

高效能門禁管理系統功能-以企業應用為例

『門禁』一言以蔽之，就是管制何人何時可以進出何出入口。如此一個看似簡單的需求，產品已經應用在市場上超過 30 年的系統，所有的功能應該都是老生常談，能有新的功能定義？其實門禁需求並沒有改變，然管理需求因為資訊技術、硬體技術、用戶規模、商業模式的改變而對門禁功能有了新的定義。『門禁』原始需求雖然簡單，但是要精確達到『有權進出的人員可以無礙進出，無權進出的人員無法進出』這個需求，到底需要付出多大的成本？在付出認為的成本後，門禁安全等級又提升了多少？日後對於維持此安全等級又需要持續投入多少維運成本？本文，我以『限制理論』的『衝突圖』做為起點，從擁有成本及安全等級的角度，來定義一個高效能門禁管理系統所需功能。

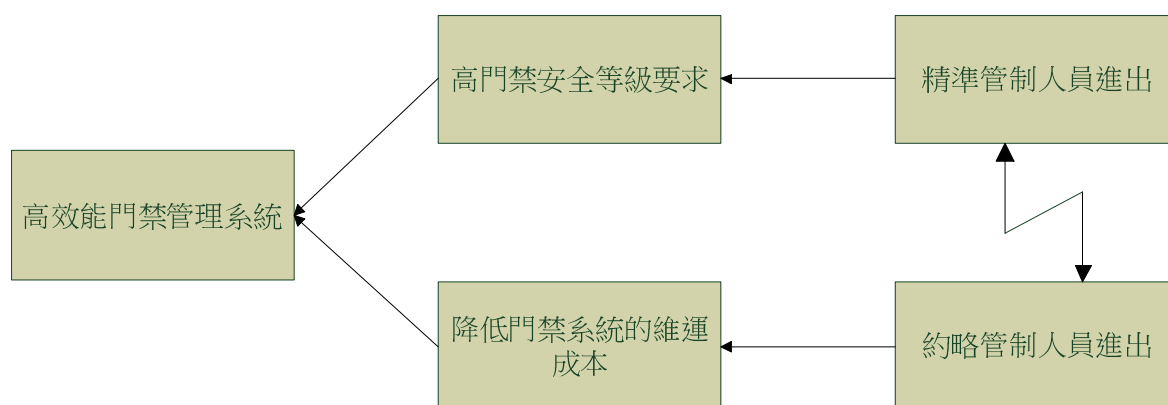


Figure 1 高效能門禁管理系統衝突圖

1 擁有成本

擁有一個門禁系統的總成本可分為採購成本與維運成本。採購成本為一次性費用，就是企業採購門禁系統的實際價格，此成本明確。維運成本為長期性不間斷的費用，就是企業為了門禁系統持續運作所投入的人力與物力，包含但不限於，操作門禁系統所花的人力成本，有權進出者刷卡無法開門所浪費的時間成本，檢查門禁異常所投入的人力成本。因為維運成本難以定量估計，常常被忽略，但對於長期使用門禁的企業而言，經年累月維運成本的累積卻是最大的成本負擔，遠遠高於當初的採購成本。筆者整理出能有效降低維運成本的重要功能。

1.1 各資訊系統連結自動化的系統

門禁管理系統會與多少企業內部的資訊系統有關聯？完全無關的看法，就是把門禁系統看成資訊的孤島，資訊完全獨立，不與外界溝通或僅有限溝通。如此，門禁管理系統的維運成本十分昂貴，花費相當多人力，資料錯誤百出，門禁安全性卻極低，產出效果十分有限。

筆者以為門禁管理系統應與 HR 系統、簽核系統、差勤系統、企業入口網站等關聯，如此方可發揮門禁管理系統的最大效益。系統之間的連結以自動化為唯一選擇。系統自動化便可降低人為操作，一來減少人員操作成本，二來降低人員操作的錯誤。系統自動化是降低維運成本最重要的方法。

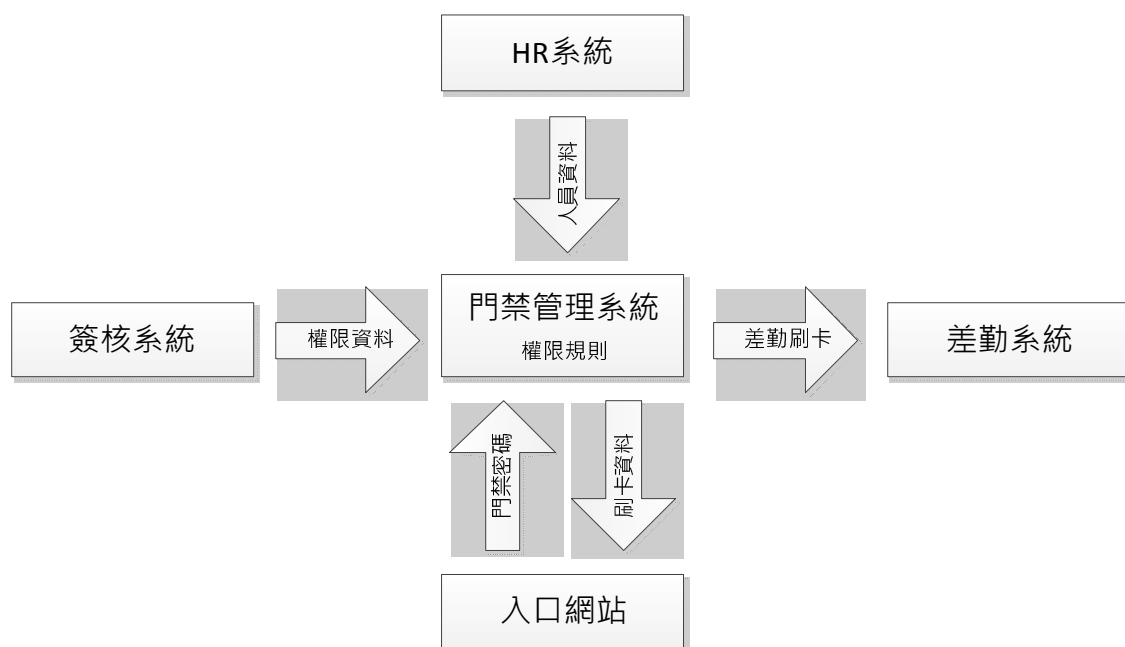


Figure 2 門禁管理系統與資訊系統關係圖

1.1.1 與 HR 系統的自動化連結

當企業有新進人員到職時，人事管理員會將新進員工的人事資料，工號、姓名、卡號、部門、職稱、性別...等，輸入 HR 系統。此時，門禁系統應依照新進員工的部門、職稱、性別...等資料，自動且及時的於到職日依權限規則開通該員預設有權進出的出入口權限，讓該員可進出自己的部門及公共區域，也可持卡做差勤刷卡及用餐刷卡。反之，當人員離職時，人事管理員在 HR 系統中標註離職。此時，門禁系統應該自動於離職日關閉該離職員工的所有門禁、差勤及用餐權限。此權限開通或關閉過程

是及時且完全無需人員操作，此便是 HR 系統與門禁系統的自動化資料連結，既精準管制人員門禁權限又降低管理成本。

1.1.2 與簽核系統的自動化連結

當人員因為工作需要額外開通某些出入口權限時，會使用企業的門禁申請簽核流程，該流程可能是電子簽核流程。當門禁權限被核可後，門禁系統應該自動且及時開通該員申請的出入口權限。此權限開通過程是及時且完全無需人員操作，此便是簽核系統與門禁系統的自動化資料連結，既精準管制人員門禁權限又降低管理成本。

1.1.3 與差勤系統的自動化連結

刷卡除了作為門禁管制外，一般也作為差勤上下班的打卡依據。傳統上是利用文字檔將差勤刷卡資料以批次方式匯入差勤系統。此種方法，無法讓管理人員及時掌握員工的出缺勤狀態，無法做到即時管理的效率要求。門禁管理系統應該將差勤刷卡資料即時寫入差勤系統中，如此便是差勤系統與門禁系統的自動化資料連結，既精準取得差勤資料又降低管理成本。

1.1.4 與企業入口網站的自動化連結

企業內部入口(Portal)網站，整合企業內常用網路資源。入口網站與門禁系統有何關係？入口網站可以顯示員工最近差勤及用餐刷卡紀錄，因為刷卡資料的及時收集，員工便可以在第一時間做自我差勤管理或反應差勤異常，完全無須人事管理者手動通知。

在高安全區域出入口，會啟用刷卡+密碼的雙重驗證功能。員工個人進出密碼如何輸入系統？傳統上是交由他人代為輸入，此種方式毫無安全等級可言。應可透過企業入口網站，讓員工設定自己的門禁密碼，此便是企業入口網站與門禁系統的自動化資料連結，既提高門禁安全又降低管理成本。

1.2 穩定的系統

穩定的系統不容易發生異常，異常處理成本也較低。但穩定並非定量名詞，不易評估。所以常常聽到廠商讚美自己的門禁管理系統很穩定，但是客戶卻常常抱怨自己的門禁管理系統不穩定。本文，我們藉由說明系統必須具有哪些功能，才可以提供穩定的系統，希望能給穩定一詞提供可評估的方法。

1.2.1 系統自我健康管理

門禁系統是由門禁控制器、線路及管理系統組合的 7*24 系統。門禁管理系統應隨時監視門禁控制器及線路的健康情形，當門禁控制器斷線、故障或是刷卡資料異常時，管理系統應該自動及時的通知管理人員處理並留下事件紀錄。同時，對於門禁系統的錯誤，應提供事件紀錄，以利維護人員做診斷異常。如此可以降低管理成本，提高設備的妥善率。

1.2.2 線路品質的容錯設計

線材、干擾、佈線均影響著門禁管理系統與門禁控制器之間的通信。當線路品質十分惡劣時，管理系統與控制器之間的通信中斷，自然由人員維修線路。但當線路品質不良，線路斷斷續續時，管理系統應還能正常運作，考驗著門禁系統線路品質的容錯能力。

線路品質不良導致人員權限資料下載到控制器失敗，管理系統應有自動重新下載機制，以保持門禁控制器中的人員權限正確。管理系統應隨時偵測門禁控制器連線狀態，當門禁控制器連線恢復時，自動接續收集刷卡資料，無須人為介入操作。同時，管理系統不應因控制器斷線產生效率不彰的情形。

1.2.3 刷卡資料二階段提交的接收機制

常常聽到企業用戶反應，持卡人認為有刷卡，但是管理系統中卻查無刷卡紀錄，這便是刷卡資料丟包問題。減少刷卡資料遺失，便能降低管理成本。

刷卡資料從刷卡到管理系統經歷過感應讀頭、門禁控制器、線路、最後才到管理系統，任何一個環節閃失都會造成刷卡資料的遺失。門禁系統與控制器之間的刷卡資料接收，應該當管理系統確實將刷卡資料儲存到資料庫後，再下指令將刷卡資料從門禁控制器中移除。這便是兩階段提交的接收機制。

另外，可能因門禁控制器的問題，在控制器記憶體中有些刷卡資料便已經毀損。此時。管理系統收到此些毀損的刷卡資料，應將此類刷卡紀錄另外存檔，而非丟棄忽略。丟棄忽略毀損的刷卡資料，也有可能造成刷卡資料丟包的問題。

1.2.4 有權卻無法進出的自動修復機制

常常聽到門禁持卡人抱怨應該有權進出某出入口，但是刷卡卻無法進出。或是，昨日還可刷卡進出，今日卻無法刷卡進出。假設門禁管理系統中，該人員的進出權限設定是正確的，那便是應該存在門禁控制器中的該人員卡號權限不在控制器中。有可能是因為權限下載當時，控制器剛好發生斷線，導致下載失敗。也有可能是因為門禁

控制器誤將該人員卡號權限刪除。不管發生原因為何，該人員已發生刷卡無法進出的異常，接著是找總務人員處理及發牢騷的時間。穩定的系統應可自行排除此問題，如此可減輕總務人員的負擔，降低維運成本。

1.3 具企業管理思維的系統

企業管理思維是指企業針對門禁管理時會採用的管理方式。

1.3.1 以人為本的進出管理

門禁進出管制的管理主體應該是『人員』而非『卡片』。反映到應用實況，某人員有權進出某門，並不應因為該門鎖的辨識方式(生物辨識、鑰匙、卡片)不同而有不同。當有權人員持有某卡片時，該卡片在該感應控制器上便代表該人員，而有權進出。若人員今日領用臨時卡，無需重新設定臨時卡的權限(因為是同一人員)，僅做人員領卡動作，便可以使用臨時卡進出原有權進出的門，當歸還臨時卡時，該臨時卡便無法再進出任何一個門。

想像一下情境，假設您今天上班時忘記攜帶卡片，於是到總機處請領一張臨時卡，總機沒有開通進出權限的權利，僅有發給您臨時卡的授權。您拿著新領的臨時卡，權限可與原始員工卡相同，所有可進出的門依然可刷卡進出，所有不可進出的門依然受到管制。當歸還臨時卡時，該臨時卡便無法再進出任何一個門。這便是以人為本的進出管理。若您拿的臨時卡，僅能進出公共區域，便是以卡為本的進出管理。

1.3.2 一人多角色的進出權限及規則

人員有權進出某門，是因為工作扮演角色需要，而不是因為職務高低。而人員在公司中會同時扮演不同的角色。例如，研發副總，同時屬於研發人員及高階主管兩個角色。如果該副總為女性同事，又多一女性角色。而許多的角色共同決定該人員有權進出門的內定值。例外情形，再使用個別人員微調作業，調整該人員的個別門進出權限。如此機制，不僅當下可以正確指定人員允許進出的門，若搭配角色規則的應用，可以達到當人員因職務或部門異動，系統自動調整有權進出門。

1.3.3 多人同時管理的門禁管理系統

企業若有不同的廠區，可能會指定各廠區的門禁管理員，電腦機房或庫房也可能需要各自的門禁管理員。各自門禁管理員的存在是因為安全等級較高的需求。但是，每個管理人員擁有各自獨立的門禁管理系統，不僅增加管理成本，同時也降低門禁系統的安全等級。多花成本，卻產生事與願違的反效果，何故？若人員遺失卡片，各自獨立的門禁系統能否自動且及時收到停卡通知？當人員離職，各自獨立的門禁系統能

否自動且及時收到離職通知？管理越人工，安全漏洞越大。最好能夠在一套門禁管理系統便達到擁有各自管理空間的功能，如此便產生多人同時管理門禁的需求。

多人管理門禁的實現，必須考慮資料權限及系統部署的議題。一般持卡人可以使用管理系統設定自己的密碼，但是不可以設定別人密碼；甲區管理人員可以管理甲區門禁，不可以管理乙區門禁，這便是資料權限的設計。最好的部署為安裝一次後，其他電腦的使用者無需再安裝的單一部署。Web 版本的門禁系統，僅需安裝在主機端，各不同電腦的使用者端用瀏覽器便可使用門禁管理功能，完全符合多人管理的方便部署需求。

1.3.4 事先排定的概念

當員工已經確定 10 天後離職，何時可以將此離職資訊輸入門禁管理系統。如果可以在確認此訊息的當下輸入，但是 10 天後自動生效，應該是管理成本最低而且安全性最高的做法。當員工借用臨時卡時，便可輸入臨時卡借用起訖時間，時間一到臨時卡自動啟用或失效，也是一種事先排定的概念。

又例如，某甲因為專案支援的緣故需要在 5/10 到 5/15 進出某門。最好在排定專案支援時，便將某甲此期間門禁開放需求輸入門禁管理系統中。待 5/10 一到，某甲便可刷卡進出該門，5/15 一過該進出權限自動失效，期間再無須人為操作。這也是一種事先排定的概念。

1.3.5 排程服務

排程服務可以取代許多人工維護系統的常規操作。例如：人員資料匯入、卡機校時、卡號下載、移除事件記錄、截轉記錄、差勤資料檔案匯出、假日表跨年自動切換...等都可以設計為排程及手動操作兩種版本。平時由排程自動執行，降低管理疏失及成本。有特殊需要時可由手動執行，增加系統彈性度。

排程執行結果應可設定主動回報機制，可即時確認排程是否正確執行及執行結果。同時，排程執行結果應提供事件紀錄，以利事後查詢。

1.4 開放的系統

1.4.1 二次開發的完整性

商業環境是多變的。不管目前我們定義的門禁功能多麼符合當下需要，日後總會發生此時意想不到的功能需求。門禁管理系統二次開發的完整性影響著解決未知需求的能力。

門禁管理系統應提供異質資訊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 WebService API 為介接技術，提供完整功能的 API。

系統應提供不影響系統效能的方法，而可取得即時刷卡資料的擴充技術。

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，以便利對資料的二次開發應用。

1.4.2 不同廠商門禁控制器的兼容性

現今產業併購盛行。不同公司合併後，若原兩公司使用相同門禁設備供應商的門禁控制器，那麼整合無問題。然大部分的情形是分屬於不同硬體供應商的門禁控制器，彼此間的軟硬體完全不相容，這時業主面臨無法整合的難題。若不整合，日後系統維護成本變為 2 倍，也大幅降低門禁安全等級。

藉由整合不同廠商的門禁控制器於單一門禁管理系統中，不僅僅解決不同廠商不同門禁控制器機型的整合問題，降低管理成本，延長現有門禁設備使用年限，業主更可以根據不同的應用場合選用最適當的設備，任意搭配，不必增加管理成本。

1.5 高容量的系統

隨著企業規模不斷擴大，門禁管理系統規模也會不斷的成長。管理門數由數十門，成長為數百門。持卡人數由數百人，成長為數千人，甚至數萬人。在在都對管理系統的適用性提出嚴峻的考驗。

門禁管理系統複雜度與門數 * 持卡人數 * 管理者數 存在正相關。

門數	持卡人數	管理者數	門禁複雜度
10	100	1	簡易
10	1000	1	簡易
50	1000	1	標準
100	2000	2	些微複雜
200	5000	2	有些複雜
500	10000	3	複雜
1000	100000	50	極複雜

圖表 1 門禁系統複雜度比較表(以 50 門, 1000 持卡人, 1 管理者為標準計量)

系統越複雜，越不容易穩定。門禁管理系統對維運成本的影響，隨者系統複雜度提高而呈倍數成長。企業在選擇門禁管理系統時，應至少考慮未來 5 年企業成長的需求，選擇較目前需求高容量的系統。

1.5.1 高效率的系統

筆者曾經看過一套門禁管理系統，管理 30 台門禁控制器，執行在雙 CPU+4G 記憶體的伺服器上，該伺服器的 CPU 使用率一直保持在 70% 以上。顯然，此系統的效率有改善空間。

門禁管理系統的程式架構及設計，影響著門禁效能。雖然我們無法看到程式碼，但藉由 CPU 使用率，硬碟使用率，資料庫使用率的高低，還是可以評估出門禁系統的效率好壞。

同一功能，同樣門數、持卡人數、管理者數，系統使用的 CPU% 及硬碟使用率，大致反映出系統效率。低效率管理系統，需要較高的硬體規格方可達到相同執行速度。同時，低效率管理系統會讓硬體保持高使用率，容易讓硬體設備毀損，尤其是硬碟的傷害。

1.5.2 支援原生 64 位元的系統

64 位元作業系統搭配原生支援 64 位元的門禁管理系統可以使用超過 4G 的記憶體，管理系統可支援的門禁控制器數量將大為提升。同時，64 位元的資料庫系統效能也遠高於 32 位元資料庫系統。管理系統支援原生 64 位元，提供伴隨企業成長所需的 Scalability。

1.5.3 系統的使用實績

門禁管理系統的容量限制，很難從規格或操作介面上得知。規格上通常會看到支援台數無限制。是的，在程式設計上是無限制，但實際上我們想知道的數據是在多少門或是多少台門禁控制器下，該管理系統依然可以穩定的運作。規格及型錄是不會標示此數據的，僅能從管理系統的實際使用案例中去推估其容量限制。若考慮容量因素時，系統實際使用案例的參考十分重要。

2 安全等級

筆者討論了降低門禁管理系統擁有成本的一些重要功能，其中許多功能同時兼具有降低擁有成本，提高門禁安全等級的雙重功效，在此不再累述此些功能。以下僅針對單純提高門禁安全等級的功能做說明。

2.1 支援不同的生物辨識設備

指紋、臉型、掌紋、掌靜脈、指靜脈都是常見的生物辨識特徵。不同的生物辨識特徵提供不同的成本及安全等級。企業內不會所有門的安全需求都相同，一般區域的門禁使用感應卡刷卡即可，高安全區域可以使用刷卡＋密碼，最高安全區域(機房)可以使用刷卡＋生物特徵，亦可視安全等級要求，提供不同的生物辨識特徵技術。

企業對於不同區域的安全等級要求，會隨著商業環境的改變而變化。在選擇門禁管理系統時，必須考慮日後安全需求變化的可能，以避免日後必須安裝兩套管理系統，反倒增加維運成本，降低安全等級。

2.2 中央監控系統整合

中央監控系統(CMS)管理著企業內所有設備的狀態監視，含安防與其他設備。中央監控系統透過 OPC 或 Modbus 兩種標準協議與設備溝通。門禁管理系統支援 OPC 或 Modbus，便可以與中央監控系統整合提高系統安全等級。

門禁管理系統與中央監控系統整合後，門禁警報及狀態，如：逾時關門、強行進入、非法刷卡、門位狀態、控制器連線狀態...便可以在中央監控畫面上顯示，並藉由中央監控系統達到與視頻監控的連動。另外，門禁門鎖的控制，如：遙控開門、釋放門鎖...也可以在中央監控畫面上操作，並藉由中央監控系統達到與消防警報的連動。

2.3 視頻監控系統的整合

門禁系統搭配中央監控系統可以達到與視頻監控系統整合的功能。但是，並非所有企業均設置有中央監控系統。大部分企業僅設置視頻監視系統及門禁系統，而無中央監控系統，此時，門禁系統與視頻監視系統便須直接整合。

門禁系統與視頻監視系統整合後，提供當門禁警報發生時，將事件發生地附近的 Camera 視頻顯示在門禁系統上，便於警衛查看及時視頻，掌握現場狀況。或是利用門禁管理系統對刷卡紀錄的多條件查詢功能，查出刷卡資料並顯示當時刷卡視頻，便於管理者查看當時視頻，確認刷卡人員真實身分。或是利用管理系統對門禁警報紀錄的多條件查詢功能，查出門禁警報資料並顯示事件發生當時視頻。

2.4 消防連動的設計

裝設門禁，自然許多出入口平常是上鎖的，僅有權進出者可以刷卡進出。但是，當消防警報發生時，火警發生點附近的門禁管制點應該自動立即解鎖，以方便人員逃生，此為消防連動功能。

消防連動的機制有許多種方式，各有其優缺點。

利用消防警報乾接點直接連接到卡機的消防接點，當火警警報發生時，門禁控制器直接收到乾接點訊號，自動釋放門鎖。此種做法，消防連動反應最即時，但因為是硬接線方式，僅適合建物尚未裝潢前佈線施作，且火警警報點連動門禁控制器關係不易改變。

消防警報乾接點連接到中央監控系統，再由中央監控系統通知門禁管理系統，最後由管理系統通知門禁控制器，釋放門鎖。或是，消防警報乾接點連接到門禁管理系統，再由管理系統通知門禁控制器，釋放門鎖。此兩種方式均通過電腦系統的轉介，消防連動反應速度較硬接線慢，但因不牽涉到實體接線的變更，彈性度高，火警警報點連動門禁控制器關係容易依實際動線規劃需要隨時更動，同時也容易於建物裝潢後再行附加功能。

消防連動的方式並非互斥，可以同時混搭使用多種方式，畢竟多一種連動機制，多一層保障。

2.5 資訊安全的設計

門禁管理系統為執行於電腦上的程式，自然應該遵循程式設計領域的資安要求。登入密碼的強度要求，重複登入錯誤的帳號鎖定功能，密碼不可被管理者讀取...是基本的資安原則。

門禁管理系統若是 Web 架構，亦應防止 SQL Injection，Cross-site scripting (XSS) 的資安攻擊。管理系統是否有能力阻擋此類資安攻擊，很難從規格或是操作介面中看出端倪，必須借助公正第三方的弱點掃描程式偵測。

2.6 進出權限稽核

門禁管理系統應該提供各種查詢方式，便利使用者確認此門(或此區域)授權進入的人員有哪些，或是某員工允許進出的門有哪些。便利的查詢，有助於稽核門禁權限是否設定正確，進而提高門禁安全等級。

管理系統也應該提供各種刷卡資料的查詢條件，便利使用者確認此門(或此區域)刷卡進出的人員有哪些，或是有哪些員工嘗試進入未授權出入口。

本文並未描述個別企業對門禁功能需求上的差異，也未做功能的細部設計，僅針對企業對門禁管理系統降低擁有成本，提高安全等級的一般性需求，提出門禁管理系統應具備的功能，藉以建構出高效能的門禁管理系統功能。

本文由嘉因資訊有限公司提供 <http://www.tquark.com.tw>