因而，在一些實施例中，環境600之模組中之任何一或多者可體現爲電氣裝置之電路或集合(例如，安全通訊電路、遙測資料監控電路、遙測資料封包電

路及啓動執行電路等)。另外或替代地，在一些實施例中，例示性模組中之一或多者可形成另一模組之一部分，及/或例示性模組及/或子模組中之一或多者可體現爲獨立或非依賴性模組。

[0084] 安全通訊模組610經組配以促進資料(例如，訊息、遙測資料等)至及自NFV安全性服務代理之安全傳輸。舉例而言，如圖4中所示，NFV基礎結構108之NFV安全性服務代理經組配以使用藉由NFV安全性服務控制器102提供之保護憑證將遙測資料傳輸至NFV安全性監控分析系統438及審計資料庫410。遙測資料監控模組620經組配以監控組件之遙測資料及/或NFV安全性服務代理所位於之層級。遙測資料監控模組620另外經組配以主動地及/或被動地監控遙測資料。遙測資料可包括虛擬及/或實體組配資料，以及安全性統計資料、完整網路封包、網路封包標頭，或與特定流、特定裝置、特定演進型節點B (亦稱爲，E-UTRAN節點B、eNodeB及eNB)、特定地理或任何管理性組配之流相關聯之所有網路封包。

[0085] 遙測資料封包模組630經組配以收集及封裝遙測資料，諸如在遙測資料監控模組620處受監控之遙測資料。因此，所收集及所封裝的遙測資料可爲任何類型之資料，包括NFV基礎結構108或VIM 106之硬體資源(例如，計算、儲存及網路資源)、虛擬化軟體及/或虛擬資源(例如，計算、儲存及網路資源)的資訊，諸如VNF組配設定、I/O子系統206設定、NIC 220設定、交換器222設定、虛擬路由器464設定、

虛擬交換器設定、虛擬閘道器設定、vEPC設定、控制器設定、網路訊務資訊、完整及/或部分網路封包等。此外，遙測資料封包模組630經組配以將經封裝遙測資料安全地傳遞至專用分析系統(例如，圖4之NFV安全性監控分析系統438)，諸如經由安全通訊模組610。

[0086]遙測資料監控模組620及/或遙測資料封包模組630可另外包括代理特定子模組以監控及/或收集特定遙測資料。舉例而言，例示性遙測資料監控模組620包括SFC遙測資料監控模組622以監控特定於NFV基礎結構108之服務功能鏈(例如，服務功能鏈450)之遙測資料。類似地，例示性遙測資料封包模組630包括SFC遙測資料封包模組632以收集及封裝特定於諸如藉由SFC遙測資料監控模組622監控的網路基礎結構之服務功能鏈的遙測資料。另外，遙測資料封包模組630及SFC遙測資料封包模組632各自經組配以使用安全時鐘(例如，圖2之安全時鐘216)對供傳輸至審計資料庫410以安全儲存的遙測資料加時間戳記。

[0087]啟動執行模組640經組配以執行用以部署NFV安全性服務代理之啟動，其將NFV安全性服務代理載入於計算節點(例如，計算節點110中之一者)上。啟動執行模組640經進一步組配以在NFV安全性架構116之網路處理組件中之任一者上執行啟動，該等網路處理組件包括(例如)VNF執行個體(例如，服務功能鏈450之服務功能鏈VNF 452中之一者)、超管理器462及平台480中之一者。

[0088]現參看圖7，在使用中，NFV安全性服務控制器

102可執行用於管理NFV安全性架構116之安全性監控服務的方法700。方法700在區塊702開始，其中NFV安全性服務控制器102經由安全通訊頻道(例如，至VIM 106的圖4之通訊頻道414)將安全性監控策略傳輸至NFV基礎結構108內的已經具現化之VNF。如先前所描述，安全性監控策略包括各種監控規則，VNF使用該等監控規則判定什麼遙測資料需要監控及如何組配VNF之資源及功能性。在使用中，NFV安全性服務控制器102經由安全通訊頻道414將安全性監控策略傳輸至具有唯一地識別NFV安全性服務控制器102之識別符的NFV安全性服務提供者420。在一些實施例中，NFV安全性服務控制器102可經由NFV編排器104自外部源(諸如，外部控制器或圖4之OSS/BSS 402)接收安全性監控策略。

[0089]在區塊704，NFV安全性服務控制器102驗證VNF處之安全性監控策略。舉例而言，NFV安全性服務控制器102可在VNF執行階段或在NFV基礎結構108處之VNF裝載時驗證安全性監控策略。在區塊706，NFV安全性服務控制器102基於安全性監控策略而在多個VNF (包括其間之路徑(亦即，通訊路徑))之間安裝SFC拓撲。在一些實施例中，在區塊708，NFV安全性服務控制器102可將安全性應用於路徑以基於安全性監控策略保護跨路徑傳輸之通訊。

[0090]在區塊710，NFV安全性服務控制器102基於安全性監控策略來驗證SFC拓撲，以確保遵從安全性監控策略。在區塊712，NFV安全性服務控制器102設置用於SFC之

VNF(例如，圖4之服務功能鏈450之服務功能鏈VNF 452)的受保護傳輸策略。在區塊714，NFV安全性服務控制器102啟動SFC之VNF中之每一者。為此，NFV安全性服務控制器102可經由安全通訊頻道將啟動信號傳輸至VNF中之每一者。另外，該啟動信號(其類似於需要鑑認的自NFV安全性服務控制器102傳輸之其他信號(亦即，訊息))包括唯一識別符，以使得VNF可鑑認該啟動信號。

[0091]在區塊716，NFV安全性服務控制器102起始NFV安全性服務代理之部署(亦即，加快旋轉及具現化)。為此，NFV安全性服務控制器102針對NFV安全性服務代理執行啟動。如先前所描述，NFV安全性服務代理可遍佈VIM 106及/或NFV基礎結構108分佈以執行安全性監控操作。因此，NFV安全性服務代理可在圖4之NFV安全性架構116之許多安全性監控組件(諸如SFC之VNF中之一者)處具現化。

[0092]在區塊718，NFV安全性服務控制器102判定是否自具現化NFV安全性服務代理接收到啟動資訊。若並非如此，則方法700回送至區塊718，以繼續等待待自具現化NFV安全性服務代理接收之啟動資訊。若NFV安全性服務控制器102判定已自具現化NFV安全性服務代理接收啟動資訊，則方法700前進至720，其中NFV安全性服務控制器102通知NFV安全性服務代理具現化所在的VNF之管理器。通知包括對應於VNF之執行個體的唯一識別符及對應於NFV安全性服務代理之執行個體的唯一識別符。因此，VNF管理器可接著基於該等唯一識別符而與具現化NFV安全性服

務代理通訊且管理具現化NFV安全性服務代理。在區塊722，NFV安全性服務控制器102啟動具現化NFV安全性服務代理。在區塊724，NFV安全性服務控制器102跨遍佈VIM 106及/或NFV基礎結構108分佈之NFV安全性服務代理施行安全性監控策略。

[0093]現參看圖8，在使用中，NFV安全性服務控制器102可執行用於更新安全性監控策略之方法800。方法800在區塊802開始，其中NFV安全性服務控制器102判定是否自NFV安全性監控分析系統438接收修復策略。如先前所描述，遍佈VIM 106及/或NFV基礎結構108分佈之NFV安全性服務代理經組配以收集遙測資料，將遙測資料安全地傳輸至NFV安全性監控分析系統438以供分析，從而判定是否偵測到任何威脅及/或異常。因此，在NFV安全性監控分析系統438偵測此安全性威脅(例如，攻擊或異常)之情況下，NFV安全性監控分析系統438安全地傳輸集中於解決或另外分析觸發修復策略的偵測到之安全性威脅的修復策略。若NFV安全性服務控制器102判定未接收到修復策略，則方法800返回至區塊802，直至接收到修復策略為止。

[0094]若NFV安全性服務控制器102接收到修復策略，則在區塊804，NFV安全性服務控制器102基於在區塊802所接收之修復策略來更新當前安全性監控策略。在區塊806，NFV安全性服務控制器102經由安全通訊頻道(例如，至VIM 106的圖4之通訊頻道414)將安全性監控策略更新傳輸至NFV安全性服務提供者420。因此，安全性監控策略更新可

接著另外自NFV安全性服務提供者420傳輸至遍佈VIM 106及/或NFV基礎結構108分佈之NFV安全性服務代理。

[0095]在一些實施例中，在區塊808，NFV安全性服務控制器102另外經由安全通訊頻道將NFV安全性服務控制器102獨有之識別符隨安全性監控策略傳輸至NFV安全性服務提供者420。另外或替代地，在一些實施例中，在區塊810，NFV安全性服務控制器102另外經由安全通訊頻道將待回應於修復策略而採用之一或多個校正動作隨安全性監控策略傳輸至NFV安全性服務提供者420。舉例而言，校正動作可包括阻擋某一網路訊務、將某一網路訊務串流傳輸至深度封包檢測(DPI)VNF執行個體、速率限制或節制網路訊務等。在區塊812，NFV安全性服務控制器102跨遍佈VIM 106及/或NFV基礎結構108分佈之NFV安全性服務代理施行經更新之安全性監控策略。

[0096]現參看圖9，用於初始化NFV安全性服務代理之通訊流程900之實施例包括圖4之NFV安全性架構116之各種安全性監控組件。例示性通訊流程900包括NFV編排器104、NFV安全性服務控制器102、NFV安全性服務提供者420、NFV基礎結構108、NFV安全性服務代理(例如，NFV安全性服務代理426、NFV安全性服務代理448、NFV安全性服務代理458、NFV安全性服務代理460及NFV安全性服務代理486)中之一者及VNF管理器432。例示性通訊流程900另外包括許多資料流，該等資料流中的一些可視實施例而單獨執行或一起執行。

[0097] 資料流902至910提供用於使用NFV安全性架構116內之安全性監控VNF執行個體來佈建NFV安全性架構116之安全性監控的資料流之序列。在資料流902，NFV編排器104將自OSS/BSS 402接收之安全性監控策略傳輸至NFV安全性服務控制器102。在資料流904，NFV安全性服務控制器102將具有NFV安全性服務控制器之唯一識別符的命令安全地傳輸至NFV安全性服務提供者420以執行個體化NFV安全性服務代理。在資料流906，NFV安全性服務提供者420將具有NFV安全性服務控制器及/或NFV安全性服務提供者之唯一識別符的命令安全地傳輸至NFV基礎結構108以部署(亦即，加快旋轉及具現化)安全性服務代理。

[0098] 在資料流908，NFV基礎結構108加快旋轉NFV安全性服務代理。如先前所描述，NFV安全性服務代理可在NFV基礎結構108內之各種位置處加快旋轉，該等位置包括NFV(例如，NFV安全性服務代理448、NFV安全性服務代理458及NFV安全性服務代理460)、超管理器462(例如，安全性服務代理468)及平台480(例如，NFV安全性服務代理486)。在資料流910，將NFV安全性服務代理具現化(亦即，起始NFV安全性服務代理之啟動)。

[0099] 資料流912至916提供用於在安全性功能起動及個人化NFV安全性服務代理後播種資訊的資料流之序列。在資料流912，NFV安全性服務代理經歷啟動執行過程。在資料流914，NFV安全性服務代理將啟動資訊安全地傳輸至NFV安全性服務控制器102。在資料流916，NFV安全性服

務控制器102通知負責管理NFV安全性服務代理之VNF管理器432。通知可包括對應於NFV安全性服務代理之執行個體的唯一識別符，以及對應於NFV安全性服務代理(例如，服務功能鏈450之服務功能鏈VNF 452中之一者，超管理器462，平台480中之一者等)所在之組件的另一唯一識別符。

[0100]資料流918至922提供用於定義VNF與安全性監控VNF之間的安全性策略關聯的資料流之序列。在資料流918，具現化NFV安全性服務代理建立與VNF管理器432之管理工作階段。為此，NFV安全性服務代理可使用VNF管理器432之所提供唯一識別符(諸如網際網路協定(IP)位址、域名伺服器(DNS)、完全合格網域名稱(FQDN)、統一資源定位符(URL)等)及初始根安全性憑證(其唯一地識別NFV安全性服務代理與VNF管理器432之間的相互鑑認且可在該相互鑑認中使用)來建立與VNF管理器432之管理工作階段。

[0101]在資料流920，NFV安全性服務控制器102在NFV安全性服務提供者420處施行安全性監控策略(各種協定類型、隧道等)。應瞭解，NFV安全性服務控制器102處的策略之映射可藉由系統管理員、安全性管理員、租戶、機器學習引擎及/或任何其他技術及/或經授權人員中之一者來進行。在資料流922，NFV安全性服務提供者420在NFV安全性服務代理處施行安全性監控策略之NFV安全性服務代理部分。

[0102]資料流924及926提供用於將工作負載訊務映射

至安全性策略的資料流之序列。舉例而言，NFV安全性服務代理可與虛擬交換器互動以在將訊務遞交至安全性監控VNF執行個體之前轉譯VNF群組至安全性策略之映射。在此等實施例中，VNF群組可基於工作負載訊務類型(例如，VLAN、多協定標籤切換(MPLS)、通用封包無線電服務(GPRS)隧道傳輸協定(GTP)等)及待藉由安全性監控VNF施行之相關聯安全性策略。因此，映射可由於任意數目之原因(包括新租戶加入、現有租戶離開、訊務工程、工作負載平衡等)而改變。結果，OSS/BSS系統可將此等變化輸送至NFV安全性服務控制器102。因而，NFV安全性服務控制器102接著可使新安全性策略至NFV安全性服務代理(例如，安全性監控VNF之NFV安全性服務代理)的發佈自動化。

[0103]在資料流924，NFV安全性服務控制器102啟動NFV安全性服務代理。為此，NFV安全性服務控制器102經由安全通訊頻道將啟動信號提供至NFV安全性服務代理。另外，與藉由NFV安全性服務控制器102傳輸的需要鑑認之其他訊息一致，啟動信號可包括唯一識別符。在資料流926，NFV安全性服務代理將網路訊務映射至安全性監控策略。因此，NFV安全性服務代理可根據安全性監控策略來監控及收集遙測資料。應瞭解，網路訊務映射之檢查可由NFV安全性服務控制器102基於傳遞至NFV安全性服務代理之安全性策略來執行。

[0104]現參看圖10，在使用中，NFV安全性服務代理中之一者可執行用於監控NFV安全性架構116之安全性之方

法1000。方法1000在區塊1002開始，其中NFV安全性服務代理判定是否接收到具現化請求。若未接收，則方法1000返回至區塊1002以繼續等待具現化請求。若在區塊1002接收到具現化請求，則方法1000前進至區塊1004。在區塊1004，NFV安全性服務代理執行用以部署NFV安全性服務代理之啟動過程，其將NFV安全性服務代理載入於計算節點(例如，計算節點110中之一者)上。因此，啟動過程可允許基於NFV基礎結構108及/或NFV安全性服務代理部署所在的NFV基礎結構108之組件的最佳化，諸如跨NFV基礎結構108之安全性服務代理的加速度、可擴充性、快速部署等。

[0105]在區塊1006，NFV安全性服務代理將啟動資訊傳輸至NFV安全性服務控制器102。舉例而言，啟動資訊可包括可由啟動使用以具現化NFV安全性服務代理之啟動組配參數、特定NFV安全性服務代理執行個體之個人化資訊及/或NFV安全性服務代理執行個體之使用權資訊。在區塊1008，安全性服務代理建立與VNF管理器(例如，VNF管理器432)之管理工作階段。因此，VNF管理器(管理工作階段已經與其建立)可採用NFV安全性服務代理之管理控制。在區塊1010，NFV安全性服務代理經由NFV安全性服務提供者420自NFV安全性服務控制器102接收用於主動式及/或被動式監控之安全性監控策略。因此，NFV安全性服務代理可僅接收安全性監控策略的關於NFV安全性服務代理之一部分。

[0106]在區塊1012，NFV安全性服務代理基於安全性監

控策略來映射用於監控及/或收集之網路訊務資料。換言之，NFV安全性服務代理基於安全性監控策略來映射什麼網路訊務需要監控。在區塊1014，NFV安全性服務代理基於安全性監控策略來執行安全性監控(例如，映射後網路訊務之安全性監控)。為此，在區塊1016，NFV安全性服務代理對控制、管理及/或資料平面執行安全性監控。在一些實施例中，基於安全性監控策略，監控可為連續監控，其具有經佈建遙測監控或基於人工或自動異常偵測之特定監控策略輸送及啟動。另外或替代地，在一些實施例中，監控可由管理員基於管理員所規定之準則來觸發。

[0107]在區塊1018，NFV安全性服務代理收集遙測資料。所收集的遙測資料可包括虛擬及/或實體網路統計資料、網路健康監控資訊、網路封包(例如，網路封包、隨機網路封包等之完整流)及/或任何其他組件組配或網路封包相關資料。在一些實施例中，NFV安全性服務代理可經由經組配以在受保護本端儲存器處收集遙測資料的安全性監控收集代理(例如，圖4之安全性監控收集代理472)來收集遙測資料。在區塊1020，NFV安全性服務代理封裝所收集的遙測資料、安全輸送密鑰及NFV安全性服務代理之唯一識別符以用於受保護傳輸。在區塊1022，NFV安全性服務代理經由安全通訊頻道(例如，圖4之安全通訊頻道490)將經封裝遙測資料、安全輸送密鑰及唯一識別符安全地傳輸至經組配以針對威脅及/或異常來分析遙測資料的NFV安全性監控分析系統(例如，圖4之NFV安全性監控分析系統438)。

[0108]應瞭解，在一些實施例中，方法700、800及/或1000中之任何一或多者可體現為儲存於電腦可讀媒體上之各種指令，該等指令可由處理器202、網路介面控制器220及/或計算節點110之其他組件執行以使計算節點110執行各別方法700、800及/或1000。電腦可讀媒體可體現為能夠由計算節點110讀取的任何類型之媒體，包括(但不限於)記憶體208、資料儲存器214、網路介面控制器220之本端記憶體、計算節點110之其他記憶體或資料儲存裝置、計算節點110之周邊裝置可讀的攜帶型媒體及/或其他媒體。

[0109]現參看圖11，展示了用於(例如，在圖4之例示性服務功能鏈VNF 452處)監控NFV安全性架構116之服務功能鏈(SFC)之安全性的通訊流程1100之實施例。如先前所描述，許多安全性監控組件可經特定組配或包括額外及/或替代性安全性監控組件，以監控NFV基礎結構(例如，NFV基礎結構108)內所執行之服務功能鏈之安全性。舉例而言，圖4之例示性NFV安全性架構116之SFC特定安全性監控組件包括NFV安全性服務控制器102之SFC安全性控制器408、VIM 106之NFV安全性服務提供者420之SFC安全性提供者422及NFV基礎結構108的在各種網路監控及/或處理組件(虛擬的及實體的)中遍佈NFV基礎結構108分佈的許多SFC代理(例如，SFC代理470)。亦如先前所描述，儘管SFC代理470經展示於NFV安全性服務代理468中，但應瞭解，遍佈NFV基礎結構108分佈之NFV安全性服務代理中之每一者可包括一SFC代理。因此，在一些實施例中，SFC代理

可駐留於SFC之VNF中(例如，服務功能鏈450之服務功能鏈VNF 452中之一者)。

[0110]例示性通訊流程1100包括SFC 代理470、安全性監控收集代理472、NFV安全性監控分析系統438、SFC安全性控制器408及SFC安全性提供者422。例示性通訊流程1100另外包括許多資料流，該等資料流中的一些可視實施例而單獨執行或一起執行。在資料流1102，SFC代理470將安裝、啟動及過濾策略以及SFC代理470之唯一識別符安全地傳輸至安全性監控收集代理472。安裝、啟動及過濾策略包括關於SFC代理470之安裝、啟動及保護的各種指令及資訊，以及安全性監控收集代理472可用來過濾相關網路訊務的各種指令及資訊。舉例而言，安全性監控收集代理472可過濾網路訊務以僅監控由安裝、啟動及過濾策略指示之網路訊務。因此，在資料流1104，安全性監控收集代理472基於安裝、啟動及過濾策略來監視及收集遙測資料。

[0111]在資料流1106，安全性監控收集代理472封裝所收集的遙測資料以供安全傳輸至NFV安全性監控分析系統438。在資料流1108，安全性監控收集代理472經由安全通訊頻道將經封裝遙測資料安全地傳輸至NFV安全性監控分析系統438。另外，經封裝遙測資料亦可包括SFC代理470之唯一識別符。在資料流1110，NFV安全性監控分析系統438接收經封裝遙測資料且對接收之遙測資料執行安全性威脅分析。在資料流1112，在偵測到安全性威脅(諸如，攻擊或異常)後，NFV安全性監控分析系統438經由安全通訊

頻道安全地傳輸修復策略及NFV安全性監控分析系統438之唯一識別符。修復策略可包括回應於偵測到安全性威脅可採用之一或多個校正動作，諸如，以解決威脅或驗證異常。舉例而言，校正動作可包括阻擋某一網路訊務、將某一網路訊務串流傳輸至深度封包檢測(DPI) VNF執行個體、速率限制或節制網路訊務等。

[0112]在資料流1114，SFC安全性控制器408基於修復策略及其中所含之一或多個校正動作來更新當前安全性策略。在資料流1116，SFC安全性控制器408經由安全通訊頻道將經更新的安全性策略隨SFC安全性控制器408之執行個體獨有之識別符安全地傳輸至SFC安全性提供者422。應瞭解，在一些實施例中，SFC安全性控制器408可視VIM 106之拓撲及分佈而與一個以上SFC安全性提供者422安全通訊。因此，SFC安全性提供者422中與SFC安全性控制器408通訊(例如，提供安全性監控策略)之SFC安全性提供者可取決於安全性監控策略。舉例而言，若服務功能鏈橫跨多個存在點(POP)(例如，存取點)，則單一SFC策略(亦即，特定於SFC之安全性監控策略)可在不同POP傳遞多個SFC安全性提供者422。換言之，每一POP可執行獨立VIM 106，且因而執行獨立SFC安全性提供者422。

[0113]在資料流1118，SFC安全性提供者422跨VIM 106(例如，VIM控制器424、其他VIM組件428等)輸送經更新的安全性策略。在資料流1120，SFC安全性提供者422將經更新的安全性策略及SFC安全性提供者422之執行個體獨

有之識別符安全地傳輸至SFC代理470。

[0114]現參看圖12，在使用中，安全性監控VNF(例如，圖4之安全性監控VNF 446)在操作期間建立環境1200。NFV安全性服務控制器102之例示性環境1200包括佈建管理模組1210、個人化管理模組1220、策略更新管理模組1230及安全性監控模組1240。環境1200之模組、邏輯及其他組件中之每一者可體現為硬體、軟體、韌體或其組合。

[0115]舉例而言，環境1200之各種模組、邏輯及其他組件可形成安全性監控VNF 446之硬體組件之一部分或以其他方式藉由安全性監控VNF 446之硬體組件建立。因而，在一些實施例中，環境500之模組中之任何一或多者可體現為電氣裝置之電路或集合(例如，佈建管理電路系統1210、個人化管理電路系統1220、策略更新管理電路1230及安全性監控電路系統1240等)。另外或替代地，在一些實施例中，例示性模組中之一或多者可形成另一模組之一部分及/或例示性模組及/或子模組中之一或多者，該等模組可體現為獨立或非依賴性模組。

[0116]例示性環境1200進一步包括用於儲存個人化資料之個人化資料庫1202，個人化資料包括可用以組配安全性監控VNF之一或多個功能(例如，安全性功能)之資料，諸如安全組配資料、安全性監控VNF 446之一組初始參數、NFV安全性架構116的元資料、關於其他VNF (例如，VNF執行個體440之網路VNF 442、服務功能鏈VNF 452等)之連接資訊、供應商特定資訊、效能資料、工作負載訊務工程

資料及/或服務品質(QoS)參數及策略。在一些實施例中，個人化資料庫1202可另外包括佈建相關資料，諸如安全性監控VNF 446之唯一識別符、安全性監控VNF 446執行所在之平台之唯一識別符及安全性憑證。例示性環境1200另外包括用於儲存安全性監控VNF 446之安全性策略資訊及安全性監控資訊(例如，記錄檔、警示訊息、統計資料等)的安全性策略資料庫1204。安全性策略資訊可包括租戶特定安全性處理策略、安全性訊務策略、安全性群組策略、網路服務處理策略等。應瞭解，在一些實施例中，任何一或多個模組及/或子模組可經組配以將資料儲存於個人化資料庫1202及/或安全性策略資料庫1204中及/或擷取個人化資料庫及/或安全性策略資料庫中之資料。

[0117]佈建管理模組1210經組配以自NFV安全性服務控制器102接收佈建資料(例如，VNF之識別符、平台之識別符、安全性憑證等)，且執行相互鑑別密鑰交換程序以建立安全性監控VNF 446與VNF管理器(例如，VNF管理器432)之間的安全通訊路徑(例如，安全通訊頻道434)。為此，安全性監控VNF 446可使用包括具有自NFV安全性服務控制器102接收之佈建資料的安全性憑證。在一些實施例中，佈建資料可使用帶外(OOB)通訊技術來接收。

[0118]個人化管理模組1220經組配以經由安全通訊路徑自VNF管理器432接收個人化資料，個人化資料可用以組配安全性監控VNF之一或多個功能(例如，安全性功能)，諸如藉由佈建管理模組1210建立之安全通訊路徑。個人化管

理模組1220經進一步組配以執行個人化操作以基於自VNF管理器432接收之個人化資料來組配安全性監控VNF。另外，個人化管理模組1220經進一步組配以將個人化操作狀態及策略更新操作狀態傳輸至VNF管理器432。個人化操作狀態及策略更新操作狀態接著可進一步傳輸至NFV安全性服務控制器102，該NFV安全性服務控制器接著可判定對於藉由安全性監控VNF 446監控之網路訊務是否啓動全網路安全性策略。

[0119]策略更新管理模組1230經組配以經由安全通訊路徑(諸如，藉由佈建管理模組1210建立之安全通訊路徑)自VNF管理器432接收策略資訊。策略更新管理模組1230經進一步組配以執行策略更新操作以更新安全性監控VNF之安全性策略。安全性監控模組1240經組配以監控網路工作負載訊務以判定安全性監控資訊且經由安全通訊路徑將安全性監控資訊傳輸至VNF管理器432。在一些實施例中，安全性監控資訊可經由安全性監控收集代理(例如，圖4之安全性監控收集代理472)安全地自安全性監控VNF傳輸至VNF管理器432。安全性監控資訊可包括網路工作負載訊務相關之各種資料，諸如記錄檔、警示訊息及統計資料。

[0120]現參看圖13，展示了用於佈建安全VNF個人化及策略協定之通訊流程1300之實施例。例示性通訊流程1300包括安全性監控VNF 446、OSS/BSS 402、NFV安全性服務控制器102及VNF管理器432。例示性通訊流程1300另外包括許多資料流，該等資料流中之一些可視實施例而單獨地

執行或一起執行。

[0121]如上所述，安全性監控VNF 446之安全具現化(例如，經由安全啟動)實現動態地具現化之安全性監控VNF 446與其各別VNF管理器(例如，圖4之VNF管理器432)之間的安全頻道。應瞭解，在一些實施例中，安全頻道可能已局部具現化。應進一步瞭解，安全性監控VNF 446先前已佈建以在圖13之通訊流程之前建立與其各別VNF管理器(例如，圖4之VNF管理器432)之管理工作階段。另外，應瞭解，安全性監控VNF 446亦已在佈建之後及在圖13之通訊流程之前經啟動。

[0122]因此，現在啟動之安全性監控446可經個人化，個人化可包括安全地傳遞VNF供應商特定專用資訊(例如，安全性憑證)、利用一組初始參數執行安全組配、供應可應用元資料及狀態資訊、建立VNF間連接之狀態(例如，在SFC中)以及播種任何其他VNF特定資訊。此外，個人化可包括安全傳遞策略之起動集合及/或特定於安全性監控VNF 446經組配以執行之功能之行爲參數。此等策略及參數可爲動態的且取決於部署安全性策略及程序。應瞭解，在一些實施例中，策略可初始安全後啟動時及/或在安全性監控VNF 446之主動執行期間傳遞。應進一步瞭解，在一些實施例中，個人化及策略協定可爲動態且自動的。舉例而言，在編排驅動系統中，安全性監控VNF 446中之每一者可使用上文所述之協定及程序而動態地且安全地安裝。

[0123]如先前所描述，安全性監控VNF 446先前已經具

現化及佈建，在該時間期間，安全性監控VNF 446接收VNF管理器432之唯一識別符(例如，IP位址、DNS、FQDN、URL等)，及NFV安全性服務控制器102用來佈建安全性監控VNF 446執行個體之安全性憑證。在資料流1302中，NFV安全性服務控制器102為VNF管理器432供應安全性監控VNF 446之識別符及平台之識別符(例如，圖4之平台480中之一者的識別符)，以及NFV安全性服務控制器102用來佈建安全性監控VNF 446之安全性憑證。應瞭解，佈建步驟(亦即，資料流2)可為安全性監控VNF 446與管理安全性監控VNF 446之對應VNF管理器之間的安全且受信任之已建立通訊頻道的先決條件。在一些實施例中，佈建步驟可使用安全之帶外(OOB)佈建技術來執行。

[0124]在資料流1304中，安全性監控VNF 446及VNF管理器432使用可如先前所描述供應之安全性憑證來執行相互鑑別密鑰交換程序。相互鑑別安全性協定之選擇可使用NFV部署之安全性策略(例如，輸送層安全性(TLS))建立。在資料流1306中，使用於資料流1304中所建立之安全且受信任之頻道，安全性監控VNF 446將安全性監控資訊(例如，記錄檔、警示訊息、統計資料等)安全地傳輸至VNF管理器432。在一些實施例中，安全性監控VNF 446可打開與VNF管理器432之專用頻道(例如，管理頻道)以傳輸安全性監控資訊。在資料流1308中，可在OSS/BSS 402佈建一或多個安全性監控VNF 446以與租戶、服務及/或網路相關聯。此關聯可基於新租戶、服務或網路之安全性策略，且因此

可如此佈建。在一些實施例中，租戶或服務/網路管理員可將適當安全性監控VNF 446指派給一或多個工作負載。

[0125]在資料流1310中，OSS/BSS 402將此新租戶、服務或網路佈建傳達至NFV安全性服務控制器102，以使得策略可在NFV安全性服務控制器102處設定。在一些實施例中，該等通訊可經由中間物(諸如，圖4之例示性NFV安全性架構116之NFV編排器104)進行。因此，在此等實施例中，NFV編排器104可負責將策略(例如，安全性策略)自OSS/BSS 402安全地傳達至NFV安全性服務控制器102。安全性策略可使用(例如)租戶之識別符來識別，且與可組配之安全性群組及/或其他可程式化結構及/或資料庫(諸如圖4之例示性NFV安全性架構116中所示之結構及/或資料庫)相關聯。應瞭解，NFV編排器104及NFV安全性服務控制器102可具有安全、相互鑑別之頻道以在其間安全地傳輸資訊。

[0126]在資料流1312中，NFV安全性服務控制器102可佈建或更新用於租戶、服務或網路之新策略，及相關聯安全性群組或其他安全性策略資訊。因此，在一些實施例中，新策略可儲存於資料庫(諸如，圖4之NFV安全性資料庫412)中。在一些實施例中，安全性策略(包括敏感資訊)可使用加密而安全地儲存資料庫中且此後基於安全性策略來安全地存取。

[0127]在資料流1314中，NFV安全性服務控制器102基於在資料流1312處更新或佈建之策略來設定用於安全性監控446之策略。應瞭解，在一些實施例中，在設定時，NFV

安全性服務控制器102跨負責管理VNF執行個體中之每一者的所有VNF管理器發佈安全性策略。策略發佈可經由可靠協定來進行。因此，在此等實施例中，NFV安全性服務控制器102可維持狀態且確保跨NFV安全性架構116之策略一致性及傳遞保障。在一些實施例中，諸如在混合VNF網路架構中，NFV安全性服務控制器102可將安全性策略傳遞至管理實體網路功能及/或虛擬網路功能之VNF管理器。在資料流1316中，VNF管理器432將安全性監控VNF 446之個人化資料推送至安全性監控VNF 446。此個人化資料發佈可經由可靠協定進行。

[0128]應瞭解，個人化資料可推送至受新租戶、服務及/或網路佈建影響之額外安全性監控VNF執行個體。因此，各別安全性監控VNF執行個體之VNF管理器中之每一者可維持狀態且確保所有安全性監控VNF執行個體已接收個人化資料。個人化資料可包括用於執行新具現化安全性監控VNF可能需要處理工作負載訊務的佈建之資料，包括安全組配資料、安全性監控VNF之一組初始參數、元資料、關於其他VNF之連接資訊、供應商特定資訊、效能資訊、訊務工程資料、服務品質(QoS)參數及策略等。

[0129]在資料流1318中，VNF管理器432將租戶、服務及/或網路安全性策略推送至安全性監控VNF 446，以使得安全性監控VNF 446可更新安全性監控VNF 446之本端策略。網路安全性策略可包括任何安全性相關策略，包括租戶特定安全性處理策略、安全性訊務策略、安全性群組策

略、網路服務處理策略等。應瞭解，此網路安全性策略發佈可經由可靠協定進行。因此，VNF管理器432可維持狀態且確保安全性監控VNF 446接收網路安全性策略及/或個人化資料。

[0130]在資料流1320中，安全性監控VNF 446可將指示個人化及策略更新成功之一指示提供至NFV安全性服務控制器102。在資料流1322中，在更新個人化及安全性策略(例如，自安全性監控VNF 446接收指示，如在資料流1320中)後，VNF管理器432將個人化及/或策略更新經成功執行之指示報告回至NFV安全性服務控制器102。因此，NFV安全性服務控制器102亦可將可能已發生之所有故障及/或錯誤報告回至VNF管理器432。應瞭解，NFV安全性服務控制器102可處理任何報告之故障及/或錯誤，且回應於報告之故障及/或錯誤對NFV安全性架構116之安全性管理員發出警示訊息及/或狀態更新。另外或替代地，NFV安全性服務控制器102可安全地記錄故障及/或錯誤，以及警示訊息及/或狀態更新。

[0131]在資料流1324中，在自VNF管理器432接收成功回應後，NFV安全性服務控制器102可啟動用於跨NFV安全性架構116延伸之工作負載訊務的安全性策略。因此，為實現及啟動用於租戶之工作負載訊務，NFV安全性服務控制器102可安全地與全網路訊務交換元件(諸如，SDN控制器、開放式堆疊中子星外掛程式、各種虛擬及實體交換器/路由器管理等)通訊。

[0132]在一般NFV操作中，安全性監控VNF可經具現化且根據如上文所定義之協定由個人化及策略資訊觸發。在動態且自動之NFV部署中，現有服務、租戶及/或網路策略可經更新且以均勻分散方式跨NFV安全性架構116安全地且不斷地推送(包括至任何實體/混合網路功能)，如安全性策略所指定。此等安全性及監控更新可藉由租戶之添加或移除、租戶工作負載遷移、租戶之服務等級協議(SLA)及QoS之更新、基於地理之更新、調節要求更新、故障等來觸發。如先前所描述，安全性策略之更新可被視為回應於NFV之健康風險緩解安全性威脅(例如，惡意程式碼偵測、網路DoS攻擊及/或其他此等安全性威脅)的校正動作。

[0133]現參看圖14，展示了用於更新安全VNF個人化及策略協定之通訊流程1400之實施例。類似於圖13之通訊流程1300，例示性通訊流程1400包括安全性監控VNF 446、OSS/BSS 402、NFV安全性服務控制器102及VNF管理器432。例示性通訊流程1400另外包括許多資料流，該等資料流中的一些可視實施例而單獨地執行或一起執行。

[0134]應瞭解，在更新通訊流程1400經執行之前，VNF個人化及策略協定之初始佈建(如圖13中所描述)已成功地執行。在資料流1402中，驗證安全性監控VNF與VNF管理器432之間的安全通訊頻道(例如，在圖13之通訊流程1300中建立之安全通訊頻道)。如先前所描述，安全性監控VNF 446及VNF管理器432可能已在其間建立用以通訊之安全、相互鑑別之頻道。因此，在一些實施例中可使用彼已建立

之通訊頻道。然而，在一些其他實施例中，NFV安全性部署策略可定義：新的安全頻道將針對更新程序設置以確保安全性憑證當前仍然有效。

[0135]在資料流1404中，藉由OSS/BSS 402俘獲及/或轉送之系統事件可觸發安全VNF個人化及策略更新程序。如上所述，更新程序可藉由偵測到租戶之添加/移除、回應於網路或系統威脅、其他安全性策略更新等來觸發。應瞭解，系統事件可為自動的、人工的、時間驅動的及/或動態的。在資料流1406中，將新策略自OSS/BSS 402(例如，經由NFV編排器104)傳遞至NFV安全性服務控制器102。在資料流1408中，NFV安全性服務控制器102將新安全性策略、安全性群組及其他相關聯組配更新至安全資料庫(諸如NFV安全性資料庫412)中。

[0136]在資料流1410中，NFV安全性服務控制器102將安全策略更新傳輸至VNF管理器432。應瞭解，NFV安全性服務控制器102傳輸所有受影響VNF管理器。因此，NFV安全性服務控制器102可追蹤VNF管理器以用於所有VNF及/或部署於NFV安全性架構116中之安全性監控VNF。在資料流1412中，VNF管理器432將新策略更新推送至安全性監控VNF 446。應瞭解，新策略更新可被推送至額外之受影響安全性監控VNF執行個體。在接收新策略更新後，安全性監控VNF 446可放棄當前執行，退出、阻擋所有訊務，然後繼續執行，直至接收到另一觸發事項等為止。

[0137]在一些實施例中，在資料流1414中，安全性監控

VNF 446可將指示策略成功地經更新之指示傳輸至NFV安全性服務控制器102。在資料流1416中，VNF管理器432將更新操作之狀態(例如，成功、失敗、錯誤等)之指示提供至NFV安全性服務控制器102。因此，NFV安全性服務控制器102亦可將可能已在策略更新期間發生之所有故障及/或錯誤報告回至VNF管理器432。應瞭解，NFV安全性服務控制器102可處理任何報告之故障及/或錯誤，且回應於報告之故障及/或錯誤對NFV安全性架構116之安全管理員發出警示訊息及/或狀態更新。另外或替代地，NFV安全性服務控制器102可安全地記錄故障及/或錯誤，以及警示訊息及/或狀態更新。

[0138]應瞭解，此等安全性策略更新已跨整個NFV安全性架構116 (例如，NFV、實體及/或混合網路)推送至一或多個其他安全性監控VNF執行個體。在資料流1418中，在接收指示策略更新成功完成之狀態後，可基於安全性策略藉由NFV安全性服務控制器102全網路地啟動新策略。應瞭解，策略更新協定之成功執行應確保NFV部署之安全、恆定之新狀態，包括與實體安全性功能之混合部署。

實例

[0139]下文提供本文中所揭示之技術的例示性實例。技術之實施例可包括下文所描述之實例中之任何一或多個及其任何組合。

[0140]實例1包括一種用於執行一網路功能虛擬化(NFV)架構中之安全性監控的安全性監控虛擬網路功能

(VNF)，該安全性監控VNF包含：一或多個處理器；及一或多個記憶體裝置，該一或多個記憶體裝置中儲存有在藉由該一或多個處理器執行時使該安全性監控VNF進行以下操作的多個指令：自與該安全性監控VNF網路通訊的該NFV架構之一NFV安全性服務控制器接收佈建資料；使用該佈建資料之至少一部分執行與該NFV架構之一VNF管理器之一相互鑑別密鑰交換程序，以建立該安全性監控VNF與該VNF管理器之間的一安全通訊路徑；經由該安全通訊路徑自該VNF管理器接收個人化資料，其中該個人化資料包括可用以組配該安全性監控VNF之一或多個安全性功能的資料；及執行一個人化操作以基於該個人化資料來組配該安全性監控VNF。

[0141] 實例2包括實例1之標的物，且其中該等多個指令進一步使該安全性監控VNF進行以下操作：經由該安全通訊路徑自該VNF管理器接收策略資訊；及執行一策略更新操作以更新該安全性監控VNF之一安全性策略。

[0142] 實例3包括實例1及實例2中任一者之標的物，且其中該策略資訊包括一租戶特定安全性處理策略、一安全性訊務策略、一安全性群組策略及一網路服務處理策略中之至少一者。

[0143] 實例4包括實例1至實例3中任一者之標的物，且其中用以接收該佈建資料包含用以使用一帶外通訊接收該佈建資料。

[0144] 實例5包括實例1至實例4中任一者之標的物，且

其中該佈建資料包括該安全性監控VNF之一唯一識別符、該安全性監控VNF正被執行所在的一平台之一唯一識別符及一安全性憑證。

[0145] 實例6包括實例1至實例5中任一者之標的物，且其中用以執行該相互鑑別密鑰交換程序包含用以使用該安全性憑證來執行該相互鑑別密鑰交換程序。

[0146] 實例7包括實例1至實例6中任一者之標的物，且其中該等多個指令進一步使該安全性監控VNF進行以下操作：經由該安全通訊路徑將安全性監控資訊傳輸至該VNF管理器，其中該安全性監控資訊包括該安全性監控VNF之記錄檔、警示訊息及統計資料中之至少一者。

[0147] 實例8包括實例1至實例7中任一者之標的物，且其中該個人化資料包括以下各者中之至少一者：安全組配資料、該安全性監控VNF之一組初始參數、該NFV架構的元資料、關於其他VNF之連接資訊、供應商特定資訊、效能資料、工作負載訊務工程資料及服務品質(QoS)參數及策略。

[0148] 實例9包括實例1至實例8中任一者之標的物，且其中該等多個指令進一步使該安全性監控VNF進行以下操作：將一個人化操作狀態及一策略更新操作狀態傳輸至該VNF管理器，其中該個人化操作狀態及該策略更新操作狀態可由該NFV安全性服務控制器使用以判定針對由該安全性監控VNF監控的網路訊務是否啓動一全網路安全性策略。

[0149] 實例10包括一種用於一網路功能虛擬化(NFV)架構中之一安全性監控虛擬網路功能(VNF)的安全個人化之方法，該方法包含：藉由該安全性監控VNF，自與該安全性監控VNF網路通訊的該NFV架構之一NFV安全性服務控制器接收佈建資料；藉由該安全性監控VNF，使用該佈建資料之至少一部分執行與該NFV架構之一VNF管理器之一相互鑑別密鑰交換程序，以建立該安全性監控VNF與該VNF管理器之間的一安全通訊路徑；藉由該安全性監控VNF，經由該安全通訊路徑自該VNF管理器接收個人化資料，其中該個人化資料包括可用以組配該安全性監控VNF之一或多個安全性功能的資料；及藉由該安全性監控VNF，執行一個人化操作以基於該個人化資料來組配該安全性監控VNF。

[0150] 實例11包括實例10之標的物，且其進一步包含：藉由該安全性監控VNF，經由該安全通訊路徑自該VNF管理器接收策略資訊；及藉由該安全性監控VNF，執行一策略更新操作以更新該安全性監控VNF之一安全性策略。

[0151] 實例12包括實例10及實例11中任一者之標的物，且其中接收該策略資訊包含接收一租戶特定安全性處理策略、一安全性訊務策略、一安全性群組策略及一網路服務處理策略中之至少一者。

[0152] 實例13包括實例10至實例12中任一者之標的物，且其中接收該佈建資料包含使用一帶外通訊接收該佈建資料。

[0153] 實例 14 包括實例 10 至實例 13 中任一者之標的物，且其中該佈建資料包括該安全性監控 VNF 之一唯一識別符、該安全性監控 VNF 正被執行所在的一平台之一唯一識別符及一安全性憑證。

[0154] 實例 15 包括實例 10 至實例 14 中任一者之標的物，且其中執行該相互鑑別密鑰交換程序包含使用該安全性憑證來執行該相互鑑別密鑰交換程序。

[0155] 實例 16 包括實例 10 至實例 15 中任一者之標的物，且其進一步包括：藉由該安全性監控 VNF，經由該安全通訊路徑將安全性監控資訊傳輸至該 VNF 管理器，其中該安全性監控資訊包括該安全性監控 VNF 之記錄檔、警示訊息及統計資料中之至少一者。

[0156] 實例 17 包括實例 10 至實例 16 中任一者之標的物，且其中接收個人化資料包含接收以下各者中之至少一者：安全組配資料、該安全性監控 VNF 之一組初始參數、該 NFV 架構的元資料、關於其他 VNF 之連接資訊、供應商特定資訊、效能資料、工作負載訊務工程資料及服務品質 (QoS) 參數及策略。

[0157] 實例 18 包括實例 10 至實例 17 中任一者之標的物，且其進一步包含：藉由該安全性監控 VNF，將一個人化操作狀態及一策略更新操作狀態傳輸至該 VNF 管理器，其中該個人化操作狀態及該策略更新操作狀態可由該 NFV 安全性服務控制器使用以判定針對由該安全性監控 VNF 監控的網路訊務是否啟動一全網路安全性策略。

[0158] 實例19包括一種計算裝置，其包含：一處理器；及儲存有多個指令之記憶體，該等多個指令在由該處理器執行時使該計算裝置執行實例10至18中任一者之方法。

[0159] 實例20包括一或多個機器可讀儲存媒體，該一或多個機器可讀儲存媒體包含儲存於其上的回應於經執行而使計算裝置執行實例10至18中任一者之方法。

[0160] 實例21包括一種用於執行一網路功能虛擬化(NFV)架構中之安全性監控的安全性監控虛擬網路功能(VNF)，該安全性監控VNF包含：佈建管理電路系統，其用以進行以下操作：自與該安全性監控VNF網路通訊的該NFV架構之一NFV安全性服務控制器接收佈建資料；及使用該佈建資料之至少一部分執行與該NFV架構之一VNF管理器之一相互鑑別密鑰交換程序，以建立該安全性監控VNF與該VNF管理器之間的一安全通訊路徑；及個人化管理電路系統，其用以進行以下操作：經由該安全通訊路徑自該VNF管理器接收個人化資料，其中該個人化資料包括可用以組配該安全性監控VNF之一或多個安全性功能的資料；及執行一個人化操作以基於該個人化資料來組配該安全性監控VNF。

[0161] 實例22包括實例21之標的物，且其進一步包括策略更新管理電路系統，其用以進行以下操作：經由該安全通訊路徑自該VNF管理器接收策略資訊；及執行一策略更新操作以更新該安全性監控VNF之一安全性策略。

[0162] 實例23包括實例21及實例22中任一者之標的

物，且其中該策略資訊包括一租戶特定安全性處理策略、一安全性訊務策略、一安全性群組策略及一網路服務處理策略中之至少一者。

[0163] 實例24包括實例21至實例23中任一者之標的物，且其中用以接收該佈建資料包含用以使用一帶外通訊接收該佈建資料。

[0164] 實例25包括實例21至實例24中任一者之標的物，且其中該佈建資料包括該安全性監控VNF之一唯一識別符、該安全性監控VNF正被執行所在的一平台之一唯一識別符及一安全性憑證。

[0165] 實例26包括實例21至實例25中任一者之標的物，且其中用以執行該相互鑑別密鑰交換程序包含用以使用該安全性憑證來執行該相互鑑別密鑰交換程序。

[0166] 實例27包括實例21至實例26中任一者之標的物，且其進一步包括：安全性監控電路系統，其用以經由該安全通訊路徑將安全性監控資訊傳輸至該VNF管理器，其中該安全性監控資訊包括該安全性監控VNF之記錄檔、警示訊息及統計資料中之至少一者。

[0167] 實例28包括實例21至實例27中任一者之標的物，且其中該個人化資料包括以下各者中之至少一者：安全組配資料、該安全性監控VNF之一組初始參數、該NFV架構的元資料、關於其他VNF之連接資訊、供應商特定資訊、效能資料、工作負載訊務工程資料及服務品質(QoS)參數及策略。

[0168] 實例29包括實例21至實例28中任一者之標的物，且其中該個人化管理電路系統進一步用以將一個人化操作狀態及一策略更新操作狀態傳輸至該VNF管理器，其中該個人化操作狀態及該策略更新操作狀態可由該NFV安全性服務控制器使用以判定針對由該安全性監控VNF監控的網路訊務是否啟動一全網路安全性策略。

[0169] 實例30包括一種用於執行一網路功能虛擬化(NFV)架構中之安全性監控的安全性監控虛擬網路功能(VNF)，該安全性監控VNF包含：佈建管理電路系統，其用以自與該安全性監控VNF網路通訊的該NFV架構之一NFV安全性服務控制器接收佈建資料；用於使用該佈建資料之至少一部分執行與該NFV架構之一VNF管理器之一相互鑑別密鑰交換程序，以建立該安全性監控VNF與該VNF管理器之間的一安全通訊路徑之構件；個人化管理電路系統，其用以經由該安全通訊路徑自該VNF管理器接收個人化資料，其中該個人化資料包括可用以組配該安全性監控VNF之一或多個安全性功能的資料；及用於藉由該安全性監控VNF執行一個人化操作以基於該個人化資料來組配該安全性監控VNF之構件。

[0170] 實例31包括實例30之標的物，且其進一步包括：策略更新管理電路系統，其用以經由該安全通訊路徑自該VNF管理器接收策略資訊；及用於執行一策略更新操作以更新該安全性監控VNF之一安全性策略之構件。

[0171] 實例32包括實例30及實例31中任一者之標的

物，且其中用於接收該策略資訊的該構件包含用於接收一租戶特定安全性處理策略、一安全性訊務策略、一安全性群組策略及一網路服務處理策略中之至少一者之構件。

[0172] 實例33包括實例30至實例32中任一者之標的物，且其中用於接收該佈建資料的該構件包含用於使用一帶外通訊接收該佈建資料之構件。

[0173] 實例34包括實例30至實例33中任一者之標的物，且其中該佈建資料包括該安全性監控VNF之一唯一識別符、該安全性監控VNF正被執行所在的一平台之一唯一識別符及一安全性憑證。

[0174] 實例35包括實例30至實例34中任一者之標的物，且其中用於執行該相互鑑別密鑰交換程序的該構件包含用於使用該安全性憑證來執行該相互鑑別密鑰交換程序之構件。

[0175] 實例36包括實例30至實例35中任一者之標的物，且其進一步包括：用於經由該安全通訊路徑將安全性監控資訊傳輸至該VNF管理器之構件，其中該安全性監控資訊包括該安全性監控VNF之記錄檔、警示訊息及統計資料中之至少一者。

[0176] 實例37包括實例30至實例36中任一者之標的物，且其中用於接收個人化資料的該構件包含用於接收以下各者中之至少一者之構件：安全組配資料、該安全性監控VNF之一組初始參數、該NFV架構的元資料、關於其他VNF之連接資訊、供應商特定資訊、效能資料、工作負載

訊務工程資料及服務品質(QoS)參數及策略。

[0177]實例38包括實例30至實例37中任一者之標的物，且其進一步包括用於將一個人化操作狀態及一策略更新操作狀態傳輸至該VNF管理器之構件，其中該個人化操作狀態及該策略更新操作狀態可由該NFV安全性服務控制器使用以判定針對由該安全性監控VNF監控的網路訊務是否啓動一全網路安全性策略。

【符號說明】

100...用於監控網路通訊之安全性的系統	212...基本輸入/輸出系統(BIOS)
102...NFV安全性服務控制器	214、308...資料儲存裝置
104...NFV編排器	216...安全時鐘
106...虛擬基礎結構管理器(VIM)	218、312...通訊電路系統
108...NFV基礎結構	220...網路介面卡(NIC)
110、112、114...計算節點	222...交換器
116...網路功能虛擬化(NFV)安全性架構	224...安全性引擎
118、120...端點裝置	310...周邊裝置
202、302...處理器	402...操作支援系統及商務支援系統(OSS/BSS)
204...受信任執行環境(TEE)支援	404...通訊頻道
206、304...輸入/輸出(I/O)子系統	406、414、416、418、430、434、436、466、474、488、490...安全通訊頻道
208、306...記憶體	408...SFC安全性控制器
210...安全記憶體	410...審計資料庫

412...NFV安全性資料庫	520...安全性監視政策管理模組
420...NFV安全性服務提供者	522...安全性監控策略發佈模組
422...SFC安全性提供者	524...安全性監控策略施行模組
424...VIM控制器	530...受保護傳輸控制模組
426、448、458、460、468、	534...訊息鑑認模組
486...NFV安全性服務代理	540...NFV 安全性服務代理控
428...VIM組件	制模組
432...VNF管理器	550...遙測資料審計模組
438...NFV安全性監控分析系統	602、1204...安全性策略資料庫
440...NFVI	604...遙測資料庫
442...網路VNF	620...遙測資料監控模組
444...封包處理器	622...SFC遙測資料監控模組
446...安全性監控VNF	630...遙測資料封包模組
450...服務功能鏈	632...SFC遙測資料封包模組
452...服務功能鏈VNF	640...啟動過程執行模組
454、456...VNF	700...用於管理NFV 安全性架構
462...超管理器	之安全性監控服務的方法
464...虛擬路由器	702、704、706、708、710、712、
470...SFC代理	714、716、718、720、722、
472...安全性監控收集代理	724、802、804、806、808、
480、482、484...平台	810、812、1002、1004、
492...VSF目錄資料庫	1006、1008、1010、1012、
500、600、1200...環境	1014、1016、1018、1020、
510、610...安全通訊模組	1022...區塊

800...用於更新安全性監控政策之方法	1000...用於監控NFV安全性架構之安全性的方法
902、904、906、908、910、912、914、916、918、920、922、924、926、1102、1104、1106、1108、1110、1112、1114、1116、1118、1120、1302、1304、1306、1308、1310、1312、1314、1316、1318、1320、1322、1324、1402、1404、1406、1408、1410、1412、1414、1416、1418...資料流	1100...用於監控NFV安全性架構之服務功能鏈接(SFC)之安全性的通訊流程 1202...個人化資料庫 1210...佈建管理模組 1220...個人化管理模組 1230...策略更新管理模組 1240...安全性監控模組 1300...用於佈建安全VNF個人化及策略協定之通訊流程 1400...用於更新安全VNF個人化及策略協定之通訊流程

申請專利範圍

1. 一種計算平台，其包含：

一網路介面控制器，

一記憶體裝置；以及

耦接至該網路介面控制器以及該記憶體裝置之至少一處理器，該至少一處理器用以執行用於一虛擬網路功能(VNF)之一安全性服務代理，即用以進行下列動作：

接收至少一網路協定(IP)位址及一初始根安全性憑證；

使用該安全性憑證來執行與一VNF管理器之一相互鑑別密鑰交換程序之部分，以建立一安全且受信任的頻道；

開啟與該VNF管理器之一管理頻道；

使用該管理頻道來致使至該VNF管理器之資訊的傳輸；

從該VNF管理器接收個人化資料，其中該個人化資料包含下列一或多者：安全組配資料、安全性監控VNF參數之一初始組、元資料、關於其他VNF之連接資訊、供應商特定資訊、效能資訊、訊務工程資料、或一服務品質(QoS)參數或策略之至少一者；以及

從該VNF管理器接收至少包含下列一或多者之一策略：一租戶特定安全性處理策略、一安全性訊務

策略、一安全性群組策略、或一網路服務處理策略。

2. 如請求項1之計算平台，其中，使用該安全性憑證來執行與VNF管理器之相互鑑別密鑰交換程序之部分以建立一安全且受信任的頻道包括傳輸層安全性(TLS)之使用。
3. 如請求項1之計算平台，其中該資訊包含下列一或多者：記錄檔、警示訊息、統計。
4. 如請求項1之計算平台，其中從該VNF管理器所接收之該個人化資料包含一可靠協定之使用。
5. 如請求項1之計算平台，其中該至少一處理器係用以儲存用於在一服務功能鏈中之VNF間之連接的狀態。
6. 如請求項1之計算平台，其中用於一VNF之該安全性服務代理係關聯於下列一或多者：一超管理器、或一硬體實體平台。
7. 一種用以執行用於一虛擬網路功能(VNF)之一安全性服務代理的方法，其包含：

接收至少一網路協定(IP)位址及一初始根安全性憑證；

使用該安全性憑證來執行與一VNF管理器之一相互鑑別密鑰交換程序之部分，以建立一安全且受信任的頻道；

開啟與該VNF管理器之一管理頻道；

使用該管理頻道來致使至該VNF管理器之資訊的傳輸；

從該 VNF 管理器接收個人化資料，其中該個人化資料包含下列一或多者：安全組配資料、安全性監控 VNF 參數之一初始組、元資料、關於其他 VNF 之連接資訊、供應商特定資訊、效能資訊、訊務工程資料、或一服務品質(QoS)參數或策略之至少一者；以及

從該 VNF 管理器接收至少包含下列一或多者之一策略：一租戶特定安全性處理策略、一安全性訊務策略、一安全性群組策略、或一網路服務處理策略。

8. 如請求項7之方法，其中使用該安全性憑證來執行與一 VNF 管理器之一相互鑑別密鑰交換程序之部分以建立一安全且受信任的頻道包括使用傳輸層安全性(TLS)。
9. 如請求項7之方法，其包含儲存用於在一服務功能鏈中之 VNF 間之連接的狀態。
10. 如請求項7之方法，其中用於 VNF 之該安全性服務代理係關聯於下列一或多者：一超管理器、或一硬體實體平台。
11. 一種包含指令儲存於其上之非暫態電腦可讀取媒體，當該等指令被至少一處理器執行時會致使該至少一處理器用以執行用於一虛擬網路功能(VNF)之一安全性服務代理，其用以執行如請求項7至10之任一或多項之方法。
12. 一種計算平台，其包含：
 - 一網路介面控制器；
 - 一記憶體裝置；以及
 - 至少一處理器，其耦接至該網路介面控制器及該記憶體

裝置，該至少一處理器用以執行用於一虛擬網路功能(VNF)之一安全性服務代理，即用以進行下列動作：

建立部分之安全相互鑑別頻道以與一VNF管理器通訊；

要確保安全性憑證係目前的且啟用的，使用該安全相互鑑別頻道，或建立及使用用以與該VNF管理器通訊之一新的安全頻道；

從該VNF管理器接收一策略更新；並且

基於該策略更新的接收，執行下列至少一或多者：放棄當前執行、退出、阻擋至少一些訊務、或繼續執行直至接收到一觸發為止，其中從該VNF管理器接收一策略更新係基於一系統事件，其包含一附加或是移除租戶、一網路或是系統威脅、或是其他安全性策略更新。

13. 如請求項12之計算平台，其中該系統事件係下列至少一或多者：自動的、人工的、時間驅動的、或動態的。

14. 如請求項12之計算平台，其中用於一VNF之該安全性服務代理係關聯於下列一或多者：一超管理器、或一硬體實體平台。

15. 一種執行用於一虛擬網路功能(VNF)之一安全性服務代理的方法，該方法包含：

建立部分之安全相互鑑別頻道以與一VNF管理器通訊；

要確保安全性憑證係目前的且啟用的，使用該安全相互鑑別頻道或建立及使用一新的安全頻道，用於與該

VNF管理器通訊；

從該VNF管理器接收一策略更新；並且

基於該策略更新之接收，執行下列至少一或多者：

放棄當前執行、退出、阻擋至少一些訊務、或繼續執行直至接收到一觸發為止，其中從該VNF管理器接收一策略更新係基於一系統事件，其包含一附加或是移除租戶、一網路或是系統威脅、或其他安全性策略更新。

16. 如請求項15之方法，其中該系統事件係下列至少一或多者：自動的、人工的、時間驅動的、或動態的。

17. 如請求項15之方法，其中用於一VNF之該安全性服務代理係關聯於下列一或多者：一超管理器、或一硬體實體平台。

18. 一種包含指令儲存於其上之非暫態電腦可讀取媒體，當該指令由至少一處理器執行，致使該至少一處理器去執行用於一虛擬網路功能(VNF)之安全性服務代理，其執行請求項15至17之任一或多者之方法。

19. 一種計算平台，其包含：

一網路介面控制器；

一記憶體裝置；以及

至少一處理器，其耦接至該網路介面控制器及該記憶體裝置，該至少一處理器用以執行一虛擬網路功能管理器(VNFM)，其係用以：

從一網路功能虛擬化(NFV)安全性控制器接收下列一或多者：用於一虛擬網路功能(VNF)之一安全性服

務代理(SSA)之一識別符、一平台之識別符、由該NFV
安全性控制器所使用以佈建一SSA之一安全憑證；

使用該安全性憑證以執行與用於該VNF之該SSA
之一相互鑑別密鑰交換程序之部分，來建立一安全且信
任的頻道；

使用一管理頻道來從用於該VNF之該SSA接收資
訊；

從該NFV安全性控制器接收用於安全性監控之一
策略；

推送個人化資料至用於該VNF之該SSA；

推送該租戶、服務、或網路安全性策略之一或多者
至用於該VNF之該SSA；以及

提供該個人化以及策略更新係成功之一指示至該
NFV安全性控制器。

20. 如請求項19之計算平台，其中該至少一處理器係用以：
藉由使用該安全且信任的頻道或是建立並使用一新安
全頻道，來確保安全性憑證仍係目前的且啟用的，以用
於與該SSA之一更新程序。

21. 如請求項19之計算平台，其中該至少一處理器係用以：
從該NFV安全性控制器接收一安全策略更新。

22. 如請求項19之計算平台，其中該至少一處理器係用以：
推送一新策略更新至用於該VNF之該安全性服務代理。

23. 如請求項19之計算平台，其中該至少一處理器係用以：
接收在用於該VNF之該安全性服務代理之該策略係成

功的被更新之一指示；以及

提供具有包含至少成功、失敗、或是錯誤之該更新操作之一狀態之一指示至該NFV安全性控制器。

24. 一種執行一虛擬網路功能管理器(VNFM)的方法，該方法包含：

從一網路功能虛擬化(NFV)安全性控制器接收下列一或多者：用於一虛擬網路功能(VNF)之一安全性服務代理(SSA)之一識別符、一平台之識別符、及由該NFV安全性控制器所使用以佈建一SSA之一安全憑證；

使用該安全性憑證以執行與用於該 VNF 之該 SSA 之一相互鑑別密鑰交換程序之部分，來建立一安全且信任的頻道；

使用一管理頻道從用於該 VNF 之該 SSA 接收資訊；

從該 NFV 安全性控制器接收用於安全性監控之一策略；

推送個人化資料至用於該 VNF 之該 SSA；

推送該租戶、服務、或網路安全性策略之一或多者至用於該 VNF 之該 SSA；以及

提供該個人化以及策略更新係成功之一指示至該 NFV 安全性控制器。

25. 如請求項24之方法，該方法包含：

藉由使用該安全且信任的頻道或是建立並使用一新的安全頻道，來確保安全性憑證仍係目前的且啟用的，以用於與該 SSA 之一更新程序。

26. 如請求項24之方法，該方法包含：

從該NFV安全性控制器接收一安全策略更新。

27. 如請求項24之方法，該方法包含：

推送一新的策略更新至用於該VNF之該安全性服務代理。

28. 如請求項24之方法，該方法包含：

接收在用於該VNF之該安全性服務代理之該策略係成功的被更新之一指示；以及

提供具有包含至少成功、失敗、或是錯誤之該更新操作之一狀態之一指示至該NFV安全性控制器。

29. 一種非暫態電腦可讀媒體，其包含儲存於其上之指令，當由至少一處理器執行時，致使該至少一處理器用以執行一虛擬網路功能管理器(VNFM)，其用來執行如請求項24至28之任一或多項之方法。

圖式

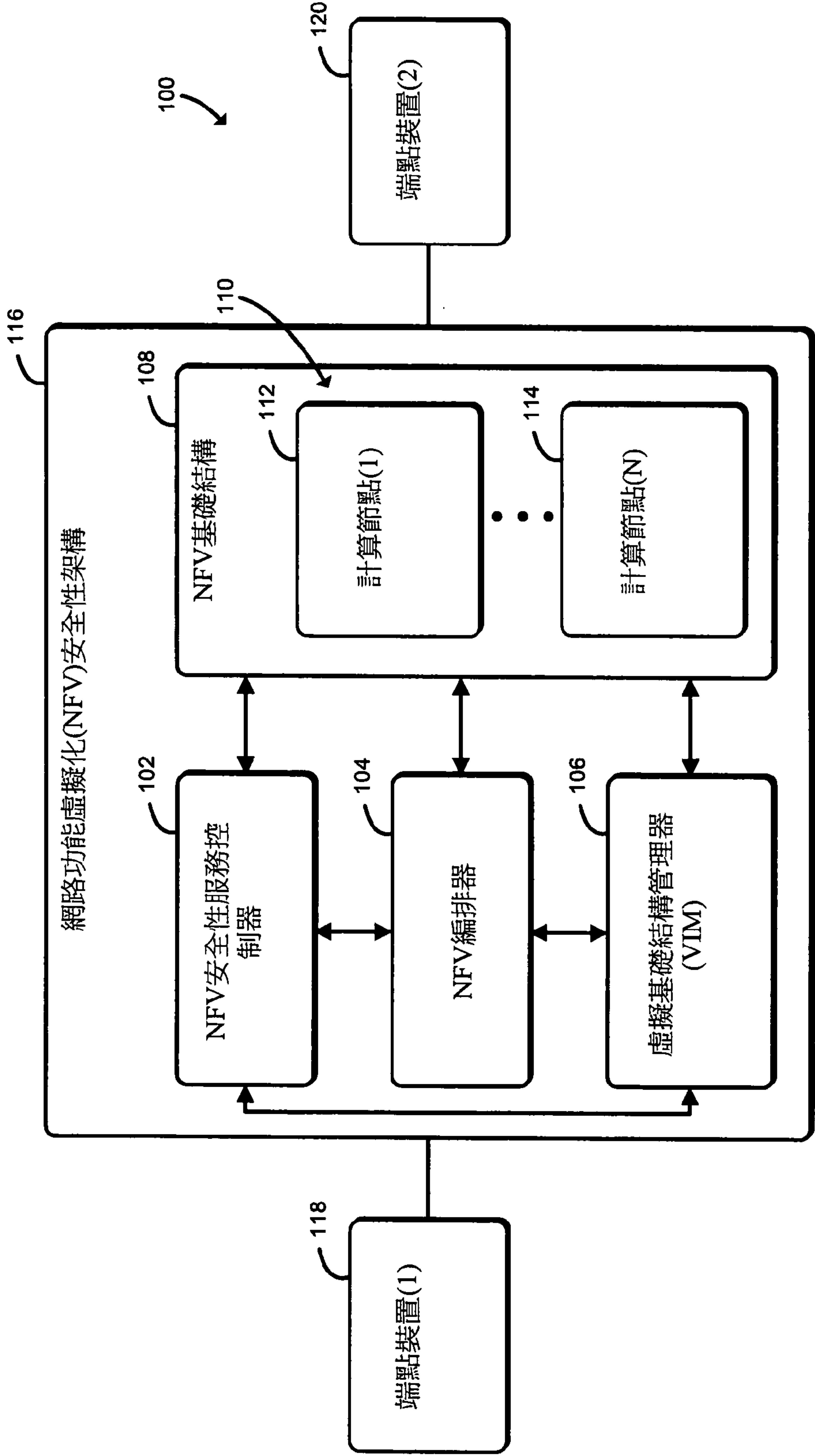


圖1

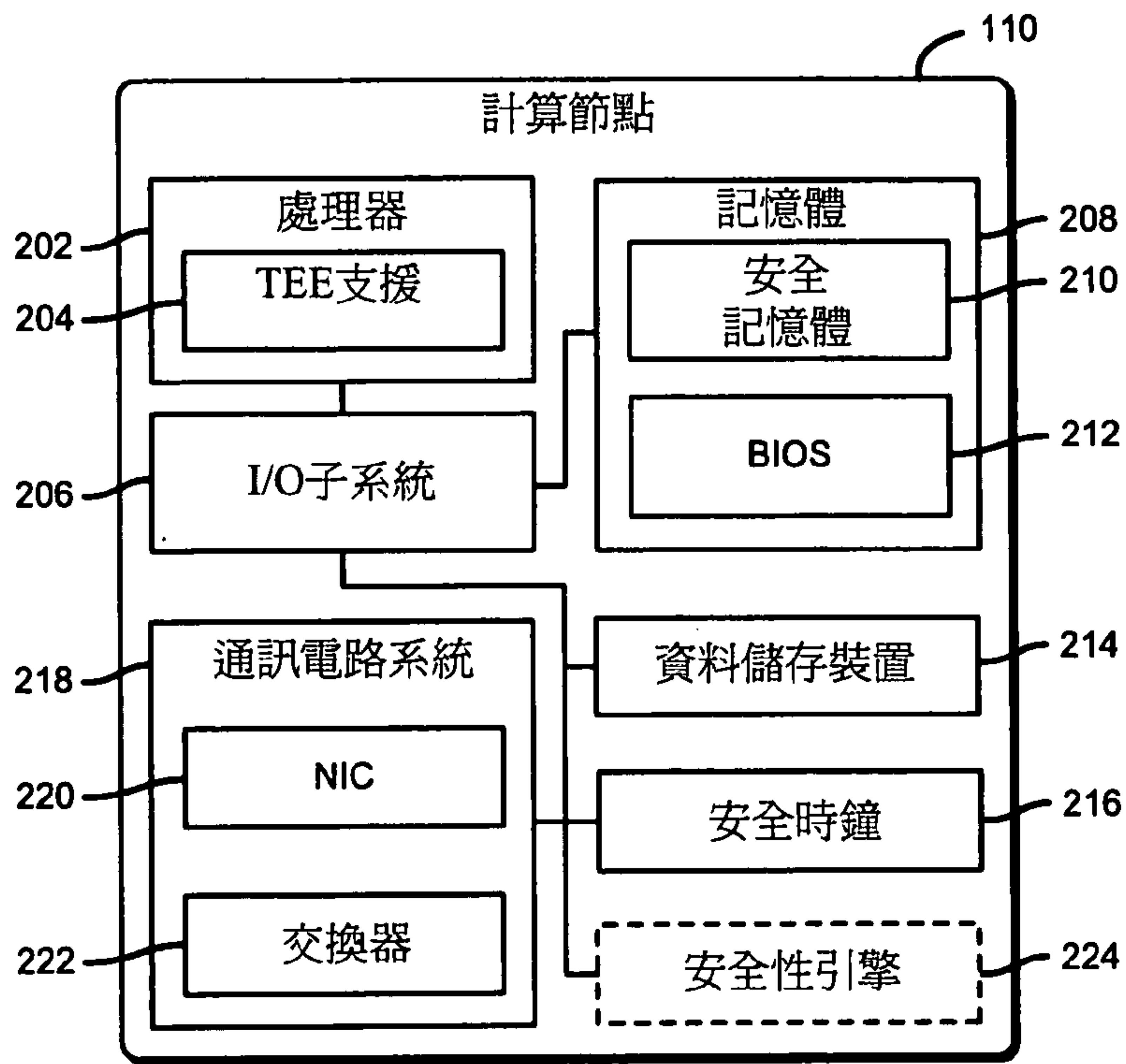


圖2

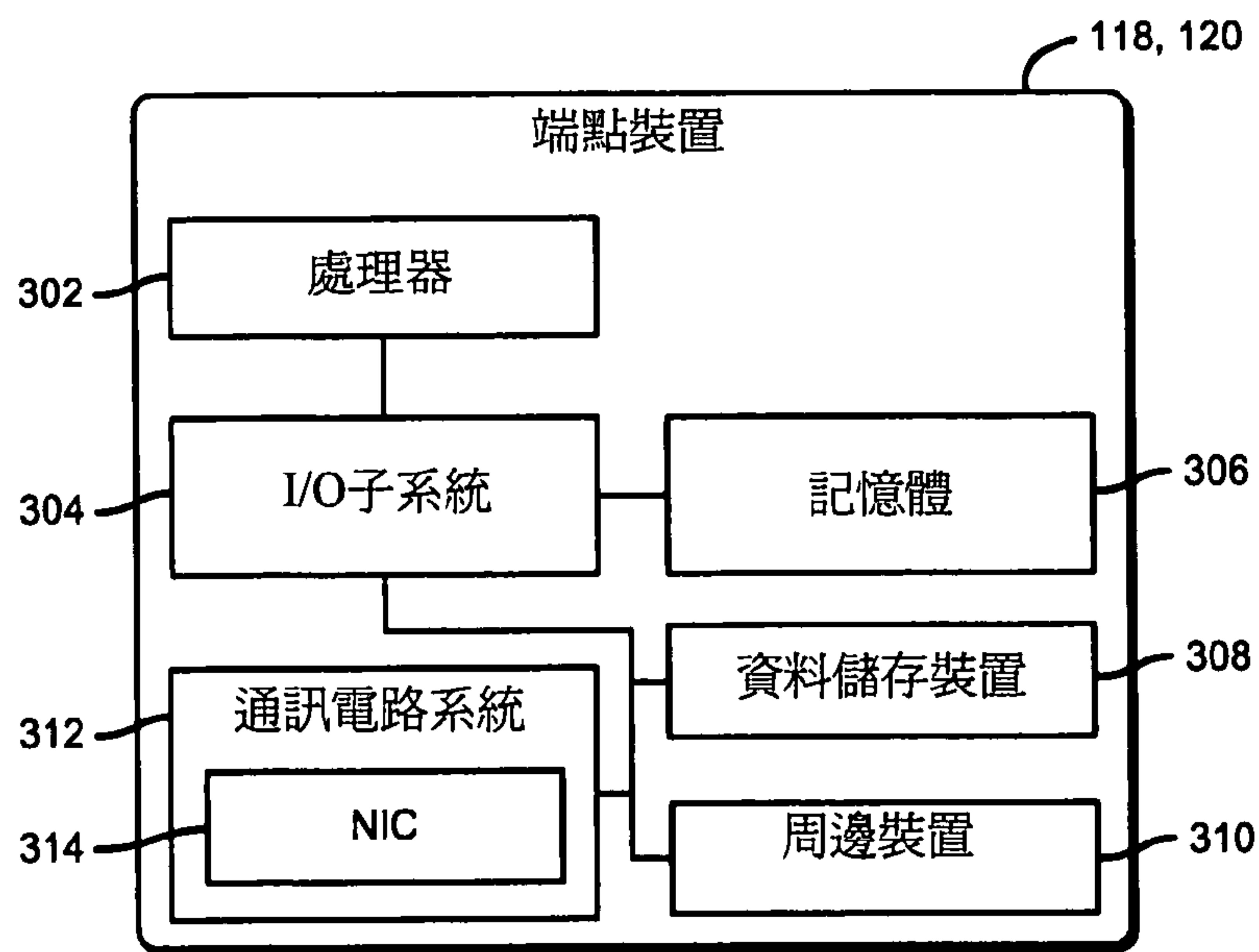
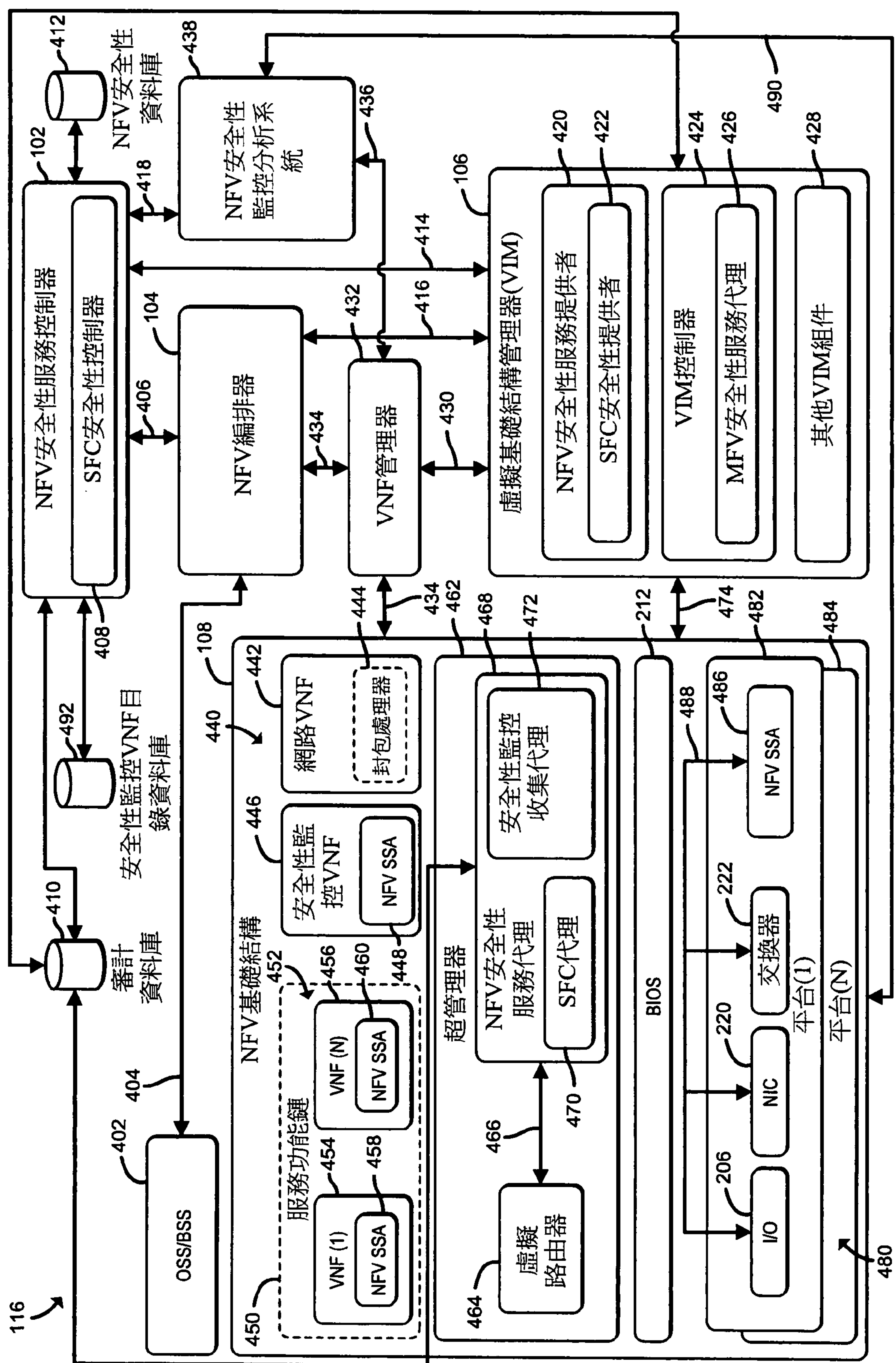


圖3



回

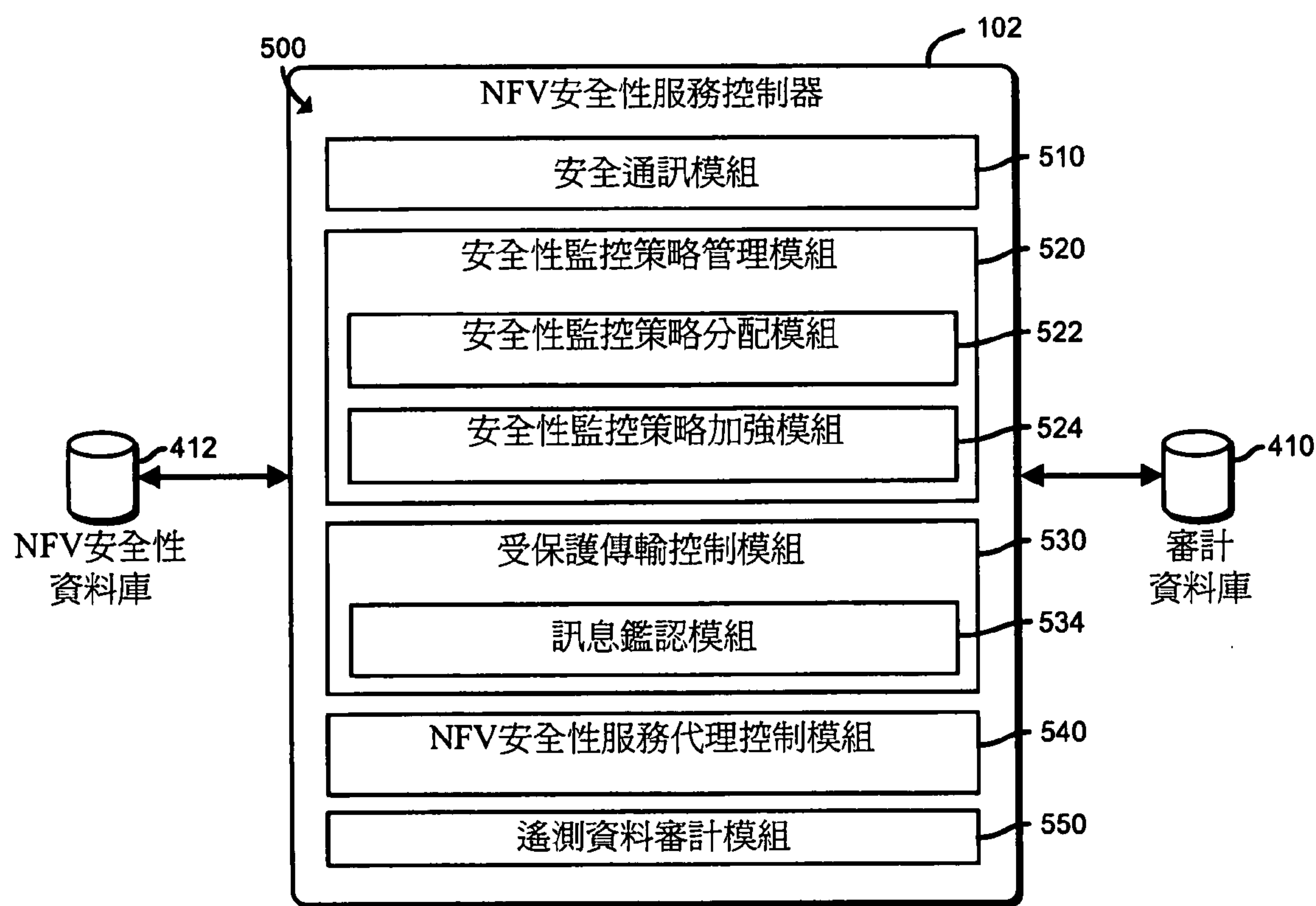


圖5

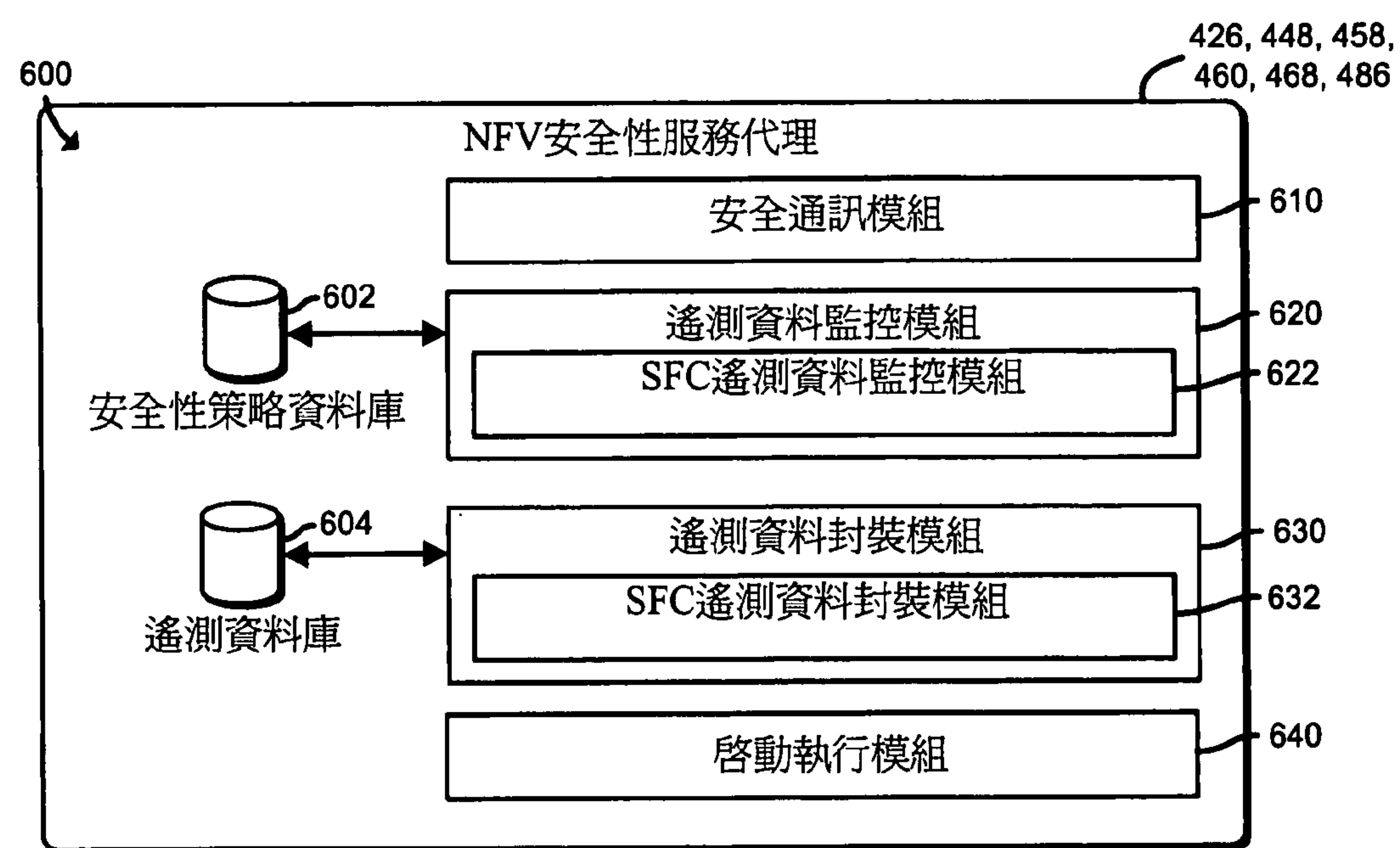


圖6

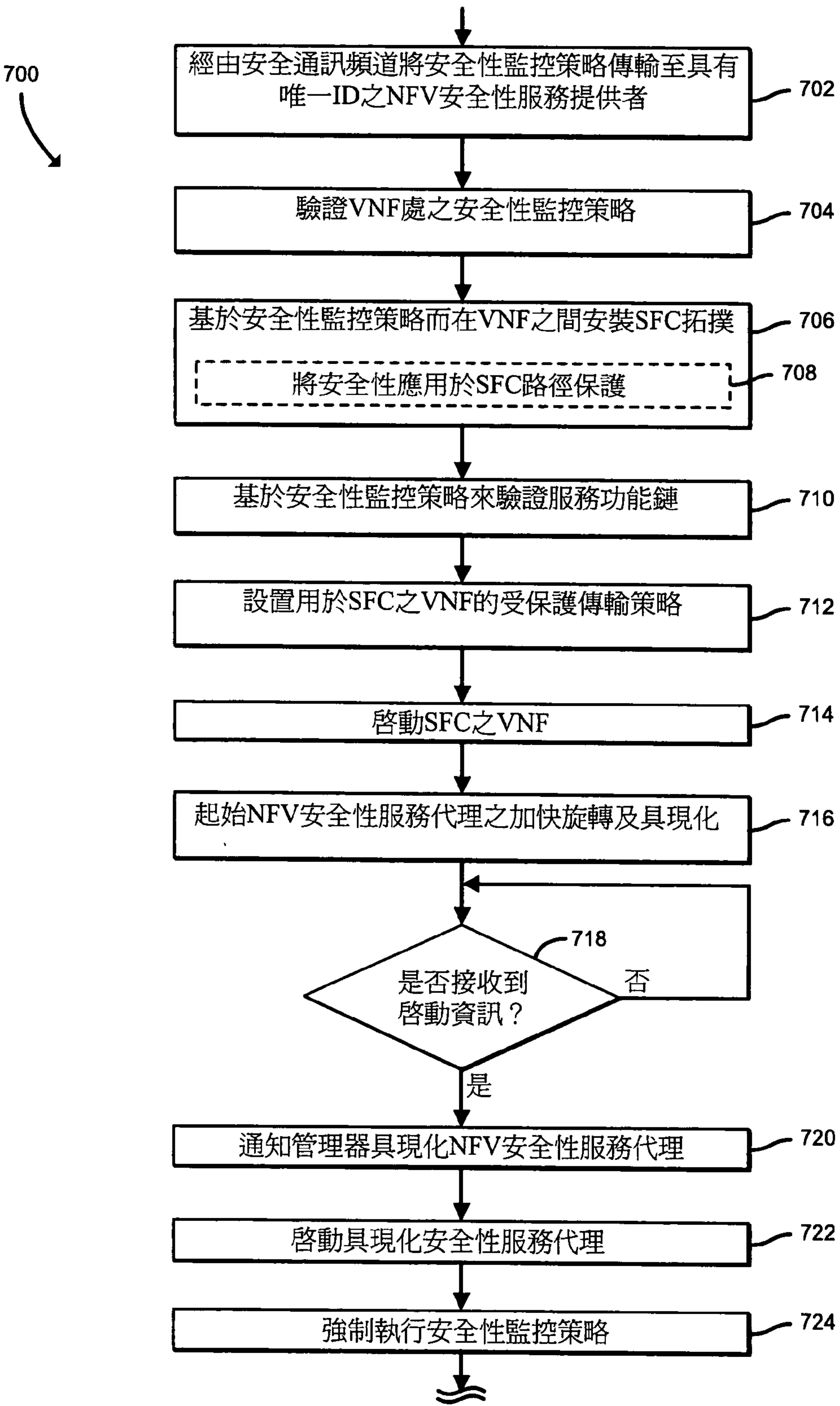


圖7

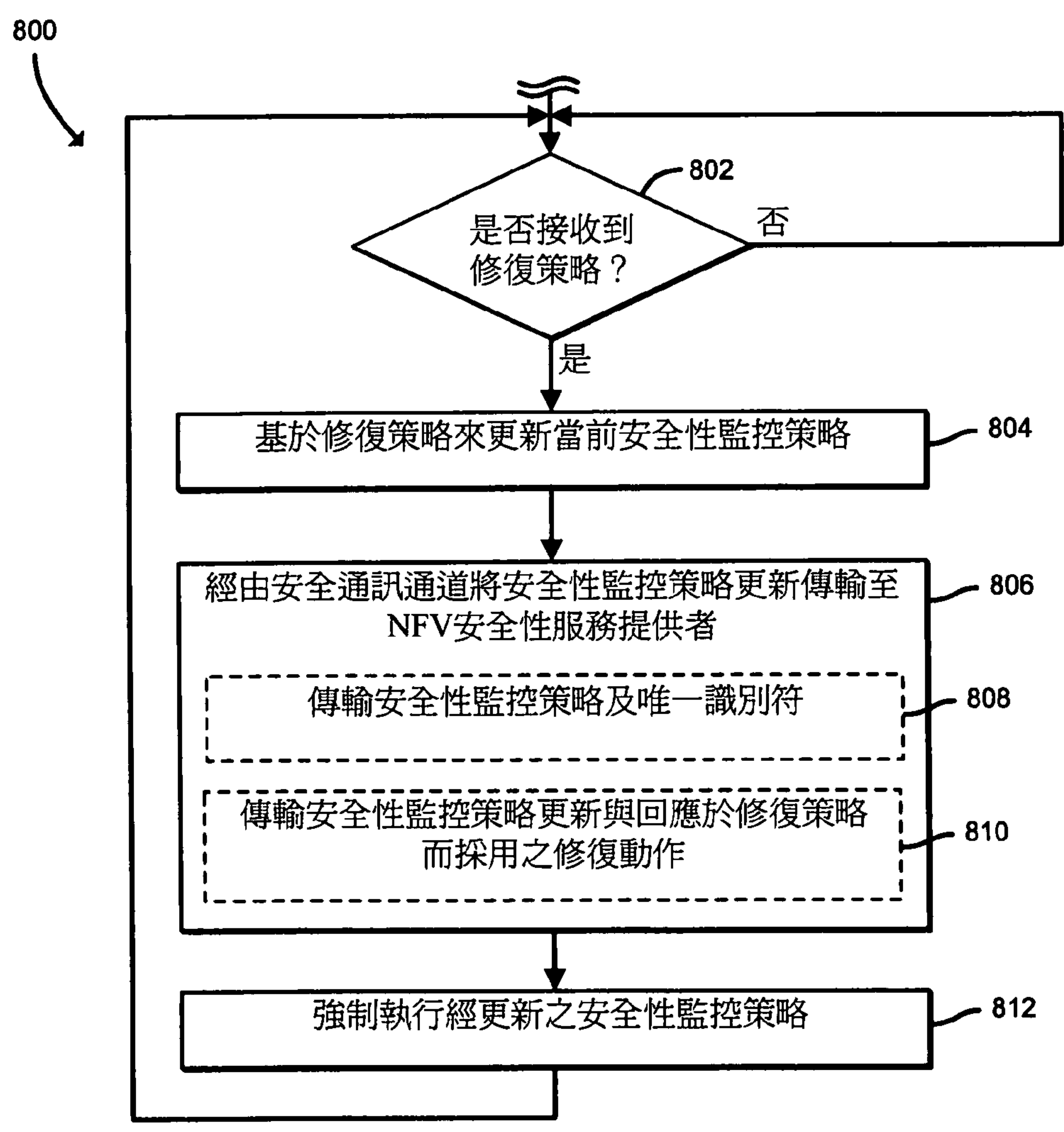


圖8

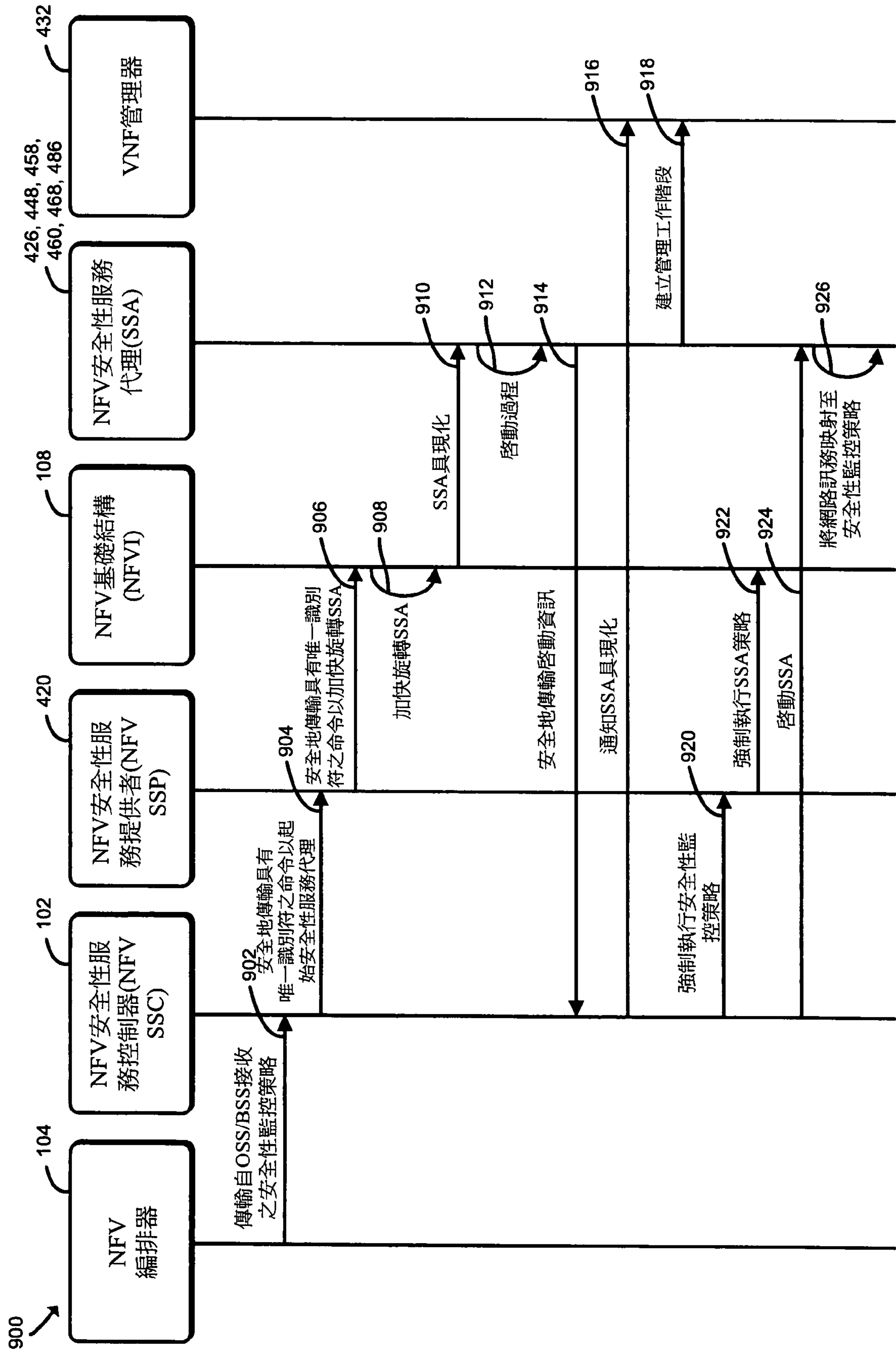


圖9



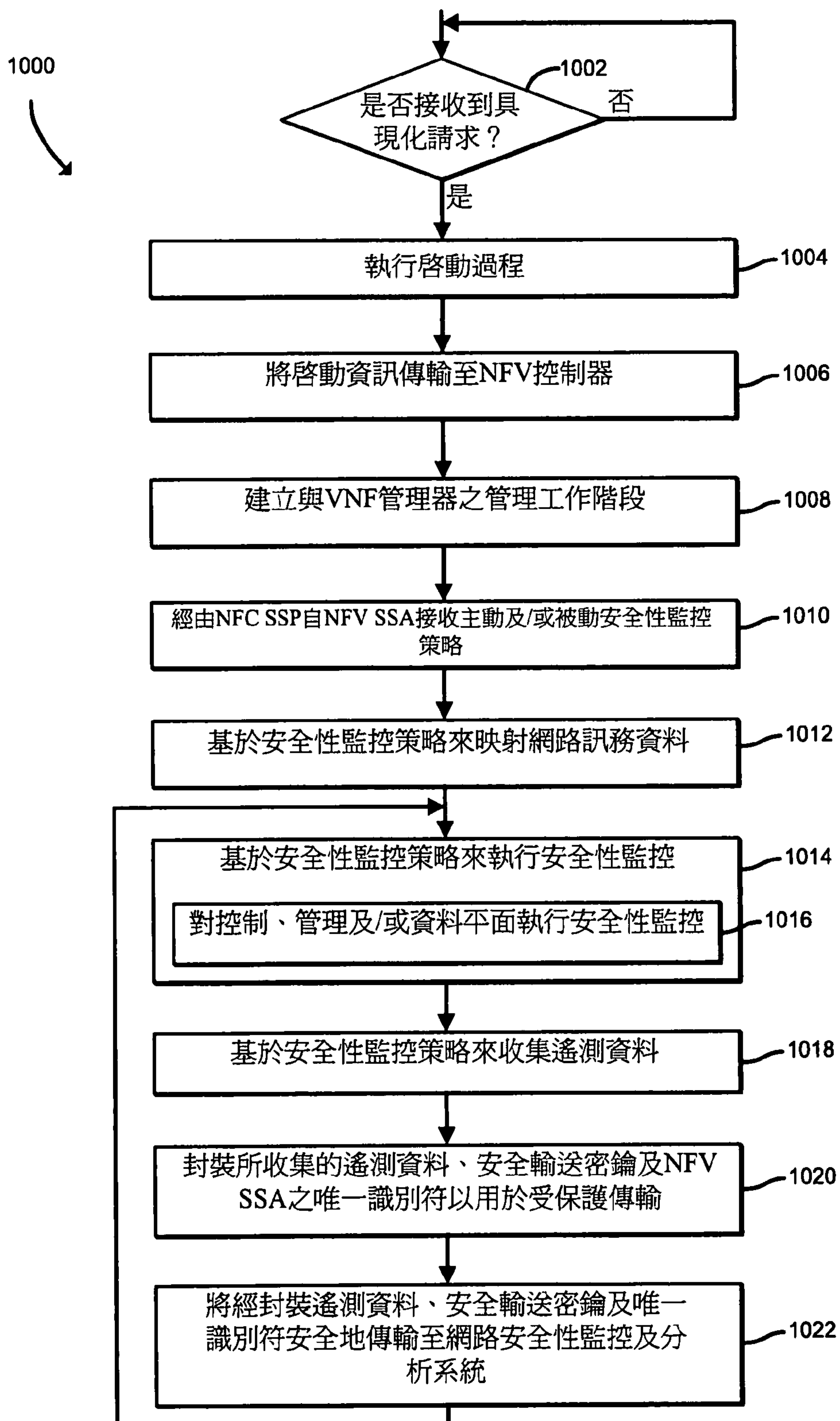


圖10

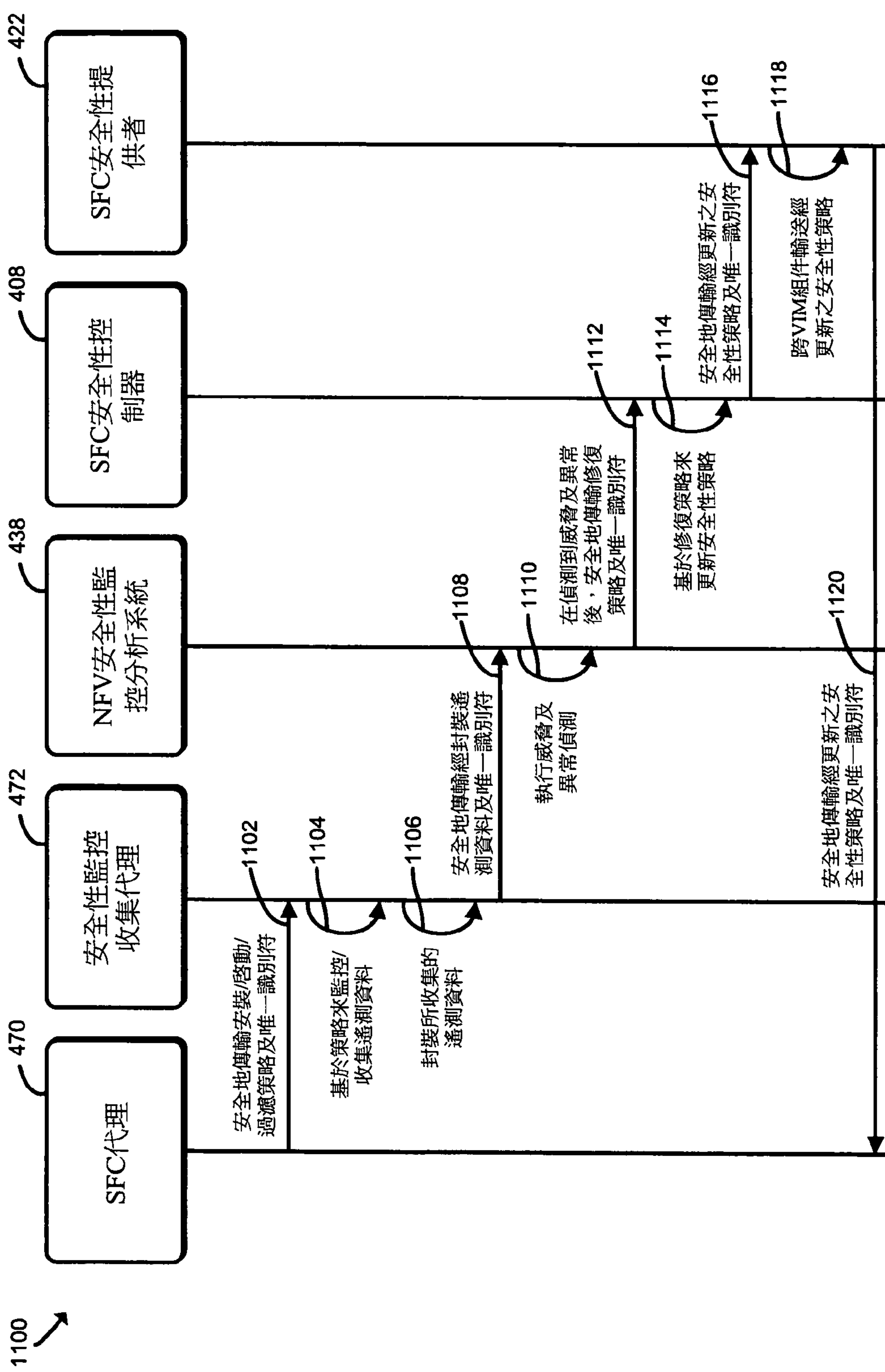


圖11

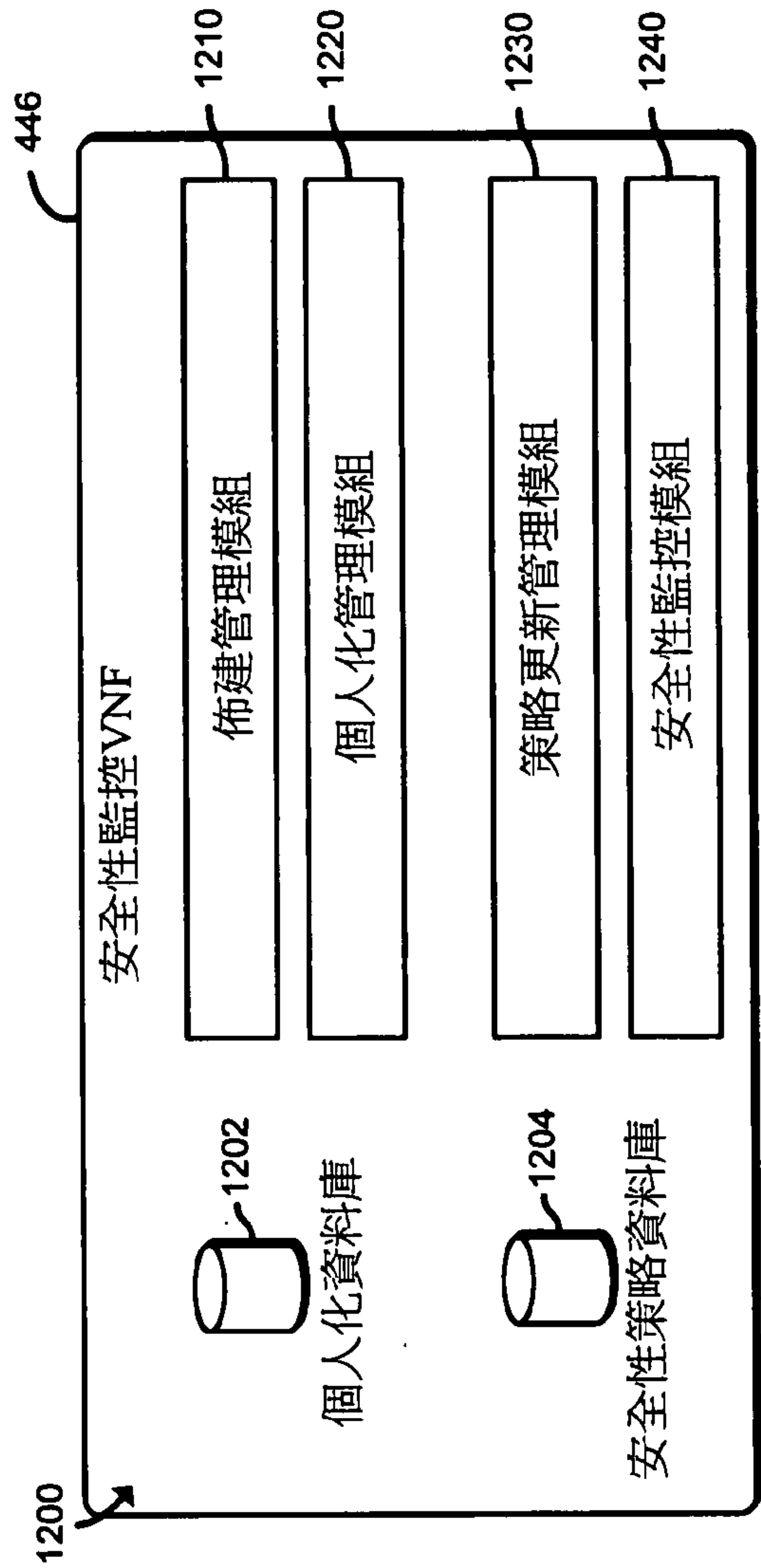


圖12

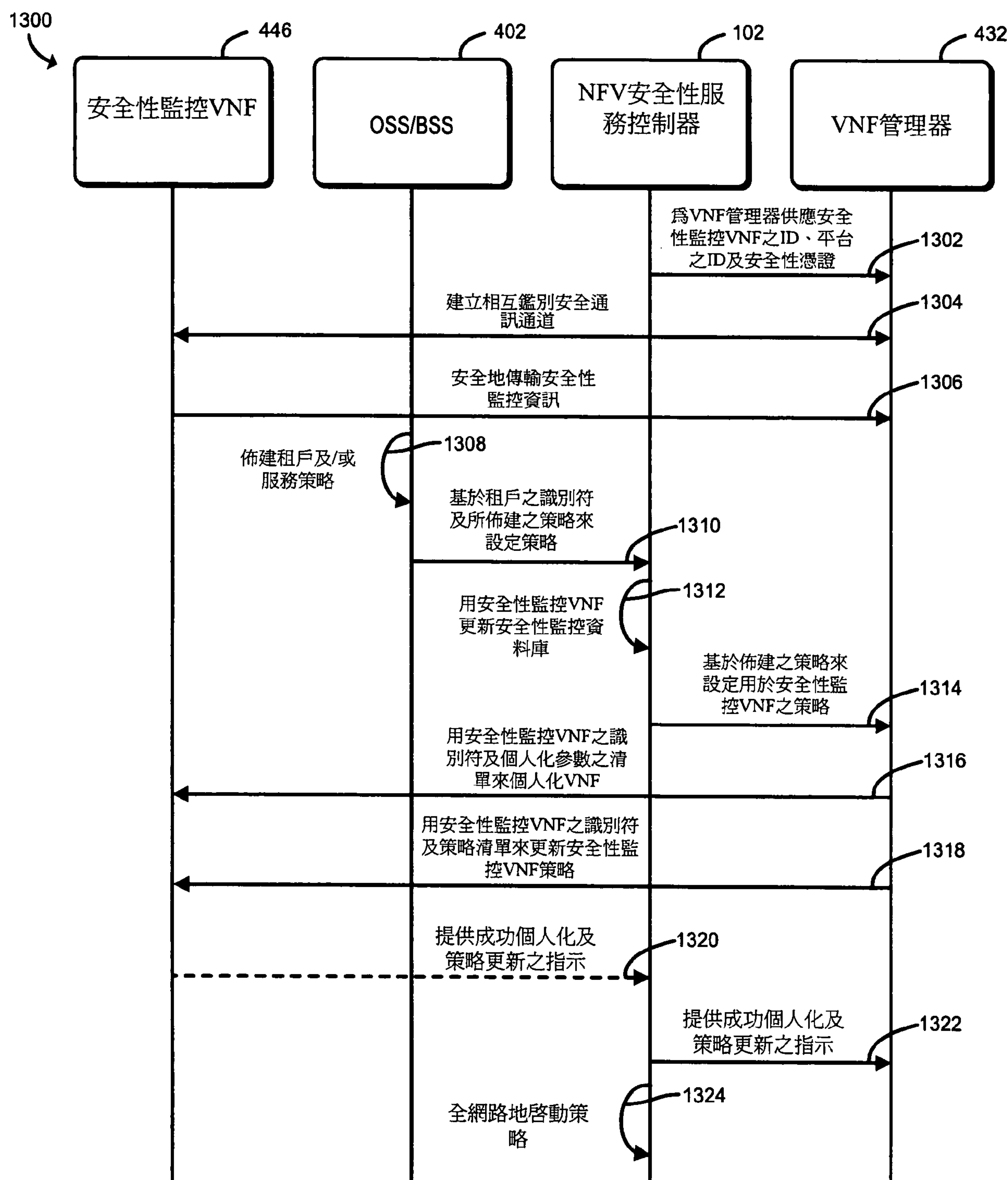


圖13

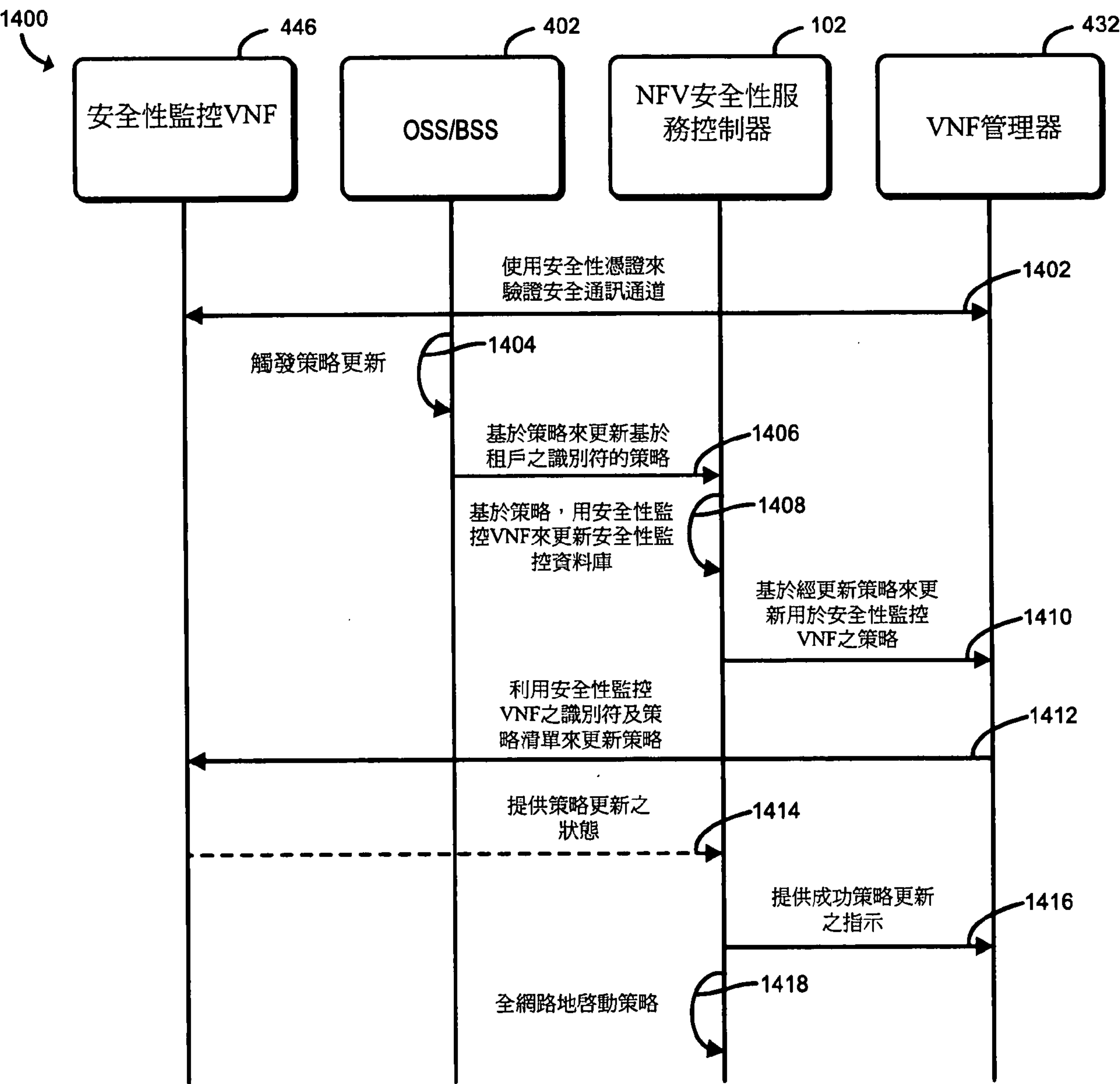


圖14