門禁控制網路佈線安全技術的應用

張潯福

前言：

門禁系統是進出管理系統的一個子系統，通常它採用刷卡、密碼或人體生物特徵識別等技術，在管理軟體的控制下，對人員或車輛出入口進行管理，讓取得認可進出的人車自由通行，而對那些不該出入的人則加以禁止及干涉。由於門禁系統可以快速識別來人或車的身份，門禁系統十多年來它迅速地從各種可能衍變中發展出來，在使用上走入了住宅，進入了辦公大樓辦公室，停車場、捷運和旅館飯店的門口，都可以使用它來確認來訪者的身份。也可以說，在許多需要核對人車身份的處所門禁系統以成了不可缺少的配置項目。因此在弱電工程項目上，門禁以是安全防衛中一項獨特的工程技術，而門禁技術項目中又以聯網通訊技術數於比重較大部份，本刊就來探討一下這些門禁網路通訊實際應用的技術。

門禁系統應用模式有那些？

我們在探討門禁網路的施工應用技術前，因應門禁模式的不同，在進行網路與通信建構前當然要對門禁主要的模式先有一番認識與瞭解，這樣對於要談網路與通訊的技術就會較有架構的概念，在施工上也比較能掌握施工的方式要點。

門禁系統中的所有設備及配件在性能安全可靠運轉的同時，還應符合台灣或國際有關的網路安全標準，並可在非理想環境下有效工作。強大的即時監控功能和連動功能，充分保證使用者環境的安全性，門禁系統的技術不斷向前發展，用戶需求也在發生變化，因此門禁系統的設計與實施應考慮到將來可擴展的實際需要，亦即:可靈活增減或更新各個子系統，滿足不同時期的需要，保持長時間領先地位，成為智能建築的典範。系統設計時，對需要實現的功能進行了合理配置，並且這種配置是可以改變的，設置甚至在工程完成後，這種配置的改變

也是可能的和方便的.系統軟體根據開發商符合不同歷史時期市場的需求進行相應的升級和完善，並免費為相應的應用客戶進行免費的軟體韌體升級。同時，可以擴展為交通付費、支付系統、考勤系統、會議簽到系統、巡邏管理系統，就餐管理系統及醫病管理等一卡通工程等項目。

門禁系統結構和配置，大致上依功能管理結構模式可分為以下四種方式以利們禁網路工程應用施工參考：

模式一：單向感應式（讀卡器＋控制器＋出門按鈕＋電鎖）

使用者在門外出示經過授權的感應卡，經讀卡器識別確認合法身份後，控制器驅動打開電鎖放行，並記錄進門時間。按開門按鈕，打開電鎖，直接外出。適用於安全級別一般的環境，可以有效地防止外來人員的非法進入。是最常用的管理模式。

模式二：雙向感應式（讀卡器＋控制器＋讀卡器＋電鎖）

使用者在門外出示經過授權的感應卡，經讀卡器識別確認身份後，控制器驅動打開電鎖放行，並記錄進門時間。使用者離開所控房間時，在門內同樣要出示經過授權的感應卡，經讀卡器識別確認身份後，控制器驅動打開電鎖放行，並記錄出門時間。適用於安全級別較高的環境，不但可以有效地防止外來人員的非法進入，而且可以查詢最後一個離開的人和時間，便於特定時期（例如失竊時）落實責任提供證據。

模式三：卡＋密碼式（讀卡器＋控制器＋出門按鈕＋電鎖）

刷完卡後，必須輸入正確的密碼，才能開門。密碼是個性化的密碼，即一人一密碼。這樣做的優點在於，用於安全性更高的場合，即使該卡片給人揀到也無法進入，還需要輸入正確的密碼。並且可以方便地進行模式的設置，例如對於同一個門，有些人必須卡＋密碼才允許進入，有些人可以刷卡，無需密碼就可以進入，特定的人輸入密碼即可放行。

模式四：卡＋密碼＋時間段（獨立門禁主機＋出門按鈕＋電鎖）

該模式無需要再外接讀卡器，讀卡器與控制器集成。開門方式分為：1卡＋時間段2密碼＋時間段3卡＋密碼＋時間段。

從上述四種架構我們可以清楚瞭解到不管是那一種模式，設備的架構大致上以就是這些部份，這些部份的連線方視與連網安全就關係到整個們禁系統的應用安全，當然過去也有很多使用者與廠商都表示，門禁不過就是一個區域性的封閉線路或網路環境，何來入侵安全顧慮，這話在過去當然無可厚非，但在今日現階段一切都講求遠端制控及網路IP化的今天，套一句在網通界最常說的話〝只要系統走上網路化就無所謂絕對安全可言〞，可見網路應用安全在門禁系統也是不可忽式的部份，接下來就讓我們來看看門禁工程網路通訊上的有無線傳送結構與網路應用安全的關係。

門禁系統通訊工程原理與網路佈線原則

門禁系統的通訊原裡與其它自動控制系統或智能樓宇系統的原理基本類似，它的運行可以分為傳感、管理和執行三個環節，只是它比較緊湊，比較簡單而已。

傳感：讀卡器、密碼鍵盤、各種生物識別器、出門按鈕、鎖狀態傳感器都屬於傳感器件，它們的任務是接受命令，將信號上傳或在核對後上傳（生物識別器）。

管理：控制器和管理軟體承擔著門禁系統的管理功能，它們在收到傳感器發來的資訊後，根據時間、卡號及其它資訊對是否開門做出判斷，如果開門，則發出開門命令給電鎖。而在收到鎖狀態傳感器時，則開始計時，超時則報警。

執行：電鎖在收到開門或關門的命令（供電或斷電）時，它〝執行〞命令將工作狀態調整到與命令一致。而電鎖內的鎖狀態傳感器則起到了反饋和監督的作用。

有些控制器可以使用繼電器（或其他觸點開關，俗稱乾接點）將控制信號輸出，以控制聯動的攝影機及緊急防盜照明燈。

門禁系統的傳輸線路

由上述工作原理可知，在門禁系統中有以下幾種傳輸線路：

- **電源線：**門禁系統的電源大多來自機房的UPS，以免在現場突發性斷電時造成開門的誤動作。電源線通常會處於220V交流傳遞的方式，目的是減少電源線上的壓降。在控制器旁，配備有穩壓電源，將交流220V

電源變換成直流12V電源，分別供給控制器和電鎖。門禁系統用的電鎖絕大多數屬於12V直流供電方式。在電鎖開斷的瞬間，由於電鎖中線包（電磁鐵線圈）的作用，會在電源線上產生很強的電流，它容易引起電源波動，而這一電源波動對控制器的穩定工作極其不利，所以在可靠性要求比較高的門禁系統中，控制器與電鎖分別使用不同的電源模組，即220V交流供電到控制器時，使用兩個12V直流的電源模組各自整流/穩壓後，分別供給電鎖和控制器。各種電源線的選用基本上都是基於電工手冊，選用標準的電源線。

- **控制器訊號線：**控制器中有三組信號線，分別連接到讀卡器、電鎖中的鎖狀態傳感器和出門按鈕。這三路信號線可以使用綜合佈線中的雙絞線替代。為了避免空間的電磁干擾，讀卡器信號線應採用隔離線，另兩種信號線則可以採用隔離線，也可以採用非隔離線。
- **遠端網路訊號線：**從控制器到管理電腦之間，有一根信號線，它的傳輸協議大多是RS485，在距離近的時候則可能是RS232（以減少一個RS232/RS485轉換器），在要求傳輸速率快的時候，則採用TCP/IP協議，使用以太網傳輸。這三種協議都可以使用雙絞線，只是在RS485或RS232傳輸時，基本上在門禁控制器的產品手冊中都要求採用隔離線。為了避免電磁干擾，這根信號線應採用屏隔離絞線。當控制器需要使用輸出乾接點直接控制錄影機（在刷卡開門時同步錄影）時，這根控制線（2芯）宜採用隔離線，以免因錄影機輸入信號幅值小的時候因電磁干擾而引起誤觸發。但如果是用乾接點直接傳輸照明燈的電源時，則應該採用電源線。根據上述分析可知，在傳輸電源（為電鎖、控制器和照明燈供電）時，應採用電源線，其截面積可以根據電流所產生的壓降和發熱計算，也可以查電工手冊獲得。在傳輸傳感器信號和控制信號時，應該根據讀卡器和控制器的安裝手冊，選擇隔離線或非隔離線。隨著門禁系統鎖控制的門數越來越多，對系統網路傳輸速度與佈線安全的要求也就越來越高，而且從事門禁系統的施工也比須同時進行綜合佈線系統的施工，因此使用網路雙絞線作為門禁系統的傳輸線，已經成為門禁系統的線纜主要選擇。根據對各種門禁線纜的分析，讀卡器、控制器、管理電腦之間的信號線和控制線都可以使用網路雙絞線。

在同時進行門禁系統與綜合佈線的案例中，距離如果短於20米的網路雙絞線往往不符合綜合佈線工程中的利用價值，成為工程廢線。但這些短距

離的線材，對於分佈式安裝的控制器而言，出門按鈕信號線、讀卡器信號線和鎖狀態信號線都卻往往都是利用這些廢線來做為佈線的。對於使用TCP/IP協議的遠端網路信號線，必然是使用雙絞線傳輸，它完全可以使用綜合佈線系統的標準星型結構實現信號遠傳。RS485線和RS232線也可以使用網路雙絞線，根據門禁控制器的安裝原則，這些設備應該採用隔離雙絞線，以免電磁干擾造成誤動作。

門禁系統中網路應用綜合佈線注意事項

在使用綜合佈線系統作為門禁的傳輸線路時，應該注意以下因素：接線方法應完全按照各種門禁設備上的接線規則，並保留詳細的接線圖，以免維護時判斷線路時的痛苦。隔離雙絞線的隔離層應根據讀卡器、控制器的安裝手冊完成接地。

如果使用網路屏蔽雙絞線傳輸TCP/IP，則可完全採用隔離佈線系統的隔離層端接規則。當使用TCP/IP協議時，最好不要與其他AI智慧系統（包括辦公自動化系統等軟體系統）共用網路交換機，即為門禁系統單獨配備網路交換機，以免因協議衝突發生傳輸上的意外。當使用網路TCP/IP協議時，可以將門禁系統的管理電腦認為是門禁網路中的一台伺服器，使用雙絞線或光纜連接到配線架上。總成佈線系統可以用於門禁系統，這一點已經為門禁系統的供應商和安裝商所證實，只是在工程中應全面評估造價、施工和性能，以求達到最佳的效果。

門禁系統傳輸有無線網路安全應用原則

無線門禁產品從誕生到現在，經過技術的不斷演化已經出現了通過FSK、GPRS、藍牙、ZigBee還有一些如SigFox低功耗長距離傳輸等傳輸方式的產品。而隨著物聯網技術的興起，物聯網門禁產品受到了安全產業的普遍關注。如同前二段落所述；傳統的門禁解決方案通過布置到每個門點的線纜進行聯網和控制。但是隨著項目的一個展開，越來越多的業內同行及客戶開始意識到了有線聯網系統自身存在著線纜眾多，安裝施工麻煩。例如，傳統的鎖具（電插鎖，磁力鎖）既不美觀，可靠性也差、斷電後無法使用、維護麻煩等方面的缺陷。因此許多有實力的門禁企業都在探索既能滿足安防系統對門禁的苛刻要求，又能避免目前有線聯網門禁系統眾多缺陷的新型產品，無線門禁逐漸開始被人們所認識並得到一定的應用。

人們選擇無線門禁產品，主要目的是希望減輕布線的復雜度。因為門禁具有集中管理的要求，每個門點都要和中心進行通訊，如果在門禁點和中心之間選擇無線通訊，則可以省掉過

多門禁點和中心的通訊線，這在有些布線不便的場合具有很大的吸引力。第一代無線門禁就是在以上的技術背景下誕生的，這類設備主要是通過一些國家的自由頻段進行通信規定，採用的通訊技術也相對簡單，一般采用FSK或FMK等基本的無線調制方法，頻點固定，多設備一起工作時會有互相干擾，通訊速率也較低，一般在300bps到1200bps之間。因為技術手段相對單一，在使用中普遍存在通訊穩定性和可靠性欠佳的問題，這類產品目前已逐步淡出了市場。手機無線門禁概念是伴隨著手機技術的發展而提出的，因為第一代無線門禁在通訊和傳輸距離上無法滿足一些特定場所、行業的需求，因此，部分門禁廠家將手機模塊和門控器綁定在一起，控制信號通過聯通、移動的網絡通過短信或GPRS進行無線傳輸，以達到遠距離信號傳輸的目的。但是手機無線門禁由於設備成本、手機月租費等相關費用的收取，使用成本較高，同時信號通過GSM網絡傳輸延遲較大，性能也不夠理想（通訊速率一般只能達到20-40kbps，並且速度不穩定），使得手機無線門禁產品目前僅局限在有一定需求的場合、行業中使用。

與此同時，應用了無線物聯網技術的無線物聯網門禁系統也受到了市場上的普遍關注，據行業預測物聯網已成為與互聯網一樣改變人們生活的技術，而將物聯網技術應用到無線門禁中去無疑是搶占了未來無線門禁技術的高地，市場前景將會十分巨大。和單純採用藍牙、ZigBee技術進行信號無線傳輸的無線門禁不同，物聯網門禁更側重於門禁的智能感知和低功耗，藍牙和ZigBee雖然也是低功耗短距無線傳輸的技術，但應用在電池供電的物聯網門禁系統裏還是太費電。

無線物聯網門禁系統：無需布線、可靠、節能

門禁系統從誕生的第一天開始就伴隨著大量的佈線，一個完整的門禁系統由讀卡器、控制器、電鎖、出門開關、門磁、電源、管理中心這八個模組組成，每個模組都需要聯線。同時，門框的正反面和頂部、門的頂部都要打孔安裝設備，因此，施工繁瑣是很直觀的問題。無線物聯網門禁將門點的設備簡化到了極致：一把電池供電的鎖具。除了門上面要開孔裝鎖外，門的四周不需要安裝任何輔助設備。整個系統簡潔明了，大幅縮短施工工期，也能大大降低後期維護的成本。

跳頻、加密是無線門禁的另一個核心。無線和有線一個很大的區別就是無線信號是在空中傳播的，因此很容易受到外界的干擾，同時也很容易被外界所捕獲。因此安全性與可靠性可以說是無線門禁產品的生命線。無線物聯網門禁系統的安全與可靠主要體

現在以下兩個方面：無線數據通訊的安全性保證和傳輸數據的穩定性。無線物聯網門禁系統通過智慧跳頻技術來確保信號能迅速避開干擾，同時通訊過程中採用動態密鑰和AES加密算法，哪怕是相同的一個指令，每一次在空中傳輸的通訊封包都不一樣，讓監聽者無法截取。但是，對於無線技術來講，數據包加密技術大家能理解並接受，而無線的抗干擾能力卻是始終繞不開的話題。針對這一問題，無線物聯網門禁專門設計了脫機離線工作模式，這是一種確保在無線受干擾失效或者中心系統當機後也能正常開門的工作模式，以無線門鎖為例，在無線通訊失敗時它等同於一把不聯網的鎖，仍然可以正常的開關門（和聯網時的開門權限一致），用戶感覺不到離線和連網的區別，唯一的區別是離線時刷卡數據不是即時傳到中心，而是暫存在鎖上，在通訊恢復正常後再自動上傳。無線物聯網是一個超低功耗產品，這樣會使電池供電的壽命更長；只有電池供電，才有徹底無線的可能。無線物聯網門禁系統的通訊速度達到了2Mbps，越快的通訊速度意味著信號在空中傳輸的時間越短，消耗的電量也越少，同時無線物聯網門禁系統採用的鎖具是只在執行開關門動作時才消耗電量的。無線物聯網門禁系統可以直接替換現有的有線聯網或非聯網門禁系統。對於辦公大樓系統，應用無線物聯網門禁能明顯降低施工工作量，降低使用成本；對於旅館系統，能提升門禁的智慧化水準。但任何新生事物，市場上難免存在一些質疑聲，但隨著無線連網系統技術的穩定性、可靠性、安全性越來越成熟下。相信隨著物聯網技術的推廣和無線物聯網門禁案例的一個個展開，無線物聯網門禁系統將得到工程商與用戶的喜歡與信賴。

結論

從本質上看，安全、通信、IT這三大產業都是對門禁系統資訊的處理過程，而且都共同朝著網路平台化的方向去發展，那麼這三大門禁網路技術一定會成為門禁網路通訊的安全技術核心。 門禁在網路應用上的安全威脅不多，大致上來自於像後門或特洛伊木馬程式（Trapdoor/Trojan Horse）：未經授權的程式，可以透過合法程式的掩護，而偽裝成經過門禁授權的流程，來運行程式，或是竊聽（Sniffer）：使用者之識別資料或其他機密資料，在網絡傳輸過程中被非法的第三者得知或取得重要的門禁資訊及最後一種偽裝（Masquerade）：攻擊者假裝是某合法使用者，而獲得門禁使用權限。但這些都是在門禁網路化上不可避免的風險，以唯有在門禁網路工程施做及架構應用上做好最佳的選則才是安全上策。