

智慧化建築安全防範設備空間設計 準則之研究

內政部建築研究所自行研究報告

中華民國 100 年 12 月

(本報告內容及建議，純屬研究小組意見，不代表本機關意見)

國科會 GRB 計畫編號 PG10005-0176
(100-301070000G1059)

智慧化建築安全防範設備空間設計 準則之研究

研究主持人：張怡文

內政部建築研究所自行研究報告

中華民國 100 年 12 月

(本報告內容及建議，純屬研究小組意見，不代表本機關意見)

ARCHITECTURE AND BUILDING RESEARCH

INSTITUTE

MINISTRY OF THE INTERIOR

RESEARCH PROJECT REPORT

Study on Security Design Guidelines for Intelligent Building

By

Chang, I-Wen

Dec 31, 2011

目次

表次.....	III
圖次.....	IV
摘要.....	VII
英文摘要.....	IX
第一章 緒論	1
第一節 研究緣起與背景.....	1
第二節 研究目的與範圍.....	9
第三節 研究方法與過程.....	11
第二章 蒐集資料與文獻分析	13
第一節 臺灣智慧建築安全防範設備空間設計準則相關 發展.....	13
第二節 大陸智慧建築安全防範設備空間設計準則相關 發展.....	26
第三節 國外智慧建築安全防範設備空間設計準則相關 發展.....	30
第三章 智慧建築安全防範設備空間設計準則之研擬	57
第一節 智慧建築安全防範設備定義.....	57
第二節 智慧建築安全防範設備空間設計原理.....	62
第三節 智慧建築安全防範設備空間設計準則之研擬...	71
第四章 智慧建築安全設計案例介紹	87
第一節 美國猶他州鹽城湖社會大會堂廣場安全設計...	87
第二節 i236—新竹 U-Bobi 智慧安全社區規劃	90
第五章 結論與建議	95
第一節 結論.....	95

第二節 建議	97
附錄一 新加坡內政部「加強建築安全準則手冊-建築物安全防範設備」	99
附錄二 美國國土安全事務部「建築物防恐脆弱度評估清單」	117
附錄三 期初審查意見回應表	127
附錄四 期中審查意見回應表	133
附錄五 期末審查意見回應表	137
參考書目	143

表 次

表 1.1	內政部建築研究所 100-103 年度「智慧化居住空間產業	3
表 1.2	性別平等政策綱領-人身安全與司法篇具體行動措施三…	6
表 1.3	安全防災指標之「人身安全」指標評估原理及意義……	8
表 2.1	安全防災指標之「人身安全」指標評估基準……………	15
表 2.2	「生態社區評估系統」空間維安特徵評估表……………	18
表 2.3	「生態社區評估系統」……………	19
表 2.4	住戶自主檢查空間安全之評估表 ……………	21
表 2.5	可防禦之空間四要素 ……………	32
表 2.6	建築脆弱度評估項目 ……………	34
表 2.7	某建築安全計畫評估考慮課題例 ……………	36
表 2.8	建築安全層級或區劃 ……………	40
表 2.9	監測照明技術建議照度 ……………	43
表 2.10	建築物安全防範設備彙整 ……………	54
表 3.1	建築安全防範空間計畫要素……………	63
表 3.2	建築脆弱度評估項目 ……………	65
表 3.3	智慧建築手法彙整 ……………	79

圖 次

圖 1.1	智慧建築標章註冊圖樣	7
圖 1.2	智慧建築整合建築、機械手法創造人性化安全空間.....	10
圖 2.1	安全防災整合系統示意圖	14
圖 2.2	「人身安全」器材與程序之系統.....	16
圖 2.3	應用環境設計、安全維護設備提升人身安全研究建議	20
圖 2.4	集合住宅共用空間犯罪預防應考慮項目	24
圖 2.5	安全防範六大子系統與其它智能建築系統關係示意...	28
圖 2.6	安全防範系統構成示意-出入口控制子系統為例.....	29
圖 2.7	欠缺「自然監控」之 Pruitt Igoe 住宅.....	30
圖 2.8	在基地外部空間設置綠籬、階梯建立空間領域形成「自	32
圖 2.9	「門對門」之空間安排方式有利於「自然監控」.....	33
圖 2.10	發展及評估建築安全規劃設計方案之架構.....	35
圖 2.11	因應恐怖攻擊之建築安全設計方案.....	37
圖 2.12	安全縱深防禦的概念	39
圖 2.13	整合安全系統流程.....	42
圖 2.14	探測門接觸情形之室內探測器	45
圖 2.15	被動式紅外傳感.....	45
圖 2.16	接近或接觸式智能卡讀寫器.....	47
圖 2.17	光學開門.....	48
圖 2.18	訪問卡和讀卡器.....	48
圖 2.19	掌紋辨識器.....	49
圖 2.20	電動門檔和磁力鎖	50
圖 2.21	請求退出探測器	50

圖 2.22 固定式中央攝影監控相機·····	51
圖 2.23 雲台變焦攝像機·····	52
圖 2.24 防爆半球攝像機·····	52
圖 3.1 美國康乃狄克州城市廣場大廈·····	58
圖 3.2 Harrison 提出「智慧建築金字塔」模型·····	60
圖 3.3 建築安全防範空間設計思考流程·····	64
圖 3.4 善用基地周圍建築條件進行自然監控·····	71
圖 3.5 善用基地條件增加建築物受自然監控之可能·····	72
圖 3.6 兼顧建築美學之汽車障礙物·····	73
圖 3.7 兼顧建築美學之汽車障礙物·····	73
圖 3.8 電子籬笆例·····	74
圖 3.9 建築物與基地界線間之安全縱深可增加人員反應時間··	75
圖 3.10 調整建築形式擴大「自然監控」可視範圍·····	76
圖 3.11 高風險卸貨區與主要建築物分離·····	77
圖 3.12 採取窄而高或凹下之窗戶較不易碎裂·····	78
圖 3.13 安全監控畫面品質影響安全評估及報警之正確性····	82
圖 3.14 照明環環境及視線良好之安全監控室工作效率·····	83
圖 3.15 結構挑空設計易使建築物遭受炸彈攻擊時發生倒塌··	84
圖 3.16 空調外氣引入口應設置於不易遭投擲有害物質處····	85
圖 4.1 美國猶他州鹽城湖「社會大會堂廣場」·····	87
圖 4.2 i236 智慧生活科技運用計畫目標·····	91
圖 4.3 警察機關、保全業者共享監控影像·····	92

摘 要

關鍵詞：環境設計預防犯罪、智慧建築、建築設計準則、建築物安全防範設備

一、 研究緣起

為因應本所 100-103 年度「智慧化居住空間產業發展推廣計畫」發展符合國民生活需求之在地生活系統，及行政院 100 年核定之「性別平等政策綱領」人身安全與司法篇-建構安全無慮的環境議題，本研究提出以智慧建築科技建構安全無慮的生活環境，研擬相對應之建築設計準則。將綱領中有關「以性別觀點建構安全無慮環境」之抽象上位概念，轉換為可具體落實於建築設計實務中之建築設計技術。

二、 研究方法與過程

本研究方法與過程如下：首先，蒐集國內、外人身安全建築設計、建築安全科技文獻，分析彙整納入智慧建築安全防範設計可考慮項目。其次，研擬智慧建築安全防範設備空間設計準則。最後，邀請產官學研代表進行專家訪談，修正以上智慧建築安全防範設備空間設計準則。

三、 重要發現

本研究獲致以下重要發現：

1. 九一一事件後促使部分國家對於建築安全科技之應用轉趨積極，制訂相關建築技術手冊指導重點建築物之安全設計，對於台灣推動智慧化居住空間產業出口海外市場應有正面助益。
2. 智慧建築安全防範三大目標，依犯罪行為發生前、中、後分為：防範為先阻礙進入、報警與拖延及監控證據保全。智慧建築安全防範空間設計準則是提供建築師達成以上目標之設計思考架構而非設計解答，建築師研擬建築物安全整體計畫時，可依序從五

大項目著手，包括：敷地計畫與都市設計、建築設計、建築設備計畫與空間設計、安全議題敏感之建築物特殊考量、區分所有建築物之安全設備計畫與設計。置於提高安全防範性能之七項建築設計因子則是：基地周界設計、安全縱深、建築物形狀與方位、空間安全分層分區、建築物外牆設計、設備項目、區分所有建築物之安全設備點交與營運維護考量。

3. 進階功能之智慧建築安全防範設備具有自動報警、電腦輔助犯罪偵查等特性，其嚇阻犯罪功能不僅止於提升「社區監控力」。

四、 主要建議事項

立即可行之建議

推動智慧建築安全防範設計政策之性別分析

主辦機關：內政部建築研究所

協辦機關：內政部警政署、內政部家庭暴力及性侵害防治委員會

本案研擬可具體落實於建築設計實務中之安全建築設計準則。後續可就推動智慧建築安全防範設計政策進行性別分析，評估推動智慧建築安全防範設計政策對女性與男性所產生之受益程度是否產生差異，就建築設計之性別議題進行較為細緻之探討。

中長期建議

依智慧建築安全防範設計準則辦理地方示範計畫

主辦機關：內政部建築研究所

協辦機關：各地方機關團體及產業

透過與地方有關機關團體及產業合作發展，藉由警察、社區居民、公寓大廈管理組織及產業參予，使智慧建築安全科技能與庶民生活結合，並引導產業開發符合民眾真實需要之產品，才能使智慧科技產生價值。

ABSTRACT

Keywords : crime prevention through environmental design (CPTED), intelligent building, building design guidelines, building security technologies

1. Background and Problems

In response to this the 100-103 annual "intelligent living space industry development plan to promote" development needs in line with national life in the life of the system, and the Executive Yuan approved the "Gender Equality Policy" personal security and justice chapter - Construction safe and secure environment issues, this study proposes to construct intelligent building technology safe and secure living environment, to develop corresponding guidelines of architectural design. Of the Statement relating to the "safe and secure environment" of the upper abstract concepts into building design can be implemented in practice of building design.

2. Methodology and process

The research method and process is as follows: first, to collect the reference of security building design, building security technologies, and analysis of exchange into the wisdom of the entire security building designed to consider the project. Second, develop security building design guidelines. Finally, invited representatives of industry, government, academic and research expert interviews, more than correct security building design guidelines.

3. Major findings

This study addressed the following key findings were:

1 After the September 11 attacks prompted some countries the application of science and technology for building security become more active, developing technical manuals related to construction safety building design guidance focus for Taiwan to promote intelligent living space industry exports in overseas markets should be positive benefit.

2 Building three security goals, according to the criminal acts occurred before, during, and divided into: first hamper access to prevention, alarm and monitoring with delay in the preservation of evidence. Wisdom of building security design criteria is to provide space to reach these objectives, the architect designed a framework for thinking instead of design solutions, architects develop overall security master plan, can proceed in sequence from the five major projects, including: apply to site planning and urban design, architectural design, building security technologies, safety issues sensitive to the special considerations of the building, the distinction between the safety equipment of all planning and building design. Place to improve security performance of seven architectural design factor is: site perimeter design, safety depth, building shape and orientation, building security zoning, building security equipment items, the distinction between the safety of all buildings point of delivery and maintenance of equipment operating considerations.

3 Advanced Features of the wisdom of building a security alarm equipment, computer-aided crime detection and other features,

the deterrence of crime not only to enhance the function of natural Surveillance."

4. Major recommendations

Immediately feasible proposal

Designed to promote the intelligent security building policy of gender analysis

Major authorities: Architecture and Building Research Institute

Assistant authorities: National Police Agency, Ministry of the Interior and Domestic Violence and Sexual Assault Prevention Committee, Ministry of the Interior

Develop specific case can be implemented in practice in architectural design architectural design of safety guidelines. May promote the wisdom of building up security policies for gender analysis designed to assess the wisdom of building security designed to promote policies for women and men, whether the level of benefit arising from a difference on the architectural design of gender issues in a more detailed study.

Long-term recommendations

Intelligent security building in accordance with design criteria for local demonstration projects

Major authorities: Architecture and Building Research Institute

Assistant authorities: local authorities and industry groups

Through the relevant authorities and local development organizations and industry cooperation, by the police, community residents, apartment building management bodies and industry to participate, so that wisdom construction safety technology

combined with the ordinary folk, and guide industry development in line with the real needs of people and products in order intelligence technology to produce value.

第一章 緒 論

第一節 研究緣起與背景

壹、內政部建築研究所 100-103 年度「智慧化居住空間產業發展推廣計畫」工作要項(三):規劃發展符合國民生活需求之在地生活系統及示範應用

智慧建築係以達成「人性化空間」目的為出發點。臺灣自 78 年引進智慧建築之觀念以來，各相關產業隨之活絡，內政部建築研究所亦持續進行智慧建築的基本調查、發展評估系統、建築設計規範等相關研究。並於 91 年制訂了智慧建築的評估指標，92 年推出智慧建築標章，之後再依據 94、95 年行政院產業科技策略會議（SRB）決議，為促進資通訊(ICT)與建築產業跨領域結合發展，提出之 96-99 年「智慧化居住空間產業發展計畫」總體計畫、100-103 年度「智慧化居住空間產業發展推廣計畫」，以發揮臺灣科技優勢，善用電子化、數位化、資訊化的科技技術，創造人文與科技兼顧的智慧生活空間願景。

其中，96-99 年度「智慧化居住空間產業發展計畫」是以「促進推動智慧化居住空間產業整體發展」為計畫之發展目標；經由該階段 4 年計畫執行，智慧化居住空間產業發展在跨部會協調、推動產業發展、教育宣導與應用已具初步規模及成果，如何整合應用創新服務，推廣智慧化居住空間產業發展則是下一階段計畫之重點。

100-103 年度「智慧化居住空間產業發展推廣計畫」則是建立在 96-99 年度「智慧化居住空間產業發展計畫」成果基礎上，進行第二階段之延續性計畫，以達成 2009 年全國第八次科技會議決議推動措施：「結合資通訊科技優勢，建置與推廣在地民生服務、健康照護與

智慧住居、智慧能源系統，以滿足國民安全、健康、節能及舒適便利的優質生活環境，並因應高齡少子女化社會的來臨及能源短缺問題。」，更進一步探討資訊、通訊及電子電機技術、設備與建築領域之整合與深度應用，期盼透過應用建築物理環境感測、資訊、通訊、電子化、自動化技術及設備，賦予建築物智慧化功能，再結合健康照護、安全防災、永續節能等相關服務業，實現空間人性化之理想，使國民生活環境更加安全、健康、舒適、便利及永續。本 4 年度計畫具體工作要項 如表 1.1 所示，其中「規劃發展符合國民生活需求之在地生活系統及示範」為「智慧化居住空間產業發展推廣計畫」重點之一。

表 1.1 100-103 年「智慧化居住空間產業發展推廣計畫」工作要項

分項計畫	工作要項	100	101	102	103
(一)推動辦公室與推動小組運作	1. 推動辦公室與定期召開推動小組會議 2. 跨部會協調聯繫工作 3. 推動智慧綠建築協商整合 4. 計畫管考與彙報 5. 專屬網站之維護與系統擴充運作 6. 計畫宣導與公共資訊訊息傳播	→	→		→
(二)產業發展與人才培育	1. 推廣智慧化居住空間產業聯盟運作交流 2. 辦理創新應用之創作競賽 3. 辦理智慧化產業發展課程獎助及專業人才培育 4. 舉辦國內外交流研討會	→	→		→
(三)示範應用與展示推廣	1. 智慧化居住空間之示範應用-展示中心維運工作 2. 既有建築物智慧化改善示範工作 3. 規劃發展符合國民生活需求之在地生活系統及示範 4. 辦理智慧綠建築示範推廣	→	→		→
(四)創新服務與整合發展	1. 居家服務平台技術建構整合及推廣 2. 在地國民生活需求調查及生活服務模式 3. 推動研擬在地民生服務及智慧居住系統 4. 探討在地生活系統創新應用服務模式 5. 智慧綠建築整合推廣	→	→		
(五)相關機制研擬與法規研修	1. 推廣智慧建築認證機制 2. 國民生活需求調查及生活應用服務模式機制探討 3. 研訂新舊建築綜合佈線系統落實機制 4. 居家服務平台產業發展推廣機制 5. 建立智慧化住居系統之整合程序與標準規範 6. 研(修)訂推動智慧綠建築相關法制作業	→	→	→	→

(資料來源：內政部建築研究所 100-103 年「智慧化居住空間產業發展推廣計畫」)

貳、內政部「性別平等政策綱領」(草案)－人身安全與司法篇－具體行動措施(三)建構安全生活空間－2.環境規劃與安全－(1)提升公共環境與公共設施之安全設計，檢討相關建築法令。

內政部於100年3月召開首次由中央政府主辦之「全國婦女國是會議」，會中並就所研擬的「性別平等政策綱領」(草案)進行討論，本次會議結論將併同會前座談會建議，邀集相關部會研商修正草案後，提送行政院婦女權益促進委員會報告，並奉行政院頒布後，作為我國推動性別主流化的指導方針。馬總統在開幕式致詞時表示：「追求性別平等已是文明世界的普世價值，很高興在政府與民間團體的攜手合作下，臺灣已有相當不錯的成績，這也顯示出兩性目前在潛能擴展及參與經濟政治等活動的機會，都已漸趨平等。」(內政記事本，2011)。

我國「性別平等政策綱領」(草案)提到，過去半個多世紀以來，為達成性別平等目標，聯合國先後召開四次重要的世界婦女大會，以及一次特別會議。在1985年所召開的第三次世界婦女大會中，回顧過去成效後指出，過去十年的目標雖在提昇婦女地位，但結果卻只有少數婦女因此受益。於是提出婦女權益問題不僅要在家庭、就業、健康、教育、社會服務等傳統領域中被關心，未來在工業、科學、通訊及環境各種領域中都要被討論。因此，在該綱領(草案)除了提出「消除性別歧視與性別暴力是捍衛人身安全的重要關鍵」等8項性別平等之基本理念外，尚進一步研提「人身安全與司法」等七大領域不同課題，將前述基本理念具體化。(李安妮，2011)

上開綱領(草案)「人身安全與司法」專篇中，首先，就我國人身安全現況與背景進行了性別統計分析，提出公共生活或私人生活中，發生基於性別原因的暴力行為仍多所存在；檢視我國相關統計資料顯示，性侵害犯罪、家庭暴力及性騷擾等問題，是對女性造成

最大傷害與威脅的項目，凸顯人身安全議題仍存在性別的困境。此些暴力行為對婦女身心與性自主方面造成嚴重的傷害與威脅，阻礙實現平等發展。其次，該專篇提出「以性別觀點建構安全無慮的環境」等「基本理念與觀點」及「政策願景與內涵」，認為國家政策應致力保障每一個人的安全，由於女性、兒童與少數族群者在社會上仍處於相對弱勢，生活上較易遭遇危險傷害，因此政府施政應思考如何在硬體空間設置與各項軟體服務層面上，建構讓女性、兒童與各族群免於恐懼與威脅的生活環境。應檢視相關建築法令規範，引導安全之公共環境規劃與設計，減少犯罪發生機會，增加社區監控力（王珮玲，2011）。根據以上理念研擬之具體行動措施（草案）如表 1.2 所示。

表 1.2 性別平等政策綱領-人身安全與司法篇行動措施（三）（草案）

（三）建構安全的生活空間	相關部會
<p>（三）1. 科技與安全</p> <p>（1）鼓勵民間參與開發相關安全科技設施與設備，強化政府與民間合作，推動社區科技防治安全網。</p> <p>（2）建置婦幼人身安全扶助系統、夜歸婦女呼叫協助服務、以及研議高危機被害人衛星定位與警方連線系統等。</p> <p>（3）維護社區錄影監視系統之功能，並檢討監視器畫面資料之管理、保護與使用規定，以維護民眾之隱私權。</p>	內政部警政署、 經濟部
<p>（三）2. 環境規劃與安全</p> <p>（1）提升公共環境與公共設施之安全設計，檢討相關建築法令，推動情境犯罪預防，減少犯罪發生機會。</p> <p>（2）落實社區治安死角之查報，警政系統應諮詢社區民眾與婦幼之意見，即時回應規劃治安維護作為。</p> <p>（3）公共運輸系統應規劃相關安全措施，各公私立停車場應有燈光、動線與安全配備之標準規範。</p>	內政部營建署、 內政部建築研究所、交通部、 內政部警政署
<p>（三）3. 社區參與</p> <p>（1）積極獎助各式創意防暴方案推展，鼓勵成果發表、人才培育以及相關表揚活動。</p> <p>（2）鼓勵發展因地制宜的社區安全維護方案，提升民眾參與社區安全維護的工作。</p>	內政部警政署、 內政部家防會

參、推廣內政部建築研究所「智慧建築標章」，善用智慧化建築設備，提升空間安全性

「智慧建築」是指藉由導入資通訊系統及設備之手法，使空間具備主動感知之智慧化功能，以達到安全健康、便利舒適、節能永續目的之建築物。而「智慧建築標章」係內政部建築研究所依「商標法」規定註冊之證明標章，該標章係由該所同意之人使用，證明建築物符合「智慧建築解說與評估手冊」與「智慧建築標章推動使用作業要點」所訂之標準。此外，對於已取得建造執照尚未完工之新建建築物，或施工中之特種建築物，若符合以上標準，亦可向內政部建築研究所申請候選智慧建築證書。



圖 1.1 智慧建築標章註冊圖樣

有關提升公共環境與公共設施之安全設計，減少犯罪發生機會，提升建築物使用者人身安全課題，係內政部建築研究所之「智慧建築解說與評估手冊 2011 年版」中「安全防災指標」評估項目之一，安全防災指標著重在「主動性防災」以及各自動化系統間其整合及連動程度的評估，鼓勵以主動控制之積極手段設計更安全之建築物。其評估原理與意義參表 1.3 所示。

表 1.3 安全防災指標之「人身安全」指標評估原理及意義

項次	分項指標	指標項目	評估意義
一	建築物 防災	防火系統	評估建築物防火系統，如火警警報、人員疏散導引、自動滅火及消防設備監控的智慧化程度。
		防震抗風系統	評估建築物防震或抗風系統，如隔震、制震、抗風以及結構體安全狀態監測設備的智慧化程度。
		防水系統	評估建築物防水系統，如對滲漏水預警、監視設備及防淹水措施的智慧化程度。
二	人身 安全	防盜系統	評估建築物防盜系統，如門禁管制及防盜監控設備的智慧化程度。
		防破壞系統	評估建築物防破壞系統，如偵測爆裂物、防止人為蓄意破壞的智慧化程度。
		防有害氣體系統	評估建築物防有害氣體系統，如瓦斯、一氧化碳外洩偵測及警報設備的智慧化程度。
		緊急求救系統	評估建築物緊急求救系統，如使用緊急按鈕求救設備的智慧化程度。

（資料來源：本所智慧建築解說與評估手冊 2011 年版）

第二節 研究目的與範圍

壹、研究目的

建築安全防範設計與設備二者，是目前建築設備教科書中較少被探討之一環，近年來關於建築安全防範設計、預防犯罪之環境設計雖有增加，但仍缺少將被動式建築設計手法、機械手法進行技術層面統合，與實際應用面之探討。由於智慧化建築安全防範設備可使建築物具備主動感知之智慧，進而輔助被動式建築設計、被動式建築安全防範設備之不足，創造更為人性化之安全空間，因此，妥適應用智慧化建築安全防範設備，與建築設計手法彼此相輔相成之技術，構成「安全之智慧建築」，是內政部研訂建構安全生活空間所需之建築規劃、設計、設備技術規則，引導建築師發展安全之建築設計方案、應用建築設備之重要課題。

貳、研究範圍

100 年 1 月 5 日修正公布之建築法第九十七條規定，除建築規劃、設計、設備之建築技術規則，由內政部定之等原有規定外，並新增應落實建構兩性平權環境之政策，同法第 13 條則明訂建築物之設計、監造人為建築師。

因此，本研究著重於在內政部主管建築事務、建築師可操作之權責範圍內，發展「智慧建築安全防範設備空間設計準則」，使該準則具有供主管建築機關研訂人身安全建築設計技術規範之參考價值，並依據該準則發展一「智慧建築人身安全設計示範應用方案」，作為建築師發展建築物設備空間設計方案之參考，以便有效達成內政部建築研究所 100-103 年度「智慧化居住空間產業發展推廣計畫」發展符合國民生活需求之示範應用方案之目標，引導建築師善用智慧建築安全防範設備，並落實內政部「性別平等政策綱領」（草案）有關建構安全生活空間之課題。

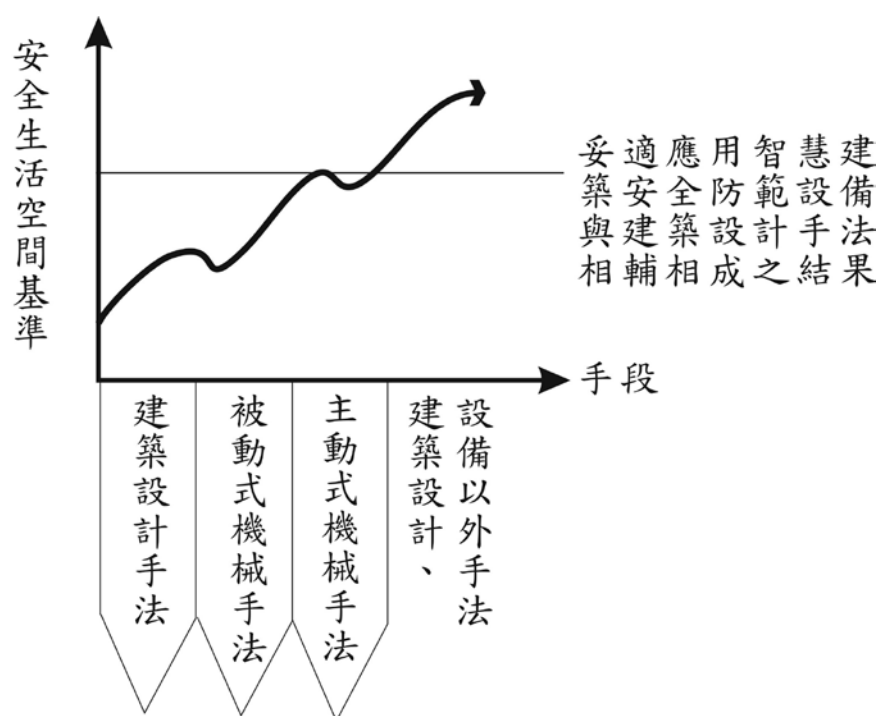


圖 1.2 智慧建築整合建築、機械手法創造人性化安全空間

(資料來源：自行繪製)

第三節 研究方法與過程

一座建築物可以說是許多專業者分工合作的結果，但是對住的人或使用的立場來說，仍然是一個整體，但整體並非部分的單純集合體，「統合建築」是建築師之職責，在有限的條件中尋求平衡解的關鍵，因此必須瞭解自己主宰領域的全盤，負起完成一座建築過程中之領航責任（吳讓治，1984）。

本研究嘗試發展「建築」與「智慧化建築安全防範設備」之溝通平台，釐清內政部研訂建構安全生活空間所需建築技術規則應考慮項目，使建築師發展建築設備空間設計方案使用，並作為本所推動智慧建築標章、智慧化居住空間產業發展推廣計畫、既有建築物智慧化改善補助計畫執行之參考。

本研究方法與過程如下：

1. 參考國內、外人身安全建築設計、建築設備研究成果，分析彙整適合納入智慧建築安全防範設備空間設計考慮之項目。
2. 研擬智慧建築安全防範設備空間設計準則。
3. 邀請產官學研代表進行專家訪談，修正以上智慧建築安全防範設備空間設計準則。

第二章 蒐集資料與文獻分析

本章旨在依據第一章所擬研究目的與範圍、研究方法與過程，蒐集國內、外相關文獻，彙整研擬智慧化建築安全防範設備空間設計應考慮項目，以便於內政部研訂相關建築規劃、設計、設備技術規則，據以引導建築師應用智慧建築安全防範設備，發展安全之建築設計方案，使建築物具備主動感知之智慧，成為更為人性化之安全空間。

第一節 臺灣智慧建築安全空間設計準則之相關發展

建築師在發展建築設計方案初期，若能先建立一建築整體「人身安全」空間計畫構想，擬定防盜、防入侵、避難逃生、外部救援活動需求等課題，再對應之建築設計手法，並輔以各種主、被動式機械手法，即可成機械設備數量合理、能源消耗及設備線路減量，並善用資通訊科技與遠端之警察、保全等外部救援系統連接之智慧建築。

因此，內政部建築研究所自民國 81 年參考日本「高度資訊化建築物整備事業融資推薦基準」，制定了臺灣之「智慧型建築指標與基準」(許宗熙、楊逸詠等，1992)，接續進行臺灣智慧型建築之發展現況調查與法令研修建議等相關研究。85 年在「智慧型公寓大廈自動化系統設計準則研究」(溫琇玲、邵文政等，1996)。91 年參考國內、外建築物之評價方法，制訂了臺灣智慧建築評估系統，成為臺灣智慧建築設計之初步技術規範，92 年推出智慧建築標章，

100 年則將臺灣智慧建築評估系統作了大幅度之修正，發展出以八項評估指標構成智慧建築標章評估系統，據以評估建築物是否符合「智慧建築」之基準，包括：「綜合佈線」指標、「資訊通信」指標、「系統整合」指標、「設施管理」指標、「安全防災」指標、「健康舒適」指標、「貼心便利」指標及「節能管理」指標。

其中，「安全防災指標」再細分為「建築防災」與「人身安全」

2 大部分，「建築防災」是在既有相關法規對於建築物防火、耐震等規範基礎上，更進一步強調智慧建築之「人性化空間」理念，就建築設計方案之「主動性防災性」，以及「各自動化系統間其整合及連動程度」進行評價。而「人身安全」指標則是評估建築設計方案是否能藉助自動化設備，對於盜匪入侵、人為蓄意破壞、有害氣體外洩等，危害或威脅建築物使用者人身安全事故，進行事先防範或防止其擴大，以及當使用者遇到危急事故時能藉由自動化系統有效避難或待援求助之智慧化性能指標項目，並且鼓勵採用更好的新工法新技術，在合用並且有效的前提下，亦能獲得鼓勵性的分數，建築師在發展智慧建築整體「人身安全」空間計畫構想時，可以參考表 2.1 安全防災指標之「人身安全」指標評估項目與基準，研擬之防盜、防入侵、避難逃生、外部救援活動需求等安全防災課題及對應手法。



圖 2.1 安全防災整合系統示意圖

（圖片來源：內政部建築研究所，智慧建築解說與評估手冊 2011 年版）

表 2.1 安全防災指標之「人身安全」指標評估基準

項次	指標項目	評估類別	評估基準
一	防盜系統	偵知通報與顯示性能	設置防盜自動警報設備
			設置人車自動監視設備
			設置影音對講設備
		侷限與排除性能	設置自動門禁管制設備
			設置停車管理設備
		其他	可達實質成效且視需求採用之創新技術與工法
二	防破壞系統	偵知通報與顯示性能	設置偵測爆裂物等危險物品設備
		其他	可達實質成效且視需求採用之創新技術與工法
三	防有害氣體系統	偵知通報與顯示性能	設置致命有害氣體之監測設備或措施(如一氧化碳、瓦斯等)
		侷限與排除性能	設置防止致命有害氣體擴散之設施
		其他	其他創新並有效之新技術與新工法
四	緊急求救系統	避難引導與緊急救援	升降梯、直通樓梯等處設緊急求救按鈕或可對外聯繫之緊急電話
			緊急求助系統能與錄影監視系統連動
		其他	可達實質成效且視需求採用之創新技術與工法

(來源：內政部建築研究所，智慧建築解說與評估手冊 2011 年版)

壹、應用空間規劃、設計、建築安全維護設備預防犯罪

美國學者紐曼(Oscar Newman)曾提出「可防禦之空間」概念，

是著名的應用空間規劃、設計方法進行犯罪預防之理論，開啟了一系列相關研究，新建建築物可在設計階段依據其建議預為規劃，並可與其他建築安全設備發揮相輔相成之功能，如圖 2.2 所示。

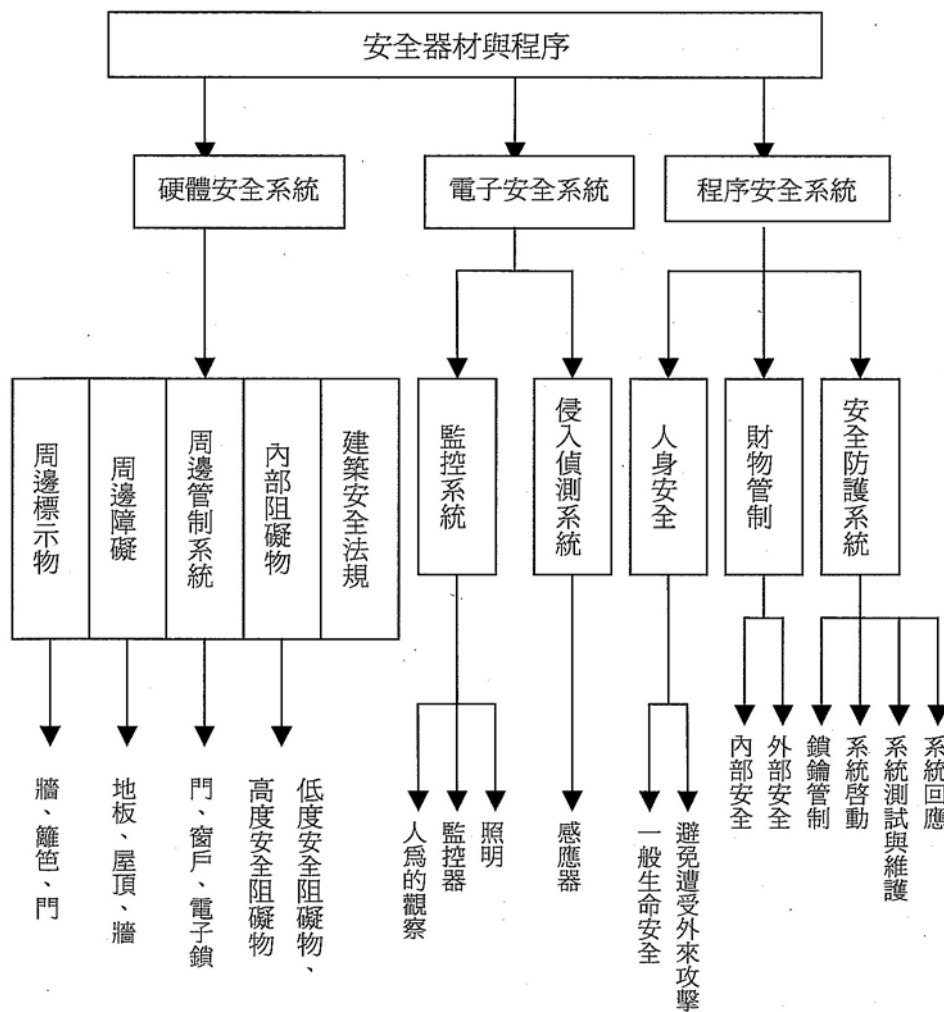


圖 2.2 「人身安全」器材與程序之系統圖

（資料來源：許春金，犯罪預防與私人保全）

依據「可防禦之空間」研究，我國都市住宅的環境問題如下：（謝園，2001）

1. 自明性不足：都市土地使用大多為住商混合，社區很難分辨外人或居民
2. 領域不清：道路規劃為棋盤式巷弄，交通穿越性太強
3. 視覺死角：防火巷狹小，建築距離不足，沿巷弄停車位
4. 建築物公共空間死角：
 - (1) 大門視覺穿透性不足，有陌生人進入關上門，自室外便看不見其行動
 - (2) 樓電梯間在建築物中央，或窗子太小，透明性不足
 - (3) 地下停車場，地下及屋頂機電室
 - (4) 自住宅窗戶或陽台看不見大門進出的人及活動
 - (5) 住戶不來往

而住戶可依據以下原則，選擇安全的居住環境：（謝園，2001）

1. 選擇住宅時，注意社區安全，公寓及住戶的領域及自明性
2. 公寓大門之視覺穿透性
3. 在公共空間之視覺死角裝設電子監視器材，由管理員或住戶可觀察到，如：樓電梯間，停車空間，屋頂，機電房等處
4. 社區，公寓，大廈之聯防或通報系統

內政部建築研究所除了 91 年發展出之智慧建築評估系統制訂「安全防災」指標外，在 99 年所發展之「生態社區評估系統」也有關於安全之「治安維護」範疇評估，強調從建築與都市計畫領域應有治安維護考量，安全之空間規劃、設計應就住宅類型、犯罪死角、社區街道型態、設置公設監視器等因子納入考量，並進一步設計量化評

估表如表 2.2、2.3 所示。

表 2.2 「生態社區評估系統」空間維安特徵評估表

大指標	分項指標	說明	評估標準	計分方式
空間維安特徵 C ₁	住宅類型	一般公寓大樓因住戶較多，空間分佈上較一般透天厝來得多變，在居家安全性上亦相對的較其他類型來得高	社區型中央管理系統	50分
			集合住宅(公寓大廈)、電梯公寓有警衛管理服務	50分
			樓梯公寓、透天住宅有警衛管理服務	40分
			樓梯公寓、透天住宅有私人保全系統	30分
			集合住宅(公寓大廈)、電梯公寓無警衛管理服務	20分
			樓梯公寓、透天住宅無警衛管理服務	10分
		$\Sigma(\text{戶數} \times \text{各項原始給分}) / \text{總戶數} = \text{得分}$		
	犯罪角落(或死角)	易躲藏歹徒之屋角、牆角、遮蔽物、街道設施、中高型灌木叢(高60~200cm者)	有一處，扣一分，最多扣10分	-10~0
	入侵透天住家之攀爬物(公寓大廈免評估)	有助於歹徒攀爬、翻越圍牆窗戶之花台、矮牆、街道設施	有一處，扣一分，最多扣10分	-10~0
	街道維安特徵	整體社區之巷道規劃攸關於社區安全之防範，住家巷道以棋盤式較為安全，另死巷或後巷道、防火巷則容易形成安全死角	死巷	有一條扣30分
			無人維護之後巷道、防火巷	有一條扣50分
			$\Sigma(\text{道路長度} \times \text{各項原始給分}) / \text{總道路長度} = \text{得分}$	
	鄰地維安狀態	所謂空地：指已完成道路、排水及電力設施，於有自來水地區並已完成自來水系統，而仍未依法建築使用之私有及公有非公用建築用地。空屋：指荒廢、無人居住或已被徵收或部分拆除後棄置之建築物。住屋鄰接若為施工中之工地，因施工鷹架常成為竊賊攀爬侵入之媒介，而較危險。另外，鄰接為空屋或空地也易成為歹徒侵入之弱點	鄰接施工工地	有一處扣1分，-5~0
			鄰接空屋	有一處扣1分，-5~0
			鄰接空地	有一處扣1分，-5~0

(資料來源：內政部建築研究所，生態社區解說與評估手冊 2010 年版)

表 2.3 「生態社區評估系統」

大指標	分項指標	說明	評估標準	計分方式
防範設備與守望相助 C ₂	社區管理與社區巡守隊	社區巡守隊對社區安全防範具有無形之保護作用，雖然，雖然巡守隊員無法如警員擁有武力嚇阻，但可以群體力量制止正要發生及正在發生中之犯罪行為	有社區管理及定時定點巡邏	50
			定時定點巡邏	40
			沒有	30
			$\Sigma(\text{戶數} \times \text{各項原始給分}) / \text{總戶數} = \text{得分}$	
	公設監視器(含警方、區公所之設置)	裝設於公共空間之公設監視器一般被視為事發後，警方偵查之主要依據。其雖有嚇阻作用，但成效仍不及私設監視器	12m以上交叉路口應設置監視器	(無設置監視器路口數/總路口數) × (-10) = 所扣分數，-10~0
	社區周邊娛樂場所	社區內若有視聽歌唱、理髮、三溫暖、舞廳、舞場、酒家、酒吧、特種咖啡茶室、電子遊戲和網咖，影響治安等十大行業，出入份子較複雜，將影響社區之社會秩序	社區內及相鄰周邊此十大行業家數，有一家扣一分	-10~0

(來源：內政部建築研究所，生態社區解說與評估手冊 2010 年版)

對於行政院婦女權益促進委員會人身安全小組第 18 次及第 19 次會議決議。內政部建築研究所辦理了公共空間婦女人身安全課題研究。提出適用於我國之安全維護設施範例，並詳加說明分析，以提供建築專業者參考應用；此外，提出應用環境設計預防犯罪，必須區分為公共空間、公寓大廈共用部分及專有共用部分空間三個層次：政府部門應投入公共空間的改善，共用空間改善有賴於住宅社區及管委會組織運作，至於私人使用空間，是屬於住戶自發性強化居住安全的範圍，需提供方法諮詢，鼓勵民眾自行投入資金；最後並提出。新建建築物可在設計階段依本研究成果進行規劃設計，但既有建築物受空間不易變更之限制，可應用預防犯罪設備改善等未來研究課題（靳燕玲，2006），如圖 2.3 所示。

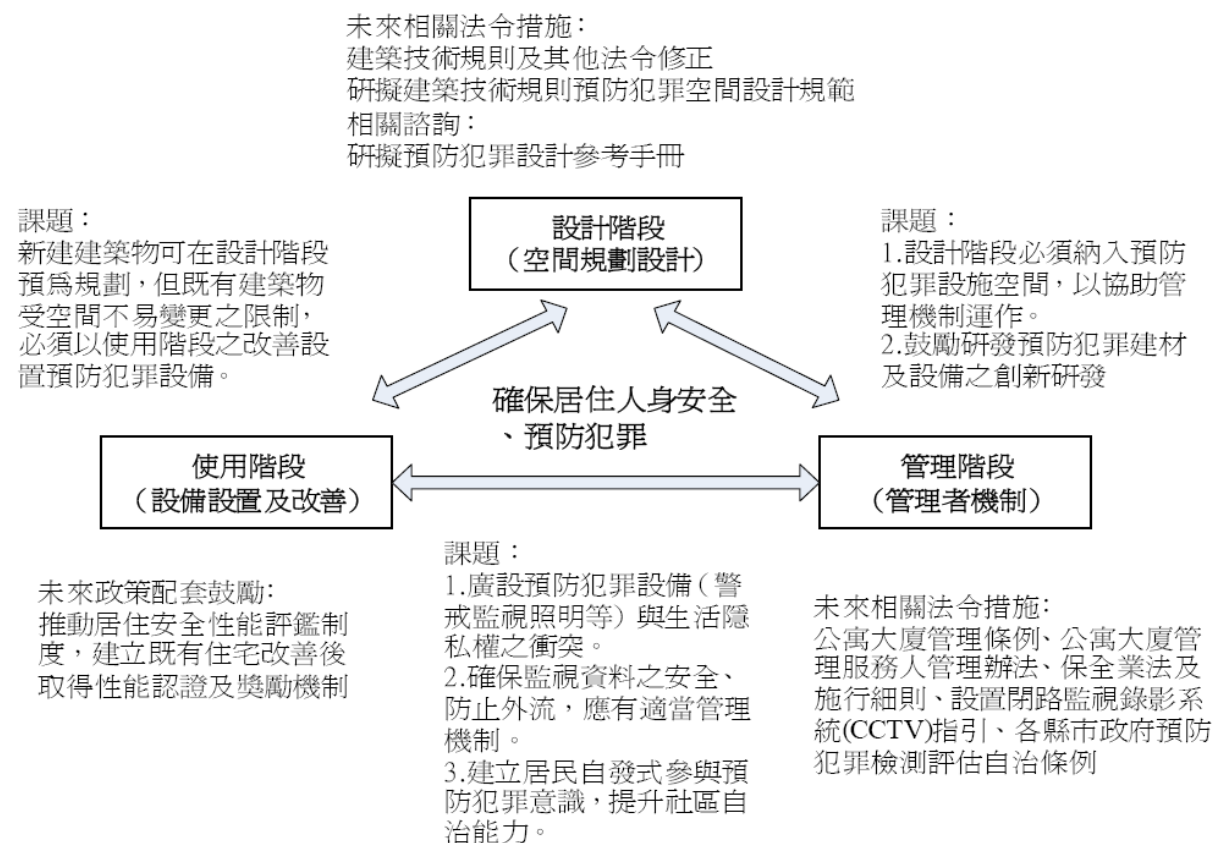


圖 2.3 應用環境設計、安全維護設備提升人身安全研究建議課題

(資料來源：靳燕玲，集合住宅社區共用空間安全防範設施設置方法研究)

內政部建築研究所接續以上研究，透過實際住宅案例調查。提出集合住宅共用空間安全維護設計通則，提出集合住宅共用空間在犯罪預防方面應考慮「社會監控、自然監控、設備監控」三個監控項目（餐圖 2.4），並提出表 2.4 所示之住戶自主檢查空間安全之評估項目（蔡淑瑩，2007）。

表 2.4 住戶自主檢查空間安全之評估表

填表日期	年 月 日	住宅名稱		
建築位置 或地址			犯罪紀錄	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有 發生點：_____
住宅年齡	____年	住宅樓層	地上：_____樓 地下：_____樓	居住樓層 _____樓
住宅類型	<input type="checkbox"/> 獨棟 <input type="checkbox"/> 雙併 <input type="checkbox"/> 三併或四併 <input type="checkbox"/> 長走廊（共用走廊）式 <input type="checkbox"/> 中庭型 <input type="checkbox"/> 門字型 <input type="checkbox"/> L 字型 <input type="checkbox"/> 簇群式 <input type="checkbox"/> 連棟式 <input type="checkbox"/> 其他_____（可複選）			
說明：1. 如果題目需要勾選為 <input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5.，請依欄下文字選擇，例如： <input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5.，越趨近 1 越不高，越趨近 5 越高。 不高 高				
項目			勾選	
社會 監 控	1. 社區是否有守望相助巡守隊巡邏？		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
	2. 承上題，守望相助巡邏隊巡邏的程度？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不高 高	
	3. 入口是否有管理員。		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
	4. 住宅是否有管理委員會？		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
	5. 管理委員會對住宅的管理程度？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不高 高	
	6. 警察對住宅的巡邏程度？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不高 高	
	7. 鄰長或里長對住宅的關心程度？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不高 高	
	8. 住宅管理單位是否有請私人保全機構管理維護住宅？		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
自然 監 控	1. 鄰房攀爬進入住宅社區內的程度？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易	
	2. 建築配置是否有輕易監看公共開放空間（如兒童遊戲區、社區小公園）？		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
	3. 信箱是否有統一管理在住宅內部？		<input type="checkbox"/> 有 <input type="checkbox"/> 沒有	
	4. 您家與隔壁鄰居陽台是否可以攀爬過來？		<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易	

(承上頁)

自然 監控	5. 您覺得您家與社區是否有共同領域精神？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不高 高
	6. 如果住宅為住商混合，出入之大門有分離嗎？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	7. 住宅周邊是否有圍籬或籬笆阻隔，防止小偷？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	8. 承上題，圍籬及籬笆是否可以輕易看清楚裡面？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不容易 容易
	9. 住宅屋頂是否可以互相連通？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易
	10. 陽台或雨遮是否容易攀爬進入室內？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易
	11. 陽台欄杆是否容易攀爬？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易
	12. 停車場是否有陰暗死角讓人害怕？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 有 沒有
	13. 防火間格是否可以讓陌生人任意躲藏？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易
	14. 植栽是否容易阻擋視線穿透？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 容易 不容易
	15. 植栽是否種植太密集容易躲人？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 有 沒有
	16. 住宅入口大門是否有設在較有人走動經過的地方？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	17. 住宅入口大門是否有視覺穿透性？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
設備 監控	1. 您覺得您家附近的街道晚上燈光昏暗嗎？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 是 不是
	2. 鄰里街道是否有裝設監視系統嗎？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	3. 您家住宅社區晚上的燈光照明夠亮嗎？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不夠 夠
	4. 您家的住宅是否有加裝監視系統？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	5. 樓梯間是否有加裝緊急求救按鈕？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	6. 樓電梯是否有加裝監視系統？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	7. 陰暗角落（如地下室、防火巷、垃圾間）晚上及白天是否有加裝感應式照明？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有
	8. 屋頂層是否有加裝監視系統或熱度感應，有人在屋頂層就會發出照明或聲響？	<input type="checkbox"/> 有 <input type="checkbox"/> 沒有

(承上頁)

9. 停車場的燈光照明是否夠亮？	<input type="checkbox"/> 1. <input type="checkbox"/> 2. <input type="checkbox"/> 3. <input type="checkbox"/> 4. <input type="checkbox"/> 5. 不夠 夠
合計：_____分，社會監控：_____分，自然監控：_____分，設備監控：_____分	

請民眾將填寫完之問卷作分數的計算，回答「有」之答案得1分，沒有則得0分，而填寫□1、□2、□3、□4、□5的答案，請依填寫欄的數字計算分數。

※低於 15 分之住宅，請您最好馬上改善您家的犯罪預防維護設施！！

※高於 50 分之住宅，恭喜您家安全指數很高，不過還是要定期檢查安全設施喔！

※介於 15~50 分中間之住宅，注意您勾選分數較低或 0 分之題目，趕快改善！

(資料來源：本研究自行研擬)

(資料來源：蔡淑瑩，集合住宅共用空間安全維護設施評估研究)

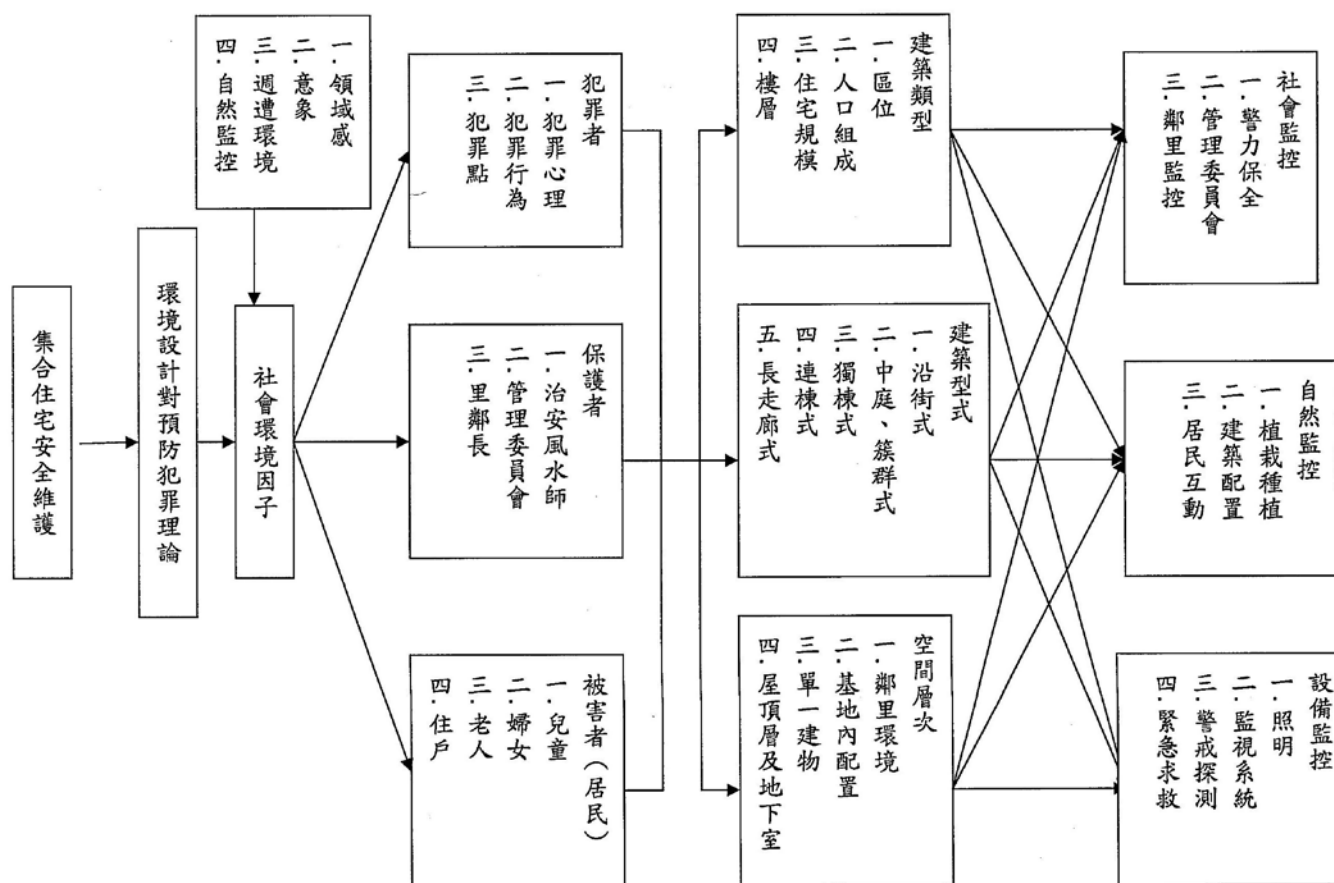


圖 2.4 集合住宅共用空間犯罪預防應考慮項目

(資料來源：蔡淑瑩，集合住宅共用空間安全維護設施評估研究)

內政部營建署則於 96 年 1 月發布增訂建築技術規則建築設計施工編第四章之一建築物安全維護設計，規定供公眾使用建築物之公共空間應設置：照明、監視攝影、緊急求救、警戒探測 4 種「安全維護裝置」，並規定設置地點，及設置基準。

此外，內政部警政署亦曾提出選用建築物防盜系統之建議考慮項目如下：（內政部警政署，犯罪預防寶典）

- (1) 防盜警報系統的考量：設定保護範圍、產品品質良好、採用警報器聲響型態：立即或延遲警報聲、或靜音警報，並與警察機關連線、偵測器或感應器的選擇：動態或磁性感應、充足的警報線路，且電器插頭應設置於需要電力之處、裝設整棟建築物的聯防警報、檢驗監視設備的方法、警報器觸動或外人入侵時的處理。
- (2) 閉路電視系統的考量：產品品質良好、鏡頭與監視器的型態、監視器的監視者與維修者、監視中心的空間大小、電器插頭與線路的設置、外人入侵時的處理
- (3) 通道電子卡片的考量：刷卡位置的考量、電路干擾警報的偵測、備用電池、偵測干擾的能力、其他各種安全設備與措施的配合使用（如：警報器、閉路電視、感溫器、燈光照明、電梯控制、通道控制、人員巡邏）

第二節 大陸智慧建築安全防範設備空間設計準則之相關發展

大陸將「智能建築」列為「建築電器」領域之一項重要主題，「建築電器」是指：「以建築為平台，利用現代先進科學理論及電力、資訊、智能化技術，在有限之空間內，創造人性化生活環境之一門應用學科。」相當於臺灣「建築設備」領域探討範圍。該領域涵蓋廣泛，除「智能建築」外，尚包括：建築供配電、建築照明、建築節能與太陽能應用等（中國建築學會建築電器分會，2010）。

「智能建築」是建立在 20 世紀電子、電腦網路、自動控制、系統工程技術之高度發展之基礎上，充分應用該技術所整合研發出之智慧化設備，創造出之安全、便利、舒適人性化空間（許錦標等，2010）。2007 年 7 月發布實施之「智能建築設計標準」GB/T 50314-2006，將「智能建築」定義為：「以建築物為平台，兼備信息設施系統、信息化應用系統、建築設備管理系統、公共安全系統等，集結構、系統、服務、管理及其優化組合為一體，向人們提供安全、高效、便捷、節能、環保、健康之建築環境。」

由於「智能建築」在大陸屬熱門行業，根據世界銀行預測，21 世紀全球百分之 50 之智慧建築將誕生在大陸，在對於智能建築專業人才有大量需求之背景下，大陸教育部於 2005 年訂定「080712S 建築電器與智能化」專業，並批准許多高校投入該專業，也配合十一五計畫編寫許多智能建築相關教材。（王娜，2010）

「智能建築」與傳統建築之最主要差別在於擁有「人工智慧」，並應有以下 4 種功能：（苗月季等，2010）

1. 對環境和使用功能之變化具有感知能力。
2. 具有傳遞、處理感知信號、資訊能力。
3. 具有綜合分析、判斷能力。

4. 作成決定，並發出指令信號、資訊能力。

大陸「智能建築」探討範圍主要包括以下項目：

1. 建築設備管理系統(Building Management System, BAS)：供配電設備監測、照明監控、空調監控、給排水監控、電梯監控系統。
2. 安全系統：安全防範系統、消防報警系統、緊急通報系統。
3. 通信網路及信息系統：綜合佈線、電話交換系統、多媒體會議系統、公共廣播、衛星通信、有線電視及衛星電視接收系統、電腦網路系統、室內移動通信覆蓋系統。
4. 系統集成。

其中，智能建築安全防範系統大致上可細分以下六大子系統，而安全防範系統，與其他智能建築系統間之關係如圖 2.5 所示，建築師可參考該架構發展智慧建築安全防範構想方案，這些安全防範子系統，實際上是以電子探測設備、有線或無線通信設備、電腦網路設備、攝影監控、讀卡機…等硬體設備單元，搭配警察、保全服務、建築物設施管理加以優化組合所構成如圖 2.6：

1. 出入口控制系統
2. 入侵報警系統
3. 攝影監控系統
4. 電子巡更系統
5. 停車空間管理系統
6. 其他個別特殊設置系統

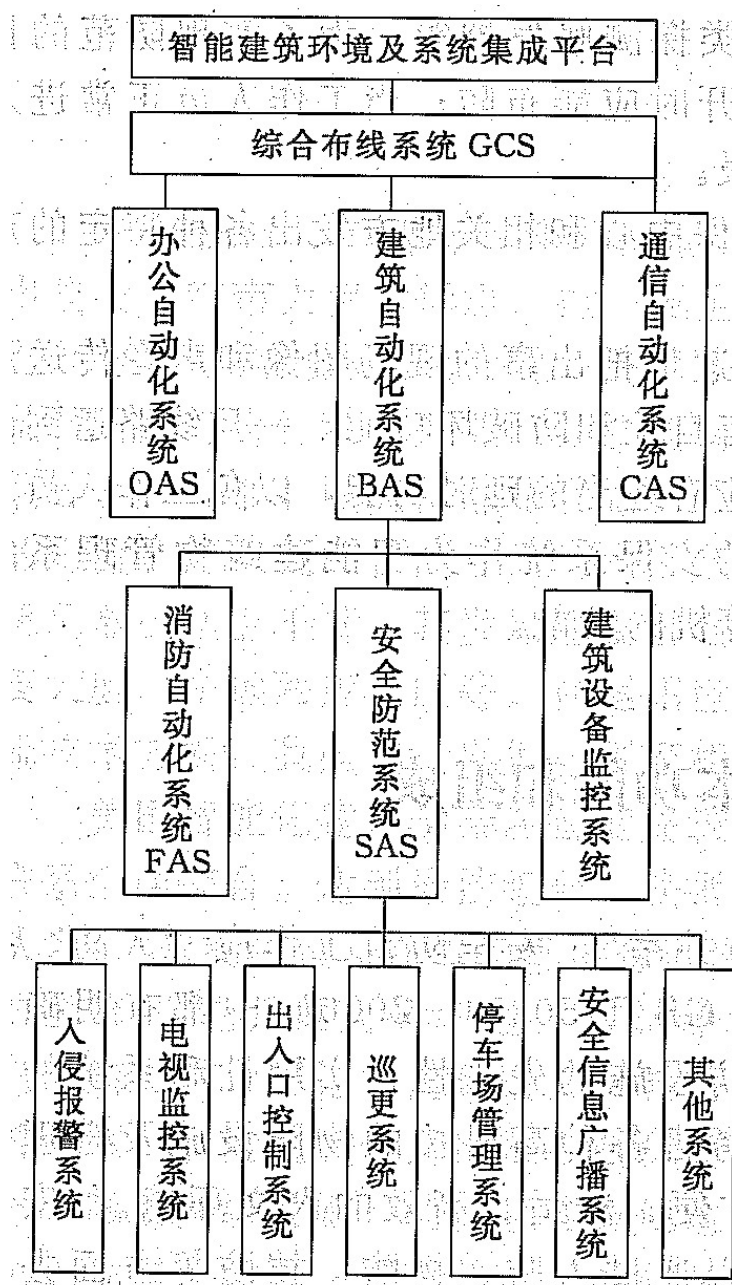


圖 2.5 安全防範六大子系統與其它智能建築系統關係示意

(圖片來源：魏立明，智能建築消防與安防，2010)

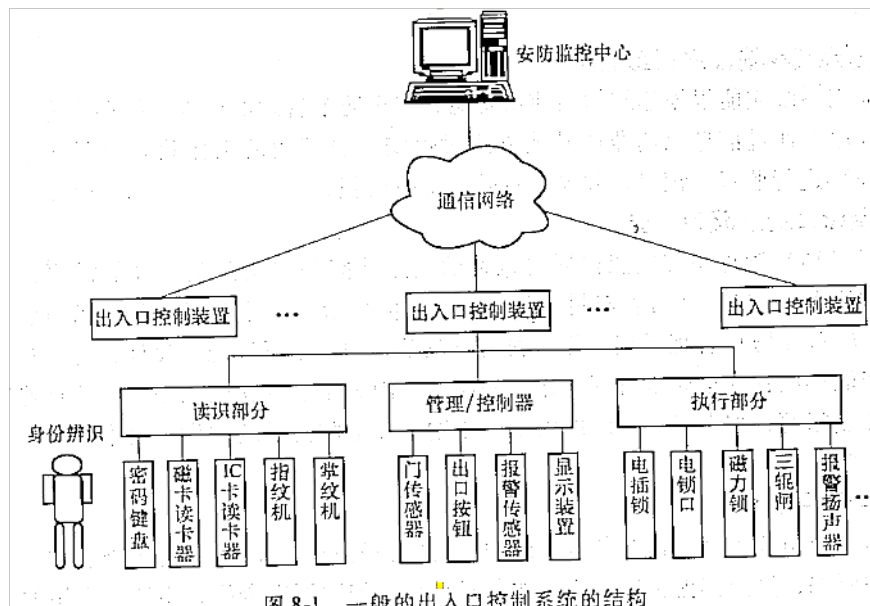


图 8-1 一般的出入口控制系统的结构

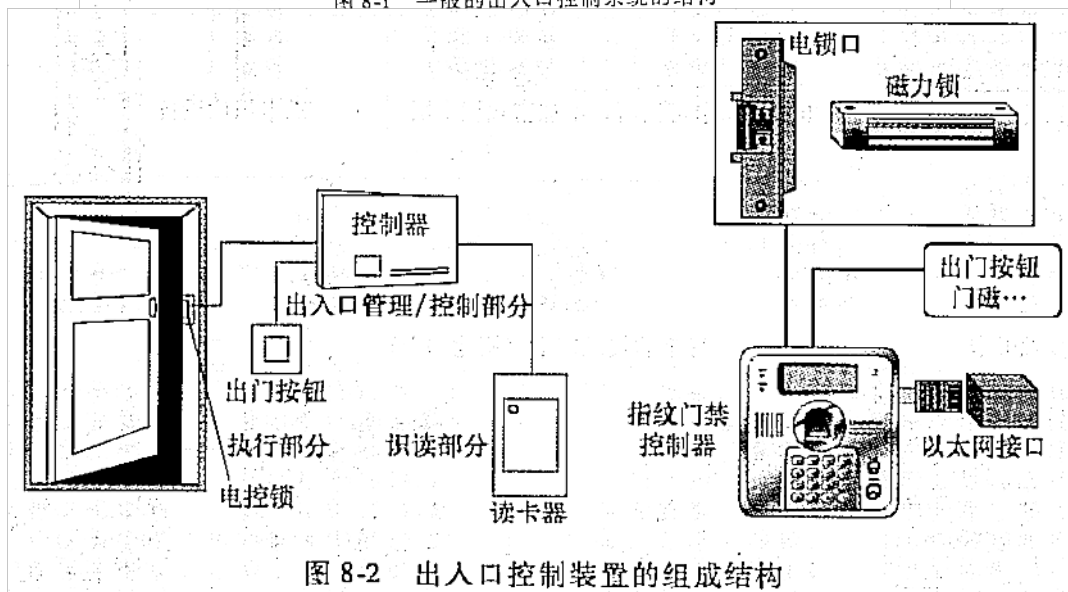


图 8-2 出入口控制装置的组成结构

圖 2.6 安全防範系統構成示意-出入口控制子系統為例

(資料來源：許錦標等，樓宇智能化技術第3版)

第三節 國外智慧建築安全計畫之相關發展

1. 利用環境設計預防犯罪 (CPTED)

J. Jacobs 於 1961 年出版之「美國大城市之生與死」(The death and life of great American cities) 提及受現代主義影響之建築及都市規劃師，在追求幾何秩序，以及威權式之藍圖規劃主流價值影響下，迷信嚴格之土地使用分區管制、超大街廓等空間規劃觀念，這使得居民無法透過建築物之開窗，觀察城市街道活動，進而發揮「自然監控」之功能，是現代城市犯罪率上升原因之一。此一觀念影響美國聖路易斯市政府，認為於二戰結束後由日本山崎實建築師，以超大街廓觀念規劃設計之 Pruitt Igoe 住宅（如圖 2.7），因欠缺自然監視，是犯罪激增原因，於 1972 年以戲劇性之爆破方式拆除，並被建築評論家形容為現代建築主義之死。



圖 2.7 欠缺「自然監控」之 Pruitt Igoe 住宅

（圖片來源：

<http://www.google.com.tw/imgres?imgurl=http://upload.wikime>

dia.org/wikipedia/commons/thumb/0/09/Pruitt-Igoe_1968March03.jpg)

美國在 1968 年於國會通過街頭安全條款，並編列預算研究防治都市犯罪增高後的新技術，由 O. Newman 與紐約市住宅，警察等部門合作，期透過都市設計的方法以預防，減少犯罪，並將研究成果出版了一本書「可防禦的空間」，他們依據公有住宅社區發生過的類型，次數，時段等資料，研究住宅社區的道路與戶外空間型態，建築配置，樓層，戶數，入口位置，門廳，樓電梯，走廊類型，開窗位置等多種條件，對照研究二者之關係，發現以下建築設計方式與犯罪數有正相關（謝園，2001）：

1. 樓層越高，居民越多的公寓大廈：95%的犯罪案件，發生在 7 層以上的公寓及規模 1000 人以上的社區
2. 越多戶數共用一個門廳，樓電梯的公寓：例如：兩棟 36 戶公寓同為三層樓，一棟每層 12 戶共用一個門廳，一座樓梯及走廊，另一棟則每層 4 戶分用三個門廳，三座樓梯，前者犯罪率較高
3. 中央走廊：有視覺死角，單邊走廊較易被戶外看到
4. 有視覺死角的戶外空間：陰暗，高而密的灌木叢，雜亂的環境，狹小窄長的空間，視覺不能穿透或遙不可及的公園
5. 一群相同型式的建築：像穿制服一樣的公寓群

而 O. Newman 透過對美國大城市建築與犯罪二者關聯性之統計分析研究，於 1973 年提出「可防禦之空間」（Defensible space）概念，認為若能透過適當之空間規劃，建立人們之「領域感」（sense of territoriality），並避免規劃大規模住宅，使得外來之陌生人容易引起注意，有助於犯罪預防，例如：社區規劃採用囊底路道路形式，會使得外來人車引起道路周圍住戶之助益，形成「自然監控」。此外，空間領域之建立，尚可透過在建築基地外部空間設置綠籬、階

梯、面對空地設置建築物開口部等各種建築手法，以減少空間「匿名性」，如圖 2.8 所示，並提出可防禦之空間四要素（表 2.5）。



圖 2.8 基地外部空間設置綠籬、階梯建立空間領域

（圖片來源：日本建築學會，建築設計資料集成-人體空間篇，2003）

表 2.5 可防禦之空間四要素

論點	說明
領域感 (territoriality)	係指土地、建築物之所有權者是否將半私有（公共）用地納入監控，將區域再加以細分，加強領域感的形成。
自然監控 (natural surveillance)	利用建築環境之設計，使土地建築所有者有較佳的監控視野，以監控陌生人之活動，在必要時採行防護措施。
意象 (image)	建築物避免過於獨特且具正面形象，減少犯罪之侵害。
周遭環境 (milieu)	指將社區安置於一低犯罪、高度監控之區域，減少犯罪之活動。

（資料來源：賴銘昌，空間型構與汽車竊盜之關聯性研究—以台灣某都市為例，2005）

英國倫敦大學之 B. Hillier 及蘇智鋒，則提出與 O. Newman 可

防禦之空間完成迥異之看法，從透過對城市空間組織與住宅竊盜犯罪紀錄之實證資料統計分析，認為社區採囊底路規劃，反而使穿越性交通減少，不利「自然監控」。並提出社區道路兩旁之住宅，若採用圖 2.9 所示「門對門」方式進行空間安排，較有利於「自然監控」（王子熙，2006）。

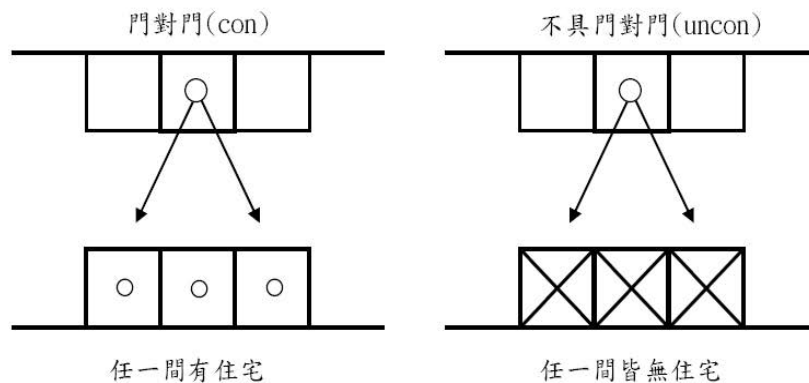


圖 2.9 「門對門」之空間安排方式有利於「自然監控」

（圖片來源:王子熙，都市住宅區空間組構型態與竊盜犯罪傾向之研究 -以台灣某城市為例，2006）

2. 美國國土安全部，建築安全規劃參考手冊

美國國土安全部過去主要投入自然災害預防，於 2001 年 911 事件後，加入恐怖攻擊等人為危害預防事務，並出版「減少建築物受恐怖攻擊參考手冊」將過去用於自然災害預防之風險管理理論，應用於人為危害預防，並提出建築安全評估模型（圖 2.10），以及風險

量化公式，供建築師、工程師進行建築安全規劃設計參考。其中，風險量化公式如下：

$$\text{風險} = \text{資產價值} \times \text{威脅等級} \times \text{建築脆弱度} \quad (\text{式 2.1})$$

式 2.1 說明：

1. 資產價值：根據建築物主要服務、使用者、訪客、建築物機基礎設施之價值認定
2. 威脅等級：根據建築物受各類恐怖攻擊、非法入侵可能性進行分級
3. 建築脆弱度：評估項目包括基地、建築物、結構系統、建築物外牆、維生系統、機械系統。管線及瓦斯系統、電子系統、火災警報系統、通訊及資訊系統、設施營運管理、安全系統及安全整體計畫。(表 2.6)

表 2.6 建築脆弱度評估項目

1. 基地
2. 建築
3. 結構系統
4. 建築物外殼
5. 電力、電信等公用事業服務系統
6. 機械系統（暖氣、通風和空調（HVAC）、化學、生物 1 和放射性物質控制）
7. 給排水管和天然氣
8. 電氣系統
9. 火災報警系統
10. 通信和信息技術（IT）系統
11. 設備操作和維護
12. 安防系統
13. 安全總體規劃

（資料來源：美國國土安全部，建築安全規劃參考手冊）

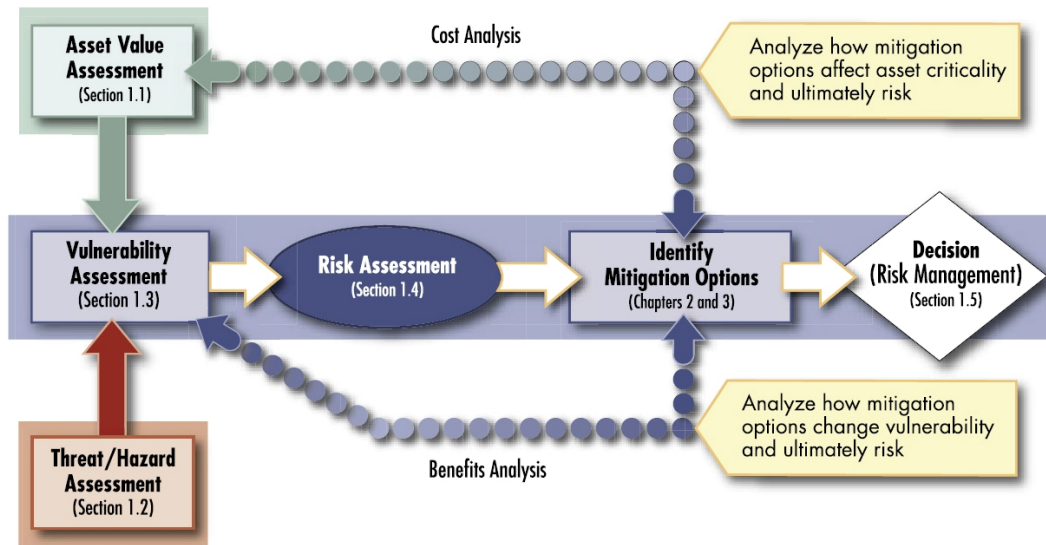


圖 2.10 發展及評估建築安全規劃設計方案之架構

(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

此外，該手冊整理建築物安全電子系統技術 (Electronic Security System, ESS)，供建築師、工程師使用。提出一個建築安全電子系統是由三個主要元素構成：探測 (detection)、延遲 (delay) 和響應 (response)。並以佈設在建築物外、內部的探測器 (sensor)、閉路電視 (CCTV)、電子入境管制系統 (EECSS)、雙數據傳輸模式 (DTM)、監測異常警報、控制系統，及各種報警和系統信息顯示系統等電子設備構成。

3. 美國建築師協會，建築安全計畫與設計指引

2001 年 911 事件後，美國建築師協會 (American Institute of Architects, AIA) 亦在 2004 年出版了「給建築師及建築設計專業的建築安全計畫與設計指引」一書，全書說明建成環境中的安全課題、安全威脅、安全設計概念、應用風險管理理論進行安全計畫評估、強化建築物、建築安全科技、使用生化及放射線物質建築物之保護等，

除介紹因應恐怖攻擊之建築安全技術外（圖 2.11），並擴及利用環境設計預防犯罪（CPTED）、甚至防止性騷擾、性侵害之課題（表 2.7），最後，並提出許多建築安全設計實例供建築實務界參考，該手冊強調將安全融入建築設計，可使建築物具有房地產市場優勢。

表 2.7 某建築安全計畫評估考慮課題例

- 來自外部人員之犯罪：如性侵，殺人，搶劫，毆打，爆竊，盜竊和破壞行為的罪行。這一類還包括外部的威脅，並包括恐怖襲擊，這些事件可以發生在車庫，停車場，或其他半公開的空間，包括鄰近的公共區域。
- 來自內部人員之犯罪：如盜竊、設備破壞。人員可能來源是組織內心懷不滿的職員、供應商等，通常這些人熟悉事先建築保全措施。
- 毒品交易和暴力犯罪：如心懷不滿員工的報復行為，員工彼此毆打，或是在工作場所買賣毒品等。
- 竊取智慧財產或資訊：此類型可能是內、外部人員之聯手的行為，包括竊取商業秘密、客戶名單、電腦資訊，和通信竊聽等。
- 性侵害和性騷擾：性侵犯和性騷擾可能發生在任何工作環境，但針對可能的性侵害，可以針對開放式或封閉式的停車場、人行道等重點進行安全評估。

（資料來源：整理自 Security Planning and Design）

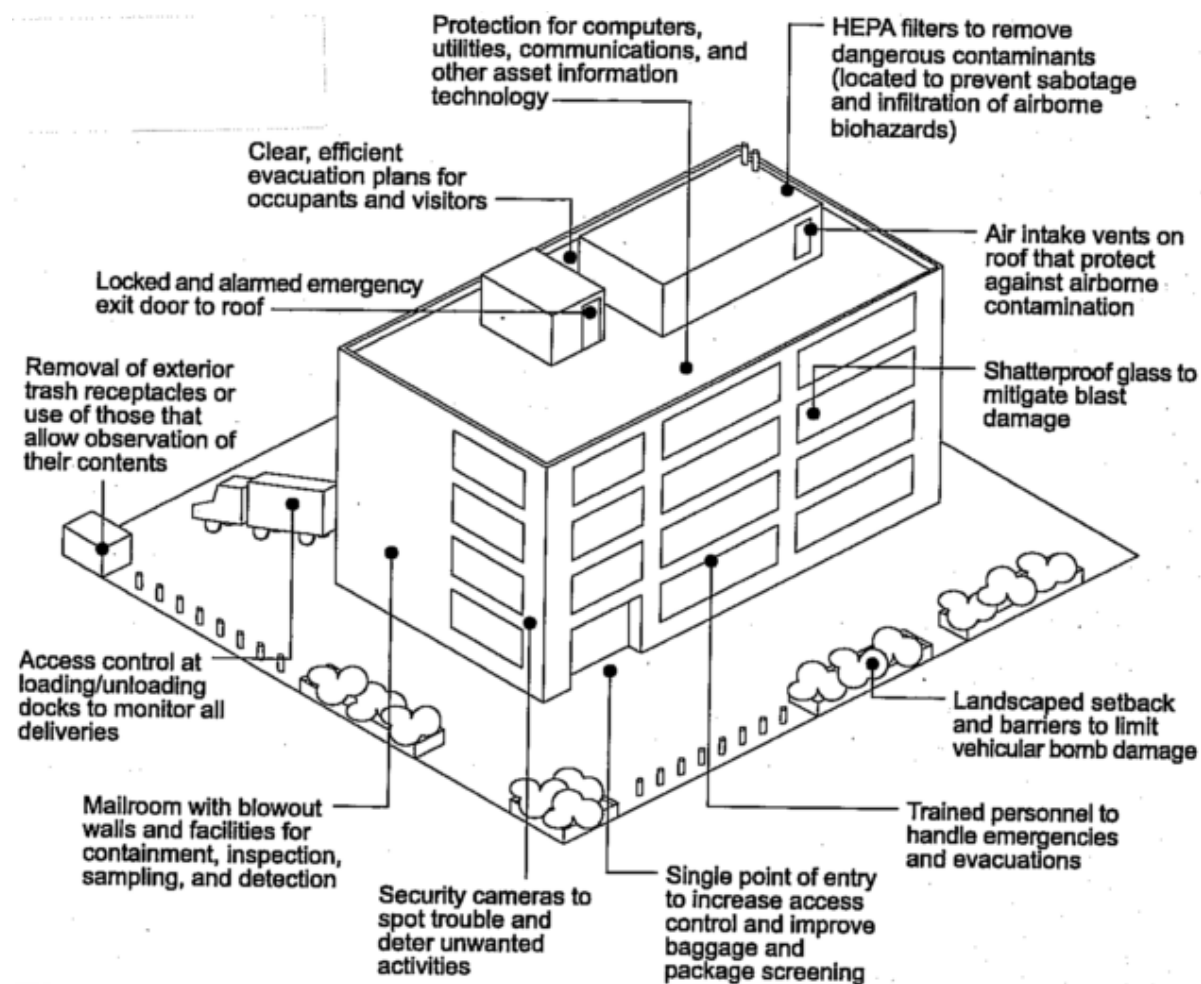
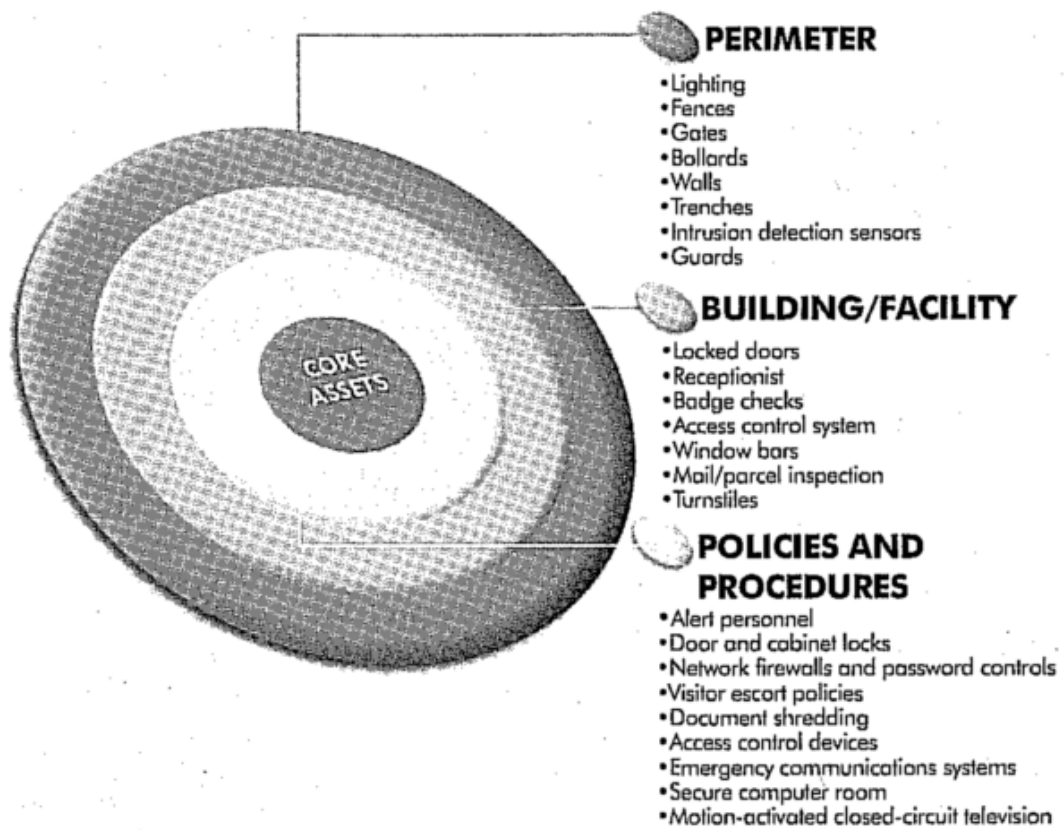


圖 2.11 因應恐怖攻擊之建築安全設計方案

(圖片來源： Security Planning and Design)

該手冊提出建築安全計畫與設計時，可依空間用途或構造劃分安全層級與區劃（圖 2.12），增加安全防禦之縱深（表 2.8），安全分層和分區提供工具CPTED的概念和策略結合使用，可將其納入建築設計的保安措施。將安全分層可分為三層：基地和地界線，建築外殼，和建築物內部，每一層都可視化為同等級的安全區。

同時也進一步提出應用「3D方法」(Designation, Definition, Design 3-D Approach)，將空間指定用途 (Designation)、考慮該空間之文化、心理、社會定義 (Definition)，彈性組合建築設計手法、機械手法、訪問控制、監視和加強領域等方法進行設計 (Design)，提升建築安全，避免受限於傳統設計經驗，依賴鋼筋混凝土牆、高安全性門鎖等方法提升安全，限制了設計之可能性。



說明：

圖 2.12 安全縱深防禦的概念

安全縱深	防禦對策
1. 基地四周	照明、柵欄、門、矮柱、牆壕溝、入侵檢測傳感器、警衛隊
2. 建築物/設施	鎖著的門、接待員、識別證檢查、門禁系統、窗台、信件 / 包裹檢查、十字轉門
3. 警衛和應急應變	快遞人員、門和櫥櫃鎖、網絡防火牆和密碼控制、訪客引導、文件銷毀、訪問控制設備、應急通信系統、安全之電腦機房、轉動之閉路電視

(圖片來源：整理自 Security Planning and Design)

表 2.8 建築安全層級或區劃

空間用途 或構造	建築安全 層級或區 劃	應考慮事項
基地四周	第一層安全防線	要考慮因素包括：地形、地貌、植被、相鄰土地用途、車輛和行人流通模式、鄰里的犯罪模式、警察巡邏的模式、視線、隱蔽性領域、公用管線位置、照明。在基地選址過程中，應首先進行安全評估與規劃。
建築物外殼	第二層安全防線	著重防止入侵或強行進入。外殼除建築物外牆、屋頂板外，還包括與外部連通之管道。可能入侵點包括：門、窗、屋頂、可爬行之高架地板、天花板內空間、管道間、下水道等。應注意加強門框、插梢、門鎖、鉸鏈、四周牆壁和門扇、窗戶玻璃材料、窗框、開口大小及五金。
建築物室內	第三層安全防線	包括在建築物內部各種具體的安全措施。例如：劃出需要特別保護之敏感區，使用安全技術、人力和限制通行路徑等方式加以組合，以便於減少安全人力成本。而在公共大堂區，則可發給賓客通行證，讓他們進入必要之室內空間、電梯、樓梯等。員工則以識別證、出入卡片，進入限制區，除可以入侵敏感區外，亦可減少交通擠塞。
安全區劃	無限制區	應注意該區可能是在指定使用時間內不受限制，例如：大廳、接待區、小吃店、某些人員和行政辦公室，和公共會議室等。動線設計上

		應使人可順利辦理業務，但不必進入控制區或限制區。
	控制區	進入這些空間應有明確進入目的，包括：行政辦公室、員工餐廳、安全辦公室、辦公室、工作區、卸貨區等場所。
	限制區	這些空間是提供經許可之工作人員使用之敏感區。限制區內部分通道可能需要額外進行出入控制。例如：金庫、敏感記錄存儲、化學品和藥品、食物配製、機械領域、電話設備、電氣設備、控制室、實驗室、洗衣房、消毒供應、專用設備等。尤其在辦公建築、學校、醫院、監獄、法院、實驗室、工業廠房等設施更為重要。

（來源：整理自 Security Planning and Design）

為有效地應用安全技術於建築物，建築師必須對這些技術有基本了解。該手冊提供了選擇和應用安全技術相關的基本課題，整合安全系統流程（圖 2.13），並提供實用安全技術介紹。

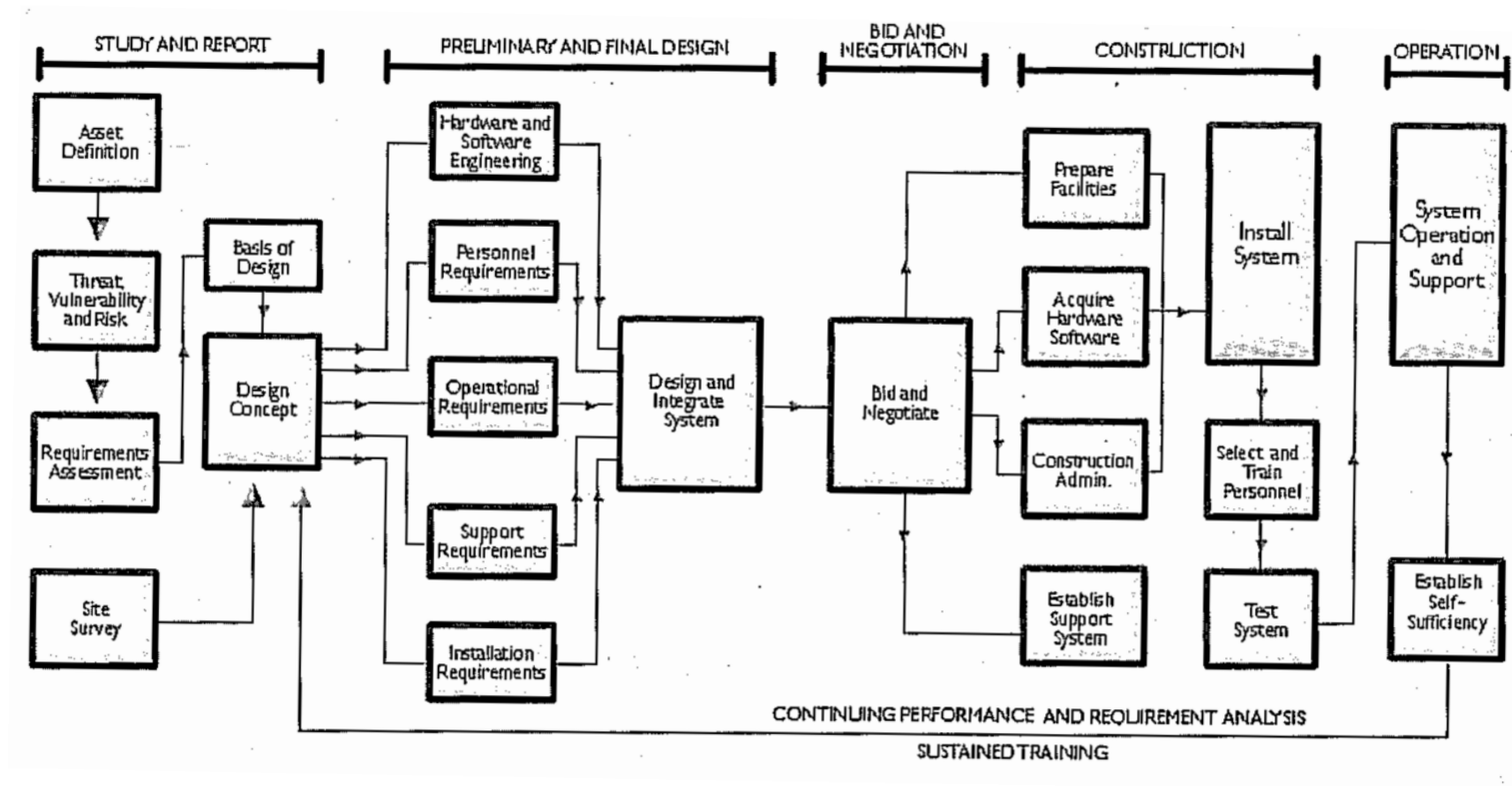


圖 2.13 整合安全系統流程

(圖片來源： Security Planning and Design)

在設計與選擇上，應確認所應用之安全技術項目是符合需求之解決方案。採用開放式、封閉式專利科技時，應考慮與其他系統相容性、應遵守建築法規，例如：使用門禁系統時，仍維持通道逃生避難功能、技術性能標準應符合美國施工規範學會（CSI）規定。選擇技術時應考慮環境條件，如：電力、電磁干擾、振動等。以及安全措施之隱蔽性和美觀，特別是不易掩飾之閉路電視CCTV，常會對開放和行動自由感造成干擾，而一些超薄訪問讀卡器，則因很容易安裝在門柱，系統安裝變得更切合美觀的考慮。出租建築物之基礎設施應選擇相容性較高之系統，以便與承租人個別安全設備兼容。初期、操作和維護成本之考慮，安裝營運完成第2年起，安全系統之維修費用，一般約為初期成本之11至12%，超過5年後，升級之成本約與建置相當。由於安全技術可以同部查看多個空間使用情形，大幅度地減少人力監測的需要，業主甚至可以在下班時間從遠端監控，使警衛及安全控制中心人員數量最小化。使用監測照明技術應提供充足的照明，該手冊建議照度如表2.9所示。

表 2.9 監測照明技術建議照度

場所	照度
大樓入口	54
人行道	16
停車場	54
基地景觀設施	5
周圍的建築	11
街道	5

（來源：整理自 Security Planning and Design）

一般建築物應用之安全技術包括：電子入侵檢測，外圍保護，訪問控制，系統和閉路電視技術。特殊高層建築或政府建築物，則可能需要額外的篩選技術。每種技術都有不同的性能特點與優勢，安裝和維護也有不同要求，因此，重要的是安裝公司應有每種技術規範，使安全管理系統能正常運作。常見安全技術包括以下六類：

1. 入侵檢測技術：使用內、外部探測器(sensor) 探測人員跨越地界或進入禁止區之訊息，它可被用來增加對保護區外或內的特定點或空格的控制，主要目的是為了提醒保安人員，人員有入侵或其他安全事故的可能性。

(1) 室外探測器技術：以單獨或重疊方式圍繞保護區佈建，可安裝於地面上圍欄或建築物，或埋設於地面下。探測器分為微波、脈衝紅外光束、被動紅外線、靜電電場、同軸電纜、光纖電纜等類型。外部傳感器安裝費用高昂，特別是配置多條檢測線路時，非常重要之保護區域通常需要兩組互相支援之檢測線。外部傳感器需要相當大之設備空間，但很容易安裝。

(2) 室內探測器技術

室內探測器在人員侵入受保護區域時，可即時探測並提供警報資訊，有效大幅減少聘僱安全人員名額。點狀探測器可保護門、窗、其他開口部，及重要和特殊財產。體型探測器可探測走廊內的入侵者及移動行為並報警。室內玻璃破碎探測器或牆壁滲透探測器檢測出所有可能的入侵情況下（例如，透過破壞屋頂、天花板或外牆後侵入）。紅外線、超音波、微波探測器是最常用的探測器。門「開關」或「接觸」是最常用的入侵檢測設備，用於高度安全性用途時，通常另配有一防拆報警（圖 2.14），紅外線和微波或超聲波裝置（圖 2.15），可在更困難環境條件和更複雜的入侵者提供更多的保護，「智能探測器」可有效減少誤報。

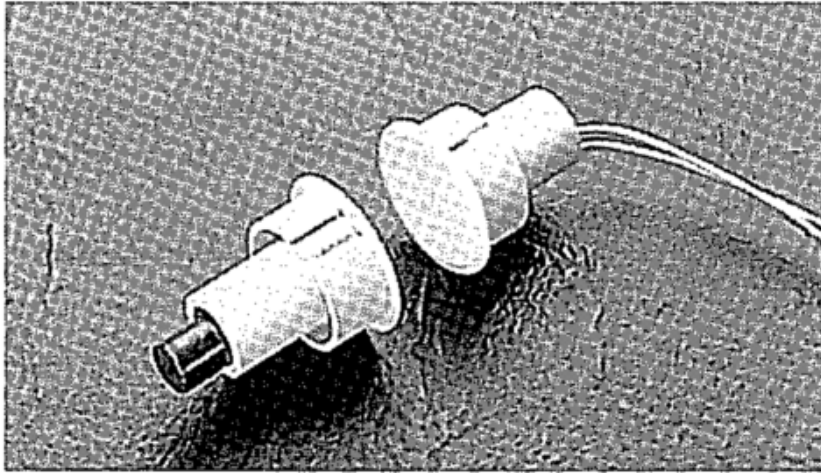


圖 2.14 探測門接觸情形之室內探測器
(圖片來源： Security Planning and Design)

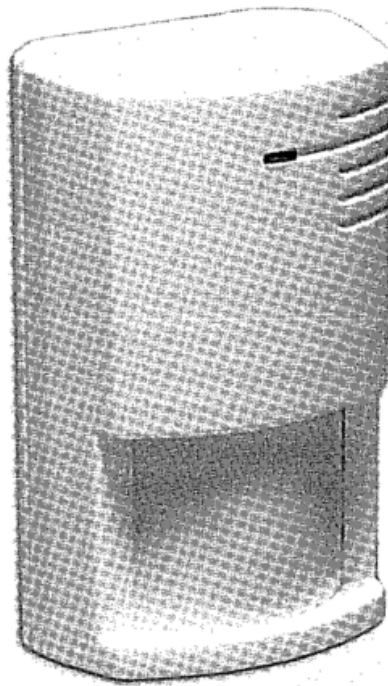


圖 2.15 被動式紅外傳感器
(圖片來源： Security Planning and Design)

(3)電子鍵盤控制裝置：通常設在入口處的，報警或訪問控制面板收集入侵傳感器和安全控制中心報告任何狀態變化的信號。

(4)面板：防盜面板通常是獨立面板。訪問控制面板，同時接受探測器和接入設備的輸入訊號，通常連結至網絡，並有發送報警、授權或拒絕訪客進入信號等功能。

2. 篩選技術 (Screening Technology)

違禁物品檢測技術已被開發出來，現在可於建築物中使用。包括：金屬探測器、X光檢查系統，已即可探測出塑膠武器、塑膠炸藥和放射性材料等爆炸物之跟蹤探測器等。門戶式或手持式金屬探測器，可以被設置在入口處為探測隱藏之槍支和其他金屬物品、並產生警報聲音。X射線系統，由人員透過投影螢幕上顯示的手提袋或行李圖像進行評估，亦可配備半自動篩選功能。

3. 訪問控制技術

訪問控制是一建築安全程序，用於允許或拒絕人、車、物品進入建築物、區域或監控其移動情形。自動訪問允許人員進入，並在某些情況下離開。

電子門禁系統採用了與電子鎖裝置，持卡人須提出識別證或編碼卡由讀卡機識別（見圖 2.16），訪問授權序列必須符合相關規範才能與設備溝通。一般情況下，電子門禁系統包括一登記站、中央控制器、授權訪問的數據庫表、交易顯示器，並控制個人進出憑證編碼。

憑證的編碼系統與傳統的鎖和鑰匙相比有幾個優點，他下放訪問授權，由一單一系統管理員從遠程位置集中管理，如果證件丟掉，可以很容易地被替換或作廢，將識別數據從系統中刪除。主機處理器不斷刷新的訪問授權資訊，記錄存儲在遠端的訪問面板中，監視遠端閱讀器，以便必要時進行調查或其他用途，供日後檢索所有的訪問活動之

歸檔記錄。

自動存取控制系統越來越普及，主要是因為成本降低。電子控制訪問和執行輔助功能。這個系統，是一中央運營商不斷提供報警顯示、控制、以及相關系統整合功能的主機處理器。隨著資料儲存容量和個人電腦處理速度提升，一整合訪問控制系統可以控制和監視多個地點、多個建築物達數以千計出入控制點。

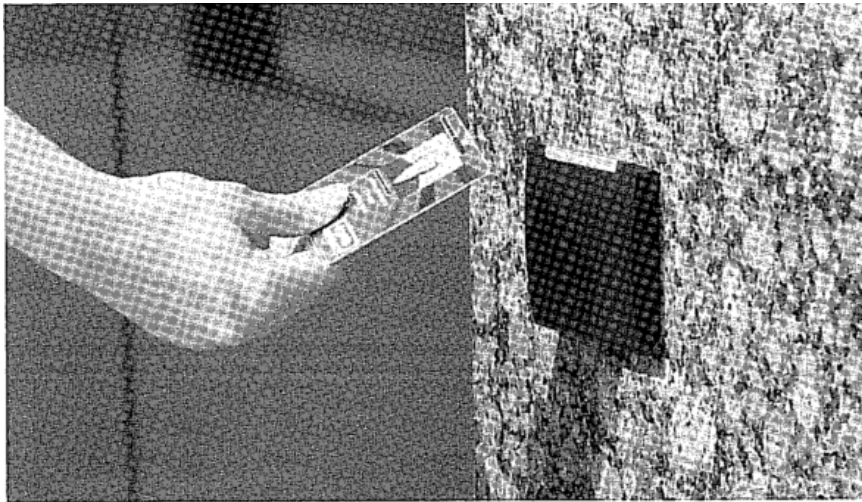


圖 2.16 接近或接觸式智能卡讀寫器

(圖片來源： Security Planning and Design)

訪問控制元素尚可以再整合光學十字轉門（圖 2.17）等阻隔設備，以便尖峰時間控制大廳、通道人數。

相關控制裝置如下：

- (1) 以卡片為基礎的進入控制裝置：電子設備讀取卡片授權碼，或拒絕卡片從特定地點進入或記錄。卡片可印照片等身份證明。有許多不同卡片技術可用，但一般喜歡感應卡和讀卡器，因為它們很容易使用，並提供比較好的安全。(圖 2.18)。
- (2) 人員識別/驗證設備：適用於高安全性要求處，這種設備可能包括編碼鍵盤、內置讀卡器、用於臉部確認之閉路電視CCTV，或生物識

別器。

(3)主機和分佈式處理遠端現場控制面板：主機處理器結合各地區的授權、時間分區、訪問規則、禁止或其他功能。以智能卡讀卡機和探測器遠端設備連接到遠處地板，人員通過報告連接到主機，或透過區域網絡進行資訊交換和報警。

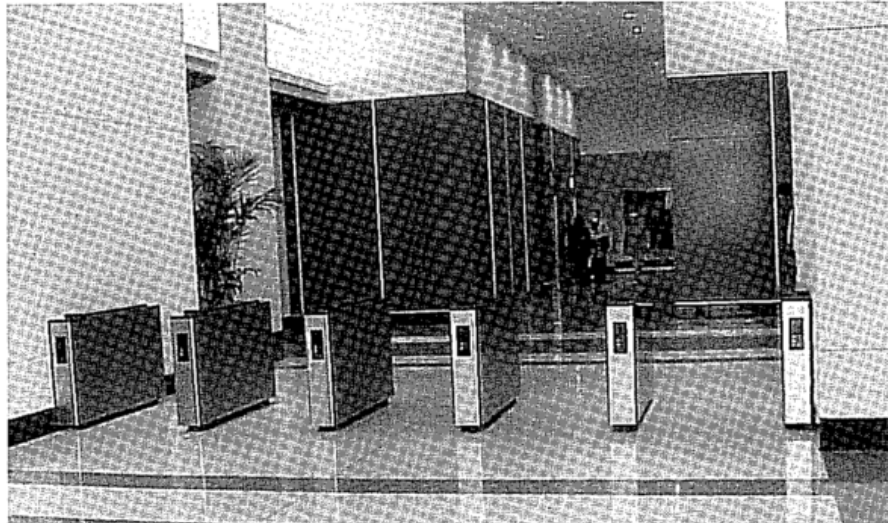


圖 2.17 光學閘門

(圖片來源： Security Planning and Design)

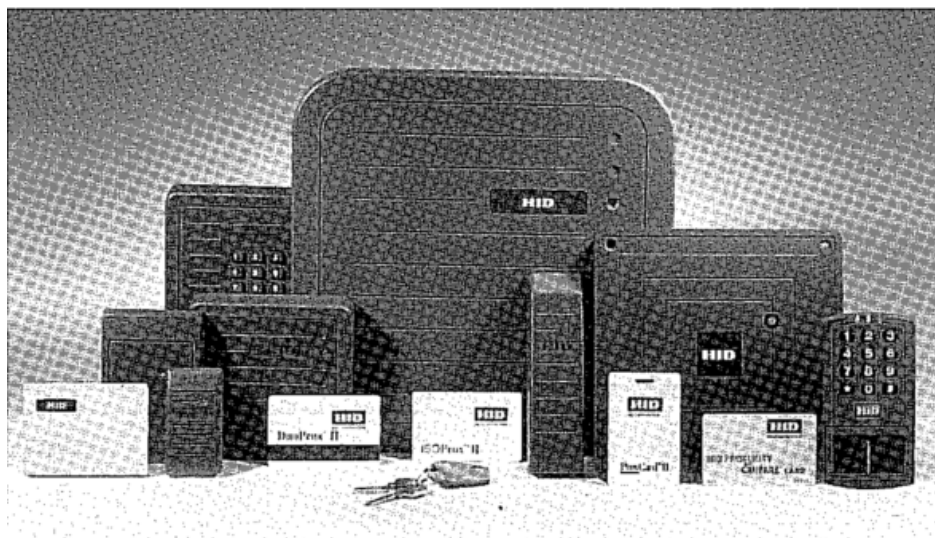


圖 2.18 訪問卡和讀卡器

(圖片來源： Security Planning and Design)

二次驗證常用的技術包括個人識別號碼（PIN）、攝影圖像比對、生物識別系統、掌紋辨識器等（圖 2.19）。PIN 是最常用的二次核査制度，因為準確的數據輸入是比較容易的。



圖 2.19 掌紋辨識器

（圖片來源： Security Planning and Design）

訪問控制鎖定五金應與自動化系統相容，包括電動門檔、電動螺栓、磁力鎖等（見圖 2.20）。設計人員須選擇適合之五金類型。一般來說，所有出口之電子訪問措施，都必須配置在火災報警事件引起故障下之安全操作模式，並裝設在某些情況下，可中斷電源請求門鎖退出之電磁鎖（見圖 2.21）。

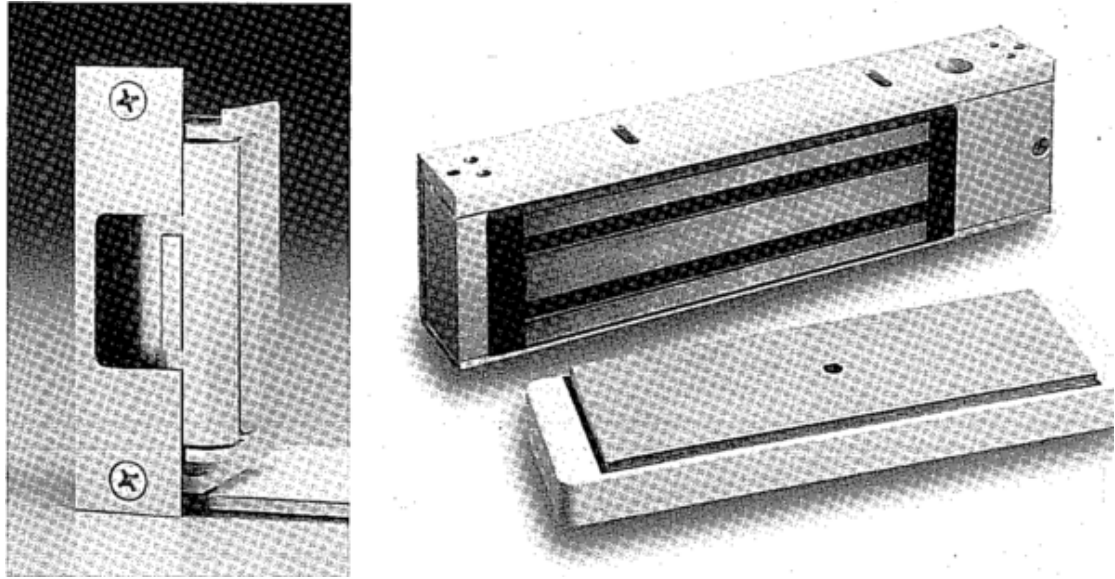


圖 2.20 電動門檔和磁力鎖

(圖片來源： Security Planning and Design)

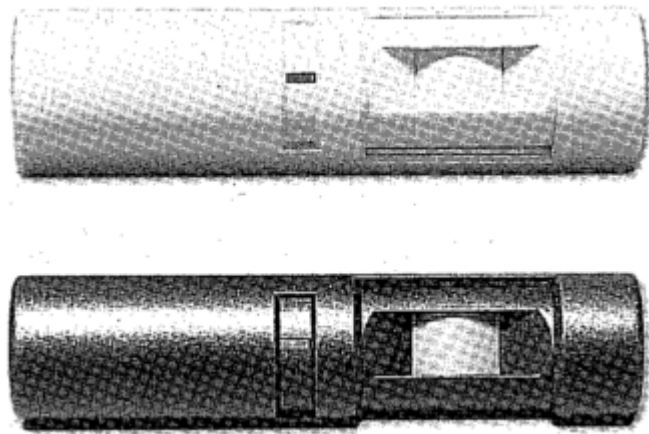


圖 2.21 請求退出探測器

(圖片來源： Security Planning and Design)

訪問控制系統的選擇還涉及到很多因素，由於從市售現成系統進行選擇時，兩個主要的考慮因素是設備和支持其使用設備之安裝公司經驗能力，無法安裝或維修，亦無法發揮詳細設計之優點。

4. 錄影監視技術

錄影監視必需注意可靠性。敏感區需有連續監測、報警評估

可以完成。可靠的閉路電視技術可以同時提供控制，以便對於威脅作出正確反應。使用遠端遙控設備直接影響到整體建設成本，因為它可以由單一營運人員，進行建築物整體安全監測和控制，並只在有需要時啟動安全反應。

中央攝影監控技術有 3 個不同但互補之功能。首先，是對警報區進行視覺評估活動，提高保安人員對可疑事件評估之有效性或提高評估效率，例如：大廳或卸貨區活動。

中央攝影監控也可以用於建築物外部和內部之監視、監測，或在關鍵領域例如：主要出入口，卸貨區、商品倉庫內之活動。自動化之活動式攝影監控裝置，應提供足夠之中央攝影監控覆蓋

中央攝影監控裝置之另一個功能是威懾。暴露在外之之閉路電視攝影機可能會阻止攝影範圍內，之可能性犯罪活動或可疑活動（圖 2.22、圖 2.23、圖 2.24）。某些錄影系統之特點是能夠在檢測到可疑活動時，自動警報，報警監視器可顯示錄影區域場景，並開始連續記錄當中之活動。

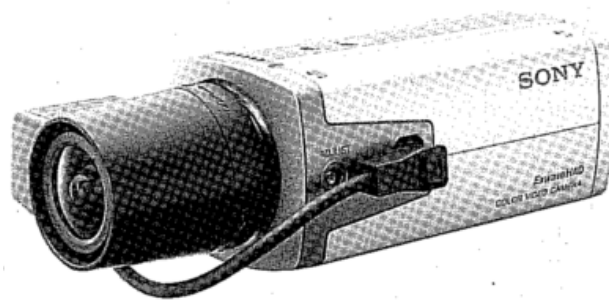


圖 2.22 固定式中央攝影監控相機

（圖片來源： Security Planning and Design）

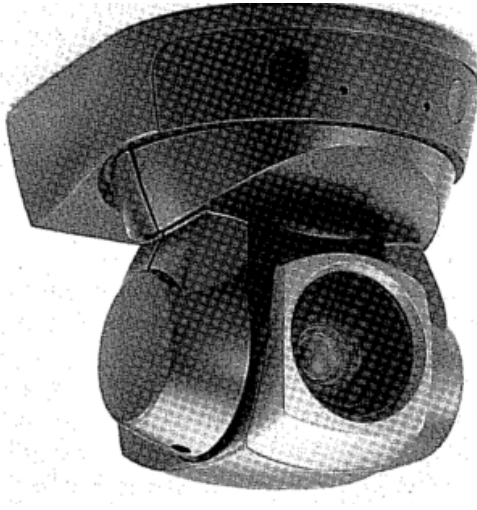


圖 2.23 雲台變焦攝像機

(圖片來源： Security Planning and Design)



圖 2.24 防爆半球攝像機 (Vandalproof dome camera)

(圖片來源： Security Planning and Design)

照明是中央攝影監控的性能和反應力之關鍵，因此，選擇的照明系統應該可支持中央攝影監控系統進行評估與監控。為了避免昂貴之既有照明環境改造，照明設計應與安全系統的設計協調。選擇攝影機位置時，必須考慮最大限度利用可用之光線。在建築物外部使用時，特別是停車場，閉路電視攝影機，最常安裝在離地面約 4.3 公尺之路燈桿上，將它們放在光源下。另一個閉路電視攝影機之共同位置是圍牆，至少離地面 4.3 公尺以上，有時甚至在屋頂女兒牆。

閉路電視攝影機位置越高，監控視角和覆蓋距離更大。但是，如果距離太遠，其功能可能無法發揮，因為相機主要是在追蹤其視野內之活動，當監控面積過大時，同時須追蹤活動可能過多。此外，攝影機亦提供額外功能，例如：交通流量監測。一基本閉路電視系統組件包括鏡頭、相機、電纜或其他傳輸介質、顯示器和相關組件。選擇合適之閉路電視攝影機，需要慎重考慮設置操作需要和性能。彩色顯示攝影機可識別出更多細節，但它們受限在日間才能發揮其功能，因此夜間攝影機將自動由彩色切換到黑色功能，或需另設光源。此外，攝影機錄影畫素是影像品質之重要因素，同時，所使用之顯示器亦必須具有同等品質，才能將拍攝之影像在顯示器上獲得最佳顯示效果。

至於顯示器之選擇應考慮中央控制台之大小和配置，以及人員報警評估之要求，減少操作人員之疲勞。須是現場決定顯示器尺寸的要求。顯示器一般提供規格為 9、15、20 英吋。可每兩個報警防區兼用一顯示器，最多不超過 5 個。具平移、傾斜和變焦控制功能之攝影機（PTZ）雖會增加額外費用，但可減少需要多個攝影機監視區域，甚至還可以通過程式進行自動平移、鏡頭自動變焦、報警和自動巡邏。

外部閉路電視攝影機之外殼形狀、安裝支架、外形美感、位置，是屬於建築師應關心之空間設計問題。近年生產之套裝相機，都受惠於小型化，並有更賞心悅目之外觀。亦可使用小型攝影機，在建築物牆壁或天花板內安裝攝影鏡頭，利用大小對比之設計手法，使攝影機變得不顯眼。

綜上所述，本節 建築物安全防範設備彙整如表 2.10。

表 2.10 建築物安全防範設備彙整

安防設備分類	原理	產品例
1. 入侵檢測	防止入侵	  探測門接觸情形之室內探測器 被動式紅外傳感器
2. 篩選	防止入侵	  貨櫃車檢查設備
3. 訪問控制	防止入侵	  讀卡機 與自動化系統相容之磁力鎖
4. 錄影監視	攝影監控	   各類CCTV

(資料來源：本研究整理)

第三章 智慧建築安全防範設備空間設計準則之研擬

本章首先，提出定義智慧建築安全防範設備。其次，依據國內、外相關文獻分析結果，彙整研擬智慧化建築安全防範設備空間設計應考慮項目，最後，嚐試研擬智慧建築安全防範設備空間設計準則，藉由系統化思考協助建築師觀察基地條件、解釋設計方案之意義、累積專業經驗、進行創意設計、檢討反省設計問題之思考架構，以便於引導建築師妥適應用智慧建築安全防範設備，發展安全之建築設計方案，使建築物具備主動感知之智慧，成為更為人性化之安全空間。

第一節 智慧建築安全防範設備定義

一、智慧建築由「自動化綜合管理」轉變為「國家資訊高速公路」節點發展歷程

美國康乃狄克州哈特福特市於 1984 年 1 月完工之「城市廣場大廈」(City Place Building) 被認為是世界上第一幢智慧建築（圖 3.1），建築高度 163 公尺、地上 38 層樓，除地面層為商店外，主要作商業辦公使用，設計人為美國著名之 SOM 建築師事務所，該建築物使用電腦將建築物內之空調、給水、防火、防盜及供電系統進行「自動化綜合管理」，並對建築物使用者提供語音、數據等資訊服務，創造舒適、便利、安全之環境。（王娜，2010）



圖 3.1 美國康乃狄克州城市廣場大廈

(圖片來

源：<http://keepitupdavid.wordpress.com/2011/05/16/piles/>)

後因 20 世紀末各國重視電腦及網路科技發展之未來發展趨勢，尤其美國柯林頓政府於 1993 年公布「資訊通信基礎建設行動綱領」(The National Information Infrastructure: An Agenda for Action)，該綱領包括三大部分：網路實體的建設(即建構「資訊高速公路」)、建立資料庫、應用軟體研發及推廣，透過稅率鼓勵私人企業籌建「資訊高速公路」、研發先進電腦與超高容量高速網路、電子資料庫來改善全國資訊應用基礎環境，並以「可負擔價格」提供所有美國國人使用。在此之後，「資訊高速公路」之建設成為日本、歐州、新加坡等先進國家資訊科技建設之重要任務，台灣則在 1994 年 9 月設置行政院「國家資訊通信基本建設專案推動小組」。而智慧建築作為資訊高速公路重要節點之一，也因此成為 21 世紀建築設計之時代性課題之一。

二、現行建築法規欠缺建築設備整合規定，各設備單元之間無法透過網路交換資訊

建築法第 10 條規定：「本法所稱建築物設備，為敷設於建築物之電力、電信、煤氣、給水、污水、排水、空氣調節、昇降、消防、消雷、防空避難、污物處理及保護民眾隱私權等設備。」。

而建築技術規則建築設計施工編第 116 條之 2 規定，供公眾使用建築物之公共空間，應採取建築物安全維護設計，而為達成建築物安全維護設計，應採用 4 種規定之「安全維護裝置」，包括：照明、監視攝影、緊急求救、警戒探測。

另建築技術規則建築設備編第 3 條規定：「建築物之各處所除應裝置一般照明設備外，應依本規則建築設計施工編第 116 條之 2 規定設置安全維護照明裝置，並應依各類場所消防安全設備設置標準之規定裝置緊急照明燈、出口標示燈及避難方向指示燈等設備。」。

以上規範係將敷設於建築物之不同功能設備視為各自獨立之機械裝置，敷設於建築物內之「各設備單元」之間，及「各設備單元」與管理者之間無法資訊、信號進行「溝通」，容易造成功能重複、無法互補，或無法即時因應環境負荷、使用行為，開關或調整設備運轉方式等問題。

三、21 世紀之後智慧建築應強調以電腦及網路進行建築設備整合

歐洲學者 Harrison 曾提出「智慧建築金字塔」模型，以 5 個時期，說明智慧建築概念之演進：(圖 3.2)

1. 第一階段 1980 年代以前：將建築物內之設備視為各自獨立、彼此無關之單一裝置或設備 (Single apparatus)。
2. 第二階段 1980 至 1985 年代：將建築物內之安全、進出控制、空調、電話、傳真、電視等，視為各自獨立、彼此無關之單一功能、

- 專用系統 (Single function/dedicated systems) 裝置或設備。
3. 第三階段 1985 至 1990 年代：已可進一步將建築物內之安全、進出控制裝置整合為保全及進出控制多功能系統裝置或設備；電話、電視則整合為影像多功能系統裝置或設備。
 4. 第四階段 1990 至 1995 年代：將敷設於建築物內之裝置或設備分別整合為建築自動化、通信二大系統，並能與遠端監控、可傳遞地聲音、資料之細胞通訊技術進行整合，以便與建築物外部服務、資訊連結。
 5. 第五階段 1995 至 2000 年代：透過電腦整合之敷設於建築物內之裝置或設備 (Computer integrated building, CIB)，並可透過網路進行管理或工作。
 6. 第六階段 2000 年代之後：藉由智慧型網路組合，逐漸形成智慧地區/城市。

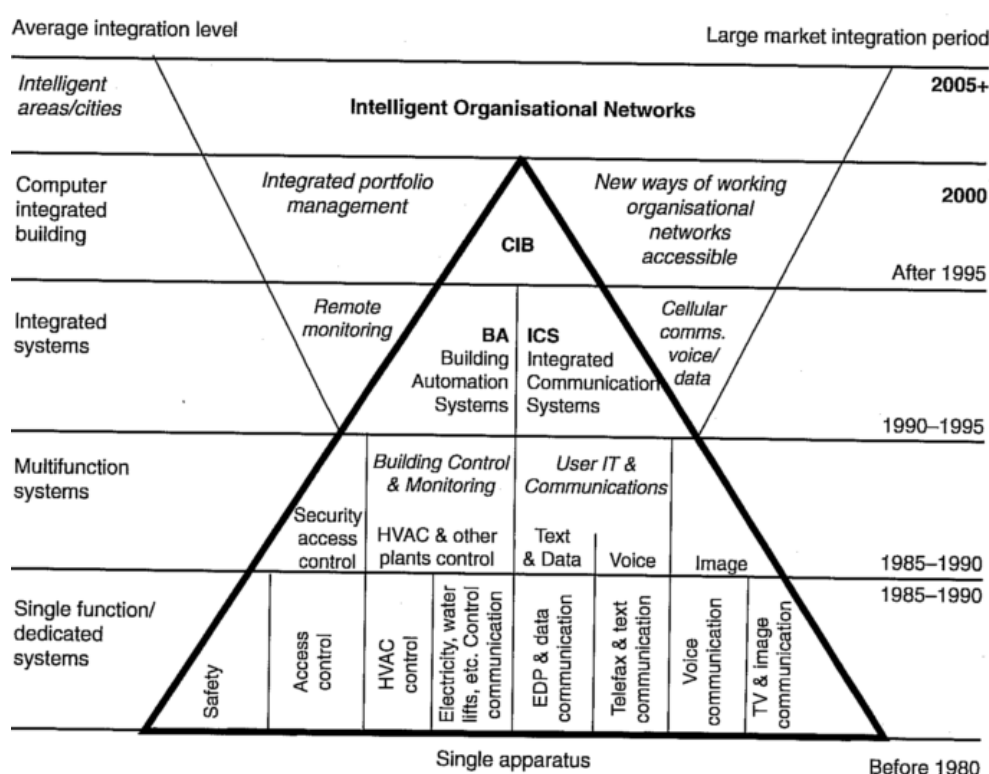


圖 3.2 Harrison「智慧建築金字塔」模型

(圖片來源：Intelligent Buildings：Design Management and

Operation)

根據以上智慧建築之理念，及現行建築設備之定義，本研究認為「智慧建築安全防範設備」應具有三種涵義：

1. 首先，以透過電腦整合敷設於建築物內之裝置或設備，並可透過網路進行監視控制。
2. 其次，具有感知環境負荷變化之能力。
3. 最後，則是即時因應環境負荷變化，使安全硬、軟體裝置及服務運轉最佳化。

依以上涵義本研究將「智慧建築安全防範設備」定義如下：

「指透過電腦及網路將敷設於建築物之進出控制、入侵報警、攝影監控等安全硬體裝置、相關軟體及服務進行最佳化整合，使建築物具備主動感知、防止及紀錄危險事件，確保建築物內使用者生命及財產安全之設備。」

第二節 智慧建築安全防範設備空間設計準則原理

一、 建築安全防範空間計畫要素及設計思考流程

關於建立安全防範系統之基本要素有許多學說探討，包括：

1. 四要素說：打消 (Deny)、阻擋 (Deter)、延遲 (Delay)、偵防 (Detect) (黃富源，2006)
2. 三要素說：探測 (Detection)、延遲 (Delay)、反應 (Response) 說 (中國建築學會建築電器分會，2010)
3. 環境設計預防犯罪三原則說 (CPTED)：出入口控制、視覺監視、領域強化。
4. 十要素說：欺敵 (Deceive)、阻擋 (Deter)、預見敵意 (Anticipate)、打消 (Deny)、偵防 (Detect)、延遲 (Delay)、評估 (Assess)、救援部署 (Deploy)、抵銷 (Neutralize)、減緩 (Mitigate) (Sewell，2004)

為便於建築設計者能應用以上原則，發展有利於安全防範之建築設計方案，本研究將建築安全防範空間計畫要素，簡化為於人身安全事件發生前、中、後，七大安全防範要素，並列舉可應用之建築設計手法及機械手法，如表 3.1 所示，建築設計者可先依該計畫要素研擬整體建築安全防範空間計畫，再進一步決定是否選用建築設備？並進行設備空間細部設計。(表 3.1、圖 3.3)

表 3.1 建築安全防範空間計畫要素

		安全防範原理	建築手法	被動式機械手法	主動式機械手法
人身安全事件	發生前	防範為先，阻礙犯罪者進入(Deterrence)	設置圍籬、圍牆 立領域感 門鎖	設置刷卡機、指紋機等、對講機	設置探測器感測入侵、刷卡機、指紋
	發生中	(1) 提早察覺犯罪行為，通報警察處理(Detect) (2) 利用警報聲響引人注意(Conspicuousness) (3) 拖延犯罪者接近目標物時間(Delay)阻斷犯罪者接近目標物通道(Deny) (4) 阻斷犯罪者逃出建築物(anti-removal design)	增加牆厚、加強材質、設置多道牆體、動線分區	電話、手動式緊急求救設備	機、對講機 警報設備、門窗開關、出入口或通道門鎖、連動、錄影監視
	發生後	利用攝影監控(Surveillance Cameras)進行證據保全	將建築物開口方位面對街道、防火間隔、前後側院，以便於社區居民進行「自然監視」	錄影監視	

(資料來源：：本研究整理)



圖 3.3 建築安全防範空間設計思考流程

（資料來源：本研究整理）

二、 建築設計方案安全評估方法

建築物設計人可在完成初步建築設計方案時，以風險管理方法進行評估方案之安全性，其中，資產價值與起造人、所有權人或住戶投資於建築物之經費、以及建築物遭破壞所導致之損失有關，而威脅發生可能性與犯罪率、恐怖攻擊活動頻率因素有關，以上二者並非建築設計可控制之因素，惟可參考式 2.1，藉由調整建築設計方案以減少建築物之脆弱度（表 3.2）。

$$\text{風險} = \text{資產價值} \times \text{威脅等級} \times \text{建築脆弱度}$$

表 3.2 建築脆弱度評估項目

項次	脆弱度評估因子
1	基地
1.1	遏制不受控制車輛接近建築物
1.2	設周邊柵欄或其他類型人流控制，過濾訪客
1.3	在受保護區域周邊規劃檢查車輛之空間
1.4	是否可能從基地管線潛入？
1.5	基地或建築物現有車輛障礙設施
1.6	安全緩衝距離
1.7	街道家具、雕塑、綠化可作為阻止車輛之障礙
1.8	規劃基地交通動線，減少車輛的速度
1.9	提高步道、樓梯間、門廳、電梯間、各停車位可視性，觀察人員進入和離開
1.10	基地景觀設施和街道家具是否提供許入侵者隱匿藏身之處？
1.11	信箱開口過大易遭投入爆裂物
1.12	基地是充足的照明，確保人員安全進入和停車區，現場照明應配合閉路電視系統。
1.13	規劃設計行人和車輛動線、建築物開口部應避免基地外部窺視重點保護區。
1.14	車輛和人員管制區標誌應簡單清晰
1.15	考量消防車等緊急車輛進入建築物活動空間，考量基地消防栓位置
2	建築
2.1	基地規劃和建築設計是否納入通過環境設計預防犯罪策略（CPTED），重點是建立可防禦空間： 1、自然出入控制：

項次	脆弱度評估因子
	<p>街道、人行道、建築物人車入口應清楚地界定公眾私人禁止進入區域</p> <p>2、自然監控：</p> <ul style="list-style-type: none"> -基地規劃和景觀設計集中行人活動、限制入口/出口，消除隱匿的機會以利自然監控。 -門窗設計應最大限度保持街道、停車區、建築入口可視性 -灌木應保持高度 60 公分以下，維持可視性 -喬木樹枝保持離地面至少 2.5 公尺 -行人和車輛動線應易於管制 -外部空間應有充足之夜間照明 <p>3、加強空間領域感：</p> <ul style="list-style-type: none"> -定義私人財產界線 -利用景觀植栽設計、動線安排、牆、路障、標牌、籬笆區分私人/受限制空間使用，與公共空間分離 -利用交通障礙的設備管制車輛 -賦予空間明確用途減少「失落之空間」。 <p>4、重點區安全補強：</p> <ul style="list-style-type: none"> -門窗設鎖禁止進入 -採取出入控制措施（住戶/訪客停車）和入侵檢測系統 <p>5、設置閉路電視攝影機。</p>
2.2	出入複雜之出租建築物，可利用門廳分離、訪問控制、加強分區。
2.3	基地及建築物垃圾桶、郵箱和街道家具開口的大小應限制，避免被用來隱藏爆炸裝置，
2.4	如果預計建築物外會有排隊行為，應規劃基地專用排隊區、入口雨遮，避免訪客佔用建築物管制空間

項次	脆弱度評估因子
2.5	公共和私人活動分開了嗎？ 公共廁所、服務空間、樓梯或電梯應位於公眾入口附近
2.6	員工及訪客通過主入口點之管制措施：可視簡潔之指示牌設計、大廳接待員活動空間設計、電子門禁控制系統等電子安全設備空間
2.7	區分員工和訪客搭乘電梯
2.8	安全防護重點建築物應設識別檢查，電子門禁、十字轉門、金屬探測器和 X 射線設備空間
2.9	動線設計避免無關人員可對內部空間及活動一覽無遺
2.10	關鍵建築構件補強：包括：應急發電機、燃油系統、水箱、消防、主開關、電話分佈、控制中心、不間斷電源系統控制、疏散和救援需要、主系統和備份系統應分。
2.11	收發室和卸貨區與主要建築物分離，可採當幾幢建築物共享一個收發室，降低風險，並簡化保護措施。
2.12	收發室有足夠的空間設備可用來檢查傳入的包和爆炸物處理容器
2.13	樓梯間保持正壓（可能需要特殊的過濾）或其他煙霧控制系統
2.14	劃分建築物的安全分級
3	結構系統
3.1	增加贅餘力避免受人為爆炸攻擊而倒塌
4	建築物外殼
4.1	特殊建築物窗戶可採防爆玻璃材質
4.2	重要防護空間採無窗戶設計，仍應注意遭強行破壞侵入
5	給水電力電信系統.
5.1	生活用水是否有一個安全替代飲用水供應嗎

項次	脆弱度評估因子
5.2	確保只有授權人員可接近供水設施
5.3	設計備用電源供應設備空間
5.4	是否有多個電話和備用通信服務設備空間？
5.5	水、電、通訊等重要維生管線應採隱埋、設備箱保護設計。
6	機械系統（HVAC 及生物化學放射線防護）
6.1	進氣口應設在屋頂或盡可能提高，以防止遭投擲有害物質。
6.2	特殊建築物應有 HEPA 等空氣過濾器處理化學、生物和放射性污染物質
6.3	建築自動化和控制資訊系統入侵可能會危及系統運作，應列入安全防護空間重點區，並允許快速關機。
6.4	是建築資訊、電路圖、設備運轉程序、計劃技術規格的資訊應受到嚴格控制，並只提供給授權人員。
6.5	空調維修人員應有適當的訓練，程序和預防性維修時間表，以確保 CBR 的設備功能。
7	配管及瓦斯系統
7.1	給水管採中央管道間設計較分散式立管配置更加脆弱
7.2	單一熱水燃料來源比多種來源和多種類型的燃料更脆弱。
8	電子系統
8.1	緊急和普通的電氣設備應分別安裝在不同的地點，並盡可能相距甚遠。
9	通訊與資訊技術系統
9.1	應設有主電話配電室、通信系統佈線室、主配電設施、數據中心、路由器、防火牆、伺服器、資訊備份場所，並位於安全重點區域，確保只有授權人員可接近，防止系統被篡改。

項次	脆弱度評估因子
9.2	電話系統應有不間斷電源（UPS）
9.3	重要防護空間應提供備用通信設備所需空間
10	設備操作和維護
10.1	是否有標示主要基礎設施位置和性能，並和現況相符的之圖說文件，與更新操作和維護手冊。
11	安全系統
11.1	選擇之黑白色或彩閉路電視攝影機確實可進行每天 24 小時、每週 7 天之監測之記錄，並考慮夜間彩色攝影機影像品質較差，應混合使用黑白攝影機。
11.2	外部攝影機可考慮防止炎熱、寒冷天氣之保護。
11.3	在重要的公共區域、車庫和停車場，及其他高風險的地點應提供呼叫管理指揮人員按鈕、報警按鈕或感知器
11.4	對講通話箱在停車區或沿建築物週界嗎？
11.5	設置外部及屋頂入侵檢測玻璃破碎感知器、電子籬笆，防止入侵
11.6	閉路電視攝影機位置及外殼應有防止暴露或篡改之考量
11.7	應有訪問控制系統的備用電源供應設備空間
11.8	收發室應受到保護，只有授權的人員允許進入篩選郵件。
11.9	任何有潛在危險的化學品、易燃、有毒物質應儲存監測區，避免入侵者接觸。
11.10	安全控制室應有足夠大小及擴充空間，並有良好環境控制品質（例如：空調、照明、空氣流通、備用電源），符合人體工程學設計。
11.11	設置電子巡更系統，驗證安全人員到站巡邏地點、日期和時間。

項次	脆弱度評估因子
11.12	金庫或保險箱除加強牆體、樓地板、門窗外，可能還需要安全感知器和閉路電視攝影機設備。
12	安全體系文件
12.1	應繪製安全系統竣工圖概述系統規範和佈局使用安全設備，是故障排除，更換和添加其他安全系統的硬體和軟體之重要參考文件。
13	安全總體規劃 (Security Master Plan)
13.1	研擬基地或建築物書面安全的總體規劃方案概述的策略方向、願景、操作、管理和技術、使命，並提供達成目標之路線圖。

(資料來源：本研究整理)

第三節 智慧建築安全防範設備空間設計準則之研擬

建築物設計人可在完成初步建築設計方案時，以風險管理方法進行評估方案之安全性，其中，資產價值與威脅等級並非建築設計可控制之因素，惟可參考以下設計準則，藉由調整建築設計方案以減少建築脆弱度。

一、敷地計畫與都市設計方面：

1. 基地周圍建築開口部調查：

善用基地周圍建築條件，將容易成為入侵地點之門窗等弱點場所設置於鄰房使用者視線可視範圍，或是公共監視設器監控範圍內之位置，同時亦應考慮鄰房使用年限，改建後之影響等因素。(圖 3.4、圖 3.5)

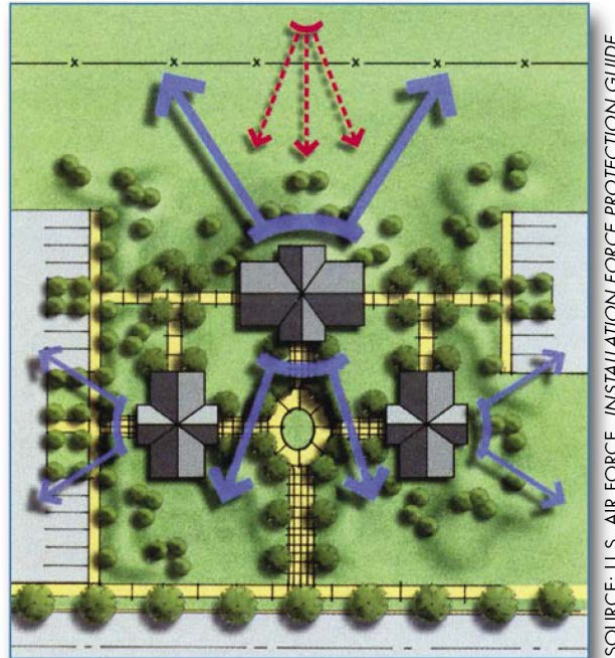


圖 3.4 善用基地周圍建築條件進行自然監控

(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

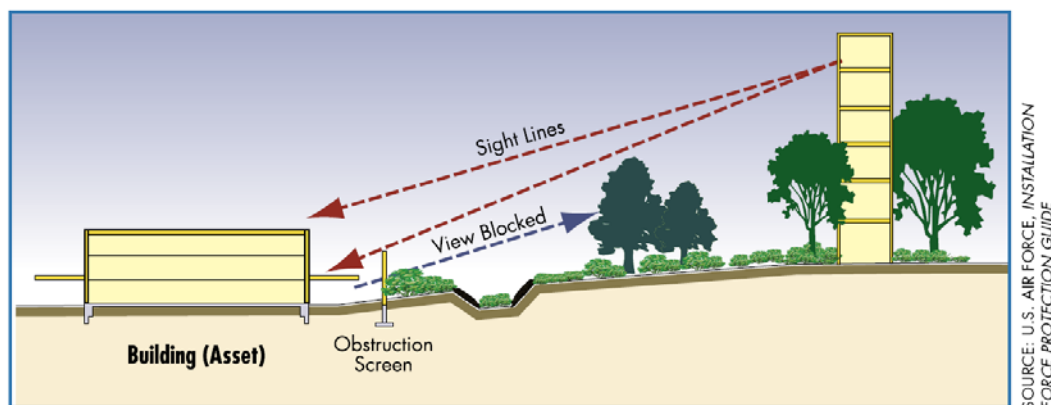


Figure 2-6 Improper building siting and view relationships

圖 3.5 善用基地條件增加建築物受自然監控之可能
(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

2. 基地周界設計：

良好之基地周界安全設計，是建築安全設計之第一道防線，對於政府機關、地標建築等易受恐怖攻擊之建築物，亦應評估於基地外部空間設置可防止汽車炸彈攻擊之景觀式圍籬或汽車障礙物，或設置透空式之垃圾桶，以便於觀察內部是否遭放置可疑爆裂物，使安全與建築美學能達成平衡。(參圖 3.6、圖 3.7)



圖 3.6 兼顧建築美學之汽車障礙物

(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

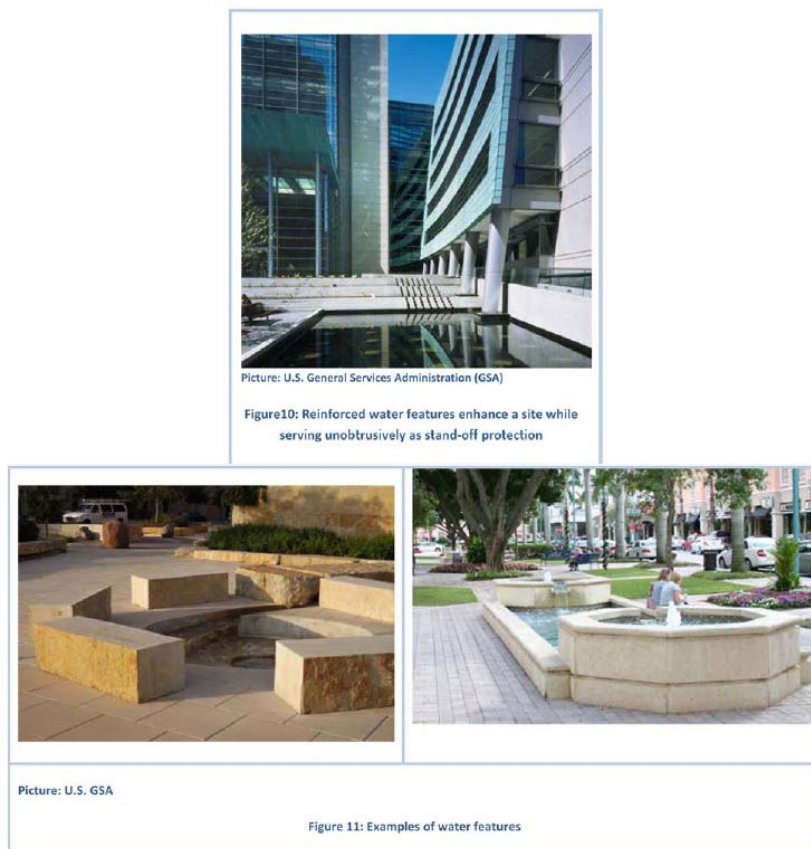


圖 3.7 兼顧建築美學之汽車障礙物

(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

此外，除設置圍牆外，對於安全敏感區亦可設置電子籬笆或外部感測器手法，將入侵者阻絕於基地外（參圖 3.8）。

Taut wires	These are wires that are stretched along a fence and have an electric current running through them. The alarm system connected to these wires is usually configured to give an indication if the wires are cut, pulled or bridged (electrically). In some cases taut wires can also be configured to convey a non lethal electric shock if touched. Taut wires may be installed in a variety of configurations such as on top of a fence or outside it.	
Infrared active motion detectors	Infrared active motion detectors project infrared light towards a designated area. When an object passes through the lighted area, the sensors send a signal to the relevant command centre. These detectors can be installed in such a way as to be almost completely unobtrusive.	
Video Motion Detectors (VMD)	VMD is a video imaging based surveillance system. The VMD system monitors a specified area; any change in the picture of the monitored area will trigger an alarm. An intruder might see the VMD cameras but has no way of knowing if they have motion detecting capabilities.	
Vibration detectors	Vibration detection systems are usually based on vibration sensors that are installed on wires which run through the length of a fence. An intruder trying to climb the fence will cause an alarm to be triggered in the command centre.	
Microwave motion detectors	Microwave motion detectors project microwave beams in order to create an invisible line. Crossing this line will send a signal to the command centre. Microwave detectors are usually noticeable and hard to conceal.	
Weight detectors	Weight detectors are used to detect someone applying pressure against the top of a barrier wall or laying a ladder against it. These detectors are made out of coils that are covered by light material. When the material covering the coils is bent, as a result of the weight of someone climbing onto the wall or for some other reason, the detectors will send a signal to the relevant command centre.	
Infrared beam detectors	Infrared beams are usually used to create an invisible line or web. When the line/web is crossed the system sends a signal to the relevant command centre. These detectors are usually relatively noticeable.	

圖 3.8 電子籬笆例

（圖片來源：Guidelines for Enhancing Building Security in Singapore.）

3. **增加安全縱深：**增加建築物與基地界線間之退縮距離，可以增加人員反應時間。(參圖 3.9)

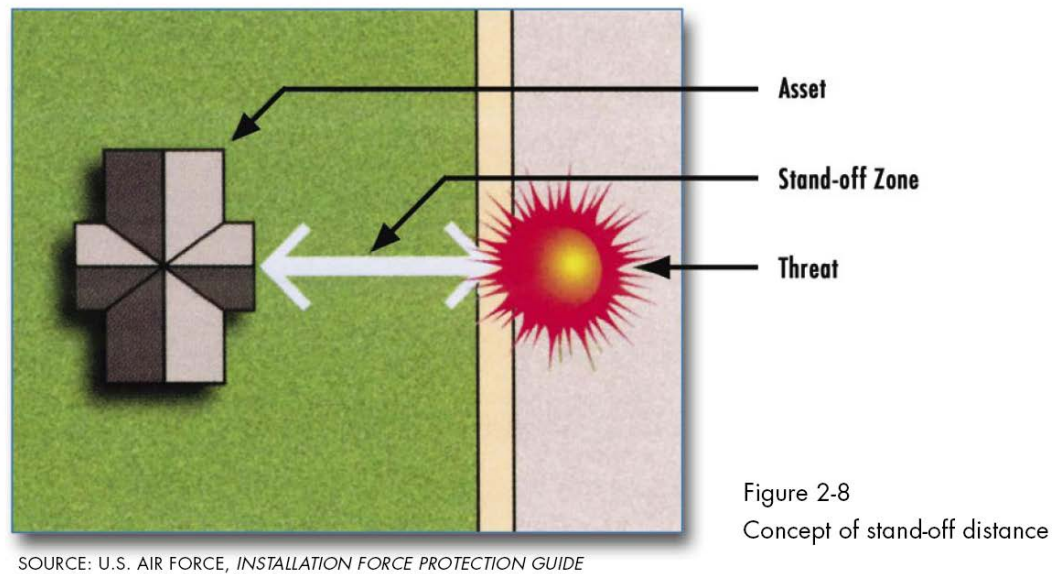


圖 3.9 建築物與基地界線間之安全縱深可增加人員反應時間
(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

二、 建築設計方面

1. **建築物形狀與方位：**進行建築設計時，盡可能增加「自然監控」，例如：將建築物外牆線與基地界線維持非平行可使「自然監控」可視範圍擴大。(參圖 3.10)

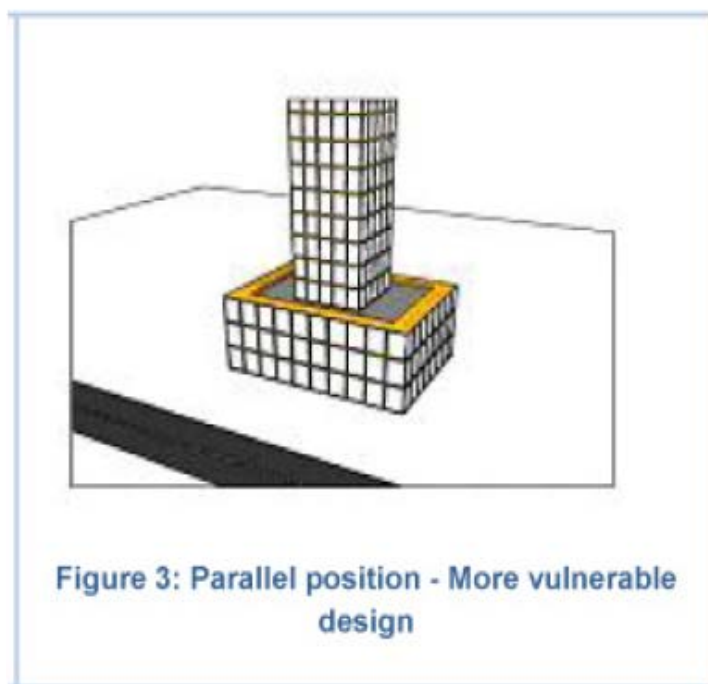
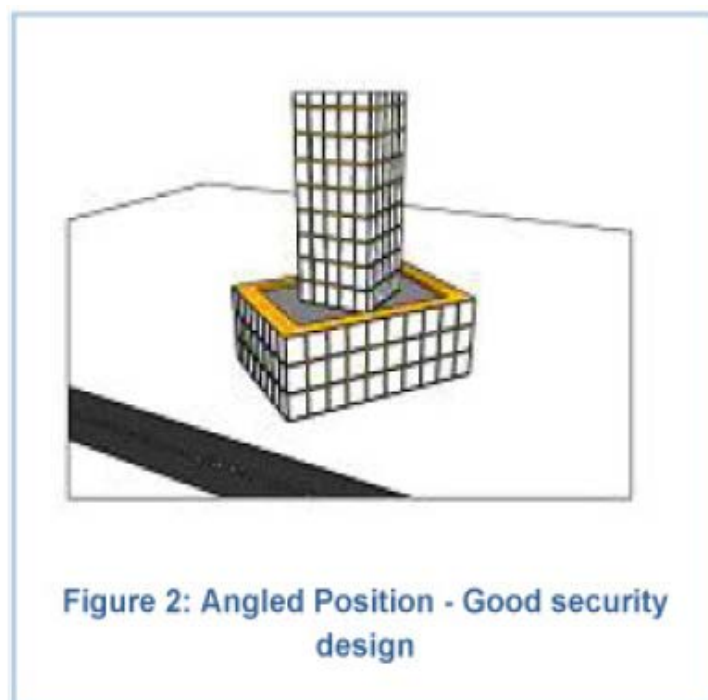


圖 3.10 調整建築形式擴大「自然監控」可視範圍
(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

2. 建築空間安全分層、分區：

為降低設置門鎖、鐵窗、雇用警衛人員，或採用相關建築安全設備等費用成本，可依建築空間用途劃分安全等級，進行空間布局、設計動線，將重要敏感區域集中配置，降低安全監控設備、警衛人員數量及成本。(參圖 3.11)

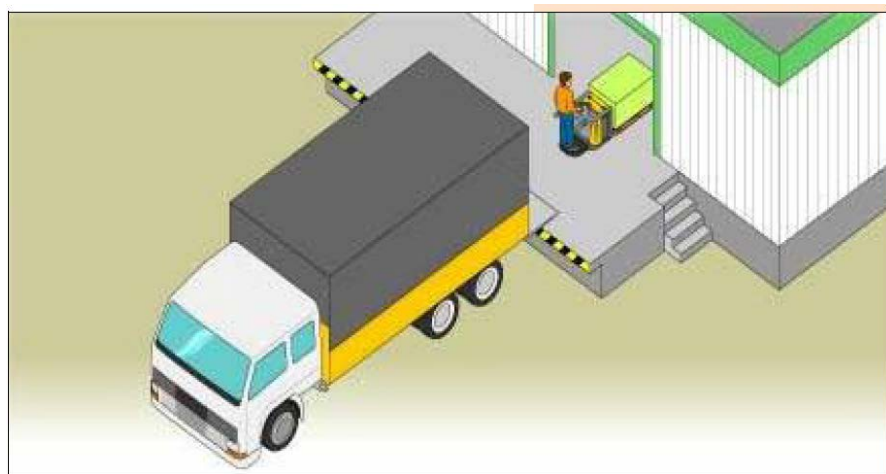


圖 3.11 高風險卸貨區與主要建築物分離

(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

3. 建築物外牆設計：

除考慮自然監控需求外，為減少爆炸攻擊時之損害，可以採取窄而高或凹下之窗戶，較大面積開窗安全。(圖 3.12)

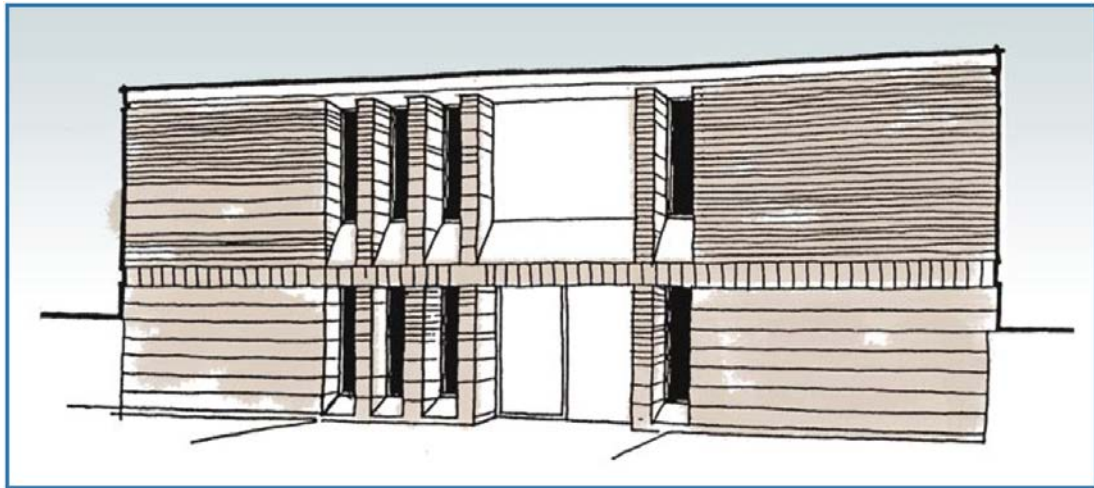


圖 3.12 採取窄而高或凹下之窗戶較不易碎裂

(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

三、 建築設備計畫與空間設計方面

1. 設備項目及空間需求調查：

一般建築物之安全設備可概分為：出入口控制、停車場管理設備、入侵報警、電子巡更、攝影監控、其他（生化、放射線、金屬、爆炸物探測設備 6 大類，可先就建築物人員安全及財產價值等因素，考綠採建築設計手法或機械手法後，再進行設備需求分析，決定採用設備項目、數量及並安排設備空間。(表 3.2)

表 3.2 智慧建築手法彙整

建築空間別		建築手法				機械手法							安防原理						
													安全事件發生						
		自然監控			防止入侵		防止入侵		報警	設備監控	特殊功能			前		中		後	
空間區位安排	動線設計	建築物開口部門窗設計	增加牆厚	設置圍籬、圍牆	設置門鎖、鐵窗	出入口控制	停車場管理設備	入侵報警	電子巡更	攝影監控	生化、放射線、金屬、爆炸物探測設備	防範為先阻礙侵入或危險物	察覺異常報警	發出警報促使放棄犯罪	拖延犯罪時間	阻斷犯罪通道	防止犯罪者脫逃	證據保全	
流通性空間	基地周界				●				●				●						
	進出口	●	●			●	●	●	●		●	●	●	●	●		●	●	●
	走廊、樓梯、電梯間		●				●				●					●	●		
停留性空間	安全監控室、警衛室或人員主要活動	●	●	●					●	●				●	●			●	●

智慧化建築安全防範設備空間設計準則之研究

建築空間別		建築手法					機械手法							安防原理						
														安全事件發生						
		自然監控			防止入侵		防止入侵		報警	設備監控	特殊功能			前		中			後	
		空間區位安排	動線設計	建築物開口部門窗設計	增加牆厚	設置圍籬、圍牆	設置門鎖、鐵窗	出入口控制	停車場管理設備	入侵報警	電子巡更	攝影監控	生化、放射線、金屬、爆炸物探測設備	防範為先阻礙侵入或危險物	察覺異常報警	發出警報促使放棄犯罪	拖延犯罪時間	阻斷犯罪通道	防止犯罪者脫逃	證據保全
	空間																			
	信件收發室												●	●						
	停車空間	●							●			●		●						
	資訊機房、金庫等重點區域	●			●		●	●		●		●		●	●	●	●		●	●
附屬空間	廁所等人員易落單處						●			●		●				●				●
	管道間												●	●	●					
	高	●	●	●				●					●	●						

第三章 智慧建築安全防範設備空間設計準則之研擬

建築空間別	建築手法					機械手法							安防原理					
													安全事件發生					
	自然監控			防止入侵		防止入侵		報警	設備監控	特殊功能			前		中		後	
空間區位安排	動線設計	建築物開口部門窗設計	增加牆厚	設置圍籬、圍牆	設置門鎖、鐵窗	出入口控制	停車場管理設備	入侵報警	電子巡更	攝影監控	生化、放射線、金屬、爆炸物探測設備	防範為先阻礙侵入或危險物	察覺異常報警	發出警報促使放棄犯罪	拖延犯罪時間	阻斷犯罪通道	防止犯罪者脫逃	證據保全
層建築設備層																		

(來源：本研究整理)

安全監控室之空間量與安全監控螢幕數量密切相關，螢幕數量取決於需納入中央攝影監控之地點數量及面積，其推估方式可以每一螢幕不小於 10 英吋，常用為 15 或 17 英吋，每一安全人員監控畫面不超過 8 個。

此外，提高安全監控攝影機設置位置，雖可使監控面積加大，達到減少設置數量、降低成本之效果，但安全監控畫面之品質亦將隨之降低，將影響安全人員評估異常事件及報警之正確性。(圖 3.13)

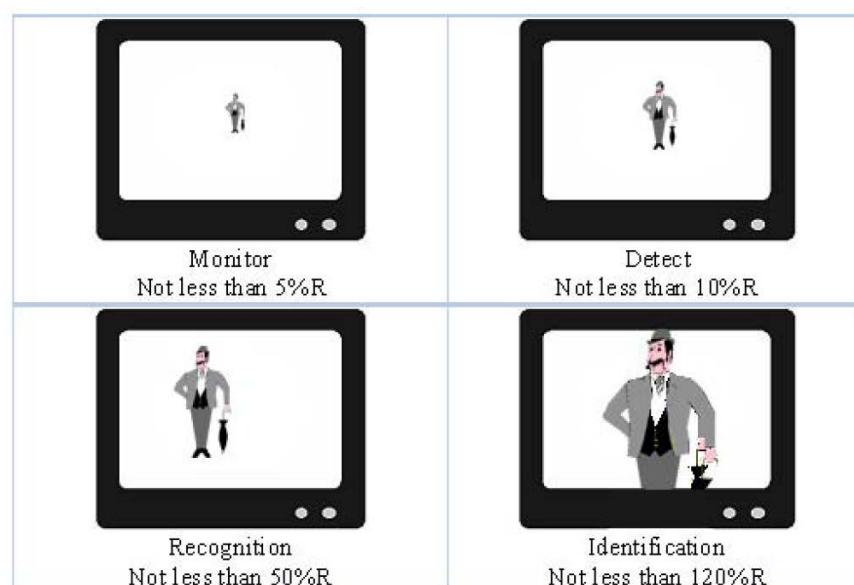


圖 3.13 安全監控畫面品質影響安全評估及報警之正確性
(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

2. 設備動線應考慮更新維護需求：

2. 由於安全設備技術進步快速，因此，除考慮設備安裝及維護管理動線外，由應考慮日後更新設備之搬運。

3. 設備空間細部設計：

除攝影監控可參考表 2.9 進行照明環境設計外、亦應考慮設配線隱蔽、設備保護，避免因設備遭入侵者破壞，而無法發揮功能。(參圖 3.14)

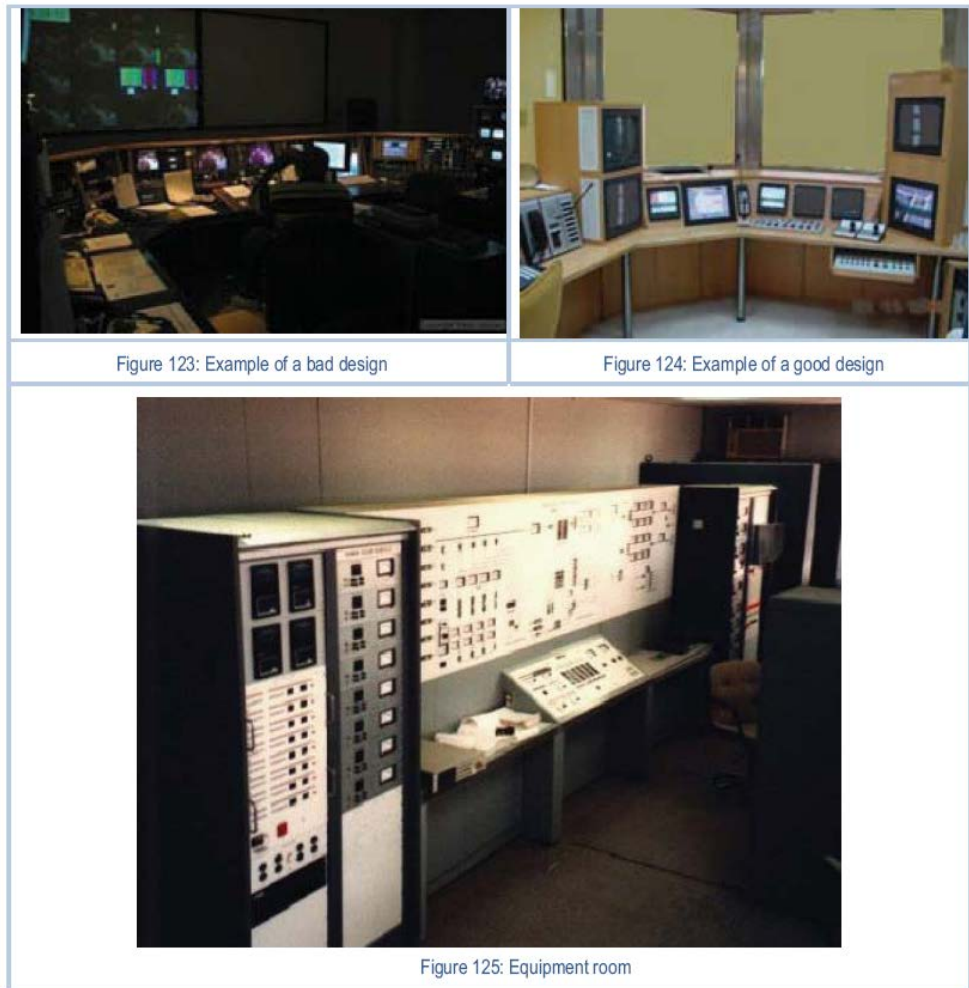


圖 3.14 照明環環境及視線良好之安全監控室工作效率
(圖片來源：Guidelines for Enhancing Building Security in Singapore.)

四、 安全議題敏感之建築物特殊考量：

鑒於 1990 年代後世界各地遭遇恐怖攻擊次數件漸增，因此，對於地標建築、政府機關、跨國企業營運總部等，除防止侵入竊盜外，亦應評估恐怖攻擊之可能性，考慮是否將爆炸載重納入結構設計考量採用防爆玻璃或防爆毯，避免結構挑空設計，增加靜不定次數，可延長建築物遭受炸彈攻擊時，發生倒塌之時間，爭取生救災時間，以及引入

相關安全顧問，於建築物導入監控生化、放射性物物質或毒氣之探測、排除裝置，並對於亦遭投擲該類有害物質之屋頂管道間開口、地下室通氣口等設置防護措施。

（參圖 3.15、圖 3.16）



圖 3.15 結構挑空設計易使建築物遭受炸彈攻擊時發生倒塌
（圖片來源：Guidelines for Enhancing Building Security in Singapore.）

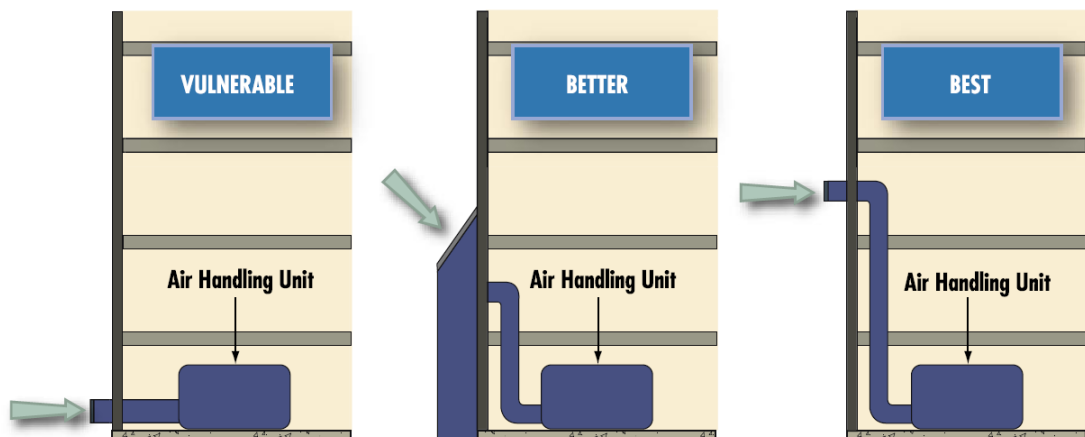


圖 3.16 空調外氣引入口應設置於不易遭投擲有害物質處
(圖片來源：Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings)

五、 公寓大廈管理方面

1. 協助起造人製作「共用部分」或「約定共用部分」之安全設備點交文件：

建築物出入口控制、停車場管理設備、攝影監控等安防設備通常設置於公寓大廈之「共用部分」或「約定共用部分」，該類設備應依公寓大廈管理條例第 57 條第 1 項規定，由起造人將設施設備使用維護手冊及廠商資料、併同使用執照謄本及管線圖說等，於管理委員會成立或管理負責人推選或指定後 7 日內會同政府主管機關、公寓大廈管理委員會或管理負責人現場針對水電、機械設施、消防設施及各類管線進行檢測，確認其功能正常無誤後，移交之。

2. 設備動線應考慮更新維護需求與產權問題：

由於公寓大廈管理條例第 6 條第 1 項第 4 款明定，

住戶於維護、修繕專有部分、約定專用部分或設置管線，必須使用共用部分時，應經管理負責人或管理委員會之同意後為之。為因應安全設備技術進步快速之特性，為使住戶日後更新專有部份之安防設備時，較容易新設、拆除或變更配線，建議可在各專有部分設置專用管道間或綜合佈線。

第四章 智慧建築安全設計案例介紹

本章彙整國內、外智慧建築安全防範設備空間設計案例，以便於建築師應用發展建築安全設計方案、智慧建築安全防範設備，使建築物具備主動感知之智慧，成為更為人性化之安全空間參考。

第一節 美國猶他州鹽城湖社會大會堂廣場安全設計

一、 建築設計條件與安全防範目標

美國國防部反恐機構，在 1999 年提出智慧建築可以減輕恐怖攻擊之損害，研擬在既有建築物內安裝一組可以抵禦生化武器威脅之智慧建築設備構想，以便展示說明生化保護系統之元素有哪些？這些元素如何構成抵禦生化武器威脅之系統？

美國國防部依據以上構想，進一步提出將 1996 年完工之美國猶他州鹽城湖「社會大會堂廣場」(Social Hall Plaza) 改造成為智慧建築之提案，該建築物地上 6 層主要作出租辦公室使用，地下 3 層為可停放約 470 輛車之停車場，並於改造完成後，作為 2002 年冬季奧運會期間之營運中心。



圖 4.1 美國猶他州鹽城湖「社會大會堂廣場」

(圖片來

源：http://www.energystar.gov/ia/business/labeled_buildings

[//images/1004948.gif](http://images/1004948.gif))

二、 建築生化保護安全設備計畫目標之研擬

該改造計畫為達成以上建築安全防範目標，訂定以下建築安全設備選用原則：

1. 模組化 (modularity) 及具有可搬運性
(transportability)，可在既有建築物內快速拆除或安裝。
2. 模組內只使用市售商業零件，這些零件未來還可以拆下利用。
3. 性能要求：
 - (1) 可在高壓狀態下快速過濾大量有害氣體。
 - (2) 檢測生物、化學、放射線物質之感知器。
 - (3) 能為進入避難處所的人員提供緊急淨化處理。
 - (4) 整合所有零件之進階控制系統。
 - (5) 建築物內部和周圍提供人員及車輛交通安全管理。

三、 建築安全設計方案之研擬

最後發展出之建築設計方案是在 5、6 層樓設置多種類型之探測器及空氣正壓保護設備，以便處理建築物內大量洩漏生物與化學製劑之污染空氣，並安裝一緊急發電以防突然斷電；建築物入口處並設置可充水之臨時防撞欄、電子進出控制裝置及安檢站。重要設備概要如下：

1. 集中式空氣過濾保護系統：由於 5、6 層為奧運營運中心，為使在當中之工作人員在生化攻擊事件中仍可繼續工作免穿戴防護面罩及衣物，故將空間進行安全區劃，使營運工作人員集中於此，並設置 HEPA 高效率空氣過濾器保護系統，過濾速度達 20,000 立方

呎/分(CFM)；其次，就室內氣密性進行補強，控制使 5、6 層樓間空氣滲漏量。完工時並進行滲漏試驗。

2. 生化探測系統：為探測化學武器、有毒工業化學品、生物武器及放射性氣溶膠，採用 2 種不同化學探測器（離子遷移光譜技術、表面聲波技術），以便減少錯誤警報。探測器布置於能盡早探測出有毒氣體之位置，並能夠依探測器反應順序確認滲漏地點。並設有伽瑪探測器則用於探測放射性物質，以及生物節點探測系統探測生物製劑。此外，並在空氣回風處設置取樣罐，以便定期或通報異常警報時取樣檢驗空氣品質。
3. 控制系統：系統控制室設於 6 層，監控安全系統中之重要參數，並將緊急應變程序設於互動式資料庫中，以便即時查詢。當探測警報發出室內空氣受汙染之警報時，系統便可自動將空氣排出，反之，若探測到戶外空氣受汙染時，便可將建築物設置為開口部緊閉模式，減少外部空氣進入。
4. 淨化系統：於 5、6 層梯廳設置空氣閘門、受汙染人員淨化室，並於奧運會期間以人員手持探測器檢查進出人員。
5. 系統性能：相關探測器在設置後須經過不斷之測試、重新調整，本案發現在未發出警報之情況下，仍可測得有毒化學氣體，因此必須經由實測，才能將探測器之靈敏度調整至適當水準，避免誤報。此外，監控建築物營運之重要電腦設有不斷電電源，以及 24 小時連續工作所需之柴油發電機緊急供電燃料。

第二節 i236—新竹 U-Bobi 智慧安全社區規劃

2008 年行政院以六大核心概念，規劃「愛台灣十二大建設藍圖」暨藍圖 12 項優先公共建設，揭露「智慧台灣」、「智慧生活」產業與環境的營造；同年「行政院第 28 次科技顧問會議」之議題—智慧生活科技運用推動策略—中，建議政府「發展智慧生活科技運用，希望藉由科技與人性的結合，發展出各種智慧應用，以提高人民的生活品質，讓台灣有機會在 2020 年成為生活型態的先驅者，並推動生活應用服務產業發展」。經濟部提出配合智慧生活科技運用計畫（i236），於 2009-2010 年起實施。（圖 4.2）

i236 智慧生活科技運用計畫目標希望定義出智慧城鎮(Smart Town)與智慧經貿園區(i-Park)之系統架構、規格、介面，透過規模實證展現出其可能性及專業能力，向世人證明台灣可以整合出一套非常具有競爭力之解決方案，分階段以推動由工研院與資策會合組國際推廣團隊，結合國際大廠力量、籌組國際級大公司，或以國際科技合作模式，向中國大陸、義大利、紐西蘭、印尼等預期目標市場推廣，這些地區之 ICT 市場規模總和約為 9,575 億美元(約相當於新台幣 30.6 兆)，若預估 2020 年台灣在目標市場的可攻下 5%市佔率，則智慧城鎮與智慧經貿園區整案輸出海外將有新台幣 1.5 兆元的潛在市場。

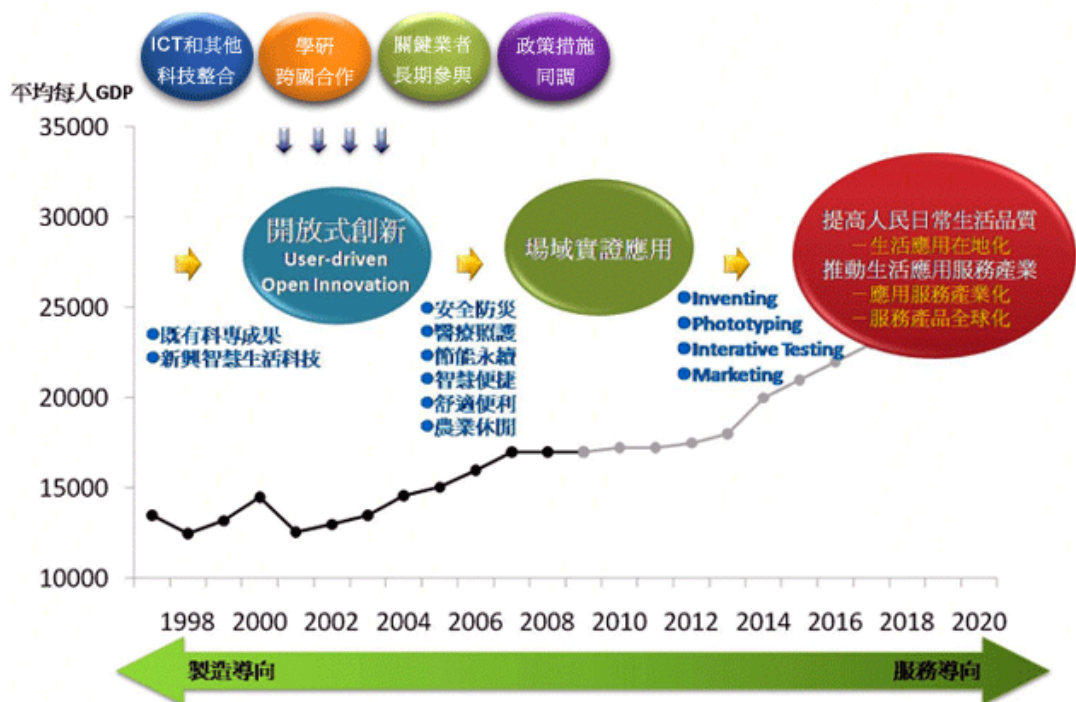


圖 4.2 i236 智慧生活科技運用計畫目標

（圖片來源：i236 智慧生活科技運用計畫網站）

「新竹 U-Bobi 智慧安全城市規劃」為 i236 智慧生活科技運用計畫中之一項計畫，由經濟部技術處補助 400 萬元，於 2011 年 10 月建置完成。計畫名稱為「安全城市規劃」，但實際計畫範圍是以新竹市湳雅七聯里作為實驗場域，重點是提升「社區安全監控力」，透過社區監視系統與警察局路口監視器為基礎，導入智慧型影像分析監控技術（IVS），藉由即時影像資訊之傳遞，達到即時報警及事前預警之目的，未來並將逐步推動到全新竹縣市及全國其他地區，成為智慧安全城市。

一、智慧安全社區課題

基於過去社區安全資訊未能共享，造成警察、保全業者、社區守望相助隊、居民無法共同協力進行「自然監控」，共享「設備監控」

資料。保全業也有以人力監控影像監視畫面，因視覺疲勞遺漏監看畫面，其實用價值偏向嚇阻作用等可改進之處。因此，發展出結合「智慧型影像分析系統（Intelligent Video System, IVS）技術」及「光纖寬頻網路架構」之解決方案，使警察機關、保全業者中控中心、公寓大廈駐衛保全人員得以共享監控影像，發揮「整合」功效。（圖 4.3）

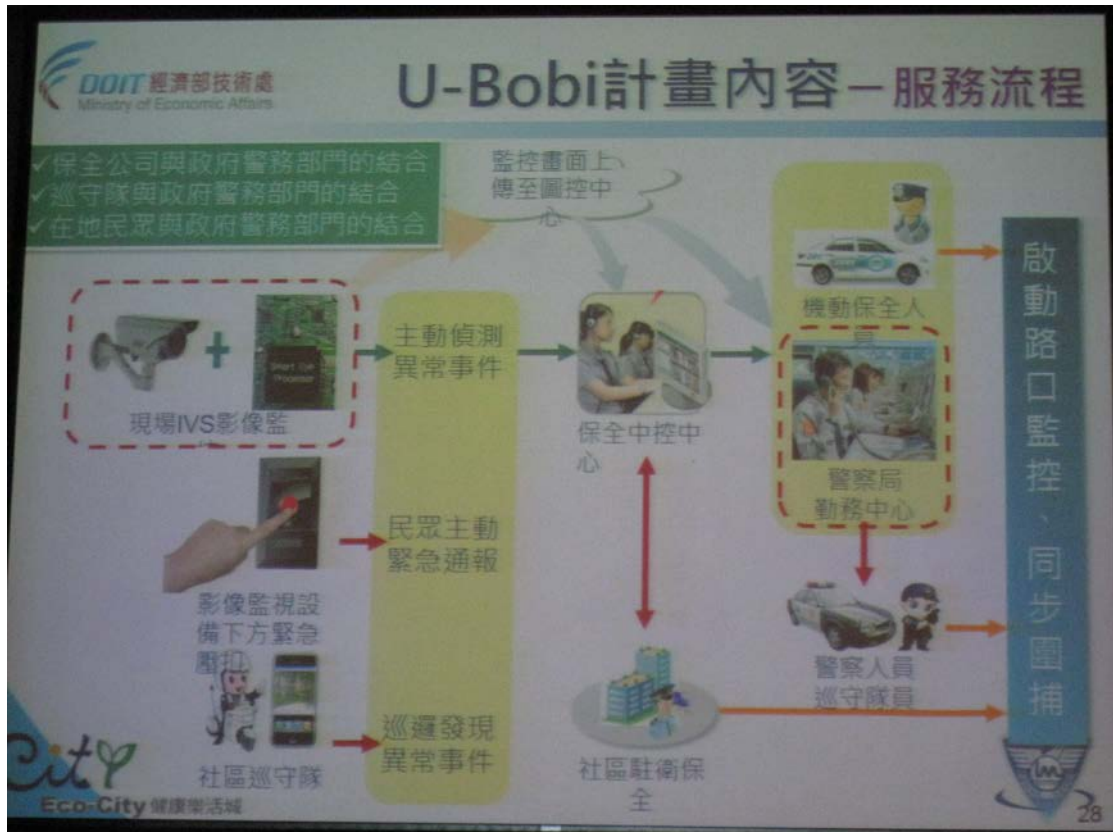


圖 4.3 警察機關、保全業者共享監控影像

（圖片來源：2011 全球智慧城市高峰論壇，智慧科技服務模組於未來城市之應用-以 i236 計畫與遠雄智慧社區為例簡報資料）

二、安全智慧社區聯防服務架構

在新竹市政府及警察局協助下，選定新竹市「荷蘭村」、「新竹第一或第三信用合作社」、「Hi-Life 便利超商」、「舊社國小」及滿雅街底等 5 處地點，設置網路保全設備，包括：服務據點影像分析、處理

與網路設備架設、滿雅派出所警報事件管理平台安裝、巡守隊與保全員手持設備支配置、24 小時影像監控中心備變提供服務，以提供各不同產業消費者、住民及一般民眾之保全、安全之實際體驗。

由於過去之影像監控系統實際應用上，會有檔案越積越多、難以管理檢索等問題。「智慧型影像分析系統技術」，可在儲存畫面的同時，系統主動同步分析畫面內容，發現畫面出現異常時，例如：畫面出現留置不明物體、超越虛擬警戒線、人物動態，系統隨即透過預設條件、管道發出警示訊息，使安全人員在問題發生的第一時間，即掌握現場狀況，並快速排除問題事件。

「智慧型影像分析系統技術」除了有監控影像區分錄製位置、日期、時間進行檔案管理分類，或藉由改變攝影畫面的角度與所監看範圍，避免出現監看死角等基本功能外，尚能針對影片資料庫進行智慧搜尋，包括以時間、場所、甚至下達更多其他檢索限制條件，加速檢索所需監控片段的操作效能。甚至在監控進行過程中，利用 ICT 技術，主動即時針對畫面內容，與警察局之犯罪資料庫資料進行比對分析，將片段資訊進行整合。

第五章 結論與建議

本研究回顧並分析國內外有關智慧建築安全防範相關文獻與案例，本章作為研究之總結，首先就本研究提出結論，其次，提出可執行之建議。

第一節 結論

- 一、九一一事件後促使部分國家對於建築安全科技之應用轉趨積極，對於台灣推動智慧化居住空間產業出口海外市場應有正面助益：

九一一事件後美國國土安全部除了賡續辦理自然災害預防業務外，並開始積極關注建築物人身安全議題，彙整分析國內外發生之重大恐怖攻擊事件，出版「減少建築物受恐怖攻擊可能性」等一系列書籍，指導建築師、建築工程師從事安全之建築設計，核心概念是保護建築物使用者及建築物關鍵基礎設施，除彙整相關「建築設計手法」外，並介紹可因應生化、放射線、毒氣攻擊之相關安全電子科技產品，針對易受攻擊之政府機關、跨國企業總部、大眾運輸車站等地標建築，可考慮以「機械手法」減少災害，而新加坡等國家也跟進出版「加強建築安全準則」等建築安全設計刊物，供建築師、建築工程師參考，對於台灣推動智慧化居住空間產業出口海外市場應有正面助益。

- 二、智慧建築安全防範空間設計準則是提供建築師進行「以性別觀點建構安全無慮環境」之設計思考架構而非僵化之設計解答：

統合建築是建築師之職責，建築安全防範設計解答是建築師依個案建築基地條件、使用者需求、預算、技術、建築美學等面向所提出之平衡解答，可能採用「建築設計手法」、「機械

手法」或混合二者手法。因此，訂定智慧建築安全防範空間設計準則應著重協助建築師建立正確之思考模式，有系統地從安全觀點評估基地潛力與限制條件、解釋設計方案優劣、反省錯誤、累積專業經驗，將建築物個案之安全防範元素，作具有創造力之組合，妥適應用智慧建築安全防範設備。

三、進階功能之智慧建築安全防範設備具有自動報警、電腦輔助犯罪偵查等特性，其嚇阻犯罪功能不僅只於提升「社區監控力」：

1960 年代開啟之一系列環境設計預防犯罪（CPTED）研究，經過 30 年之發展，主要偏重在以建築設計手法提高自然監控所需之可視性，強調藉由社區道路形式、建築物與鄰房間開窗位、社區領域範圍之明確界定等建築設計可控制之因子，提高犯罪行為「被社區居民看見之機會」，進而發揮守望相助嚇阻犯罪之功效。

近年發展之智慧型影像分析監控技術（IVS），可在儲存畫面的同時，系統主動同步分析畫面內容，發出警示訊息。甚至在監控進行過程中，利用 ICT 技術，主動即時針對畫面內容，與警察局之犯罪資料庫資料進行比對分析，將片段資訊進行整合，其功能已由以監視攝影畫面作為犯罪證據，擴大至主動報警、輔助犯罪偵查等功能。

第二節 建議

建議一

推動智慧建築安全防範設計政策之性別分析：立即可行之建議

主辦機關：內政部建築研究所

協辦機關：內政部警政署、內政部家庭暴力及性侵害防治委員會

說明：本案依據「性別平等政策綱領」及「智慧化居住空間產業發展推廣計畫」，蒐集分析國內外相關規範、案例等資料，先就綱領中有關「以性別觀點建構安全無慮環境」之抽象上位概念，研擬可具體落實於建築設計實務中之安全建築設計準則。後續可就推動智慧建築安全防範設計政策進行性別分析，將內政部警政署犯罪地點統計資料，及內政部家庭暴力及性侵害防治委員會性侵害事件通報案發地點等統計資料與發生地點之建築形式進行分析，除驗證本研究所研提之智慧建築安全設計準則之效度與信度外，並評估推動智慧建築安全防範設計政策對女性與男性所產生之受益程度是否產生差異，就建築設計之性別議題進行較為細緻之探討。

建議二

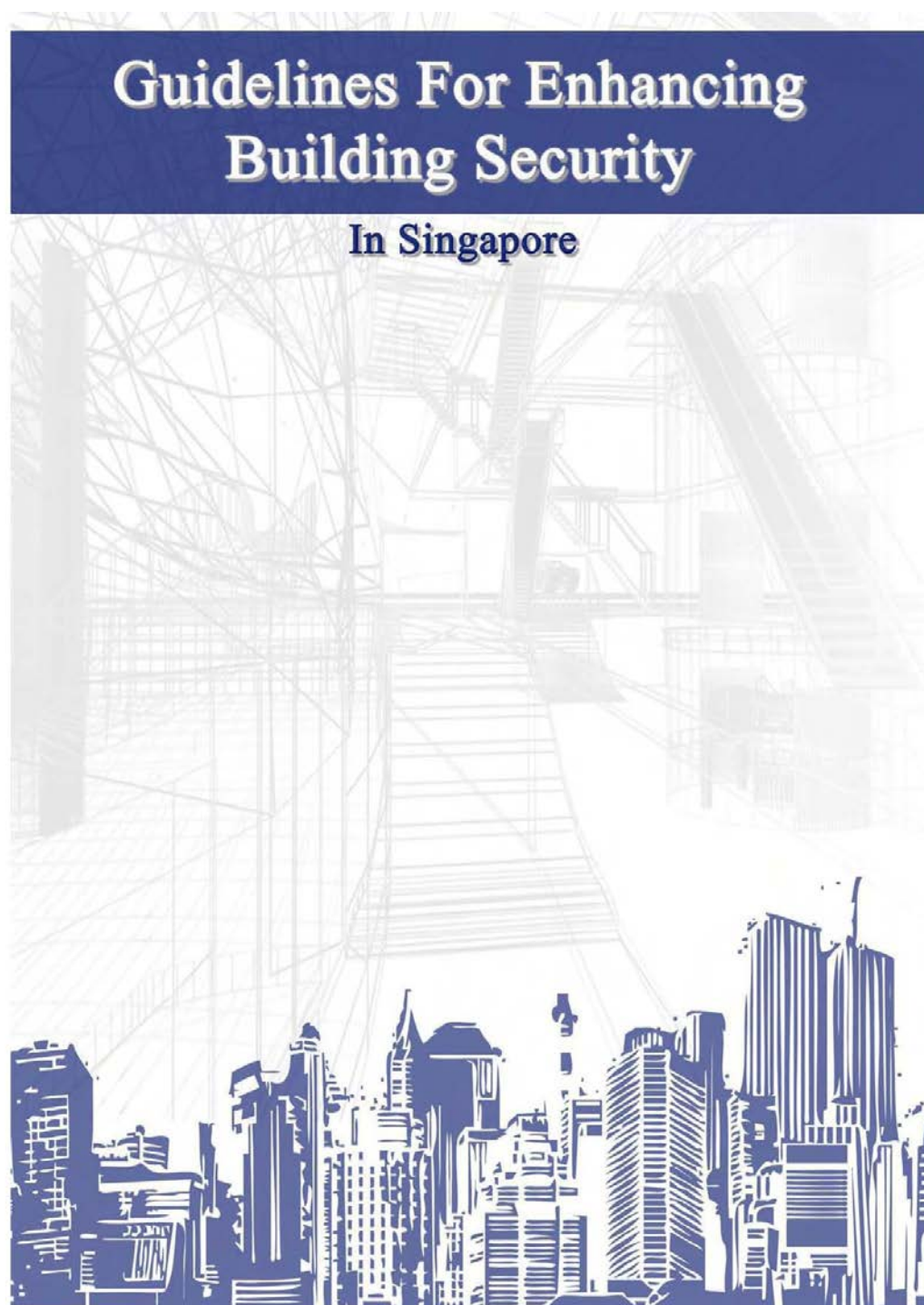
依智慧建築安全防範設計準則辦理地方示範計畫：中長期建議

主辦機關：內政部建築研究所

協辦機關：各地方機關團體及產業

說明：透過與地方有關機關團體及產業合作發展，藉由警察、社區居民、公寓大廈管理組織及產業參予，使智慧建築安全科技能與庶民生活結合，並引導產業開發符合民眾真實需要之產品，才能使智慧科技產生價值。

附錄一 新加坡內政部「加強建築安全準則手冊-建築物安全防範設備」



(Updated as at July 2010)

The **Guidelines for Enhancing Building Security in Singapore (GEBSS)** is a follow-up from the earlier 'Enhancing Building Security' booklet and has been prepared by **Homefront Security Division - Ministry of Home Affairs** in consultation with:
Singapore Police Force;
Internal Security Department;
Singapore Civil Defence Force;
Building and Construction Authority;
Urban Redevelopment Authority;
as well as with inputs from external consultants.

The GEBSS is a 'live' document which will be updated when necessary. For feedback or queries, please write to MHA_Guidelines_BuildingSecurity@mha.gov.sg.

No part of the GEBSS shall be reproduced in whole or part without prior written consent of the Ministry of Home Affairs.





SECURITY SYSTEMS

The objective of this chapter is to provide basic security design guidelines that will enable architects and electric system engineers to make the right decisions when choosing the specifications of the security equipment that is to be used and when deciding on its positioning throughout the building.

Technical and electronic systems such as CCTV and alarm systems are part of every modern building plan and are considered basic. These security systems which are installed throughout the building usually consist of:

- End points, which are the systems' data gathering sensors (e.g. detectors, cameras, etc.).
- Base points, which receive and process all the input gathered by their system's end point (e.g. CCTV matrix, alarm system).
- Cabling, infrastructure and wireless channels.

The systems are usually meant to assist in the implementation of the building maintenance plan, the administration plan or the security plan. Some systems are dedicated to serve one of these plans while others play two or even three roles assisting in more than one field. Integrating the electronic security systems into the overall electrical design of the building has many advantages. It will help to assure that the end points are positioned in a manner that enables them to perform in the best way. It will also help to assure that the systems' cabling will be installed in such a way that will make it as unnoticeable as possible and that the spaces and features in which the systems are meant to be located are adequate, and will not hamper their performance.

Early planning of the systems will also allow important coordination between the building domain, the human domain and the technology domain. This will assure minimal changes and additions once the building is occupied and hence avoid additional and unnecessary security costs.

Today's market is filled with a large number of technical security products made by different manufacturers. Only a relatively small number of these systems are tested and approved by national laboratories or military institutions around the world. These technical systems are usually not considered to be "life saving" systems but are operated as "support" systems that give an extra value to the security deployment of a building. It is therefore advised that the project team consider whether their specified need warrants the use of an approved system (which is usually more expensive). In some cases non-approved systems might be adequate for performing a minor supportive role.

Security systems, unlike physical protection elements, have a relatively moderate life span (usually not more the 10 years). It is therefore advisable to design the relevant parts in the building's infrastructure to enable changing and updating of these systems at minimal extra expenses and / or damage to the buildings.

Security systems are usually used for the following purposes:

- Detect illicit activities or intrusions.
- Warn designated security personnel of hostile activity and/or breaches of security to the building.
- Monitoring of activity in sensitive or vulnerable locations.
- Recording activities for future investigations.
- Deterrence.
- Replacing or supporting human security resources for cost effectiveness.
- Assuring the proper function of physical security elements.

When planning the security systems layout for a building, it is recommended to take into account possible future upgrades and enhancements of the systems' capabilities. Such planning should enable the system at least 50% growth and should include extra deployment and installation of alternatives for the system and added infrastructure that will enable the installation of more end points. This pre-planning will allow the building's security to conduct low-cost future upgrades when necessary.

8.1 HOW TO USE THIS CHAPTER

This chapter contains information on security systems and security related systems, located in the various parts of a building development. The Protection Recommendation Tables (PRT) in Chapter 4, mention a list of protection elements that can be found in this chapter. Each protection element is described in its own section together with its specification and protection role. If desired, protection elements in this chapter can be implemented even if they are not recommended for implementation in the PRT. For each element, the levels of protection are mentioned and standards are described. The level of detail provided is not intended to provide a full technical specification but rather to provide basic knowledge and to assist in the procurement procedure to ensure that the right demands are made of suppliers and/or protection engineers.

The following protection elements appear in this chapter:

Subject	Description	Section
Control room	Central security control room where all relevant security systems are located.	8.2
Intercom System (combined security and admin system)	Wall units, desk units, switchboard	8.3
Public Address system (combined security and admin system)	Speakers, amplifiers, microphones	8.4
Alarm System (security system)	Detectors, sensors, main units	8.5
Access control systems (combined security and admin system)	For pedestrians and vehicles	8.6
CCTV System	Cameras, recorders, monitors	8.7
Security Lighting	Lighting for security systems	8.8

8.2 SECURITY CONTROL ROOM

8.2.1 INTRODUCTION

The security command control room is the nerve centre of security operations for a building and should receive and provide vital information to and from the security personnel on shift, commanders, executives and first responders both in routine and emergency situations.

An effective control room that focuses on relevant threats can make the difference between a proper response and chaos, once an incident has been initiated.

A building's security operation should be aimed at both crime and terror prevention. The level of effectiveness in which crime and terror prevention operations are carried out is greatly dependant on the capabilities of the control room and its operating staff.

A typical control room should contain all of the main operating stations of the security systems installed throughout the building. The control room should also contain sub-stations of several of the building's management systems such as the air-conditioning and lift control systems. Some of these substations should have overriding authority over the main station, whereas others can have regular operating capabilities or should be limited to view only.

The following systems should be included in a security control room:

Security System	Type of Operating Station
CCTV Monitors	Main
CCTV Recording	Main
External phone line (a direct line)	Main
Alarm System	Main
Access Control, pedestrian and vehicles	Main
Public Address	Sub-station (overwriting ability)
Intercom	Sub-station
Fire Detection	Sub-station
Air-conditioning	Sub-station (overwriting ability)
Security Lighting	Sub-station (overwriting ability)
Lift System	Sub-station

The security control room design must allow it to function as an effective tool for managing the security operations of the building in both routine and emergency situations. In order to perform its tasks, the security control room must have the following capabilities:

- Collecting all the data required in order to formalise a clear and complete picture of the current situation throughout the building. The data received and presented should relate to, among other things, any regular and irregular activities, crowd concentrations and security related incidents. The data should be collected during both routine and emergency situations.
- Prioritising and filtering out relevant information is done by cutting down the number of monitors that need to be watched and prioritising inputs received from the security cameras and the alarm system in a way that will make sure that only real incidents are picked up by the control room systems. Other benefits include:
 - Communicating information to both staff and visitors in emergency situations.
 - Assisting in and monitoring the evacuation of the building's occupants when necessary.
 - Supporting commanders and decision makers and first responders while they are performing their respective responsibilities.
 - Operate in full function during post attack periods.

8.2.2 TERMS AND DEFINITIONS

System Administrator	A system that is completely under the control and responsibility of the control room.
System Sub-station	A system that is usually located in the building management system room and is connected to the security control enabling it to receive inputs and take limited action.
Access control system	The layout of access control devices connected to electric locks enabling control of doors/entrances either by the person entering (proximity card, etc.), or by the control room granting access.
Equipment	Examples of equipment are: computers, switchboards, cable relays, multiplexers, UPS.
Equipment Room	A room housing the equipment used for the security systems.

8.2.3 DESIGN OF A SECURITY CONTROL ROOM

GENERAL

I. It is recommended to design the control room as a dedicated unit (i.e. that it will not serve a dual purpose as both a security control room and an access control guard post).

II. The security control room should have a direct connection to or integrated with the building's management systems that are considered to be critical or security related (e.g. air conditioning systems). This is meant to enable the security control room staff to override or control these systems when the situation requires it¹⁰.

III. Protection and backup of all critical systems is required in order to allow the security systems to continue operating during emergency situations in which the security control room is damaged and during events of power failure.

IV. The security control room plays a critical role in a building's security deployment. It is therefore recommended to design its protection in a robust manner. The purpose of these measures is to make the security control room able to withstand an attack either against the building it occupies or a direct attack against the security control room and continue to function both during and after the emergency. The entrance to the security control room should be equipped with an access control system and forced entry. These measures are meant to ensure that no un-authorised persons will gain access to the security control room.

V. The lighting in the control room should be designed in a way that will ensure that it does not cause glare on the various monitors. For this purpose, it is recommended that the control room uses fluorescent lights.

VI. The security control room should be equipped with a working surface that is positioned in way that will allow the security control room operator to have a good view of the monitors.

VII. The security control room should be equipped with emergency power and lighting to enable it to continue to function during power failures.

VIII. The security control room should be equipped with a climate control system. This is meant to help create a more comfortable working environment that will assist the security control room operators to stay alert, especially during night-time and long shifts.

IX. The security control room should be supplied by at least two separate power lines. One dedicated to security systems while the other for administrative purposes.

X. When planning the security control room, there is a need to designate an area for administrative proposes. This area should be planned and positioned in a way that will ensure that any activities conducted within do not interfere with the security control room's regular operation and in emergencies.

XI. The control room should be equipped with a dedicated phone line that has a direct external line.

¹⁰It is not recommended to have both the security systems and the building's management systems installed in the same room.

EQUIPMENT ROOM

I. It is recommended to place other electrical equipment used by the security control systems that are located in the security control room, in an adjoining but separate room.

II. A false floor is recommended for both rooms in order to allow cabling to be installed.

III. A concentration of electrical equipment in a closed room can cause the temperature in the room to rise considerably. The rise in temperature may even damage the electrical systems causing them to fail. It is therefore recommended to install climate control systems in the equipment room.

IV. The fire extinguishing measures installed in the security control room and its adjoining equipment room (where applicable) must be of a kind that, if operated, will not cause damage to the electrical equipment.

V. It is recommended that both the security control room and (where applicable) the adjoining equipment room, should not have water pipes running through them.

CCTV MONITORS & RECORDERS

I. The number of constantly viewed monitors should be limited to a minimum and should not exceed 8 images per person. The images for each person could either be presented on a single large monitor or on several smaller ones.

II. The minimal image size is 10".

III. The monitors should be located in a way that allows the person in the control room to perform his regular duties (phone, log book, access control) and monitor the cameras without interference.

IV. All data received by the systems (CCTV, alarm, access control) should be recorded for post incident investigation. The required recording rate (FPS), the recording's resolution, and the period that the recordings are stored for, should follow the guidelines in Section 8.7. It is important to note that issues pertaining to data storage have implications both on operational matters (e.g. face recognition) and on administrative matters (e.g. amount of space required for holding the equipment).

ALARM

I. Indication of alarms, transferred to the security control room, should appear in the most accurate way possible. Alarm indications are required to relay the exact location of the breach or event to the security control room operator. Each indication should also be accompanied by a visual picture of the location where the breach or event is taking place.

EXAMPLES OF DESIGNS



Figure 123: Example of a bad design

Figure 124: Example of a good design



Figure 125: Equipment room

8.3 INTERCOM AND COMMUNICATION SYSTEM

8.3.1 INTRODUCTION

An intercom is a private telecommunication system that allows people from two or more locations to communicate with each other. Although usually considered administrative systems, intercom systems and other similar communication systems play an important role in a building's security deployment. This is especially true with regards to access control. The intercom system enables the personnel operating the access controlled doors or gates to communicate with the people wishing to enter the building, without exiting the relatively secure inner area in which they are positioned (whether it is located inside the building or in an external security post).

There are many types of systems that can be used as an intercom system, these include:

- Standard point to point intercom system (party line systems).
- Matrix systems.
- Videophone systems.
- Wireless systems.
- Telephone based systems and others.

8.3.2 TERMS AND DEFINITIONS

Intercom System	An electronic system that allows simplex, half-duplex, or full-duplex audio communications.
Intercom master station	Part of an intercom system that monitors one or more intercom door/gate stations; this station will typically receive the initial communication.
Intercom switcher	Part of an intercom system that controls the flow of communications between various stations.
Video intercom system	An intercom system that also incorporates a small CCTV system for verification.
Full Duplex	A type of system that enables two end units operating on the same line to simultaneously broadcast and receives data.
Anti vandal	Built in a way that does not allow sabotage.

8.3.3 DESIGN OF AN INTERCOM AND COMMUNICATION SYSTEM

I. The system's volume and background noise filtering levels should be set after taking into consideration the noise levels of the operating environment (e.g. an intercom located on the street requires different volume and noise filtering than one installed in a room).

II. The applied levels of both volume and background noise filtering should be set after taking into account the average distance that the users will be from the unit while operating it (e.g. an intercom used by drivers in their cars requires a different volume and noise filtering level than one installed at a pedestrian entrance).

III. It is recommended to combine intercom units employed for use in access control, with CCTV coverage, and proper lighting. This will enable the security personnel to screen incoming persons in a more effective manner.

IV. Prior to deciding whether to use a specific intercom system for security purposes, it is important to check whether the levels of amplification and noise filtering it is capable of, are adequate for use in the building's environment.

V. Electric infrastructure might create interference with the intercom system's audio signals. This occurs if the two systems are positioned too close to each other. It is therefore recommended to maintain proper separation between intercom

VI. When designing a non-matrix intercom system for access control, it is important to make sure that the system's cabling enables communications between the unit installed at the access point and the units installed both at the access control point and the security control room.

VII. Most intercom systems need to undergo maintenance on a regular basis. It is therefore recommended to install them at a location that will allow for the maintenance work to be conducted in a convenient manner.

VIII. Exterior intercom units should be protected against environmental conditions such as temperature, humidity and rain.

IX. Exterior intercom units should be designed with anti-vandalism measures.

X. Intercom units that are installed at vehicle entrances should be designed in a way that will not require drivers to exit their car in order to operate them. For example a call initiator can be connected to a detector that operates it as soon as a car approaches the designated area.

XI. Deep basement floors and buildings with relatively small window openings could potentially stop radio communication with emergency responders who are inside the building. With the installation of cell enhancers, communication by radio among emergency responders becomes possible between the interior and exterior of the building and within the building between the different storeys including basement levels.

Standards

The system should comply with the relevant construction and electricity related standards.

8.3.4 EXAMPLES OF DESIGNS



Figure 126: Master station (matrix system)



Figure 127: Basic wall unit



8.4 PUBLIC ADDRESS SYSTEM

8.4.1 INTRODUCTION

The public address (PA) system plays an essential role when it comes to emergency procedures. During emergency situations the system can be used to convey life-saving instructions to the general public. The PA system must be designed as an integrated part of the building's intercom system and other security systems. A typical PA system will include the following:

- Indoor / outdoor speakers
- Amplifier
- Microphone
- Area division panel (to be able to address parts of the building individually)

8.4.2 TERMS AND DEFINITIONS

Pre recorded messages	Messages providing emergency instructions recorded on CD or in the system making it not necessary for the operator to speak clearly or remember the messages.
Coverage	The ability to hear and understand the messages being given.

8.4.3 DESIGN OF A PUBLIC ADDRESS SYSTEM

- A building should always have one PA system that can be controlled from the security control room.
- Access to the PA system should be provided to the security manager's office as he usually has the authority to call for evacuation.
- The system should include pre-recorded messages in all relevant languages covering the required response to the various attack scenarios.
- The speaker coverage should be complete and cover each and every room.
- The system should be easy to operate under emergency situations.

Standards

The system should comply with the construction and electricity related standards.

8.5 ALARM SYSTEM

8.5.1 INTRODUCTION

Alarm systems installed in buildings and/or complexes are aimed at detecting both unlawful intrusion and lawful entry into a defined space. Alarm systems are usually made out of a combination of elements (sensors, keyboards, control units and others) that create a "smart" system. This "smart" system is programmed to be able to monitor various parameters, which may include, but are not limited to, the following: opening of doors and/or windows; crossing of lines; movement in defined areas; shifts in temperature; change in lighting etc. The type and number of parameters monitored by the system can vary and should be designed according to the requirements of the building's security plan.


An alarm system will usually consist of:

- Detectors of various types
- Keyboards
- Control Units
- Display units
- Diallers
- Cabling
- Sirens
- Backup batteries
- Optional – remote controls/ wireless items / signal lights


There are many types of anti-intrusion detectors that are used to protect different types of areas throughout different types of complexes and buildings. The following are some examples of the various detector types:



PERIMETER LINE DETECTORS

Protecting a perimeter line and fencing is usually done using "smart" fences which are fences with detection systems installed on them. These systems are configured to provide an alert when someone or something attempts to cross the fence line.

Taut wires	These are wires that are stretched along a fence and have an electric current running through them. The alarm system connected to these wires is usually configured to give an indication if the wires are cut, pulled or bridged (electrically). In some cases taut wires can also be configured to convey a non lethal electric shock if touched. Taut wires may be installed in a variety of configurations such as on top of a fence or outside it.	
Infrared active motion detectors	Infrared active motion detectors project infrared light towards a designated area. When an object passes through the lighted area, the sensors send a signal to the relevant command centre. These detectors can be installed in such a way as to be almost completely unobtrusive.	
Video Motion Detectors (VMD)	VMD is a video imaging based surveillance system. The VMD system monitors a specified area; any change in the picture of the monitored area will trigger an alarm. An intruder might see the VMD cameras but has no way of knowing if they have motion detecting capabilities.	
Vibration detectors	Vibration detection systems are usually based on vibration sensors that are installed on wires which run through the length of a fence. An intruder trying to climb the fence will cause an alarm to be triggered in the command centre.	
Microwave motion detectors	Microwave motion detectors project microwave beams in order to create an invisible line. Crossing this line will send a signal to the command centre. Microwave detectors are usually noticeable and hard to conceal.	
Weight detectors	Weight detectors are used to detect someone applying pressure against the top of a barrier wall or laying a ladder against it. These detectors are made out of coils that are covered by light material. When the material covering the coils is bent, as a result of the weight of someone climbing onto the wall or for some other reason, the detectors will send a signal to the relevant command centre.	
Infrared beam detectors	Infrared beams are usually used to create an invisible line or web. When the line/web is crossed the system sends a signal to the relevant command centre. These detectors are usually relatively noticeable.	

INTERNAL AND EXTERNAL DETECTORS

Magnetic Switches	Magnetic switches are the most common detector used in alarm systems. They are usually required to perform a dual task, indicating to both the alarm system and the access control system if a door/window/hatch is opened or closed. These sensors are generally made out of 2 magnets. One magnet is connected by cable to a control unit that is installed in the door/window/hatch frame. A second magnet is installed in the door/window/hatches itself.	
Motion detectors	Infrared active motion detectors project infrared light to a designated area. When an object passes through that area, a signal is conveyed to the alarm system's control unit. There are different types of infrared motion detectors: Vial detectors usually cover an area of up to 150 degrees over a distance of up to 15 meters; Ceiling detectors usually provide 360 degrees of coverage; Outdoor sensors are usually used as virtual screens placed in front of windows and balconies. Motion detectors are usually used to cover rooms and corridors considered secured or paths that are considered most likely to be used by an intruder.	

Video Motion Detectors (VMD)	VMD is a video imaging based surveillance system. The VMD system monitors a specified area; any change in the picture of the monitored area will trigger an alarm. An intruder might see the VMD cameras but has no way of knowing if they have motion detecting capabilities. This detection method is much more effective indoors than outdoors.	
Vibration detectors	Vibration detection systems are made out of a sensor that is installed on a window or partition (safe wall). The sensor is configured to detect relatively slight movement. An intruder trying to break in will cause an alarm to be triggered at the control unit.	
Glass break detectors	These detectors are based on audio detection. The sound of breaking glass will make the sensors send a signal to the systems control unit.	
Panic buttons	A panic button is a push button, either mobile or fixed (e.g. installed on a wall or desk), that when pushed activates sends a signal to the relevant control room.	
Heavy Duty detectors	Heavy duty detectors are used for outdoor purposes. These detectors are mainly installed on large gates. They are basically magnetic detectors that are specially designed to be able to withstand outdoor conditions and vandalism.	

8.5.2 TERMS AND DEFINITIONS

Alarm control unit	An electronic system that receives inputs from various types of detectors analyzes these inputs and provides indicative outputs
Standard system	A system operated and configured by using a keypad
Zone	A single or group of detectors representing an area in the alarm system. Zones are meant to enable the system to define the area that has been breached
Smart system	A system operated and configured using a computer and dedicated software
Detector / Sensor	An electronic device able to detect a change in a situation and provide an electronic output as a result

8.5.3 DESIGN OF AN ALARM SYSTEM

- I. The type of detector that is to be used should only be determined after all location (e.g. indoors, outdoors etc.) and environmental (e.g. humidity, temperature etc.) issues have been taken into consideration.
- II. An alarm system should include several types of detectors.
- III. Cabling for alarm detectors should always be installed in a protected manner.
- IV. It is recommended to avoid installing detectors with a relatively high false alarm rate. A high false alarm rate (more than one false alarm per week for the whole system) will reduce the effectiveness of the system and add to the probability that a true alarm will be ignored.
- V. The display unit should provide clear information as to which zone and detector were set off. A smart system should clearly display the zone and detector on a computerised map of the protected site. A standard system may display the information on the keypad unit.

VI. Alarm systems should have two sets of detectors defined: (a) 24 hour detectors that are installed on openings that are supposed to be permanently closed (e.g. emergency exits), and (b) day/ night detectors, that are installed on doors that are regularly opened during day/ activity hours but closed during after office hours /night time. Defining these two types of detectors will enable the system to prioritise its outputs in a more efficient manner. The two sets of detectors should be designed to sound/ give out different types of alarms at different situations (e.g. a buzzer during the day and siren at night).

VII. An alarm system should be configured to prioritise the inputs received from the detectors (e.g. sounding different alarms for different amount of weight applied to weight sensors).

VIII. An alarm system should include a dialler so that it would be able to alert response forces in case of a breach. A siren or other alarm element should be considered.

IX. Magnetic or mechanical switches that are installed on window frames are an effective tool to make sure that windows are closed after hours. However, it must be noted that they are not able to detect situations in which the window's glass is broken.

X. All external doors need to be fitted with detection equipment.

XI. All external openings that can be reached by people from the outside must be fitted with detectors. This includes ground level openings and those openings that can be reached by climbing.

XII. It is recommended that an independent expert in the field of alarm systems be consulted before designing a building's alarm system.

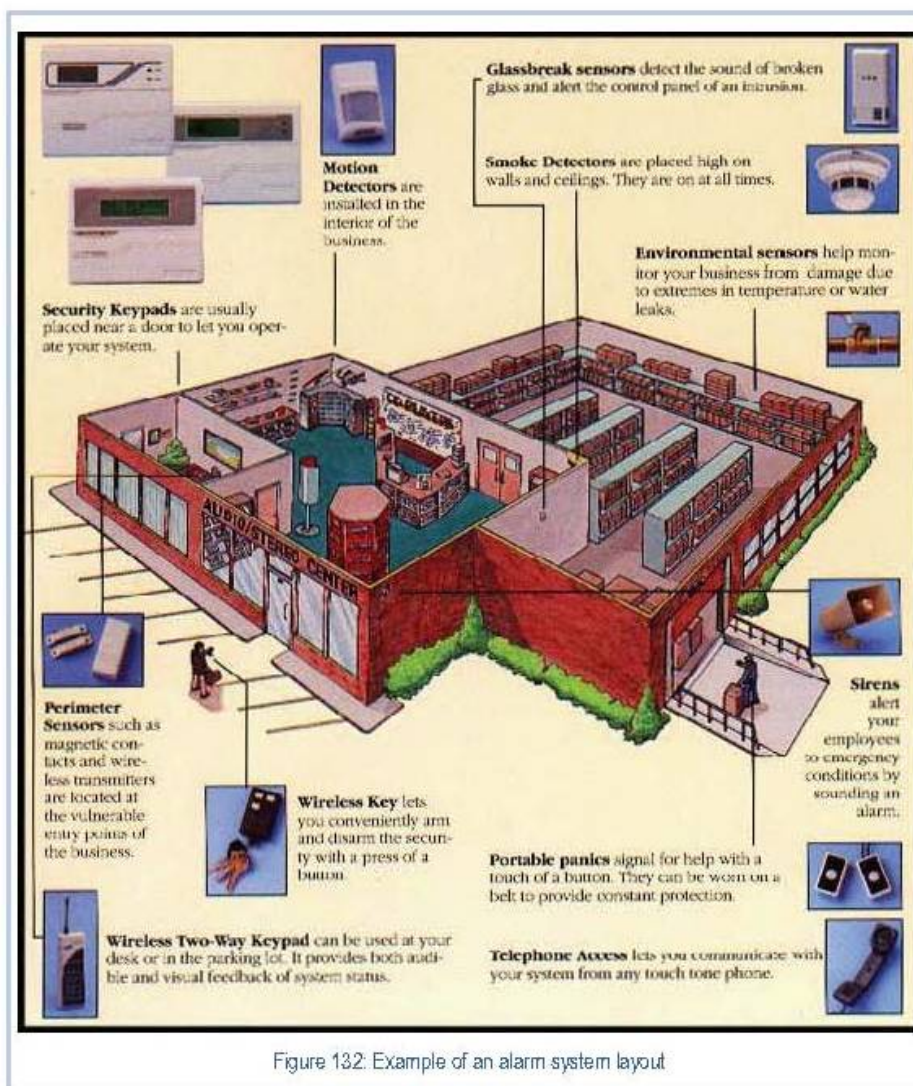
Standards

The system should comply with the construction and electricity related standards.

8.5.4 EXAMPLES



Figure 131: Samples of magnetic switches installed on doors – embedded (left), and visible (right)



8.6 ACCESS CONTROL SYSTEM

8.6.1 INTRODUCTION

Access control is the ability to determine who may and who may not enter specific areas or access particular assets. It is a fundamental principle of access management, and an important aspect of any effective security system. When applying access control, the following issues need to be taken into account:

- The number of entrances to the building/installation should be minimised.
- Identifying and deciding areas to which access should be limited.
- The employed measures should not interfere with fire protection and safety systems.
- The measures must still facilitate access to the building by the disabled.

When designing an access management plan, developers should analyse which areas and assets need to be protected by access control measures. After deciding which areas and assets should be protected, the proper measures need to be selected and deployed. Entry-point screening is typically employed at the entrance to secure/ non-public areas. This type of screening can employ the following measures: identity verification measures, physical screening (e.g. people, bags, vehicle, etc.), x-ray screening, weapons detection measures, explosives detection measures, and chemical/ biological agent detection measures.

The security related access control system must be designed together with the other security systems. This section will relate to access control systems while other access control issues can be found in **Section 5.4**.

Access control is a combination of physical elements and security procedures. The physical access control measures usually include the following and more:

- Card readers.
- Control panels for opening doors.
- Electromagnetic locks.
- Electric locks.
- Emergency escape buttons (glass break).
- Open door detectors (magnetic switches).
- Access control management software.
- Access control management stations.
- A door closer.

8.6.2 TERMS AND DEFINITIONS

Access Control	Any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.
Electromagnetic lock	An electric lock that functions by creating a magnetic field. When installed in doors, usually applies forces ranging from 150 kg to 500 kg.
Electric lock	An electric lock whose internal mechanic parts are operated by electricity. When the lock is instructed to open (by applying an electric current to it) the portal it locks can be pushed open without the use of a lever.
Break glass button	A button enclosed in a glass covered container and installed next to an access controlled door. When pressed, the button immediately unlocks the door it is installed next to. Break glass buttons are meant to allow access control doors to be opened by the public in an event of an emergency.

8.6.3 DESIGN OF AN ACCESS CONTROL SYSTEM

- I. All external doors that are used on a regular basis but should be closed to the general public would require access control.
- II. All access controlled doors should be equipped with a closer.
- III. If in doubt, infrastructure should be prepared to allow access control measures to be deployed, as adding the infrastructure at a later stage will be very difficult.
- IV. The main entrance doors should be equipped with an automatic locking mechanism allowing external guards to lock the doors if an emergency situation occurs outside.
- V. A door that is supposed to be protected against forced entry must be equipped with an electromagnetic lock rather than an electric lock.

Standards

The system should comply with the construction and electricity related standards.

8.6.4 EXAMPLES OF DESIGN

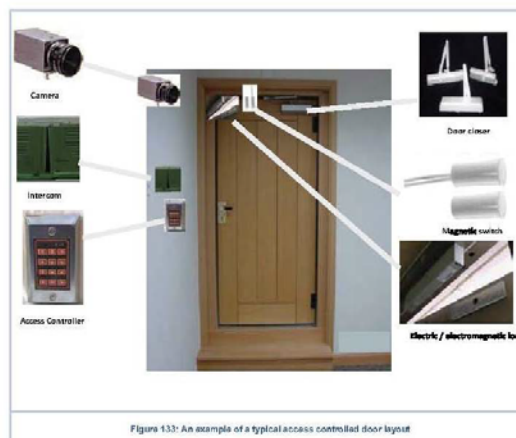


Figure 133: An example of a typical access controlled door layout

8.7 CCTV SYSTEM

8.7.1 INTRODUCTION

The primary purpose of a CCTV system is to support and enable the overall management of a building's security. Video surveillance facilities are an aid to security monitoring, especially of vulnerable or sensitive areas. CCTV systems may also act as an investigative tool as a post-incident source of evidence, or may deter potential criminals/terrorists if they perceive that their actions are being monitored. However, the CCTV system does not perform an active protective role and should not be designed to serve as the sole protective measure in a specified area, but must work in conjunction with other security measures (e.g. access controls, alarm systems, etc.).

THESE GUIDELINES HAVE BEEN DEVELOPED TO PROVIDE FOR A UNIFORM AND CONSISTENT APPROACH TO THE RECOMMENDED SPECIFICATION, INSTALLATION, OPERATION AND PERFORMANCE OF CCTV SYSTEMS ACROSS BUILDINGS IN SINGAPORE.

Given the dynamic CCTV market, these guidelines will not spell out specific technologies and capabilities within the system but relate to general concepts and design considerations that should be taken into account when developing a building's CCTV system.

AS THERE ARE MANY CCTV OPTIONS AVAILABLE ON THE MARKET, IT IS RECOMMENDED TO EMPLOY A PROFESSIONAL CONSULTANCY WHEN DESIGNING CCTV SYSTEMS.

8.7.2 TERMS AND DEFINITIONS

Closed circuit television (CCTV)	An electronic system consisting of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.
CCTV pan-tilt-zoom camera (PTZ)	A CCTV camera that can be moved side to side, up and down, and zoom in or out.
CCTV pan-tilt-zoom control	The means of controlling the PTZ functions of a camera.
CIF	Common Intermediate Format (CIF) is used to standardise the horizontal and vertical resolutions in pixels of sequences in video signals (e.g. 4 CIF has a resolution of 704 x 576 pixels).
Codec	A codec is a device or programme capable of performing encoding and decoding on a digital data stream or signal.
Frame Frequency	The number of times per second that the frame is scanned. The U.S. standard is 30 frames per second.
Multiplexer / matrix switcher	The number of times per second that the frame is scanned. The U.S. standard is 30 frames per second.
Frame	The total area, occupied by the television picture, which is scanned while the picture signal is not blanked.
Resolution	The level to which video details can be determined in a CCTV scene is referred to as resolving ability or resolution.
Rotakin	The Rotakin target was developed by the Police Scientific Development Branch, Home Office (United Kingdom) as a means of auditing the efficiency of a CCTV system. It consists of a human silhouette target 1.6m in height. When the target fills the screen vertically it is said to be 100%R.

8.7.3 DESIGN CONSIDERATIONS

CAMERAS

- I. The CCTV system should consist of multiple cameras distributed throughout the building to give comprehensive coverage of all common areas¹¹ to a height of 2m from floor level.
- II. Cameras in common areas should be situated where they cannot be easily evaded, damaged or obscured and should be clearly visible to members of the public. Where headroom is restricted and cameras may obstruct public passage, cameras should be mounted in recesses so as to avoid the possibility of injury to members of the public.
- III. Cameras located in vulnerable locations should be protected against vandalism by means of vandal resistant materials and design (e.g. vandal-resistant enclosures with non-reflective, shatter-resistant glass viewing ports).
- IV. All cameras should provide colour images to maximise the scope for crime detection and to enable clear identification of offenders.
- V. Cameras should be suitable for internal or external use (depending on location) and provide sufficient quality of picture and view in all weather conditions.

- VI. All cameras at key areas should be static and fitted with fixed focal length and field of view that cannot be adjusted by non-authorised users. In addition to these, it may be good to install PTZ cameras (especially in areas where there may be mass congregations or main thoroughfares) to allow the security surveillance operators to pan, tilt or zoom as and when required.

MONITORS

- I. All monitors should be capable of displaying colour images and have appropriate adjustment controls (e.g. contrast, brightness, sharpness, etc.).
- II. The displayed picture on monitors should be sharply defined, stable, with accurate colour reproduction, and should be free of noise, interference or pulsing effects.
- III. Monitor sizes should be appropriate for the intended viewing distance within the room housing the viewing facilities. The system should allow multi-view display on CCTV monitors.

RECORDING EQUIPMENT

- I. The system must incorporate sufficient image recording capacity to enable the continuous 24-hour recording of each camera and archival of at least 28 days, with an additional 10% minimum buffer. Sufficient reserve recording media should also be kept to replace those seized by security agencies for post incident investigations.
- II. The system should have duplex multiplexing capability or greater. This is meant to allow simultaneous image recording and playback. The system should be designed in a way that enables playback of footage without causing interruption to the recording process.
- III. The system integrator or vendor should propose codecs to achieve optimal compression ratios while ensuring no or little loss of image/ video quality (e.g. MPEG4 and M-JPEG2000). The video container format proposed for the DVR recorded images and viewer software should be open-source container formats and/or common multi-media container formats (e.g. *.avi (Microsoft), *.mov (Apple QuickTime), *.mp4 (MPEG)).
- IV. An authentication mechanism should be included to ensure the integrity of all recordings by allowing for detection of any alteration or tampering (e.g. watermarking). This should include the recording of the camera ID and date and time (synchronised from a single source), which must not be adjustable by the operator.

QUALITY OF RECORDED IMAGES

- I. Images captured by the CCTV cameras should be recorded using digital video recorders (recommendation subject to change with future advancements in technology).
- II. The footage collected by each camera should be recorded at a minimum of 6 frames per second (for indoor) or 12 frames per second (for outdoor). In addition, the capability to record from selected or designated cameras in real time mode at 25 frames per second would be useful.
- III. The recording equipment should be able to record colour images of sufficient quality to assist in prosecution with the image quality meeting a resolution of at least 4CIF or equivalent.

¹¹These include general access locations such as main entrance lobbies, corridors, taxi stands, car parks, pavements, streets within the development's boundary line.

IV. The recorded image should at all times be accurate, sharply defined and with accurate colour reproduction under normal lighting. For reduced lighting or emergency lighting conditions, the recorded image should minimally be an accurate and defined reproduction of the scene in monochrome.

PLAYBACK FACILITIES

I. The CCTV system should provide for the playback, removal or transfer of any image from any camera recorded up to 28 days prior (in a controlled environment).

EXPANSION CAPABILITY

I. The installed CCTV system should be designed to allow for future expansion or additional capacity with minimum disruption to the working system.

COVERAGE AT KEY AREAS

I. Common Areas – Comprehensive coverage throughout common areas is necessary to enable the monitoring of the flow of people, the identification and mitigation of potential overcrowding situations and the identification of undesirable, illegal or anti-social behaviour. This includes general access areas such as main entrance lobbies, street areas, pavements, car parks and vehicle boarding and alighting points such as taxi stands, bus-stops and vessel docking points within the development's boundaries. For hotel premises, coverage should include to the lobby, front desk, concierge, entrance/exit points and corridors. General views should meet a minimum image height at 'Detection (10%R)' level (refer to later section on defining and measuring fields of view for CCTV systems).

II. Entrances & Exits - All external public access doors, emergency exits and vehicle entrances/exits (e.g. at the gantry points of car parks) should be fitted with cameras which provide a clear, unobstructed image of all persons entering/exiting through them (frontal view). The cameras must be mounted at a suitable height (e.g. where they cannot be evaded, damaged or obscured) – looking towards, rather than down at the doorway or driver, and meet a minimum image height of 'Enhanced Detection (20%R)' level. For buildings with sizeable open areas included in its boundary, the minimum image height would be 'Recognition (50%R)' level.

III. Lifts – For lifts which act as alternate entry and exit points to the building, frontal view of the lift doors for people entering the building and general views of the associated lift lobby areas are to be monitored at 'Enhanced Detection (20%R)' level.

IV. Checkpoints – For locations that involve security checks or registration before people are granted permission to proceed further into the building like checkpoints and ticket issuance counters, the CCTV system should capture the frontal view of people at 'Recognition (50%R)' level.

V. Sensitive areas – These include rooms or open areas that house important and critical equipment, documents, property and people e.g. warehouses, locker facilities, etc. In particular, cameras should also cover facilities involving monetary transactions, such as at banks, money changers and ATM machines locations. Cameras at these areas should be installed with a minimum image height of 'Enhanced Detection (20%R)'. In addition, each door should be fitted with an intrusion alarm and upon activation of the alarm, trigger the display of the image of the relevant camera(s) automatically on a dedicated monitor.

Table16: Summary of Recommendations for Key Areas

Location	Defined Areas	Detection – 10%R	Enhanced Detection – 20%R	Recognition – 50%R	Identification – 120%R
Common Areas	Extensive Coverage of Common Areas (e.g. main entrance lobby).	Yes			
	Street Areas Within Building's Boundaries (including pavements, walkways).	Yes			
	Vehicle boarding and alighting points (including taxi stand) and Parking areas.	Yes			
Entrances & Exits	Frontal view of people entering the building's premises via main entrances/ exits.		Yes		
	Vehicle description and number plate to be captured at vehicle entrances/ exits/ loading and unloading bay.		Yes		
	Entrances/ Exits (along passageways, walkways & subways) leading to the concourse area.		Yes		
	Emergency Exits (Both Sides).		Yes		
	Designated Entrances and Exits for buildings with sizeable open spaces.			Yes	
Lifts	Frontal view of the lift doors for people entering the building premises.		Yes		
	General views of the associated lift lobby areas.		Yes		
Checkpoints	Frontal view of people registering at counter.			Yes	
Sensitive Areas	External view of access for enclosed areas.		Yes		
	Intrusion-alarm triggered image viewing on security monitors when enclosed area is breached.		Yes		
	100% coverage of open areas.		Yes		

8.7.4 INSTALLATION & OPERATION

INSTALLATION OF THE CCTV SYSTEM

I. The positions of the cameras should be carefully planned and located to provide the required coverage with the minimum number of cameras. Account should be taken of the effect that periods of maximum human density may have on the achievement of the operational requirement.

II. Notices strategically located around the building should be provided to inform members of the public that the CCTV system is being continuously monitored and recorded.

III. Upon successful hand-over of a fit for purpose system, a soft and hard copy of each of the agreed camera views and image quality (both monitor view and the recorded image) should be taken and reviewed by the building's Security Manager, to ensure that the field of view and image quality from each camera fit the building's security requirements.

IV. If the same proprietor owns adjacent buildings, it would be useful for each building's CCTV system to include the capability of accessing images from the adjacent locations as well.

V. To facilitate incident management by Emergency Agencies during a crisis situation, it would be good to provide capabilities for the Emergency Agencies' mobile command post to retrieve live images for remote viewing. This could include up to 3 video output channels and one control port extended to, and terminated at the room housing the building's viewing facilities.

VI. The storage facilities for the CCTV systems should be capable of keeping the recordings in a secure environment protected from excessive moisture and dust, with preventive measures against unauthorised removal or viewing of the recordings. The location of the recording and storage facilities should be decided on a local risk assessment which takes into account security and crime-related risks, and should be sited in the inner parameter of the building and away from vehicular access. If the location of these facilities is located in the inner parameter of the building but still deemed to be high-risk (e.g. open to public access), then it is recommended that the room be built with adequate reinforcement/protection to withstand the explosion of a 10kg TNT or equivalent charge (with fragmentations) at a distance of 5 meters away.

VII. The network must have sufficient bandwidth to support the requirements of the CCTV system (e.g. in terms of the maximum number of concurrent feeds).

USE OF THE CCTV SYSTEM

I. Within the CCTV viewing facility, the operator should be able to select any camera picture for display on any monitor at any time or alternatively to set up a scanning sequence as desired. The dwell time of the scanning sequence should be adjustable.

II. The camera selection control system should allow rapid selection of any camera using minimum manual effort and be consistent across the CCTV network.

III. The CCTV system should include a 'default settings' function which allows cameras with fixed zones of coverage to auto reset to their original position after a pre-determined time duration.

IV. Any one user selecting a live image (feed) should not preclude other users selecting the same live image (feed), or any other live images (feed) on the same system.

V. For viewing of recorded images, the recording equipment should have capabilities of normal play, replay, still field, fast forward, rewind, record, stepping frame, visual search – forward & reverse, speed search and stop.

VI. The camera ID and the date and time should be displayed on monitors in a single imposition and for the recorded image be located where it is least likely to obscure or interfere with the image of the main subject.

VII. The numbering of cameras and the associated recording sequence should be carefully planned in order to facilitate both the rapid and seamless tracking of targets' movement and the speedy retrieval of recorded images.

CCTV OPERATING STAFF

I. The shift patterns adopted for the CCTV operating staff should include sufficient breaks to ensure health and productivity of the staff.

II. The CCTV operating staff should undergo the appropriate training as stipulated by the building's Security Manager for security personnel. They should rudimentarily be taught what to look out for and be able to react when a potential incident occurs, to monitor the event accurately and not lose information that could be pertinent to any future investigation.

III. It would also be beneficial to have Standard Operating Procedures (SOPs) in place for reference and to conduct regular refreshers to ensure that the CCTV operating staff are familiar with the SOPs.

8.7.5 ESSENTIAL SUPPORT

POWER SOURCE

I. Uninterruptible power supply (UPS) with at least 30 minutes of backup capacity should be provided for the CCTV system.

II. The CCTV system should feature an alert system for loss of power or image due to technical failure.

LIGHTING FOR CCTV

I. The building should be provided with adequate lighting 24/7 to ensure that quality coloured images for facilitating monitoring, investigation and prosecution are captured.

II. In the event of lighting failures, the CCTV system should be capable of producing images that will enable evacuation of the building to be effectively managed under emergency lighting conditions.

MAINTENANCE AND AUDIT OF CCTV SYSTEM

I. The CCTV system should be supported by a maintenance regime that ensures the operational requirements are consistently met and availability of all parts of the system are maximised. System availability should be set at 95% over a 12 month time frame.

II. The quality of the visual and recorded images should be monitored and compared to a set of auditing standards, implemented by the building's Security Manager. Any deterioration should be rectified immediately.

III. All system fault rectifications should be rectified within 24 hours, or sooner if the fault results in serious loss of CCTV coverage.

IV. The building's Security Manager should also be responsible for auditing the correct implementation of the CCTV system to meet the operational requirements and identify any improvements (if necessary).

8.7.6 DEFINING AND MEASURING FIELDS OF VIEW FOR CCTV SYSTEM

CATEGORIES OF VIEW

I. Fields of view required for CCTV systems are described by four categories of view as follows:

a) **Detection** – The figure occupies at least 10% of the available screen height. Following an alert an observer can, after a search, ascertain with a high degree of certainty whether or not a person is visible in the pictures displayed to him.

b) **Enhanced Detection (ED)** – Following an alert an observer can, after a search, ascertain with a high degree of certainty whether or not a person is visible in the pictures displayed to him. It must be noted that 'Enhanced Detection (ED) (20%R)' is used throughout this document, and is a specific measure.

c) **Recognition** – When the figure occupies at least 50% of the screen height, viewers can say with a high degree of certainty whether or not the individual shown is the same as someone they have seen before.

d) **Identification** – When the figure occupies at least 120% of the screen height, picture quality and detail is sufficient to enable the identity of a subject to be established beyond reasonable doubt.

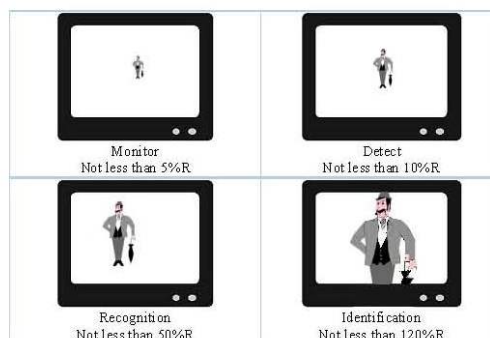
II. The categories are measured by relating the views to the image height of a standard test target 1.6 m high. When the image of the target fills the screen vertically the image height is said to be 100%R, where 'R' is the abbreviation of 'Rotakin'. For use in the building's environment, these have been defined as follows:

- a) **Detection** - Not less than 10% R.
- b) **Enhanced Detection (ED)** - Not less than 20% R.
- c) **Recognition** - Not less than 50% R.
- d) **Identification** - Not less than 120% R.

III. For Detection (10%R) and Enhanced Detection (20%R), it is assumed that the image contrast of the target is sufficiently above the threshold of human sensitivity and that the picture is not unduly cluttered with non-targets.

IV. For Recognition (50%R) and Identification (120%R), it is assumed that the angle of view and lighting is suitable and no significant degrading effects such as image blur due to motion or out of focus is evident.

V. It should however be noted that these measurement guidelines were originally set up using a fully analogue PAL system with a fixed resolution of 576 lines and may not transfer faultlessly into the digital domain. For digital systems, consideration should be given to the number of 'pixels on target' when attempting to categorise the level of detail required in the image. It is also important to examine the recorded picture quality to ensure that the picture quality is not reduced due to the image compression technology.



THIS GUIDELINE OF RECOMMENDED STANDARDS FOR CCTV SYSTEMS FOR BUILDINGS HAS BEEN JOINTLY PRODUCED BY HOMEFRONT SECURITY DIVISION AND SINGAPORE POLICE FORCE OF THE MINISTRY OF HOME AFFAIRS, SINGAPORE.

8.7.7 REFERENCES

- I. London Underground Limited - Station Surveillance CCTV Standard (Reference No: 2-03066-004, version A3, dated July 2005);
- II. Video Surveillance System (VSS) – Standard For Bus Interchanges (Version 3.0, dated July 2006);
- III. Video Surveillance System (VSS) – Standard For Mass Rapid Transit (MRT) Stations (Version 3.0, dated July 2006);
- IV. Building a Building Security Code (BSC) Framework in Singapore (Version 7.0, dated 18 Aug 2006);
- V. CCTV Cameras Standards for Police Establishments (Version: 3.0, dated 22 Dec 2006);
- VI. Draft for Public Australian Comment Standard – AS 4806.1 Closed Circuit Television, Management & Operation Code of Practice (dated 16 Sep 2005);
- VII. CCTV Operational Requirements Manual – Home Office Scientific Development Branch (Version 4.0, dated Jan 2007).

8.8 SECURITY LIGHTING FOR CCTV SYSTEMS

This section discusses the lighting requirements for security systems including CCTV. For general lighting considerations, please see Section 5.7.

8.8.1 INTRODUCTION

Sufficient lighting is necessary for people to see and be seen. From a security point of view, lighting that is strategically placed can increase the effectiveness of CCTV systems and guard work while reducing the chance of criminal acts occurring in the illuminated area. The basic level of lighting should allow the security deployment (CCTV and guards) to identify a human face from a distance of about 10 metres.

If the area is intended to be used during the hours of darkness, the lighting system should provide adequate visibility for the intended night time operation. Pedestrian walkways, back lanes and access routes open to public areas should have a basic level of lighting. Inset spaces, signs, entrances and exits should be adequately lit so that CCTV coverage would provide a clear picture.

Security lighting is employed in order to increase the visibility around perimeter lines, buildings, and sensitive locations. It is a security management tool that is applicable in almost all environments within an urban development. Proper lighting can greatly improve the combined operation of other security systems, particularly CCTV and other surveillance measures, and therefore it must be designed to compliment these systems.

8.8.2 TERMS AND DEFINITIONS

Continuous lighting	Continuous lighting is the most commonly used form of security lighting systems. These systems consist of a series of fixed light sources that are configured to light up a specified area on a continuous basis. The light sources are usually configured to create overlapping cones of light during the hours of darkness. There are two primary types of continuous lighting: <i>Glare Projection.</i> This type of lighting is useful when the desired effect is a glare of lights directed toward the exterior of a facility and into the eyes of a potential intruder. The lighting used at vehicle entrances is a good example. A vehicle that approaches a vehicle entrance during night time is illuminated, but the guard post remains in relative darkness. <i>Controlled Lighting.</i> This lighting is used most often at locations where it is necessary to limit the width of the lighted strip outside the perimeter fence because of nearby residential areas, public thoroughfares, or other activity centres. When applying controlled lighting, the width of the lighted strip can be controlled and arranged as required. For instance, one possible configuration might be a wide band of illumination inside the fence and a narrower band on the exterior of the fence.
Standby Lighting	Standby lighting systems are similar to continuous lighting systems and have to meet the same security lighting specifications. The difference is that standby lighting is only used in certain circumstances. For example, when a possible intruder is detected, the security system or guard force can activate the standby lighting system for extra illumination. Standby lighting differs from the continuous lighting in that only security personnel or the security system software have control over the system.
Portable Lighting	These lighting systems are made out of manually operated portable light sources and luminaires such as searchlights. These systems can be moved as needed to cover specific areas. Movable lights are normally used to supplement continuous or standby systems.
Emergency Lighting	This lighting system may be deployed side by side with any of the other three systems. It is only used during periods of main power failure. While, when possible, security lighting should be connected to an uninterruptible power system, emergency lighting should depend on a separate, alternate power source, such as portable generators or batteries.

8.8.3 STANDARDS

The recommended standards are based on the US DOT standards FTA-TRI-MA-267085-05 and DOT-VNTSC-FTA-05-02.

Table 17: Illuminance Specification

Lighting Target	Illuminance	Lux	Foot-candles
LARGE OPEN AREAS (Standard System)	Average minimum illuminance	2	0.2
	Absolute minimum illuminance	0.5	0.05
LARGE OPEN AREAS (Glare System)	Average minimum illuminance	2	0.2
	Absolute minimum illuminance	0.5	0.05
SURVEILLANCE OF CONFINED (low ceiling / interior) AREAS	Average minimum illuminance	5	0.5
	Absolute minimum illuminance	1	0.1
SURVEILLANCE OF VEHICLE OR PEDESTRIAN ENTRANCES	Average minimum illuminance	10	1
	Absolute minimum illuminance	2.5	0.25
CCTV SURVEILLANCE	Varies with individual systems (Consult CCTV manufacturer)		

8.8.4 DESIGN OF SECURITY LIGHTING

- I. Lights located in vulnerable locations should be protected against vandalism by means of vandal resistant materials and design.
- II. Lighting design should take into account the various current and future obstructions that may cause light to be blocked (e.g. various types of vegetation, such as trees).
- III. Design proposals should take into account the possibility of night time outdoor activities and should specify the type, location and intensity of the various lighting elements that will be installed.
- IV. Lighting should be equally spread out, reducing contrast between shadows and lightened areas. It is recommended to use more fixtures with lower wattage rather than fewer fixtures with higher wattage. This will help reduce the creation of deep shadows and will help avoid excessive glare.
- V. Where possible, lighting fixtures should be located at heights that enable easy maintenance and replacement.
- VI. The lighting plan should locate areas that may be shadowed and light them up.
- VII. Lighting at manned entrances must be adequate to identify persons, examine credentials, inspect vehicles entering or departing the facility premises through designated control points (vehicle interiors should be clearly lighted), and prevent anyone from entering unobserved into the premises.
- VIII. The lighting illuminating the building's entrance should allow for person identification during hours of darkness and extreme environmental conditions (e.g. heavy downpour).
- IX. Security posts at entrance points should have a reduced level of interior lighting to enable the security guards to see his surroundings while minimising the adversary's ability to look inside the posts.
- X. The controls of the lighting systems should be positioned in a secured area, preferably in the security control room.
- XI. Lighting should be continuous and should be sufficient to support the CCTV coverage.
- XII. Cones of illumination should overlap to provide coverage in the event of bulb burnout.
- XIII. Lighting should be arranged so as to create minimal shadows and minimal glare.
- XIV. Lighting should be turned on automatically by clock or photoelectric cell.

8.8.5 EXAMPLE



Figure 134: An image taken from CCTV showing optimal lighting (left), glare caused by too much light (middle) and a shadow caused by insufficient lighting (right).

附錄二 美國國土安全事務部「建築物防恐脆弱度評估清單」

本研究摘錄美國國土安全事務部（Federal Emergency Management Agency）於 2008 出版之「保護現有商業大廈使用者和建築物免受恐怖襲擊」一書，其中「建築物防恐脆弱度評估清單」供建築師及相關專業者之參考。

2.3 IDENTIFYING INTEGRATION OPPORTUNITIES FOR INCREMENTAL BUILDING PROTECTION

Typical maintenance and capital improvement projects in commercial buildings fall into two categories:

- Maintenance and capital improvements that are common to all four types of commercial buildings—office, retail, and multifamily apartment buildings, and hotels.
- Maintenance and capital improvements specific and unique to each of the four types of commercial buildings.

These categories may also vary by building classification (A, B, or C). The following categorizations of maintenance and capital improvements are typical and reflect groupings of building elements, administrative and funding categories, tenant versus public spaces, or other parameters. Owners can substitute their own categories.

Common categories of maintenance and capital improvement projects:

1. Roofing maintenance and repair/reroofing
2. Exterior wall and window maintenance/façade modernization
3. Fire and life safety improvements
4. Public area modernization (Retail: mall public areas; Hotels: public and service areas)
5. Underfloor and basement maintenance and repair
6. HVAC upgrade and energy conservation
7. Hazardous materials abatement
8. Landscaping and site work

Occupancy-specific categories of maintenance and capital improvement projects:

Office Buildings:

1. New technology accommodations
2. Tenant alterations and improvements

Retail Buildings:

1. Retail area modernization

Multifamily Apartment Buildings:

1. Kitchen and bathroom modernization

Hotels and Motels:

1. Guestroom finishing, furniture, and equipment (FF&E)
2. Public area FF&E

Both of these respective categories are used as the horizontal axes of the integration matrices presented on the following pages.

How to Use the Matrices

In order to identify integration opportunities, a building owner should follow these three steps:

1. Identify the column of the planned maintenance or capital improvement.
2. Identify the physical increments of building protection with a corresponding check mark in the column.
3. Consider integration of the physical increments with the planned maintenance or capital improvement activities.

Matrix 1: Integration Opportunities for Common Categories of Maintenance and Capital Improvement Projects

		Maintenance and Capital Improvement Projects							
		Roofing maintenance & repair	Exterior wall & window work	Fire & life safety improvements	Public area modernization	Underfloor & basement work	HVAC upgrade & energy work	Hazardous material abatement	Landscaping
1. Site									
1.1 Increased standoff distance (3.3)									✓
1.2 Anti-ram vehicle barriers (3.3)									✓
1.3 Speed calming devices (3.3)									✓
1.4 Operable barriers (3.3)									✓
1.5 Security lighting (5.8)									✓
1.6 Detection & assessment measures	1.6.1 Exterior intrusion detection systems (5.2.1)								✓
	1.6.2 Access control systems (5.2.4)								✓
1.7 Interdiction/response measures	1.7.1 Guard force — detection/delay role (5.3.1)								✓
2. Architectural									
2.1 Bracing or reinforcing masonry walls at interior stairs (3.5)				✓	✓				
2.2 Restraint of hazardous materials containers (3.5)				✓	✓	✓	✓	✓	
2.3 Architectural isolation of lobby, mailroom, cloakroom, & loading docks (4.3.2)					✓				
2.4 Architectural measures to isolate mechanical spaces that require large volumes of outside air (4.4.3.2)				✓	✓				
2.5 Vestibules or revolving doors for highly protected zones (4.3.5, 4.3.6)				✓	✓				
2.6 Vestibules or revolving doors for protected zones (4.3.7)				✓	✓				
2.7 Access control systems (5.2.4)				✓	✓				
3. Structural Systems (3.6)									
3.1 Upgrading the structure to make it more ductile			✓	✓	✓	✓	✓	✓	
3.2 Upgrading spandrel beams to achieve catenary response			✓						
3.3 Upgrading slabs to achieve catenary response					✓	✓			
3.4 Standoff distance around vulnerable columns (3.6.1)			✓		✓				
3.5 Localized hardening of vulnerable columns (3.6.1)			✓		✓				
3.6 Floor slab upload resistance (3.6.2)					✓				

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

Matrix 1: Integration Opportunities for Common Categories of Maintenance and Capital Improvement Projects (continued)

		Maintenance and Capital Improvement Projects							
		Roofing maintenance & repair	Exterior wall & window work	Fire & life safety improvements	Public area modernization	Underfloor & basement work	HVAC upgrade & energy work	Hazardous material abatement	Landscaping
3.7 Load-bearing URM ¹ (3.6.3)	3.7.1 Shotcrete		✓	✓	✓	✓	✓	✓	
	3.7.2 Steel sections		✓	✓	✓	✓	✓	✓	
	3.7.3 Stiffened steel-plate wall system		✓	✓	✓	✓	✓	✓	
	3.7.4 Reinforcing		✓	✓	✓	✓	✓	✓	
3.8 Transfer girder retrofit (3.6.4)			✓						
4. Building Envelope									
4.1 Glazing	4.1.1 Fragment retention film (3.4.2)		✓	✓	✓		✓		
	4.1.2 Laminated glass (3.4.3)		✓	✓	✓		✓		
	4.1.3 Blast curtains (3.4.4)			✓	✓		✓		
	4.1.4 Glazing catch cable/bar (3.4.5)			✓	✓		✓		
	4.1.5 Energy absorbing cable systems (3.4.6)			✓	✓		✓		
4.2 URM (3.4.7)	4.2.1 Sprayed-on polymer		✓	✓	✓		✓		
	4.2.2 Geotextile fabric			✓	✓		✓		
	4.2.3 Steel stud and sheetmetal construction			✓	✓		✓		
4.3 Other building envelope retrofits	4.3.1 Bracing parapets, gables, ornamentation, & appendages (3.4.8)	✓	✓						
	4.3.2 Cladding anchorage (3.4.1)		✓						
	4.3.3 Anchorage of masonry veneer (3.4.8)		✓						
	4.3.4 Anchorage of steel stud backup (3.4.8)		✓	✓	✓		✓		
	4.3.5 Anchorage of exterior wythe in cavity walls (3.4.8)		✓						
	4.3.6 Debris catch systems for façade elements (3.4.8)		✓	✓	✓		✓		
	4.3.7 Increasing the roof's resistance to blast (3.6)	✓							
	4.3.8 Upgrading connections of light metal deck roofs to structure (3.6)	✓							
4.4 Sealing measures to tighten the envelope of the building and selected safe rooms (4.3.3)			✓		✓				

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

1. URM = unreinforced masonry

Matrix 1: Integration Opportunities for Common Categories of Maintenance and Capital Improvement Projects (continued)

		Maintenance and Capital Improvement Projects							
		Roofing maintenance & repair	Exterior wall & window work	Fire & life safety improvements	Public area modernization	Underfloor & basement work	HVAC upgrade & energy work	Hazardous material abatement	Landscaping
5. Utility Systems									
5.1 Light, secure, and monitor water service access points (5.8)					✓		✓		✓
5.2 Intrusion detection sensors for all utility services to the building (5.8)			✓		✓		✓		✓
5.3 Redundant utility systems to support security, life safety, and rescue functions					✓		✓		
5.4 Attachment and bracing of tanks (3.5)		✓			✓	✓	✓		✓
6. Mechanical Systems (HVAC)									
6.1 Fastening and bracing of mechanical equipment above ceilings (3.5)				✓	✓		✓	✓	
6.2 Attachment and bracing of boilers and chillers (3.5)							✓		
6.3 Enhanced physical security (4.4.2.2)	6.3.1 Secure air intakes against unauthorized access (5.8.1)	✓	✓				✓		✓
	6.3.2 Secure mechanical rooms & HVAC plenums against unauthorized access				✓		✓		
6.4 Enhanced sheltering in place (4.4.3.2)	6.4.1 Single-switch control of fans for sheltering and purging						✓		
	6.4.2 Automatic dampers for outside air intakes and exhaust fans		✓				✓		
	6.4.3 Separate fans & air streams for ventilation and recirculation for conditioning safe rooms						✓		
	6.4.4 Recirculation filter units in safe rooms			✓	✓		✓		
6.5 Aerosol filtration, medium level (4.4.4.2)	6.5.1 Sealing filter frames to minimize bypass						✓		
	6.5.2 Installation of filters of greater depth/surface area & higher MERV ² rating						✓		
	6.5.3 Operating at positive internal pressures						✓		
6.6 Gas-phase filtration, medium level (4.4.5.2)	6.6.1 Indoor-air-quality type, low resistance adsorbers						✓		
	6.6.2 Operating at positive internal pressures						✓		
6.7 Aerosol filtration, high level (4.4.6.2)	6.7.1 Installation of ventilation/makeup-air units with HEPA ³ filtration						✓		
	6.7.2 Operating at positive internal pressures						✓		

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

2. MERV = Minimum Efficiency Reporting Value

3. HEPA = High Efficiency Particulate Air

Matrix 1: Integration Opportunities for Common Categories of Maintenance and Capital Improvement Projects (continued)

		Maintenance and Capital Improvement Projects							
		Roofing maintenance & repair	Exterior wall & window work	Fire & life safety improvements	Public area modernization	Underfloor & basement work	HVAC upgrade & energy work	Hazardous material abatement	Landscaping
6.8 Gas-phase filtration, high level (4.4.7.2)	6.8.1 Ventilation/makeup-air units with high efficiency adsorbers & HEPA filtration						✓		
	6.8.2 Operating at positive internal pressures						✓		
6.9 Secure and monitor exterior mechanical spaces and equipment (5.8)			✓						✓
6.10 Secure and monitor interior HVAC access points (5.8)					✓		✓		
7. Plumbing & Gas Systems									
7.1 Attachment and bracing of sprinkler piping (3.5)				✓	✓		✓	✓	
8. Electrical Systems									
8.1 Attachment and bracing of emergency lighting (3.5)				✓	✓		✓	✓	
8.2 Fastening and bracing of electrical equipment above ceilings (3.5)				✓	✓		✓	✓	
8.3 Attachment and bracing of transformers (3.5)		✓			✓	✓			✓
8.4 Attachment and bracing of emergency generators (3.5)		✓			✓	✓			✓
9. Fire Alarm Systems									
10. Communications and IT Systems									
10.1 Public address system to achieve rapid implementation of emergency actions (4.4.3.2)				✓	✓		✓		
11. Equipment Operations & Maintenance									
12. Security Systems									
12.1 Exterior intrusion detection systems (5.2.1)			✓		✓				✓
12.2 Interior intrusion detection systems (5.2.2)				✓	✓	✓	✓		
12.3 CCTV ⁴ systems (5.2.3)		✓	✓	✓	✓	✓	✓	✓	✓
12.4 Duress alarms (5.2.6)				✓	✓	✓	✓		
13. Security Master Plan									

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

4. CCTV = closed circuit television

Matrix 2: Integration Opportunities for Occupancy-Specific Categories of Maintenance and Capital Improvement Projects

		Maintenance and Capital Improvement Projects					
		OFFICE		RETAIL	APARTMENT	HOTEL	
		New Technology	Tenant Alterations	Retail Area Modernization	Kitchen & Bath Modernization	Guestroom FF&E	Public Area FF&E
1. Site							
2. Architectural							
2.1	Bracing or reinforcing masonry walls at interior stairs (3.5)						
2.2	Restraint of hazardous materials containers (3.5)	✓	✓	✓			✓
2.3	Architectural isolation of lobby, mailroom, cloakroom, & loading docks (4.3.2)						
2.4	Architectural measures to isolate mechanical spaces that require large volumes of outside air (4.4.3.2)						
2.5	Vestibules or revolving doors for highly protected zones (4.3.5, 4.3.6)						✓
2.6	Vestibules or revolving doors for protected zones (4.3.7)						✓
2.7	Access control systems (5.2.4)						✓
3. Structural Systems							
3.1	Upgrading the structure to make it more ductile	✓	✓	✓	✓	✓	✓
3.2	Upgrading spandrel beams to achieve catenary response (3.6.2)						
3.3	Upgrading slabs to achieve catenary response (3.6.2)		✓	✓		✓	✓
3.4	Standoff distance around vulnerable columns (3.6.1)			✓			✓
3.5	Localized hardening of vulnerable columns (3.6.1)			✓			✓
3.6	Floor slab upload resistance (3.6.2)		✓	✓		✓	✓
3.7 Load-bearing URM (3.6.3)	3.7.1 Shotcrete	✓	✓	✓	✓	✓	✓
	3.7.2 Steel sections	✓	✓	✓	✓	✓	✓
	3.7.3 Stiffened steel-plate wall system	✓	✓	✓	✓	✓	✓
	3.7.4 Reinforcing	✓	✓	✓	✓	✓	✓
3.8	Transfer girder retrofit (3.6.4)						
4. Building Envelope							
4.1 Glazing	4.1.1 Fragment retention film (3.4.2)		✓	✓		✓	✓
	4.1.2 Laminated glass (3.4.3)		✓	✓		✓	✓
	4.1.3 Blast curtains (3.4.4)		✓	✓		✓	✓
	4.1.4 Glazing catch cable/bar (3.4.5)		✓	✓		✓	✓
	4.1.5 Energy absorbing cable systems (3.4.6)		✓	✓		✓	✓

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

Matrix 2: Integration Opportunities for Occupancy-Specific Categories of Maintenance and Capital Improvement Projects (continued)

		Maintenance and Capital Improvement Projects					
		OFFICE		RETAIL	APARTMENT	HOTEL	
		New Technology	Tenant Alterations	Retail Area Modernization	Kitchen & Bath Modernization	Guestroom FF&E	Public Area FF&E
4.2 URM (3.4.7)	4.2.1 Sprayed-on polymer		✓	✓		✓	✓
	4.2.2 Geotextile fabric		✓	✓		✓	✓
	4.2.3 Steel stud and sheetmetal construction		✓	✓		✓	✓
4.3 Other building envelope retrofits	4.3.1 Bracing parapets, gables, ornamentation and appendages (3.4.8)						
	4.3.2 Cladding anchorage (3.4.1)						
	4.3.3 Anchorage of masonry veneer (3.4.8)						
	4.3.4 Anchorage of steel stud backup (3.4.8)		✓	✓		✓	✓
	4.3.5 Anchorage of exterior wythe in cavity walls (3.4.8)						
	4.3.6 Debris catch systems for façade elements (3.4.8)		✓	✓		✓	✓
	4.3.7 Increasing the roof's resistance to blast (3.6)						
	4.3.8 Upgrading connections of light metal deck roofs to structure (3.6)						
4.5 Sealing measures to tighten the envelope of the building and selected safe rooms (4.3.3)			✓	✓	✓	✓	✓
5. Utility Systems							
5.1 Light, secure, and monitor water service access points (5.8)							
5.2 Intrusion detection sensors for all utility services to the building (5.8)							
5.3 Redundant utility systems to support security, life safety, and rescue functions							✓
5.4 Attachment and bracing of tanks (3.5)							
6. Mechanical Systems (HVAC)							
6.1 Fastening and bracing of mechanical equipment above ceilings (3.5)		✓	✓	✓	✓	✓	✓
6.2 Attachment and bracing of boilers and chillers (3.5)							
6.3 Enhanced physical security (4.4.2.2)	6.3.1 Secure air intakes against unauthorized access (5.8.1)						
	6.3.2 Secure mechanical rooms & HVAC plenums against unauthorized access.						✓

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

Matrix 2: Integration Opportunities for Occupancy-Specific Categories of Maintenance and Capital Improvement Projects (continued)

		Maintenance and Capital Improvement Projects					
		OFFICE		RETAIL	APARTMENT	HOTEL	
		New Technology	Tenant Alterations	Retail Area Modernization	Kitchen & Bath Modernization	Guestroom FF&E	Public Area FF&E
6.4 Enhanced sheltering in place (4.4.3.2)	6.4.1 Single-switch control of fans for sheltering and purging						
	6.4.2 Automatic dampers for outside air intakes and exhaust fans						
	6.4.3 Separate fans & air streams for ventilation and recirculation for conditioning safe rooms						
	6.4.4 Recirculation filter units in safe rooms		✓	✓	✓		✓
6.5 Aerosol filtration, medium level (4.4.4.2)	6.5.1 Sealing filter frames to minimize bypass						
	6.5.2 Installation of filters of greater depth/surface area & higher MERV rating						
	6.5.3 Operating at positive internal pressures						
6.6 Gas-phase filtration, medium level (4.4.5.2)	6.6.1 Indoor-air-quality type, low resistance adsorbers						
	6.6.2 Operating at positive internal pressures						
6.7 Aerosol filtration, high level (4.4.6.2)	6.7.1 Installation of ventilation/makeup-air units with HEPA filtration						
	6.7.2 Operating at positive internal pressures						
6.8 Gas-phase filtration, high level (4.4.7.2)	6.8.1 Ventilation/makeup-air units with high efficiency adsorbers & HEPA filtration						
	6.8.2 Operating at positive internal pressures						
6.9 Secure and monitor exterior mechanical spaces and equipment (5.8)							
6.10 Secure and monitor interior HVAC access points (5.8)			✓	✓		✓	
7. Plumbing & Gas Systems							
7.1 Attachment and bracing of sprinkler piping (3.5)		✓	✓	✓	✓	✓	✓
8. Electrical Systems							
8.1 Attachment and bracing of emergency lighting (3.5)		✓		✓			✓
8.2 Fastening and bracing of electrical equipment above ceilings (3.5)		✓	✓	✓	✓	✓	✓
8.3 Attachment and bracing of transformers							
8.4 Attachment and bracing of emergency generators							

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

Matrix 2: Integration Opportunities for Occupancy-Specific Categories of Maintenance and Capital Improvement Projects (continued)

	Maintenance and Capital Improvement Projects					
	OFFICE	RETAIL	APARTMENT	HOTEL		
	New Technology	Tenant Alterations	Retail Area Modernization	Kitchen & Bath Modernization	Guestroom FF&E	Public Area FF&E
9. Fire Alarm System						
10. Communications and IT Systems						
10.1 Public address system to achieve rapid implementation of emergency actions (4.4.3.2)	✓					✓
11. Equipment Operations & Maintenance						
12. Security Systems						
12.1 Exterior intrusion detection systems (5.2.1)						✓
12.2 Interior intrusion detection systems (5.2.2)	✓	✓	✓			✓
12.3 CCTV systems (5.2.3)	✓	✓	✓		✓	✓
12.4 Duress alarms (5.2.6)	✓	✓	✓			✓
13. Security Master Plan						

Note: The references in parentheses refer to the applicable discussions in Chapters 3, 4, and 5.

資料來源：Federal Emergency Management Agency (U.S.)，
Incremental Protection for Existing Commercial Buildings From
Terrorist Attack: Providing Protection to People and Buildings:
Providing Protection to People and Buildings，2008

附錄三 期初審查意見回應表

內政部建築研究所 100 年度第 8 次研究業務協調會議紀錄

一、時間：100 年 5 月 11 日(星期三)上午 9 時 30 分正

二、地點：本所簡報室

三、主席：何所長明錦 記錄：邱玉茹、張怡文、郭建源

四、出席人員：詳簽到簿

五、主席致詞：會議紀錄請確實如期簽辦。

六、研究案主持人簡報：(略)

七、發言要點及回應：智慧化建築安全防範設備計畫要領之研究案：

發言要點	回應
1. 應把握本所智慧建築標章目前推動重點方向，設計智慧建築、妥適應用智慧化建築設備之原則。計畫名稱可調整為「智慧化建築安全防範設備空間設計準則或設備計畫指引」。	業已修正計畫名稱。
2. 有關設備管理維護、工程費用估算等細節資料，免列入探討；研究範圍界定係指智慧化人身安全建築設備。研究方向可探討如何先將建築物設計為安全空間，再以安全設備輔助；並說明安全監控設備與保	業已調整計畫探討內容及方向。

發言要點	回應
全人員二者之功能差異性，是否有相互輔助之關係。	
3. 本研究可加強國內、外案例介紹，供建築師實務工作參考。	業已蒐及新加坡、美國有關建築安全防範設計實務相關手冊及案例，納入成果報告第 2、3、4 章。
4. 本案重點是給建築師一套完整的應用智慧化建築設備「系統思維」，研究成果應有一定深度，才可指引建築師將「個別安全防範設備」加以串連，構成「建築物整體安全防範系統」。	業於第 1、5 章說明本研究著重提供建築師「建構安全無慮環境」之設計思考架構而非僵化之設計解答，有系統地從安全觀點評估基地潛力與限制條件、解釋設計方案優劣、反省錯誤、累積專業經驗，將建築物個案之安全防範元素，作具有創造力之組合，妥適應用智慧建築安全防範設備。
5. 建築師瞭解設備應用原則後，即可針對新建、既有建築物、集合住宅用途別等個別條件進行設計，不需要針對建築物類型進行細分探討。	已調整研究探討範圍。
6. 本所 95 年曾進行 CCTV 對隱私權之影響研究；營建署亦曾針對建築物設置影響通行之刷卡機是否符合法規進行解釋，可在成果報告適當處提醒	本研究著重提供建築師「建構安全無慮環境」之設計思考架構，CCTV 只是可能之設計解答之一，CCTV 對隱私權之影響並非本研究探討範圍。

發言要點	回應
設置錄影監控設備有相關法律問題。	

八、會議結論：

本次會議與會同仁之寶貴意見，請各計畫主持人納入後續研究參採並修正內容，使研究成果更為豐富完整。

九、散會：(上午 11 時 00 分)

內政部建築研究所

召開本所 100 年度第 8 次研究業務協調會議簽到簿

時 間：100 年 5 月 11 日(星期三)上午 9 時 30 分正			
地 點：本所簡報室(新北市新店區北新路 3 段 200 號 13 樓)			
主 席：何所長明錦 <i>何明錦</i>		記 錄： <i>邱玉如</i> 代	
出席人員	簽 到 處	代 理 人	
		職 稱	簽 到 處
陳副所長瑞鈴			
鄭主任秘書元良	<i>鄭元良</i>		
毛組長華		簡任研究員	<i>王昭倫</i>
陳組長建忠	<i>林建忠</i>		
林組長建宏	<i>陳建忠</i>		
廖組長慧燕	<i>廖慧燕</i>		
相關人員			
<i>吳秉宸</i>	<i>陶其則</i>	<i>吳子承</i>	
	<i>簡文生</i>	<i>劉青峰</i>	
<i>白櫻芳</i>	<i>陳伯超</i>	<i>盧珽瑞</i>	<i>歐俊顯</i>
<i>郭建源</i>	<i>郭建源</i>	<i>張怡文</i>	<i>郭明遠</i>
<i>郭明遠</i>	<i>曹源峰</i>	<i>郭明遠</i>	<i>郭明遠</i>

[業務協調會議 S]

	蔣紹偉		
	盧文欽	蘇靖	
	李奕忠	林福廷	
	蔡宜中	林招煒	
	施文和		
	黃華澤		
	劉介元		

附錄四 期中審查意見回應表

內政部建築研究所 100 年度自行研究案「智慧建築安全防範設備空間設計準則之研究」、「高層集合住宅外牆磁磚剝落原因與解決對策探討（2/2）—水泥砂漿硬底壓貼工法之實驗研究」及「紅外線熱影像法於外牆磁磚表面溫度檢測特性之實驗研究」等 3 案期中審查會議紀錄

一、時 間：100 年 08 月 12 日（星期五）上午 9 時 30 分

二、地 點：簡報室

三、主持人：林組長建宏 記錄：張怡文、盧珽瑞、林谷陶

四、出席人員：（詳出席簽到單）

五、主席致詞：（略）

六、報告人簡報：（略）

七、綜合討論：「智慧建築安全防範設備空間設計準則之研究」案

發言要點	回應
1. 因為是期中報告，所以尚未看出具體研究成果，但由目次可看出本研究方向是正確的。	感謝委員之肯定。
2. 建議第二章第三節之後，加強安全防範設備內容之分析、比較說明（如：巡更系統），以及改良採用取捨之彙整。	第二章第三節業已增加建築物安全防範設備彙整
3. 本研究太偏向以設備器材維護安全，預防犯罪不限於設備，建築設計亦很重要，應該從都市計畫納入預防犯罪之環境規劃意識。例如：日本有	研究第一章已敘明，本案係依據本所 100-103 年度「智慧化居住空間產業發展推廣計畫」辦理之研究，研究重點係在建築師及主管建築機關可操作範圍內，探討

發言要點	回應
<p>相關文獻探討採大面積集中式空地，搭配高層集合住宅之建築型態，結果不利5歲以下幼兒利用空地，亦不利於凝聚共識。</p> <p>4. 建議先釐清使用者為何？如設備專業、建築師再來研擬設備空間設計準則。</p>	<p>智慧建築安全防範設備之應用，供建築師發展建築設備空間設計方案及主管建築機關等使用者參考，因此，設定之成果使用端並非設備專業從業人員，而以都市計畫或高層建築規劃設計手法，或是利用犯罪心理學進行犯罪預防等研究方向，不在本案探討範圍。</p>
<p>5. 準則架構採用發生前、中、後之順序，並配合建築手法、被動式機械手法、主動式機械手法分析整理，已經相當清楚完整，但是從空間區位來檢索，例如：地下停車場、樓梯間、出入口、屋頂平台等，可較有利於建築設計者應用參考。</p>	<p>第三章智慧建築手法彙整表業依審查意見修正。</p>
<p>6. 目前進度在文獻收集第二章，未見初步研究成果或初步草案，未來進度要加快。</p>	<p>業已補充研究成果。</p>
<p>7. 安全性可增加性能等級設定、重要性排序。</p>	<p>於第1、5章說明本研究著重提供建築師「建構安全無慮環境」之設計思考架構，安全性能等級不在本研究探討範圍。</p>
<p>8. 可考慮如何與貴所建築防火等相關研究成果進行水平</p>	<p>建築防火不在本研究探討範圍，未來若有水平整合研究再予</p>

發言要點	回應
整合。	以納入。

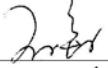
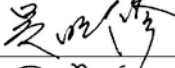
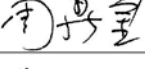
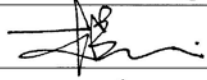
八、結論：

1. 與會專家學者意見，請各案主持人參採辦理或妥予回應，納入最後之成果報告；有關期中與期末報告審查會議之審查意見，應以回應表之方式逐項回覆，並詳實呈現於期末成果報告之附錄中。
2. 本次 3 案之期中報告審查原則通過，請掌握後續之研究期程，確實完成各項計畫之執行，充實研究內容，完成成果報告書之撰寫與印製。

九、散會：(上午 11 時 20 分)

內政部建築研究所

召開本所 100 年度自行研究案「智慧建築安全防範設備空間設計準則之研究」、「高層集合住宅外牆磁磚剝落原因與解決對策探討(2/2)－水泥砂漿硬底壓貼工法之實驗研究」及「紅外線熱影像法於外牆磁磚表面溫度檢測特性之實驗研究」等 3 案期中審查會議簽到簿

時 間：100 年 8 月 12 日(星期五) 上午 9 時 30 分正			
地 點：大坪林聯合開發大樓第三會議室(新北市新店區北新路 3 段 200 號 15 樓)			
主 席：林組長建宏 林建宏		記 錄：張怡文	
出席人員	簽 到 處	代 理 人	
		職 稱	簽 到 處
石建築師正義			
吳建築師明修			
周教授鼎金			
林教授世堂	表面意見		
高教授健章	請假		
陳建築師昶良	請假		
楊教授詩弘			
謝建築師園	出國		
內政部營建署			
臺北市政府建築管理處			
中華民國全國建築師公會	曹昌勝		
中華民國電機技師公會全國聯合會	李華輝		

[怡文開 1000808S]

附錄五 期末審查意見回應表

內政部建築研究所 100 年度自行研究案「智慧建築安全防範設備空間設計準則之研究」、「高層集合住宅外牆磁磚剝落原因與解決對策探討（2/2）—水泥砂漿硬底壓貼工法之實驗研究」及「紅外線熱影像法於外牆磁磚表面溫度檢測特性之實驗研究」等 3 案期末審查會議

一、時 間：100 年 11 月 25 日（星期五）上午 9 時 30 分

二、地 點：大坪林聯合開發大樓第 3 會議室

三、主持人：林組長建宏 記錄：張怡文、盧珽瑞、林谷陶

四、出席人員：（詳出席簽到單）

五、主席致詞：（略）

六、報告人簡報：（略）

七、綜合討論：「智慧建築安全防範設備空間設計準則之研究」案

發言要點	回應
本研究案內容與架構已甄完善，惟 76 頁表 3.2 智慧建築手法彙整內容建議「建築空間別」增加「高層建築設備層」，以及針對高齡化社會來臨，建議增加同一樓層鄰房住戶間之緊急求救鈴。	已增加高層建築設備層項目；課予公寓大廈住戶之間相互救助義務較為複雜，本研究暫不討論。
對於停車場所、建築物停車空間之安全防範建議增加攝影監控，以強化嚇阻效果。	業依審查委員意見修正智慧建築手法彙整表。
計畫內容係以人身安全（及居家安全、防盜、防爆）為主（如表 1.3 項次二所示），另外表 2.1 及	探討內容係依期初審查意見辦理，將研究範圍界定為先將建築物設計為安全空間，再以安全設

發言要點	回應
圖 2.5 等應為研究探討之對象，但不宜離開「設備」之主題，第三章第三節已非設備之範疇。	備輔助。
表 3.2 安全度及脆弱度皆有，不宜如此表達。又 2.8 之建築物安全分級宜先訂定，才能將各脆弱度（或安全度）之項次個別指定之，此因不可能將公寓大廈與重要機構之建築物以相同項次進行評估。	已修正相關用語。
內容及文字圖表仍須大幅修正，英文字宜譯出。	已修正。
內容涵蓋人員生命及財產安全之維護，並非僅人身安全。	已修正相關用語。
資料蒐集完備。	感謝審查委員肯定。
設計準則之落實宜量化，如：監測照度，使設計者能有所本。建議準則各項採計分，然後整體安全需達一定分數後再予以審查。第二章表 2.4 中「設備監控」之評估項目 1、3、9 對於照明是否夠亮，建議於表中提供 CNS 照度建議值供參考，避免因個人主觀而致爭議。 第三章表 3.2 中項次 1.12 建議適度說明作法及數據，比如提供進	本研究目的已敘明著重提供一個簡單思考架構，協助建築師有系統地從安全觀點：評估基地潛力與限制條件、解釋設計方案優劣、反省錯誤、累積專業經驗，將建築物個案之安全防範元素，作具有創造力之組合，妥適應智慧建築安全防範設備，兼測照度是屬於細部設計層次問題，不在本研究探討範圍。

發言要點	回應
<p>出入口及停車空間之 CNS 照度要求，及閉路電視監視範圍應提供監視設備所需照度。</p> <p>第三章表 3.2 中項次 11.1 建議增加細部建議，如儲存之影像解析度及每秒張數等。</p>	
本研究除達成智慧化居住空間產業發展推廣目的外，能從回應性別平等政策綱領—人身安全維護課題進行實質討論值得鼓勵。	感謝審查委員肯定。
本研究蒐集國內外智慧化安全防範案例，並由都市空間及建築角度探討智慧安全防範設備之重要性，其案例資料非常值得參考。	感謝審查委員肯定。
研究成果「智慧建築安全防範設備空間設計準則」建議提供智慧建築解說與評估手冊中安全防災指標之參考，並可提供智慧建築設計技術規範之應用。	研究成果可提供有關機關訂定規範參考。
「安全監控室」名詞與現行法規「防災中心」或智慧建築中之「中央監控室」是否為同一空間？	建築技術規則設計施工編地 12 章高層建築物之「防災中心」主要係因應火災而設置，與本研究所稱安全監控室並不相同，
目前內容完成空間設計準則須儘速完成第四章之應用示範案例，以實質提供建築或都市空間設計	感謝審查委員肯定。

發言要點	回應
者參考。	
設計準則之用詞可再研究是否採用手冊等其他更為妥適之名詞。	本研究成果主要供建築師使用，參考國內、外建築師實務用語以設計準則較為普及易懂。
第二章表 3.2 中分項指標「社區管理與巡守隊」之評估標準，建議將定時定點巡邏改為定點巡邏，實務上不定時巡邏比定時巡邏有嚇阻效果。	修正該用語並非本研究探討範圍，建議將另轉知有關計畫主持人參考。

八、結論：

1. 與會專家學者意見，請各案主持人參採辦理或妥予回應，納入最後之成果報告；有關期中與期末報告審查會議之審查意見，應逐項回覆並詳實記錄，附於期末成果報告附錄中。
2. 本次 3 案之期末報告審查通過，請掌握最後研究期程，確實完成研究內容，修正並完成成果報告書之撰寫與印製。

九、散會：(上午 11 時 50 分)

內政部建築研究所

召開本所 100 年度自行研究案「智慧建築安全防範設備空間設計準則之研究」、「高層集合住宅外牆磁磚剝落原因與解決對策探討(2/2)－水泥砂漿硬底壓貼工法之實驗研究」及「紅外線熱影像法於外牆磁磚表面溫度檢測特性之實驗研究」等 3 案期末審查會議簽到簿

時 間：100 年 11 月 25 日(星期五)上午 9 時 30 分			
地 點：大坪林聯合開發大樓第 3 會議室(新北市新店區北新路 3 段 200 號 15 樓)			
主 席：林組長建宏 林建宏 記 錄：張怡文 盧瑞松 徐國			
出席人員	簽 到 處	代 理 人	
		職 稱	簽 到 處
石建築師正義	200		
邱顧問昌平	邱昌平		
周教授鼎金	請假		
林教授世堂	林世堂		
高教授健章	請假		
陳建築師祖良	請假		
溫教授琇玲	溫琇玲		
謝建築師園	請假		
內政部營建署	請假		
臺北市建築管理處	請假		
中華民國全國建築師公會	請假		

谷陶

[開 1000712S]

中華民國電機技師公會 全國聯合會	吳建興		
中華民國建築開發商業 同業公會全國聯合會			
中華民國室內設計裝修商 業同業公會全國聯合會			
林研究員谷陶	林谷陶		
盧副研究員珽瑞	盧珽瑞		
張助理研究員怡文	張怡文		
相關人員			

[開 1000712S]

陶

參考書目

1. 內政部建築研究所，智慧化居住空間產業發展推廣計畫，民國 99 年。
2. 內政部性別平等政策綱領（草案），民國 100 年 6 月。
3. 建築技術規則
4. 內政部建築研究所，智慧建築解說與評估手冊 2011 年版，民國 100 年。
5. 內政部建築研究所，智慧建築解說與評估手冊 2003 年版，民國 92 年 12 月。
6. 內政部警政署刑事警察局全球資訊網，
http://www.cib.gov.tw/crime/Crime_Book.aspx，犯罪預防寶典。
7. 內政部全球資訊網-內政記事本：全國婦女國是會議」圓滿閉幕
http://www.moi.gov.tw/pda/pda_moi_note/moi_note_detail.aspx?sn=71&pages=4
8. 謝園，校園人身安全與空間設計--以國外住宅社區研究為例，第六屆全國婦女國是會議論文，民國 90 年。
9. 靳燕玲，集合住宅社區共用空間安全防範設施設置方法研究，內政部建築研究所自辦研究，民國 95 年。
10. 許瑞生，「防範住宅入侵之設計規範」，國立成功大學建築研究所碩士學位論文，民國 83 年。
11. 郭晉勳，「創造安全的城市--經由環境設計預防犯罪」，國立台北大學都市計劃研究所碩士學位論文，民國 90 年。
12. 宋仲儒，「犯罪決意考量因素與監視錄影系統之關聯性研究」，中央警察大學刑事警察研究所碩士學位論文，民國 95 年。

13. 許錦標，樓宇智能化技術第3版，機械工業出版社，民國99年。
14. 中國建築學會建築電氣分會，智能建築新技術，中國建築工業出版社，民國99年。
15. 王娜等，智能建築概論，中國建築工業出版社，民國99年。
16. 賴銘昌，「空間型構與汽車竊盜之關聯性研究—以台灣某都市為例」，逢甲大學建築及都市計畫研究所碩士學位論文，民國94年。
17. 盧建霖，「公有地下停車場之環境犯罪預防設計—以台北市為例」，國立台北大學犯罪學研究所碩士學位論文，民國98年。
18. 許錦標，樓宇智能化技術第3版，機械工業出版社，民國99年。
19. 莊嘉文，建築設備概論，詹式書局，民國73年。
20. 吳讓治，建築設備概論序，詹式書局，民國73年。
21. 周鼎金，建築設備，茂榮書局，民國86年。
22. 經濟部，i236智慧生活科技運用計畫網站，
<http://www.i236.org.tw/>
23. 2011全球智慧城市高峰論壇，智慧科技服務模組於未來城市之應用—以i236計畫與源雄智慧社區為例簡報資料，民國100年。
24. Oscar, N., Create Defensible Space, U.S. Department of Housing and Urban Development Office of Policy Development and Research, 1996
25. Hillier, B. Can streets be made safe? Urban Design International 9, 31-45, 2004
26. Barbara A. Nadel, Building Security: Handbook for Architectural Planning and Design, McGraw-Hill Professional; 1 edition, 2004

27. Shengwei Wang , Intelligent Buildings and Building Automation , Spon Press; 1 edition , 2009
28. Andrew Harrison , Intelligent Buildings in South East Asia , Taylor & Francis; First edition , 1998
29. Walter T. Grondzik , Mechanical and Electrical Equipment for Buildings , Wiley; 11 edition , 2011
30. The American Institute of Architects , Security Planning and Design: A Guide for Architects and Building Design Professionals , Wiley; 1 edition , 2003
31. Vaughn Bradshaw , The Building Environment: Active and Passive Control Systems , Wiley; 3 edition , 2006
32. Linda O'Shea , Design and Security in the Built Environment
33. James M Sinopoli , Smart Buildings Systems for Architects, Owners and Builders, Butterworth-Heinemann; 1 edition ,2009
34. Federal Emergency Management Agency (U.S.) , Incremental Protection for Existing Commercial Buildings From Terrorist Attack: Providng Protection to People and Buildings: Providing Protection to People and Buildings , 2008
35. Federal Emergency Management Agency (U.S.) , Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings , 2003
36. Guidelines for Enhancing Building Security in Singapore , Homefront Security Division-Ministry of Home Affairs , 2010
37. Enhancing Building Security—The Fight Against Terror Singapore's National Security Strategy , Homefront Security Division-Ministry of Home Affairs , 2004

38. D. Clements-Croome , Intelligent Buildings: Design
Management and Operation , Thomas Telford Publishing, 2004