I519152

(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 I519152 B**

(45)公告日： 中華民國 105 (2016) 年 01 月 21 日

(21)申請案號：101105182 (22)申請日： 中華民國 101 (2012) 年 02 月 17 日

(51)Int. Cl.： ***H04N5/225 (2006.01)*** ***H04N7/18 (2006.01)***
H04L29/02 (2006.01)

(30)優先權：2011/06/24 香港 11106546.3

(71)申請人：千里眼科技有限公司 (香港地區) SIGNAL COMMUNICATIONS LIMITED (HK)
香港

(72)發明人：何家豪 HO, KA HO (HK) ；謝正學 TSE, CHING HOK (HK) ；呂鎵進 LU, KA CHUN (HK)

(74)代理人：黃慶源；陳彥希

(56)參考文獻：

TW	I283837	TW	200937955
CN	101945086A	US	2010/0208082A1
US	2011/0149080A1		

審查人員：黃筱喬

申請專利範圍項數：30 項 圖式數：5 共 45 頁

(54)名稱

連接網路式相機至視訊站之方法及對應的視訊監控系統、視訊站、及網路式相機

METHODS OF CONNECTING NETWORK-BASED CAMERAS TO VIDEO STATIONS, AND CORRESPONDING VIDEO SURVEILLANCE SYSTEMS, VIDEO STATIONS, AND NETWORK-BASED CAMERAS

(57)摘要

網路攝像機與視頻工作站的連接方法及視頻監視系統。網路攝像機的安裝比模擬攝像機複雜。而且由於源自 IP 攝像機的視頻資料通過共用網路發送，駭客通過連接到共用網路能容易地訪問這些攝像機並獲取敏感視頻資料，或替換從攝像機發送給 NVR 的視頻圖像。為至少解決一些上述問題，本發明提供的方法使網路攝像機和與它連接的介面間的所有權能被鎖定，使得任何時候至少一個介面中的每一個均只鎖定對唯一網路攝像機的所有權，且只能從被該介面鎖定了所有權的唯一網路攝像機接收視頻。由於本發明的介面只能與唯一一個擁有能被視頻工作站接受的攝像機識別標記且優選地擁有鎖定匙的網路攝像機進入鎖定關係，因此電子欺騙的機會將實質地減少。

Installation of network-based cameras is more complicated than analog cameras. Further, because video data from the IP-based cameras is sent over a shared network, hackers can easily access the cameras by connecting to the shared network and acquire the sensitive video data, or replace video images sent from the camera to the NVR. To at least resolve some of these issues, the current invention provides methods of connecting network-based cameras to video station such that the ownership between the network-based camera with the respective connected socket can be locked, such that at any time, each of the at least one socket can lock ownership of only one network-based camera, and receives video from the only one network-based camera with ownership locked by the respective socket. As the socket of the current invention can now engage into “locking” relationship with only one network-based camera with camera-identification tag

acceptable to the video station, and preferably with the lock key, the chance of spoofing can be substantially reduced.

指定代表圖：

符號簡單說明：

10・・・視頻監視系統

12・・・網路攝像機

14・・・視頻工作站

16・・・介面

20・・・視頻記錄器

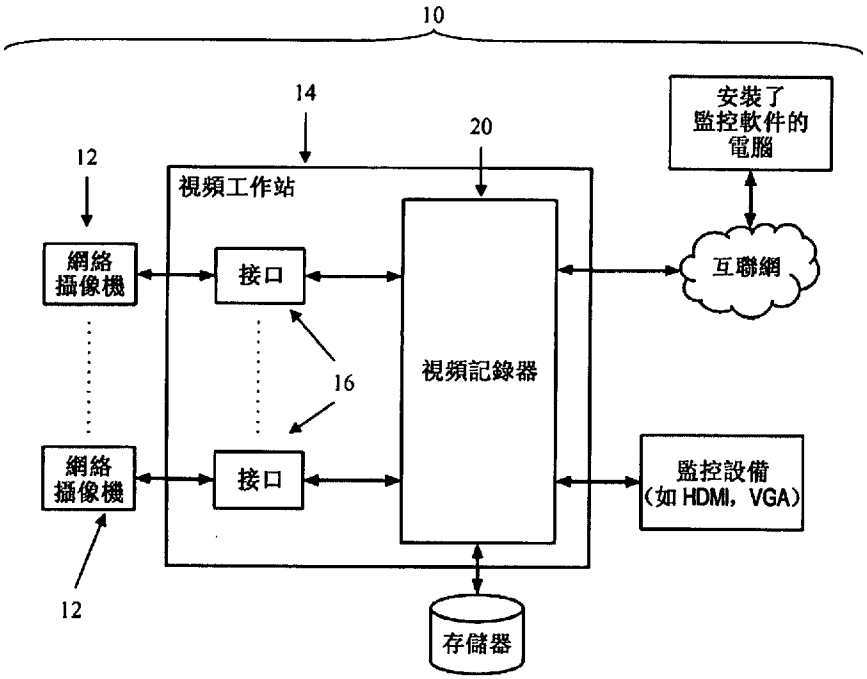


圖 2

I519152

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：101105182

※申請日：101.2.17　※IPC分類：H04N 5/225 (2006.01)
H04N 7/18 (2006.01)
H04L 29/02 (2006.01)

一、發明名稱：（中文/英文）

連接網路式相機至視訊站之方法及對應的視訊監控系統、視訊站、及網路式相機

METHODS OF CONNECTING NETWORK-BASED CAMERAS TO VIDEO STATIONS, AND CORRESPONDING VIDEO SURVEILLANCE SYSTEMS, VIDEO STATIONS, AND NETWORK-BASED CAMERAS

二、中文發明摘要：

網路攝像機與視頻工作站的連接方法及視頻監視系統。網路攝像機的安裝比模擬攝像機複雜。而且由於源自 IP 攝像機的視頻資料通過共用網路發送，駭客通過連接到共用網路能容易地訪問這些攝像機並獲取敏感視頻資料，或替換從攝像機發送給 NVR 的視頻圖像。為至少解決一些上述問題，本發明提供的方法使網路攝像機和與它連接的介面間的所有權能被鎖定，使得任何時候至少一個介面中的每一個均只鎖定對唯一網路攝像機的所有權，且只能從被該介面鎖定了所有權的唯一網路攝像機接收視頻。由於本發明的介面只能與唯一一個擁有能被視頻工作站接受的攝像機識別標記且優選地擁有鎖定匙的網路攝像機進入鎖定關係，因此電子欺騙的機會將實質地減少。

三、英文發明摘要：

Installation of network-based cameras is more complicated than analog cameras. Further, because video data from the IP-based cameras is sent over a shared network, hackers can easily access the cameras by connecting to the shared network and acquire the sensitive video data, or replace video images sent from the camera to the NVR. To at least resolve some of these issues, the current invention provides methods of connecting network-based cameras to video station such that the ownership between the network-based camera with the respective connected socket can be locked, such that at any time, each of the at least one socket can lock ownership of only one network-based camera, and receives video from the only one network-based camera with ownership locked by the respective socket. As the socket of the current invention can now engage into "locking" relationship with only one network-based camera with camera-identification tag acceptable to the video station, and preferably with the lock key, the chance of spoofing can be substantially reduced.

四、指定代表圖：

(一)本案指定代表圖為：第（2）圖。

(二)本代表圖之元件符號簡單說明：

10	視頻監視系統
12	網路攝像機
14	視頻工作站
16	介面
20	視頻記錄器

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無

六、發明說明：

【發明所屬之技術領域】

本發明涉及視頻監視系統，特別是具有基於 IP 的數位攝像機和數位視訊記錄器的視頻監視系統。

【先前技術】

視頻監視系統在諸如預防犯罪、企業管理、交通監控等眾多不同領域發揮著重要作用。監視系統幾乎隨處可見，如銀行、 娛樂場所、機場、軍事設施以及商店。

為了更好的解析度和輸出品質，在監視領域中，數位攝像機取代類比攝像機的趨勢日益增長。在數位視訊監視系統中，使用基於網路或 IP 的攝像機來取代傳統的模擬攝像機，其中這些基於網路或 IP 的攝像機獲取影像並立刻將影像轉化為數位格式、並通過網路（典型的是依據 IP 協定通過乙太網）將視頻資料發送給網路視頻記錄器（NVR）或視頻工作站。

儘管那些基於網路或 IP 的監視系統日趨普及，但是它們存在一些缺點。首先，安裝基於 IP 的攝像機比安裝模擬攝像機更複雜。操作員需要擁有廣泛的網路知識以配置每台相連接的攝像機。每當一台新的攝像機接入系統時，設置工作與傳統的類比監視系統相比會牽涉更多的配置的更改，如預防 IP 地址衝突。第二個問題涉及安全性。由於來自基於 IP 的攝像機的視頻資料是通過共用網路發送的，駭客可以通過連接到共用網路而輕鬆地訪問到這些攝像機並獲取敏感視頻資

料，或者替換由攝像機發送給 NVR 的視頻圖像。事實上互聯網上有很多可以輕鬆實現這些的工具。圖 1 顯示了一種可能出現的情況，駭客通過使用與註冊在視頻工作站的 IP 攝像機具有相同的 IP 和 MAC 位址的電腦來替換從 IP 攝像機發送給 NVR 的視頻圖像，通常將這種行為稱為“電子欺騙”。

因此，有必要設計更安全的利用基於網路或更具體地說是基於 IP 的攝像機和 NVR 或視頻工作站的視頻監視系統。

【發明內容】

本發明目的：

因此，本發明的目的是解決現有技術中陳述到的至少一個或者更多問題。特別地，本發明意在提供使用更容易安裝和/或更安全的網路攝像機和視頻工作站的視頻監視系統。作為最低限度，本發明意在為公眾提供一種有益的選擇。

相應地，本發明提供一種將至少一個網路攝像機連接至視頻工作站的方法，該視頻工作站含有至少一個介面用於連接所述網路攝像機。本發明的方法包括以下步驟：

a）從網路攝像機向視頻工作站發送一個攝像機廣告信號，用以通告該網路攝像機的存在，所述攝像機廣告信號包含一個用於識別該網路攝像機的攝像機識別標記；

b)如果該網路攝像機處於開鎖狀態，則用與該網路

攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權；且

c)如果該網路攝像機處於鎖定狀態並且不是被該各自相應的介面所鎖定,則終止該網路攝像機與視頻工作站之間的連接

這樣，在任何時候，至少一個介面中的每一個

·只能鎖定對唯一一個網路攝像機的所有權；且

·只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

優選地，本發明的方法進一步包括如下步驟：

a1）接收到攝像機廣告信號後，決定該攝像機識別標記是否可被視頻工作站接受；且

a2）如果該攝像機識別標記不被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

優選地，上述的步驟b）和c）包括如下步驟：

·從視頻工作站向網路攝像機發送一個所有權鎖狀態詢問信號，所述所有權鎖狀態詢問信號用於詢問與網路攝像機相連接的各自相應的介面對該網路攝像機的所有權是否能夠被鎖定；

·在網路攝像機收到該所有權鎖狀態詢問信號後，

- 如果該網路攝像機處於開鎖狀態，則由該網路攝像機向視頻工作站發送一個接受鎖定信號；或
- 如果該網路攝像機處於鎖定狀態且未被該各自相應的介面所鎖定，則由該網路攝像機向視頻工作站發送一個拒絕鎖定信號；

·如果網路攝像機向視頻工作站發送了接受鎖定信

號，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權並建立一個視頻連接用於從該網路攝像機向視頻工作站發送視頻；且

·如果網路攝像機向視頻工作站發送了拒絕鎖定信號，或如果攝像機識別標記不被視頻工作站接受，則終止網路攝像機與視頻工作站之間的連接。

更優選地，所有權鎖狀態詢問信號包含一個鎖定匙，用於對網路攝像機與視頻工作站之間的資料傳輸進行解密。通過提供所有權鎖狀態詢問信號，本發明的方法進一步包含以下步驟：在網路攝像機向視頻工作站發送攝像機廣告信號前，從視頻工作站廣播網站探索信號，所述網站探索信號包含一個用於識別視頻工作站的網站識別標記。更優選地，所有權鎖狀態詢問信號進一步包括以下元素中的任何一個或它們的組合：攝像機識別標記、網站識別標記、一套被指定的網路設定，在此基礎上，通過與網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權的步驟包括如下步驟：

·記錄下面至少一個

- 在與網路攝像機相連接的各自相應的介面上記錄攝像機識別標記；和
- 在網路攝像機上記錄網站識別標記

·在視頻工作站中選擇一組獨特的網路設定作為所有權鎖定狀態詢問信號中被指定的網路設定；並且可選擇地，用該組被指定的網路設定更新網路攝像機。

優選地，攝像機廣告信號進一步包括一組攝像機網路設定和攝像機鎖定狀態中的任何一個，或它們的組合。

可選擇地，本發明的所述方法，還包括如下步驟：

·從網路攝像機向與它相連接的各自相應的介面發送一個心跳信號，用於以與該網路攝像機相連接的各自相應的介面來維持對該網路攝像機的所有權；並且

·如果在預定的時間段內未收到該心跳信號，則解鎖與該網路攝像機相連接的各自相應的介面對該網路攝像機的所有權，並且終止網路攝像機和與該網路攝像機相連接的各自相應的介面之間的連接。

優選地，網路攝像機通過網路線纜被連接到所述至少一個介面。

本發明的另一方面提供了一種具有至少一個網路攝像機和一個視頻工作站的視頻監視系統，其引入了上述的任何一種方法。

本發明的另一方面提供了一種控制至少一個網路攝像機與視頻工作站之間的連接的方法，其中從網路攝像機向視頻工作站發送一個攝像機廣告信號用以通告該網路攝像機的存在。所述攝像機廣告信號包含一個用於識別該網路攝像機的攝像機識別標記，所述視頻工作站含有用於連接所述網路攝像機的至少一個介面。所述方法包括如下步驟：

1）如果該網路攝像機處於開鎖狀態，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權；且

2）如果該網路攝像機處於鎖定狀態並且不是被該各自相應的介面所鎖定，則終止該網路攝像機與視頻工作站之間的連接

這樣，在任何時候，至少一個介面中的每一個

·只能鎖定對唯一一個網路攝像機的所有權；且

·只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

本發明的另一方面提供了一種用於視頻監視系統的視頻工作站，其引入了上述方法。

本發明還提供了一種將至少一個網路攝像機連接至視頻工作站的方法，所述視頻工作站：

·含有至少一個介面用於連接所述網路攝像機，

·在該網路攝像機處於開鎖狀態時能夠用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權，並且為該網路攝像機提供一個鎖定匙用於對網路攝像機與視頻工作站之間的資料傳輸進行解密，且

·在該網路攝像機處於鎖定狀態並且不是被該各自相應的介面所鎖定時能夠終止該網路攝像機與視頻工作站之間的連接，

所述方法包括以下步驟：

a）從網路攝像機向視頻工作站發送一個攝像機廣告信號，用以通告該網路攝像機的存在，所述攝像機廣告信號包含一個用於識別該網路攝像機的攝像機識別標記；

b）如果收到了來自視頻工作站的所有權鎖狀態詢問信號且該網路攝像機處於開鎖狀態，則在網路攝像機中記錄鎖定匙，

這樣，在任何時候，至少一個介面中的每一個

·只能鎖定對唯一一個網路攝像機的所有權；且

·只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

本發明的另一方面提供了一種用於視頻監視系統的網路攝像機，其引入了上述方法。

【實施方式】

在下面段落中將通過引用附圖以實例方式對本發明進行說明。本發明的各目的、各特徵及各方面在下面的描述中被公開並且可以從下面的描述中變得顯而易見。本領域的普通技術人員應當明白現在的討論只是對示範性實施例的描述，其目的不在於限制本發明更廣泛的方面，這些更廣泛的方面體現於這些示範性的構造中。表1展示了各部件及其在附圖中的參考編號。

參考編號	**部件名稱**
10	視頻監視系統
12	網路攝像機
14	視頻工作站
16	介面
20	視頻記錄器

表 1

參照圖 2，視頻監視系統 10 包括兩個組成部分，即，至少一個網路攝像機 12 和至少一個視頻工作站 14。視頻工作站 14 含有用於連接至網路攝像機 12 的至少一個介面 16、以及一個視頻記錄器 20。在可供使用的資源的範圍內，視頻監視系統 10 可以根據需要有多個網路攝像

機 12、視頻工作站 14 以及介面 16，這取決於影響視頻監視系統 10 使用的若干因素，包括所覆蓋區域、場所的複雜性等。本發明中的介面 16 指能夠物理上與網路攝像機 12 連接（例如通過有線連接）的物理介面。該介面 16 不是典型連網中連接若干網路設備的虛擬介面。如果需要，視頻工作站 14 通過大家所知道的技術（例如 RJ-45 介面及線纜、VGA 或 HDMI 介面及線纜、USB、IEEE1394 或 eSATA 介面及線纜）連接到互聯網、監控設備以及記憶體。

網路攝像機 12 和視頻工作站 14 分別通過適當的軟體控制模組（例如以軟體形式）來實現，以控制它們的連接。這些將會在下面的段落中詳細描述。

圖 3 示出了闡釋了本發明中網路攝像機 12 是如何被視頻工作站 14 的一個介面 16 鎖定的流程圖。當一台網路攝像機 12 連接至一個介面 16 時，網路攝像機 12 會向視頻工作站 14 發送一個攝像機廣告信號用以報告該網路攝像機 12 的存在。該攝像機廣告信號包含用以識別網路攝像機 12 的攝像機識別標記。該攝像機識別標記可以是任何能滿足需要的獨一無二代碼，該獨一無二代碼可以識別網路攝像機 12，優選是在硬體級上進行識別，如網路攝像機 12 的生產序號。如果該網路攝像機處於開鎖狀態，則網路攝像機 12 的所有權將被與其相連接的各自相應的介面 16 鎖定。如果網路攝像機 12 處於鎖定狀態且不是被該各自相應的介面鎖定，則網路攝像機 12 與視頻工作站 14 之間的連接將被終止。

網路攝像機 12 進入鎖定狀態之前，網路攝像機 12

可以主動地發出攝像機廣告信號，即，不管網路攝像機12是否檢測到與介面16的連接，或者甚至不管網路攝像機12是否檢測到與網路的連接都週期性地發出攝像機廣告信號。作為另一種選擇，網路攝像機12可以被動地發出攝像機廣告信號，即，只有在網路攝像機12檢測到與介面16的連接時或者在網路攝像機12檢測到與網路相連時，才會發出攝像機廣告信號。

可選擇地，收到攝像機廣告信號後，視頻工作站14隨後會決定該攝像機識別標記是否可被視頻工作站14接受，例如通過核查該攝像機識別標記是否包含於清單中，該清單可以儲存在視頻工作站14中或者可以通過網路連接被視頻工作站14訪問到。如果該攝像機識別標記可以被視頻工作站接受，並且如上所述，如果該網路攝像機處於開鎖狀態，則用與該網路攝像機相連接的各自相應的介面16鎖定對該網路攝像機12的所有權。否則，如果該攝像機識別標記不能被視頻工作站接受，則網路攝像機12與視頻工作站14之間的連接將被終止。

除了攝像機識別標記，攝像機廣告信號可選擇地包含指示了網路攝像機12鎖狀態的欄位，即指示了網路攝像機12對於與視頻工作站14的介面的連接而言處於鎖定狀態還是開鎖狀態。這是可取的，因為這樣視頻工作站就能夠立刻確定是否可以鎖定與網路攝像機相連接的各自相應的介面16對該網路攝像機12的所有權，或者終止該網路攝像機12與視頻工作站14之間的連接。

如果視頻工作站14例如根據攝像機識別標記未獲知網路攝像機12的鎖狀態，那麼下面的過程是適用的。具

體來說，視頻工作站 14 會向網路攝像機 12 發出一個所有權鎖狀態詢問信號，用於詢問網路攝像機 12 和與該網路攝像機相連接的各自相應的介面 16 的所有權是否可以被鎖定，網路攝像機 12 收到該所有權鎖狀態詢問信號後，如果網路攝像機 12 處於開鎖狀態，則網路攝像機 12 向視頻工作站 14 發送一個接受鎖定信號，然後與網路攝像機相連接的各自相應的介面 16 對該網路攝像機 12 的所有權將被鎖定，一個視頻連接會被建立起來供網路攝像機 12 向視頻工作站 14 發送視頻。否則，如果網路攝像機 12 處於鎖定狀態且不是被其各自相應的介面鎖定的，則網路攝像機 12 向視頻工作站 14 發送一個拒絕鎖定信號，並終止網路攝像機 12 與視頻工作站 14 之間的連接。如果網路攝像機 12 的攝像機識別標記被確定為不能被視頻工作站 14 接受，則網路攝像機 12 與視頻工作站 14 之間的連接同樣會被終止。通過上述操作，每一個介面 16 只能鎖定唯一一個網路攝像機的所有權，並且只能從被該介面鎖定了所有權的唯一一個網路攝像機接收視頻。縱使如上所述，如果視頻工作站 14 獲知了網路攝像機 12 的鎖狀態，上述過程可以作為後備方案被同樣執行。需要注意的是雖然網路攝像機 12 處於鎖定狀態，其各自相應連接的介面 16 仍然可以向網路攝像機 12 發出所有權鎖狀態詢問信號，例如用以更新網路設定、鎖定匙或任何需要的設定。在這種情況下，用來終止網路攝像機 12 與視頻工作站 14 之間的連接的拒絕鎖定信號不應被發出。

可選擇地，在網路攝像機向視頻工作站 14 發送攝像

機廣告信號前，視頻工作站 14 可以廣播一個網站探索信號。在這種情況下，攝像機廣告信號可以在收到網站探索信號之後再被發送。該網站探索信號包含一個網站識別標記，用以對視頻工作站 14 進行識別。該網站識別標記可以是任何能滿足需要的、獨一無二代碼，該獨一無二代碼可以識別視頻工作站 14，優選是在硬體級進行識別，如視頻工作站 14 的生產序號。該網站識別標記的使用將在稍後予以闡述。

除了攝像機識別標記，所有權鎖狀態詢問信號還可以包含一個鎖定匙用以解密網路攝像機 12 與視頻工作站 14 之間的資料傳輸。所有的資料傳輸都包含視頻及含有心跳信號的各種控制訊息。然而，為了減少網路攝像機 12 和視頻工作站 14 的網路開銷及對它們的處理能力的需求，優選地只解密控制訊息。各種加密方法可供使用，如 RC4(http://en.wikipedia.org/wiki/RC4)、WEP(http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) 及 DES(http://en.wikipedia.org/wiki/Data_Encryption_Standard)。鎖定匙可以通過各種方法產生，如 UUID(http://en.wikipedia.org/wiki/UUID) 或 OUI(http://en.wikipedia.org/wiki/Organizationally_Unique_Identifier)，鎖定匙可以按需要生成或存儲在視頻工作站 14 中。更加優選隨需要在視頻工作站 14 中生成鎖定匙的方式，因為這樣會降低對安全性的破壞。

另外，所有權鎖狀態詢問信號可以進一步包含以下元素中的任意一個或者它們的組合：攝像機識別標記、

網站識別標記、一套被指定的網路設定。攝像機識別標記可以提供額外的校驗作用，網站識別標記和一套被指定的網路設定的作用將會在稍後描述。

與網路攝像機相連接的各自相應的介面16對網路攝像機 12 的所有權的“鎖定”可以通過多種方式實現。例如，網路攝像機12和連接的介面16均可以與一個虛擬電子鎖狀態關聯，該狀態可以是“開鎖”或者“鎖定”，這樣的話該虛擬電子鎖狀態可以簡化為一個真/假（true/false）欄位。在對所有權的鎖定期間，網路攝像機12和連接的介面16之間的相應鎖狀態將會更新為“鎖定”。為了提高安全性，更加優選的是視頻工作站 14 選擇一組獨特的網路設定作為所有權鎖狀態詢問信號中的一套被指定的網路設定，這樣網路攝像機 12 的網路設定可以在該上鎖過程中被更新。可以遵循標準的 DHCP 過程或靜態 IP 分配程式來選擇和更新網路設定，其中可能包括 IP 位址、子網路遮罩、DNS 伺服器位址等等。

可選擇地，在對所有權的鎖定期間，攝像機識別標記被記錄在視頻工作站 14 中和/或網站識別標記被記錄在網路攝像機 12 中。這有助於提高後續校驗能力和安全性。為確保網路攝像機 12 與視頻工作站 14 之間的連接在一段時間後完整無損，優選地從網路攝像機 12 向視頻工作站 14 發送一個心跳信號。如果該心跳信號未在預定的時間段（假定每 5 至 30 秒）內收到，那麼與網路攝像機相連接的各自相應的介面 16 對該網路攝像機 12 的所有權改變為“開鎖”，即網路攝像機和連接的介面的虛擬電子鎖狀態由“鎖定”變為“開鎖”。鎖狀態的變更可以通

過例如在使用心跳信號的情況下的內部檢驗來完成，或者在使用者控制下通過向網路攝像機 12 和/或連接的介面 16 發送開鎖信號來完成。如果攝像機識別標記已被記錄在視頻工作站 14 中和/或工作站識別標記已被記錄在網路攝像機 12 中，那麼由於這些標記在硬體級別與網路攝像機 12 和視頻工作站 14 相關聯，所以這些標記可以擔任對連接安全性進行額外檢查的作用，例如，預防電子欺騙。心跳信號的處理方法已在本領域中被瞭解，這裡不再進行描述。

需要注意的是，所有權的"鎖定"是在網路攝像機 12 和與該網路攝像機相連接的各自相應的介面 16 之間完成的，而不是在網路攝像機 12 與視頻工作站 14 之間完成。這帶來的一個結果是，在任何時間，至少一個介面中的每一個只能鎖定對唯一一個網路攝像機的所有權，並且只能從唯一一個所有權被該介面鎖定的網路攝像機接收視頻。就是說，即使一個擁有多個網路埠的網路交換機或中繼器被連接到視頻工作站 14 的一個介面 16，且這多個網路埠中的每一個均分別連接至一個網路攝像機 12，這些網路攝像機 12 中也只能有一個與介面 16 處於"鎖定"關係，因此該介面 16 只能接收這個被"鎖定"的網路攝像機 12 發出的視頻。優選地，鎖定的介面 16 一旦進入鎖定狀態後就停止搜索處於開鎖狀態的網路攝像機 12，例如停止發送網站探索信號。這是不同於當前的做法，當前的做法通常使用 DHCP 作為網路連接安裝協定，這允許多個攝像機被連接到現存視頻工作站上的單個網路介面。當前的這種做法至少存在這樣的問題，即

當有過多攝像機連接到一個介面時會造成品質下降。

介面 16 與網路攝像機 12 之間的網路連接可以是無線的或有線的。在通常具有多通道的無線連接的情況下，每個物理介面 16 只允許連接唯一一個通道，以實現在任何時候一個介面 16 只鎖定對唯一一個網路攝像機 12 的所有權並且只從所有權被該對應介面 16 鎖定的該唯一網路攝像機 12 接收視頻的效果。然而，有線連接是優選的，它可以進一步提高視頻監視系統 10 的安全性。由於本發明中的介面 16 只能與唯一一個擁有能被視頻工作站 14 接受的攝像機識別標誌、且最好有鎖定匙的網路攝像機 12 建立“鎖定”關係，所以有線連接可以大大地降低“電子欺騙”的機會，這是因為通過有線連接可以對網路攝像機 12 進行物理跟蹤。相對于本發明，當前普遍的網路視頻監視系統利用允許多個攝像機連接到同一個介面的多個網路攝像機，和/或不使用如本發明中的從視頻工作站 14 發送的鎖定匙。相應地，電子欺騙的機會更高，且可能難以追蹤網路攝像機實際的物理位置。

由於一個介面 16 只連接一個網路攝像機 12，相比當前正在使用的、允許多個攝像機連接到一個介面的網路視頻監視系統，系統的安裝更加簡單。

圖 4a 至圖 4d 示出了網路攝像機 12 中用於控制其與視頻工作站 14 的連接所包括的處理的流程圖，該視頻工作站 14 已經實現了本發明中的視頻監視系統 10 的所有上述可選的組成部分。具體地，圖 4a 示出了網路攝像機 12 的鎖定狀態的控制，其中該網路攝像機 12 經檢查已準備好進行網路連接後在初始化過程中進入開鎖狀態。

如果收到所有權鎖狀態詢問信號訊息且網路攝像機 12 處於開鎖狀態，那麼網路攝像機 12 自行更新為鎖定狀態。如果收到開鎖信號、網路丟失或如圖 4b 中所示未準備好、或者網路攝像機 12 發出的心跳信號未得到回應，則網路攝像機 12 的狀態將會變為“開鎖”。監視網路狀態可以通過諸如自我調整乙太網實體層通信協定(http://en.wikipedia.org/wiki/Autonegotiation)等完成。

圖 4c 示出了網路攝像機 12 處於開鎖狀態時涉及的各種處理，包括：

· 網路攝像機 12 發出攝像機廣告信號 ADVERTISE，然後等待來自視頻工作站 14 中的介面 16 的信號；

· 如果收到了介面 16 發出的針對該網路攝像機 12 的訊息，且如果該訊息為所有權鎖狀態詢問信號 LOCK，且如果網路攝像機 12 處於開鎖狀態，則網路攝像機 12 更改其狀態為鎖定階段、更新它的網路設定、存儲鎖定匙用以隨後的資料解密、並向視頻工作站 14 中的介面 16 發送接受鎖定信號 ACCEPT LOCK。

· 如果以下情況中的一個發生，網路攝像機 12 將進入等待介面 16 發來的訊息的狀態：

1. 未收到來自介面 16 的訊息；

2. 來自介面 16 的訊息不是針對該網路攝像機 12 的；

3. 介面 16 發來所有權鎖狀態詢問信號 LOCK，但是該網路攝像機 12 已經處於鎖定狀態；

· 如果網路攝像機 12 處於鎖定狀態且如果收到了“開鎖”訊息，該訊息包含了正確的資訊，例如正確的攝

像機識別標記和網站識別標記，則網路攝像機 12 將它的鎖狀態更新為“開鎖”；

· 在任何時候，網路狀態被監控，如前文所描述。

圖 4d 示出了上面提到的監控網路狀態的處理，以及網路攝像機 12 處於鎖定狀態時涉及的各種處理，其中包括維持網路攝像機 12 和與該網路攝像機相連接的各自相應的介面 16 之間的“心跳”的處理。如上所述，由於這些過程已經在本領域中被瞭解，這裡將不再對這些過程進一步敘述。

圖 5a 至圖 5f 示出了視頻工作站 14 中用於控制其與網路攝像機 12 連接時所包括的處理的示範性流程圖，該網路攝像機 12 已經實現了前面所述的本發明的視頻監視系統 10 的所有可選的組成部分。具體地，圖 5a 示出了視頻工作站 14 中的每個介面 16 處的鎖狀態的控制，其中該介面 16 經檢查已準備好進行網路連接後在初始化過程中進入開鎖狀態。如果介面 16 處於開鎖狀態且收到網路攝像機 12 發來的接受鎖定信號，那麼介面 16 進入鎖定狀態。如果以下情況中的一個發生，介面 16 將進入“開鎖”狀態：

1. 檢測到網路攝像機 12 未連接至介面 16；

2. 收到拒絕鎖定信號 REJECT；

3. 在預定時間段內未收到網路攝像機 12 發出的心跳信號 HEART-BEAT。

圖 5b 示出了介面 16 在初始化過程中進入開鎖狀態。圖 5c 示出了介面 16 開鎖時涉及的一些處理，這些處理是通過網路攝像機 12 在硬體級別斷開與介面 16 的

連接而觸發的。

圖 5d 示出了當視頻工作站 14 的介面 16 處於檢測網路攝像機 12 的存在的狀態時涉及的各種處理，包括：

·等待網路攝像機 12 發來的攝像機廣告信號 ADVERTISE；

·如果介面 16 收到了網路攝像機 12 發來的攝像機廣告信號 ADVERTISE，且如果該信號指出網路攝像機 12 處於開鎖狀態，則視頻工作站 14 可以分配或分派一組獨特的網路設定。然後，可以產生所有權鎖狀態詢問信號 LOCK，並且向網路攝像機 12 發送所有權鎖狀態詢問信號 LOCK，以用連接的介面 16 鎖定對該網路攝像機 12 的所有權；

·如果沒有來自所連接的網路攝像機 12 的任何回應或如果沒有連接任何網路攝像機 12，則網站探索信號 DISCOVERY 將會被週期性地發送；

·在任何時候，處於硬體級別的連接狀態均被監控，如前文所描述。

圖 5e 示出了介面 16 向網路攝像機 12 發送了所有權鎖狀態詢問信號 LOCK 後涉及到的各種處理，包括：

·等待來自網路攝像機 12 發來的接受鎖定信號 ACCEPT LOCK 或拒絕鎖定信號 REJECT；

·核查接受鎖定信號 ACCEPT LOCK 或拒絕鎖定信號 REJECT 是否來自目標攝像機，例如通過對比該信號中的攝像機識別標記是否與之前發送的所有權鎖狀態詢問信號中的相符來進行核查；

·如果該信號來自目標攝像機，且如果該信號是接受

鎖定信號 ACCEPT LOCK，則與該網路攝像機之間的連接將被建立，且介面 16 進入與該網路攝像機 12 的鎖定狀態；

·如果以下情況中的一個發生，則與網路攝像機 12 的連接將被終止：

i. 該信號是拒絕鎖定信號信號 REJECT;

ii. 未連接網路攝像機 12；或

iii. 心跳維持進程導致超時；

·如果沒有來自所連接的網路攝像機 12 的任何回應或如果沒有連接到任何網路攝像機 12，則網站探索信號 DISCOVERY 會被週期性地發送；

·在任何時候，處於硬體級別的連接狀態均被監控，如前文所描述。

圖 5f 描述了網路攝像機 12 與介面 16 之間建立鎖定關係時的相關處理，包括用於處理網路攝像機 12 與介面 16 之間的心跳信號維持的各種處理。這些處理已在本領域中被瞭解，不需要再解釋。

對於所屬領域的人員來說，顯而易見的是，上述處理作為軟體程式在網路攝像機 12、介面 16 及視頻工作站 14 上實施，並且一名專業的程式師可以以上面的描述及附圖中的流程圖為基礎製作出適當的軟體代碼。現存的網路攝像機 12、介面 16 及視頻工作站 14 配備有針對處理能力、記憶體、網路連接能力的適當硬體設定，連同軟體形式的本文所描述的本發明的處理過程，可以實現本發明。執行本發明的處理方法時，處理器將會在不同時間履行不同的職責，這取決於處理器正在控制哪個

進程。就是說，處理器充當各個虛擬裝置，其中的每個執行著本發明中的不同進程，例如：當網路攝像機 12 發出攝像機廣告信號時充當攝像機廣告信號發生器；當決定攝像機識別標記是否可被視頻工作站接受時充當攝像機識別標記接受判斷設備；當網路攝像機的所有權要和與該網路攝像機相連接的各自相應的介面 16 鎖定時充當鎖狀態更新器，等等。

雖然本發明的優選實施方案通過範例予以詳細的描述，然而顯而易見的是本領域內的專業人員可以對本發明進行變型和適應性修改。此外，本發明的實施方案不應解釋為僅僅受到上文中的範例或附圖的約束。但是，需要特別明確的是，這些變型和適應性修改處於所附請求項中所述的本發明的範圍內。例如，作為一個實施方案一部分所圖示或描述的特徵可以用在另一個實施方案中，以形成進一步的新的實施方案。因此，意在使本發明覆蓋請求項及其等價物範圍內的變型和改變。

【圖式簡單說明】

本發明的優選實施方案將會通過範例輔以如下相關附圖的方式予以說明：

圖 1 示出了假冒的視頻圖像是如何通過“電子欺騙”被發送到視頻工作站的；

圖 2 示出了本發明的視頻監視系統的總體的系統體系結構；

圖 3 示出了本發明中的一個網路攝像機是如何被視頻工作站的一個介面鎖定的流程圖；

圖 4a 至圖 4d 示出了網路攝像機中用於控制其與視頻工作站的連接的處理的流程圖；以及

圖 5a 至圖 5f 示出了視頻工作站中用於控制一個介面與基於 IP 的攝像機的連接的處理的流程圖。

【主要元件符號說明】

10	視頻監視系統
12	網路攝像機
14	視頻工作站
16	介面
20	視頻記錄器

七、申請專利範圍：

1. 一種將至少一個網路攝像機連接至視頻工作站的方法，該視頻工作站含有用於連接所述至少一個網路攝像機的至少一個介面，所述方法包括如下步驟：

a）從網路攝像機向視頻工作站發送一個攝像機廣告信號，用以通告該網路攝像機的存在，所述攝像機廣告信號包括用於識別該網路攝像機的攝像機識別標記；

b）如果該網路攝像機處於開鎖狀態，則用與該網路攝像機相連接的各自相應的介面來鎖定對該網路攝像機的所有權；以及

c）如果該網路攝像機處於鎖定狀態並且不是被各自相應的介面所鎖定，則終止該網路攝像機與視頻工作站之間的連接，

這樣，在任何時候，至少一個介面中的每一個

- 只能鎖定對唯一一個網路攝像機的所有權；並且
- 只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

2. 根據請求項 1 所述的方法，還包括以下步驟：

a1）在接收到攝像機廣告信號之後，決定該攝像機識別標記是否能夠被視頻站接受；以及

a2）如果該攝像機識別標記不能夠被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

3. 根據請求項 1 所述的方法，其中步驟 b）和 c）包含如下步驟：

- 從視頻工作站向網路攝像機發送一個所有權鎖狀態詢問信號，所述所有權鎖狀態詢問信號用於詢問與網路攝像機相連接的各自相應的介面對該網路攝像機的所有權是否能夠被鎖定；
- 在網路攝像機接收到該所有權鎖狀態詢問信號後，
  - 如果該網路攝像機處於開鎖狀態，則由該網路攝像機向視頻工作站發送一個接受鎖定信號；或者
  - 如果該網路攝像機處於鎖定狀態且不是被各自相應的介面所鎖定，則由該網路攝像機向視頻工作站發送一個拒絕鎖定信號；
- 如果網路攝像機向視頻工作站發送了接受鎖定信號，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權，並建立一個視頻連接，用於從該網路攝像機向視頻工作站發送視頻；以及
- 如果網路攝像機向視頻工作站發送了拒絕鎖定信號，或如果攝像機識別標記不能夠被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

4. 根據請求項 3 所述的方法，其中所有權鎖狀態詢問信號包含一個鎖定匙，所述鎖定匙用於對網路攝像機與視頻工作站之間的資料傳輸進行解密。

5. 根據請求項4所述的方法，還包括以下步驟：在網路攝像機向視頻工作站發送攝像機廣告信號前，從視頻工作站廣播網站探索信號，該網站探索信號包含一個用於識別視頻工作站的網站識別標記。

6. 根據請求項5所述的方法，其中所有權鎖狀態詢問信號進一步包括以下元素中的任何一個或它們的組合：攝像機識別標記、網站識別標記、一套被指定的網路設定。

7. 根據請求項6所述的方法，其中用與網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權的步驟包括如下步驟：

- 記錄下面的至少一個
  - 在與網路攝像機相連接的各自相應的介面中記錄攝像機識別標記；以及
  - 在網路攝像機中記錄網站識別標記；
- 在視頻工作站中選擇一組獨特的網路設定作為所有權鎖狀態詢問信號中的被指定的網路設定。

8. 根據請求項7所述的方法，還包括步驟：用所述被指定的網路設定更新網路攝像機。

9. 根據請求項1所述的方法，其中攝像機廣告信號進一步包括以下元素中的任何一個或它們的組合：一組攝像機網路設定和攝像機鎖定狀態。

10. 根據請求項1所述的方法，還包括如下步驟：

- 從網路攝像機向與該網路攝像機相連接的各自相應的介面發送一個心跳信號，以用與該網

路攝像機相連接的各自相應的介面維持對該網路攝像機的所有權；並且

如果在預定的時間段內未收到心跳信號，則解鎖與該網路攝像機相連接的各自相應的介面對該網路攝像機的所有權，並且終止網路攝像機和與該網路攝像機相連接的各自相應的介面之間的連接。

11. 根據請求項 1 所述的方法，其中網路攝像機通過網路線纜被連接到所述至少一個介面。

12. 一種具有至少一個網路攝像機和一個視頻工作站的視頻監視系統，該視頻監視系統引入了請求項 1 至 11 中的任何一個所述的方法。

13. 一種控制至少一個網路攝像機與視頻工作站之間的連接的方法，其中從網路攝像機向視頻工作站發送一個攝像機廣告信號，用以通告該網路攝像機的存在，所述攝像機廣告信號包含一個用於識別該網路攝像機的攝像機識別標記，所述視頻工作站含有用於連接所述至少一個網路攝像機的至少一個介面，所述方法包括如下步驟：

1） 如果網路攝像機處於開鎖狀態，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權；以及

2） 如果網路攝像機處於鎖定狀態並且不是被各自相應的介面所鎖定，則終止該網路攝像機與視頻工作站之間的連接，

這樣，在任何時候，至少一個介面中的每一個

- 只能鎖定對唯一一個網路攝像機的所有權；且
- 只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

14. 根據請求項 13 所述的方法，還包括如下步驟：

1a）在接收到攝像機廣告信號之後，決定該攝像機識別標記是否能夠被視頻工作站接受；以及

1b）如果該攝像機識別標記不能夠被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

15. 根據請求項 13 所述的方法，其中步驟 1）和 2）包含如下步驟：

- 如果攝像機識別標記能夠被視頻工作站接受，則從視頻工作站向網路攝像機發送一個所有權鎖狀態詢問信號，用於詢問與網路攝像機相連接的各自相應的介面對該網路攝像機的所有權是否能夠被鎖定；
- 如果視頻工作站收到從網路攝像機發出的接受鎖定信號，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權，並建立一個視頻連接，用於從該網路攝像機向視頻工作站發送視頻；以及
- 如果視頻工作站接收到從網路攝像機發出的拒絕鎖定信號，或者如果攝像機識別標記不能夠被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

16. 根據請求項 15 所述的方法，其中所有權鎖狀態詢

問信號包含一個鎖定匙，用於對網路攝像機與視頻工作站之間的資料傳輸進行解密。

17. 根據請求項 16 所述的方法，還包括以下步驟：在網路攝像機向視頻工作站發送攝像機廣告信號前，從視頻工作站發出網站探索信號，該網站探索信號包含一個用於識別視頻工作站的網站識別標記。

18. 根據請求項 16 所述的方法，其中所有權鎖狀態詢問信號進一步包括以下元素中的任何一個或它們的組合：攝像機識別標記、網站識別標記、一套被指定的網路設定。

19. 根據請求項 18 所述的方法，其中用與網路攝像機相連接的各自相應的介面來鎖定對網路攝像機的所有權的步驟包括如下步驟：

- 在網路攝像機中記錄網站識別標記；以及
- 在視頻工作站中選擇一組獨特的網路設定作為所有權鎖狀態詢問信號中的被指定的網路設定。

20. 根據請求項 13 所述的方法，其中網路攝像機通過網路線纜被連接到所述至少一個介面。

21. 一種用於視頻監視系統的視頻工作站，該視頻工作站引入了請求項 13 至 20 中的任何一個所述的方法。

22. 一種將至少一個網路攝像機連接至視頻工作站的方法，所述視頻工作站：

- 含有至少一個介面，用於連接所述至少一個網

路攝像機，

- 在網路攝像機處於開鎖狀態時能夠用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權，以及為該網路攝像機提供一個鎖定匙來對網路攝像機與視頻工作站之間的資料傳輸進行解密，並且
- 在網路攝像機處於鎖定狀態並且不是被各自相應的介面所鎖定時，能夠終止該網路攝像機與視頻工作站之間的連接，

所述方法包括以下步驟：

a) 從網路攝像機向視頻工作站發送一個攝像機廣告信號，用以通告該網路攝像機的存在，所述攝像機廣告信號包含一個用於識別該網路攝像機的攝像機識別標記；

b) 如果收到了視頻工作站發出的所有權鎖狀態詢問信號且該網路攝像機處於開鎖狀態，則在網路攝像機中記錄鎖定匙，

這樣，在任何時候，至少一個介面中的每一個

- 只能鎖定對唯一一個網路攝像機的所有權；且
- 只能從唯一一個被該各自相應的介面鎖定了所有權的網路攝像機接收視頻。

23. 根據請求項 22 所述的方法，其中從視頻工作站向網路攝像機發送一個所有權鎖狀態詢問信號，用於詢問與網路攝像機相連接的各自相應的介面對該網路攝像機的所有權是否能夠被鎖定，所述方法還包括以下步驟：

- 在網路攝像機收到該所有權鎖狀態詢問信號後，
  - 如果該網路攝像機處於開鎖狀態，則由該網路攝像機向視頻工作站發送一個接受鎖定信號；或者
  - 如果該網路攝像機處於鎖定狀態且不是被各自相應的介面所鎖定，則由該網路攝像機向視頻工作站發送一個拒絕鎖定信號；

並且所述方法還包括以下步驟：

- 如果網路攝像機向視頻工作站發送了接受鎖定信號，則用與該網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權，並建立一個視頻連接，用於從該網路攝像機向視頻工作站發送視頻；且
- 如果網路攝像機向視頻工作站發送了拒絕鎖定信號，或者如果攝像機識別標記不能夠被視頻工作站接受，則終止該網路攝像機與視頻工作站之間的連接。

24. 根據請求項 23 所述的方法，其中所有權鎖狀態詢問信號進一步包括以下元素中的任何一個或它們的組合：攝像機識別標記、網站識別標記、一套被指定的網路設定。

25. 根據請求項 23 所述的方法，其中用與網路攝像機相連接的各自相應的介面鎖定對該網路攝像機的所有權的步驟，包括在網路攝像機中記錄網站識別

標記的步驟。

26. 根據請求項 25 所述的方法，還包括步驟：用一套指定的網路設定來更新網路攝像機。

27. 根據請求項 22 所述的方法，其中攝像機廣告信號進一步包括以下元素中的任何一個或它們的組合：一組攝像機網路設定和攝像機鎖定狀態。

28. 根據請求項 22 所述的方法，還包括如下步驟：

- 從網路攝像機向與該網路攝像機相連接的各自相應的介面發送一個心跳信號，以用與該網路攝像機相連接的各自相應的介面維持對該網路攝像機的所有權；並且
- 如果在預定的時間段內未收到心跳信號，則解鎖與該網路攝像機相連接的各自相應的介面對該網路攝像機的所有權，並且終止網路攝像機和與該網路攝像機相連接的各自相應的介面之間的連接。

29. 根據請求項 22 所述的方法，其中網路攝像機通過網路線纜被連接到所述至少一個介面。

30. 一種用於視頻監視系統的網路攝像機，該網路攝像機引入了請求項 22 至 29 中的任何一個所述的方法。

八、圖式：


倉庫
192.168.125.1
00:E2:B9:F5:A3:C4
控制室
當 IP 位址和 MAC 與路由器上的
訪問控制列表（ACL）匹配時，
防火牆允許查看來自攝像機的圖像
倉庫
192.168.125.1
00:E2:B9:F5:A3:C4
違反安全規定
控制室
如果其他設備模仿了原始攝像機的 ID，
因為 IP 位址和 MAC 與原始攝像機相同，
所以控制室不會獲知

圖 1

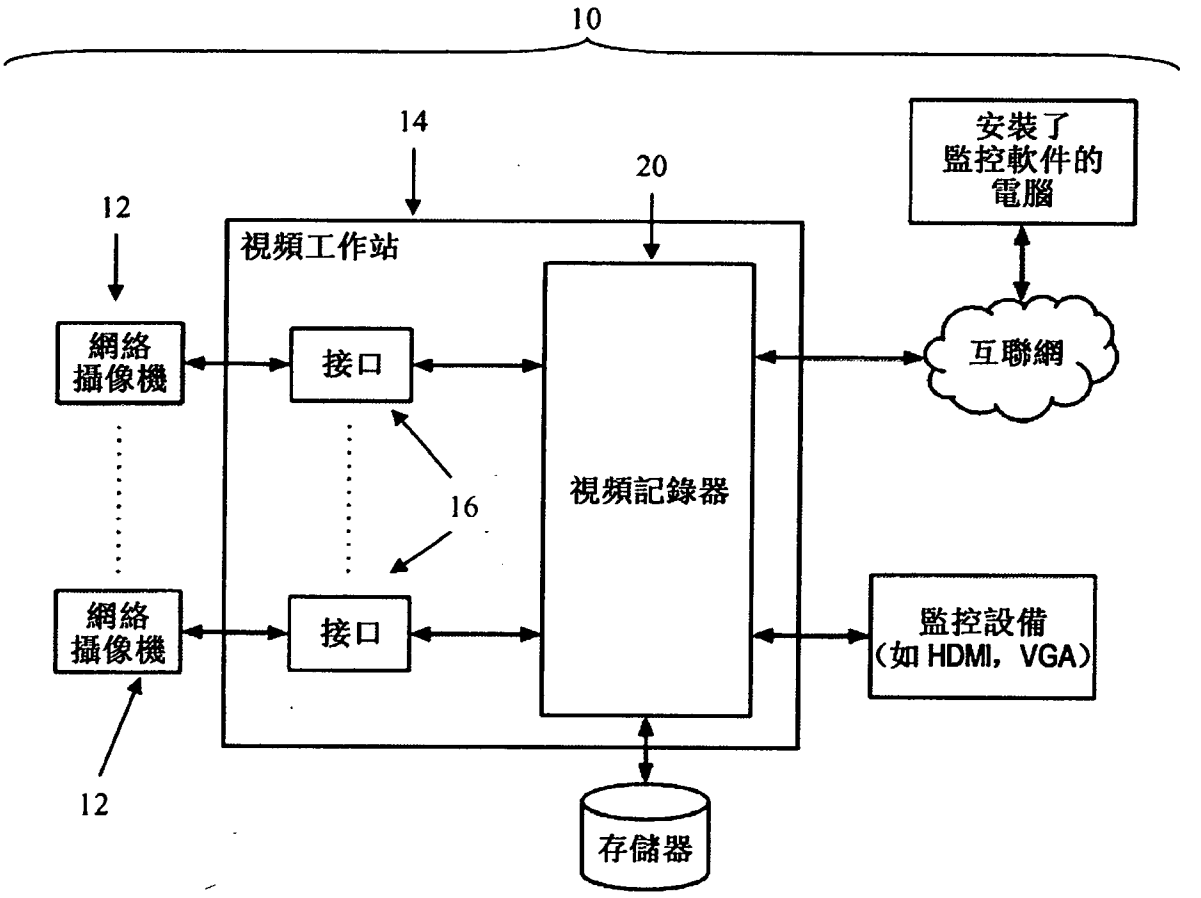

10
14
20
12
視頻工作站
安裝了
監控軟件的
電腦
網絡
攝像機
接口
互聯網
16
視頻記錄器
網絡
攝像機
接口
監控設備
(如 HDMI，VGA)
12
存儲器

圖 2

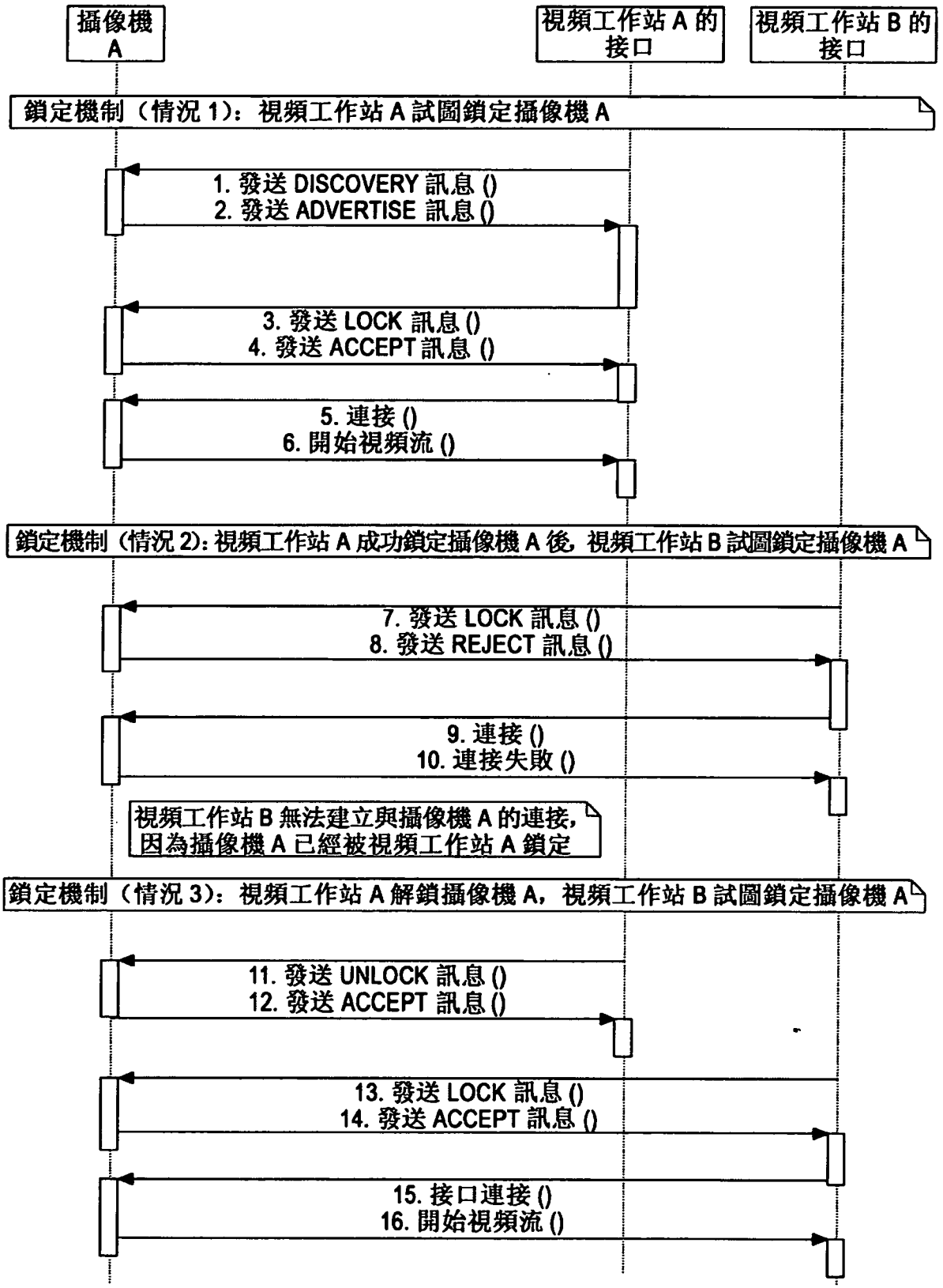

攝像機 A
視頻工作站 A 的接口
視頻工作站 B 的接口
鎖定機制（情況 1）：視頻工作站 A 試圖鎖定攝像機 A
1. 發送 DISCOVERY 訊息 ()
2. 發送 ADVERTISE 訊息 ()
3. 發送 LOCK 訊息 ()
4. 發送 ACCEPT 訊息 ()
5. 連接 ()
6. 開始視頻流 ()
鎖定機制（情況 2）：視頻工作站 A 成功鎖定攝像機 A 後，視頻工作站 B 試圖鎖定攝像機 A
7. 發送 LOCK 訊息 ()
8. 發送 REJECT 訊息 ()
9. 連接 ()
10. 連接失敗 ()
視頻工作站 B 無法建立與攝像機 A 的連接，因為攝像機 A 已經被視頻工作站 A 鎖定
鎖定機制（情況 3）：視頻工作站 A 解鎖攝像機 A，視頻工作站 B 試圖鎖定攝像機 A
11. 發送 UNLOCK 訊息 ()
12. 發送 ACCEPT 訊息 ()
13. 發送 LOCK 訊息 ()
14. 發送 ACCEPT 訊息 ()
15. 接口連接 ()
16. 開始視頻流 ()

圖 3

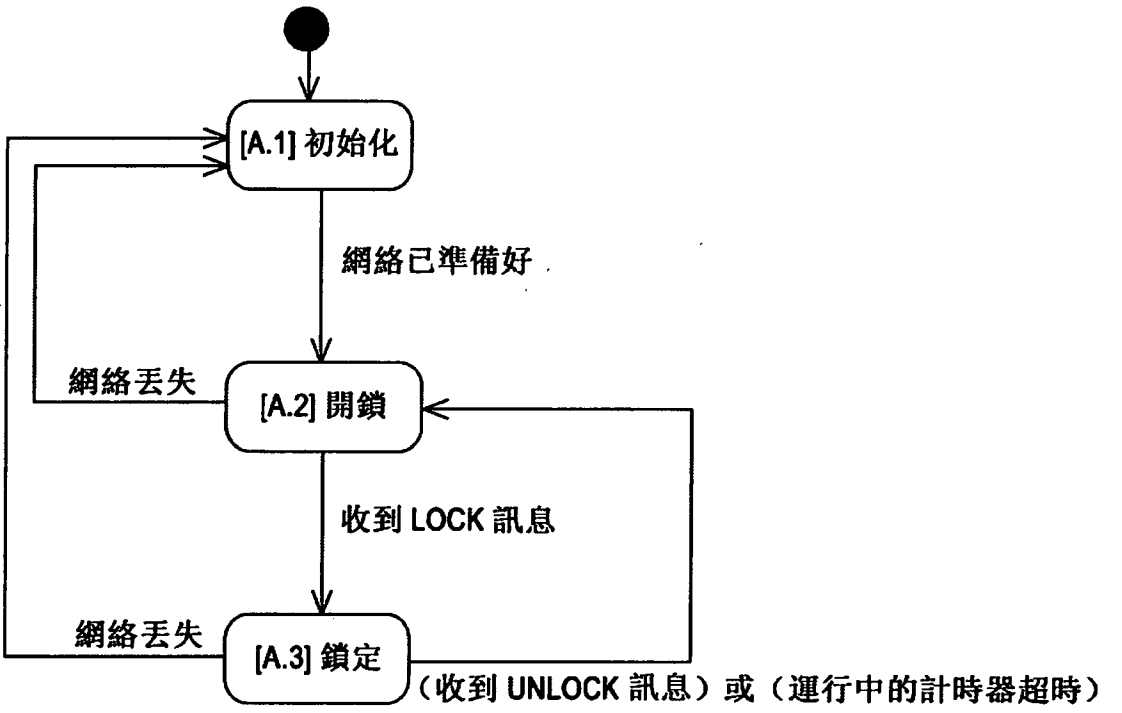

[A.1] 初始化
網絡已準備好
網絡丟失
[A.2] 開鎖
收到 LOCK 訊息
網絡丟失
[A.3] 鎖定
（收到 UNLOCK 訊息）或（運行中的計時器超時）

圖 4a

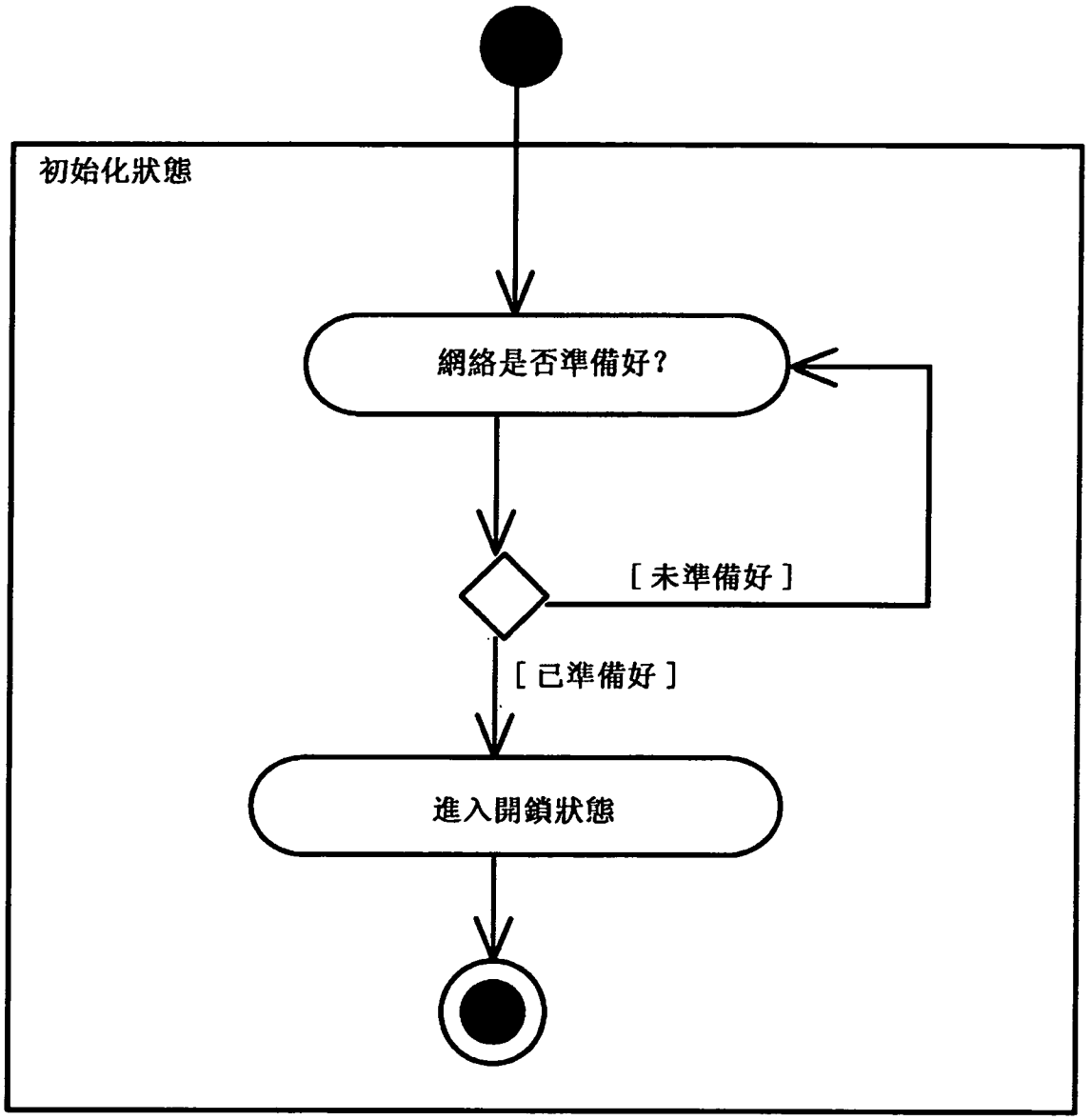


圖 4b

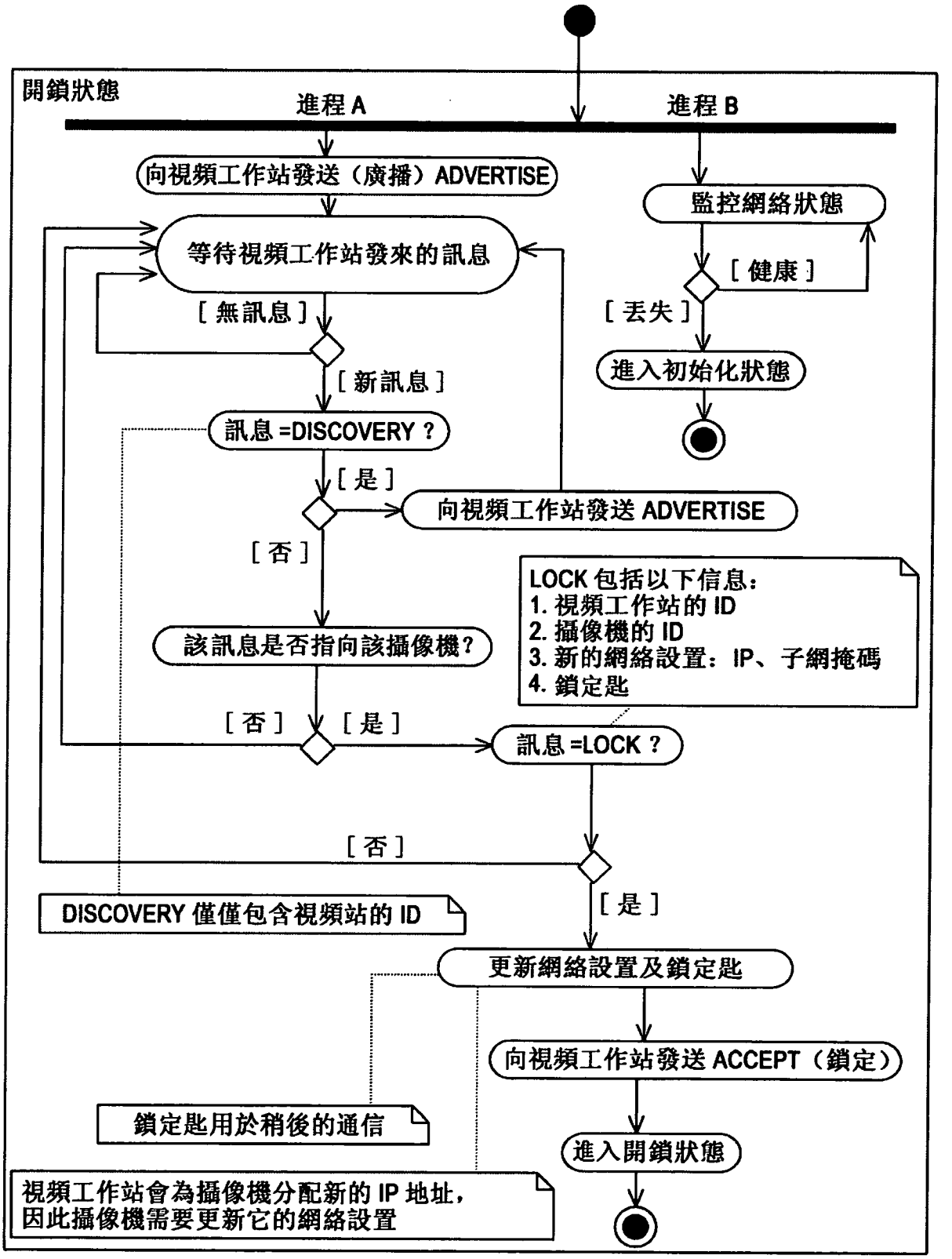

開鎖狀態
進程 A
進程 B
向視頻工作站發送（廣播）ADVERTISE
監控網絡狀態
等待視頻工作站發來的訊息
[健康]
[丟失]
[無訊息]
進入初始化狀態
[新訊息]
訊息 =DISCOVERY ?
[是]
向視頻工作站發送 ADVERTISE
[否]
LOCK 包括以下信息：
1. 視頻工作站的 ID
2. 攝像機的 ID
3. 新的網絡設置：IP、子網掩碼
4. 鎖定匙
該訊息是否指向該攝像機?
[否]
[是]
訊息 =LOCK ?
[否]
[是]
DISCOVERY 僅僅包含視頻站的 ID
更新網絡設置及鎖定匙
向視頻工作站發送 ACCEPT（鎖定）
鎖定匙用於稍後的通信
進入開鎖狀態
視頻工作站會為攝像機分配新的 IP 地址，
因此攝像機需要更新它的網絡設置

圖 4c

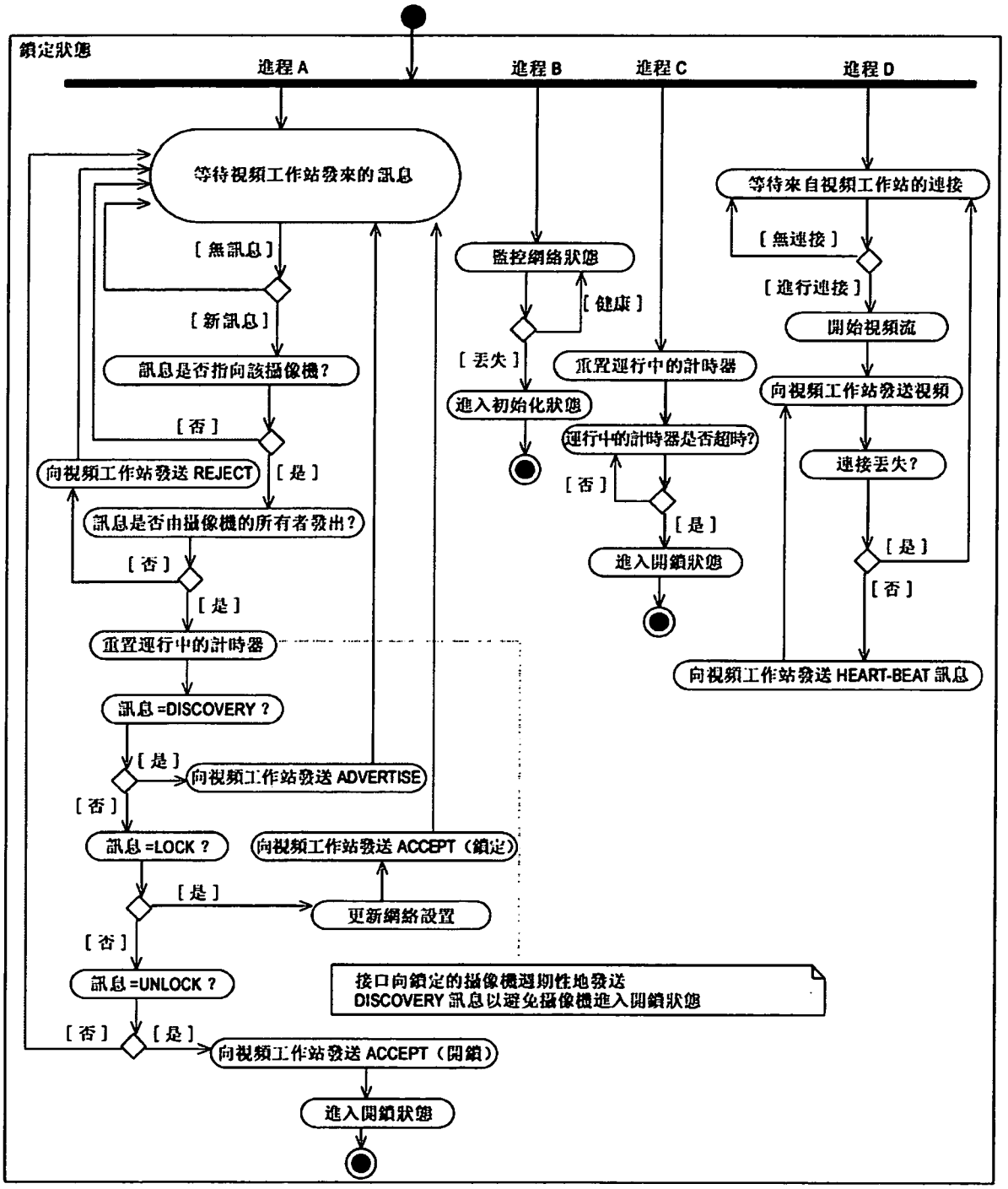

鎖定狀態
進程 A
進程 B
進程 C
進程 D
等待視頻工作站發來的訊息
[無訊息]
[新訊息]
訊息是否指向該攝像機?
[否]
[是]
向視頻工作站發送 REJECT
訊息是否由攝像機的所有者發出?
[否]
[是]
重置運行中的計時器
訊息 =DISCOVERY ?
[是]
向視頻工作站發送 ADVERTISE
[否]
訊息 =LOCK ?
向視頻工作站發送 ACCEPT（鎖定）
[是]
更新網絡設置
[否]
訊息 =UNLOCK ?
[否]
[是]
向視頻工作站發送 ACCEPT（開鎖）
進入開鎖狀態
接口向鎖定的攝像機週期性地發送
DISCOVERY 訊息以避免攝像機進入開鎖狀態
監控網絡狀態
[健康]
[丟失]
進入初始化狀態
重置運行中的計時器
運行中的計時器是否超時?
[否]
[是]
進入開鎖狀態
等待來自視頻工作站的連接
[無連接]
[進行連接]
開始視頻流
向視頻工作站發送視頻
連接丟失?
[是]
[否]
向視頻工作站發送 HEART-BEAT 訊息

圖 4d

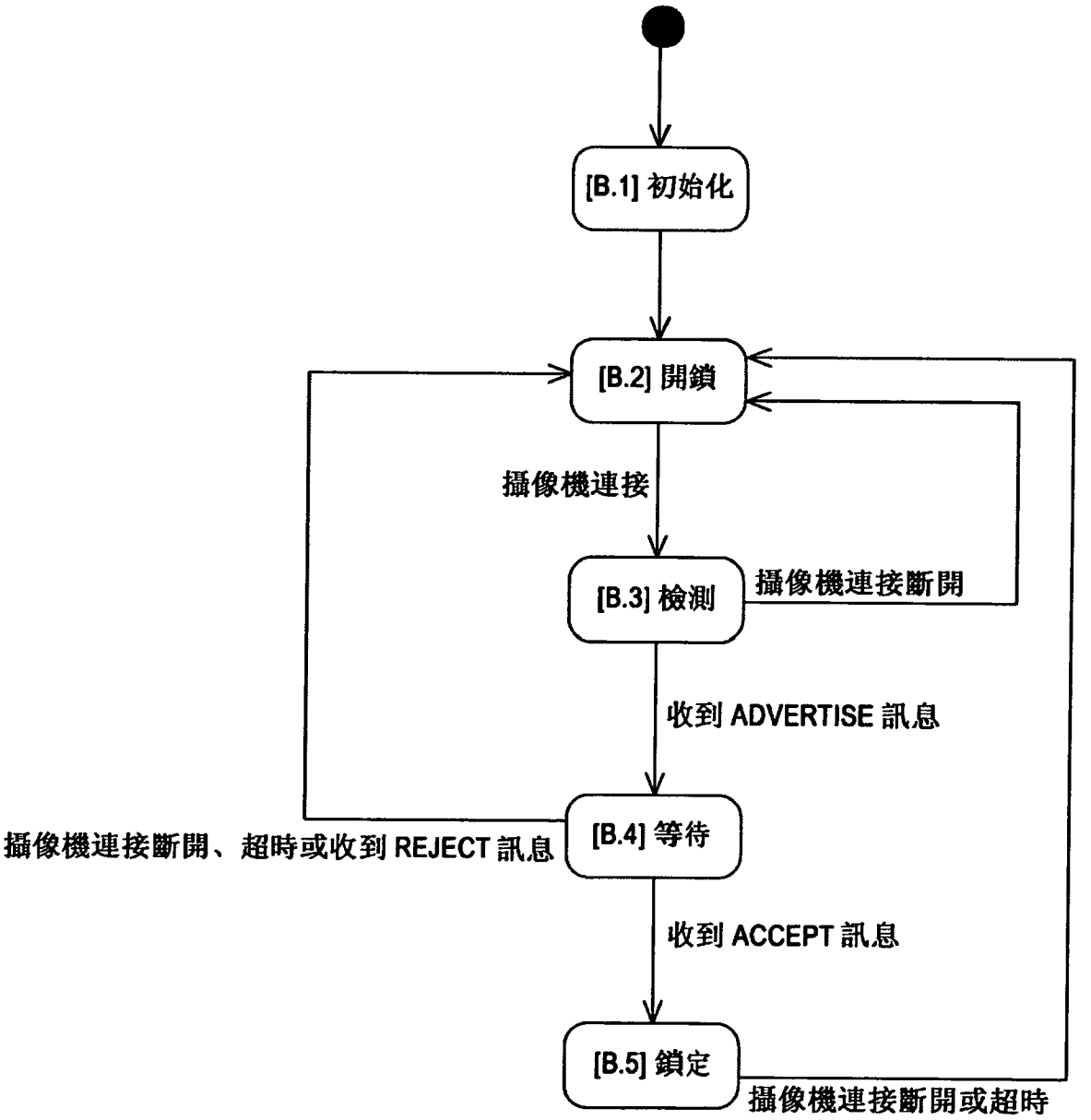

[B.1] 初始化
[B.2] 開鎖
攝像機連接
[B.3] 檢測
攝像機連接斷開
收到 ADVERTISE 訊息
攝像機連接斷開、超時或收到 REJECT 訊息
[B.4] 等待
收到 ACCEPT 訊息
[B.5] 鎖定
攝像機連接斷開或超時

圖 5a

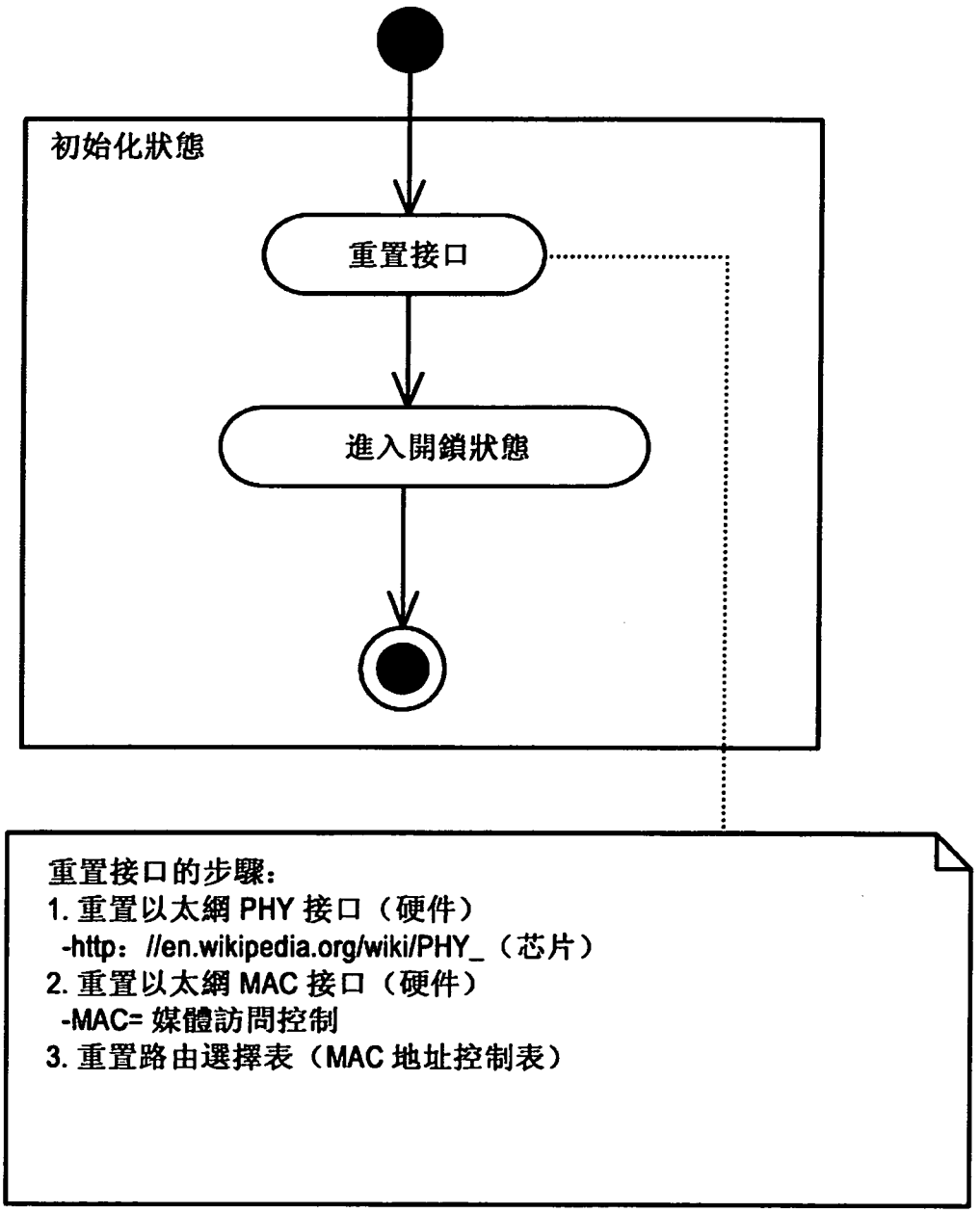

初始化狀態
重置接口
進入開鎖狀態
重置接口的步驟：
1. 重置以太網 PHY 接口（硬件）
-http：//en.wikipedia.org/wiki/PHY_（芯片）
2. 重置以太網 MAC 接口（硬件）
-MAC= 媒體訪問控制
3. 重置路由選擇表（MAC 地址控制表）

圖 5b

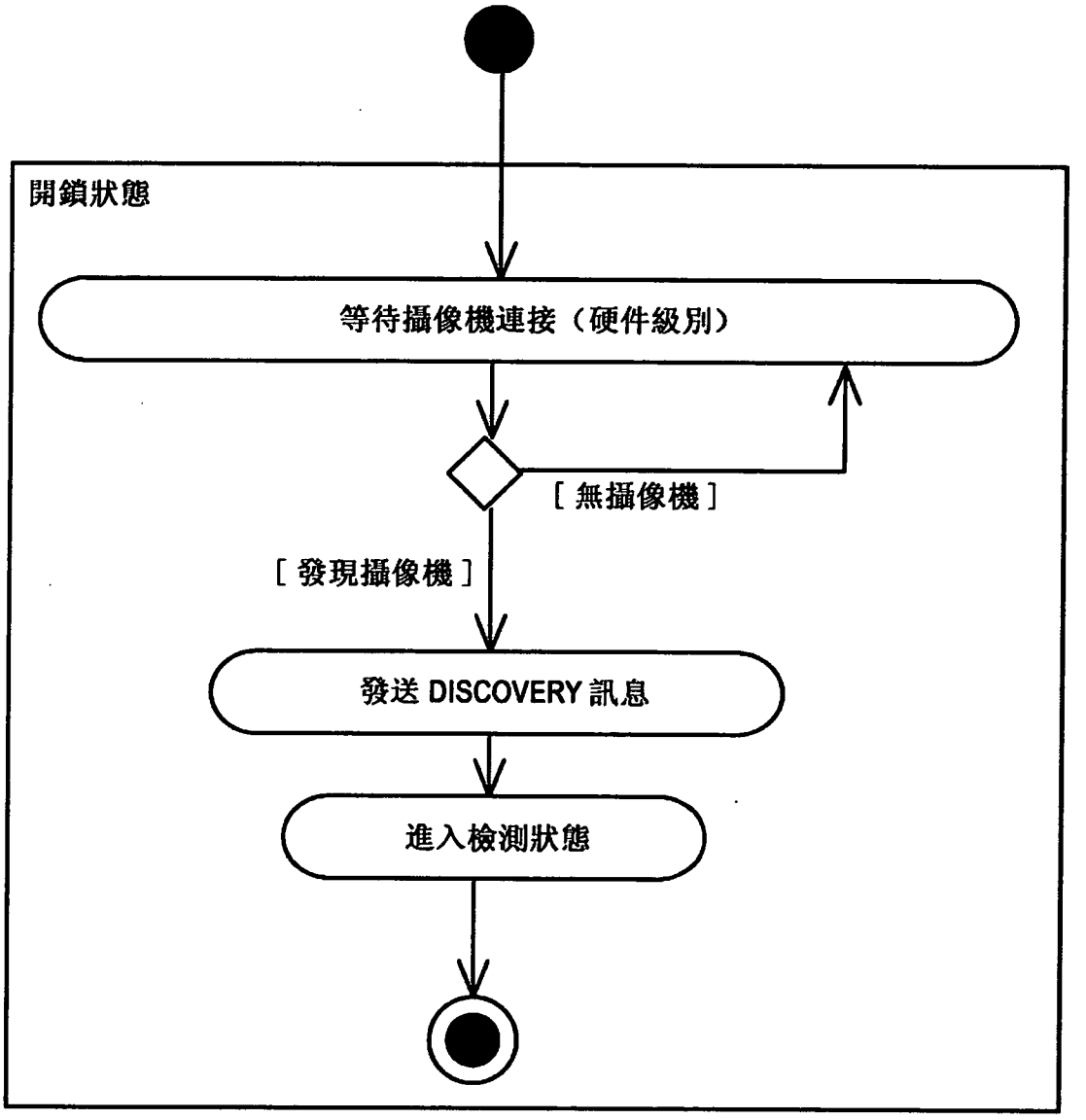


圖 5c

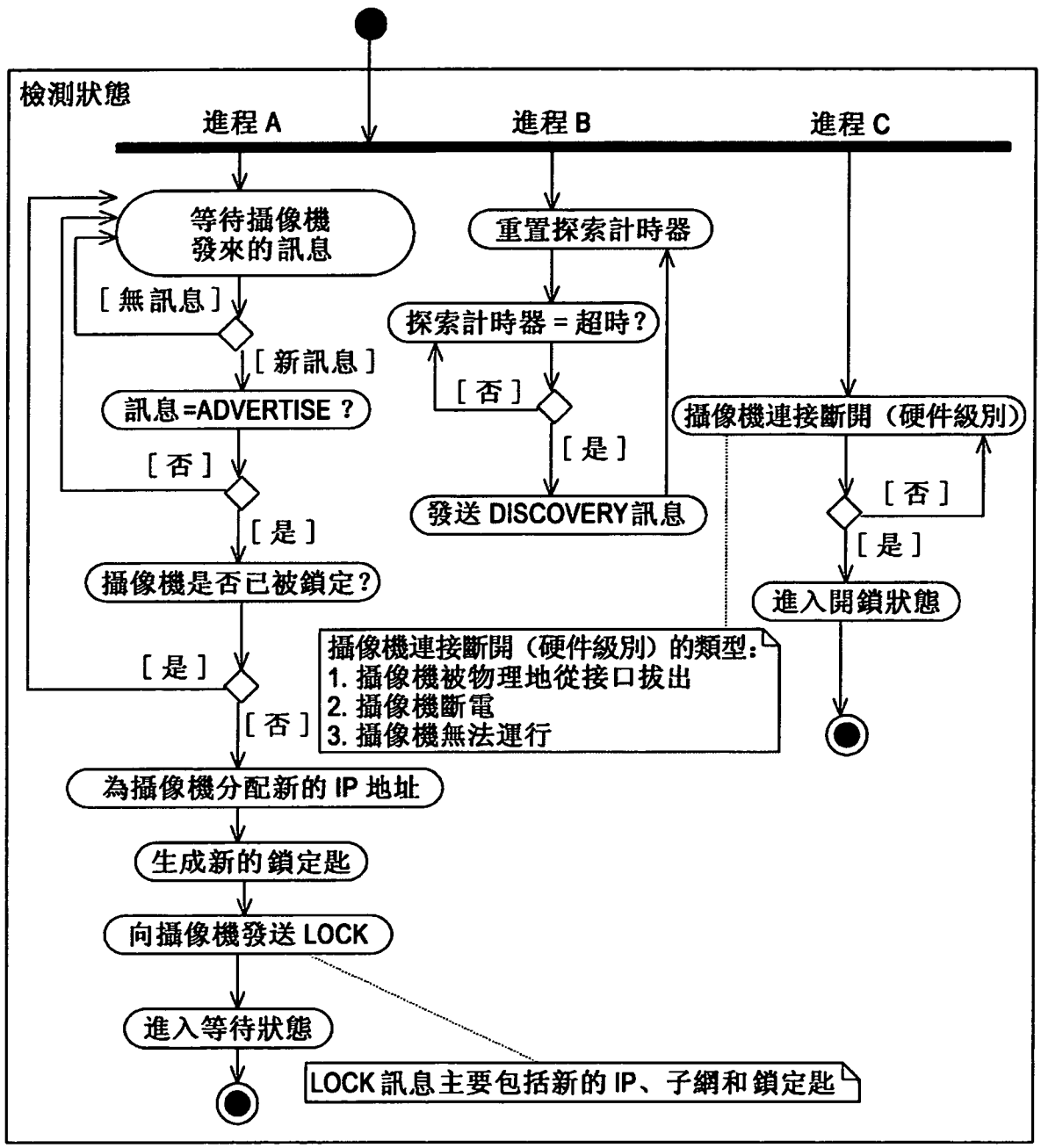

檢測狀態
進程 A
進程 B
進程 C
等待攝像機發來的訊息
[無訊息]
[新訊息]
訊息=ADVERTISE ?
[否]
[是]
攝像機是否已被鎖定?
[是]
[否]
為攝像機分配新的 IP 地址
生成新的鎖定匙
向攝像機發送 LOCK
進入等待狀態
重置探索計時器
探索計時器 = 超時?
[否]
[是]
發送 DISCOVERY訊息
攝像機連接斷開（硬件級別）
[否]
[是]
進入開鎖狀態
攝像機連接斷開（硬件級別）的類型:
1. 攝像機被物理地從接口拔出
2. 攝像機斷電
3. 攝像機無法運行
LOCK 訊息主要包括新的 IP、子網和鎖定匙

圖 5d

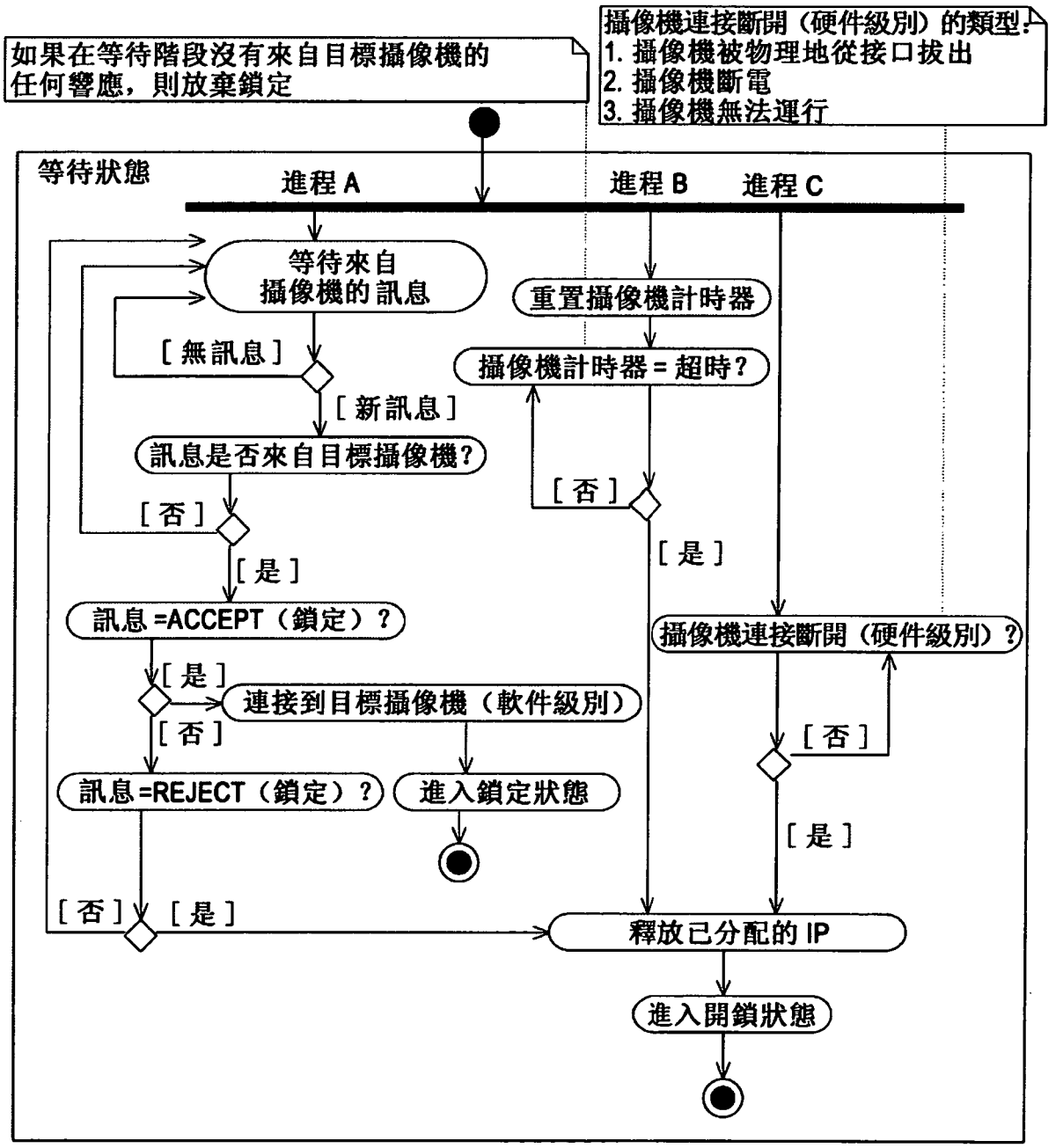

如果在等待階段沒有來自目標攝像機的
任何響應，則放棄鎖定
攝像機連接斷開（硬件級別）的類型：
1. 攝像機被物理地從接口拔出
2. 攝像機斷電
3. 攝像機無法運行
等待狀態
進程 A
進程 B
進程 C
等待來自
攝像機的訊息
[無訊息]
[新訊息]
訊息是否來自目標攝像機?
[否]
[是]
訊息 =ACCEPT（鎖定）?
[是]
連接到目標攝像機（軟件級別）
[否]
訊息 =REJECT（鎖定）?
進入鎖定狀態
[否]
[是]
重置攝像機計時器
攝像機計時器 = 超時?
[否]
[是]
攝像機連接斷開（硬件級別）?
[否]
[是]
釋放已分配的 IP
進入開鎖狀態

圖 5e

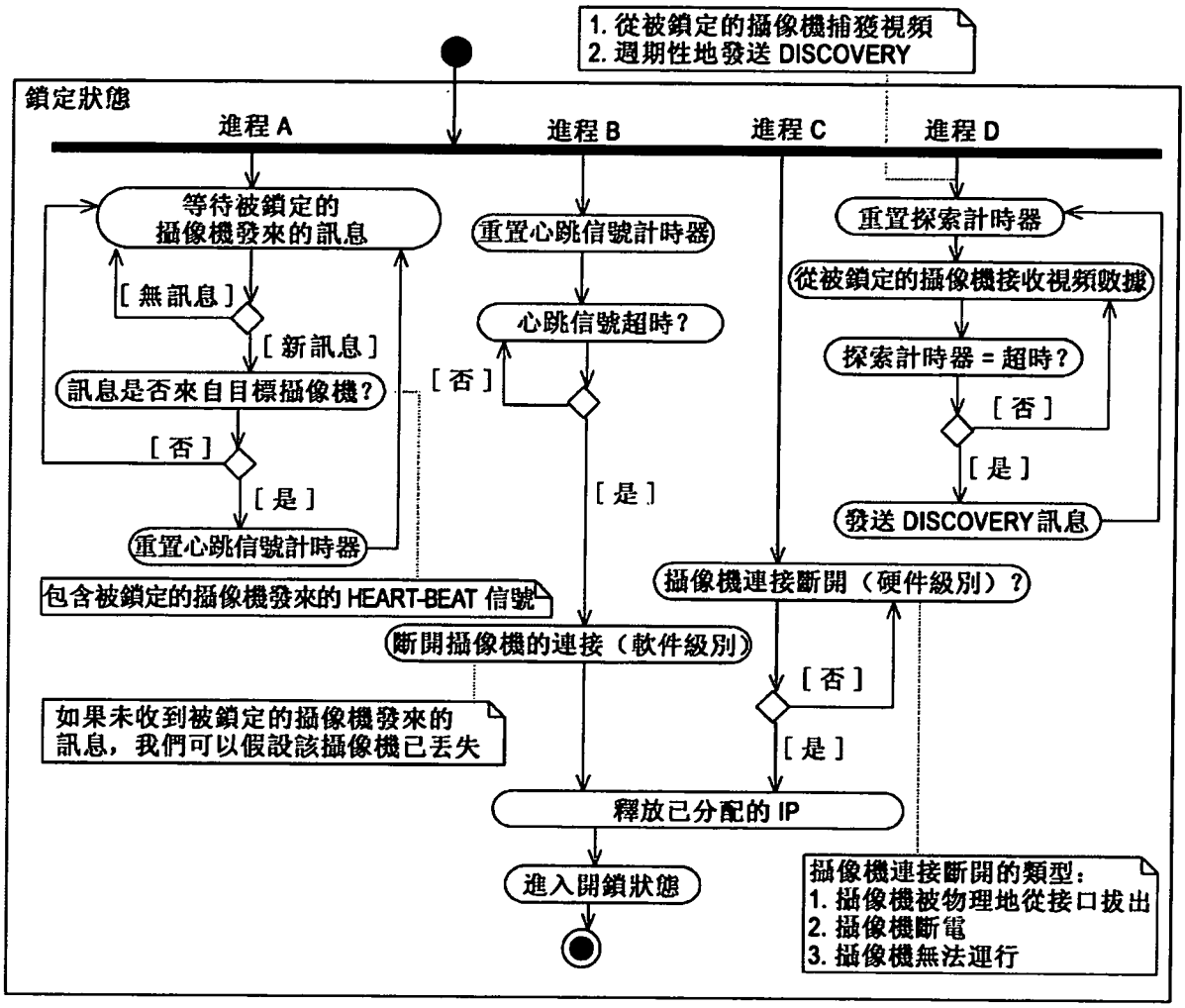

1. 從被鎖定的攝像機捕獲視頻
2. 週期性地發送 DISCOVERY
鎖定狀態
進程 A
進程 B
進程 C
進程 D
等待被鎖定的攝像機發來的訊息
[無訊息]
[新訊息]
訊息是否來自目標攝像機?
[否]
[是]
重置心跳信號計時器
包含被鎖定的攝像機發來的 HEART-BEAT 信號
重置心跳信號計時器
心跳信號超時?
[否]
[是]
斷開攝像機的連接（軟件級別）
如果未收到被鎖定的攝像機發來的訊息，我們可以假設該攝像機已丟失
重置探索計時器
從被鎖定的攝像機接收視頻數據
探索計時器 = 超時?
[否]
[是]
發送 DISCOVERY 訊息
攝像機連接斷開（硬件級別）?
[否]
[是]
釋放已分配的 IP
進入閒鎖狀態
攝像機連接斷開的類型:
1. 攝像機被物理地從接口拔出
2. 攝像機斷電
3. 攝像機無法運行

圖 5f