高科技廠辦之物聯網門禁管理系統

手機取代卡片感應開門，算不算物聯網門禁? 將門禁管理系統安裝在雲端，算不算是物聯網門禁?高科技廠辦已使用門禁系統數十年，因應管理上的需求，也多是聯網型的門禁設備，那算不算物聯網門禁? 本文提供讀者一些評估的角度，讓讀者有能力分析此類問題。

我先描述高科技廠辦門禁系統與其他系統聯動的一些情境。

消防法規規定，火警發生時，緊急用升降機及防火門，若有安裝門禁管制設備，應當解除管制。最簡單的實現方式為門禁系統與火警警報整合，當火警發生時，將所有門禁管制解除。若門禁系統進一步與逃生指示系統整合，不僅可以將逃生路線的門禁管制解除，更可控制門禁管制設備發生聲響，便於逃生路線辨識。一方面有助逃生，一方面精準解除門禁，避免有心人士趁火打劫。

有進出高科技廠辦經驗的讀者應該都知道，進廠前手機鏡頭要用資安貼紙貼起，離場後才可撕去。如果門禁系統與手機資安管理系統介接，刷卡進廠自動關閉手機相機功能，刷卡離廠自動恢復手機相機功能，無須人員介入操作。不僅可減少人力成本，降低人員操作疏忽，更提高資安管理品質。

一般門禁管制都是管制人員進出，人員靠卡感應或是使用生物特徵辨識。當工廠高度自動化後，到處充斥著自動搬運車或是移動機器人，這些設備無法靠卡也無生物特徵，如何通過該些門禁管制點?若門禁系統與工廠自動化系統整合，便可於設備到達門禁管制點時，自動開門。無須為該些設備另設通道或加設警衛人員，且不降低人員進出的管制功能。

極少人員進出的高安全管制區域如機房，可以啟用監視系統的移動物偵測功能。若有不法份子非由門禁管制點進入該區域，移動物偵測警報可對 ECC 提出告警，並利用門禁設備現場告警，同時要求警衛人員一定到現場處理。但有人員刷卡合法進入該區域時，便要關閉該區的移動物偵測以避免產生誤報。這便是門禁系統與監視系統的整合應用。

萬物聯網，各系統間整合以解決企業問題。這才是高科技廠辦物聯網門禁的精髓。

企業管理隨著營運變化，各系統間需要整合解決的問題也隨之變化。一套門禁系統使用年限至少 10 年，我們雖然知道公司當前系統整合要求，卻難以預測十年後的整合需求。所以，因應系統需適應各種不同的需求，物聯網門禁的評估角度，可由下列方式考慮。

開放式的平台設計

傳統的門禁管理系統，基於安全的考慮，均設計為封閉的系統。不僅某廠商的門

禁管理系統僅支援該廠商的門禁設備。若需要與其他系統進行物聯網整合，還需要原軟體廠商進行客製化。這樣的門禁系統，就算目前介接整合許多異質系統，都屬於封閉架構，不能稱之為物聯網門禁。

門禁管理系統二次開發的完整性影響著解決未知整合需求的能力。首先，門禁管理系統應提供異質系統整合的應用程式開發介面。以目前最開放的標準介面技術而言，應該以 Web API 為介接技術，至少須提供人員(卡片)管理、進出權限管制、設備門鎖控制的 API。再者，門禁系統應在不影響效能的前提下，提供取得系統即時訊息的擴充技術，其中訊息至少需包含設備斷連線、刷卡、告警等。第三，系統應以業界通用的資料庫為資料儲存媒體，並應提供資料庫說明文件，以便對資料的二次開發應用。最後，門禁系統是否考慮不同廠商門禁控制器的兼容性。現今產業併購盛行，不同公司若原使用不同硬體供應商的門禁設備，門禁系統亦無兼容性，彼此間的軟硬體完全不相容，便會面臨無法整合，需全區汰換的難題。

資訊安全的設計考慮

傳統的門禁管理系統，基於實體安全的考慮，大多實現在實體隔離的環境中。2016 年某銀行 ATM 盜領事件明確的告知我們，就算如銀行般高度封閉的網路環境，也有可能因為國外某分行的庶務設備被駭客入侵，導致安全環境中存在的不安全電腦系統遭受攻擊，產生巨大損失。物聯網門禁系統因為與其他系統整合的需求，已經不可能建置在一個完全實體網路隔離的環境，門禁系統掌握人員進出管制的實體安全，若遭入侵，不可能的任務：鬼影行動中監獄遙控開鎖的情節便會出現在現實生活中。

門禁管理系統應該遵循程式設計的資安要求，防止 SQL Injection，Cross-site scripting (XSS)的資安攻擊。同時，開發過程中，必須使用第三方的弱點掃描程式偵測原始碼，並修改具有高資安風險的程式碼。物聯網門禁系統須與其他許多系統聯網互動，針對不同的系統介接，除了可設定何系統可介接外，尚需要能設定該系統可介接的功能為何，可介接的門禁管制點有哪些，並且針對重要功能的介接呼叫須留下稽核紀錄。

因為篇幅及才學限制，筆者僅針對較熟悉且重要的角度來評估高科技廠辦的物聯網門禁系統，希望對讀者能有實際的幫助。