201528029

(19)中華民國智慧財產局

(12)發明說明書公開本 (11)公開編號：TW 201528029 A

(43)公開日： 中華民國 104 (2015) 年 07 月 16 日

(21)申請案號：103131972 (22)申請日： 中華民國 103 (2014) 年 09 月 16 日

(51)Int. Cl.： *G06F21/32 (2013.01)* *G06F21/60 (2013.01)*

(30)優先權：2013/09/16 美國 14/028,236

(71)申請人：安訊士有限公司 (瑞典) AXIS AB (SE)
瑞典

(72)發明人：布魯斯 馬西亞斯 BRUCE, MATHIAS (SE)；強漢森 馬爾庫斯 JOHANSSON, MARCUS (SE)

(74)代理人：陳長文

申請實體審查：無 申請專利範圍項數：15 項 圖式數：13 共 59 頁

(54)名稱

由控制器裝置執行的方法及控制器裝置

METHOD PERFORMED BY A CONTROLLER DEVICE AND A CONTROLLER DEVICE

(57)摘要

一種控制器裝置可對應於一分散實體進入控制系統中之一實體進入控制器。該控制器裝置可包含邏輯(210)，該邏輯(210)經組態以獲得對包含複數個控制器裝置(115)之進入控制資訊之一全域資料庫(354)之存取。該邏輯可進一步經組態以自該全域資料庫導出一區域進入規則表(356)，其中該區域進入規則表(356)使得使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；及自該全域資料庫(354)導出一區域憑證表(358)，其中該區域憑證表(358)使經雜湊憑證與使用者相關，其中該區域憑證表(358)針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該控制器裝置中。

A controller device may correspond to a physical access controller in a distributed physical access control system. The controller device may include logic (210) configured to obtain access to a global database (354) that include access control information for a plurality of controller devices (115). The logic may be further configured to derive a local access rules table (356) from the global database, wherein the local access rules table (356) relates users to access rules, and wherein the local access rules table is encrypted with a local access rules key; and derive a local credentials table (358) from the global database (354) , wherein the local credentials table (358) relates hashed credentials to users, wherein the local credentials table (358) stores, for a user, the local access rules key encrypted with unhashed credentials associated with the user, wherein the unhashed credentials are not stored in the controller device.

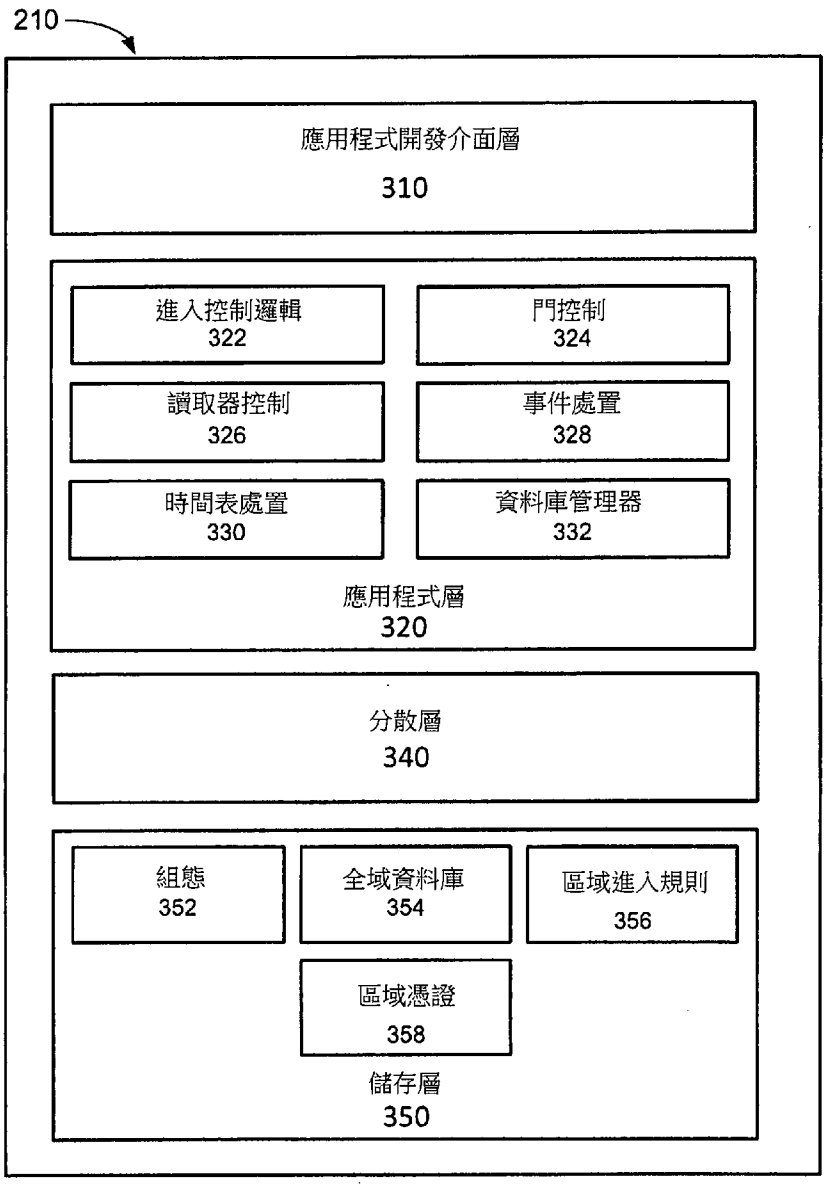

圖 3B

210・・・控制器

310・・・應用程式開發介面層

320・・・應用程式層

322・・・進入控制邏輯應用程式/進入控制邏輯

324・・・門控制應用程式/門控制邏輯應用程式

326・・・讀取器控制應用程式

328・・・事件處置應用程式

330・・・時間表處置應用程式

332・・・資料庫管理器應用程式

340・・・分散層

350・・・儲存層

352・・・組態資料庫

354・・・全域資料庫

356・・・區域進入規則資料庫

358・・・區域憑證資料庫

201528029

發明摘要

※ 申請案號：103131972

※ 申請日：103.9.16　　※IPC 分類：G06F 21/32 (2006.01)、21/60 (2006.01)

【發明名稱】

由控制器裝置執行的方法及控制器裝置

METHOD PERFORMED BY A CONTROLLER DEVICE AND A CONTROLLER DEVICE

【中文】

一種控制器裝置可對應於一分散實體進入控制系統中之一實體進入控制器。該控制器裝置可包含邏輯(210)，該邏輯(210)經組態以獲得對包含複數個控制器裝置(115)之進入控制資訊之一全域資料庫(354)之存取。該邏輯可進一步經組態以自該全域資料庫導出一區域進入規則表(356)，其中該區域進入規則表(356)使得使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；及自該全域資料庫(354)導出一區域憑證表(358)，其中該區域憑證表(358)使經雜湊憑證與使用者相關，其中該區域憑證表(358)針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該控制器裝置中。

【英文】

A controller device may correspond to a physical access controller in a distributed physical access control system. The controller device may include logic (210) configured to obtain access to a global database (354) that include access control information for a plurality of controller devices (115). The logic may be further configured to derive a local access rules table (356) from the global database, wherein the local access rules table (356) relates users to access rules, and wherein the local access rules table is encrypted with a local access rules key; and derive a local credentials table (358) from the global database (354) , wherein the local credentials table (358) relates hashed credentials to users, wherein the local credentials table (358) stores, for a user, the local access rules key encrypted with unhashed credentials associated with the user, wherein the unhashed credentials are not stored in the controller device.

【代表圖】

【本案指定代表圖】：第（3B）圖。

【本代表圖之符號簡單說明】：

210	控制器
310	應用程式開發介面層
320	應用程式層
322	進入控制邏輯應用程式/進入控制邏輯
324	門控制應用程式/門控制邏輯應用程式
326	讀取器控制應用程式
328	事件處置應用程式
330	時間表處置應用程式
332	資料庫管理器應用程式
340	分散層
350	儲存層
352	組態資料庫
354	全域資料庫
356	區域進入規則資料庫
358	區域憑證資料庫

【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】

由控制器裝置執行的方法及控制器裝置

METHOD PERFORMED BY A CONTROLLER DEVICE AND A CONTROLLER DEVICE

【技術領域】

本發明一般而言係關於進入控制系統，且更具體而言係關於進入控制系統中之匿名進入控制決策。

【先前技術】

進入控制系統可用於控制對一設施之實體進入。一進入控制系統(以及其他類型之控制系統)可具有眾多控制器，每一控制器控制系統之一不同部分。每一控制器可儲存裝置特有資訊，諸如組態資訊、周邊裝置設定等等。

【發明內容】

根據一項態樣，一種由一控制器裝置執行之方法可包含：由該控制器裝置獲得對包含複數個控制器裝置之進入控制資訊之一全域資料庫之存取；由該控制器裝置自該全域資料庫導出一區域進入規則表，其中該區域進入規則表使使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；及由該控制器裝置自該全域資料庫導出一區域憑證表，其中該區域憑證表使經雜湊憑證與使用者相關，其中該區域憑證表針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該控制器裝置中。

另外，該方法可包含：自一讀取器裝置接收一憑證值；對該所

接收憑證值進行雜湊運算；判定該區域憑證表中是否存在針對該經雜湊憑證值之一憑證項目；及當該區域憑證表中存在針對該經雜湊憑證值之該憑證項目時，在該區域憑證表中識別與該經雜湊憑證值相關聯之一使用者。

另外，該方法可包含：使用該所接收憑證值解密與該憑證項目相關聯之該區域進入規則密鑰；使用該經解密區域進入規則密鑰解密該區域進入規則表；判定該經解密區域進入規則表中是否存在針對該使用者之一進入規則項目；及當該經解密區域進入規則表中存在針對該使用者之該進入規則項目時，基於該進入規則項目而執行與該使用者相關聯之一或多個進入規則。

另外，該控制器裝置可屬於包含該複數個控制器裝置之一分散系統，且該全域資料庫可對應於該分散系統中之一分散資料集。

另外，該方法可包含：自管理員裝置接收對該全域資料庫之一更新；將該更新分散至該複數個裝置中之其他者；及使用該所接收更新來更新該全域資料庫，其中該全域資料庫係在該複數個裝置中之該等其他者處更新的。

另外，該方法可包含儲存該全域資料庫；及使得該複數個控制器裝置能夠存取該全域資料庫。

另外，該控制器裝置可屬於包含該複數個控制器裝置之一分散系統，該全域資料庫可儲存於該複數個控制器裝置中之另一控制器裝置中，且獲得對該全域資料庫之存取可包含在該另一控制器裝置處存取該全域資料庫。

另外，該方法可包含：獲得對該全域資料庫之一更新；判定該更新與該區域進入規則表或該區域憑證表中之至少一者有關；及基於判定該更新與區域資料庫有關而使用該經更新全域資料庫更新該區域進入規則表或該區域憑證表中之該至少一者。

另外，該區域憑證表可使用一區域憑證密鑰加密，且該方法可進一步包含：使用該區域憑證密鑰解密該區域憑證表；更新該區域憑證表中之一經雜湊憑證值；自該經解密全域資料庫獲得一未加密區域進入規則密鑰；及藉助一未雜湊憑證值加密該區域進入規則密鑰，其中該經加密區域進入規則密鑰與該經雜湊憑證值相關聯。

另外，該方法可包含：自該經解密全域資料庫獲得一未加密區域進入規則密鑰；使用該所獲得之未加密區域進入規則密鑰解密該區域進入規則表；更新該區域進入規則表；及加密該經更新區域進入規則表。

另外，該區域進入規則表可使一特定進入位置與一特定使用者群組及與一特定進入規則集相關聯。

另外，該方法可包含：自該全域資料庫導出該複數個控制器裝置中之另一控制器裝置之一遠端區域進入規則表；自該全域資料庫導出該另一控制器裝置之一遠端區域憑證表；及使得該另一控制器裝置能夠存取該遠端區域進入規則表及該遠端區域憑證表。

另外，在該全域資料庫中一使用者可與一全域資料庫列編號相關聯，在該區域進入規則表中該使用者可與該全域資料庫列編號相關聯，且在該區域憑證表中該使用者可與該全域資料庫列編號相關聯。

另外，該控制器裝置可對應於一嵌入式系統。

另外，該複數個控制器裝置可對應於一分散實體進入控制系統，且該控制器裝置可對應於一實體進入控制單元。

根據另一態樣，一種控制器裝置可包含邏輯，該邏輯經組態以：獲得對包含複數個控制器裝置之進入控制資訊之一全域資料庫之存取；自該全域資料庫導出一區域進入規則表，其中該區域進入規則表使使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；及自該全域資料庫導出一區域憑證表，其中該

區域憑證表使經雜湊憑證與使用者相關，其中該區域憑證表針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該控制器裝置中。

另外，該邏輯可進一步經組態以：自一讀取器裝置接收一憑證值；對該所接收憑證值進行雜湊運算；判定該區域憑證表中是否存在針對該經雜湊憑證值之一憑證項目；及當該區域憑證表中存在針對該經雜湊憑證值之該憑證項目時，在該區域憑證表中識別與該經雜湊憑證值相關聯之一使用者。

另外，該憑證值可包含以下各項中之一或多者：一小鍵盤字元序列；自一鑰匙卡獲得之一值；自一虹膜掃描獲得之一特徵向量；自一話音樣本獲得之一特徵向量；或自一指紋掃描獲得之一特徵向量。

另外，該邏輯可進一步經組態以：使用該所接收憑證值解密與該憑證項目相關聯之該區域進入規則密鑰；使用該經解密區域進入規則密鑰解密該區域進入規則表；判定該經解密區域進入規則表中是否存在針對該使用者之一進入規則項目；及當該經解密區域進入規則表中存在針對該使用者之該進入規則項目時，基於該進入規則項目而執行與該使用者相關聯之一或多個進入規則。

另外，該控制器裝置可屬於包含該複數個控制器裝置之一分散系統，且該全域資料庫可對應於該分散系統中之一分散資料集。

另外，該邏輯可進一步經組態以：自管理員裝置接收對該全域資料庫之一更新；將該更新分散至該複數個裝置中之其他者；及使用該所接收更新來更新該全域資料庫，其中該全域資料庫係在該複數個裝置中之該等其他者處更新的。

另外，該邏輯可進一步經組態以：儲存該全域資料庫；及使得複數個其他控制器裝置能夠存取該全域資料庫。

另外，該控制器裝置可屬於包含複數個控制器裝置之一分散系

統，該全域資料庫可儲存於該複數個控制器裝置中之另一控制器裝置中，且該邏輯可進一步經組態以在該另一控制器裝置處存取該全域資料庫。

另外，該邏輯可進一步經組態以：自該全域資料庫導出另一控制器裝置之一遠端區域進入規則表；自該全域資料庫導出該另一控制器裝置之一遠端區域憑證表；及將該遠端區域進入規則表及該遠端區域憑證表提供至該另一控制器裝置。

另外，該複數個控制器裝置可對應於一分散實體進入控制系統，且該控制器裝置可對應於一實體進入控制單元。

根據又一態樣，一種分散系統可包含複數個實體進入控制裝置，其中該複數個實體進入控制裝置中之特定一者經組態以：獲得對包含複數個控制器裝置之進入控制資訊之一全域資料庫之存取；自該全域資料庫導出一區域進入規則表，其中該區域進入規則表使使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；及自該全域資料庫導出一區域憑證表，其中該區域憑證表使經雜湊憑證與使用者相關，其中該區域憑證表針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該複數個實體進入控制裝置中之該特定一者中。

【圖式簡單說明】

圖1係圖解說明根據本文中所描述之一實施例之一例示性環境之一方塊圖；

圖2係圖解說明圖1之一系統單元之例示性組件之一方塊圖；

圖3A及圖3B係圖解說明圖1之系統單元之例示性功能組件之方塊圖；

圖4A至圖4C係可儲存於圖3B之資料庫中之例示性資訊之圖式；

圖5係根據一或多項實施例用於自一全域資料庫導出區域資料庫之一流程圖；

圖6係根據一或多項實施例用於更新一全域資料庫之一流程圖；

圖7係根據一或多項實施例用於更新一區域進入規則表之一流程圖之一圖式；

圖8係根據一或多項實施例用於更新一區域憑證表之一流程圖之一圖式；

圖9係根據本文中所描述之一或多項實施方案用於使用一區域憑證表及一區域進入規則表之一流程圖；

圖10係圖解說明圖1之系統單元之一例示性實體佈局之一平面佈置圖；

圖11係圖解說明圖1之系統之一例示性實體佈局之一平面佈置圖；

圖12A至圖12D係根據一或多項實施例之全域資料庫之例示性實施方案；及

圖13A至圖13C係根據一或多項實施例之一例示性資料庫使用情境之圖式。

【實施方式】

以下詳細描述參考附圖。不同圖式中之相同元件符號識別相同或類似元件。

下文所描述之實施例係關於控制系統中之匿名資料庫。可維持一控制系統之一全域資料庫。該全域資料庫可包含使用者資訊，諸如一使用者之識別資訊。該使用者資訊可進一步包含使用者之憑證值。可使用一憑證值結合該控制系統之一特定控制器裝置來證實一使用者。舉例而言，該憑證值可儲存於該使用者之一進入卡中，且一讀取器裝置可掃描該進入卡以判定是否授予該使用者之進入。該全域資料

庫可進一步包含進入控制資訊，諸如基於諸如一天之時間、進入區等等參數而應授予哪些使用者進入。

可使用該全域資料庫來導出該控制系統中之一特定裝置之一匿名區域進入規則表及/或該特定裝置之一匿名區域憑證表。該區域進入規則表可使使用者或使用者群組與和該特定裝置有關之進入規則相關。該區域進入規則表可用一區域進入規則密鑰加密。本文中所使用之術語「密鑰」可指一加密/解密密鑰。該區域憑證表可使經雜湊憑證值與使用者相關且可針對每一使用者儲存該區域進入規則密鑰之一經加密版本，其中該區域進入規則密鑰係藉助該使用者之未雜湊憑證值加密的。該等未雜湊憑證值可不由特定裝置儲存且可由一讀取器裝置(例如，一進入讀卡器)在該使用者請求進入時獲得。「匿名」可指不包含一使用者之識別資訊(例如，使用者之名稱、員工編號等等)。此外，術語「資料庫」與「表」可互換使用。因此，區域進入規則表及區域憑證表可不包含任何個人使用者資訊，且因此，若一進入裝置之安全受到危害，則無法自進入裝置中之區域表獲得個人使用者資訊。

在某些實施方案中，該控制系統可包含一分散控制系統。一分散控制系統可包含一分散實體進入控制系統。一實體進入控制系統可包含一或多個進入控制單元，其中每一進入控制單元控制對一設施之一區之實體進入。舉例而言，一進入控制單元可自一使用者獲得憑證，且若該使用者之憑證被驗證，則可將一門鎖開鎖。在其他實施方案中，一分散控制系統可包含一分散建築物管理系統、一分散監視系統、一分散安全系統及/或另一類型之一分散控制系統。

在某些實施方案中，該全域資料庫可對應於一分散資料集，系統中之每一控制單元可儲存該分散全域資料庫之一區域複本，且每一控制單元可自分散全域資料庫之區域複本導出一區域進入規則表及/

或一區域憑證表。在其他實施方案中，某些控制單元可不包含分散全域資料庫之一複本。舉例而言，一高危險區中之一控制單元可不包含分散全域資料庫之一複本。而是，另一控制單元可導出高危險控制單元之一區域進入規則表及/或一區域憑證表且可將該區域進入規則表及/或該區域憑證表提供至該高危險控制單元。在又某些實施方案中，一單個控制單元可經指定以包含該全域資料庫，且其他控制單元可存取該全域資料庫以導出其各別區域進入規則表及/或區域憑證表。在又某些實施方案中，該全域資料庫可在控制系統之外，舉例而言，儲存在一管理裝置中。

在其他實施方案中，該控制系統可不對應於一分散系統。舉例而言，該控制系統可包含可以存取一全域資料庫之網路控制裝置群組，該全域資料庫可由該網路控制裝置中之一或多者或由另一裝置(諸如一管理裝置)儲存。

圖1係可在其中實施下文所描述之系統及/或方法之一例示性環境100之一方塊圖。如圖1中所展示，環境100包含一分散控制系統110(例如，一分散實體進入控制系統)、一網路120及一管理裝置130。

分散控制系統(DCS) 110可包含一分散計算系統，該分散計算系統包含系統單元115-A至115-N (統稱為「系統單元115」且個別地稱為「系統單元115」)。系統單元115可實施為一嵌入式系統。在某些實施方案中，系統單元115可包含一實體進入控制裝置。舉例而言，系統單元115可包含控制對一安全區(諸如一房間或一房間群組)之進入之一進入控制器。系統單元115可經由一讀取器裝置接收憑證(例如，進入卡憑證)，且判定該等憑證是否為真實的並與進入該安全區之授權相關聯。若如此，則該進入控制器可發出打開一門上之一鎖或執行與授予進入該安全區相關聯之其他操作之一命令。在其他實施方案中，系統單元115可包含一不同類型之安全裝置，諸如一監視裝

置、控制一機器之操作之一裝置等等。在其他實施方案中，系統單元115可包含另一類型之嵌入式系統。

DCS 110可包含一或多個分散資料集。一分散資料集包含與多個裝置相關聯之一資料集，其中在一項實施例中，多個裝置可彼此通信及協調以對該資料集做出改變。在一項實施例中，與分散資料集相關聯之每一裝置維持該分散資料集之一區域複本，且若該等裝置同意一改變，則將該改變複製至分散資料集之區域複本。在另一實施例中，舉例而言，並非所有裝置皆儲存分散資料集之一區域複本。

在某些實施例中，達成共識以便對分散資料集(例如，一基於共識之分散資料庫)做出一改變。在其他實施例中，可在無共識之情況下對分散資料集做出一改變。一分散資料集可與所有系統單元115相關聯或可與系統單元115之一子集相關聯。一系統單元115可提議對一基於共識之分散資料集之一改變。若與分散資料集相關聯之法定數之系統單元115接受了改變，則可達成一共識，且可將改變傳播至每一相關聯系統單元115中之分散資料集之每一區域複本。因此，若法定數之相關聯系統單元115投票贊成分散資料集之一改變，則可達成關於該改變之一共識。一法定數可對應於相關聯系統單元115之最小大多數。因此，若一分散資料集與N個系統單元115相關聯，則在N/2+1個相關聯系統單元115投票贊成改變之情況下(若N係一偶數)或在(N-1)/2+1個相關聯系統單元115投票贊成改變之情況下(若N係一奇數)，可達到一法定數。需要一最小大多數達到一法定數可確保在考量兩個衝突提議時，至少一個系統單元115接收到兩個提議且選擇該等提議中之一者以達成共識。

一基於共識之分散資料集可確保與分散資料集相關聯之任何系統單元115包含由該分散資料集管理之資訊(例如，在一項實施例中，所有資訊)。舉例而言，一分散資料集可包含進入規則，且該等進入

規則可用於與該分散資料集相關聯之任何系統單元115。因此，由於一或多個分散資料集，在一項實施例中，DCS 110可對應於不具有中央控制裝置(諸如一伺服器裝置)之一非集中式系統。在其他實施例中，DCS 110可包含一非集中式系統及一中央控制裝置(諸如一伺服器裝置)兩者。對DCS 110之改變可在任何系統單元115處組態，且若改變與一分散資料集相關聯，則可將該改變傳播至與該分散資料集相關聯之其他系統單元115。此外，DCS 110可相對於裝置失效展現穩健性，此乃因可避免一單個失效點。舉例而言，若一特定系統單元115失效，則其他系統單元115可繼續操作而不會丟失資料(或使資料丟失最小化)。此外，可動態地改變DCS 110。舉例而言，可在任何時間添加應用程式且可視需要將新資料集儲存於系統單元115中。

DCS 110亦可包含非分散之資料集。作為一實例，一第一系統單元115可包含不包含於任何其他系統單元115中之一區域資料集。作為另一實例，一第一系統單元115可包含以一非分散方式複製至一第二系統單元115 (諸如藉由鏡射)之一區域資料集。作為又一實例，一第一系統單元115可包含一區域資料集之一第一版本且一第二系統單元115可包含區域資料集之一第二版本，其中第一系統單元115維持區域資料集之第一版本且第二系統單元115維持區域資料集之第二版本。在又一實例中，一第一系統單元115可自一分散資料集導出一第一區域資料集且一第二系統單元115可自分散資料集導出一第二區域資料集，其中該第一區域資料集不同於該第二區域資料集。

網路120可使得系統單元115能夠彼此通信及/或可使得管理裝置130能夠與特定系統單元115通信。網路120可包含一或多個電路交換網路及/或封包交換網路。舉例而言，網路120可包含一區域網路(LAN)、一廣域網路(WAN)、一都會區域網路(MAN)、一公共交換電話網路(PSTN)、一臨機操作網路、一內部網路、網際網路、一基於光

纖之網路、一無線網路及/或此等或其他類型網路之一組合。

管理裝置130可使得一管理員能夠連接至一特定系統單元115以便組態DCS 110、改變DCS 110之一組態、自DCS 110接收資訊及/或以其他方式管理DCS 110。管理裝置130可包含經組態以與一系統單元115通信之任何裝置。舉例而言，管理裝置130可包含一可攜式通信裝置(例如，一行動電話、一智慧型電話、一平板電話裝置、一全球定位系統(GPS)裝置及/或另一類型之無線裝置)；一個人電腦或工作站；一伺服器裝置；一膝上型電腦；平板電腦或另一類型之可攜式電腦；及/或具有通信能力之任何類型之裝置。

雖然圖1展示環境100之例示性組件，但在其他實施方案中，環境100相比圖1中所繪示之組件可包含更少之組件、不同之組件、不同配置之組件或額外組件。另外或另一選擇係，環境100中之任一裝置(或任何裝置群組)可執行描述為由環境100中之一或多個其他裝置執行之功能。舉例而言，在某些實施方案中，系統單元115可包含一輸入及/或輸出裝置(例如，鍵盤/小鍵盤及顯示器、觸控螢幕等等)，且可不需要管理裝置130。

圖2係圖解說明一系統單元115之例示性組件之一方塊圖。如圖2中所展示，系統單元115可包含一控制器210及一或多個周邊裝置230。控制器210可控制系統單元115之操作，可與其他系統單元115通信，可與管理裝置130通信，及/或可控制周邊裝置230。控制器210可包含一匯流排212、一處理器214、一記憶體216、一網路介面218、一周邊介面220及一外殼222。

匯流排212可包含准許控制器210之組件當中之通信之一路徑。處理器214可包含任何類型之單核心處理器、多核心處理器、微處理器、基於鎖存器之處理器及/或解譯並執行指令之處理邏輯(或處理器、微處理器及/或處理邏輯之族群)。在其他實施例中，處理器214

可包含一特殊應用積體電路(ASIC)、一場可程式化閘陣列(FPGA)及/或另一類型之積體電路或處理邏輯。

記憶體216可包含可儲存供由處理器214執行之資訊及/或指令之任何類型之動態儲存裝置，及/或可儲存供由處理器214使用之資訊之任何類型之非揮發性儲存裝置。舉例而言，記憶體216可包含一隨機存取記憶體(RAM)或另一類型之動態儲存裝置、一唯讀記憶體(ROM)裝置或另一類型之靜態儲存裝置、一內容可定址記憶體(CAM)、一磁性及/或光學記錄記憶體裝置及其對應磁碟機(例如，一硬碟機、光學磁碟機等等)及/或一可抽換形式之記憶體，諸如一快閃記憶體。

網路介面218可包含一收發器(例如，一傳輸器及/或一接收器)，該收發器使得控制器210能夠經由有線通信鏈路(例如，導電線、雙絞線纜線、同軸纜線、傳輸線、光纖纜線及/或波導等等)、無線通信鏈路(例如，射頻(RF)、紅外線及/或視覺光學器件等等)或無線與有線通信鏈路之一組合與其他裝置及/或系統通信(例如，傳輸及/或接收資料)。網路介面218可包含將基頻信號轉換為RF信號之一傳輸器及/或將RF信號轉換為基頻信號之一接收器。網路介面218可耦合至用於傳輸及接收RF信號之一天線。

網路介面218可包含一邏輯組件，該邏輯組件包含輸入及/或輸出埠、輸入及/或輸出系統及/或促進將資料傳輸至其他裝置之其他輸入及輸出組件。舉例而言，網路介面218可包含用於有線通信之一網路介面卡(例如，乙太網路卡)及/或用於無線通信之一無線網路介面(例如，一WiFi)卡。網路介面218亦可包含用於經由一纜線通信之一通用串列匯流排(USB)埠、一Bluetooth™無線介面、一射頻識別(RFID)介面、一近場通信(NFC)無線介面及/或將資料自一種形式轉換為另一形式之任何其他類型之介面。

周邊介面220可經組態以與一或多個周邊裝置230通信。舉例而

言，周邊介面220可包含一或多個邏輯組件，該邏輯組件包含輸入及/或輸出埠、輸入及/或輸出系統及/或促進將資料傳輸至周邊裝置230之其他輸入及輸出組件。作為一實例，周邊介面220可使用一串列周邊介面匯流排協定(諸如一韋根(Wiegand)協定、一RS-485協定及/或另一類型之協定)與周邊裝置通信。作為另一實例，周邊介面220可使用一不同類型之協定。在一項實施例中，網路介面218亦可充當用於將周邊裝置230耦合至控制器210之一周邊介面。

外殼222可封圍控制器210之組件且可保護控制器210之組件免受環境影響。在一項實施例中，外殼222可包含周邊裝置230中之一或多者。在另一實施例中，外殼222可包含管理裝置130。外殼222可在具有一個以上系統單元115及/或控制器210之一系統中界定一個系統單元115及/或控制器210與其他系統單元115及/或控制器210之邊界。

如下文所描述，控制器210可執行與管理一分散系統中之資料庫相關之特定操作。控制器210可由於一ASIC之硬連線電路而執行此等操作。控制器210亦(或另一選擇係)可回應於處理器214執行一電腦可讀媒體(諸如記憶體216)中所含有之軟體指令而執行此等操作。一電腦可讀媒體可定義為一非暫時性記憶體裝置。一記憶體裝置可實施於一單個實體記憶體裝置內或跨越多個實體記憶體裝置散佈。可將軟體指令自另一電腦可讀媒體或自另一裝置讀取至記憶體216中。記憶體216中所含有之軟體指令可致使處理器214執行本文中所描述之程序。因此，本文中所描述之實施方案並不限於硬體電路與軟體之任何特定組合。

周邊裝置230可包含將資訊提供至控制器210、由控制器210控制及/或以其他方式與控制器210通信之一或多個裝置。舉例而言，周邊裝置230可包含一讀取器裝置240、一鎖裝置250、一感測器260及/或一致動器270。儘管出於說明性目的而在圖2中展示一單個讀取器裝置

240、一單個鎖裝置250、一單個感測器260及一單個致動器270，但實際上，周邊裝置230可包含多個讀取器裝置240、多個鎖裝置250、多個感測器260及/或多個致動器270。在某些實施方案中，周邊裝置230可不包含圖2中所展示之裝置中之一或多者。另外或另一選擇係，周邊裝置230可包含圖2中未展示之任何其他類型之安全裝置。

讀取器裝置240可包含自一使用者讀取憑證並將該等憑證提供至控制器210之一裝置。舉例而言，讀取器裝置240可包含經組態以自一使用者接收一文數個人識別號碼(PIN)之一小鍵盤；用以組態在一磁條或另一類型之儲存裝置(諸如一RFID標籤)上儲存一卡代碼之一卡之一讀卡器；經組態以讀取一使用者之指紋之一指紋讀取器；經組態以讀取一使用者之虹膜之一虹膜讀取器；一麥克風及經組態以記錄一使用者之話音標誌之一話音標誌識別器；一近場通信(NFC)讀取器；及/或另一類型之讀取器裝置。讀取器裝置240可包含可提供憑證之任何類型之安全裝置，且可包含一或多個感測器裝置，諸如下文參考感測器260所描述之任何感測器裝置。舉例而言，讀取器裝置240可包含用於面部辨識之一攝影機及/或用於話音辨識之一麥克風。

鎖裝置250可包含由控制器210控制之一鎖。鎖裝置250可鎖住一門(例如，防止其打開或關閉)、一窗戶、一HVAC通風孔及/或至一安全區之另一類型之進入開口。舉例而言，鎖裝置250可包含一電磁鎖；具有由控制器210控制之一馬達之一機械鎖；一機電鎖；及/或另一類型之鎖。此外，鎖裝置250可進行一機器、運輸運載工具、電梯及/或一電裝置之鎖住/開鎖操作。

感測器260可包含一感測器裝置。作為實例，感測器260可包含：用以感測一門打開還是關閉之一門感測器；一可見光監視攝影機、一紅外線(IR)光監視攝影機、一熱標誌監視攝影機及/或另一類型之監視裝置；一報警感測器，諸如一運動感測器、一熱感測器、一壓

力感測器及/或另一類型之報警感測器；一音訊記錄裝置(例如，麥克風)；一篡改感測器，諸如位於系統單元115內側之一位置感測器；及/或位於與系統單元115相關聯之一安全區內之一「外出請求」按鈕；及/或另一類型之感測器裝置。

致動器270可包含一致動器裝置。作為一實例，致動器270可控制一照明裝置。作為其他實例，致動器270可包含：一防盜報警啟動器；用以播放訊息或產生報警信號之一揚聲器；一顯示裝置；用以移動感測器260 (例如，控制一攝影機或其他監視裝置之視域)之一馬達；用於打開/關閉一門、窗戶、HVAC通風孔及/或與一安全區相關聯之另一開口之一馬達；用以將鎖裝置250固定於一鎖住或未鎖位置中之一馬達；一滅火裝置；及/或另一類型之致動器裝置。

雖然圖2展示系統單元115之例示性組件，但在其他實施方案中，系統單元115相比圖2中所繪示之組件可包含更少之組件、不同之組件、額外組件或不同配置之組件。另外或另一選擇係，系統單元115之任何組件(或任何組件群組)可執行描述為由系統單元115之一或多個其他組件執行之任務(或若干任務)。舉例而言，在某些實施方案中，周邊介面220可對應於一網路介面。作為另一實例，在某些實施方案中，周邊裝置230可經由網路介面218而非經由周邊介面220連接至控制器210。

此外，雖然DCS 110可包含一實體進入分散控制系統，但其他實施方案可控制除實體進入系統之外的系統。另一方面，DCS 110可包含任何類型之實體進入控制系統(例如，在一操作環境中)，諸如用於打開及/或關閉一門或控制對一建築物或設施之實體進入之一控制系統。DCS 110亦可包含用以控制一風扇(例如，起動或停止)、用以起始一建築物管理系統中之一報警(例如，失敗之鑒認、成功之鑒認等等)或用以控制一工業自動化系統中之一機器人臂之一系統。

圖3A及圖3B係圖解說明系統單元115之例示性功能組件之方塊圖。舉例而言，可經由一或多個ASIC之硬連線電路來實施系統單元115之功能組件。另外或另一選擇係，可由執行來自記憶體216之指令之處理器214來實施系統單元115之功能組件。圖3A圖解說明系統單元115之功能層。如圖3A中所展示，系統單元115可包含一應用程式開發介面(API)層310、一應用程式層320、一分散層340及一儲存層350。

API層310包含經組態以與(舉例而言)管理裝置130通信之一API。作為一實例，當一管理員使用管理員裝置130登入至系統單元115中時，API層310可與管理員裝置130通信以鑒認管理員。作為另一實例，API層310可與管理員裝置130通信以改變系統單元115之一組態。API層310可自管理員裝置130接收資料並將該資料提供至分散層340及/或儲存層350。API層310亦可與管理員裝置130通信以在應用程式層320中安裝一應用程式。API層310可經組態以處置不同管理員類型。舉例而言，API層310可包含用以處置一Web服務管理員、一Linux管理員、一開放網路視訊介面論壇(ONVIF)管理員之一API及/或另一類型之API。

應用程式層320包含安裝於系統單元115上之一或多個應用程式。圖3B展示例示性應用程式。如圖3B中所展示，應用程式層320可包含一進入控制邏輯應用程式322、一門控制應用程式324、一讀取器控制應用程式326、一事件處置應用程式328、一時間表處置應用程式330及/或一資料庫管理器應用程式332。

進入控制邏輯應用程式322可基於所接收憑證且基於所儲存進入規則而判定是否授予進入。門控制應用程式324可控制一或多個門及/或相關聯鎖裝置250。舉例而言，門控制應用程式324可判定一門打開還是關閉及/或鎖住還是未鎖，且可操作一或多個裝置以打開或關閉

門及/或將門鎖住或開鎖。讀取器控制應用程式326可控制一或多個讀取器裝置240且可獲得並處理自一或多個讀取器裝置240接收之憑證。事件處置應用程式328可維持由系統單元115記錄或產生及/或由另一系統單元115記錄之事件之一紀錄。事件處置應用程式328可確保將區域記錄或產生之事件分散至DCS 110中之其他系統單元115以便在所有(或至少某些)系統單元115中維持一分散系統事件紀錄。因此，可自與系統事件紀錄相關聯之任何系統單元115檢索所紀錄事件。時間表處置應用程式330可管理與系統單元115相關聯之一或多個時間表。舉例而言，針對特定使用者群組之進入規則可基於一天之特定時間而改變。

資料庫管理器應用程式332可自全域資料庫354導出區域進入規則資料庫356及/或區域憑證表358。在某些實施方案中，系統單元115可不包含全域資料庫354。舉例而言，資料庫管理器應用程式332可在另一裝置處(諸如在另一系統單元115處或在管理裝置130處)存取全域資料庫354。在又某些實施方案中，可在另一系統單元115處自全域資料庫354導出區域進入規則資料庫356及/或區域憑證表358並將其提供至系統單元115。

應用程式層320中可包含其他應用程式(圖3B中未展示)。作為一實例，一報警應用程式可產生一報告及/或一報警並將該報告及/或報警發送至管理員裝置130 (及/或發送至另一指定裝置)及/或一或多個其他系統單元115。作為另一實例，一任務特有控制應用程式可處理與系統單元115相關聯之事件，諸如門打開事件、感測器事件、致動器事件及/或其他類型之事件。

分散層340可管理與系統單元115相關聯之一或多個分散資料集。舉例而言，分散層340可經由網路120維持與其他系統單元115之安全連接(例如，一輸送層安全(TLS)連接)。此外，分散層340可使用

一協定(例如，一PAXOS協定)來建立關於一特定基於共識之分散資料集之一改變之一共識。作為一實例，分散層340可將一改變之一提議發送至與分散資料集相關聯之其他系統單元115且可自其他系統單元115接收改變之一法定數。作為另一實例，分散層340可投票贊成自另一系統單元115接收之一提議。作為又一實例，分散層340可接收已在未投票贊成一改變之情況下達成對該改變之一共識之一指示。當接收到對一改變之共識之一指示時，分散層340可在分散資料集之區域複本中做出該改變。

儲存層350儲存與系統單元115相關聯之一或多個資料集。儲存於儲存層350中之一資料集可對應於一區域資料集或可對應於一分散資料集。一區域資料集可儲存與儲存該區域資料集之特定系統單元115相關聯(及/或僅與該特定系統單元相關聯)之資訊。一分散資料集可儲存與和該分散資料集相關聯之其他系統單元115相關聯之資訊。

圖3B中展示可包含於儲存層350中之例示性資訊。如圖3B中所展示，儲存層350可包含一組態資料庫352、一全域資料庫354、一區域進入規則資料庫356及一區域憑證資料庫358。

組態資料庫352可儲存與一特定系統單元115相關聯之組態資料，諸如控制器210之硬體組態、連接至控制器210之周邊裝置230、安裝於應用程式層320中之應用程式及/或其他類型之組態資訊。組態資料庫352可儲存與系統單元115相關聯之進入實體之一清單。

全域資料庫354可儲存與DCS 110相關聯之一全域資料庫。下文參考圖4A來描述可儲存於全域資料庫354中之例示性資訊。區域進入規則資料庫356可儲存與系統單元115相關聯之進入規則。下文參考圖4B來描述可儲存於區域進入規則資料庫356中之例示性資訊。區域憑證資料庫358可儲存與系統單元115相關聯之區域憑證。下文參考圖4C來描述可儲存於區域憑證資料庫358中之例示性資訊。

雖然圖3A及圖3B展示系統單元115之例示性功能組件，但在其他實施方案中，系統單元115相比圖3A及圖3B中所繪示之功能組件可包含更少之功能組件、不同之功能組件、不同配置之功能組件或額外功能組件。另外，系統單元115之組件中之任一者(或任何組件群組)可執行描述為由系統單元115之一或多個其他功能組件執行之功能。

圖4A係可儲存於全域資料庫354中之例示性資訊之一圖式。如圖4A中所展示，全域資料庫354可包含一或多個全域資料庫項目410、一群組表420及一進入規則表430。每一全域資料庫項目410可儲存一特定使用者之資訊。全域資料庫項目410可包含一列編號欄位412、一使用者識別(ID)欄位414、一憑證類型欄位416及一憑證值欄位418。

列編號欄位412可針對全域資料庫354中之一使用者包含一特定列。在某些實施方案中，可在多個資料庫/表中針對一使用者使用等同列編號。跨越多個資料庫/表針對一使用者使用等同列編號可簡化資訊之處理及檢索。使用者ID欄位414可儲存與一使用者相關聯之識別資訊，諸如使用者之名稱、員工編號、連絡人資訊及/或其他類型之使用者資訊。憑證類型欄位416可識別與使用者相關聯之一特定憑證類型，諸如卡憑證類型、一個人識別號碼(PIN)類型、一虹膜掃描類型、一指紋類型、一話音標誌類型及/或另一憑證類型。憑證值418可儲存與憑證類型相關聯之一憑證值，諸如一進入卡值、一PIN值、虹膜掃描資料、指紋資料、話音標誌資料及/或另一類型之憑證類型之資料。一使用者可與多個憑證類型相關聯。在某些實施方案中，在全域資料庫354中可給每一憑證類型指派一單獨列。在其他實施方案中，可將多個憑證類型儲存於同一列中。

群組表420可包含識別特定使用者群組連同屬於每一群組之特定使用者之一表。舉例而言，群組表420可識別為工程師之一使用者群組、一秘書人員使用者群組、為技術員之一使用者群組等等。每一群

組可與特定進入規則相關聯。進入規則表430可儲存各使用者群組之進入規則。

雖然圖4A展示可儲存於全域資料庫354中之例示性欄位，但在其他實施方案中，全域資料庫354相比圖4A中所繪示之欄位可包含更少之欄位、不同之欄位、不同配置之欄位或額外欄位。

圖4B係可儲存於區域進入規則資料庫356中之例示性資訊之一圖式。如圖4B中所展示，區域進入規則資料庫356可包含一或多個進入規則項目440。每一進入規則項目440可結合一或多個進入實體儲存一或多個使用者之進入規則資訊。進入規則項目440可包含一列編號欄位442、一進入實體欄位444及一進入規則欄位446。

列編號欄位442可識別對應於全域資料庫354中之使用者之與一特定進入規則相關聯之一或多個列編號。在某些實施方案中，列編號欄位442可識別一特定使用者群組。在其他實施方案中，列編號欄位442可儲存對應於全域資料庫354中之使用者之其他類型之匿名資訊(例如，指派給全域資料庫354中之一使用者之一字元串)。因此，識別一使用者之資訊可不儲存於區域進入規則資料庫356中且區域進入規則資料庫356可對應於一匿名資料庫。進入實體欄位444可識別與特定進入規則相關聯之一或多個進入實體。一進入實體可對應於一特定區，諸如一特定房間；一特定進入開口，諸如一門、窗戶、HVAC通風孔及/或另一類型之開口；一機器、運輸運載工具、電梯及/或一電裝置；及/或另一類型之進入實體。在某些實施方案中，進入實體欄位444可識別與進入實體相關聯之一特定鎖裝置250。

進入規則欄位446可儲存與進入實體及使用者群組相關聯之一或多個進入規則。一進入規則可規定授予進入所需之憑證類型，可規定其間應授予進入之特定時間，及/或可規定為了授予進入而需要滿足之其他條件(例如，與系統單元115相關聯之一特定狀態)。作為實

例，一進入規則可授予所有使用者在一火災報警事件期間進入特定進入實體。作為另一實例，若系統單元115偵測到一安全漏洞，則一進入規則可拒絕所有使用者之進入。作為又一實例，僅若與同一或另一系統單元115相關聯之一第二門關閉，則一進入規則可授予進入一第一門。

雖然圖4B展示可儲存於區域進入規則資料庫356中之例示性欄位，但在其他實施方案中，區域進入規則資料庫356相比圖4B中所繪示之欄位可包含更少之欄位、不同之欄位、不同配置之欄位或額外欄位。

圖4C係可儲存於區域憑證資料庫358中之例示性資訊之一圖式。如圖4C中所展示，區域憑證資料庫358可包含一或多個憑證項目450。每一憑證項目450可儲存與一特定使用者相關聯之一特定憑證之資訊。因此，一特定使用者可與多個憑證項目450相關聯。

列編號452可識別與特定使用者相關聯之在全域資料庫354中之一特定列編號。因此，識別一使用者之資訊可不儲存於區域憑證資料庫358中，且區域憑證資料庫358可對應於一匿名資料庫。經雜湊憑證值454可儲存與特定使用者相關聯之一特定經雜湊憑證值。因此，實際憑證值可不儲存於區域憑證資料庫358中。經加密區域進入規則密鑰456可儲存至可經加密之區域進入規則表356之一區域進入規則密鑰。該區域進入規則密鑰可為未藉助一未雜湊憑證值加密，因此不將該未雜湊憑證值儲存於持久記憶體中。當讀取器裝置240自一使用者獲得一憑證值時，可對憑證值進行雜湊運算且可使用經雜湊憑證值來識別一憑證項目450。然後，可使用未雜湊憑證值來解密經加密區域進入規則密鑰，且可使用經解密區域進入規則密鑰來解密區域進入規則表。由於系統單元115未儲存未雜湊憑證值，因此若系統單元115之安全受到危害，則無法自一受危害之系統單元115檢索未雜湊憑證

值。

雖然圖4C展示可儲存於區域憑證資料庫358中之例示性欄位，但在其他實施方案中，區域憑證資料庫358相比圖4C中所繪示之欄位可包含更少之欄位、不同之欄位、不同配置之欄位或額外欄位。

圖5係根據一或多項實施例用於自一全域資料庫導出區域資料庫之一流程圖之一圖式。在某些實施方案中，圖5之程序可由控制器210執行。在其他實施方案中，圖5之程序中之某些或全部可由與控制器210分離及/或包含控制器210之另一裝置或一裝置群組執行。

圖5之程序可包含獲得對一全域資料庫之存取(方塊510)。在某些實施方案中，系統單元115可包含全域資料庫之一經加密複本。為了獲得對全域資料庫之存取，控制器210可需要自管理員裝置130獲得一口令。可使用所獲得之口令來導出用以解密全域資料庫之一密鑰。在其他實施方案中，全域資料庫可儲存於另一系統單元115中，且另一系統單元115可獲得口令並解密全域資料庫。然後，控制器210可在另一系統單元115處存取經解密全域資料庫。在又某些實施方案中，全域資料庫可由管理裝置130 (及/或並非DCS 115之部分之另一裝置)維持，且控制器210可在管理裝置130處存取全域資料庫。可自全域資料庫導出一區域進入規則表(方塊520)。舉例而言，資料庫管理器應用程式332可存取組態資料庫352以識別哪些進入實體與系統單元115相關聯，且可自進入規則表430獲得與所識別進入實體有關之進入規則。資料庫管理器應用程式332可基於自進入規則表430獲得之資訊而產生區域進入規則資料庫356。資料庫管理器應用程式332可產生一區域進入規則密鑰且可藉助所產生之區域進入規則密鑰加密區域進入規則資料庫356。

可自全域資料庫導出一區域憑證表(方塊530)。舉例而言，資料庫管理器應用程式332可存取所產生之區域進入規則資料庫356以判定

哪些使用者與包含於區域進入規則資料庫356中之進入規則相關聯，及基於該等進入規則為了進入需要每一使用者之哪些憑證類型。資料庫管理器應用程式332可為每一使用者產生一列且可自全域資料庫獲得每一使用者及與該使用者相關聯之每一憑證類型之憑證值。可使用該憑證值來加密區域進入規則密鑰，且可將經加密區域進入規則密鑰儲存於與使用者相關聯之列中。此外，可使用一單向雜湊(諸如一SHA-256雜湊，其針對任何長度之一輸入產生一256位元經雜湊值)對該憑證值進行雜湊運算。在其他實施方案中，可使用一不同類型之雜湊程序。

在其他實施方案中，系統單元115不獲得憑證值，且區域憑證表由(舉例而言)另一系統單元115或由管理裝置130遠端地產生。作為一實例，在某些實施方案中，一第一系統單元115可包含全域資料庫354且一第二系統單元115可不包含全域資料庫354。第一系統單元115可導出第一系統單元115之一第一區域進入規則表356及一第一區域憑證表358。第一系統單元115可進一步導出第二系統單元115之一遠端區域進入規則表356及一遠端區域憑證表358。在某些實施方案中，第一系統單元115可將遠端區域進入規則表356及遠端區域憑證表358提供至第二系統單元115。在其他實施方案中，第一系統單元115可維持遠端區域進入規則表356及遠端區域憑證表358，且第二系統單元115可需要在第一系統單元115處存取遠端區域進入規則表356及遠端區域憑證表358。

圖6係根據一或多項實施例用於更新一全域資料庫之一流程圖之一圖式。在圖6中，全域資料庫被組態為一分散資料集，其中該全域資料庫之一經加密版本儲存於與該分散資料集相關聯之系統單元115中。在某些實施方案中，全域資料庫可分散於所有系統單元115中。在其他實施方案中，某些系統單元115可不與全域資料庫分散資料集

相關聯且因此可不包含全域資料庫之一複本。在某些實施方案中，圖6之程序可由控制器210執行。在其他實施方案中，圖6之程序中之某些或全部可由與控制器210分離及/或包含控制器210之另一裝置或一裝置群組執行。

圖6之程序可包含鑒認自一管理裝置之一登入(方塊610)。舉例而言，一管理員可判定需要更新全域資料庫354。舉例而言，管理員可需要添加一使用者、改變一使用者之憑證、改變一特定進入實體之一進入規則等等。管理員可使用由管理員供應之一口令登入至一特定系統單元115中。可接收對全域資料庫之一更新(方塊620)並將其分散至分散系統中之其他裝置(630)。舉例而言，系統單元115可自管理裝置354接收對全域資料庫354之一更新，且分散層340可在DCS 110中之其他系統單元115中分散對全域資料庫345之區域複本之更新。

可解密全域資料庫之一有關部分(方塊640)，且可更新全域資料庫(方塊650)。可使用該更新來判定全域資料庫354之哪一部分需要被解密。舉例而言，對一特定列編號412之一更新可僅要求包含特定列編號412的全域資料庫354之一部分需要被解密。類似地，對群組表420或進入規則表430之一更新可分別僅要求對群組表420或進入規則表430之解密。可藉助自一管理口令導出之一全域資料庫密鑰來加密全域資料庫354，且可接收自管理裝置130接收之一管理口令，使用其來導出全域資料庫密鑰，且可使用全域資料庫密鑰來解密全域資料庫354之所判定有關部分。在解密之後，可基於所接收之更新而更新全域資料庫354。類似地，可在更新已被分散至之其他系統單元115處對全域資料庫354之區域複本執行更新。

可做出關於更新是否與區域進入規則表有關之一判定(方塊655)。舉例而言，接收到更新之每一特定系統單元115處之資料庫管理器應用程式332可判定該更新是否包含與特定系統單元115相關聯之

一進入實體。若該更新與區域進入規則表有關(方塊655-是)，則可在特定系統單元115處更新區域進入規則資料庫356 (方塊660)。若該更新不與區域進入規則表有關(方塊655-否)，則處理可繼續至方塊665。

可做出關於更新是否與區域憑證表有關之一判定(方塊665)。舉例而言，接收到更新之每一特定系統單元115處之資料庫管理器應用程式332可判定該更新是否包含特定系統單元115之區域進入規則資料庫356中所包含之一使用者。若該更新與區域憑證表有關(方塊665-是)，則可在特定系統單元115處更新區域憑證資料庫358 (方塊670)。若更新不與區域憑證表有關(方塊665-否)，則處理可繼續至方塊680。在其他實施方案中，區域進入規則表及/或區域憑證表可包含DCS 110之所有使用者而非與一特定系統單元115有關之使用者之資訊。

在任何更新之後，可移除全域資料庫之經解密部分(方塊680)。舉例而言，每一特定系統單元115處之資料庫管理器應用程式332可將曾用以儲存全域資料庫354之經解密部分之記憶體空間解除分配。在某些實施方案中，可另外將經解除分配之記憶體空間徹底擦除。

圖7係根據一或多項實施例用於更新一區域進入規則表之一流程圖之一圖式。在某些實施方案中，圖7之程序可由控制器210執行。在其他實施方案中，圖7之程序中之某些或全部可由與控制器210分離及/或包含控制器210之另一裝置或一裝置群組執行。

圖7之程序可包含使用一區域憑證密鑰解密一區域憑證表(方塊710)。舉例而言，區域憑證表358可使用一區域憑證密鑰區域地加密且可經解密以便執行一更新。可在區域憑證表中更新一經雜湊憑證值(方塊720)。舉例而言，若更新改變一使用者之一憑證值，則可產生一新經雜湊憑證值並將其儲存於與使用者相關聯之經雜湊憑證值欄位454中。若一憑證值經改變，則亦可藉助新憑證值重新加密區域進入規則密鑰。因此，可自全域資料庫獲得一區域進入規則密鑰(方塊

730)，且可藉助未雜湊憑證值加密區域進入規則密鑰並將其儲存於區域憑證表中(方塊740)。

圖8係根據一或多項實施例用於更新一區域憑證表之一流程圖之一圖式。在某些實施方案中，圖8之程序可由控制器210執行。在其他實施方案中，圖8之程序中之某些或全部可由與控制器210分離及/或包含控制器210之另一裝置或一裝置群組執行。

為了更新區域進入規則資料庫356，可需要解密區域進入規則資料庫356。然而，由於區域進入規則密鑰僅以藉助使用者之憑證值之一經加密版本儲存於區域憑證資料庫358中，因此可需要自全域資料庫獲得區域進入規則密鑰。因此，圖8之程序可包含自全域資料庫獲得一區域進入規則密鑰(方塊810)且藉助區域進入規則密鑰解密區域進入規則表(方塊820)。可更新(方塊830)並加密(方塊840)區域進入規則表。在加密區域進入規則表之後，可自系統單元115刪除區域進入規則密鑰之未加密版本。

圖9係根據一或多項實施例用於使用一區域憑證表及一區域進入規則表之一流程圖之一圖式。在某些實施方案中，圖9之程序可由控制器210執行。在其他實施方案中，圖9之程序中之某些或全部可由與控制器210分離及/或包含控制器210之另一裝置或一裝置群組執行。

圖9之程序可包含自一讀取器裝置獲得一憑證值(方塊910)。舉例而言，一使用者可藉由將憑證提供至讀取器裝置240而請求對一進入實體之進入。該使用者可執行以下各項中之一或多者：將一小鍵盤字元序列鍵入至一小鍵盤中，接近一讀卡器放置一進入卡，將一虹膜放置在一虹膜掃描讀取器前方，將一手指放置在一指紋掃描機上，向一麥克風中講話以提供一話音樣本，面向與面部辨識軟體相關聯之一攝影機，及/或提供另一類型之憑證值。讀取器裝置240可將一憑證值提供至控制器210，可提供來自一小鍵盤之一PIN、來自一讀卡器之一卡

值、自一虹膜掃描獲得之一特徵向量、自一指紋掃描獲得之一特徵向量、自一話音樣本提取之一特徵向量、自面部辨識軟體獲得之一面部辨識ID及/或另一類型之憑證值。所獲得之憑證值可與一特定進入實體(例如，由控制器210控制之一特定門)相關聯。

可對所獲得之憑證值進行雜湊運算，且可在區域憑證表中識別一項目(方塊920)。舉例而言，進入控制邏輯322可對所獲得之憑證值進行雜湊運算且可試圖在區域憑證資料庫358中定位匹配經雜湊憑證值之一憑證項目450。若未找到一匹配之項目，則可拒絕進入。另外或另一選擇係，若未找到一匹配之項目，則可產生一報警、給使用者之一錯誤訊息及/或另一類型之事件。此外，在某些情形中，可甚至在未找到一匹配之項目之情況下亦可授予進入，且可結合所授予之進入而產生一報警、一紀錄事件及/或另一類型之事件。

若找到一匹配之項目，則可識別與所匹配之項目相關聯之一所使用ID (方塊940)。舉例而言，進入控制邏輯322可識別與所識別區域憑證項目450相關聯之列編號。可使用該列編號在區域進入規則資料庫358中識別使用者之一項目。

可使用所獲得之未雜湊憑證值解密儲存於所識別憑證項目450中之區域進入規則密鑰(方塊950)，且可藉助經解密區域進入規則密鑰來解密區域進入規則表(方塊960)。舉例而言，進入控制邏輯322可藉助未雜湊憑證值解密區域進入規則密鑰。未雜湊憑證值可不由系統單元115儲存。舉例而言，可自讀取器裝置240獲得未雜湊憑證值，使用其來解密區域進入規則密鑰，且然後將其自系統單元115刪除。然後，進入控制邏輯322可藉助經解密區域進入規則密鑰來解密區域進入規則資料庫356。可使用經解密區域進入規則表來應用一或多個進入規則以判定是否授予進入(方塊970)。舉例而言，進入控制邏輯322可判定區域進入規則資料庫356中是否存在針對所識別使用者之一項

目。若不存在針對所識別使用者之項目，則可拒絕進入。若針對該使用者識別出一項目，則對於與所獲得之憑證值相關聯之進入實體，可做出關於進入規則是否授予該使用者進入之一判定。作為一實例，進入規則可規定若接收到憑證值之一特定組合(例如，一卡值與一PIN)，則將授予使用者進入。作為另一實例，進入規則可規定在一天之特定時間及/或一周之特定日期間將授予使用者進入。作為又一實例，進入規則可規定僅若存在另一使用者，則將授予使用者進入(例如，基於自另一使用者接收之憑證值)。作為又一實例，進入規則可規定僅若另一裝置處於一特定條件中(例如，與另一系統單元115相關聯之門感測器指示一門為關閉的)，則將授予使用者進入。若使用者被授予進入，則門控制邏輯應用程式324 (及/或另一進入控制應用程式)可將鎖裝置250開鎖，可操作一致動器裝置270以打開一門，啟動一特定裝置，諸如一電梯等等。在某些實施方案中，若不滿足一進入規則，則可基於儲存於區域進入規則資料庫356中之資訊而給使用者提供解釋為什麼不授予進入之一訊息。

圖10係圖解說明系統單元115之一例示性實體佈局1000之一平面佈置圖。如圖10中所展示，實體佈局1000可包含一牆壁1010、一門1020、控制器210、讀取器裝置240、鎖裝置250、感測器260及致動器270。

牆壁1010封圍一安全區1030，諸如一建築物中之一房間。門1020為一使用者提供至安全區1030之進入。在此實施例中，控制器210安裝在安全區1030內側。在其他實施例中，控制器210可安裝在一非安全區中。讀取器裝置240安裝在安全區1030外側且鎖裝置250在安全區1030內側安裝至牆壁1010及門1020。在此實例中，感測器260為安裝在安全區1030外側之一監視裝置。在此實例中，致動器270包含用於控制監視裝置之視域之一馬達。

當一使用者將憑證鍵入至讀取器裝置240中(例如，藉由鍵入一PIN、掃描一進入卡、掃描一虹膜等等)時，控制器210可使用該等憑證來鑒認使用者之身份且可在區域憑證表358中及隨後在區域進入規則資料庫356中執行一查找以基於使用者之身份及進入規則而判定是否授予使用者之進入。若控制器210判定應授予進入，則控制器210啟動鎖裝置250以將門1020開鎖，因此授予使用者進入安全區1030。

雖然圖10展示實體佈局1000之例示性組件，但在其他實施方案中，實體佈局1000相比圖10中所繪示之組件可包含更少之組件、不同之組件、額外組件或不同配置之組件。另外或另一選擇係，實體佈局1000中之任一組件(或組件群組)可執行描述為由實體佈局1000之一或多個其他組件執行之一或若干任務。

圖11係圖解說明DCS 110之一例示性實體佈局1100之一平面佈置圖。如圖11中所展示，實體佈局1100可包含具有房間1120-A至1120-F之一建築物1110，及一高危險區1130。一區域網路1130 (諸如一乙太網路)可互連系統單元115-A至115-F。在此實例中，系統單元115-A控制進入至房間1120-A中之一門；系統單元115-B控制進入至房間1120-B中之一外側門；系統單元115-C控制自房間1120-B至房間1120-C之一個門，系統單元115-D控制自房間1120-C至房間1120-D之一個門；系統單元115-E控制自房間1120-D至房間1120-E之一個門；系統單元115-F控制進入至房間1120-F中之一外側門，系統單元115-G控制進入至房間1120-E中之一個門及進入至房間1120-A中之一個門；且系統單元115-H控制進入至高危險區1130中之一門。高危險區1130可位於建築物1110外側且因此可被視為具有一較高安全危險。

在此實例中，系統單元115-A至115-H不包含一中央控制裝置(例如，一伺服器)且可包含一或多個分散資料集。舉例而言，系統單元115-A至115-H可維持一分散全域資料庫及/或一分散事件紀錄。假定

一管理員使用管理裝置130登入至系統單元115-A中以添加一使用者並添加與一使用者相關聯之憑證。可將彼等所添加之憑證分散至控制至該使用者可以經由圖5至圖8中所描述之程序進入之房間之門之其他系統單元115。

雖然圖11展示實體佈局1100之例示性組件，但在其他實施方案中，實體佈局1100相比圖11中所繪示之組件可包含更少之組件、不同之組件、額外組件或不同配置之組件。舉例而言，在另一實施例中，一中央控制裝置(例如，一伺服器)可連同一或多個分散資料集一起使用。另外或另一選擇係，實體佈局1100之一或多個組件可執行描述為由實體佈局1100之一或多個其他組件執行之一或多個任務。

圖12A至圖12D係圖11中所描述之系統之全域資料庫之例示性實施方案。圖12A圖解說明其中全域資料庫對應於一分散資料集之一全域資料庫實施方案1210。在全域資料庫實施方案1210中，每一系統單元115包含全域資料庫354之區域複本且自全域資料庫354導出區域進入規則資料庫356及區域憑證資料庫358。

圖12B圖解說明一全域資料庫實施方案1220，其中一特定系統單元115導出另一系統單元115之區域進入規則資料庫356及區域憑證表358。舉例而言，由於系統單元115-H位於高危險區1130中，因此系統單元115-H可不組態有全域資料庫354。而是，系統單元115-A (或系統單元115-A至115-G中之另一者)可導出系統單元115-H之區域進入規則資料庫356-H及區域憑證資料庫358-H且可將區域進入規則資料庫356-H及區域憑證資料庫358-H提供至系統單元115-H。

圖12C圖解說明一全域資料庫實施方案1230，其中一個系統單元115儲存全域資料庫354且使得其他系統單元115能夠存取全域資料庫354。舉例而言，系統單元115-A可儲存全域資料庫354且可自全域資料庫354導出區域進入規則資料庫356-A及區域憑證資料庫358-A。系

統單元115-B可藉由在系統單元115-A處存取全域資料庫354而自全域資料庫354導出區域進入規則資料庫356-B及區域憑證資料庫358-B。類似地，系統單元115-C至115-H藉由在系統單元115-A處存取全域資料庫354而自全域資料庫354分別導出區域進入規則資料庫356-B至356-H及區域憑證資料庫358-B至358-H。另一選擇係，如在圖12B中，系統單元115-A可導出系統單元115-H之區域進入規則資料庫356-H及區域憑證資料庫358-H且可將區域進入規則資料庫356-H及區域憑證資料庫358-H提供至系統單元115-H。

圖12D圖解說明一全域資料庫實施方案1240，其中管理裝置130儲存全域資料庫354且使得系統單元115能夠存取全域資料庫354。因此，系統單元115-A至115-H藉由在管理裝置130處存取全域資料庫354而自全域資料庫354分別導出區域進入規則資料庫356-A至356-H及區域憑證資料庫358-A至358-H。

圖13A至圖13C係根據一或多項實施例之一例示性資料庫使用情境之圖式。圖13A圖解說明圖11中所展示之系統之全域資料庫354之部分。雖然圖13A中未展示，但全域資料庫354亦可包含群組表420及/或進入規則表430。如圖13A中所展示，全域資料庫354可在每一列中儲存一特定使用者之一特定憑證類型及一對應憑證值。儘管出於說明性目的而在圖13A中針對與列ID=21相關聯之使用者展示多個列，但實際上可在全域資料庫354中將使用者列ID=21之不同憑證類型儲存於同一列中。儘管在圖13A至圖13C中，使用全域資料庫354中之列ID作為匿名使用者識別符，但在其他實施方案中，可使用一不同類型之匿名使用者識別符。

圖13B圖解說明系統單元115-G之區域進入規則資料庫356-G。如圖11中所展示，系統單元115-G可控制兩個門：進入至房間1120-E中之一門及進入至房間1120-A中之一門。因此，當自全域資料庫354導

出區域進入規則資料庫356-G時，可包含與房間1120-A及1120-E相關聯之進入規則。圖13B中展示區域進入規則資料庫356-G中之四個項目。第一項目規定所有使用者可藉助一進入卡在8AM至5PM之時間之間進入房間1120-E。第二項目規定全域資料庫中與列21、55及76相關聯之使用者可藉助一進入卡與一PIN之一組合在非營業時間期間進入房間1120-E。第三項目規定全域資料庫中與列44、55、66及78相關聯之使用者可藉助一虹膜掃描在所有時間進入房間1120-A。第四項目規定全域資料庫中與列33、44及66相關聯之使用者可藉助一進入卡與一虹膜掃描之一組合在自5PM至8AM之時間中進入房間1120-A。

圖13C圖解說明系統單元115-G之區域憑證資料庫358-G。圖13C中展示區域憑證資料庫358-G中之四個項目。第一項目包含全域資料庫中與列ID=21相關聯之使用者之一經雜湊卡憑證值及藉助未雜湊憑證值(值40APCE)加密之區域進入規則密鑰。第二項目包含全域資料庫中與列ID=21相關聯之使用者之係一卡憑證值與一PIN之一組合之一經雜湊值及藉助係卡憑證值40APCE與PIN值1234之一組合之一密鑰加密之區域進入規則密鑰。第三項目包含全域資料庫中與列ID=44相關聯之使用者之一虹膜掃描值之一經雜湊版本及藉助未雜湊虹膜掃描憑證值加密之區域進入規則密鑰。第四項目包含全域資料庫中與列ID=44相關聯之使用者之係一卡憑證值與一虹膜掃描值之一組合之一經雜湊值及藉助係使用者列ID=44之卡憑證值與虹膜掃描值之一組合之一密鑰加密之區域進入規則密鑰。

假定使用者列ID=21想要在非營業時間期間進入房間1120-E。使用者可將他的卡放在緊挨房間1120-E之門之讀取器裝置240上，且讀取器裝置240可自該卡檢索卡憑證值40APCE。讀取器裝置240可將憑證值40APCE提供至系統單元356-G之控制器210。控制器210可判定讀取器裝置240與房間1120-E相關聯。控制器210可對該憑證值進行雜湊

運算且識別匹配該經雜湊值之在區域憑證資料庫358-G中之一項目。控制器210可識別使用者列ID=21且可使用所獲得之憑證值40APCE來解密區域進入規則密鑰。然後，控制器210可使用經解密區域進入規則密鑰來解密區域進入規則資料庫356-G。

一旦區域進入規則資料庫356-G被解密，控制器210便可識別針對房間1120-E之包含使用者21之項目。由於控制器210能夠識別多個項目(第一項目及第二項目)，因此控制器210可基於當前時間而選擇第二項目。控制器210可判定使用者需要提供一卡憑證值及一PIN兩者。由於使用者未提供一PIN，因此可不授予使用者之進入。在某些實施方案中，可藉由(舉例而言)告知使用者需要鍵入一PIN而告知使用者關於為什麼不授予進入。若使用者重新掃描卡並在一特定時間週期內鍵入一PIN，則可重複該程序，且控制器210可將至房間1120-E之門開鎖。

在前述說明書中，已參考附圖描述了各種較佳實施例。然而，將顯而易見，可對本發明做出各種修改及改變且可實施額外實施例，此並不背離如以下申請專利範圍中所陳述之本發明之較寬廣範疇。因此，應將本說明書及圖式視為具有一說明性意義而非限制性意義。

舉例而言，儘管已關於圖5至圖9描述了若干系列之方塊，但在其他實施方案中可修改方塊之次序。此外，可並行地執行非相依方塊。

將明瞭，在圖中所圖解說明之實施方案中，可以諸多不同形式之軟體、韌體及硬體來實施如上文所描述之系統及/或方法。用於實施此等系統及方法之實際軟體程式碼或專門化控制硬體並不限於該等實施例。因此，在不參考特定軟體程式碼之情況下來描述該等系統及方法之操作及行為--應理解，軟體及控制硬體可經設計以基於本文中之描述而實施該等系統及方法。

此外，可將上文所描述之特定部分實施為執行一或多個功能之一組件。如本文中所使用，一組件可包含硬體(諸如一處理器、一ASIC或一FPGA)或硬體與軟體之一組合(例如，執行軟體之一處理器)。

術語「包括(comprises及comprising)」規定所陳述特徵、整數、步驟或組件之存在，但並不排除一或多個其他特徵、整數、步驟、組件或其群組之存在或添加。

本申請案中所使用之元件、動作或指令不應理解為對該等實施例至關重要或必不可少，除非明確如此描述。而且，冠詞「一」意欲包含一或多個物項。此外，片語「基於」意欲意指「至少部分地基於」，除非另有明確陳述。

【符號說明】

100	例示性環境/環境
110	分散控制系統
115	控制器裝置/系統單元/第一系統單元/第二系統單元
115-A	系統單元
115-B	系統單元
115-C	系統單元
115-D	系統單元
115-E	系統單元
115-F	系統單元
115-G	系統單元
115-H	系統單元
115-N	系統單元
120	網路
130	管理裝置/管理員裝置

210	邏輯/控制器
212	匯流排
214	處理器
216	記憶體
218	網路介面
220	周邊介面
230	周邊裝置
240	讀取器裝置
250	鎖裝置
260	感測器
270	致動器/致動器裝置
310	應用程式開發介面層
320	應用程式層
322	進入控制邏輯應用程式/進入控制邏輯
324	門控制應用程式/門控制邏輯應用程式
326	讀取器控制應用程式
328	事件處置應用程式
330	時間表處置應用程式
332	資料庫管理器應用程式
340	分散層
350	儲存層
352	組態資料庫
354	全域資料庫
356	區域進入規則表/區域進入規則資料庫/第一區域進入規則表/遠端區域進入規則表
356-A	區域進入規則資料庫

356-B	區域進入規則資料庫
356-G	區域進入規則資料庫
356-H	區域進入規則資料庫
358	區域憑證表/區域憑證資料庫/第一區域憑證表/遠端區域憑證表
358-A	區域憑證資料庫
358-B	區域憑證資料庫
358-G	區域憑證資料庫
358-H	區域憑證資料庫
410	全域資料庫項目
412	列編號欄位/特定列編號
414	使用者識別欄位
416	憑證類型欄位
418	憑證值欄位/憑證值
420	群組表
430	進入規則表
440	進入規則項目
442	列編號欄位
444	進入實體欄位
446	進入規則欄位
450	憑證項目/所識別區域憑證項目/所識別憑證項目
452	列編號
454	經雜湊憑證值/經雜湊憑證值欄位
456	經加密區域進入規則密鑰
1000	例示性實體佈局/實體佈局
1010	牆壁

1020	門
1030	安全區
1100	例示性實體佈局/實體佈局
1110	建築物
1120-A	房間
1120-B	房間
1120-C	房間
1120-D	房間
1120-E	房間
1120-F	房間
1130	高危險區/區域網路
1210	全域資料庫實施方案
1220	全域資料庫實施方案
1230	全域資料庫實施方案
1240	全域資料庫實施方案

申請專利範圍

1. 一種由一控制器裝置執行之方法，該方法包括：

由該控制器裝置存取包含複數個控制器裝置之進入控制資訊之一全域資料庫；

由該控制器裝置自該全域資料庫導出一區域進入規則表，其中該區域進入規則表使得使用者與進入規則相關，且其中該區域進入規則表係藉助一區域進入規則密鑰加密的；

由該控制器裝置自該全域資料庫導出一區域憑證表，其中該區域憑證表使經雜湊憑證與使用者相關，其中該區域憑證表針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於該控制器裝置中；

由該控制器裝置自一讀取器裝置接收一憑證值；

當該所導出區域憑證表中存在與關聯於該所接收憑證值之一使用者相關聯之一憑證項目時，由該控制器裝置基於該所導出區域憑證表而識別該使用者；及

當該所導出區域進入規則表中存在針對該使用者之一進入規則項目時，由該控制器裝置基於該所導出區域進入規則表而執行與該使用者相關聯之一或多個進入規則。

2. 如請求項1之方法，其進一步包括：

對該所接收憑證值進行雜湊運算；

判定該區域憑證表中是否存在針對該經雜湊憑證值之該憑證項目；及

當該區域憑證表中存在針對該經雜湊憑證值之該憑證項目時，在該區域憑證表中識別與該所接收憑證值相關聯之該使用

者。

3. 如請求項2之方法，其進一步包括：

使用該所接收憑證值解密與該憑證項目相關聯之該區域進入規則密鑰；

使用該經解密區域進入規則密鑰解密該區域進入規則表；及

判定該經解密區域進入規則表中是否存在針對該使用者之該進入規則項目。

4. 如請求項1之方法，其進一步包括：

獲得對該全域資料庫之一更新；

基於該更新與關聯於該控制器裝置之一進入實體或該使用者相關聯而判定該更新與該區域進入規則表或該區域憑證表中之至少一者有關；及

基於判定該更新與區域資料庫有關而使用該經更新全域資料庫更新該區域進入規則表或該區域憑證表中之該至少一者。

5. 如請求項4之方法，其中該區域憑證表係使用一區域憑證密鑰加密的，該方法進一步包括：

使用該區域憑證密鑰解密該區域憑證表；

更新該區域憑證表中之一經雜湊憑證值；

自該經解密全域資料庫獲得一未加密區域進入規則密鑰；及

藉助一未雜湊憑證值加密該區域進入規則密鑰，其中該經加密區域進入規則密鑰與該經雜湊憑證值相關聯。

6. 如請求項4之方法，其進一步包括：

自該經解密全域資料庫獲得一未加密區域進入規則密鑰；

使用該所獲得之未加密區域進入規則密鑰解密該區域進入規則表；

更新該區域進入規則表；及

加密該經更新區域進入規則表。

7. 如請求項1至6中任一項之方法，其進一步包括：

自該全域資料庫導出該複數個控制器裝置中之另一控制器裝置之一遠端區域進入規則表；

自該全域資料庫導出該另一控制器裝置之一遠端區域憑證表；及

使得該另一控制器裝置能夠存取該遠端區域進入規則表及該遠端區域憑證表。

8. 如請求項1至6中任一項之方法，其中在該全域資料庫中一使用者與一全域資料庫列編號相關聯，其中在該區域進入規則表中該使用者與該全域資料庫列編號相關聯，且其中在該區域憑證表中該使用者與該全域資料庫列編號相關聯。

9. 如請求項1至6中任一項之方法，其中該複數個控制器裝置對應於一分散實體進入控制系統，且其中該控制器裝置對應於一實體進入控制單元。

10. 一種控制器裝置(115)，其包括：

邏輯(210)，其經組態以：

存取包含複數個控制器裝置(115)之進入控制資訊之一全域資料庫(354)；

自該全域資料庫(354)導出一區域進入規則表(356)，其中該區域進入規則表(356)使得使用者與進入規則相關，且其中該區域進入規則表(356)係藉助一區域進入規則密鑰加密的；

自該全域資料庫(354)導出一區域憑證表(358)，其中該區域憑證表(358)使經雜湊憑證與使用者相關，其中該區域憑證表(358)針對一使用者儲存藉助與該使用者相關聯之未雜湊憑證加密之該區域進入規則密鑰，其中該等未雜湊憑證不儲存於

該控制器裝置中；

自一讀取器裝置接收一憑證值；

當該所導出區域憑證表中存在與關聯於該所接收憑證值之一使用者相關聯之一憑證項目時，基於該所導出區域憑證表而識別該使用者；及

當該所導出區域進入規則表中存在針對該使用者之一進入規則項目時，基於該所導出區域進入規則表而執行與該使用者相關聯之一或多個進入規則。

11. 如請求項10之控制器裝置，其中該邏輯進一步經組態以：

對該所接收憑證值進行雜湊運算；

判定該區域憑證表中是否存在針對該經雜湊憑證值之該憑證項目；及

當該區域憑證表中存在針對該經雜湊憑證值之該憑證項目時，在該區域憑證表中識別與該所接收憑證值相關聯之該使用者。

12. 如請求項10或請求項11之控制器裝置，其中該邏輯進一步經組態以：

使用該所接收憑證值解密與該憑證項目相關聯之該區域進入規則密鑰；

使用該經解密區域進入規則密鑰解密該區域進入規則表；及

判定該經解密區域進入規則表中是否存在針對該使用者之該進入規則項目。

13. 如請求項10或11之控制器裝置，其中該邏輯進一步經組態以：

儲存該全域資料庫；及

使得複數個其他控制器裝置能夠存取該全域資料庫。

14. 如請求項10或11之控制器裝置，其中該邏輯進一步經組態以：

自該全域資料庫導出另一控制器裝置之一遠端區域進入規則表；

自該全域資料庫導出該另一控制器裝置之一遠端區域憑證表；及

將該遠端區域進入規則表及該遠端區域憑證表提供至該另一控制器裝置。

15. 如請求項10或11之控制器裝置，其中該複數個控制器裝置對應於一分散實體進入控制系統，且其中該控制器裝置對應於一實體進入控制單元。

圖式

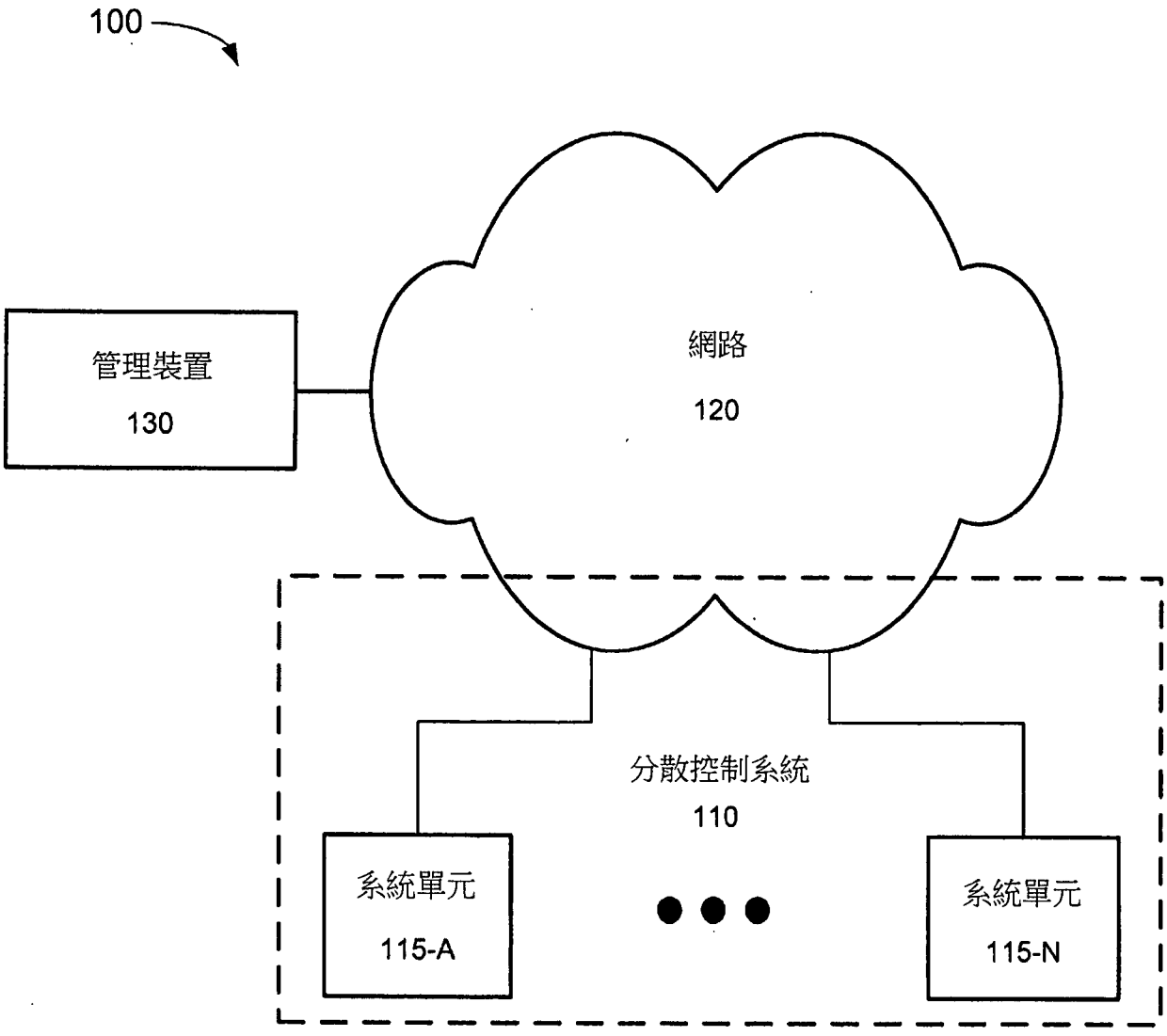

圖 1

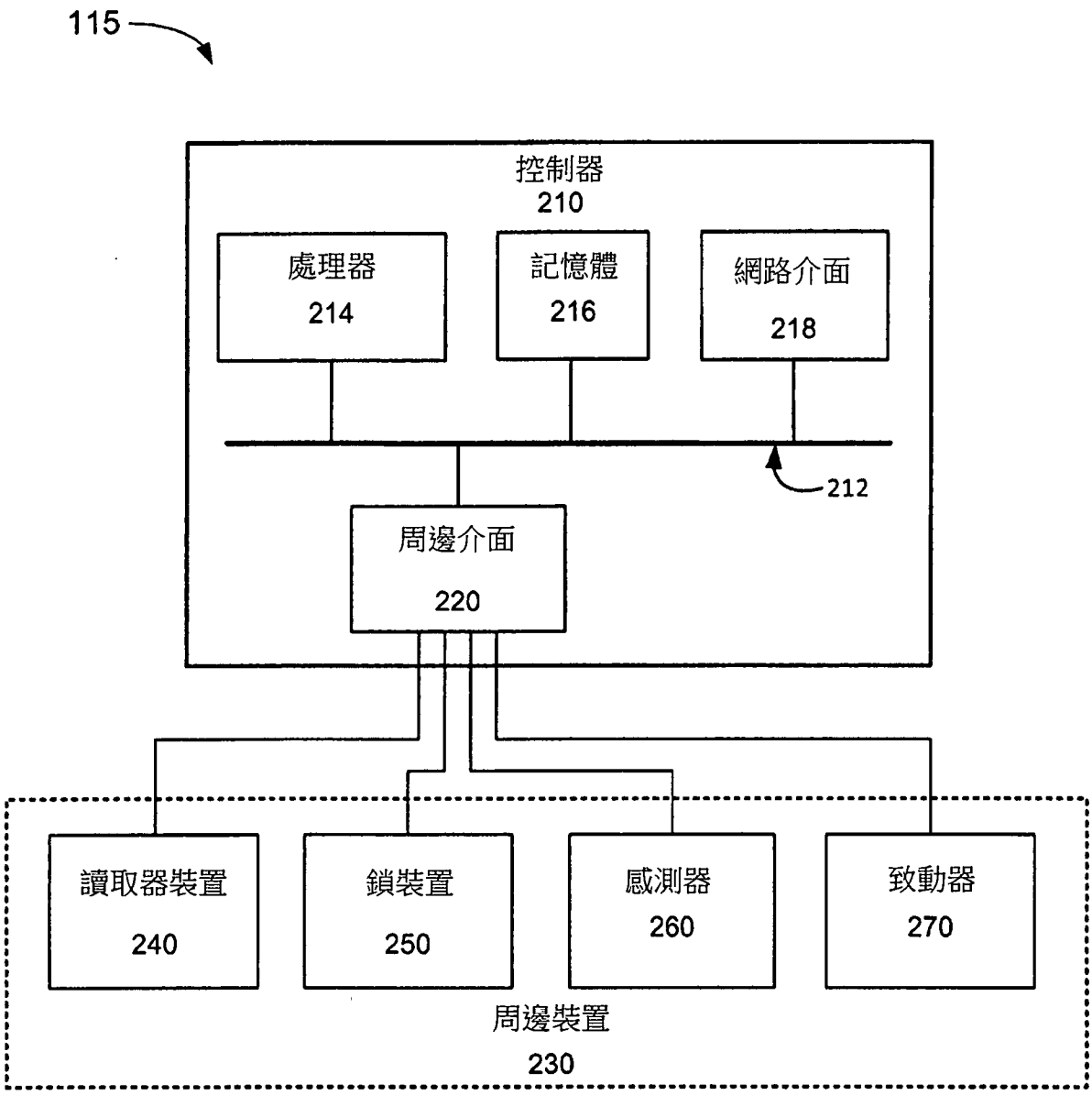
115
控制器
210
處理器
214
記憶體
216
網路介面
218
212
周邊介面
220
讀取器裝置
240
鎖裝置
250
感測器
260
致動器
270
周邊裝置
230

圖 2

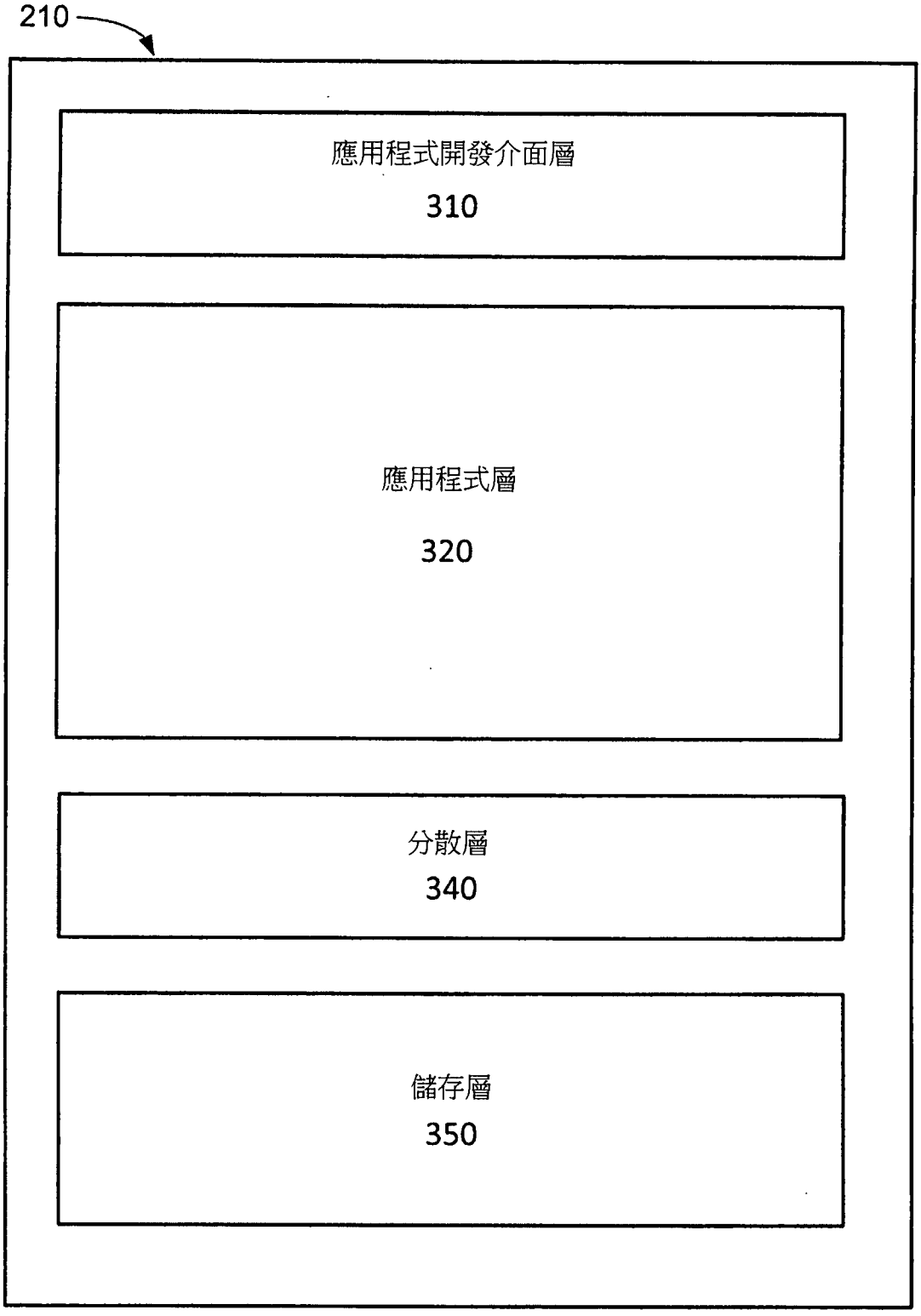

圖 3A

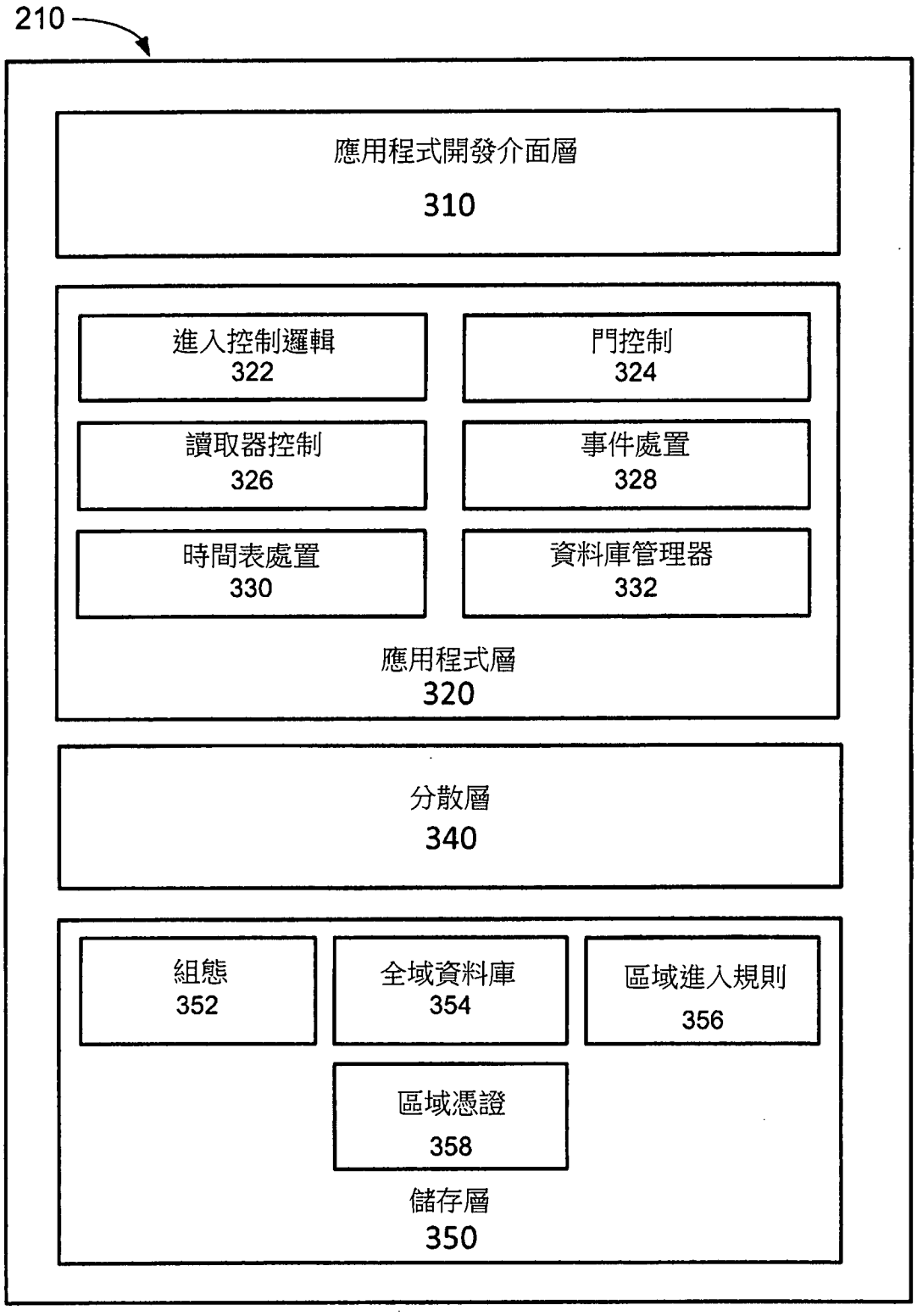
210
應用程式開發介面層
310
進入控制邏輯
322
門控制
324
讀取器控制
326
事件處置
328
時間表處置
330
資料庫管理器
332
應用程式層
320
分散層
340
組態
352
全域資料庫
354
區域進入規則
356
區域憑證
358
儲存層
350

圖 3B

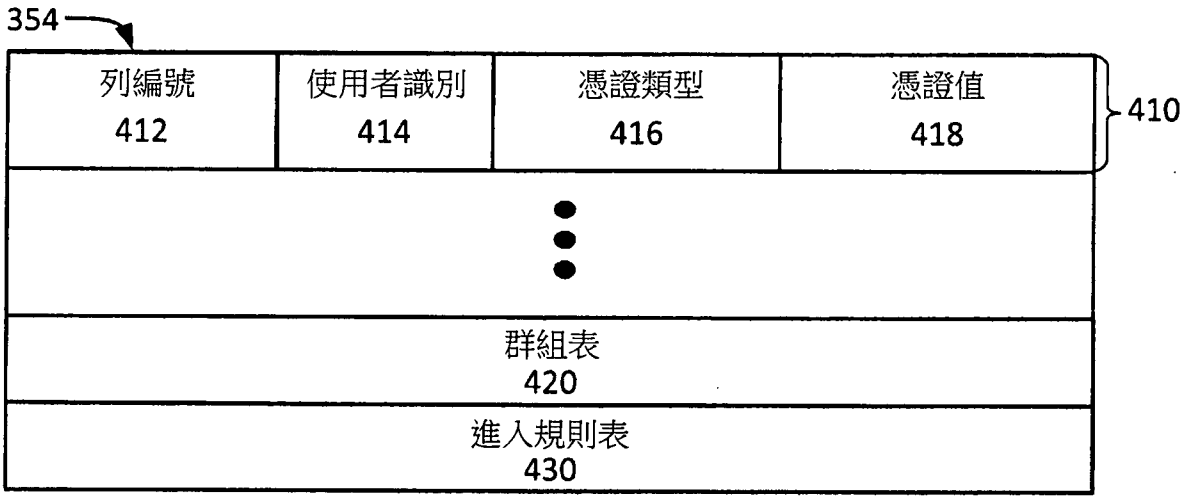
354
列編號
412
使用者識別
414
憑證類型
416
憑證值
418
410
群組表
420
進入規則表
430

圖 4A

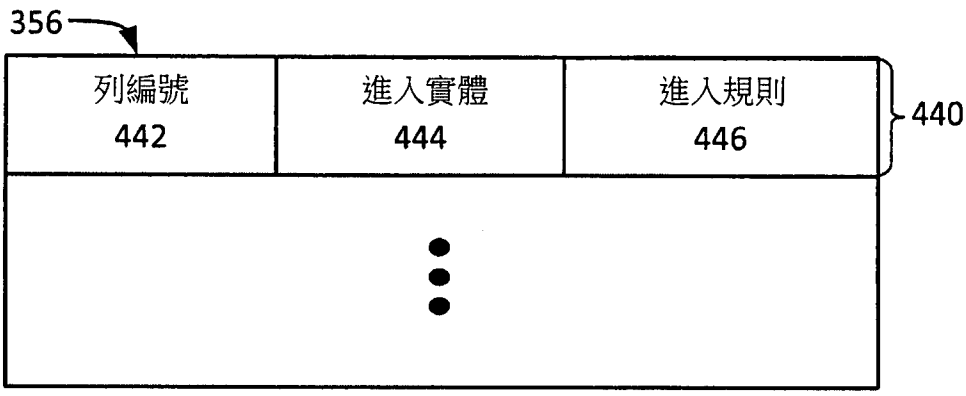
356
列編號
442
進入實體
444
進入規則
446
440

圖 4B

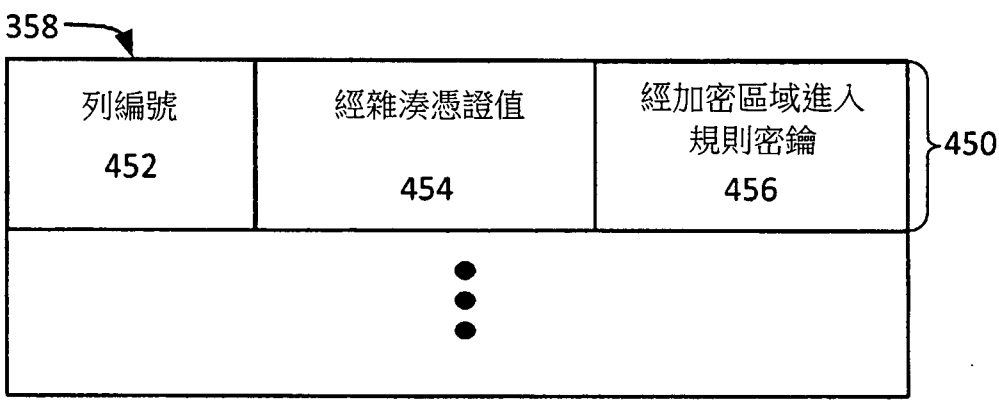
358
列編號
452
經雜湊憑證值
454
經加密區域進入
規則密鑰
456
450

圖 4C

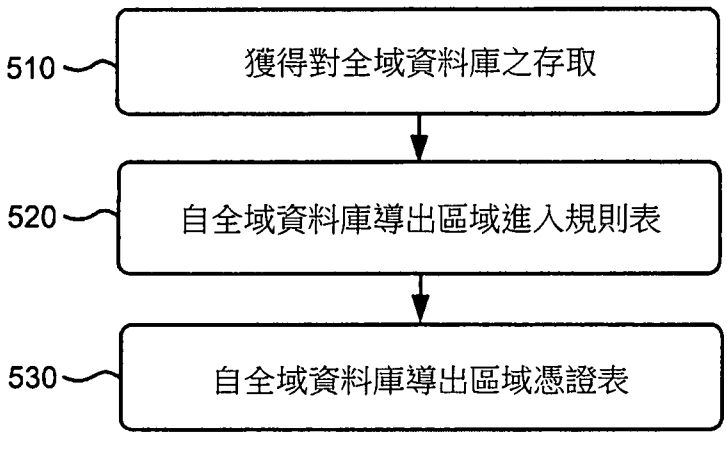

圖 5

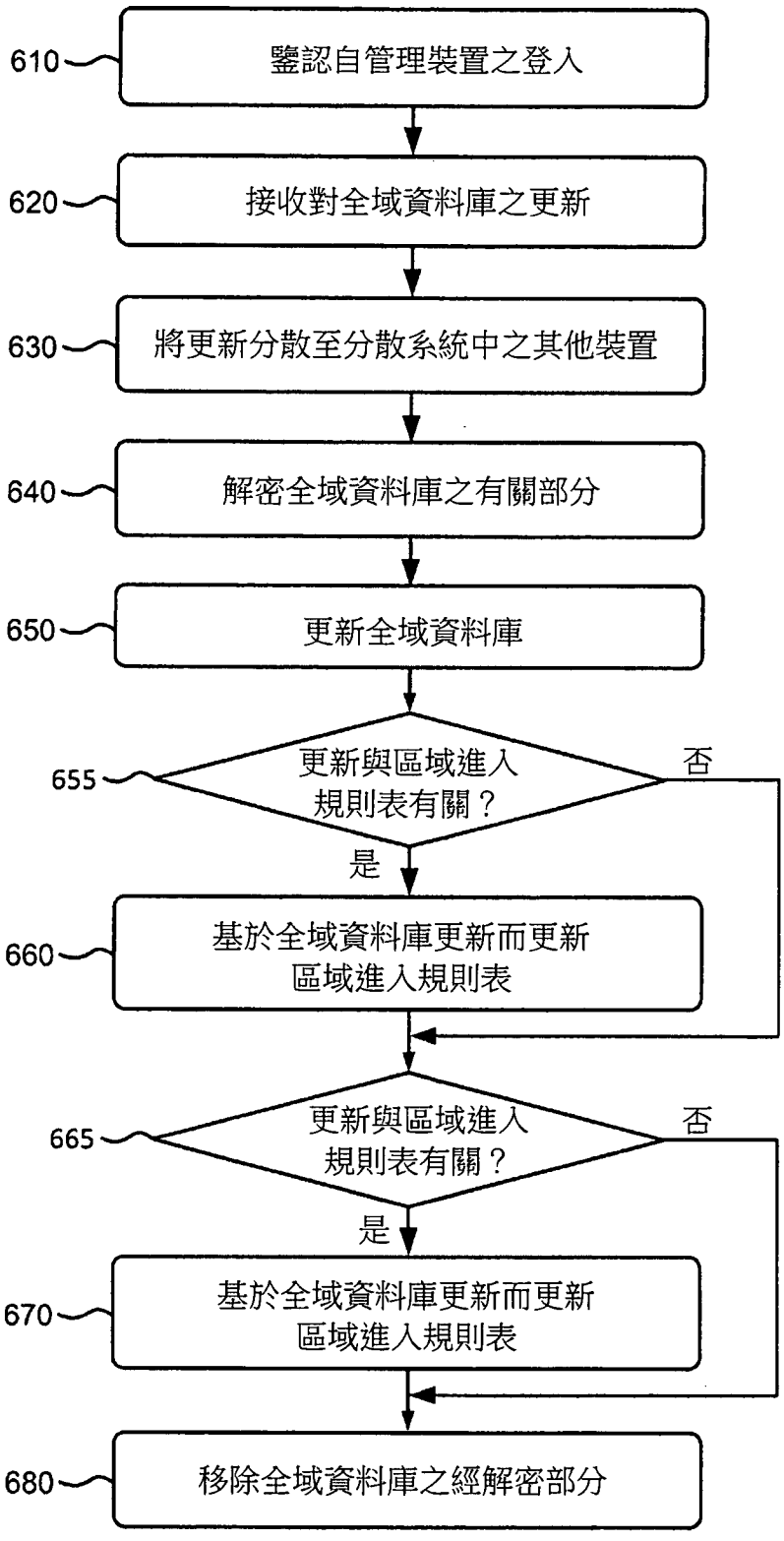
610
鑒認自管理裝置之登入
620
接收對全域資料庫之更新
630
將更新分散至分散系統中之其他裝置
640
解密全域資料庫之有關部分
650
更新全域資料庫
655
更新與區域進入規則表有關？
否
是
660
基於全域資料庫更新而更新區域進入規則表
665
更新與區域進入規則表有關？
否
是
670
基於全域資料庫更新而更新區域進入規則表
680
移除全域資料庫之經解密部分

圖 6

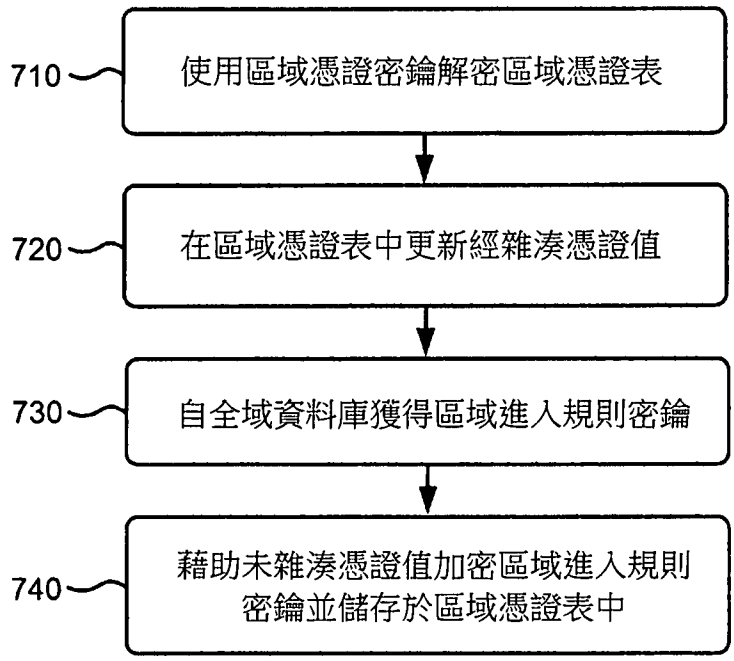
710
使用區域憑證密鑰解密區域憑證表
720
在區域憑證表中更新經雜湊憑證值
730
自全域資料庫獲得區域進入規則密鑰
740
藉助未雜湊憑證值加密區域進入規則密鑰並儲存於區域憑證表中

圖 7

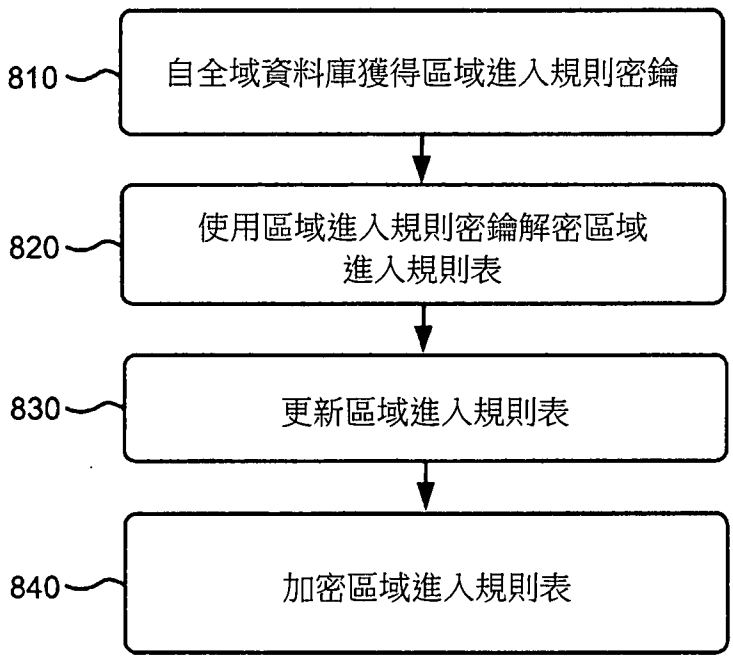
810
自全域資料庫獲得區域進入規則密鑰
820
使用區域進入規則密鑰解密區域進入規則表
830
更新區域進入規則表
840
加密區域進入規則表

圖 8

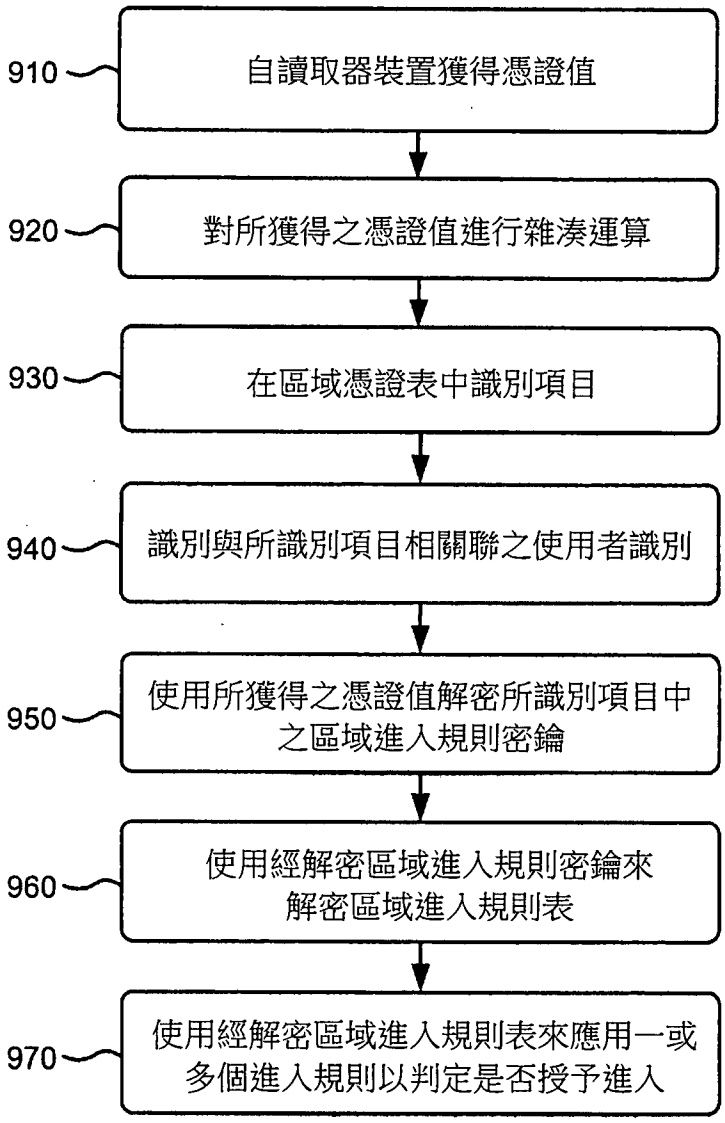
910
自讀取器裝置獲得憑證值
920
對所獲得之憑證值進行雜湊運算
930
在區域憑證表中識別項目
940
識別與所識別項目相關聯之使用者識別
950
使用所獲得之憑證值解密所識別項目中之區域進入規則密鑰
960
使用經解密區域進入規則密鑰來解密區域進入規則表
970
使用經解密區域進入規則表來應用一或多個進入規則以判定是否授予進入

圖 9

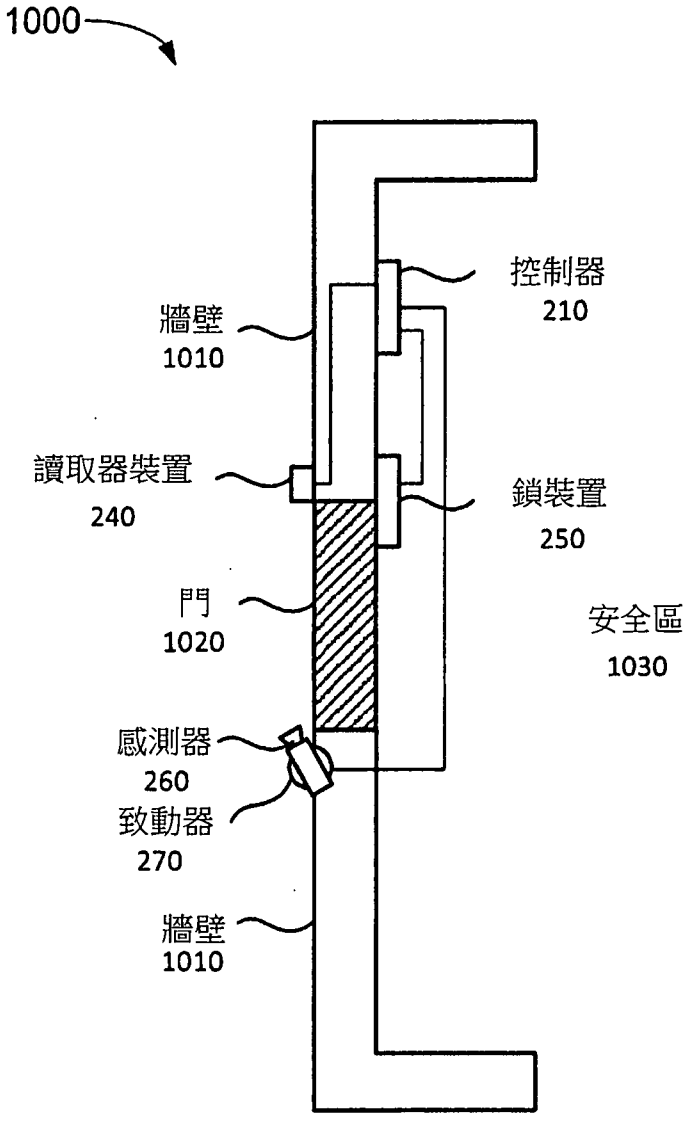
1000
控制器
210
牆壁
1010
讀取器裝置
240
鎖裝置
250
門
1020
安全區
1030
感測器
260
致動器
270
牆壁
1010

圖 10

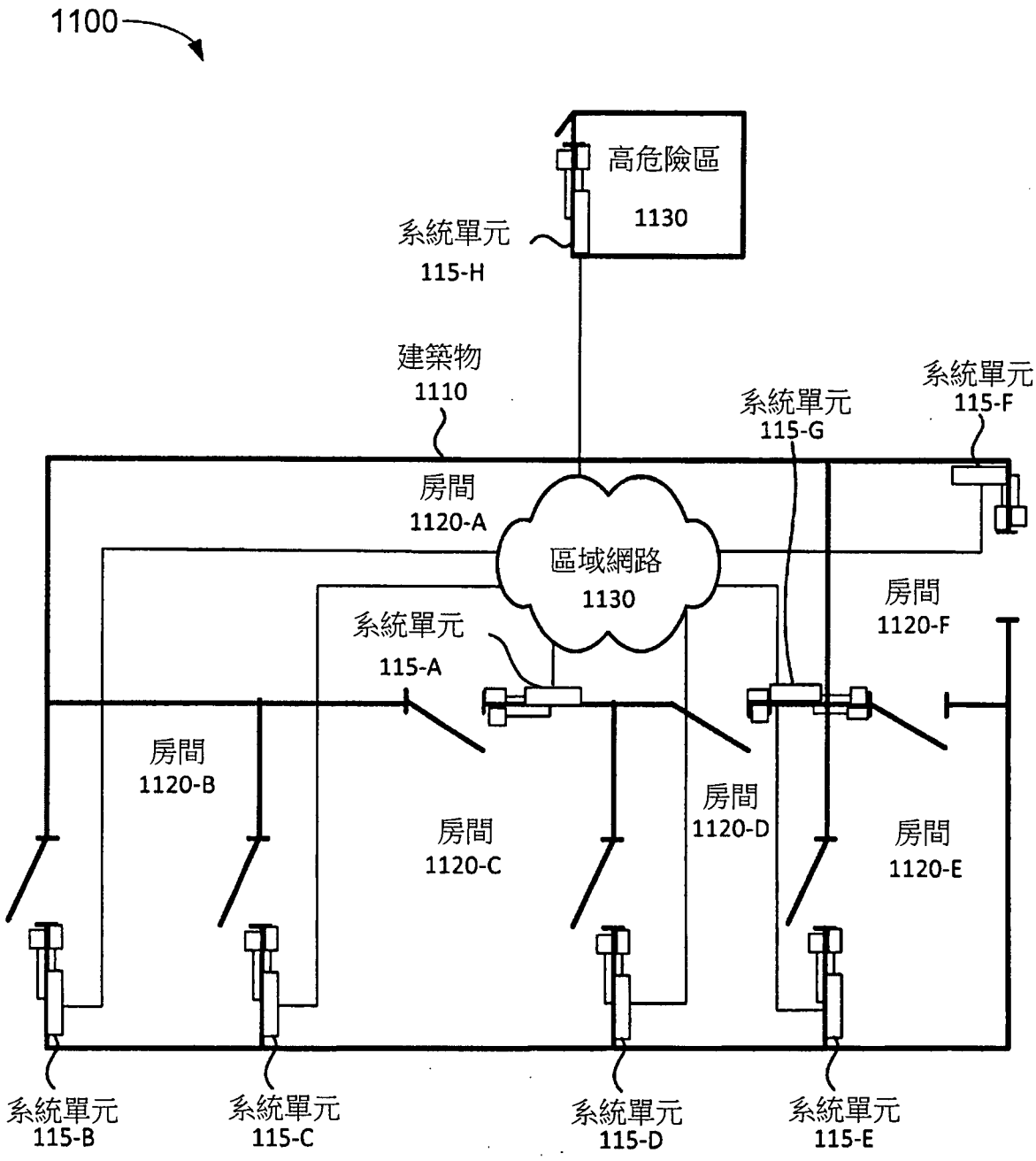
1100
高危險區
1130
系統單元
115-H
建築物
1110
系統單元
115-G
系統單元
115-F
房間
1120-A
區域網路
1130
房間
1120-F
系統單元
115-A
房間
1120-B
房間
1120-C
房間
1120-D
房間
1120-E
系統單元
115-B
系統單元
115-C
系統單元
115-D
系統單元
115-E

圖 11

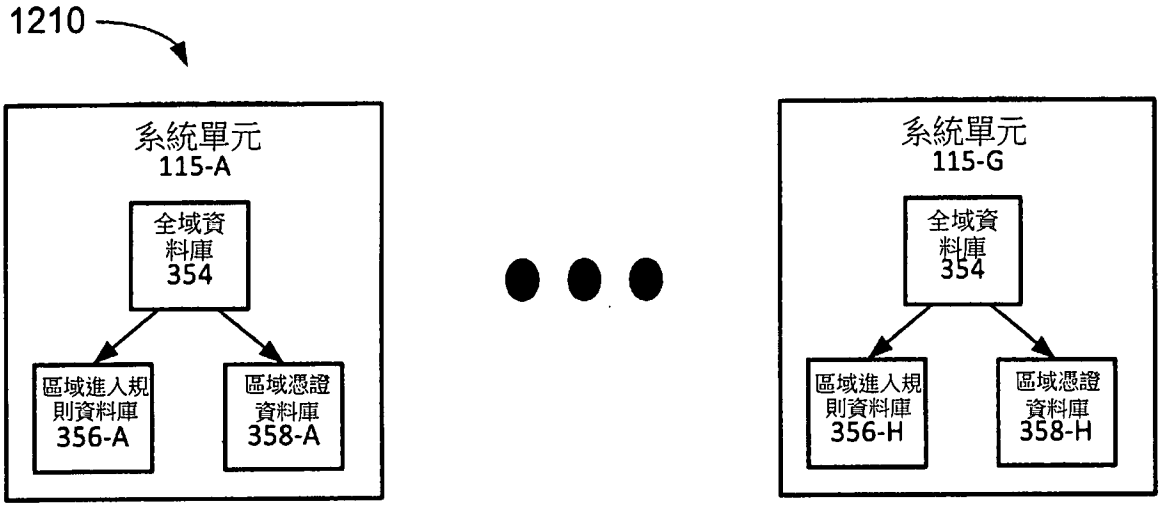
1210
系統單元
115-A
全域資料庫
354
區域進入規則資料庫
356-A
區域憑證資料庫
358-A
系統單元
115-G
全域資料庫
354
區域進入規則資料庫
356-H
區域憑證資料庫
358-H

圖 12A

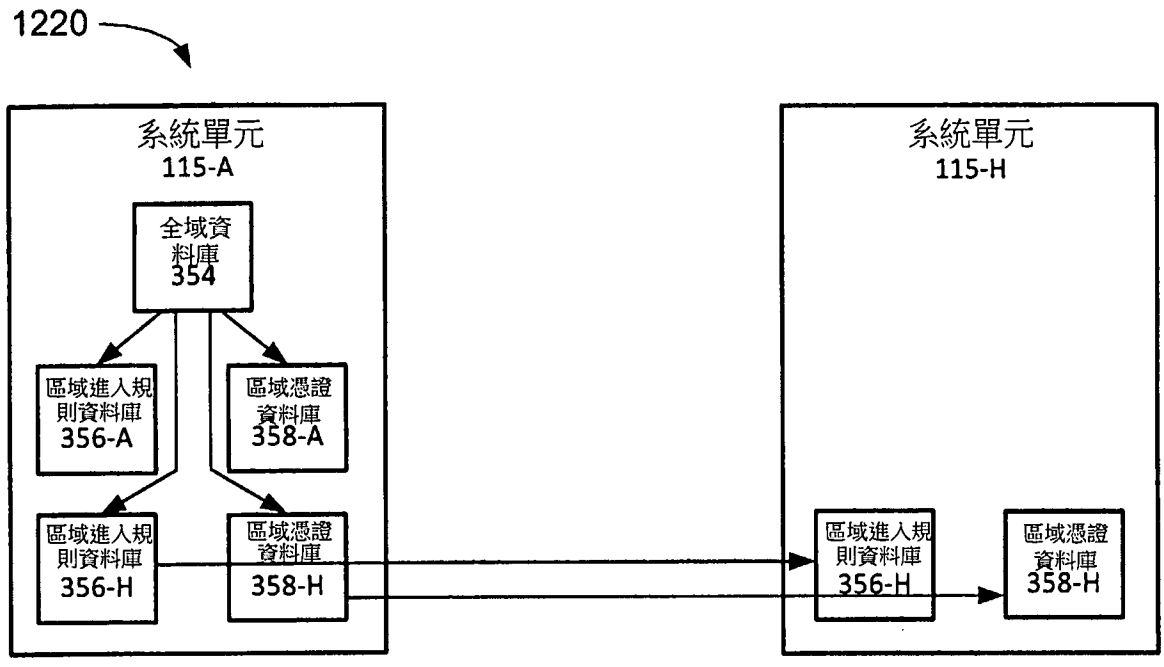
1220
系統單元
115-A
全域資料庫
354
區域進入規則資料庫
356-A
區域憑證資料庫
358-A
區域進入規則資料庫
356-H
區域憑證資料庫
358-H
系統單元
115-H
區域進入規則資料庫
356-H
區域憑證資料庫
358-H

圖 12B

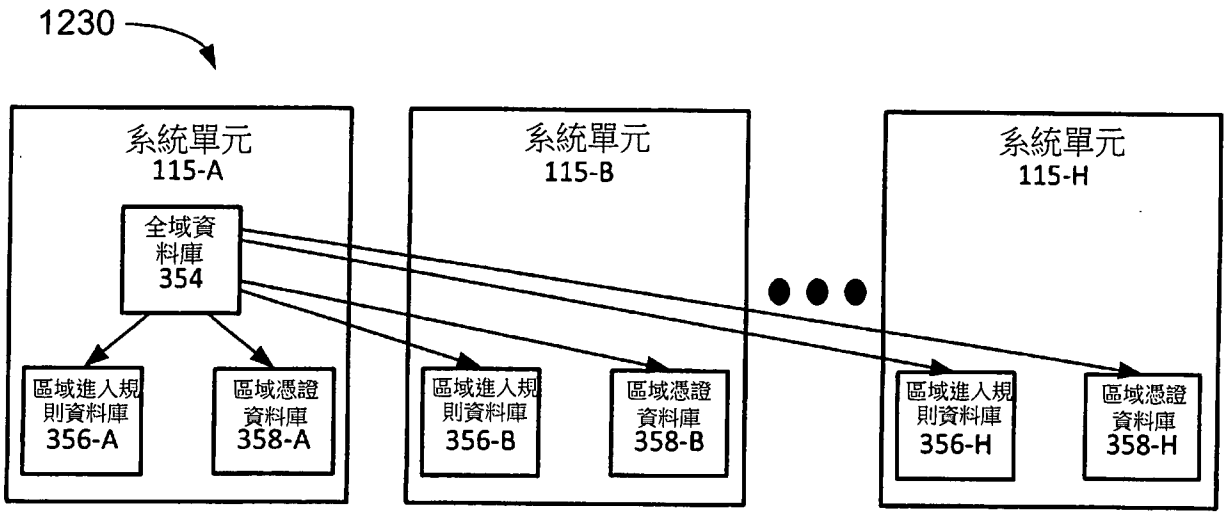
1230
系統單元
115-A
全域資料庫
354
區域進入規則資料庫
356-A
區域憑證資料庫
358-A
系統單元
115-B
區域進入規則資料庫
356-B
區域憑證資料庫
358-B
系統單元
115-H
區域進入規則資料庫
356-H
區域憑證資料庫
358-H

圖 12C

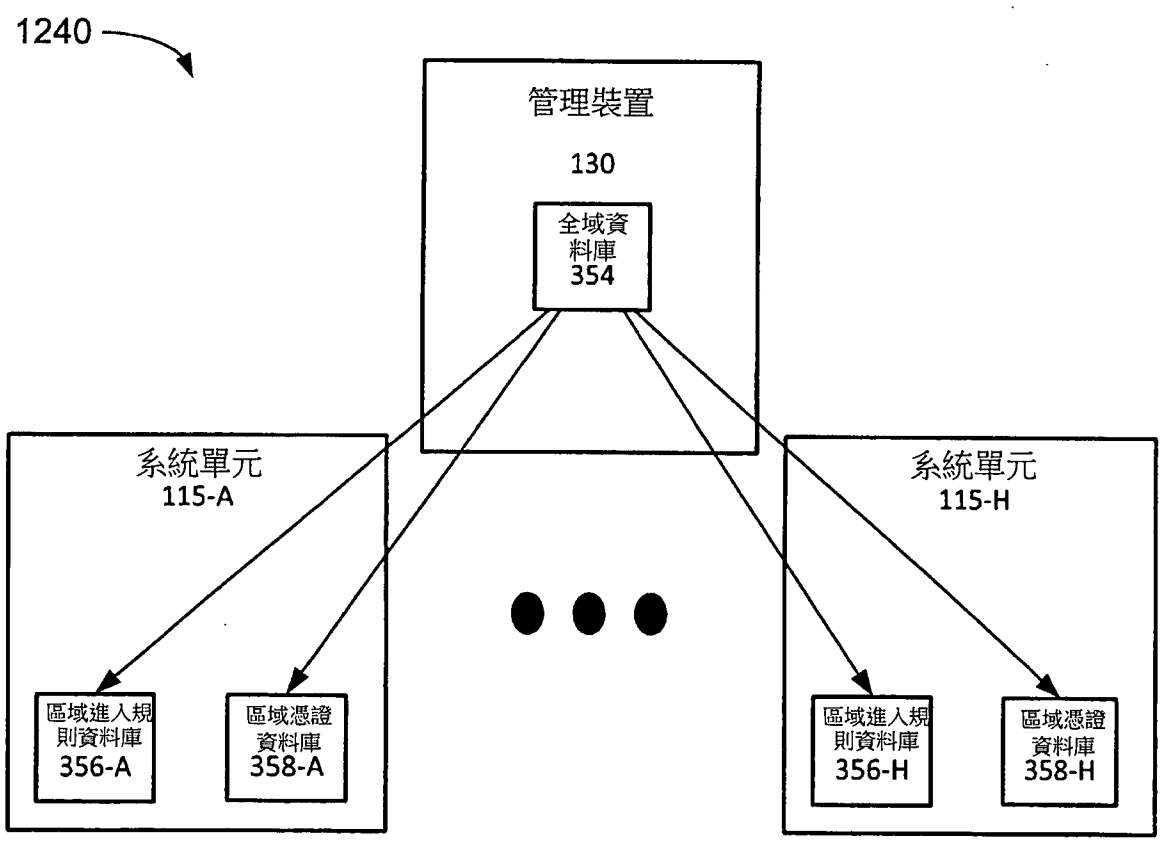
1240
管理裝置
130
全域資料庫
354
系統單元
115-A
區域進入規則資料庫
356-A
區域憑證資料庫
358-A
系統單元
115-H
區域進入規則資料庫
356-H
區域憑證資料庫
358-H

圖 12D

354

列	使用者	憑證類型	憑證值
21	傑克	卡	40APCE
21	傑克	個人識別號碼	1234
21	傑克	虹膜	虹膜掃描值
44	吉爾	指紋	指紋值
		⋮	

圖 13A

356-G

列	房間 E	8 AM 至 5 PM，卡
21, 55, 76	房間 E	非營業時間，卡+個人識別號碼
44, 55, 66, 78	房間 A	所有時間，虹膜
33, 44, 66	房間 A	5 PM 至 8 AM，卡+虹膜
	⋮	

圖 13B

358-G

列	卡雜湊	藉助 40ACPE 加密之密鑰
21	卡+個人識別號碼雜湊	藉助 40ACPE+1234 加密之密鑰
44	虹膜雜湊	藉助 44 之虹膜加密之密鑰
44	卡+虹膜雜湊	藉助卡+44 之虹膜加密之密鑰
	⋮	

圖 13C