I497438

(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 I497438 B**

(45)公告日： 中華民國 104 (2015) 年 08 月 21 日

(21)申請案號：102143193 (22)申請日： 中華民國 102 (2013) 年 11 月 27 日

(51)Int. Cl.： *G06Q50/06 (2012.01)* *G06F9/445 (2006.01)*

(71)申請人：財團法人工業技術研究院 (中華民國) INDUSTRIAL TECHNOLOGY RESEARCH INSTITUTE (TW)

新竹縣竹東鎮中興路 4 段 195 號

(72)發明人：陳耀鑫 CHEN, YAO HSIN (TW) ；徐彬海 HSU, PING HAI (TW)

(74)代理人：陳昭誠

(56)參考文獻：

TW	201227372A	TW	201334491A
CN	101183932A	CN	102111265A
US	2013/0293390A1		

審查人員：廖國智

申請專利範圍項數：12 項 圖式數：9 共 46 頁

(54)名稱

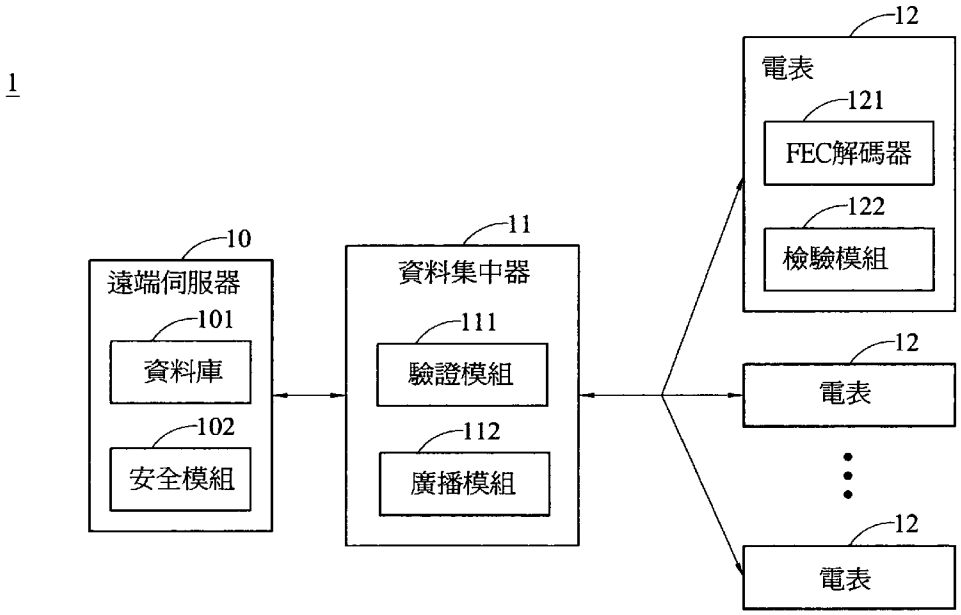
先進讀表基礎建設中之韌體更新系統及其方法

A SYSTEM FOR FIRMWARE UPGRADE IN AMI AND METHOD THEREOF

(57)摘要

本揭露提供一種先進讀表基礎建設中之韌體更新系統及其方法，首先由遠端伺服器提供韌體映像檔，資料集中器收到韌體映像檔後驗證遠端伺服器的合法性，韌體映像檔所產生之至少一編碼符號由資料集中器透過廣播方式及最少重送內容的重送機制傳送到至少一電表，令各電表接收完預定數量的編碼符號後，將所接收之編碼符號還原成原始的韌體映像檔，之後，電表接收由遠端伺服器所產生的啟動碼並驗證其合法性後，電表即可執行韌體更新。

Disclosed is a system for firmware upgrade in AMI and method thereof. A remote server provides firmware image. A data concentrator verifies the legitimacy of the remote server after receiving the firmware image. encodes At least one encoding symbol generated by the firmware imageuenc can be transmitted to at least one meter through broadcast and retransmission mechanism of the minimum retransmission content. After each meter receives the specified amount of encoding symbols, the each meter restores the received encoding symbols to the original firmware image. Then, the meters receive a activation code generated by the remote server and verify its legitimacy. Finally, the meters can perform the firmware upgrading.



1・・・先進讀表基礎建設中之韌體更新系統

10・・・遠端伺服器

101・・・資料庫

102・・・安全模組

11・・・資料集中器

111・・・驗證模組

112・・・廣播模組

12・・・電表

121・・・FEC 解碼器

122・・・檢驗模組

第1圖

公告本

發明摘要

※申請案號：102143193

※申請日：102. 11. 27

※IPC分類：G06F 9/445 (2006.01)
G06F 9/44 (2012.01)

【發明名稱】(中文/英文)

先進讀表基礎建設中之韌體更新系統及其方法

A SYSTEM FOR FIRMWARE UPGRADE IN AMI AND METHOD THEREOF

【中文】

本揭露提供一種先進讀表基礎建設中之韌體更新系統及其方法，首先由遠端伺服器提供韌體映像檔，資料集中器收到韌體映像檔後驗證遠端伺服器的合法性，韌體映像檔所產生之至少一編碼符號由資料集中器透過廣播方式及最少重送內容的重送機制傳送到至少一電表，令各電表接收完預定數量的編碼符號後，將所接收之編碼符號還原成原始的韌體映像檔，之後，電表接收由遠端伺服器所產生的啓動碼並驗證其合法性後，電表即可執行韌體更新。

【英文】

Disclosed is a system for firmware upgrade in AMI and method thereof. A remote server provides firmware image. A data concentrator verifies the legitimacy of the remote server after receiving the firmware image. encodes At least one encoding symbol generated by the firmware imageuenc can be transmitted to at least one meter through broadcast and retransmission mechanism of the minimum retransmission content. After each meter receives the specified amount of encoding symbols, the each meter restores the received encoding symbols to the original firmware image. Then, the meters receive a activation code generated by the remote server and verify its legitimacy. Finally, the meters can perform the firmware upgrading.

【代表圖】

【本案指定代表圖】：第（ 1 ）圖。

【本代表圖之符號簡單說明】：

1　先進讀表基礎建設中之韌體更新系統

10　遠端伺服器

101　資料庫

102　安全模組

11　資料集中器

111　驗證模組

112　廣播模組

12　電表

121　FEC 解碼器

122　檢驗模組

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：

本案無化學式。

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）

先進讀表基礎建設中之韌體更新系統及其方法

A SYSTEM FOR FIRMWARE UPGRADE IN AMI AND METHOD THEREOF

【技術領域】

本揭露係關於一種遠端韌體更新技術，更詳而言之，係一種適用於先進讀表基礎建設中的遠端韌體更新系統及其方法。

【先前技術】

隨著環保議題與能源問題高漲，許多國家致力於智慧電網的建設，期盼可透過監控與管理使電力資源配置與運行更有效率，以達到節省能源的目的。爲達前述目的，現行已提出一種具有雙向溝通功能的先進讀表基礎建設（Advanced Metering Infrastructure；AMI），透過 AMI 的應用使電力系統資訊化，因而 AMI 可爲智慧電網的基礎骨幹。

AMI 網路被視爲智慧電網建置的切入點，也是鏈結電力供應端與需求端的基礎建設，其包含三個基本元件：電表(Meter)、資料集中器(Data Concentrator)及頭端伺服器(Head-end Server)，透過資料集中器從中介接，使得電表（如智慧型電表）和頭端伺服器建立通訊。爲了延長使用年限，可擴充性及即時修補安全漏洞對於電表是重要的，亦即電

表是需要具備可遠端韌體更新（remote firmware upgrade）的功能，以因應未來可能增加的新應用或者是安全漏洞之修補。然而，在 AMI 中電表的數量過於龐大，且連接電表與資料集中器的通訊介面是屬於窄頻網路，像是窄頻電力線通訊（narrow-band power line communication），此情況下導致傳輸過慢而影響更新速度，嚴重者會在更新未完成下而影響電表的讀表，舉例來說，現行 AMI 中的韌體更新是採用一對一的更新方式，頭端伺服器提供韌體映像檔給資料集中器，資料集中器將韌體映像檔分割成多個檔案後以將各檔案傳送至各電表，當每一個電表缺乏的檔案不一樣時，則需資料集中器各別重送缺乏的部分，不僅沒效率也耗時過久。因此，在不影響讀表的情況下完成電表的韌體更新成了一大挑戰。

除了韌體更新效率之外，安全保護也是影響韌體更新成敗的重要條件。在韌體更新的過程中，需要避免攻擊者利用植入後門的韌體來竊取 AMI 網路上的機密資訊或侵犯使用者的隱私，特別是，如何確保資料集中器所收到韌體映像檔的來源無誤，電表如何驗證來自資料集中器的檔案是正確的，如此才能建構出完整的安全防護。由上可知，現行 AMI 網路中電表的韌體更新程序仍有需要改進者，例如：在一讀表周期（約爲 15 分鐘）內完成韌體更新程序、提供韌體來源驗證之安全防護以及端對端（end-to-end）的安全防護等，透過在電表進行韌體更新之前確保韌體來源合法，以避免因資料集中器遭受攻擊而影響整個程序的安

全。

因此，如何在不改變現有 AMI 網路架構下，找出一種具備高韌體更新效率並確保韌體更新之安全性的韌體更新方法，以提供 AMI 中電表的遠端韌體更新，實爲本技術領域之人亟欲解決的技術課題。

【發明內容】

本揭露提出一種先進讀表基礎建設中之韌體更新系統及其方法，係透過廣播/多點傳輸機制，搭配前向錯誤更正（Forward Error Correction，FEC）技術以提高更新效率，另外，還利用韌體來源驗證技術與端對端（End-to-End）安全技術來確保韌體更新的安全性。

本揭露係提供先進讀表基礎建設中之韌體更新系統，係包括：遠端伺服器、資料集中器以及至少一電表。該遠端伺服器包含用於儲存韌體映像檔之資料庫以及用於產生數位簽章資料和啓動碼之安全模組；該資料集中器係連線至該遠端伺服器，其包括：驗證模組及廣播模組，其中，該驗證模組用於透過該數位簽章資料以驗證來自該遠端伺服器之韌體映像檔的合法性，該廣播模組用於將該韌體映像檔所產生之複數個編碼符號中以超過一設定數量透過廣播方式進行發送，且依據該些編碼符號接收狀態得到最少重送內容，以於未被廣播之編碼符號中選擇符合該最少重送內容之數量並將其再次廣播；另外，至少一電表係與該資料集中器連線，各該電表，其具有：FEC 解碼器及檢驗模組，該 FEC 解碼器用於解碼來自該資料集中器之多個被廣播之編碼符號，以透過該多個被廣播之編碼符

號還原該韌體映像檔，而該檢驗模組用於確認 FEC 解碼器所還原之韌體映像檔的完成度，且自該資料集中器取得來自該遠端伺服器之該啓動碼，該啓動碼經檢驗後係用於驅動該電表進行韌體更新。

於一實施例中，該資料集中器更包括一 FEC 編碼器，該 FEC 編碼器係收集符合各該電表之韌體區塊大小及傳輸訊框大小以得到各該電表之傳輸限制，透過比對電表所能支援之傳輸限制得到該編碼符號之單位切割尺寸，並將該資料集中器所接收之韌體映像檔進行編碼以產生至少一符合該單位切割尺寸之該編碼符號，所謂單位切割尺寸可利用最小切割尺寸。

於另一實施例中，該遠端伺服器更包括一 FEC 編碼器，係用於將該韌體映像檔以特定韌體區塊大小進行編碼來產生已編碼的韌體映像檔，並傳送至該資料集中器。

本揭露還提出一種先進讀表基礎建設中之韌體更新方法，係包括：令資料集中器自遠端伺服器取得韌體映像檔，且透過來源認證機制確認該遠端伺服器的合法性；令該資料集中器利用廣播方式將該韌體映像檔所產生之至少一編碼符號發送至各該電表，且由各該電表所回傳之訊息計算出最少重送內容，該資料集中器將未被廣播之編碼符號中選擇符合該最少重送內容之數量並再次廣播直到各該電表已收集足夠之編碼符號並還原該韌體映像檔；驗證該韌體映像檔的版本及完成度；以及令各該電表取得啓動碼，且於確認該啓動碼的正確性後執行韌體更新。

前述方法中，該韌體映像檔之編碼包括令該資料集中器取得各該電表所支援之傳輸限制，並依據各該電表之傳輸限制透過編碼符號長度演算法將該韌體映像檔進行編碼以產生該至少一編碼符號，或者於該遠端伺服器中以預定之韌體區塊大小進行編碼以產生該至少一編碼符號並傳送至該資料集中器。

相較於習知技術，本揭露所提出之先進讀表基礎建設中之韌體更新系統及其方法，將現有先進讀表基礎建設中的韌體更新進行改善，首先，透過廣播及多點傳送方式，解決目前一對一傳輸韌體的低效率模式，同時本揭露提出一種編碼符號長度演算法，藉此依據各電表可支援之傳輸大小以提供適當的韌體映像檔切割方式，以達到最佳傳送效率，另外，本揭露更利用前向錯誤更正（FEC）的技術原理提出一種重送計數演算法，藉此解決現行將各電表所缺少之檔案各別重送之問題，再者，本揭露搭配來源驗證技術與端對端安全技術以確保電表所取得韌體的合法性。透過本揭露前述多項技術，可確保各電表可有效地進行遠端韌體更新，同時避免因低效率而影響電表的讀表，同時可提升韌體更新的正確性及安全性。

【圖式簡單說明】

第 1 圖係爲本揭露之先進讀表基礎建設中之韌體更新系統的系統示意圖；

第 2 圖係爲本揭露之先進讀表基礎建設中之韌體更新系統之一具體實施例的示意圖；

第 3A 和 3B 圖係爲習知韌體更新方式與本揭露之韌體更新方式差異比較的示意圖；

第 4 圖係爲本揭露之先進讀表基礎建設中之韌體更新方法之流程圖；

第 5A-5E 圖係爲第 4 圖中各流程具體實施的流程圖；

第 6 圖係爲本揭露之先進讀表基礎建設中之韌體更新系統之另一具體實施例的示意圖；

第 7 圖係爲本揭露之先進讀表基礎建設中之韌體更新方法之另一具體實施例之流程圖；

第 8A-8B 圖係爲另一具體實施例的流程圖；以及

第 9A 和 9B 圖係爲本揭露之編碼符號長度演算法及重送計數演算法之說明示意圖。

【實施方式】

以下藉由特定的具體實施形態說明本揭露之技術內容，熟悉此技藝之人士可由本說明書所揭示之內容輕易地瞭解本揭露之優點與功效。然本揭露亦可藉由其他不同的具體實施形態加以施行或應用。

第 1 圖係說明本揭露之先進讀表基礎建設中之韌體更新系統的系統示意圖。如圖所示，先進讀表基礎建設中之韌體更新系統 1 提供先進讀表基礎建設中電表的韌體更新，雖然目前先進讀表基礎建設中的電表可進行韌體更新，但其採用一對一單點傳輸方式以及分別依各電表所缺少之韌體分割檔案進行重傳，將造成韌體更新低效率，且也缺乏較佳的驗證方式，因而本揭露提出一種高效率且高

安全性的韌體更新機制。

如該圖所示，先進讀表基礎建設中之韌體更新系統 1 主要包括遠端伺服器 10、資料集中器 11 以及至少一電表 12。

遠端伺服器 10 係包含資料庫 101 和安全模組 102。資料庫 101 是用於儲存韌體映像檔，而安全模組 102 是用於產生數位簽章資料和啓動碼，數位簽章資料可用於資料集中器 11 確認所接收的資料是否來自遠端伺服器 10，而啓動碼是供電表 12 啓動更新時使用。

資料集中器 11 是連線至遠端伺服器 10，其包括驗證模組 111 以及廣播模組 112。

驗證模組 111 是利用該數位簽章資料以驗證所接收之韌體映像檔是否來自遠端伺服器，驗證模組 111 主要建立遠端伺服器 10 和資料集中器 11 之間的安全性，避免資料集中器 11 自不合法之遠端伺服器 10 接收到資料。

廣播模組 112 是將超過一設定數量之編碼符號透過廣播方式進行發送，該些編碼符號是由韌體映像檔所產生者，且依據編碼符號接收狀態得到最少重送內容，之後再次廣播符合該最少重送內容之數量的新的編碼符號，亦即先前未廣播過的編碼符號。與現有技術不同的，本實施例是透過廣播方式進行編碼符號的發送，並且由每一個電表 12 接收其編碼符號接收狀態，以計算出接下來要重送的編碼符號之數量，換言之，廣播模組 112 會比較該設定數量與各電表 12 所接收之編碼符號的數量，藉此得到各電表 12

還原出韌體映像檔所需補足之編碼符號的數量，以作爲前述之最少重送內容，之後可將先前未曾廣播的編碼符號再透過廣播方式傳送，以補足各電表 12 還原出韌體映像檔所需的編碼符號數量。

本揭露所述技術中在收到一定數量的分割檔案後，即可還原出原本被切割的檔案，換句話說，本案實施例確認每一個電表是否有足夠的編碼符號可以進行還原程序，而無論每一個電表所缺少的編碼符號爲何者。舉例來說，本實施例可採用 FEC 編碼技術，亦即，若韌體映像檔被切割成 10 個編碼符號，且透過 FEC 編碼技術僅需 5 個編碼符號就能還原，所以一開始可以先傳編號 1-5 的編碼符號，在收集各電表缺少數量後，例如數量最大值爲 2，則無論該些電表缺少的爲何者，可再重新送編號 6 和 7 的編碼符號，即有可能讓電表收集到用於還原的所需數量。

此外，多個獨立的電表 12 是與資料集中器 11 連線，各該電表 12 包括 FEC 解碼器 121 以及檢驗模組 122。其中，FEC 解碼器 121 是將來自資料集中器 11 之多個編碼符號進行解碼，以將該多個編碼符號還原成該韌體映像檔，換言之，當電表 12 收集到足夠數量的編碼符號時，FEC 解碼器 121 即可利用該些編碼符號還原出原本的韌體映像檔。

另外，檢驗模組 122 是用於確認 FEC 解碼器 121 所還原之韌體映像檔的完成度，以及自該資料集中器 11 取得來自遠端伺服器 10 之啓動碼，此啓動碼經過檢驗後，若可確認該啓動碼確實爲遠端伺服器 10 所提供者，即可用此啓動

碼進行電表進行韌體更新的驅動。

由上可知，遠端伺服器 10 提供韌體版本的控制，並且提供韌體映像檔至資料集中器 11，資料集中器 11 在收到韌體映像檔之後，利用其驗證模組 111 負責驗證遠端伺服器 10 的合法性，通過合法性驗證之後，資料集中器 11 將由韌體映像檔所產生之編碼符號，之後，利用廣播模組 112 將該些編碼符號作廣播，以將經過處理的韌體映像檔（即分割成至少一編碼符號）傳送給每一個電表 12。

電表 12 接收完由資料集中器 11 傳送過來的編碼符號之後，先經過 FEC 解碼器 121 進行解碼以還原出原始的韌體映像檔，經過完成度確認後先行暫存，待電表 12 接收由遠端伺服器 10 中的安全模組 102 所產生的啓動碼後，同樣驗證其合法性，並於合法性通過後驅動電表 12 進行韌體更新。

第 2 圖係爲本揭露之先進讀表基礎建設中之韌體更新系統之一具體實施例的示意圖。如圖所示，先進讀表基礎建設中之韌體更新系統 2 同樣由遠端伺服器 20、資料集中器 21 以及數個電表 22 所組成。

於遠端伺服器 20 中韌體映像檔資料庫 201 及安全模組 202 與第 1 圖之資料庫 101 和安全模組 102 功能相似，資料集中器 21 中驗證模組 211 以及廣播模組 213 與第 1 圖之驗證模組 111 以及廣播模組 112 功能相似，電表 22 中 FEC 解碼器 221 以及檢驗模組 222 與第 1 圖之 FEC 解碼器 121 以及檢驗模組 122 功能相似，故不再贅述。

於本實施例中，遠端伺服器 20 內還包括控制模組 203 用於提供遠端伺服器 20 的運作，例如通訊或韌體版本管理等。此外，資料集中器 21 還包括 FEC 編碼器 212、控制模組 214 和傳輸模組 215。

FEC 編碼器 212 是用於計算韌體映像檔之可最小切割尺寸，藉此將韌體映像檔進行編碼後以產生多個符合前述最小切割尺寸的編碼符號。具體來說，FEC 編碼器 212 主要是將韌體映像檔切割成適當大小後再進行傳送，這裡所述的適當大小，係由 FEC 編碼器 212 收集符合各電表 22 之韌體區塊大小及傳輸訊框大小等傳輸限制，透過比對所有電表所能支援之傳輸限制，以得到一單位切割尺寸，該單位切割尺寸可爲編碼符號之最小切割尺寸。關於映像檔區塊大小及傳輸訊框大小，後面將有更詳細說明。

此外，除了可於資料集中器 21 上執行韌體映像檔之編碼外，韌體映像檔之編碼也可在其他設備上執行，例如在遠端伺服器 20，亦即在遠端伺服器 20 先將韌體映像檔進行編碼後才傳送至資料集中器 21，關於韌體映像檔在遠端伺服器 10 之編碼的實施例之後將再詳述。

控制模組 214 是提供資料集中器 21 內的基本運作，例如操作傳輸模組 215 進行資料的傳輸，而傳輸模組 215 用於與遠端伺服器 20 和電表 22 進行資料傳輸，其後可與驗證模組 211 連線進行遠端伺服器 20 的合法性驗證，也可將 FEC 編碼器 212 所編碼的韌體映像檔經廣播模組 213 而由

傳輸模組 215 傳送出去。電表 22 內含記憶體 223，可用於暫存 FEC 解碼器 221 所解碼還原出的韌體映像檔，而傳輸模組 224 則提供電表 22 對外傳輸。

此外，遠端伺服器 20 和資料集中器 21 之間爲廣域網路（Wide Area Network，WAN），而資料集中器 21 與電表 22 爲例如電力線通訊（Power Line Communication，PLC）或是射頻（RF）的鄰近區域網路（Neighborhood Area Network，NAN）。

第 3A 和 3B 圖係爲習知韌體更新方式與本揭露之韌體更新方式差異比較的示意圖。如第 3A 圖所示，係圖示目前電表韌體更新的問題，首先，遠端伺服器將韌體映像檔傳送至資料集中器，資料集中器會將韌體映像檔分割成數個映像檔區塊來傳遞，如圖中所示的編號 1~5，資料集中器與各電表間是一對一的傳送，經傳送後，每一個電表所缺的映像檔區塊不一樣，在目前電表韌體更新的機制中，僅能要求資料集中器針對每一電表所缺的映像檔區塊進行重送，不僅沒效率且耗時，間接可能影響到讀表週期。

反觀本揭露所提出者，如第 3B 圖所示，同樣地，遠端伺服器會將韌體映像檔傳送至資料集中器，資料集中器透過 FEC 編碼器進行編碼以將韌體映像檔分割成數個編碼符號，如圖所示的編號 1~6，於本實施中，資料集中器與各電表之間並非一對一溝通，而是資料集中器以廣播方式傳遞該些編碼符號，如前所述，FEC 編碼器的解碼還原過程，無需等所有編碼符號收集到才能進行，而是僅需收集

一定數量以上編碼符號即可，這裡假設是 5 個，因而資料集中器先傳送編號 1~5。

經傳送後，每一個電表所缺的編碼符號可能不一樣（如圖所示，五個電表所接內容皆不同），但透過本實施例的 FEC 編碼機制，只要夠多數量的編碼符號即可解碼還原，剛好大家都僅缺少一個編碼符號，故資料集中器可發送編號 6 的編碼符號，若各電表取得該編號 6 的編碼符號後，即收集到足夠的編碼符號，即可進行解碼還原。

由上可知，無需知悉每一個電表所缺的編碼符號爲何，僅要知道各電表所缺編碼符號的數量即可，亦即，當電表尚未收集足夠編碼符號時，可持續提供新的（未傳送過）編碼符號讓電表來收集，因此，搭配廣播方式避免一對一傳遞所導致沒效率情況，且無需在乎電表缺少的編碼符號爲何者，僅需提供足夠數量即可，也讓整個重送機制更簡便快速。

最後，資料集中器與遠端伺服器間通過來源認證機制來達到安全控管，電表也需透過遠端伺服器所提供之啓動碼來進行韌體更新，因此，透過來源認證機制和啓動碼可確保韌體版本正確性以及傳輸安全。

第 4 圖係爲本揭露之先進讀表基礎建設中之韌體更新方法之流程圖。如圖所述，遠端伺服器和資料集中器之間是透過 TCP/IP 通訊協定溝通，資料集中器和電表之間則透過設備語言訊息規範（Device Language Message Specification，DLMS）與能源計量配套規範（Companion

Specification for Energy Metering，COSEM）連線。

資料集中器會向遠端伺服器詢問是否有新的韌體映像檔。更具體而言，若詢問到有新的韌體映像檔，則資料集中器會自遠端伺服器取得韌體映像檔。

資料集中器與電表之間進行韌體映像檔轉移的初始化，例如知悉各電表所支援的韌體區塊大小，如何將韌體映像檔作編碼切割等。

資料集中器與電表之間進行經編碼的韌體映像檔（即編碼符號）的傳送與重送，韌體映像檔是透過廣播方式傳遞，本實施例是透過 FEC 編碼機制，因而電表僅需收集一定數量的編碼符號即可進行編碼符號的解碼。

資料集中器與電表之間進行韌體映像檔的驗證，爲確保電表所接收到的檔案正確，因而資料集中器會向電表做驗證行爲，可能包括韌體映像檔的版本和完成度。

最後，電表會取得來自遠端伺服器之啓動碼，透過該啓動碼啓動電表內的韌體映像檔，以進行電表的韌體更新。

第 5A-5E 圖係爲第 4 圖中各流程具體實施的流程圖。如第 5A-5E 圖所示，各圖是將第 4 圖中的各個流程進行更詳細說明。

如第 5A 圖所示，即資料集中器向遠端伺服器詢問是否有新的韌體映像檔，必要時取得新的韌體映像檔。首先，資料集中器向遠端伺服器詢問是否有新的韌體映像檔，遠端伺服器回覆結果後，若無，則一段時間後再詢問，若有，則請求新的韌體映像檔，遠端伺服器相應地傳送新的韌體

映像檔到資料集中器。此時，資料集中器會進行來源認證，確保遠端伺服器是合法的，並且確定所接收之韌體映像檔其完整，若有錯誤則停止，若沒有錯誤則繼續下一流程。具體而言，前述之來源認證機制可利用非對稱式加密演算法來驗證遠端伺服器的合法性。

如第 5B 圖所示，即資料集中器與電表之間進行初始化韌體映像檔轉移。首先，資料集中器會自每一個電表（採一對一或廣播模式）詢問每一個電表所能支持的韌體區塊大小和傳輸訊框大小（即電表的傳輸限制），每一個電表各自回覆，接著可由資料集中器計算可使用之編碼符號的長度，例如找出編碼符號之最小切割尺寸，之後透過第 2 圖之 FEC 編碼器進行韌體映像檔的編碼，接著資料集中器通知電表韌體版本與大小等資訊，來初始化韌體映像檔轉移。

其中，關於計算編碼符號長度可透過編碼符號長度演算法來進行，亦即將各電表之傳輸限制利用各電表之映像檔區塊大小（應用層）及傳輸訊框大小（高級數據鏈路控制（HDLC）層），藉此判斷編碼符號之切割大小。

如第 5C 圖所示，係說明資料集中器與電表之間編碼符號的傳送與重送。資料集中器透過廣播方式將編碼符號傳送至各電表，接著資料集中器向各電表詢問韌體映像檔的完成度，而各電表會回傳編碼符號接收狀態，此時，若需要重送，則資料集中器會計算出最少重送內容的數量，此可由第 1 圖中資料集中器之廣播模組來進行，在未完成之前，則持續傳送編碼符號，同一時間，電表這端也會判

斷是否接收到足夠數量的編碼符號，若是，則進行編碼符號的解碼以還原出原始的韌體映像檔。

前述編碼符號長度演算法係收集各電表之韌體區塊大小與傳輸訊框大小以由兩者之中取得各該電表之傳輸限制，並比較自各電表之傳輸限制後，以最小者以作爲編碼符號之單位切割大小，例如以一最小切割尺寸作爲編碼符號的單位切割大小，且各電表於韌體映像檔傳輸過程中所回傳之訊息係指各電表所缺少之編碼符號。

由上可知，資料集中器是利用廣播方式將多個編碼符號發送至各電表中，其利用重送計數演算法將各電表所回傳之訊息計算出最少重送內容，使得資料集中器可再次廣播送出新的編碼符號直到各該電表已收集足夠之編碼符號並還原該韌體映像檔。

如第 5D 圖所示，爲資料集中器與電表之間進行韌體映像檔的完成度驗證。資料集中器會向電表進行韌體映像檔的版本或資訊的確認，若有錯誤則停止更新，若無則如第 5E 圖所示，電表取得遠端伺服器之啓動碼以進行韌體更新。首先，資料集中器會向遠端伺服器取得啓動碼，接著資料集中器向電表要求啓動韌體映像檔，此時，電表內的檢驗模組可對啓動碼進行驗證並將結果回傳至資料集中器，若電表檢驗該啓動碼時發現有錯誤，則停止更新，若沒有錯誤則將電表內現有的韌體更新爲最新的韌體。

第 6 圖係爲本揭露之先進讀表基礎建設中之韌體更新系統之另一具體實施例的示意圖。如圖所示，先進讀表基

礎建設中之韌體更新系統 6 同樣由遠端伺服器 60、資料集中器 61 以及數個電表 62 所組成。

於遠端伺服器 60 中韌體映像檔資料庫 601、安全模組 602 及控制模組 603 與第 2 圖之韌體映像檔資料庫 201、安全模組 202 及控制模組 203 功能相似，資料集中器 61 中驗證模組 611、廣播模組 613、控制模組 614 及傳輸模組 615 與第 2 圖之驗證模組 211、廣播模組 213、控制模組 214 及傳輸模組 215 功能相似，電表 62 中 FEC 解碼器 621、檢驗模組 622、記憶體 623 及傳輸模組 624 與第 2 圖之 FEC 解碼器 221、檢驗模組 222、記憶體 223 及傳輸模組 224 功能相似，故不再贅述。

於本實施例中，遠端伺服器 60 內還包括 FEC 編碼器 604。不同於第 2 圖所示之實施例，本實施例的 FEC 編碼是在遠端伺服器 60 進行，而非在資料集中器 61 中執行，也就是，先於遠端伺服器 60 中將韌體映像檔預先處理後再傳送給資料集中器 61，此實施例可在每一個電表 62 可支援的韌體區塊大小一樣之下來實施。

與第 2 圖所示之實施例相比較，第 2 圖之實施例中收集各電表 22 之韌體區塊大小及傳輸訊框大小，透過比對各電表 22 所能支援之傳輸限制以得到編碼符號之最小切割尺寸，藉此對韌體映像檔進行編碼。然於本實施例中，是先在遠端伺服器 60 將韌體映像檔以特定韌體區塊大小進行編碼以產生經編碼的韌體映像檔，並將該經編碼的韌體映像檔傳送至該資料集中器 61，以供資料集中器 61 透過

廣播方式傳送至各電表62，之後的廣播和補送機制則如先前所述的實施例。

第7圖係爲本揭露之先進讀表基礎建設中之韌體更新方法之另一具體實施例之流程圖。如圖所述，遠端伺服器和資料集中器之間是透過通訊協定溝通，例如，透過TCP/IP，資料集中器和電表之間則透過設備語言訊息規範（DLMS）與能源計量配套規範（COSEM）連線。

首先，遠端伺服器中的韌體映像檔會以特定韌體區塊大小進行編碼以產生已編碼的韌體映像檔。詳言之，資料集中器會向遠端伺服器詢問是否有新的韌體映像檔，並於詢問到有新的韌體映像檔時，向遠端伺服器取得已編碼的韌體映像檔。之後，資料集中器與電表之間進行韌體映像檔轉移程序的初始化。

接著，資料集中器與電表之間進行已編碼的韌體映像檔（即編碼符號）的傳送與重送，本實施例之編碼符號是透過FEC編碼機制來產生，因而電表在解碼過程中僅需收集一定數量的編碼符號即可進行編碼符號的解碼。

之後，資料集中器與電表之間進行韌體映像檔的驗證，藉此確保電表所接收到的檔案正確性，可包括韌體映像檔的版本和完成度。

最後，電表會取得來自遠端伺服器之啓動碼（中間可透過資料集中器），確認啓動碼安全性無誤後，則以啓動碼啓動電表內的韌體映像檔來進行電表的韌體更新。

於本流程圖中，韌體映像檔的編碼是在遠端伺服器中

執行，此於第 4 圖所示之執行編碼時間點和處理設備並不相同，由上可之，韌體映像檔主要在傳輸（廣播）前完成編碼即可，因而在遠端伺服器或資料集中器中執行編碼皆是可行的。

第 8A-8B 圖係另一實施例的流程圖。參考第 6、7 圖所示之實施例是於遠端伺服器進行韌體映像檔的編碼，編碼後資料集中器與電表間的傳遞和驗證過程不再贅述。

如第 8A 圖所示，資料集中器會向遠端伺服器詢問是否有新的韌體映像檔，待遠端伺服器回覆結果後，若無，則一段時間後再詢問，若有，則請求新的韌體映像檔，遠端伺服器相應地傳送新的韌體映像檔到資料集中器，需注意的，此新的韌體映像檔已於遠端伺服器處先進行 FEC 編碼。此後，資料集中器會進行來源認證，確保遠端伺服器是合法性及韌體映像檔的完整性，若有錯誤則停止，若沒有錯誤則繼續下一流程。同樣地，可利用非對稱式加密演算法來驗證遠端伺服器的合法性。

如第 8B 圖所示，即資料集中器與電表之間進行初始化韌體映像檔轉移。資料集中器通知電表韌體版本與大小等資訊，來初始化韌體映像檔轉移。

與第 5B 圖所示的流程相比較，由本實施例中，資料集中器已於在遠端伺服器中取得已編碼的韌體映像檔，因而資料集中器無需再對韌體映像檔進行編碼。本實施例是適用於各電表所支援的韌體區塊大小都一樣下，換言之，若預先知道各電表所支援的韌體區塊大小，則資料集中器

無需向各電表詢問可支援大小，可由遠端伺服器直接以特定韌體區塊大小對韌體映像檔進行編碼。在第 8A 和 8B 圖之後，可接續第 5C 至 5E 圖所示流程繼續進行，於此將不再重述後續流程。

第 9A 和 9B 圖係爲本揭露之編碼符號長度演算法及重送計數演算法之說明示意圖。如第 9A 圖所示，其說明編碼符號長度演算法的基礎理論，編碼符號長度演算法主要是收集每一個電表的傳輸限制，並計算出最合適的編碼符號長度。具體而言，要傳送檔案封包大小一般是以應用層（Application layer，AL）的傳送大小爲主，但若高級數據鏈路控制（High-Level Data Link Control，HDLC）層無法以應用層大小傳送，將會切割成更小長度的封包進行傳送，如圖所示，若單一編碼符號被分成四個部分傳送時，若其中有一個部分傳送失敗，則整個編碼符號是無法被還原的，因此，未避免前述情況發明，將會以韌體區塊大小或傳輸訊框大小兩者較小者爲編碼符號該被切割的長度大小。

下面爲本實施例的編碼符號長度演算法：

```
Procedure Calculate_E
for i = 1 to n do
  if i = 1 then
      E = (BS_i < HFS_i) ? (BS_i - ALH) : (HFS_i - HH));
  else
      min_E = (BS_i < HFS_i) ? (BS_i - ALH) : (HFS_i -
```

HH));

E = min(E, min_E);

end

return E;

於上述演算法中，BS_i 爲第 i 個電表的韌體區塊大小（位元組），HFS_i 爲第 i 個電表的 HDLC 層內支援的框大小（位元組），ALH 爲應用層標頭大小（位元組），HH 爲 HDLC 層標頭大小（位元組），E 爲編碼符號長度（位元組）。其中，因爲有 n 個電表所以要執行 n 次，在若 BS_i 小於 HFS_i 時則 E=BS_i-ALH，若 BS_i 大於 HFS_i 時則 E=HFS_i-HH，最後，用相同方式計算出 min_E，然後比較 E, min_E 的大小取最小的當成下一次的 E，在執行 n 次之後最小的就是 E。

如第 9B 圖所示，其說明重送計數演算法的理論，重送計數演算法主要用於計算重送時需送多少個編碼符號，若能越少者則能提高傳輸效率。如圖所示，資料集中器係與五個電表連接，在傳送一段時間後，每一個電表接收後所缺的編碼符號不相同，因而可透過 1 和 0 的位元串（bit-string）來表示收到與否，亦即電表會將接收編碼符號情況回報給資料集中器，如圖左邊所示，計算每一個位元串中 0 的個數（即表示未收到編碼符號），取該些位元串中 0 的個數的最大值，於此實施例爲 2，即爲下次傳送新的編碼符號所需個數。由此可知，在韌體更新過程中，資料集中器無需要知道每一個電表已收到哪些編碼符號或者

缺少那一個編碼符號，而是由是否收到足夠編碼符號可供還原該韌體映像檔即可，亦即電表僅要收到足夠的編碼符號即可還原出原始的韌體映像檔。

下面爲本實施例的重送計數演算法：

```
Procedure Calculate_R
  R = 0;
  s = ceil(L/E);
  for each i = 1 to n do
      R = max( R, s - popcount(TS_i));
  end
  return R
```

於上述演算法中，其中，TS_i 爲第 i 個電表中編碼符號接收狀態的位元串，L 爲韌體映像檔長度（位元組），E 爲編碼符號長度（位元組），R 爲重送編碼符號的數量。其中，韌體映像檔被切割成 s 個韌體區塊，總數 s 扣除幾個 1 後就表示有幾個 block 還沒傳，同樣計算 n 次並取最大的 R 值，即是我們需要的。Popcount( ) 函數是用於計算一個位元串中有幾個 1。

綜上所述，本揭露提出一種先進讀表基礎建設中之韌體更新系統及其方法，用於改善先進讀表基礎建設中的韌體更新效率與安全。首先，本揭露透過廣播及多點傳送方式避免目前採用一對一傳輸方式所導致的效率不高問題，本揭露是利用一種編碼符號長度演算法，透過收集各電表可支援的傳輸大小以將韌體映像檔進行適當切割，藉此使

傳送達到最佳效率，且本揭露還利用 FEC 編碼技術提出一種重送計數演算法，以解決目前僅能將各電表所缺少之檔案分別進行重送之缺陷，另外，本揭露透過來源驗證及端對端安全驗證以確保所取得韌體其合法性，藉此達到有效率且安全的遠端韌體更新，不會因爲更新低效率而影響電表的讀表，也可提升韌體更新的正確性及安全性。

上述實施形態僅例示性說明本揭露之原理及其功效，而非用於限制本揭露。任何熟習此項技藝之人士均可在不違背本揭露之精神及範疇下，對上述實施形態進行修飾與改變。因此，本揭露之權利保護範圍，應如後述之申請專利範圍所列。

【符號說明】

1、2、6	先進讀表基礎建設中之韌體更新系統
10、20、60	遠端伺服器
101	資料庫
102、202、602	安全模組
11、21、61	資料集中器
111、211、611	驗證模組
212、604	FEC 編碼器
112、213、613	廣播模組
12、22、62	電表
121、221、621	FEC 解碼器
122、222、622	檢驗模組
201、601	韌體映像檔資料庫

203、603	控制模組
214、614	控制模組
215、615	傳輸模組
223、623	記憶體
224、624	傳輸模組

103年8月19日修正劃線頁(本)

第 102143193 號專利申請案
103 年 8 月 19 日修正替換頁

申請專利範圍

1. 一種先進讀表基礎建設中之韌體更新系統，係包括：

遠端伺服器，係包含用於儲存韌體映像檔之資料庫以及用於產生數位簽章資料和啓動碼之安全模組；

資料集中器，係連線至該遠端伺服器，包括：

驗證模組，係透過該數位簽章資料以驗證來自該遠端伺服器之韌體映像檔；及

廣播模組，係用於將該韌體映像檔所產生之複數個編碼符號中以超過一設定數量透過廣播方式進行發送，且依據該些編碼符號之被接收狀態得到最少重送內容，以於未被廣播之編碼符號中選擇符合該最少重送內容之數量並將其再次廣播；以及

至少一電表，各該電表係與該資料集中器連線以接收該被廣播之編碼符號，該電表包括：

FEC 解碼器，係用於解碼來自該資料集中器之多個被廣播之編碼符號，以透過該多個被廣播之編碼符號還原該韌體映像檔；及

檢驗模組，係用於確認該 FEC 解碼器所還原之韌體映像檔的完成度，且自該資料集中器取得來自該遠端伺服器之啓動碼，該啓動碼經檢驗後係用於驅動該電表進行韌體更新。

2. 如申請專利範圍第 1 項所述之先進讀表基礎建設中之韌體更新系統，其中，該廣播模組係比較該設定數量

與該電表所接收之編碼符號的數量，藉此得到該電表還原該韌體映像檔所需補足之編碼符號的數量，以作爲該最少重送內容。

3. 如申請專利範圍第 1 項所述之先進讀表基礎建設中之韌體更新系統，其中，該資料集中器更包括一 FEC 編碼器，該 FEC 編碼器係收集各該電表之韌體區塊大小及傳輸訊框大小以得到各該電表之傳輸限制，透過比對所有電表所能支援之傳輸限制得到該編碼符號之單元切割尺寸，並將該資料集中器所接收之韌體映像檔進行編碼以產生至少一符合該單元切割尺寸之該編碼符號。

4. 如申請專利範圍第 1 項所述之先進讀表基礎建設中之韌體更新系統，其中，該遠端伺服器更包括一 FEC 編碼器，係用於將該韌體映像檔以特定韌體區塊大小進行編碼以產生已編碼的韌體映像檔，並傳送至該資料集中器。

5. 一種先進讀表基礎建設中之韌體更新方法，係包括：

令資料集中器自遠端伺服器取得韌體映像檔，且透過來源認證機制確認該韌體映像檔的合法性；

令該資料集中器利用廣播方式將該韌體映像檔於編碼後所產生之至少一編碼符號以一設定數量發送至各該電表，且由各該電表所回傳之訊息計算出最少重送內容，由該資料集中器將未被廣播之編碼符號中選擇符合該最少重送內容之數量並再次廣播直到各該電

表已收集足夠之編碼符號並還原該韌體映像檔；

驗證該韌體映像檔的版本及完成度；以及

令各該電表取得啓動碼，且於確認該啓動碼的正確性後執行韌體更新。

6. 如申請專利範圍第 5 項所述之先進讀表基礎建設中之韌體更新方法，其中，該來源認證機制係透過非對稱式加密演算法以驗證該韌體映像檔的合法性。

7. 如申請專利範圍第 5 項所述之先進讀表基礎建設中之韌體更新方法，其中，該韌體映像檔之編碼包括令該資料集中器取得各該電表所支援之傳輸限制，並依據各該電表之傳輸限制透過編碼符號長度演算法將該韌體映像檔進行編碼以產生該至少一編碼符號，或者於該遠端伺服器中以預定之韌體區塊大小進行編碼以產生已編碼的韌體映像檔並傳送至該資料集中器作傳送。

8. 如申請專利範圍第 7 項所述之先進讀表基礎建設中之韌體更新方法，其中，各該電表之傳輸限制係包括各該電表所支援之該韌體區塊大小及該傳輸訊框大小，該資料集中器係以各該電表之傳輸限制來判斷該至少一編碼符號之單元切割尺寸。

9. 如申請專利範圍第 7 項所述之先進讀表基礎建設中之韌體更新方法，其中，該編碼符號長度演算法係收集各該電表所支援之該韌體區塊大小與該傳輸訊框大小以由兩者之中取得各該電表之傳輸限制，並比較自各

第 102143193 號專利申請案
103 年 8 月 19 日修正替換頁

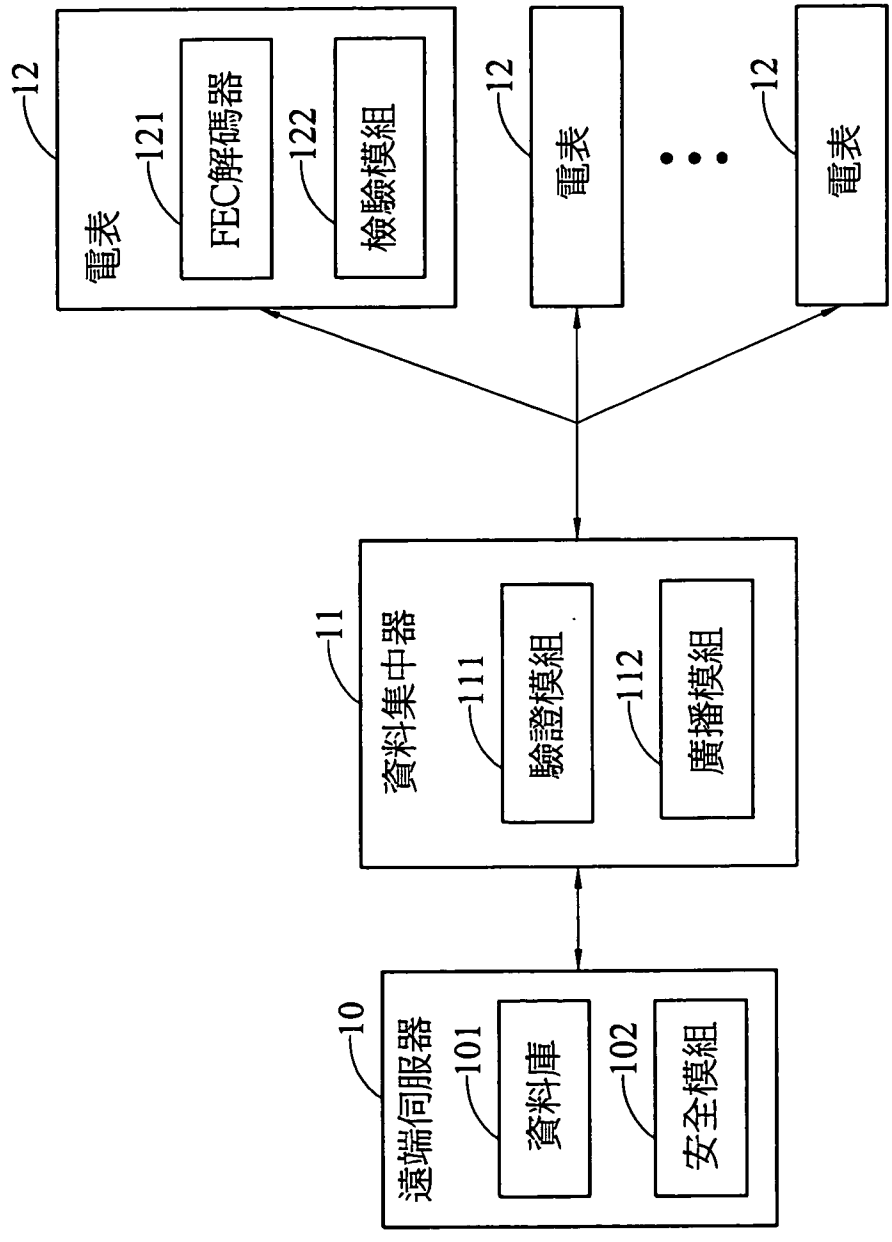
該電表之傳輸限制後以最小者以作爲該至少一編碼符號之單元切割尺寸。

10. 如申請專利範圍第 5 項所述之先進讀表基礎建設中之韌體更新方法，其中，各該電表所回傳之訊息係指各該電表對於該被廣播之編碼符號的接收狀態。

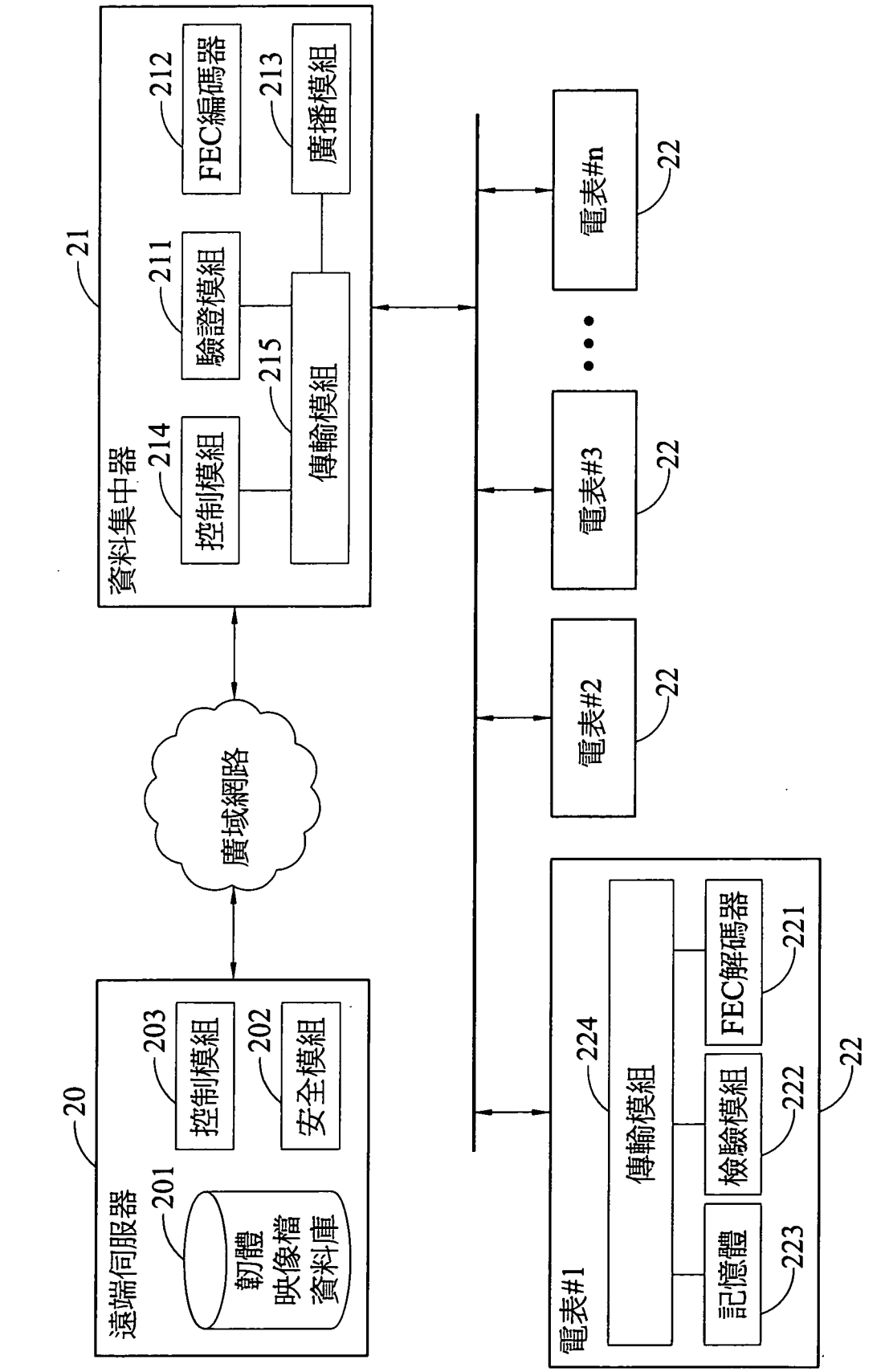
11. 如申請專利範圍第 5 項所述之先進讀表基礎建設中之韌體更新方法，其中，計算該最少重送內容包括利用重送計數演算法將各該電表所接收之編碼符號的數量與各該電表之一韌體區塊數量作比較，以計算出各該電表還原該韌體映像檔所需補足之編碼符號的數量，並取其最大者爲該最少重送內容。

12. 如申請專利範圍第 5 項所述之先進讀表基礎建設中之韌體更新方法，其中，各該電表取得該啓動碼並執行韌體更新包括令該資料集中器自該遠端伺服器取得各該電表之啓動碼並分別傳送至各該電表。

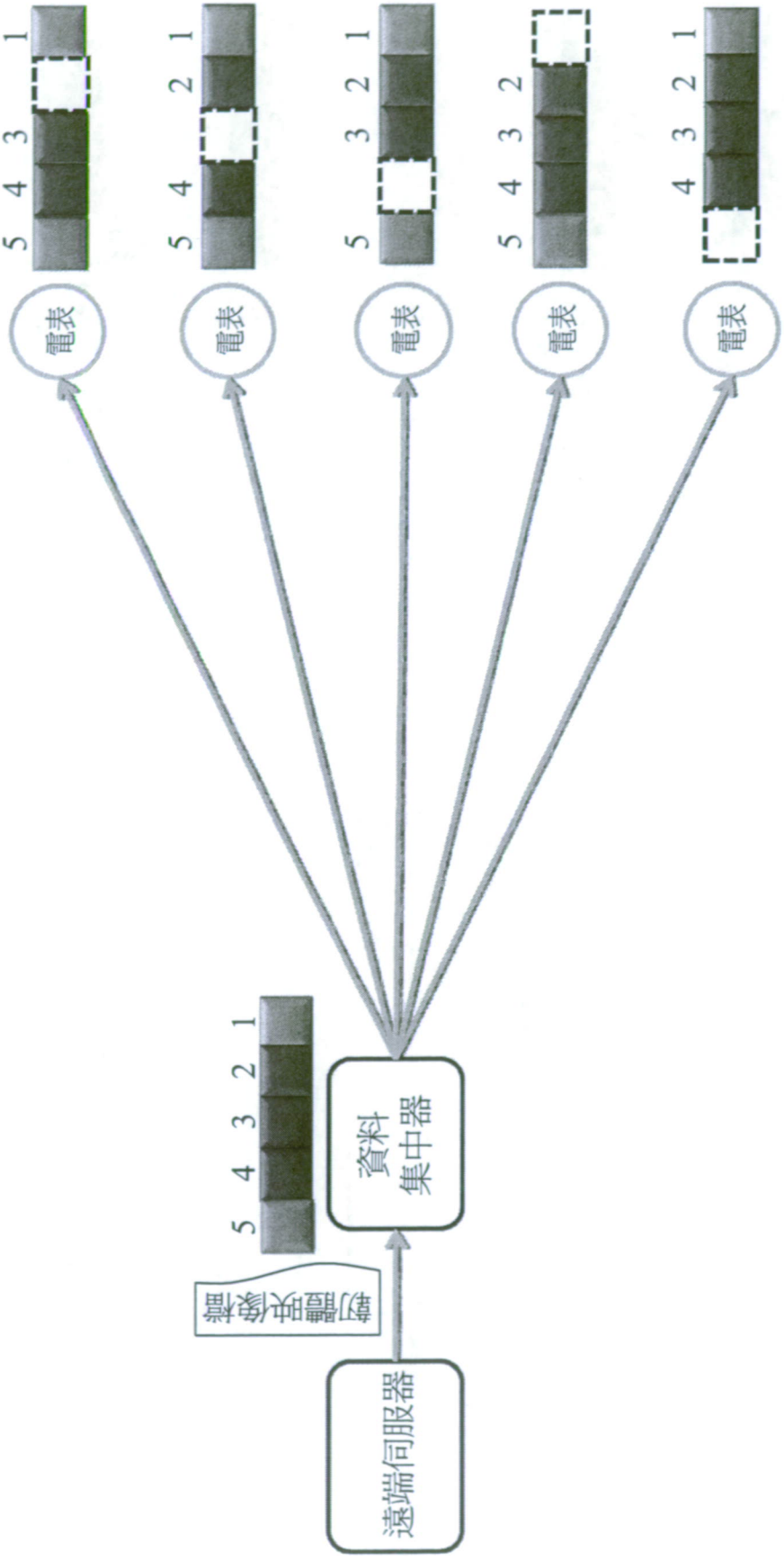
圖式


1
遠端伺服器
10
101
資料庫
102
安全模組
資料集中器
11
111
驗證模組
112
廣播模組
電表
12
121
FEC解碼器
122
檢驗模組
電表
12
電表
12

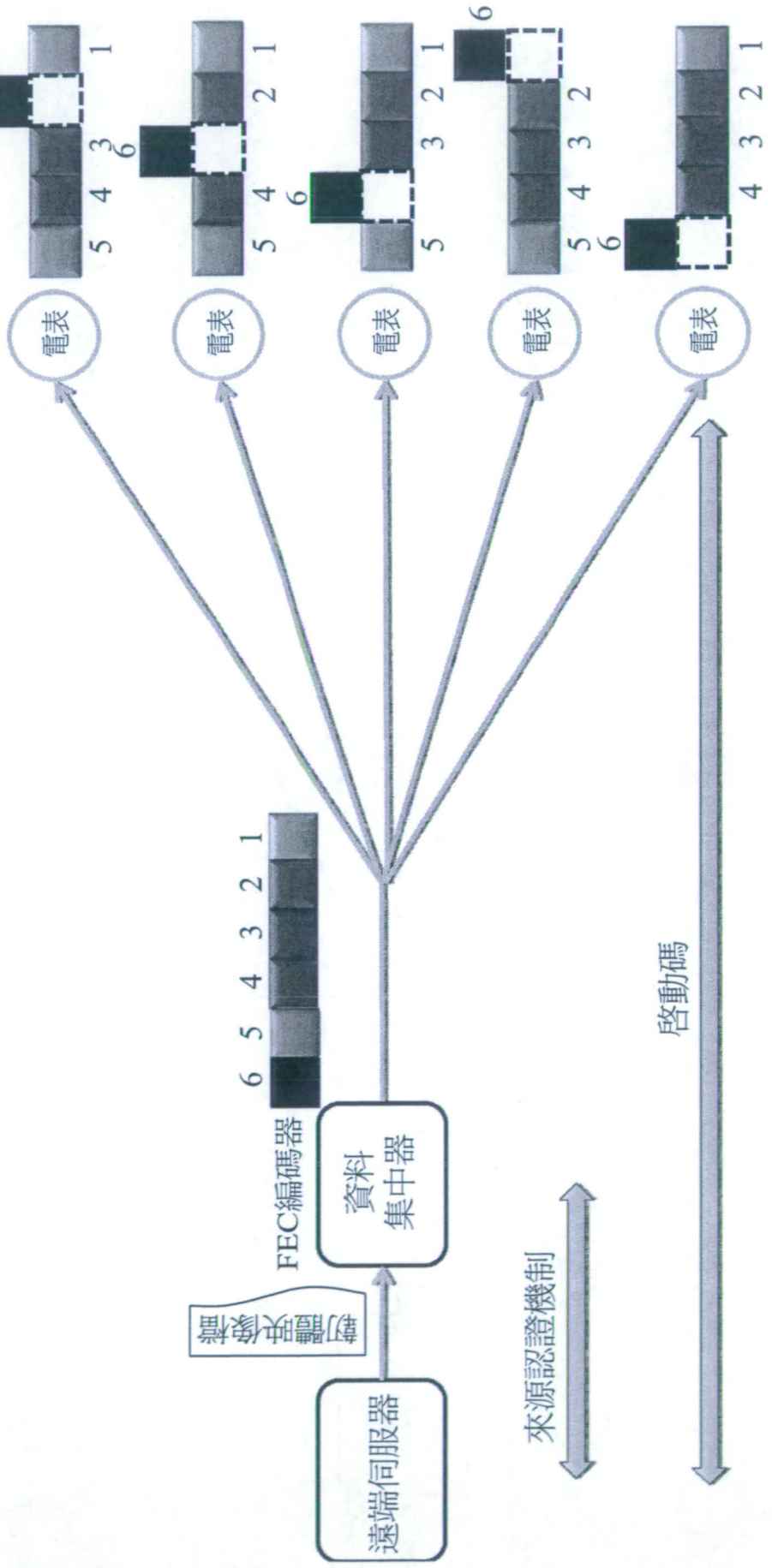
第1圖


2
20
遠端伺服器
201
韌體
映像檔
資料庫
203
控制模組
202
安全模組
廣域網路
21
資料集中器
214
控制模組
211
驗證模組
215
傳輸模組
212
FEC編碼器
213
廣播模組
電表#1
224
傳輸模組
223
記憶體
222
檢驗模組
221
FEC解碼器
22
電表#2
22
電表#3
22
電表#n
22

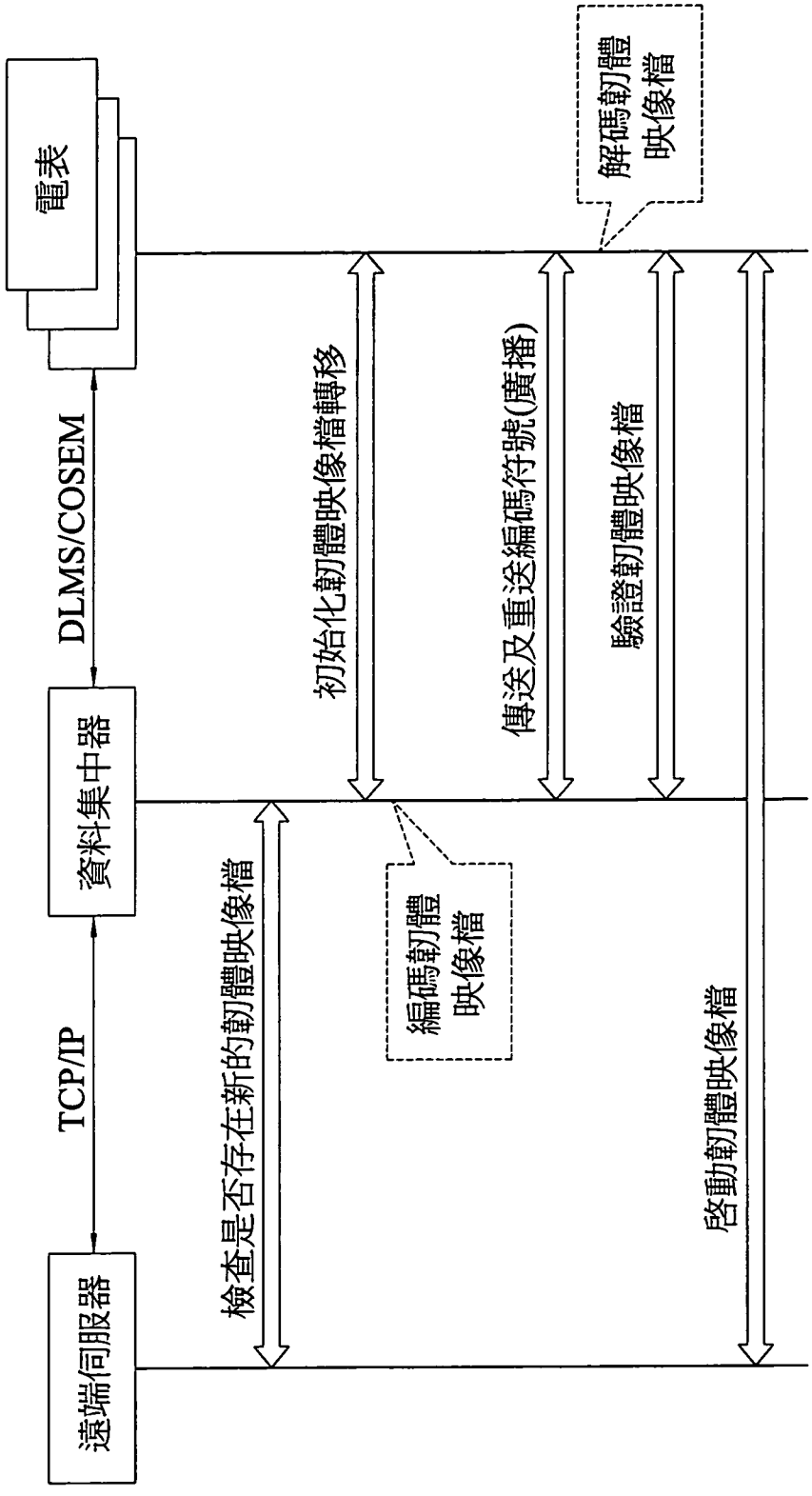
第2圖



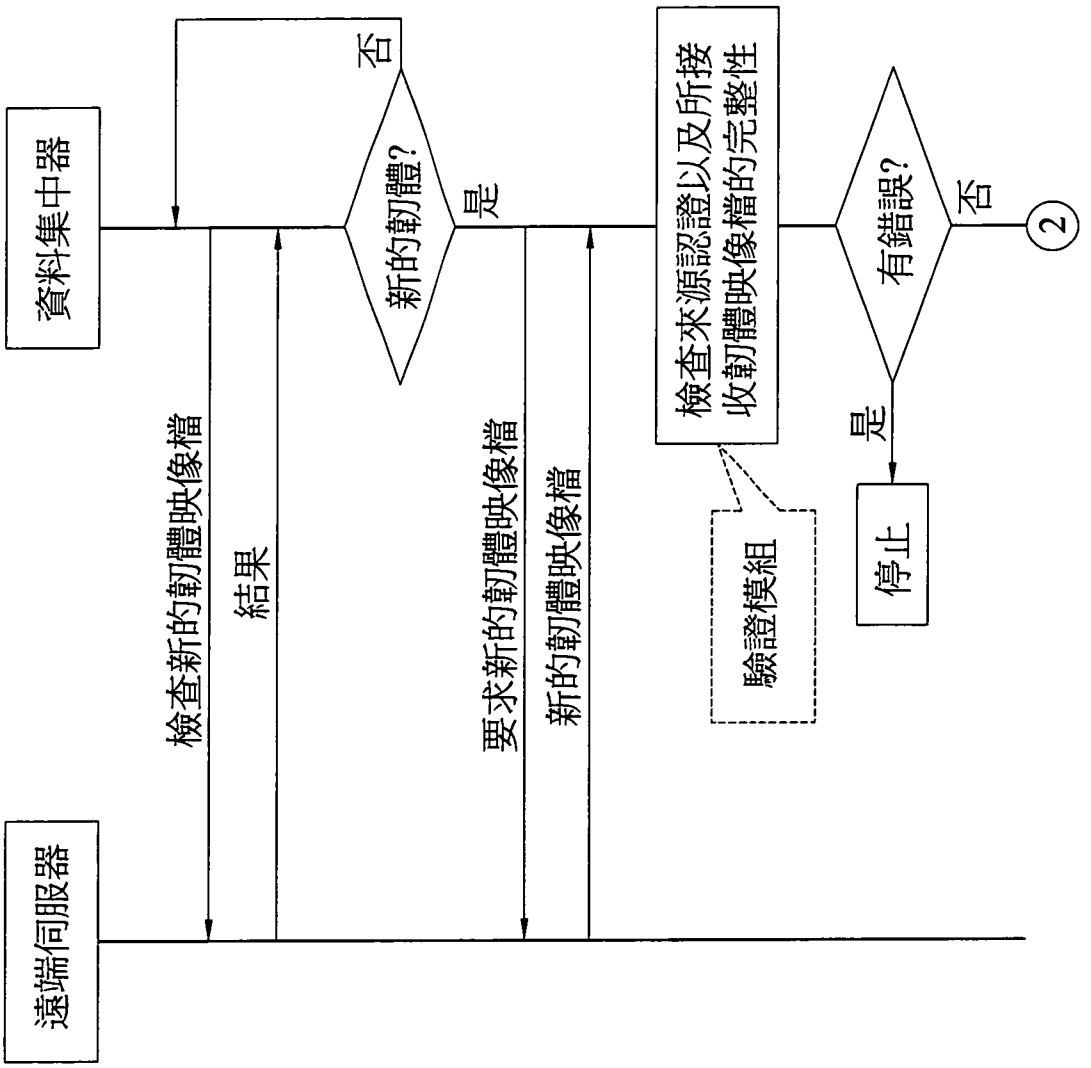
第3A圖



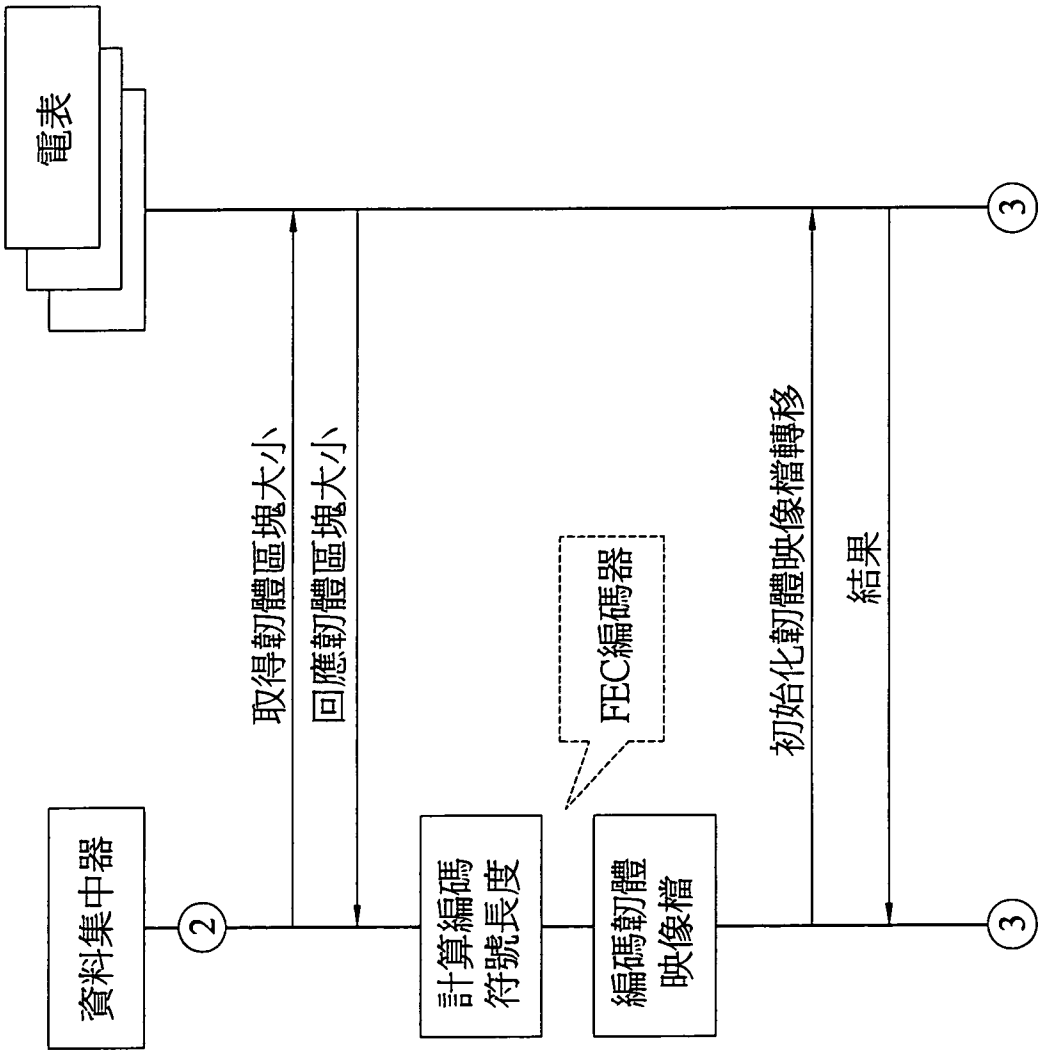
第3B圖


電表
DLMS/COSEM
資料集中器
TCP/IP
遠端伺服器
初始化韌體映像檔轉移
傳送及重送編碼符號(廣播)
驗證韌體映像檔
啓動韌體映像檔
檢查是否存在新的韌體映像檔
編碼韌體
映像檔
解碼韌體
映像檔

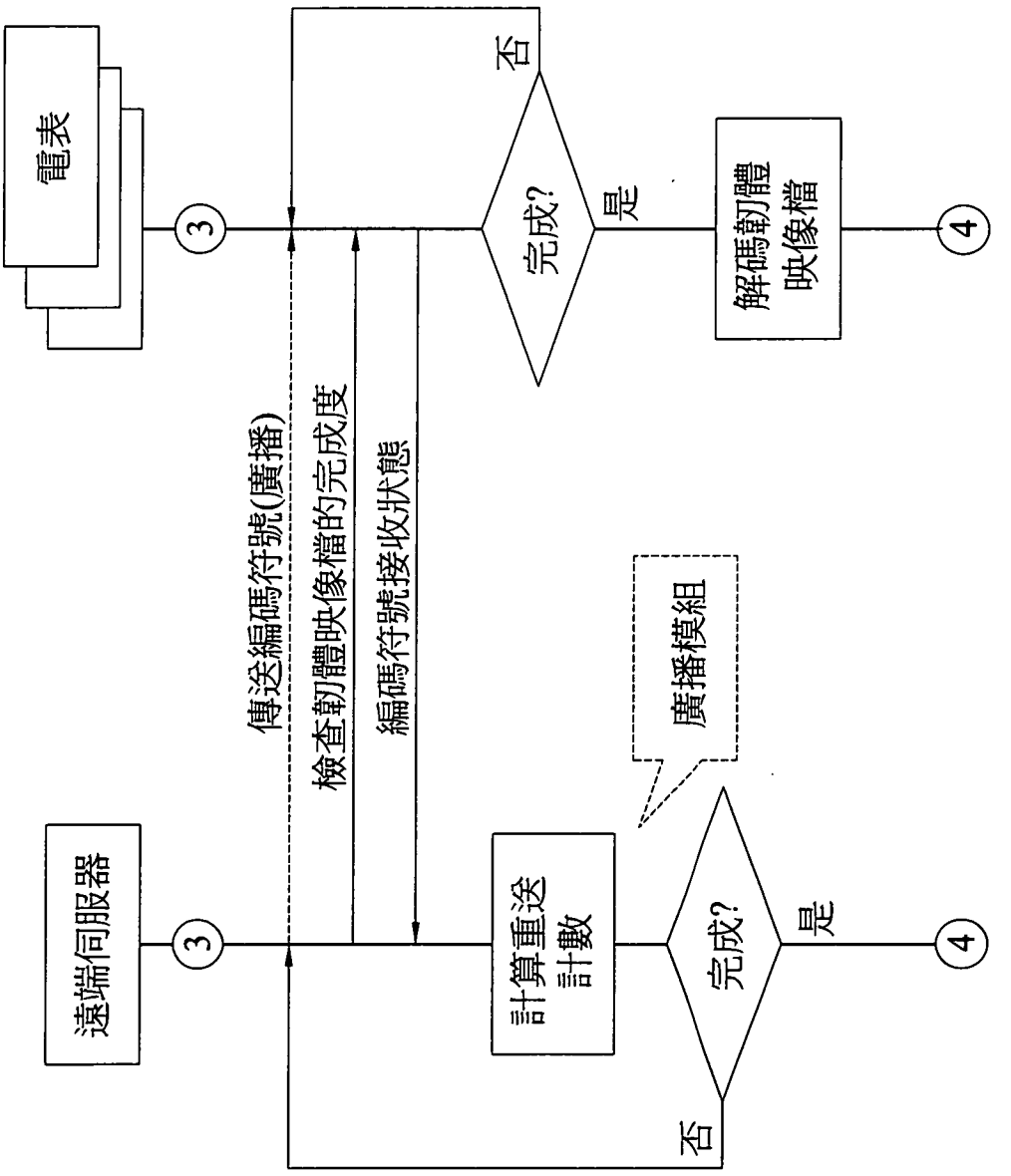
第4圖


資料集中器
遠端伺服器
檢查新的韌體映像檔
結果
新的韌體?
否
是
要求新的韌體映像檔
新的韌體映像檔
檢查來源認證以及所接收韌體映像檔的完整性
驗證模組
有錯誤?
是
否
②
停止

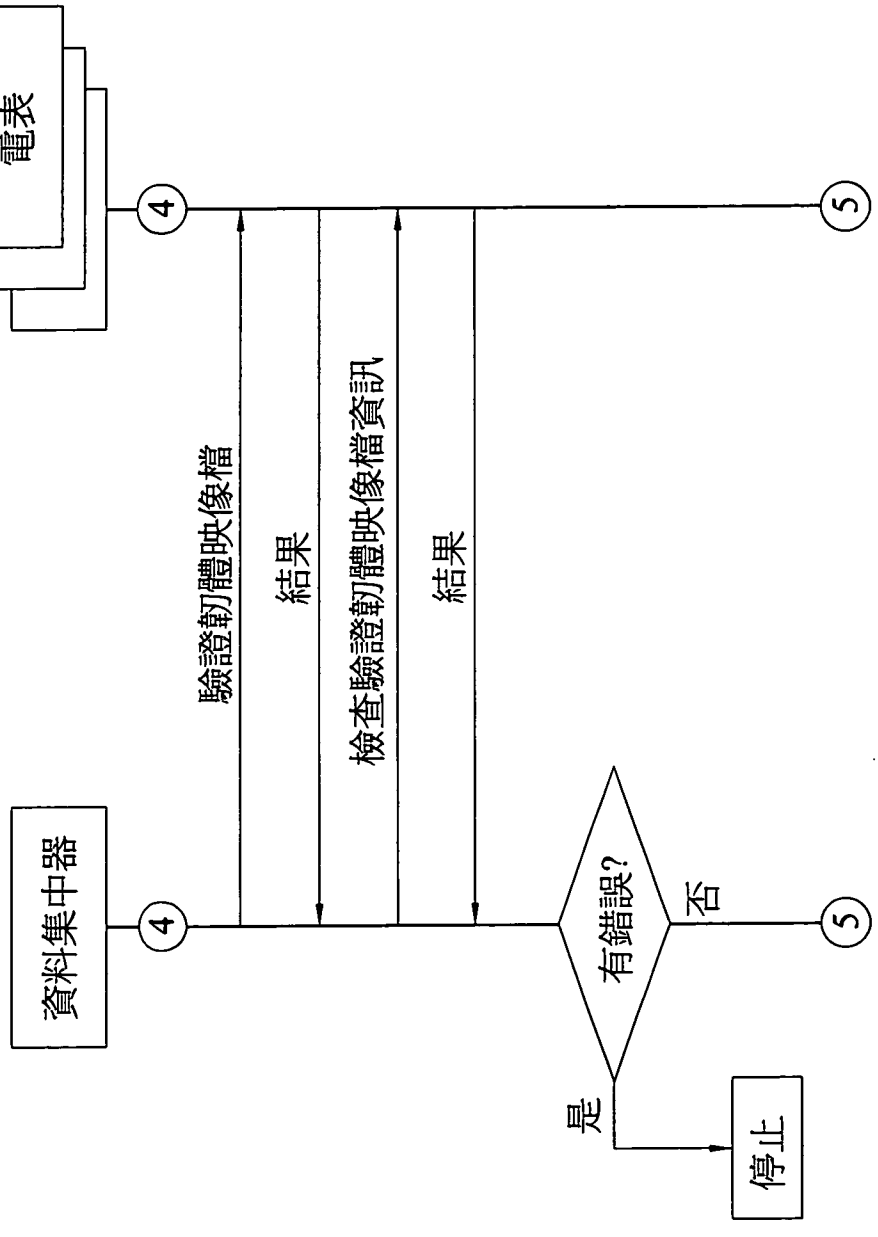
第5A圖


電表
資料集中器
②
取得韌體區塊大小
回應韌體區塊大小
計算編碼符號長度
FEC編碼器
編碼韌體映像檔
初始化韌體映像檔轉移
結果
③
③

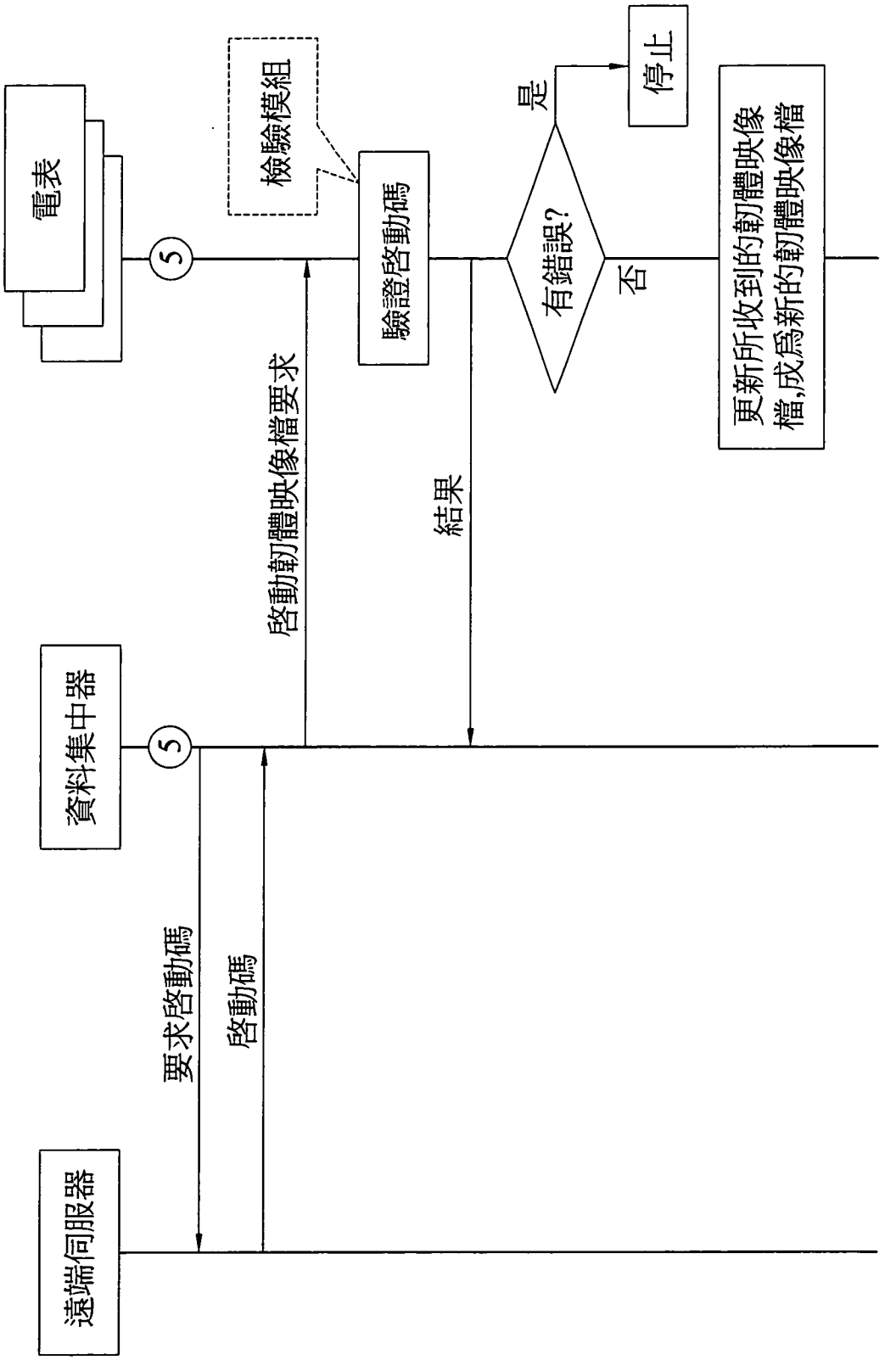
第5B圖


電表
遠端伺服器
3
3
傳送編碼符號(廣播)
檢查韌體映像檔的完成度
編碼符號接收狀態
計算重送計數
廣播模組
完成?
否
是
完成?
否
是
解碼韌體映像檔
4
4

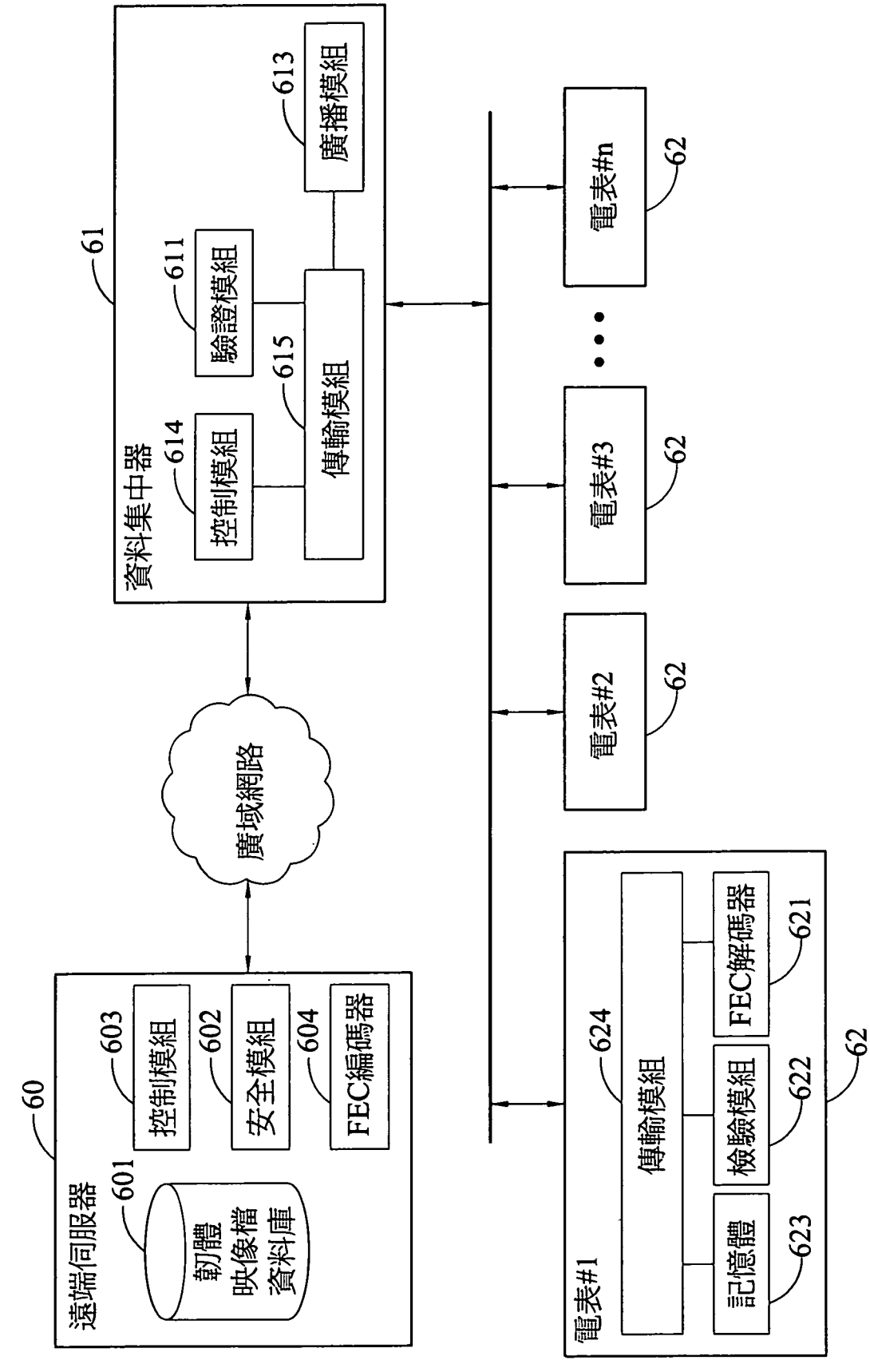
第5C圖



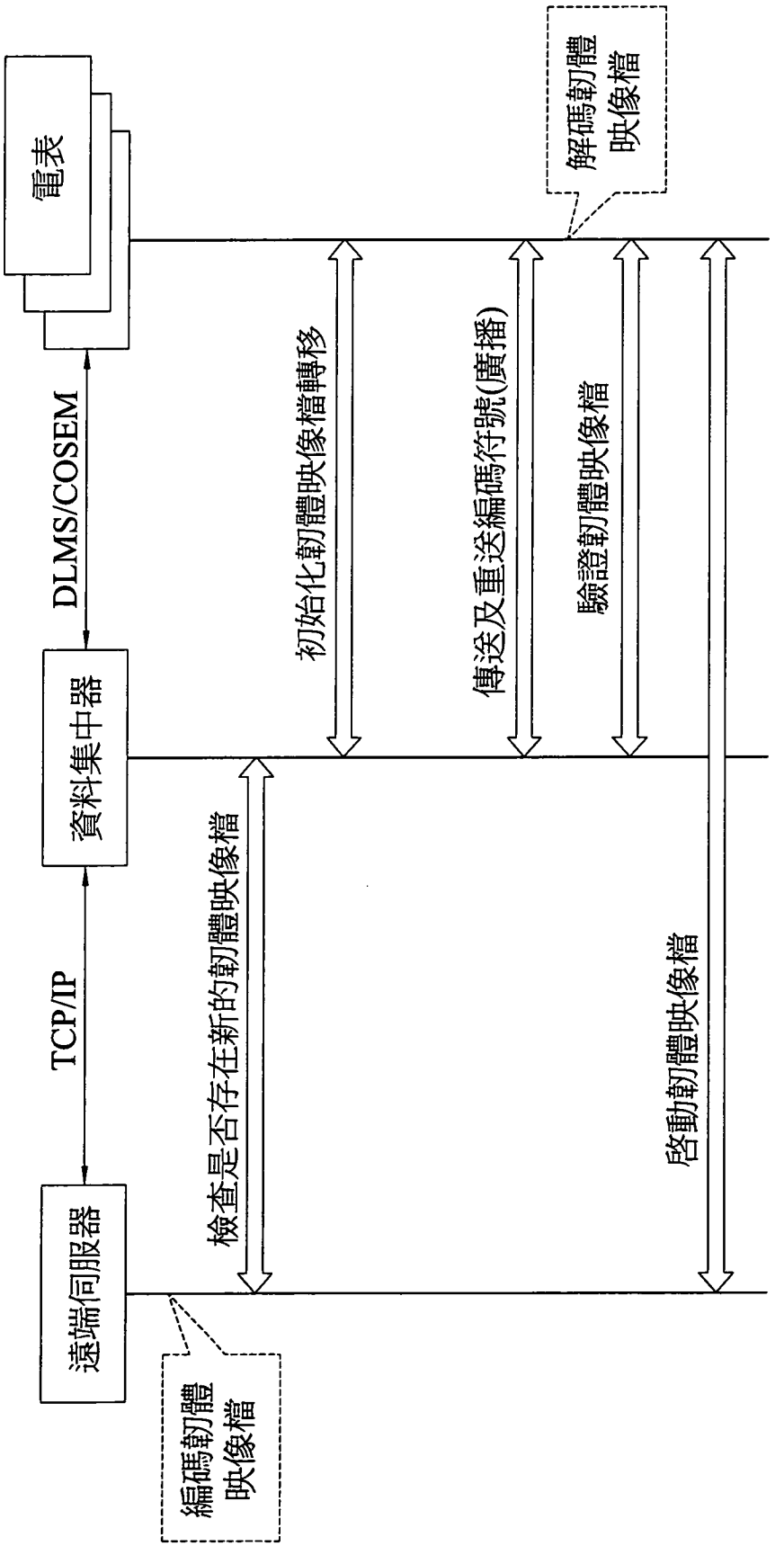
第5D圖


遠端伺服器
資料集中器
電表
5
5
要求啓動碼
啓動碼
啓動韌體映像檔要求
結果
檢驗模組
驗證啓動碼
有錯誤?
是
停止
否
更新所收到的韌體映像檔,成爲新的韌體映像檔

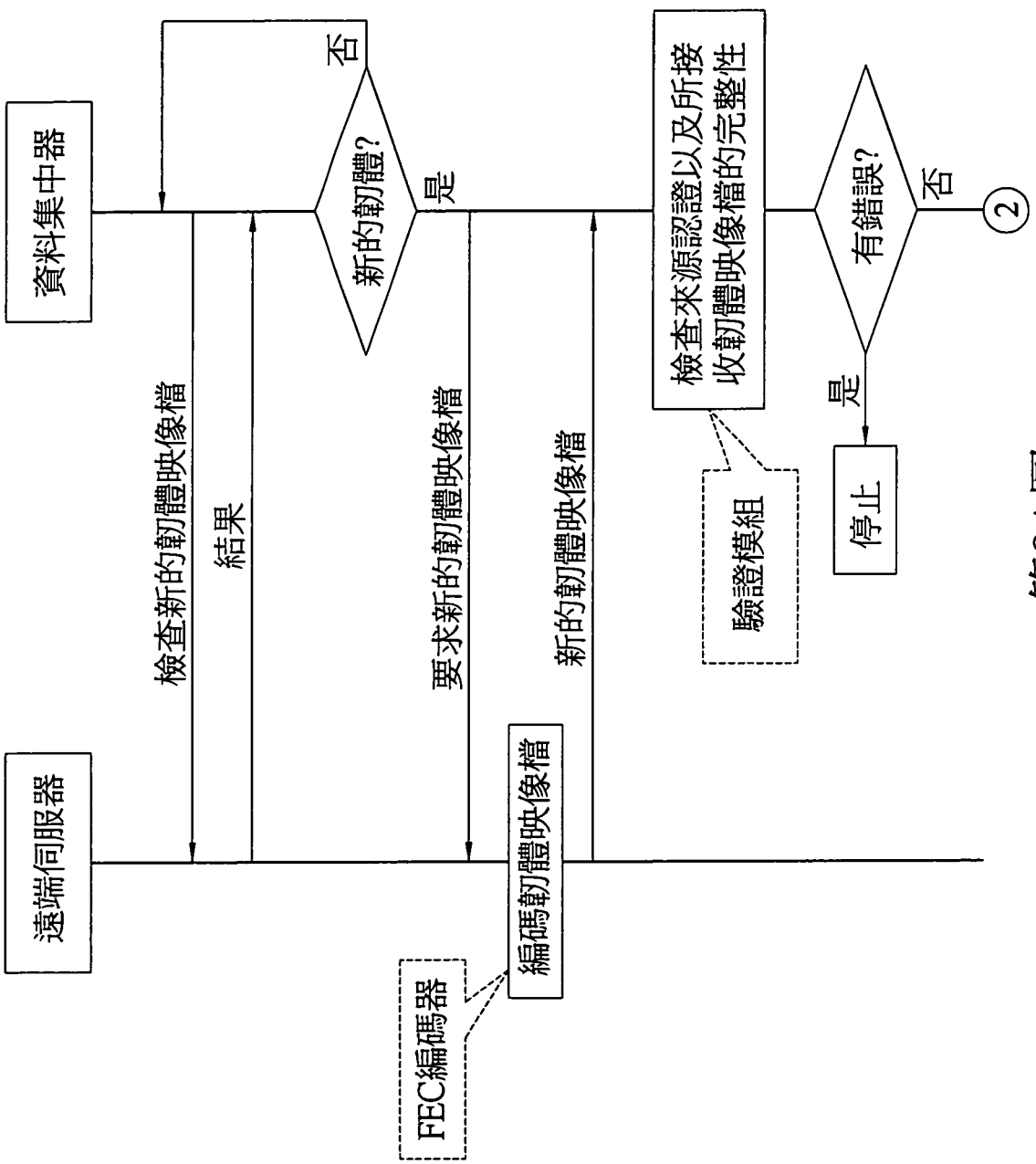
第5E圖


6
遠端伺服器
60
601
韌體映像檔資料庫
603
控制模組
602
安全模組
604
FEC編碼器
廣域網路
資料集中器
61
614
控制模組
611
驗證模組
615
傳輸模組
613
廣播模組
電表#1
62
624
傳輸模組
622
檢驗模組
623
記憶體
621
FEC解碼器
電表#2
62
電表#3
62
電表#n
62

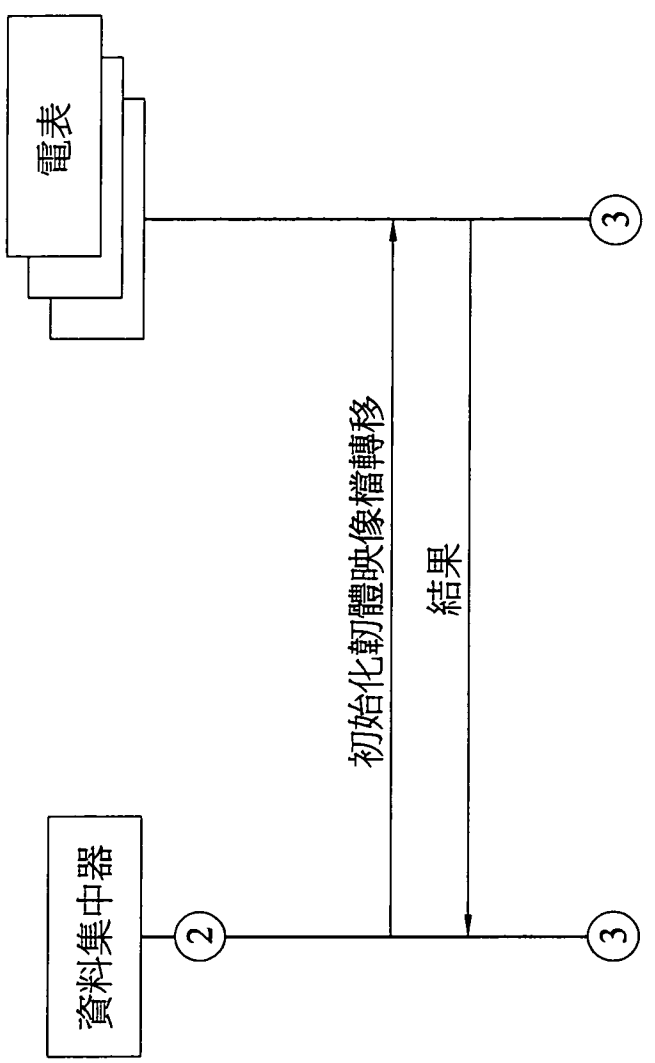
第6圖


電表
DLMS/COSEM
資料集中器
TCP/IP
遠端伺服器
編碼韌體映像檔
檢查是否存在新的韌體映像檔
初始化韌體映像檔轉移
傳送及重送編碼符號(廣播)
驗證韌體映像檔
啓動韌體映像檔
解碼韌體映像檔

第7圖


遠端伺服器
資料集中器
檢查新的韌體映像檔
結果
新的韌體?
否
是
要求新的韌體映像檔
編碼韌體映像檔
新的韌體映像檔
FEC編碼器
檢查來源認證以及所接收韌體映像檔的完整性
驗證模組
有錯誤?
否
是
停止
②

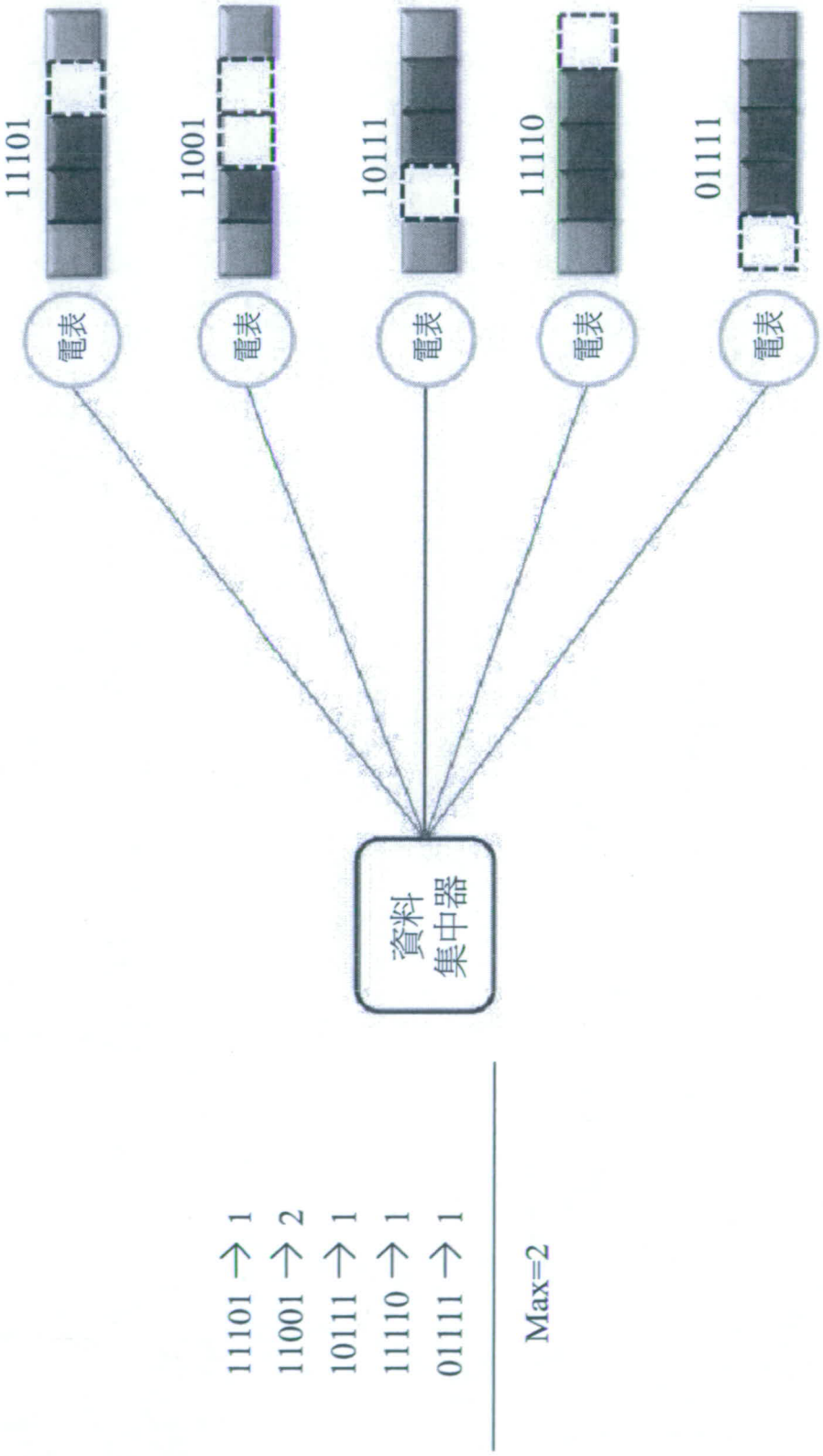
第8A圖



第8B圖

AL
HDLC
只考慮韌體區塊大小
編碼符號大小等同最大訊框
編碼符號
Encoding symbol
接收編碼符號失敗
傳送失敗的訊框

第9A圖


11101
11001
10111
11110
01111
電表
電表
電表
電表
電表
資料
集中器
11101 → 1
11001 → 2
10111 → 1
11110 → 1
01111 → 1
Max=2

第9B圖