GUIDELINES FOR ENHANCING BUILDING SECURITY IN SINGAPORE

The Guidelines for Enhancing Building Security in Singapore (GEBSS)
has been prepared by

Joint Operations Group - Ministry of Home Affairs
in consultation with:

Building and Construction Authority;

Internal Security Department;

Institute of Safety and Security Studies;

Singapore Civil Defence Force;

Singapore Police Force;

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.

TABLE OF CONTENTS

1

INTRODUCTION TO BUILDING SECURITY

THREAT OF TERRORISM

The cost to orchestrate an act of terrorism compared to the potential costs as a result of a successful terror attack is insignificant in comparison. The terrorist attacks in the United States on 11 September, 2001 ("9/11") cost the terrorists about US$500,000 to stage, claimed 3,000 lives and the total losses of life and property cost insurance companies approximately US$40 billion. This direct cost pales in comparison to the indirect costs. Shopping centres and restaurants across the country were closed for at least 24 hours, high-risk office buildings (such as the former Sears Tower in Chicago) were evacuated; planes were grounded; and the stock market ceased trading for four consecutive days. The effects were not only felt in New York. The Florida tourist industry was also badly affected where the total tourism activity had been reduced by one-third, or about US$20m per day. More recently, the March 2015 attack by 2 brothers during the Boston Marathon using 2 pressure cooker nail bombs inflicted an estimated US$333 million in damages from economic lost, medical costs and infrastructure damages.

Other than the loss of human lives and injuries suffered, there are also business costs that can come in the form of rebuilding costs, insurance pay-outs, shattered investor confidence, psychological damage to the affected region, and reputational costs. These are just a small sample of the many costs that businesses and governments have to deal with in the wake of a terrorist bomb attack on or in the vicinity of their establishment.

Closer to home, the Oct 2002 Bali Bombing, which cost the terrorists approximately US$20,000 to stage, claimed the lives of around 200 innocent people and devastated Indonesia's US$6 billion tourism industry. The Indonesian stock market crashed and the Bali tourist economy, which contributes about 5% of the country's GDP, came to a halt, contracting by an estimated 36% in nominal terms over a one year period. Overall, the attack resulted in a 2% drop in Indonesian GDP for 2002.

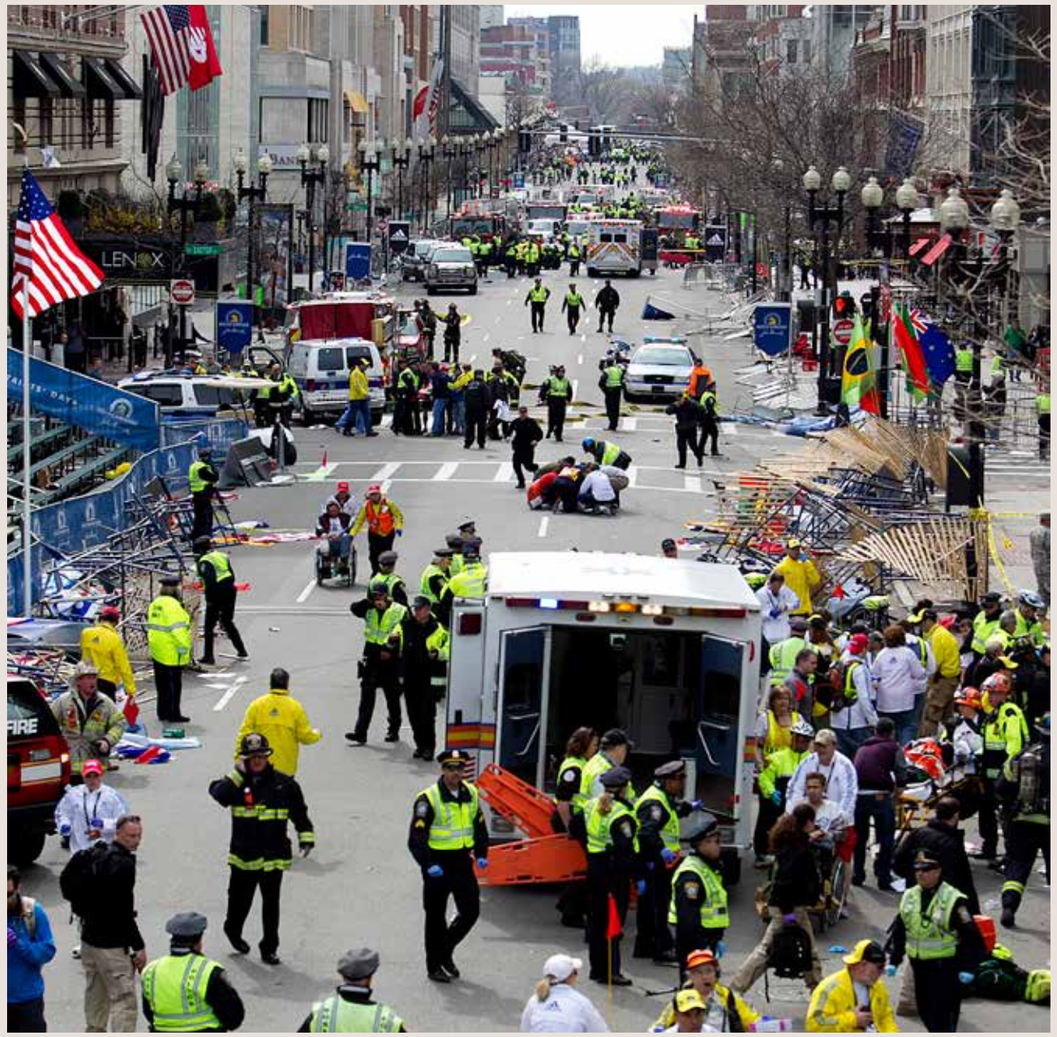
Attacks in the region have shown that terrorists continue to actively pursue their terror campaigns, which very often target hotels, resorts or popular shopping destinations. The attack on the Islamabad Marriott Hotel (Sep 2008), co-ordinated attacks in Mumbai which included two hotels, The Taj Mahal Palace & Tower and The Oberoi Trident (Nov 2008), the bombings in Jakarta's JW Marriott and Ritz Carlton hotels (Jul 2009), the Erawan Shrine bomb attack in Bangkok's city centre (Aug 2015) and the gun and bomb attacks in central Jakarta near Sarinah Plaza (Jan 2016) are a few such examples.

BOSTON MARATHON BOMBING

COST OF BOMBS:
UNDER US$100 PER BOMB

COST OF MEDICAL CARE:
MORE THAN US$9M

COST TO LOCAL ECONOMY:
AT LEAST US$333M



Top photo:
First responders tend to the wounded where two explosions occurred along the final stretch of the Boston Marathon on Boylston Street in Boston, Massachusetts, U.S., on Monday, April 15, 2013.

THREAT OF TERRORISM IN SINGAPORE

The emergence of the Islamic State in Iraq and Syria has changed the global terrorism landscape. Instead of of large-scale terrorist acts involving groups of attackers planning bomb attacks characteristic of other terrorist organisations such as Al-Qaeda, recent ISIS-linked attacks such as those in Paris, San Bernardino and Jakarta showed that the attackers took hostages not to negotiate but to inflict maximum casualties using readily available weapons and relatively smaller quantity of explosives.

With the proliferation of pro-ISIS and Jemaah Islamiyah (JI) groups in Indonesia and the arrests in Malaysia of more than 100 persons suspected to be linked to ISIS, the terrorism threat to Singapore remains the highest in years.. The unravelling and arrest of a terror cell consisting of 27 radicalised Bangladeshi foreign workers in Jan 2016, belonging to the Islamic State of Bangladesh supporting the armed jihad ideology of terrorist groups such as Al-Qaeda and ISIS, as well as the arrest of five domestic helpers radicalised through social media, shows that there can be individuals and groups planning terrorist attacks right within our midst. Given this persistent and present threat of terrorism, Singapore must be more vigilant in our preparation against terrorism. In particular, the business risks from the threat of terrorism provide a compelling case for building owners and occupiers to give special attention to the security of their premises.

Right photo:
Medics move a wounded man near the Boulevard des Filles-du-Calvaire after an attack November 13, 2013 in Paris, France.

OVERVIEW OF THE GUIDELINES

The GEBSS aims to provide a menu of good security practices and considerations to help building owners incorporate pragmatic security procedures, physical protection concepts and security technology into their building's security plans. As the GEBSS is intended to be used for all types of premises, with varying sizes and given that the risks associated with the premise varies considerably, the intention is not to provide recommendations, but provide information that should be considered when planning for the security of a building. Building owners and designers will have to choose the appropriate measures corresponding to the risks and threats that are applicable to their premises. Security should be designed in consideration with other design constraints, including accessibility, costs, and aesthetics etc. The intent is to ensure that the counter-measures are not obtrusive and congruent with the overall design of the building, with integrated solutions that serve both functional and security purposes. The GEBSS will serve as a common frame of reference and ensure a minimum level of acceptable security standards in the industry. For example, the guidelines will state internationally recognised standards where relevant (e.g. for vehicle barriers: IWA 14-1 2013, PAS68 etc.) that manufacturers should adopt if they wish for their equipment to be used in Singapore. Building owners and consultants will also be able to use these standards as a basis to determine the technical requirements of the security measures to put in place.

"It is no longer a question of whether an attack will take place, but really, when is an attack going to take place in Singapore and we have to be prepared for that."

Minister of Home Affairs
K. Shanmugam

Left photo:
Medics move a wounded man near the Boulevard des Filles-du-Calvaire after an attack November 13, 2013 in Paris, France.

The intent for the GEBSS is not to assume or recommend that maximum protection is required as a standard but suggests design considerations and ways of preparing the infrastructure for later implementation of higher levels of protection. If project constraints prohibit the full implementation of the relevant guidelines, it is up to the project developer or user of this guide to decide on the extent to which the various protective elements will be implemented, based on the location of the potential threats and subsequent analysis.

Top photo:
A wrecked car sits in the intersection of 45th and Broadway in Times Square, May 18, 2017 in New York City. According to reports there were multiple injuries and one fatality after the car plowed into a crowd of people.

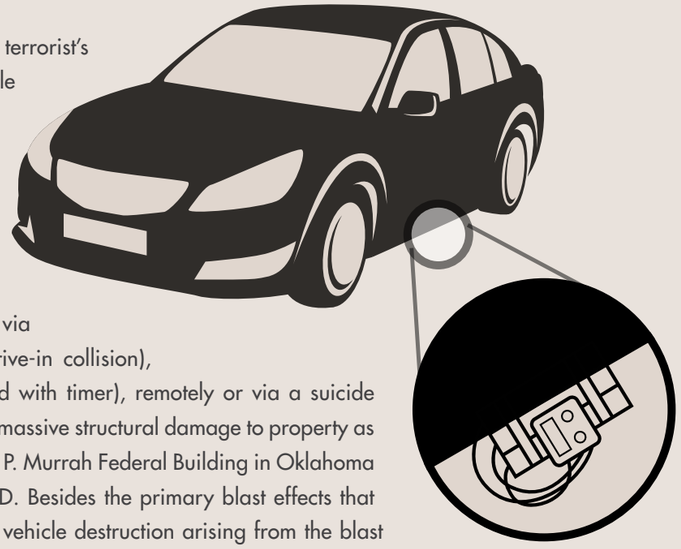
ASSUMPTION

The philosophy introduced in these guidelines is that appropriate protection can be provided for new development projects either at a reasonable cost or at no additional cost. Building designs that employ factors to eliminate or limit the possibility of an attack help reduce the need to employ hardening measures across the entire structure and/or in specific vulnerable areas.

POSSIBLE THREATS TO BUILDINGS

The threats discussed in this section are derived from the terrorists' known capability and modus operandi, and used to determine the possible threat scenarios that are likely to be executed at a building's various locations that are assessed to be vulnerable.

VEHICLE BORNE IMPROVISED EXPLOSIVE DEVICES (VBIED)

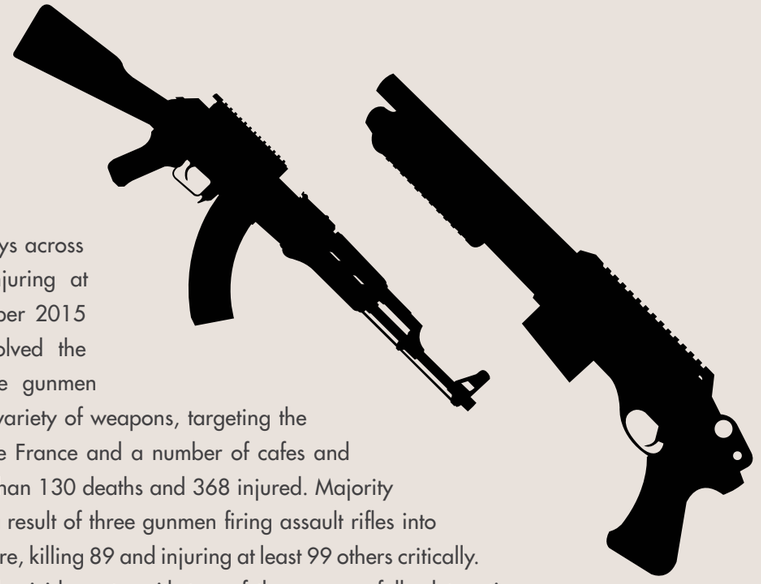


One of the most effective weapons in a terrorist's arsenal, VBIEDS involves using a vehicle as the vessel to conceal an explosive device, and can include a variety of vehicles – e.g. cars, vans/ pick-ups, buses, lorries, delivery trucks, with the ability to carry larger amounts of explosives that could cause greater damage. VBIEDs can be detonated via a ramming detonation attack (e.g. drive-in collision), timer-activated detonation (e.g. parked with timer), remotely or via a suicide operation, and are capable of causing massive structural damage to property as seen in the terrorist attack on the Alfred P. Murrah Federal Building in Oklahoma City (1995), which used a parked VBIED. Besides the primary blast effects that can cause massive structural damage, vehicle destruction arising from the blast can result in additional shrapnel and fuel causes the vehicle to turn into an incendiary device.

The stand-off distance, which is the distance between the VBIED and the nearest façade of the building, is the most important factor when establishing the extent of damage that a building can suffer due to a VBIED. Any extra stand-off will have significant influence on the ability to mitigate the VBIED threat.

Areas to consider protecting against VBIED threats would be the perimeter protection, the adjacent areas, as well as vehicle access control into and around the building premise.

ATTACK BY ARMED ASSAILANTS



Coming to prominence in the 2011 Mumbai attacks, 10 gunmen carried out a series of 12 coordinated armed assaults lasting four days across Mumbai, killing 164 and injuring at least 308 others. The November 2015 armed assaults in Paris involved the coordination of at least nine gunmen and suicide bombers using a variety of weapons, targeting the Bataclan Theatre, the Stade de France and a number of cafes and restaurants, resulting in more than 130 deaths and 368 injured. Majority of the casualties occurred as a result of three gunmen firing assault rifles into the crowd at the Bataclan Theatre, killing 89 and injuring at least 99 others critically. All three gunmen had donned suicide vests, with two of them successfully detonating their vests when confronted by the police towards the end of a two and a half hour siege.

Armed assaults involving a number of assailants armed with weapons such as submachine guns, small arms and small charges (e.g. IEDs, grenades) are becoming the choice modus operandi as seen in recent terrorists attacks. The key characteristic of this form of threat is that the main weapon used is guns instead of IEDs. Guns are relatively easier to obtain compared to bomb-making, requires minimal training and is an efficient way to cause mass casualties, especially in confined places.

Possible measures would be the surveillance of the premises for suspicious persons, armed security patrols around and within the premise, access control measures and security screening. A key capability to have against armed assailant attacks for a building would the ability to secure key parts of the building to secure and confine the gunmen while allowing for the people to escape. Escape planning and briefings should be promulgated to emergency services, authorities, staff and occupants of the facility, and the plans should be tested at least annually.

CHEMICAL AND BIOLOGICAL AGENTS

With the materials harder to obtain and complex to execute effectively, there have been relatively few chemical attacks in comparison to other threats. The most notable was the sarin gas attack on the Tokyo subway (1995), which killed 12 people another notable example was the anthrax letters incident in the United States which killed five people.

The impact of any CBR attack depends on the success of the chosen dissemination method and the weather conditions at the time of the attack, as well as the crowd within the area of impact. The occurrence of an incident may not be evident immediately, particularly with an attack involving radiological or biological materials. First indicators may be the sudden appearance of powders, liquids or strange smells within the building, with or without an immediate effect on people.

Against chemical attacks include access control measures and security screening for entry into the building, as well as surveillance and security patrols around and within the premise. Air intake and outlet vents should be located at an adequate height and secured, and access to water tanks and key utilities should be restricted. As the CBR attack might be via mails and parcels, the staff should receive proper training to identify possible indicators that a delivered item may be of concern, and the steps to take upon receipt of such an item.

UNAUTHORISED ENTRY

The failure to secure a building against unauthorised entry, typically via forced entry, can expose the building to a wide variety of threats and risks, varying from theft, to the destruction of physical assets/information to the worst case scenario of a successful terrorist attack within the building. Poorly designed access control measures make it that much easier for attacks to carry out attacks. One of the key objectives of the layered protection concept (to be discussed in Chapter 3), is the implementation of comprehensive security measures integrating physical, technological, and operational measures to minimise the risk of unauthorised entry into the building.

IMPROVISED EXPLOSIVE DEVICE

An IED is a non-military bomb or "homemade" bomb that is made and concealed to avoid detection, e.g. a haversack, luggage, parcel, mail, suicide vest, etc. IEDs can come in many forms, such as pipe bombs, shoe bombs and typically contain smaller amounts of explosives. However, they are an effective mode of attack as they can be easily concealed. If Strategically placed beside critical structural elements, the consequences of such IEDs can be catastrophic. The pressure cooker bombs used in the Boston Marathon bombing on 15 April 2013 is an example of an IED. Packed with nails, ball bearings and black powder inside, the explosions killed 3 civilians, and injured an estimated 264 persons, with at least 14 maimed. Similar modes of attack were noted in the 3 coordinated bombings in Belgium in March 2016.

Possible measures against IED threats would be the surveillance of the premises, security patrols around and within the premises, preventing unauthorised entry through access control measures and security screening. Glazing protection measures and hardening measures will provide additional protection to the occupants to minimise casualties arising from fragmentation and progressive collapse.

FACTORING SECURITY EARLY IN THE BUILDING DESIGN

ACHIEVING AESTHETICS

Building security measures must be balanced with the need to maintain the aesthetics of a building. However, many solutions available today meet the objective of raising the level of security yet blend in well into the architectural design.

The best time to assimilate elements of building security will be during the planning and design stages of the development life cycle. Indeed, effective building security design can be factored in as early as the conceptual design stage. This will not be at the expense of the architectural vision envisaged by the building owners. It is possible to design-out security risks while still preserving the essence of the design.

MAINTAINING BUILDING FUNCTIONALITY

Building functionality can be maintained if security design is taken into account from the early stages of the building development life cycle. For example, the failure of a main transfer beam led to the progressive collapse of a substantial portion of the Alfred P. Murrah Federal Building in Oklahoma City. In fact, most of the structural damage, and a vast majority of the fatalities were caused by this progressive collapse, and not by the direct effect of the bomb blast.

MAINTAINING BUILDING FUNCTIONALITY (CONTINUED)

According to testimony by an expert witness to the US Congressional committee investigating the attack, progressive collapse could have been avoided through the installation of additional strengthening structures. In fact, additional strengthening structures would not even have to be installed, if building designers had taken this propensity to progressively collapse into account early on.

MANAGING COSTS

Security designs, if factored in early in the design phase of a new development, can result in minimal cost implications while at the same time, increase the inherent protection level provided to the building. This can be met through prudent master planning, and through following good design and construction practices which typically result in minimal constraints on the design and architecture. By factoring in elements of protective security early in the design stage, the developer will be able to avoid costly retrofitting which may be required in an elevated threat environment. This will help to minimise the impact of additional security measures, and thus control costs more effectively. Hence, implementing these guidelines will have positive effects on the building's day-to-day security operation and its cost.

WHO SHOULD READ THE GUIDELINES

architects, structural engineers, **urban construction developers**, construction project managers, **security consultants**, security system designers **and others**

The GEBSS describe concepts and provide detailed information for security-oriented building design. The targeted audiences include, but are not limited to, building owners, architects, structural engineers, urban construction developers, construction project managers, security consultants, security system designers and others engaged in the design and construction of buildings.

General information is included to provide senior managerial staff and decision makers with an understanding of security concepts and to help emphasise the importance of physical design in security. At the same time, it also provides developers, engineers and architects with a resource for determining security-oriented design approaches to protect buildings against terrorist-related incidents.

The security principles and considerations highlighted in this document are applicable to any type of civilian building, especially those serving large numbers of people on a daily basis such as commercial buildings and shopping complexes. These can either be new buildings or existing buildings undergoing repairs, alterations or additions (whether carried out within or outside the building).

NEED FOR SECURITY, BLAST & PROTECTIVE DESIGN CONSULTANTS

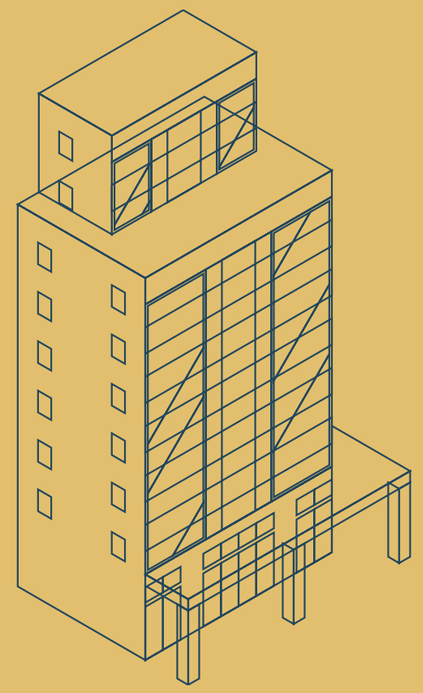
Building owners and developers should decide on the extent of security provisions that they would like to incorporate into their building design. In this regard, building owners and developers are encouraged to engage professional security and protective design/blast consultant(s), as early as the project concept stage to conduct a risk assessment of the building, and to recommend appropriate security measures. This is especially if the security needs of the building are complex.

FEEDBACK & QUERIES

Building owners who are members of the Safety and Security Watch Group (SSWG) may approach their respective SSWG Community Liaison Officer for security advice. Users of the GEBSS can also e-mail feedback and queries to MHA at

MHA_Guidelines_BuildingSecurity@MHA.gov.sg

2



BUILDING PLANNING & DESIGN CONSIDERATIONS

INTRODUCTION

Security considerations are most effectively incorporated during the conceptualization and planning stages of a facility's development. Key considerations include selection of site and understanding the environment and terrain; positioning and orientation of the buildings within the development; landscaping to create security buffer and provision of car parks and internal access roads within the development. Further considerations include the structural scheme, curtain walls and facades, locations of car parks, locations of critical assets and areas of mass congregation.

Incorporating physical security concepts into the initial architectural design of a project is the most efficient and cost-effective way to achieve the required security level. Apart from the financial benefits of early planning, by considering the security aspects from the onset enables architects and planners to work with security consultants to blend the required protection elements into the design of the facility to satisfy both security and aesthetic requirements.

Incorporating physical security concepts into the initial architectural design of a project is the most efficient and cost- effective way to achieve the required security level

For building owners that assess their facility to be at a greater risk of attack (because of the nature of the business conducted or location of the premise), it would be necessary to ensure that your building information is not available on public domain such as the Internet. Building information includes architectural layout, structural plans, location of critical assets, tenants or targets that may be attractive to adversaries.

GENERAL ARCHITECTURAL CONSIDERATIONS

Security considerations should be deliberated during the initial stages of a development project so that cost effective protective solutions can be incorporated into the structural, layout and system designs, thereby reducing the need for hardening measures.

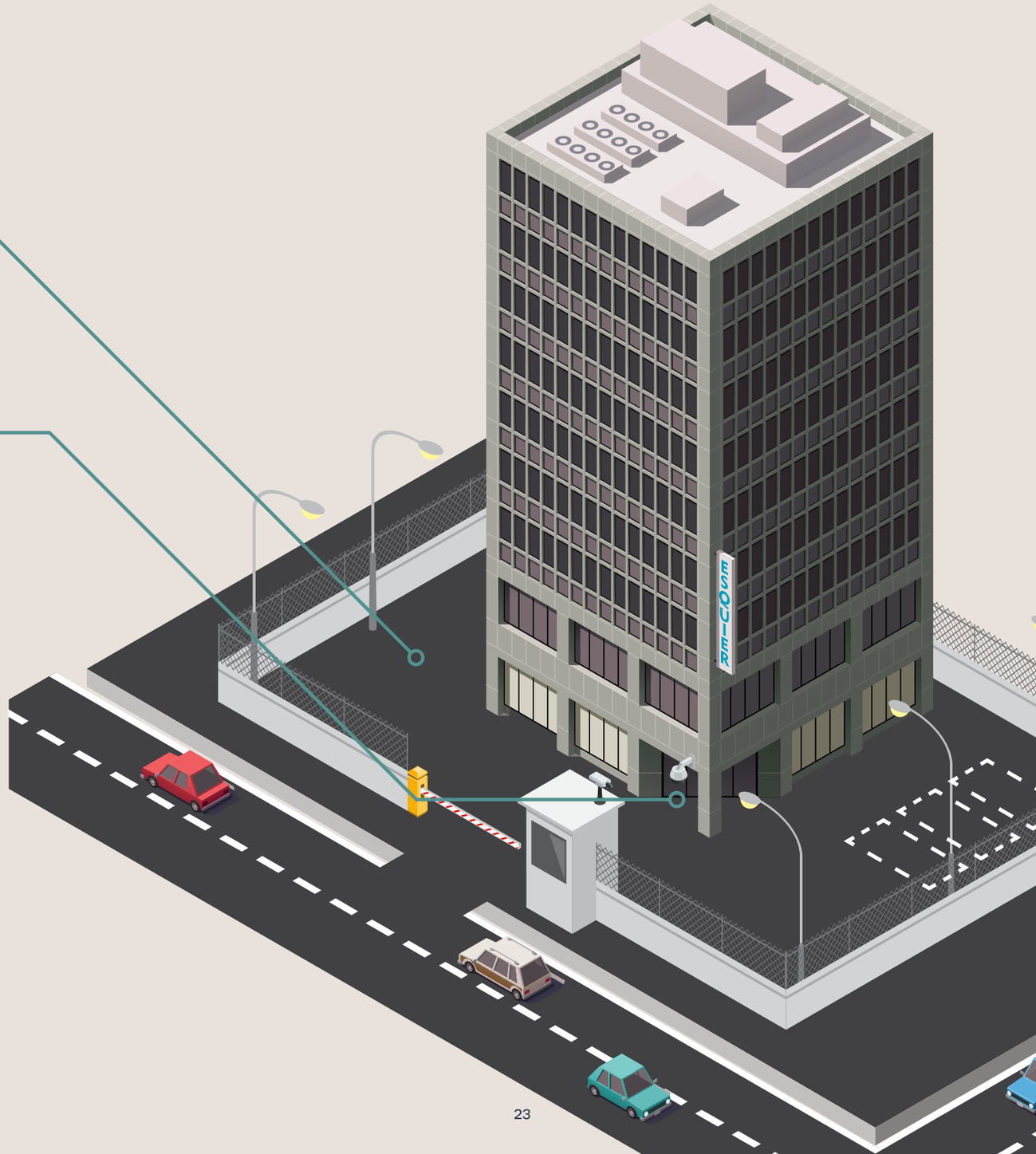
CREATING STAND-OFF DISTANCE

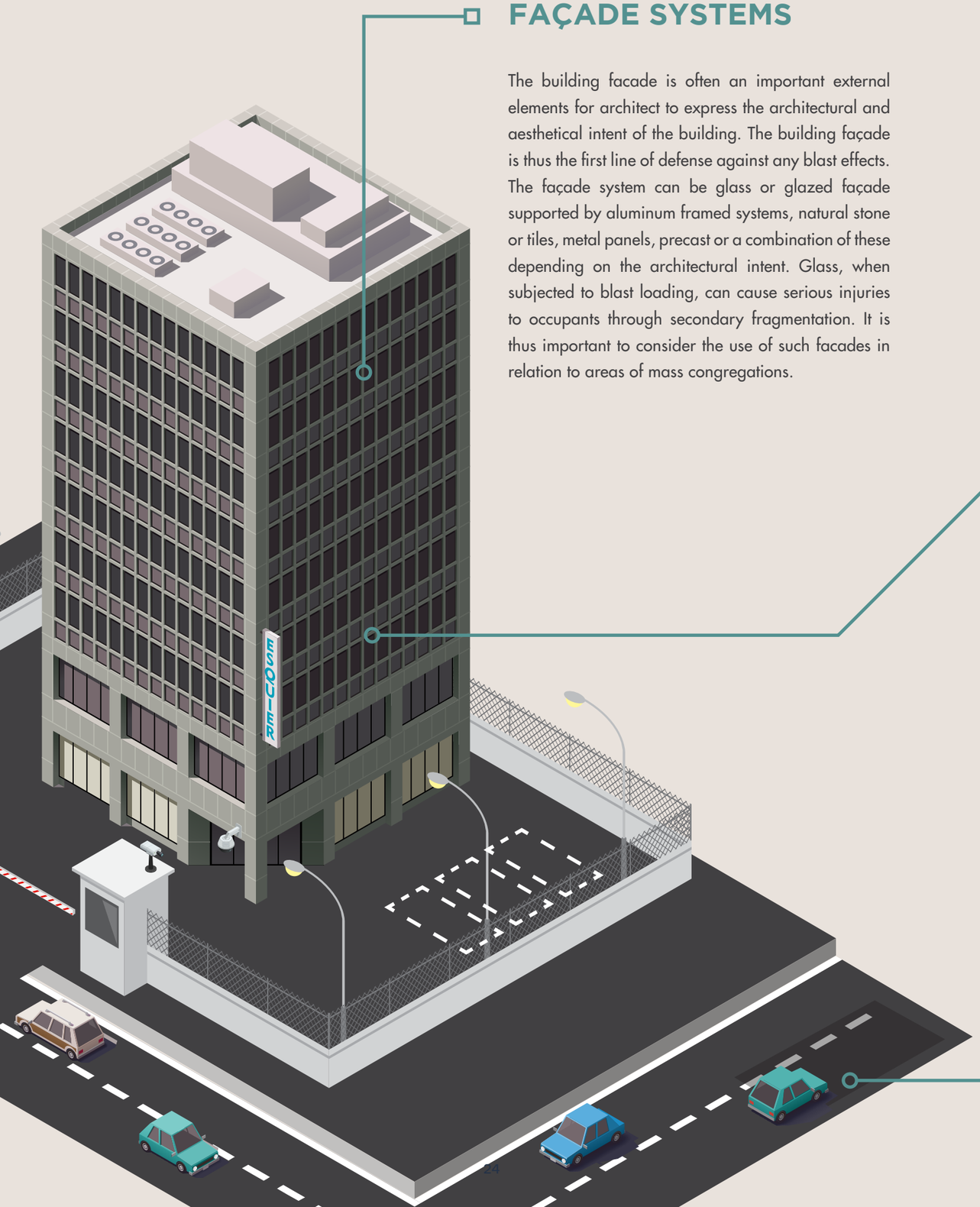
Stand-off distance is defined as the distance between the detonation point and the targeted building. Stand-off distance is the single most important factor when mitigating the effects of a vehicle-borne IED. Increasing the stand-off distance would drastically reduce the blast effects, thereby saving significant resources to harden the structure. Key considerations are to site drop-off points, car parks, loading/unloading bay away from the building. If this is not possible, such facilities should be sited away from the footprint of the tower blocks.

However, given the scarcity of land in Singapore and the need to optimise land use, large stand-off distance may not be feasible. In such instances, area of mass congregation should be located away from glass façade and critical assets (identified by building owners and stakeholders) moved towards the centre of the building.

BUILDING ORIENTATION

Positioning of the tower blocks should be considered carefully as the orientation of the building may influence its vulnerability against threats such as firearms that require direct line-of-sight to be effective. By taking advantage of the horizontal and vertical angles and obscuring the lines of sight from a potential threat, the requirements for window protection against firearms may be reduced significantly. Locating critical assets (identified by building owners and stakeholders) as high as possible and away from public areas may reduce their vulnerabilities against explosive threats.





FAÇADE SYSTEMS

The building facade is often an important external elements for architect to express the architectural and aesthetical intent of the building. The building façade is thus the first line of defense against any blast effects. The façade system can be glass or glazed façade supported by aluminum framed systems, natural stone or tiles, metal panels, precast or a combination of these depending on the architectural intent. Glass, when subjected to blast loading, can cause serious injuries to occupants through secondary fragmentation. It is thus important to consider the use of such facades in relation to areas of mass congregations.

AREA OF MASS CONGREGATION

Some facilities are characterised by the presence of large crowds at specific areas within the building. These areas of mass congregation are considered highly attractive for terrorists and therefore should be given special consideration during the design stage. Areas of mass congregation should be housed away from glass facades, main entrances or lower levels, where there could be direct impact from possible threats.

CRITICAL ASSETS

Critical assets are defined as facilities, systems or equipment which, if destroyed, degraded or rendered unavailable, will affect the operation of the organisation or business, for example Security Control Room, Operations Command Centre, Building Maintenance Room, Fire Control Room, Data Centre, Server Room.

Assets that are a single point of failure or difficult to replace, and are essential to the operation of the business can also be defined as critical assets. Critical assets should be located away from any road access and or in specially protected areas. Emergency water supply, fire extinguishing systems and pumps and emergency electricity supply must be concealed to prevent sabotaging. Shielding or re-position it away from areas which are open to the public would also help to mitigate the risks.

TRAFFIC FLOWS, ACCESS ROADS & PARKING

Vehicular access control and screening measures must be carefully planned such that it does not excessively impede the movements of vehicles into/out of the premises. A smooth flow of traffic facilitates the conduct of security checks.

A Traffic Impact Assessment could be performed, where it should take into account the vehicle screening requirements such as the number of screening bays, the type of screening measures and the average time taken to screen each vehicle.

At an early stage, efforts should be taken to balance vehicular access control and screening requirements with having an efficient flow of traffic and people. Once the building has been constructed, it is extremely difficult to change the design and allocate space for such requirements. Hence, making sure that physical measures at access points are weaved into the overall traffic management of the premises (i.e. covering access roads, driveway, drop-off points, entrances to the building, and car parks), will help to ensure proper functionality when the site is operational.

The structural framing system and method of construction (cast-in-situ, precast, prestressed, structural steel, etc.) affect the robustness of the building when subjected to blast loading. It has been well documented that cast-in-situ construction provides more robustness as compared to precast and the failure of a prestressed element can serious consequence on the remaining structural elements.

TRANSFER BEAM/ GIRDER

Typically a transfer beam/girder is introduced as part of the structural system when there is a desire to create a column-free space e.g. banquet halls. Transfer beams/girders reduce the number of columns which means that there is less redundancy. Damage or loss of the transfer beam/girder or the columns supporting it may result in progressive collapse. To reduce the vulnerability, it is necessary to span the transfer beam/girder over several supports or to create two-way redundancy thereby allowing alternate load path to take place.

BLAST RESISTANCE

The ability of the structure to resist blast pressure depends on the section properties of the structural elements, including the spans and the connection details. Simple structural scheme consisting of a beam/column/slab system should be adopted where possible..

PROGRESSIVE COLLAPSE MITIGATION

Progressive collapse is defined as the spread of an initial local failure from element to element, eventually resulting in the collapse of an entire structure or a disproportionately large part of it. Progressive collapse occurs when the building sustains the loss of one or more critical columns.

The critical structural elements (e.g. columns and load bearing wall) are essential parts of the facility, which support the building and provide the resilience against progressive collapse, in the event of a blast. Typically, adopting a straightforward approach (direct transfer of load without transfer beam/girder) which involves design of primary structural elements against local failure or provide redundancy of critical elements for the given threat and stand-off distance will normally suffice.

SPECIAL ATTENTION AREAS

Most buildings have rooms or operational areas that require special attention in terms of security. These operational areas are usually required for the important functions of the building such as access control, loading and unloading, parking, building maintenance, mail delivery etc. Addressing the security and protection requirements for these areas is essential for maintaining the security level in the building. Ideally, the protection should be designed in such a way that is integrated with the original operational design of the building. Most of the security changes to these areas will be aimed at the following goals:

Prevention of the entry of unauthorised people or packages.

Protection of the building structure and inhabitants from an event occurring at those locations.

Protection of the areas to prevent a localised attack that may affect the whole building.

The objective of this section is to provide basic protection design guidelines for these areas thereby enabling the architect to make decisions regarding their positioning, design and construction.

UNDERGROUND CAR PARKS

The impact of an explosion in an underground car park or enclosed area has a greater effect on the structure as compared to an open location.

A blast wave in an enclosed space such as an underground car park is subject to multiple reflections, where the resultant blast energy is concentrated in a much smaller space than compared with a free-field explosion in the open air. The lifting forces are therefore expected to be very high and a breach of floors and ceilings must be considered and studied. Where possible, underground car parks should be segregated into public and private car parks, with the public car parks placed outside the main building's footprint to prevent progressive collapse from unscreened Vehicle-Borne Improvised Explosive Devices (VBIEDs).

Car Park Lots

Car park lots next to columns or load-bearing walls or adjoining critical areas such as the Fire Control Centre (FCC), water tanks or other key areas should be avoided. If it is unavoidable, parking should be limited to screened vehicles. In all cases, physical barrier is required to maintain a distance between the vulnerable element and the lots.

Car Parks Ingress and Egress

The ingress to car parks should be designed with check points, which can either be automated or controlled by trained security personnel. The ingress point are the most likely locations for attacks and therefore should be positioned further away from primary structural elements. The ingress point should also be positioned a significant distance away from crowded critical areas.

The ingress and egress points should be equipped with anti-ramming vehicle barriers to an adequate level (see Chapter 4 for details).

BUILDING ENTRANCE & EXIT

Entrance and exit points as well as lobbies are the most vulnerable areas in a building as these are likely places where perpetrators will attempt to enter the building. For architectural and aesthetic reasons, the entrance lobby is typically a wide and open area with glass facade. The principal recommendations in this section are relevant for every opening that separates the inner part of the building (the secured area) from public or unsecured areas.

Main Lobby Entrance

To deter and detect perpetrators from entering the building, screening has to be conducted at the entry point. Equipment such as X-Ray machines, Walk-Through Metal Detectors (WTMD), Hand Held Explosive Detectors (HHED) "Sniffers" and security checking tables and turnstile gates may be deployed to support screening operations. It is recommended to make provision for the additional loading and plan for space, as well as electricity and low voltage infrastructure in the relevant locations for future equipment. It is advisable to physically shield or separate the screening area from the inner lobby. The intent is to isolate the screening area and contain an attack should the perpetrators be discovered at the screening area. It is advisable to plan for a security standing point, room, or booth positioned in such a way as to give security personnel an unobstructed view of the entire entrance area.

Elevators or Staircases

When designing elevators or staircases at entrance areas, it is necessary to plan options for deploying access control systems and forced-entry resistant gates/doors which can be locked during periods of high alert. The entrance area which usually connects to the elevator or staircase should be equipped with electricity and low voltage infrastructure and space to cater for the possible deployment of screening equipment in the future.

Emergency Doors

Every emergency exit door must be equipped with a detector connected to an alarm system which will raise an alert in case of unauthorised opening. It should also have a locking mechanism suitable for an emergency door according to the regulations and standards.

The entrance area which usually connects to the emergency exit via a corridor should be equipped with electricity and low voltage infrastructure to allow for the deployment of screening equipment at a later stage should the door be converted to a normal entrance.

WASTE DISPOSAL DOCK

Waste disposal docks can be designed in many ways. From a security point of view, it is an area that is close to or inside the building, and which has openings to both the secure areas of the building and to the unprotected areas outside of its perimeter.

LOADING/UNLOADING BAYS

Most modern buildings have designated areas for loading/unloading of office equipment, food, merchandise and all other deliveries to the building. Commercial buildings such as shopping malls or hotels require the loading/unloading bays to be a relatively large area. The bays can be located within or outside the buildings.

In this section, the security and protection issues for loading/unloading bays are considered. These guidelines will have to be coordinated with the operational procedures which, especially in commercial buildings, must take into account the unloading time, queuing time and subsequent line of waiting vehicles which could build up.

Design Considerations of Loading/Unloading Bays

The entrance to the loading/unloading bays should be designed with a vehicle anti-ramming barrier and access control or security personnel. The gate and access control point must be placed as far away from the building as possible and where possible, it should not be under the building and/or below or next to a primary structural element.

During high alerts, for other security reasons or even at peak delivery times during normal alert levels, the queuing vehicles must be taken into consideration. The security checking time at the entrance point may take a number of minutes and delivery vehicles may even be asked to turn around and exit. Space must be allocated for cars to turn around (without them passing the check point) and for vehicles to safely queue. The loading/ unloading area must be located as far as possible from any crowded areas or areas where large numbers of people gather (such as conference rooms) or critical functional areas of the building such as the security control room, safe haven or key building utilities.

It is advisable to allocate an area in the loading dock for checking deliveries and goods. This should include provisions for X-ray or other checking equipment.

Loading/Unloading Bays Located Underneath the Building

No primary structural elements should be located in the loading dock. If this is unavoidable, then the structural engineer must design the primary structural elements for maximum redundancy. The floors above and below should be treated as in the same manner, and no critical building element or important building functions should be located there.

Loading/Unloading Bays Located at the Side of the Building

The loading dock should be located as far away from the building's wall and primary structural elements as. No large opening should be located at or overlooking the loading bay. If this is not possible, glass and other building materials must be protected to the highest blast resistant level.

MAIL ROOMS

In such rooms, mail, parcels and delivery items arrive and are stored until collected by the recipient. They also typically receive large boxes. From the security point of view, if such rooms are not properly designed and positioned, it may allow the entry of threats into the building.

The room should be located near the entrance to the building in order to prevent delivery people from entering the building unnecessarily. It should be located to the side of the building and never in or attached to a main structural element such as a building core or staircase. It is recommended to build the room from reinforced concrete and design it as a structurally insulated box with walls that can withstand an inner static pressure load of 300 kpa. The floor should be designed to allow the insulated mail room an additional permissible load of 10 kpa for inspection equipment. The door must open inwards and be designed to withstand the aforementioned blast load.

The room should have no connection to the building's main ventilation system or openings. All openings or ventilation for the mail room should be separate and ventilated to the outside. The room should be provided with an electricity and low voltage infrastructure to support X-ray equipment, HHED and other detection equipment. The room should be fitted with adequate coverage and an intercom and door which should be closed during inspection.

VIP ROOMS

VIP holding rooms are common in modern buildings and especially in government buildings and luxury hotels. Such rooms should be designed in a way that physical protection and security procedures will be relatively easy to implement.

The VIP holding room may be designed with a dual purpose or used for an alternative function, provided that this does not impact its ability to serve as a VIP room. These rooms should be located near function areas where VIPs are expected to congregate. They should be located as close as possible to an emergency escape route that will be under the total control of the security forces during an event or emergency, which lead to an onsite car park and/or adjacent roads. The main entrance to the room should not lead to the emergency escape route. It is preferable to have a second exit from the VIP room that leads to the escape route.

The walls, ceiling and floor of the VIP holding room must all be accessible for thorough inspection by the security team. The main entry way is recommended to be via a double-door interlocking entry hall with forced entry resistant capabilities on the inner door. There should also be CCTV and intercom equipment to cover both doors. Note that all the walls and openings of the VIP holding room should minimally provide 15 minutes forced entry resistance.

It is preferable to have a second exit from the VIP room that leads to the escape route.

The VIP holding room should preferably be without windows. If this is not possible, all exterior windows or glass façades in the room should be blast protected.

All windows or glass façades that can be seen from public areas and that can allow identification of the VIP should be ballistic resistant to the level of the threat. All windows and doors are recommended to be fitted with magnetic switches and/or glass-break detectors connected to an alarm system.

It is recommended to consider allocating an area for the security attachment. This would typically include bodyguards in an adjacent room with the security equipment infrastructure connecting the two rooms and a line of sight to the VIP room's interlocking entrance.

It is also recommended to allocate an area for VIP cars. The area should be closed or protected against all types of intruders including pedestrians and should be covered by CCTV and detectors. There must also be escape routes close by.

MECHANICAL, ELECTRICAL AND UTILITIES SYSTEM CONSIDERATIONS

The general design and security considerations for mechanical, electrical and utilities systems should also be considered at an early stage. Compatibility and integration with the general design in the initial stage will help achieve an effective assimilation of systems into the overall facility. Such consideration will also prevent conflict between the system requirements and other factors such as the urban planning, landscaping, lighting and fire safe.

The solutions should take into consideration the capacity for future upgrades, expansion and replacements. Any software and hardware used should therefore be modular and upgradeable with adequate physical space catered for future replacement.

Typically, many systems are either shared by security, safety and administration or at least must take into account the requirements and environment of each other. This has to be considered at an early stage to ensure that the requirements of all parties are met and that there is adequate integration between them.

CENTRAL UTILITY ROOMS

A building's central utility rooms serve most of its areas and are connected to almost every location within it. The main functions of the utility rooms which are of interest from the security point of view are water, electricity, communications and air-conditioning. It should be noted that terror attacks can be perpetrated through a building's utility ducts, pipes and other supply channels.

Utility rooms must be located in areas which are well away from potential threats. They should therefore not be close to public car parks or public areas. If this is not possible, then the rooms must be built with adequate protection, such as a shielding wall to protect them from blast related threats on all exposed facades. Entrances to the utility rooms should be locked at all times, controlled by an access control system and monitored from the control room by CCTV and intruder detectors.

Every window or other opening, including ventilation or air-conditioning ducts must be closed off with forced entry resistant bars that can resist forced entry attempts for at least 5 minutes . It is highly advisable to have all the above openings fitted with detectors connected to an alarm system which can alert against intruders or an attempted break-in. Areas containing supply lines for drinking water, water tanks and filtration systems must be locked at all times and access should only be permitted for authorised personnel.

AIR CONDITIONING SYSTEM

A central air-conditioning system supplies the entire building with fresh and treated air. The typical central air-conditioning system usually draws air in from the outside (via vents in the roof or other locations), mixes it with the inner treated air and pumps it back into the ventilation system through the cooling system. Air conditioning systems may be used by an adversary to introduce chemical or biological agents into the building's environment.

These guidelines will refer to central air-conditioning systems that are found in large buildings and could be infiltrated to pose a threat to the building's occupants. They do not relate to relatively small individual systems which are typical to private houses or individual rooms.

The vents which provide the intake of fresh air must be positioned as high as possible to ensure that they are not accessible to the public. The air intakes should be designed and located in a way that makes it difficult for an intruder to access, and such that an object cannot be thrown into them from a distance of at least 10m away. It is highly recommended to place the collection of intakes on the private protected building roof as far as possible from any threat.

Any feed or exhaust for the air-conditioning system including air pipes, air intakes and vents should be closed with forced entry resistant bars or mesh to a minimum level of 5 minutes resistant (see Chapter 6 for testing standards). In addition, it is highly advisable to have all the above openings fitted with detectors and connected to an alarm system to alert against intruders or an attempted break in. It is also recommended to provide the infrastructure for future installation of detectors of toxic or other biological/chemical agents

in the air-conditioning system (these can be combined with smoke detectors). These should be located at the main intake of fresh air and on the exhaust vent from each floor (especially public ones).

It is highly advisable to install valves/shutters to close not only the main fresh air intake, but the intake and exhaust vent from every room. These valves/shutters will be activated when a biological/chemical agent or smoke is sensed by the detectors. They can be operated automatically or manually by the security or operational control room. It is also highly advisable to allocate an area and make mechanical arrangements to insert an air filtering system into the main air-conditioning system. This will provide a future option for providing filtered air directly to specific floors via the floor's shutters or valves.

WATER SUPPLY & WATER TANKS

Water in most buildings in Singapore is supplied through large pipes that feed into reservoir tanks located within the building. The threat to the drinking water supply is mainly from contamination of biological or chemical agent. Sabotage can be done through the pipes or more simply, into one of the reservoir tanks. In most buildings there are separate tanks for drinking water and utilities. Mandatory requirements for security of water storage tanks for potable water supply in buildings are stipulated in the Public Utilities Act, Public Utilities (Water Supply) Regulations and the Singapore Standard CP 48 – Code of Practice for Water Services.

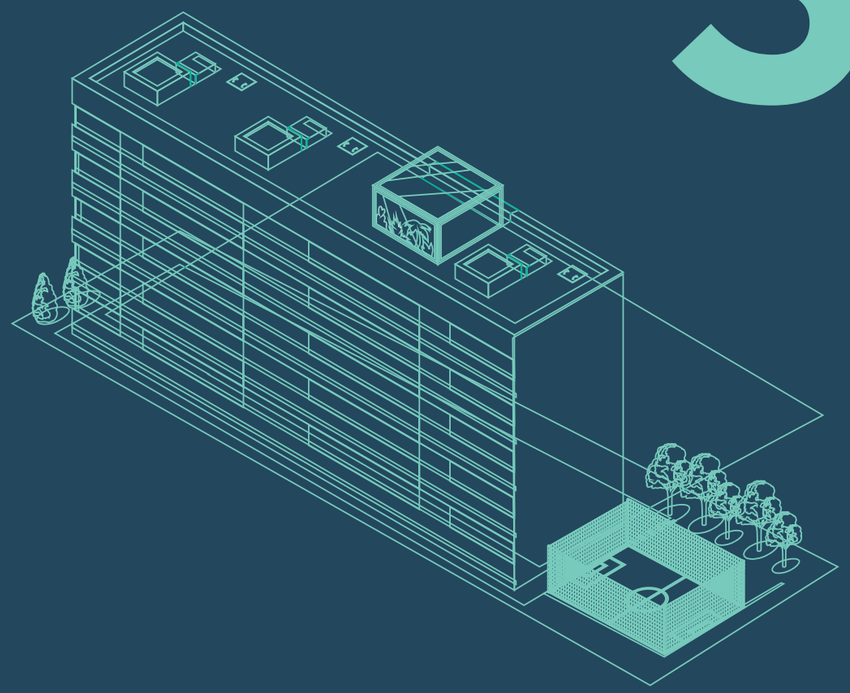
The requirements state that all drinking water tanks and their ancillary equipment must be secured against unauthorised access. They must be housed in a secured and locked dedicated tank/pump room or located within a secured and locked enclosure. The discharge from the overflow pipes of the water tanks shall be within the secured and locked dedicated tank/pump room, enclosure or area and the overflow pipes shall not protrude outside the secured and locked room, enclosure or area.

Additional security measures to be considered would be for all entrances to the water tanks rooms or openings and pipes main valves to be closed with forced entry resistant doors/ mesh and windows. It is highly advisable to add detectors to all the above openings and to send an alert to security in the event of intruders or an attempted break-in. This is all designed to make it very hard for anyone to sabotage the system or insert dangerous materials into it.

If there is a water treatment or purification facility in the facility it must be locked in a room with the same protection level as above (5 min forced entry resistant) and must include an access control system on the door and detectors against unauthorised entry.

It is highly recommended to make necessary provision for toxicity and biological/chemical detectors (this can be combined with water purification detectors) to be incorporated into the system. It is desirable to locate such detectors at the main intake pipe (to check the incoming water) and the supply exiting from the tank (to check the water supplied to the building's residents).

3



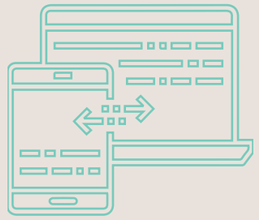
SECURITY PRINCIPLES & RISK MANAGEMENT

DEFINITION OF PROTECTIVE SECURITY

Protective security refers to the protection of people, information and assets from potential threats and dangers such as espionage, terrorism and sabotage. It involves the identification, assessment and review of security measures and procedures to address the risks. Protective security encompasses physical security, personnel security and information security. It is important to consider all these aspects, as they reinforce each other.

PERSONNEL SECURITY

Personnel security is a set of policies and operating procedures that reduce the risk of staff exploiting their access to premises and information for unauthorised purposes. Personnel security measures include robust pre-employment screening, advocating strong security culture in the organisation, and having clear processes for staff exit procedures, including the removal of access rights to restricted areas immediately.



INFORMATION SECURITY

Information security is a set of policies and practices that protect the confidentiality, integrity and availability of information. The risks faced are unauthorised access, use, disclosure, destruction, modification or distribution. Information security measures include access control measures for sensitive information, as well as having an off-site backup of critical data.

PHYSICAL SECURITY

Physical security is a set of measures that reduces the risk of a physical attack or intrusion into a building, and reduces damage or injuries should one occur. It begins with a security review of the facility to identify risks and appropriate measures. The key principle of physical security is the layered protection concept, which focuses on the ability to deter, detect, delay, deny and response to any security threats.

The objective of the Guidelines for Enhancing Building Security in Singapore is to address the physical security component of buildings. However, building owners are also encouraged to consider personnel security and information security as a holistic suite.

LAYERED PROTECTION CONCEPT

The layered protection concept involves five layers of measures: "Deter, Detect, Delay, Deny, and Response. Otherwise known as "Defence-In-Depth", it is an adaptation of the military principle that a multi-layered defence system is harder to penetrate as compared to a single layer of defence. It also gives security forces sufficient time to detect and respond to the incident. These layers should complement each other through a combination of physical, operational and technological measures. This provides coordinated protection of critical assets.

1. DETER

Deterrence is a psychological strategy which aims to prevent an attack by making it clear to an adversary that the risk of failure or getting caught is high. The deterrence layer forms the first layer farthest from the asset. It is an effect of visible physical security measures and clear warnings that the building is protected. For example, surveillance technology along the perimeter (i.e. fencing or wall) coupled with adequate lighting. Prominent security equipment, warning signs that the area is under surveillance and visible guards and patrols all aid deterrence.

2. DETECT

Detection identifies threats early so an alert can be raised. Details such as time of incident, specific location and images capturing the incident are needed. Detection measures include video analytics systems, intrusion detection systems placed on perimeter walls, fences, entrances and/or openings such as vibration sensor detection systems, magnetic switches and passive infrared motion sensors, as well as access control systems. Dual technology systems (i.e. paired solutions such as CCTVs with an intruder detection system) can promptly and accurately detect when an incident occurs.

3. DELAY

Delay aims to slow down a perpetrator by using obstacles that buy time for an appropriate response. This will make it difficult for the perpetrator to penetrate further into the facility. Measures to delay perpetrators include having access control measures, such as intrusion resistant doors and or physical barriers, and the ability to lockdown specific areas of the building to limit movement. Surveillance cameras in this layer will allow security forces to monitor the situation and respond appropriately.

4. DENY

Deny ensures that only authorised persons are allowed entry into protected areas. This can be achieved through access control measures to verify identies. There are various ways of doing this, ranging from biometric or card access systems to deploying security guards at access control points. Creating separate zones within the building can limit exposure if an intruder manages to enter one of them.

5. RESPONSE

Response refers to the means taken to counter an intrusion, or attack so as to protect important assets. Response measures can include turning on lights, sounding sirens, focusing surveillance cameras at the point of intrusion, and dispatching security personnel. Response measures must be integrated with detection and delay measures for the response to be effective and timely.

RISK MANAGEMENT APPROACH

Building owners should adopt a risk management approach to put in place security measures that address identified threats. Risk management involves first working through possible threat scenarios and consequences should existing security measures fail. Then, measures to mitigate these risks such as enhanced physical protection of critical assets can be considered. Assets refer to persons, property, information, or any other possessions of value to the organisation.

In order for protection measures to be focused and effective, the risk management process can calibrate protection needs based on assets, threats and existing protection level. The risk management process is a cycle with four key steps:

STEP 1:
GATHER DATA AND IDENTIFY ASSETS

Gather Data

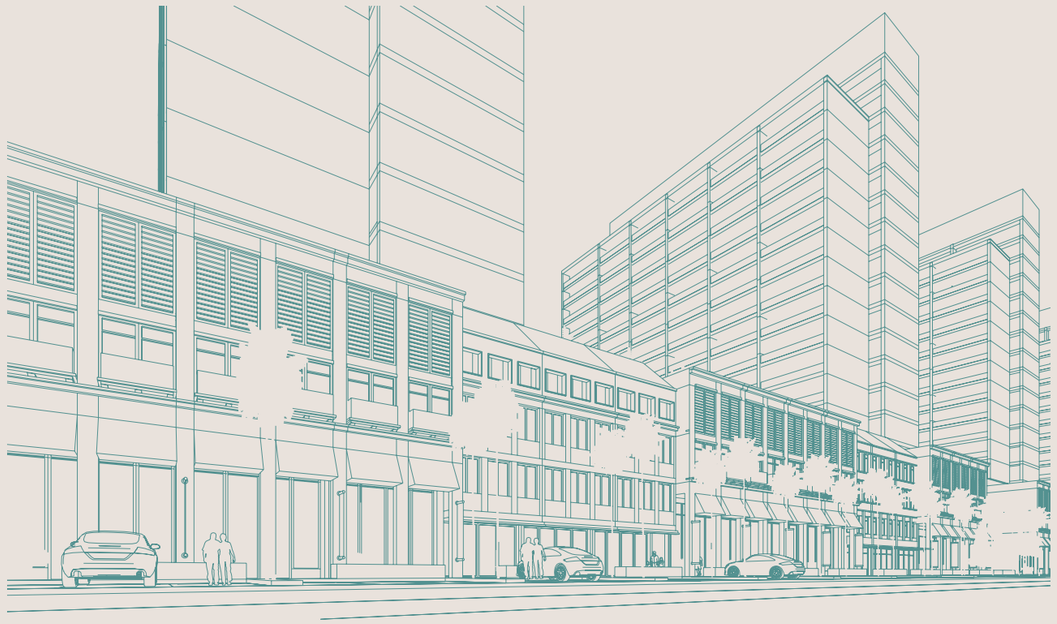
Gathering data is the foundation of the risk management cycle. As all subsequent analysis will be based on the data gathered, it is essential to ensure the data is of high quality. This will determine the quality and completeness of the assessment. The data gathering exercise aims to obtain a complete picture of the current facility, to determine the vulnerabilities and existing measures, so as to establish the most suitable, and cost-effective mitigation measures for the facility.

The data gathering exercise should include an introduction of the facility, including the purpose, nature of its business, how it functions, the list of critical assets supporting the operations, its location and layout, and existing security measures. The building owner should gather data in the following three categories:

- Outer Vicinity and Perimeter - Description/ map of area, topography, vegetation, neighbouring buildings, access roads and other modes of transportation, parking areas, perimeter security, traffic directions, roadblocks

- Building Operations - Usage/purpose/function, size, capacity/number of personnel/ employees/ visitors, operation hours, employee arrival and departure times

- Building Layout - Architectural layout such entrances, windows, loading bays, elevators and staircases, emergency exits, utility rooms, connecting passages; and Structural layout such as critical columns, load bearing walls, beams, transfer girders and slab



Identify Assets

It is important to identify critical assets so that priority can be given to protect them effectively. Building owners should identify and prioritise assets that are essential to carrying out and sustaining of a facility's functions:

• Physical infrastructure (including M&E and utility areas highlighted in Chapter 2)

• People (such as tenants, staff, visitors, contractors, delivery personnel, customers and the public)

• Information (includes both electronic and physical data, including standard operating procedures and emergency response plans)

The building owner should assess what the consequences will be if critical assets are damaged, whether there are any effective redundancies, and identify their location. The building owner should also take note of areas storing dangerous goods such as flammables substances.

STEP 2: IDENTIFY THREATS AND REVIEW SECURITY MEASURES

Identify Threats

Chapter 1 has described the main threats and how they may affect the different assets. The building owner should review if the location of the premises, its tenants, staff and activities are of particular interest to adversaries, or render it an attractive terrorist target, or as an aid to terrorists' activities. In considering the threat, the building owner can review attacks conducted on similar facilities elsewhere, and what the characteristics of these attacks were. This information can be used to determine the types of threats relevant to a facility as well as the location that these threats can occur in their premises.

Review Current Security Measures

For existing buildings, the next step is to study and understand security measures that are already in place. This may include operational and technological measures as well as the deployment coverage, standard operating procedures and emergency response plans. This can be done through observations, interviews and evaluations to understand the following security measures:

• Manpower (e.g. Armed/unarmed security officers, level of training, security plans, deployment, shift schedule, security manager, patrolling schedule, quality assurance)

• Operational & Technological measures (e.g. Fences, crash barriers, doors, locks, alarm systems, panic buttons, access control systems, intrusion detection, CCTV, motion detectors/sensors, communication systems)

• Standard Operating Procedures & Policies
(e.g. Delivery and mail procedures, service providers and maintenance employees clearances, access control procedures, visitor access and screening procedures, emergency procedures, contingency plans, information security)

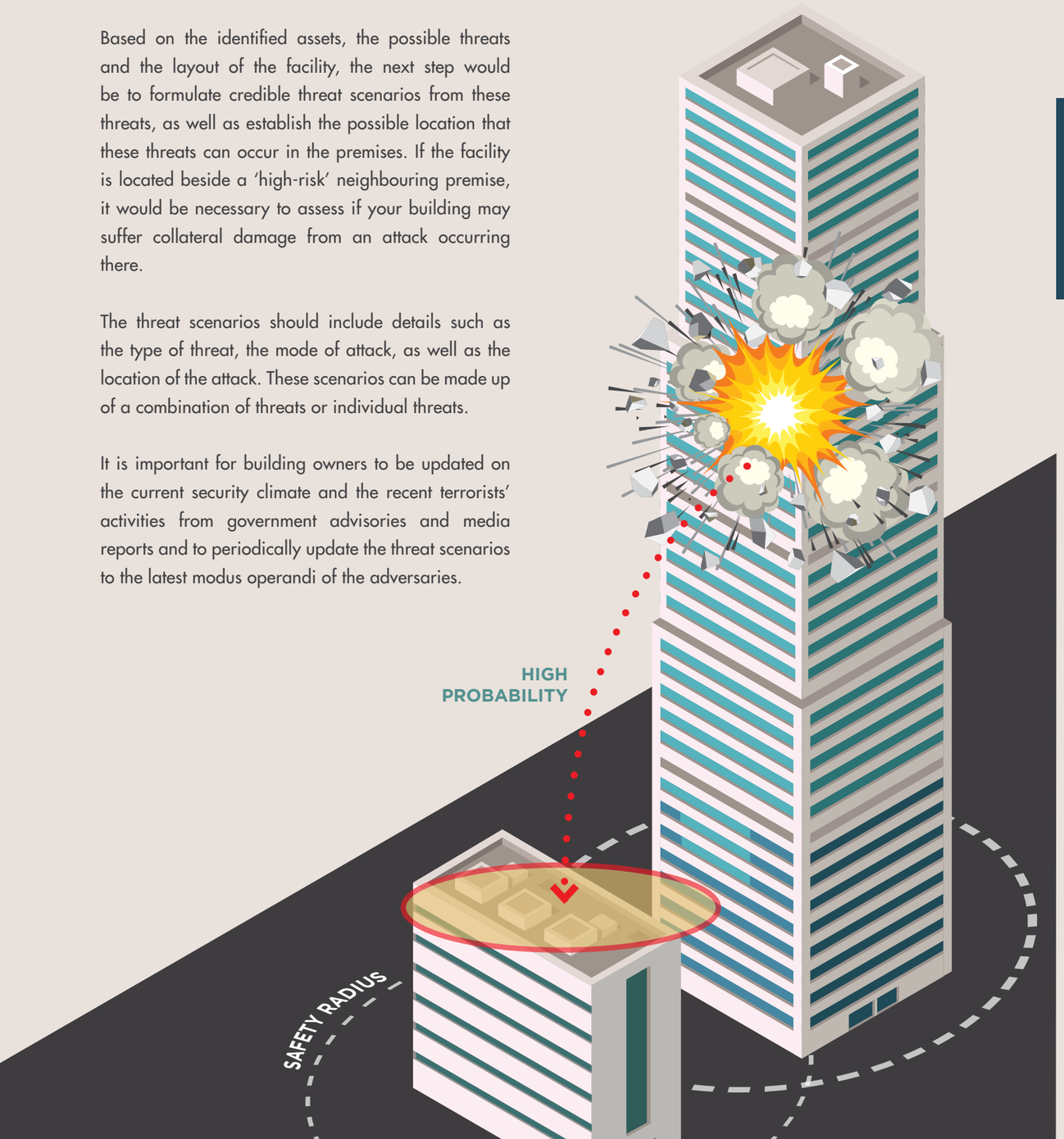
STEP 3:
DESIGN MITIGATION MEASURES

Develop Threat Scenarios

Based on the identified assets, the possible threats and the layout of the facility, the next step would be to formulate credible threat scenarios from these threats, as well as establish the possible location that these threats can occur in the premises. If the facility is located beside a 'high-risk' neighbouring premise, it would be necessary to assess if your building may suffer collateral damage from an attack occurring there.

The threat scenarios should include details such as the type of threat, the mode of attack, as well as the location of the attack. These scenarios can be made up of a combination of threats or individual threats.

It is important for building owners to be updated on the current security climate and the recent terrorists' activities from government advisories and media reports and to periodically update the threat scenarios to the latest modus operandi of the adversaries.



Risk Assessment

Comparing the developed threat scenarios, the critical assets identified and the existing protection capabilities, the building owner can then do a risk assessment for each threat scenario identified based on the following:

RISK = [T]HREAT X [V]ULNERABILITY OF CRITICAL ASSET X [C]ONSEQUENCES OF A SUCCESSFUL ATTACK

Risk is defined in the DHS Risk Lexicon, 2010, as the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" and is assessed as a function of Threats, Vulnerability and Consequence.

Consequence is defined in the DHS Risk Lexicon, 2010, as "effect of an event, incident, or occurrence". Specifically for risk assessment, it refers to the magnitude of damage that can be expected if the threat scenario succeeds as a result of the vulnerabilities of the facility. It is generally measured in terms of effects on humans, economic cost, and intangible impact such reputational or psychological damage.

Vulnerability is defined in DHS Risk Lexicon, 2010, as the "physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard." Vulnerability is a combination of the attractiveness of a facility as a target and the level of deterrence and/or defence provided by the existing countermeasures. Target attractiveness is a measure of the asset or facility in the eyes of a perpetrator and is influenced by the function and/or symbolic importance of the facility.

In calculating the risk of a threat scenario, the common measurement of vulnerability is the likelihood that an attack is successfully carried out, given that it is attempted. Predisposing conditions such as redundancies, back-ups in systems and existing security measures will affect the vulnerability of the facility.

The GEBSS will be adopting the use of qualitative risk assessment for ease of application and understanding. The threats listed in Chapter 1 will be deemed to likely and carry the same weightage, thus will not need to be included in the computation of risk for each threat scenario.

Chart 1: Risk Assessment

Consequences of a successful attack [C]

Vulnerability of critical asset [V]	Very Low	Low	Medium	High	Very High
Very Low	Very Low	Very Low	Low	Low	Low
Low	Very Low	Low	Low	Medium	Medium
Medium	Low	Low	Medium	Medium	High
High	Low	Medium	Medium	High	Very High
Very High	Low	Medium	High	Very High	Very High

Scoring the Risk

For Vulnerability, the key considerations would be how easy or difficult it would be for an attacker to carry out the operations described in the scenarios, as well as how weak or strong the defences are. A score of Very Low would imply a very well protected facility, while a score of Very High would imply a very weak and vulnerable facility.

For Consequences, the building owner would have to assess how badly damaged the protected assets would be, in the event of a successful attack. A score of Very Low would imply that minimal damage or disruption would result should a successful attack take place. A score of Very High would mean devastating damage to the facility and its operations. For example, significant loss of life or the facility becomes unusable.

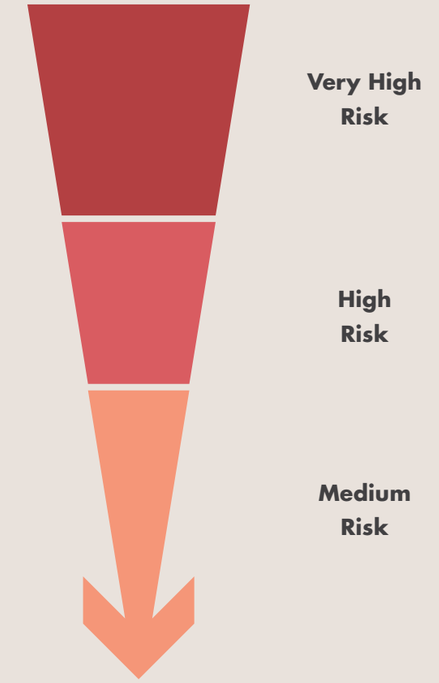
Design Mitigation Measures

With the risk established for each threat scenario, the building owner can then proceed to prioritise the protection requirements. Starting with the highest risk, specific mitigation measures and/or strategies can then be developed based on the nature of the scenarios, with the intent to either reduce threats, vulnerabilities or consequences. An example of measures implemented to reduce vulnerability would be to implement physical security checks on people and belongings for all who enter the facility, while an example of measures to reduce consequences would be to implement laminated glazing at the building façade.

The measures that can be deployed for specific areas will be further discussed in Chapter 4.

Re-Evaluation

With all the mitigation measures proposed, the building owner should then re-evaluate the scores of the Risk Assessment, taking into consideration the new scoring with these measures in place. To illustrate, the installation of glazing protection (e.g. lamination or anti-shatter film) will not prevent the occurrence of VBIED, but it will reduce the loss of lives and/or injuries due to glass fragmentation. From Chart 1, supposing the risk is 'very high' without any protection, it will move down to 'high' after the installation. However, installing the glazing protection does not prevent the entire glass panel from projecting inwards during an explosion to cause fatalities and/or injuries. If the building owner decides to further enhance the protection by installing a cable catcher system or energy absorbing unit to catch the glass panel, then the risk will further reduce from 'high' to 'medium'. The building owner will have to re-evaluate the measures put in to a level that the risk is acceptable to him.



STEP 4:
REGULARLY REVIEW AND UPDATE SECURITY MEASURES AND PLANS

Interim Measures

Some mitigation measures will take time to implement. Therefore provisional plans should be put in place to manage the risk in the interim.

Regular review of security measures and response plans

It is crucial to regularly review and update the security measures and response plans to maintain relevance and effectiveness. The frequency of such reviews should be a deliberated decision by building owners and managers, taking into account the evolving threat situation at the local level (which can be assessed by security personnel on site) or at the national level (which may be communicated from time to time by the relevant authorities). Rehearsals and exercises should be conducted to validate operational plans and SOPs to ensure all relevant parties are aware of their roles and responsibilities in times of an emergency. It is also important to cultivate a security-conscious culture in the organisation. This means educating all personnel on the need for security measures, and what responsibilities each person has to play.

Existing emergency response plans for fire, security manuals, crisis response plans, standard operating procedures and business continuity plans should be regularly reviewed, updated and communicated to the relevant staff. This will ensure that all personnel are familiar with plans and the responses required of them during emergencies. Regular exercises should be conducted to test out these response plans, and to resolve any operational issues.

Security Training

The building owner should also incorporate security training plans for both security and non-security personnel, to familiarise them with the following:

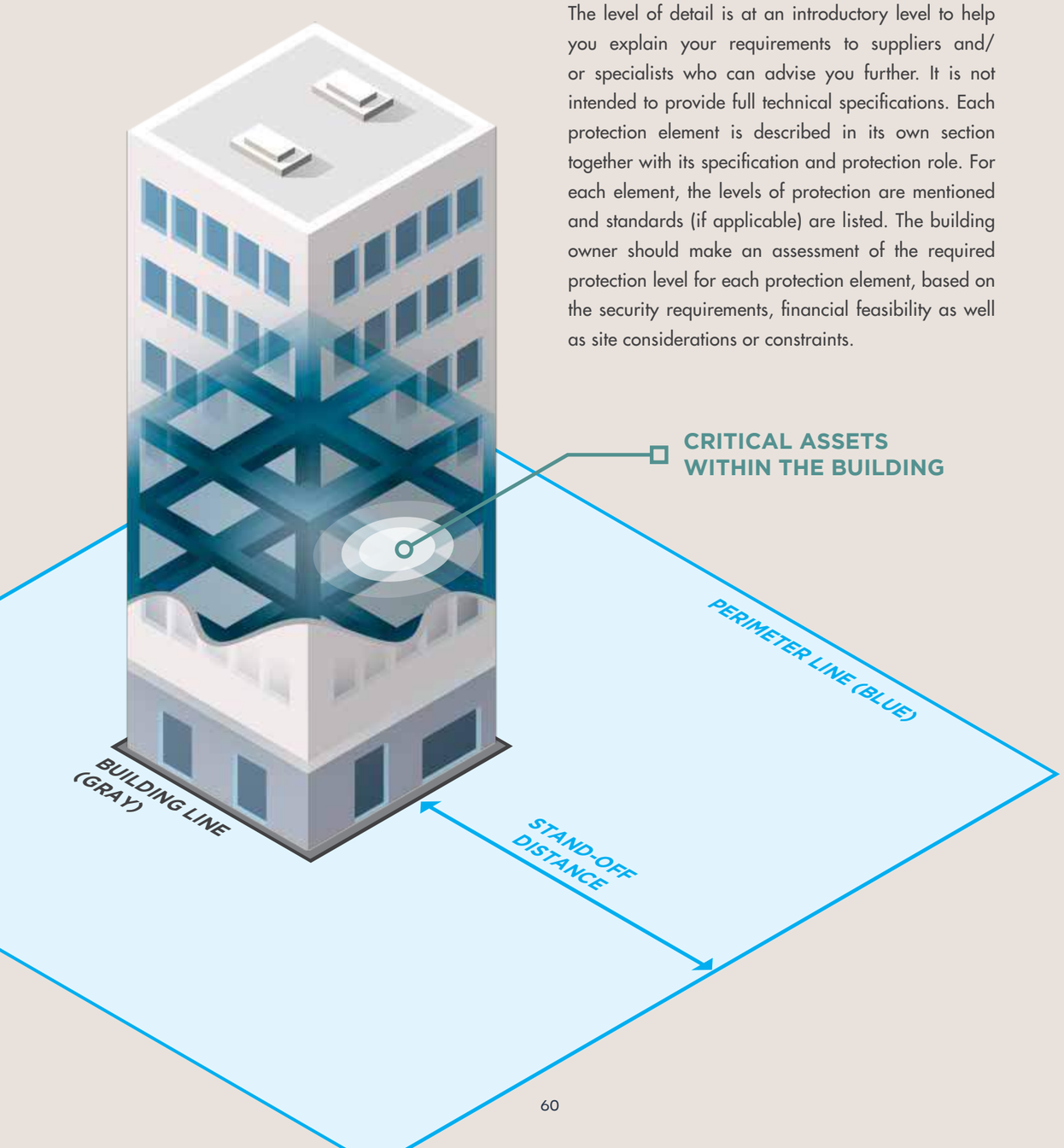
- Identification and management of suspicious:
  - o Activities
  - o Persons
  - o Vehicles
  - o Items
- Incident reporting procedures;
- Response(s) to bomb/terrorist threats; and,
- Familiarisation with the crisis response plans and evacuation plan.

New employees/tenants should also undergo a security induction programme to communicate the security policies of the premise and to share with them on their roles and responsibilities.

4

BUILDING SECURITY MEASURES

HOW TO USE THIS CHAPTER



This chapter contains descriptions and technical specifications for protection and security elements located outside of the building on the perimeter line and within the property's boundary line or building line.

The level of detail is at an introductory level to help you explain your requirements to suppliers and/or specialists who can advise you further. It is not intended to provide full technical specifications. Each protection element is described in its own section together with its specification and protection role. For each element, the levels of protection are mentioned and standards (if applicable) are listed. The building owner should make an assessment of the required protection level for each protection element, based on the security requirements, financial feasibility as well as site considerations or constraints.

Security requirements for each of these elements will be discussed in this chapter:

STRUCTURAL

1. Perimeter Design
2. Vehicle Security Barriers
3. Security Posts
4. Landscaping
5. Security Lighting
6. Carparks
7. Critical Utilities
8. Building Façade
9. Building Walls
10. Load Bearing Walls
11. Glazing
12. Doors
13. Other access points

OPERATIONAL AND TECHNOLOGICAL

14. Building Envelope Air Tightness
15. Security Systems
16. Intercom & Communication Systems
17. Public Address System
18. Intrusion Detection System
19. Access Control Systems

The required protection level for each protection element, is based on the security requirements, financial feasibility as well as site considerations or constraints.

PERIMETER DESIGN

This section aims to provide a basic understanding of perimeter design. It covers the positioning of a building within the lot and the protection elements between the building's envelope walls and the boundary line of the lot.

Examples are provided of architectural possibilities and design considerations that offer various levels of protection. This helps architects make sound decisions about the types of fence, wall or line necessary for any building, based on basic principles of security design and an understanding of the building's characteristics as described in Chapter 2.

Integrating security requirements into a comprehensive approach achieves a balance between many objectives including:

i. Eliminate or mitigate risk
ii. Achieve functionality of the building
iii. Deliver aesthetic and architectural intent

Many protection objectives can be achieved during the early stages of the design process when threat elimination and/ or mitigation are the least costly and most easily implemented. Developers, architects, and landscape designers play important roles in identifying and implementing crucial asset protection measures while considering the orientation of buildings on the site and the integration of vehicle access, control points, physical barriers, landscaping, parking, and protection of utilities to mitigate threats.

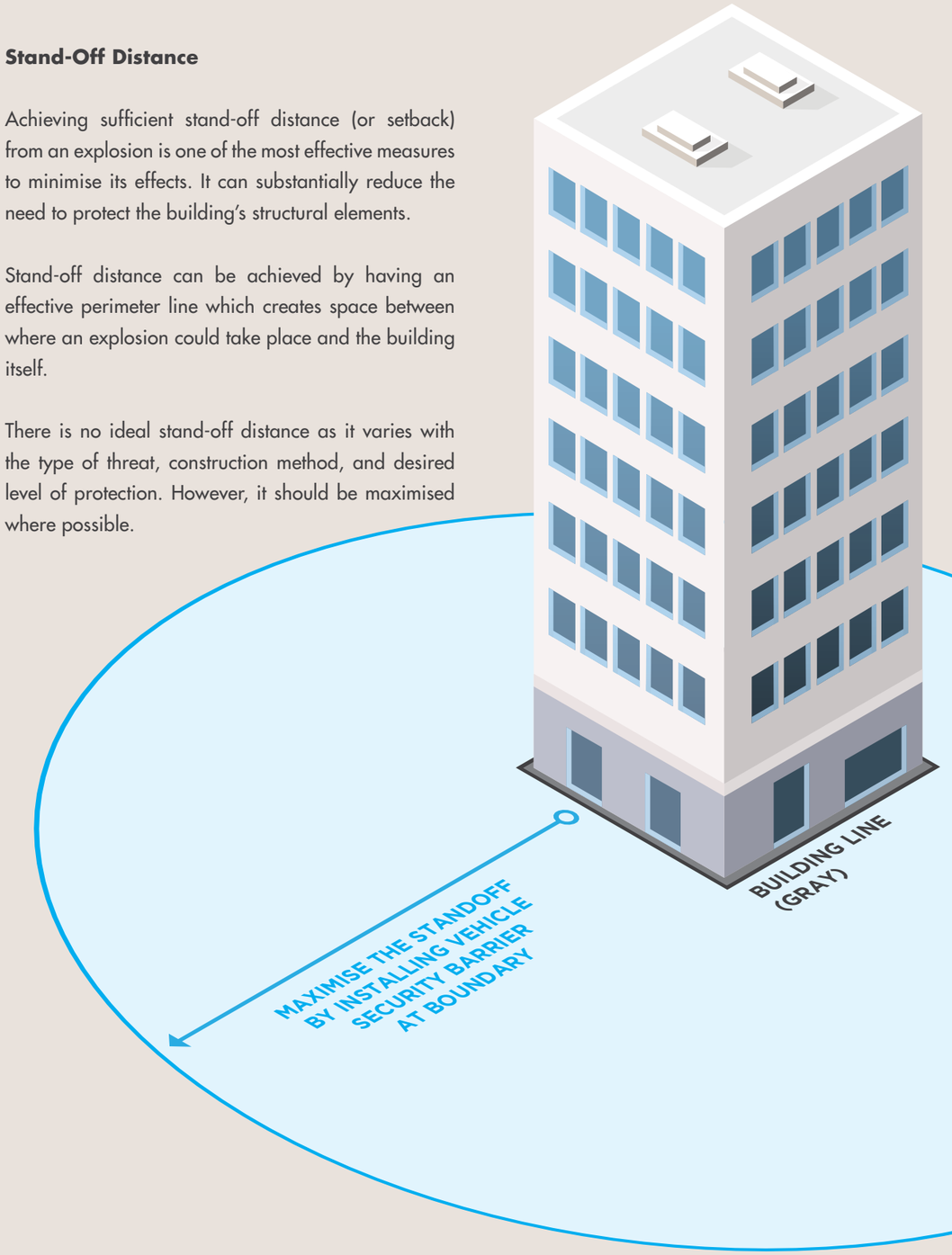
KEY COMPONENTS OF PERIMETER DESIGN

Stand-Off Distance

Achieving sufficient stand-off distance (or setback) from an explosion is one of the most effective measures to minimise its effects. It can substantially reduce the need to protect the building's structural elements.

Stand-off distance can be achieved by having an effective perimeter line which creates space between where an explosion could take place and the building itself.

There is no ideal stand-off distance as it varies with the type of threat, construction method, and desired level of protection. However, it should be maximised where possible.



Perimeter Line

A perimeter line is a physical line, usually following a site boundary, which provides a means of establishing a controlled access area around a building or asset. Physical barriers can be used to define the physical limits of a building and can help to restrict, channel, or impede access and create a continuous barrier around the site. Physical barriers are also a deterrent for anyone planning to penetrate the site. Security measures which form the perimeter line should detect, delay and/or deny access.

Unimpeded access to the building from open spaces increases the risk of an attack taking place close to the critical elements of a building, or to areas with a mass congregation of people. Perimeter line protection can prevent a threat or intruder from approaching the building envelope walls and openings, and critical areas of the building. This is especially important for more vulnerable building types such as those with glass curtain walls and/or pre-cast columns and beams.

There are many ways to create a physical barrier including various types of fences, barriers, walls, bollards, or planters. The selection of barrier elements must take into account the desired level of security based on the threat (e.g. the type of vehicle and approach speed to be protected against). A wide variety of solutions and products are available in the market, which allow building owners to balance cost, physical and architectural considerations.

PERIMETER LINE PROTECTION ELEMENTS

Vehicle Anti-Ramming Perimeter Line

The vehicle anti-ramming perimeter line aims to prevent unauthorised vehicles from entering the site boundary and coming close to the building. It may include fixed or active vehicle security barriers (VSBs) such as bollards, raised steps, concrete walls or planters. Elements to stop pedestrian threats may also be integrated, such as an anti-intrusion fence above a crash-rated low wall.

Vehicles can pose a significant security threat due to their carrying capacity, weight and speed. These threats include:

i. Delivery of large explosive devices
ii. Ramming attacks into crowds of people or critical assets
iii. Insertion of armed attackers by penetrating the perimeter line

Figure 2: A crash-rated wedge vehicle security barrier.

Figure 1: An example of a continuous Vehicle Anti-Ramming Perimeter Line.

The first consideration when planning a vehicle anti-ramming perimeter line is to reduce the number of locations where a vehicle can penetrate the perimeter line. This is done by ensuring the perimeter line is not close to any roads or any other area which allows vehicles to approach. As VSBs typically involve foundation and structural works, they should be considered early in the project design phase.

Standards for Vehicle Security Barriers

The guidelines for VSBs are based on the ISO IWA 14 Vehicle Security Barriers, which combined and updated elements from UK BSI PAS 68, PAS 69, ASTM F2656 and CWA 16221. It specifies the essential impact performance requirement for a vehicle security barrier and a test method for rating its performance when subjected to a single impact by a test vehicle. The above-mentioned test standards are crash-test standards that specifies the test methodology and performance rating for different vehicle types (e.g. from passenger cars to very heavy trucks) ramming at specific impact speeds.

Design of Vehicle Anti-Ramming Perimeter Line

The anti-ramming perimeter line should be continuous and completely surround the site. There should not be any locations where unscreened vehicles could approach or enter the site, including from neighbouring plots and open areas. Design factors to consider are:

i. The approach speed of a potential vehicle approaching the perimeter line is a design criterion which should be considered at the initial design stage when planning the access roads to the site. It is desirable to try to reduce this speed using traffic obstacles near entry control points to slow down traffic and thus lower the required protection level of the VSBs;

ii. The edge-to-edge distance between discontinuous VSBs such as bollards or clear spacing between adjacent barriers should be no more than 100cm in width for traffic having a 90-degree approach and 120cm in width for traffic paralleling the barrier;

iii. The minimum height of the VSBs should be 65 cm from the ground; and,

iv. How far a vehicle can penetrate after has made impact with the VSBs must also be considered in the design of the perimeter line, as this affects the stand-off distance used when determining how the building should be protected from blast effects.

In order for the VSB to reliably stop hostile vehicles, it must be crash-rated through a proper certification test (see Standards for Vehicle Ramming Barriers). Not all VSBs in the market are crash-rated. The certification will indicate the level of protection the VSB offers, and should be examined before choosing a VSB. The building owner should decide what level is appropriate in consultation with the architects, security and protective design/blast consultant(s).

TYPES OF VEHICLE SECURITY BARRIERS

The selection and design of vehicle security barriers has to take into consideration the site context. This is especially if physical security elements are proposed within the public realm, or in areas that are intended to be accessible / enjoyed by the general public. In such cases, designers should take a holistic approach to ensure appropriate measures are undertaken to meet the level of security required while not compromising the ease of pedestrian movement or public enjoyment of the space. Designers should ensure that physical security elements are successfully and seamlessly integrated into the design of the streetscape so as to address the security requirements while still creating pleasant public spaces. As a guide, such elements should not negatively impact the streetscape or affect pedestrian access / movement within the public realm.

Designers and building owners will need to comply with the Urban Redevelopment Authority (URA)'s development control & urban design requirements for any proposed physical elements that may compromise the public's experience of the overall streetscape.

Figure 3: Bollard line with a mix of steel bollard covers and decorative bollard covers.

Figure 4: Bollards integrated into street furniture.

Bollards

Bollards can be fixed, removable or retractable. They come in a variety of designs that incorporate different foundation types for different site conditions.

Figure 5: Hardened Planters

Hardened Planters

A planter is a concrete landscaping feature that can be hardened to stop vehicles. It can hold plants or other decorative features, making it an aesthetically pleasing alternative to bollards. It is installed partially underground and partially above ground and can be incorporated as part of the landscape design.

Figure 6: Hardened Streetscape

Hardened Streetscape Items

Items integrated into the streetscape, such as benches, sculptural or seating barriers, lamp posts or signposts can be hardened to function like bollards. These can be used effectively in combination with other barrier types.

Figure 7: Hardened Walls

Hardened Walls

Walls that are structurally reinforced can be used effectively as part of a vehicle anti-ramming perimeter. These may consist of retaining walls, plaza edges, an extension of a building's architecture or the base of a fence. It is vital that the wall's foundation be continuous. Such walls are typically used in combination with other barriers.

ANTI-INTRUSION BARRIER

Figure 8: Example of an anti-intrusion perimeter line.

A pedestrian anti-intrusion perimeter line is designed to prevent unauthorised persons from entering the site and approaching the building. This can be combined with other protection elements to also stop vehicles. Intruders can attempt to enter covertly to avoid detection, or overtly using force. The possible threats include:

i. Delivery of smaller explosive devices

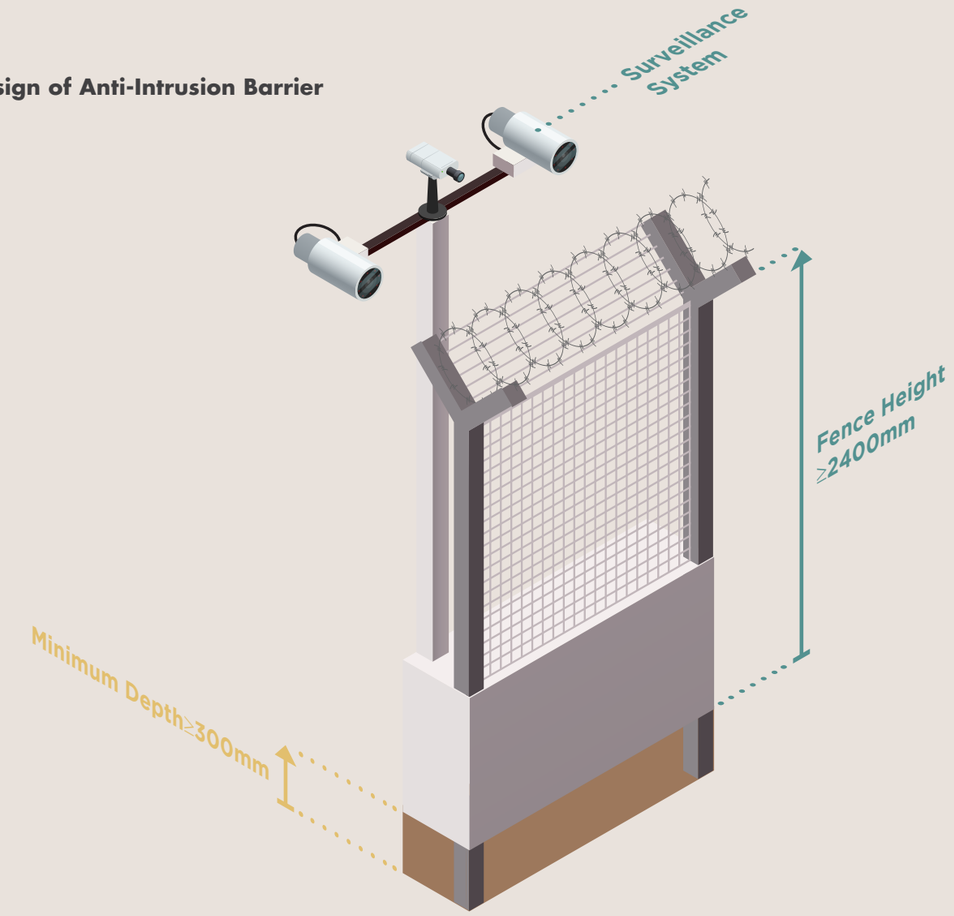
ii. Armed attack on people or critical assets

iii. Sabotage or theft

Given sufficient time, a determined intruder will eventually be able to breach any barrier. Hence, its primary aim should hence be to delay an intruder and improve the probability of their detection they are detected. This will give response forces time to arrive.

An anti-intrusion barrier can be customised for a particular project, or purchased off-the-shelf. The barrier can be combined with a system that detects intrusion attempts. In some cases, only an intrusion detection system may be used with no physical barrier. This should only be done when there is a large buffer zone so response forces have enough time to react before intruders reach the building.

Design of Anti-Intrusion Barrier



Anti-intrusion barriers consist of a fence or wall as the main physical barrier, anchored with an appropriate foundation. It may be equipped with a top guard and detection system. Key design considerations include:

- Minimum barrier height of 2400mm (As recommended in BS 1722-10:2006).
- Minimum footing depth of 300mm to delay tunnelling attempts.
- All component parts, including connectors and interfaces with the building structure should meet the required level of protection.
- Height and design should be consistent throughout the perimeter line to prevent vulnerabilities.
- There should be no footholds or objects that allow an intruder to scale the barrier. For example, trees or light poles, or footholds on the exterior face.
- Gaps below any gates should be smaller than 150mm.
- Design should consider the detection, alarm and surveillance systems to be installed.
- Line-of-sight requirements as this will determine the barrier material.

Standards for Anti-Intrusion Barrier

The guidelines for anti-intrusion fence are based on the BS 1722-10 and UFC 4-022-03 that provide guidance on anti-intrusion fences.

TYPES OF ANTI-INTRUSION BARRIERS

Welded Mesh Fencing

Figure 9: A welded mesh fence with sensor line

The welded mesh fencing should resist cutting. The UFC 4-022-03 recommends that "maximum vertical/ horizontal opening dimension must be 51mm with minimum thickness of 3.76mm. It is more secure and durable as compared to a normal chain link fence.

The fence can be combined with a crash-tested low wall to stop vehicles. However, this type fence is not typically strong enough to stop large crowds.

Figure 10: A welded mesh fence

Steel Ornamental Fence

Figure 11: A typical steel profile fence

A wide range of steel profiles can be used for fences which vary in cost and effectiveness. The decision on which profile to use is dependent on the specific need or threat and the required structural stability. The bars may also be angled outwards at the apex of the fence to discourage attempts to scale the fence.

The distance between the steel bars, and that between the fence and the ground, should not be big enough to allow a potential intruder to squeeze through. UFC 4-022-03 recommends a maximum of 152mm between the fence and the ground. Due to the weight of the fence and the desired heavy duty performance, it is particularly important to plan the pole foundation properly.

It is important to make sure that no element of the fence, or anything in the location of the fence, will allow an intruder to use it as a step.

Walls

Walls can be constructed of hollow building bricks or concrete. They can be reinforced to stop vehicles with steel bars, and/or by filling hollow bricks with concrete. To stop vehicles, the wall would need to be designed and crash-tested according to the threat level and security needs. If the wall is a prefabricated concrete wall, care must be taken to ensure the joints between the wall segments are sufficiently robust.

Top Guards

A range of systems can be installed on the top of a fence or wall to make it more difficult for a person to climb over. Some systems can also detect intruders. Installation can usually be done either when the fence or wall is built, or at a later time depending on budget and needs.

Types of Top Guards:

- Concertina Wire

  Concertina barbed wire secured to the top of a fence or wall

- Single Angle Outrigger

  300-400mm steel arms angled outwards from the poles and connected to each other by 4 to 5 lines of barbed wire. This can also support intrusion detection wires.

- Double Angle Outrigger

  300-400mm steel arms angled in two directions from the poles and connected by 4 to 5 lines of barbed wire. Concertina wire can also be installed on top.

- Spikes

  Spikes or other features can be put on the top of a fence or wall in order to discourage an intruder.

Fence Intrusion Detection System

Fence intrusion detection systems (FIDS) consist of sensors to detect intruders and a device to sound an alert. These sensors detect intruders by monitoring movement, sound, vibration or other disturbances.

Standards for Fence Intrusion Detection Systems

The guidelines for fence intrusion detection systems are based on the UFC 4-021-02 and BS 4737-4.3.

Types of Fence Intrusion Detection Systems:

- Taut Wires

  Taut wires are stretched along a fence and sound an alarm in the command centre if the wires are cut, pulled or bridged (electrically). In some cases they can also provide a non-lethal electric shock. The taut wires may come be installed in a variety of configurations such as on the top, inside or outside of a wall.

- Step Detectors

  Step detectors are used to detect someone stepping on the top of a wall or laying a ladder against it. They usually consist of covered coils running along the top of the wall. When the cover bends from the weight of a person or ladder, the command centre is alerted.

- Infra-Red Active Motion Detectors

  Infrared active motion sensors screen an area with infrared light. If anyone passes through the screened area, a signal will be passed to the 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 surveillance based system which works by using analytics to identify suspicious behaviour. For example, movement in a prohibited area. An intruder will see the cameras but will not know that a motion detector is in use.

- Vibration Detectors

  Vibration detectors are based on wires running through a fence with sensors installed along their length to detect any vibration. An intruder trying to climb the fence will cause an alarm to be triggered in the command centre.

- Microwaves Motion Detectors

  These detectors make an invisible line using microwaves. Crossing the line will send a signal to the command centre. These detectors are usually noticeable.

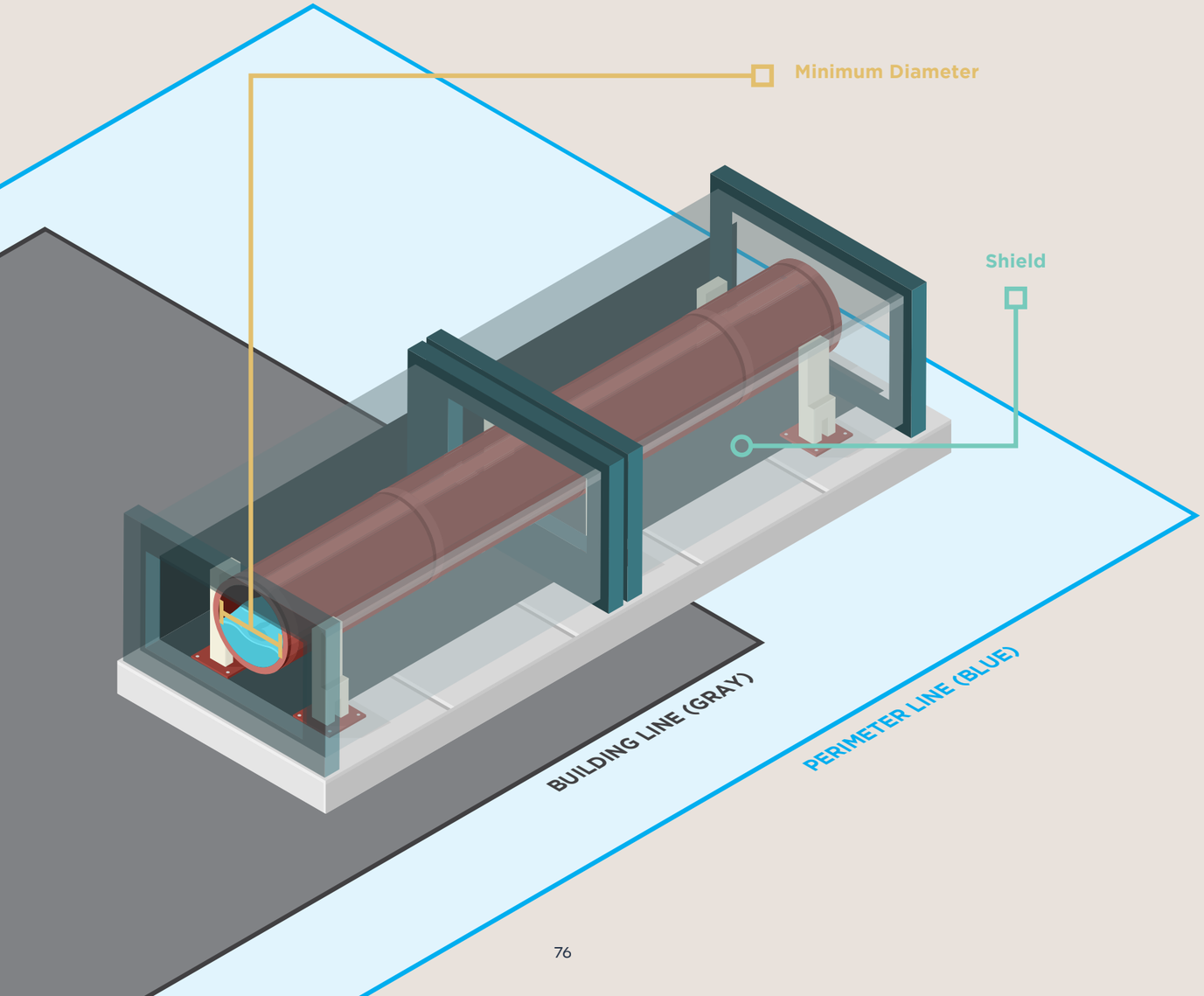
- Infrared Beam Detectors

  Infrared beams can create an invisible line or lattice that when crossed, triggers an alarm in the command centre. These detectors are usually noticeable.

INFRASTRUCTURE PIPES

Infrastructure pipes include ducts, channels, utility openings, drain and sewerage infrastructure. They can all be used to perpetrate attacks against buildings and installations. Intruders may use them to infiltrate a building/ facility, or to conceal or introduce explosive devices or hazardous materials. As these infrastructure elements are necessary, it is critical to ensure they do introduce risks.

The design of these elements often required openings or access points on the building itself (e.g. air intake ducts), at the perimeter line (e.g. rain drainage pipes in a perimeter fence) or beyond (e.g. sewerage manholes on the street).



Design of Infrastructure PIpes

The design of infrastructure pipes should minimise the size of any openings as far as possible. If the pipe creates a gap in the perimeter line or building envelope, a comparable level of protection should be provided so it does not become a weak point that can be exploited. This may include:

- Forced-entry protection such as welded wire mesh or steel grilles. If installed over a drainage ditch or vent, the diminished flow capacity and maintenance.

- Needs to be accounted for. Manhole covers can be secured with locks and hasps, by welding them shut, or by bolting them to their frame.

- Intrusion detection systems can be installed if warranted by the sensitivity of the building, complemented with visual surveillance systems.

External drainage pipes which may assist intruders to climb over the perimeter line or into the building should have anti-climbing features. For example, installing them at an angle, affixing spikes, barbed wire, or using anti-climb paint.

Standards for Protection of Infrastructure Pipes

BS 8220-2 and the UFC 4-022-03 has standards for protection of infrastructure piping available for reference, providing guidance for "protective measures for culverts, storm drains, sewers, air intakes, exhaust tunnels, and utility openings, that have a cross-section area of 620 cm^2 or greater (with the smallest dimension being more than 150mm if the opening is rectangular, or the diameter being more than 250mm if the opening is circular)".

VEHICULAR AND PEDESTRIAN ENTRANCES

All perimeter lines usually need access points for vehicles and pedestrians. These points are regarded as weak links as they create a gap in the protective line every time they are opened. Access points control the time and people permitted to enter a building or facility. In addition to controlling passage, access management usually includes the ability to observe and track movement in and out of controlled areas.

The entry points through a perimeter line will typically consist of vehicle gates, pedestrian gates, and in some cases, a guard post. The entry points provide places where the required level of vehicle or pedestrian screening and access control can be implemented. The challenge of designing an entry point is to prevent unauthorised access while maximising the flow of authorised access by pedestrians or vehicles.

Planning for vehicle and pedestrian access and entry control points for a new project should begin at the initial stages with a traffic impact assessment, which is an evaluation of the expected rates of vehicular and pedestrian access to the site. Matching the protection requirements with the flow requirements is one of the main challenges when planning an entrance of any kind. Consideration should be given to optimising the number of entrances and most importantly, positioning them at the least vulnerable locations.

For most buildings located in urban settings, the vehicle entrance often leads directly into an underground or multi-story car park. It is important to note that the security screening of passengers at a vehicle entrance usually does not provide the same level of scrutiny of persons as screening at a pedestrian entrance and therefore does not replace it. The entrance from the car park to the building will therefore require the same screening level for persons as the other pedestrian entrances.

For a typical building, three types of vehicle screening and two types of pedestrian screening entrances are required which may be at separate locations or incorporated into one.

VEHICLE ENTRANCES

- Resident/authorised entry
- Visitor entry
- Delivery vehicle entry

PEDESTRIAN ACCESS

- Resident/visitor (usually using the same access point and controlled by the same access control method)
- Contractor/Service access

Design of Vehicle Entrances

When designing for entry control points, if possible, the entry point should be at a location as far as possible from the building or facility itself. Entry roads which run under parts of the building should be avoided in all cases. Access roads should be designed to force drivers to approach at low speed. The entry control point should be positioned to allow adequate visual assessment of approaching vehicles. A route should be catered for vehicles that have been denied access at the security check to exit without having to enter the site or move vehicles in queue.

A designated entry point for delivery and service vehicles should be set up, preferably away from critical assets and areas of mass congregation. The approach to the site should be designed according to peak traffic demand without impeding traffic flow in the surrounding road network. Current and future inspection technologies (e.g. above vehicle and under vehicle surveillance systems) should be considered when putting in place the entry control points.

Active vehicle security barriers should be implemented both at the entrance and exit points. Any vehicle gate on the perimeter line should provide the same level of protection against vehicles and intruders as that provided by the rest of the perimeter line. Entrances should be designed in such a way as to enable access control to be implemented either for unattended entry using an access control system or by guards.

Design of Pedestrian Entrances

In the design of pedestrian entry control points, as much as possible, the entry point should be at a location as far as possible from the building or facility itself. The entrance should be designed to contain an attack and prevent it from progressing towards the protected facility.

Access flow requirements should be designed based on the expected flow at peaks hours. Any pedestrian gate on the perimeter line should provide the same level of protection against vehicles and intruders as that provided by the rest of the perimeter line.

Entrances should be designed to enable access controls to be implemented either for unattended entry using an access control system or by guards. Sufficient space should be allocated for proper inspection and for communication (which may be at a distance) between the people entering and those responsible for approving access.

Active Vehicle Security Barriers

Active Vehicle Security Barriers (VSBs) can be installed at vehicle entrances to prevent unauthorised vehicles from entering the premises. Active VSBs are those can be raised or lowered to allow authorised vehicles and stop hostile vehicles. A combination of elements may be used to also prevent the intrusion of pedestrians.

A vehicle getting within close proximity of the building or gaining access to an underground or multi-storey car park is one of the main threats which needs to be prevented. The range of possibilities for perpetrating threats using a vehicle is wide and can include:

i. Delivery of large explosive devices

ii. Ramming attacks into crowds of people or critical assets

iii. Insertion of armed attackers by penetrating the perimeter line

Vehicle anti-ramming perimeter entrances may sometimes need to close car parks to vehicular traffic after-hours, but still allow pedestrian access. In such cases, it would be more effective to install two separate gates at the entrance for vehicles and pedestrians, so that opening the barrier for pedestrians will not inadvertently allow unauthorised vehicles to enter.
The vehicle security barriers standards for perimeter lines will apply for the anti-ramming entrance.

Design of Vehicle Anti-Ramming Entrance

In addition to the design considerations for VSBs and vehicle entrances which have been covered above, additional considerations are required in the design of active VSBs. The foundation requirements of the proposed active VSB should be considered early on since an underground car park beneath the barrier line could limit the choice. Consideration should also be given to any requirements for pedestrian access as well as the VSB performance criteria.

Certain types of active VSBs are more suitable to remaining open for extended periods of time. These are used for sites that not require vehicle screening at all times (e.g. only at elevated or high threat levels, or during limited hours). Cycle Time / Pass-through Rates. The device pass-through rate should be consistent with the desired vehicle processing (3 to 15 seconds is suitable for most inspection and identification station requirements).

The active VSB must perform within the required parameters and include sufficient time delay after activation to allow vehicles to enter or exit the parking area. Not all active VSBs are suited to the environmental conditions at all locations. Barrier components may require protection from excessive heat, dirt, humidity, sand, high water table, or require additional maintenance.

Reliability is an important factor in selecting active VSBs. The system's failure modes need to be evaluated to ensure that the VSB will fail in the predetermined position (open or closed) based on the security and operational requirements. Backup generators or manual override capabilities are needed to ensure continuous operation during power failures or equipment malfunction.

It is important to note that active VSBs are capable of inflicting serious injury, even when used for their intended purposes. Warning devices (visible colours and patterns, reflectors, lighting, warning lights, and safety signals) should be used to mark the presence of an active VSB and enhance its visibility to drivers. Vehicle detector safety loops and road plates chequered for good traction can also enhance safety.
Screening equipment should be proposed based on the ability to discover threat devices according to the relevant threat level (e.g. if the threat to the building is a large bomb hidden in a car boot, a screening system to search the underside of a vehicle will not be effective).

TYPICAL OBSTACLES

S Curves
90 Degree Bends
Traffic Circles
Speed Bumps

The active VSB must perform within the required parameters and include sufficient time delay after activation to allow vehicles to enter or exit the parking area.

TYPES OF ACTIVE VSB

Sliding Gate

A sliding gate can be a barrier for both vehicles and pedestrians. However, they need to be of significant mass and size in order to stop a ramming vehicle (see figure 12). Apart from the profile of the steel bars or plates, how the gate is anchored on both sides is a critical factor which provides the required protection.

Sliding gates can be slow to open and close. They need to be completely closed to provide full protection. Most designs of leaf (hinged) gates are not to be able to stop a vehicle.

Figure 12: Sliding gate

Drop-Arm Barrier

A drop-arm barrier provides protection from vehicles but does not stop pedestrians. Many drop-arm barriers are available, but not many meet anti-ramming standards. In order to provide adequate protection, they will usually be equipped with an internal cable. It needs to be completely closed to provide full protection. The height of the raised arm should be provided for if there is a roof above the barrier.

Figure 13: An anti-ramming arm barrier

Retractable Bollard

Automatic retractable bollards provide protection from vehicles but does not stop pedestrians. They can be lowered and raised relatively quickly, which is an advantage where a high rate of vehicle flow is needed.

For safety reasons, bollards should be installed together with a non-crash-rated drop-arm barrier to improve visibility of the bollards.

Figure 14: Retractable anti-ramming bollards

PROTECTED PEDESTRIAN ENTRANCE

A forced entry resistant gate prevents unauthorised people from entering the premises. Both criminals and terrorists may seek to gain entry to a building. In the case of terrorist attacks, they often take place at the entrance itself, particularly when there is some form of security in place there.

When considering the pedestrian entrances at the initial planning stage of a new development project, the aims should be to:

i. Optimise the number of entrances.

ii. Position the entrances at the least vulnerable locations.

iii. Place entrances as far from the building line as possible.

iv. Locate entrances in an area that will prevent any potential incident from influencing the inner areas of the site. For example, a partition could block the line of fire towards the foyer. Sufficient empty space could be provided above an entrance to avoid an explosion at the entrance affecting anyone above.

Forced Entry Standards

How long an entrance can resist forced entry is defined in various test standards. What is required for a given facility can be determined based on the following considerations:

i. Accessibility of the entrance to a potential intruder in terms of:
   a. The length of time that an intruder can attempt to breach the entrance without being interrupted
   b. How likely it is for an intruder to gain access to the entrance, given other security measures and the layout of the facility

ii. Importance of the asset protected.

iii. Time taken for first responders to arrive.

International test standards for forced entry resistant products include European Standards EN 1627, EN1628, EN 1629, EN 1630 and EN 356; and American Standards ASTM F476, ASTM F588, ASTM F842, ASTM F1233 and ASTM F3038. Another standard, the US DOS SD-STD-01.01, is intended for use by US Department of State in its facilities throughout the world.

Design of Protected Pedestrian Entrance

The following requirements need to be considered for the design of protected pedestrian entrance. The portal at the pedestrian entrance should be built to the same protection standard as the building envelope. The gate should prevent anyone from breaking through as well as climbing over or under. Waiting areas may need to be assigned both on the exterior side (pre-security screening) and on the interior side (post-security screening). Different security requirements during and after office hours should be considered.

For the selection of the automated gates or turnstiles, the device pass-through rate should be consistent with the desired entry processing speed and the expected flow rate of pedestrians. Reliability is another important factor. In particular, the system's failure modes should ensure that the barrier will fail in a pre-determined position (open or closed) based on security and operational requirements. Backup generators or manual override capabilities are needed to ensure continuous operation during power failures or if equipment malfunctions.

Potential conflicts with safety and emergency evacuation needs should be resolved at an early stage. Some gate systems can cause injury if proper care is not taken, even when used for their intended purposes. Warning devices should be used to mark the presence of a gate.

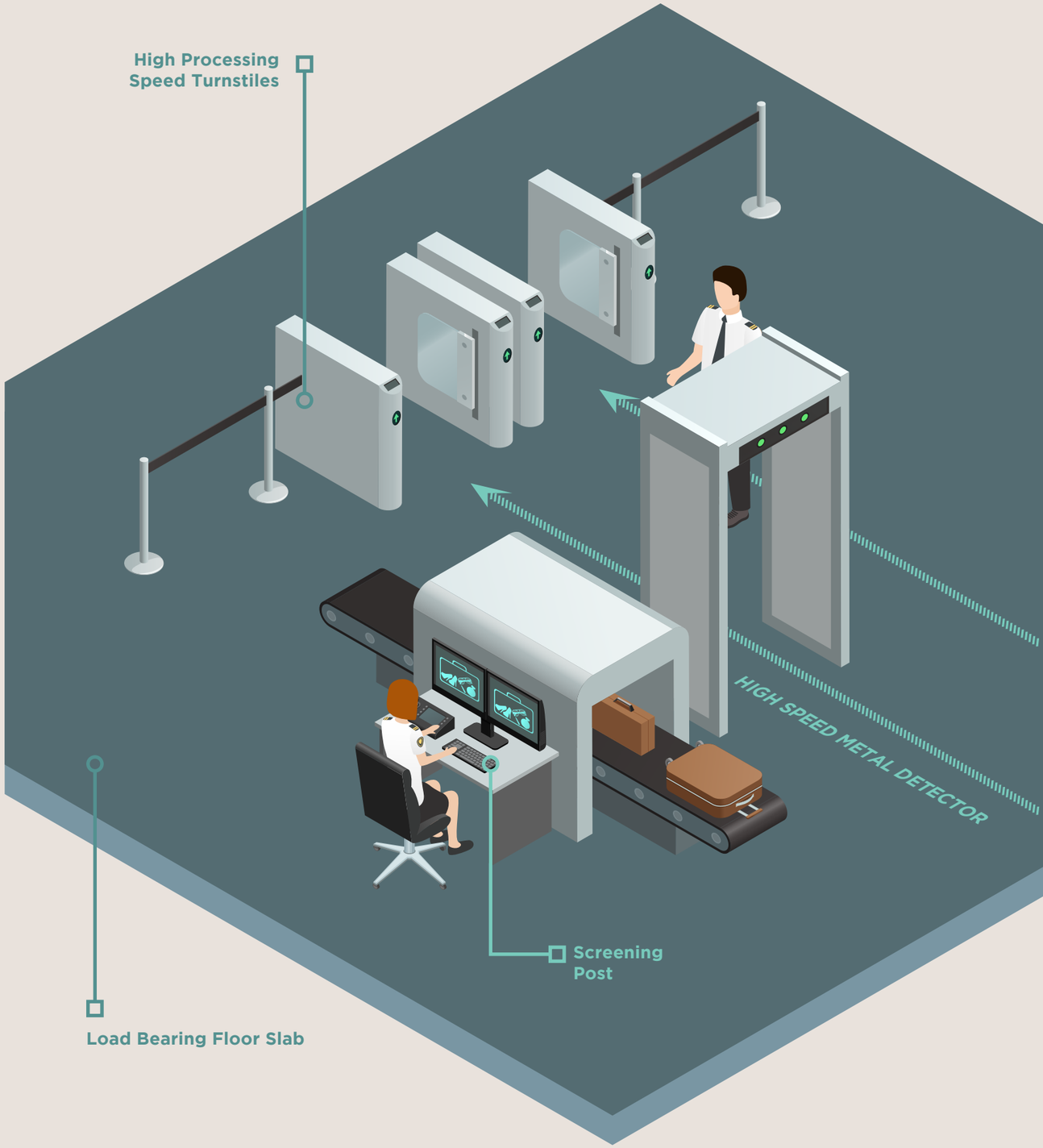
It is recommended to make provisions so that each entrance in an interlocking gates/turnstile system can be upgraded without replacing the whole system. When an interlocking system is required, it should be implemented at entrances and exits.

If screening is to be undertaken as a standard procedure either at present or in the future, it should take place before the final gate line. In case of an inter-locking system, the area between the barriers should be used as the security screening point and preferably should be outside the perimeter line. This area should not be placed under populated or vulnerable parts of the building. If it is absolutely necessary to locate the screening area under parts of the building, the area must be hardened to contain the effects of an attack there.

The entrance should be located in an area that will prevent any potential incident from affecting the inner areas of the site. For example, a partition could block the line of fire towards the foyer, or the area above an entrance could be left unoccupied to avoid an explosion at the entrance affecting anyone above. Even if procedures at normal threat levels do not require an interlocking entrance, it is recommended to try to allocate necessary space in case such a procedure is required in the future for higher threat levels.

Requirements for screening equipment (e.g. walk-through metal detectors or x-ray machines) should be considered early, which include sufficiency of:

a) Space available;
b) Loading of the floor slab;
c) Electricity infrastructure;
d) Posts for guards performing the screening;
e) Lighting of the screening area.



Examples of Protected Pedestrian Entrances

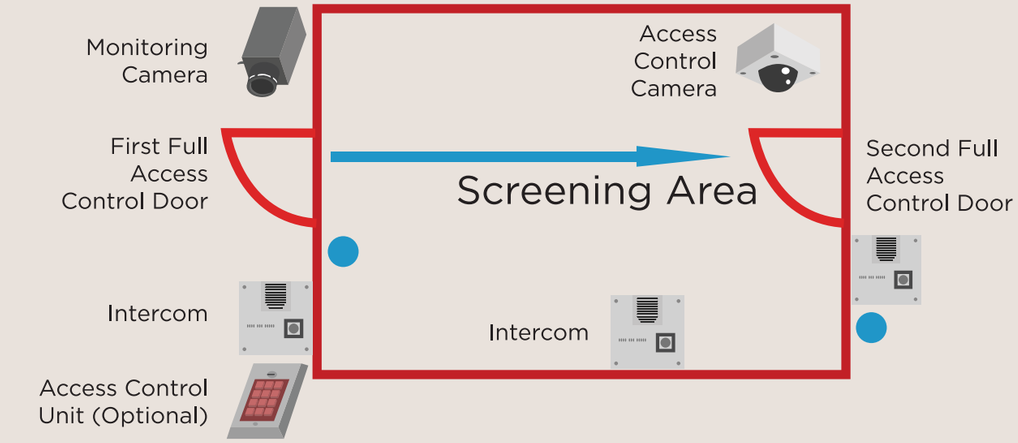


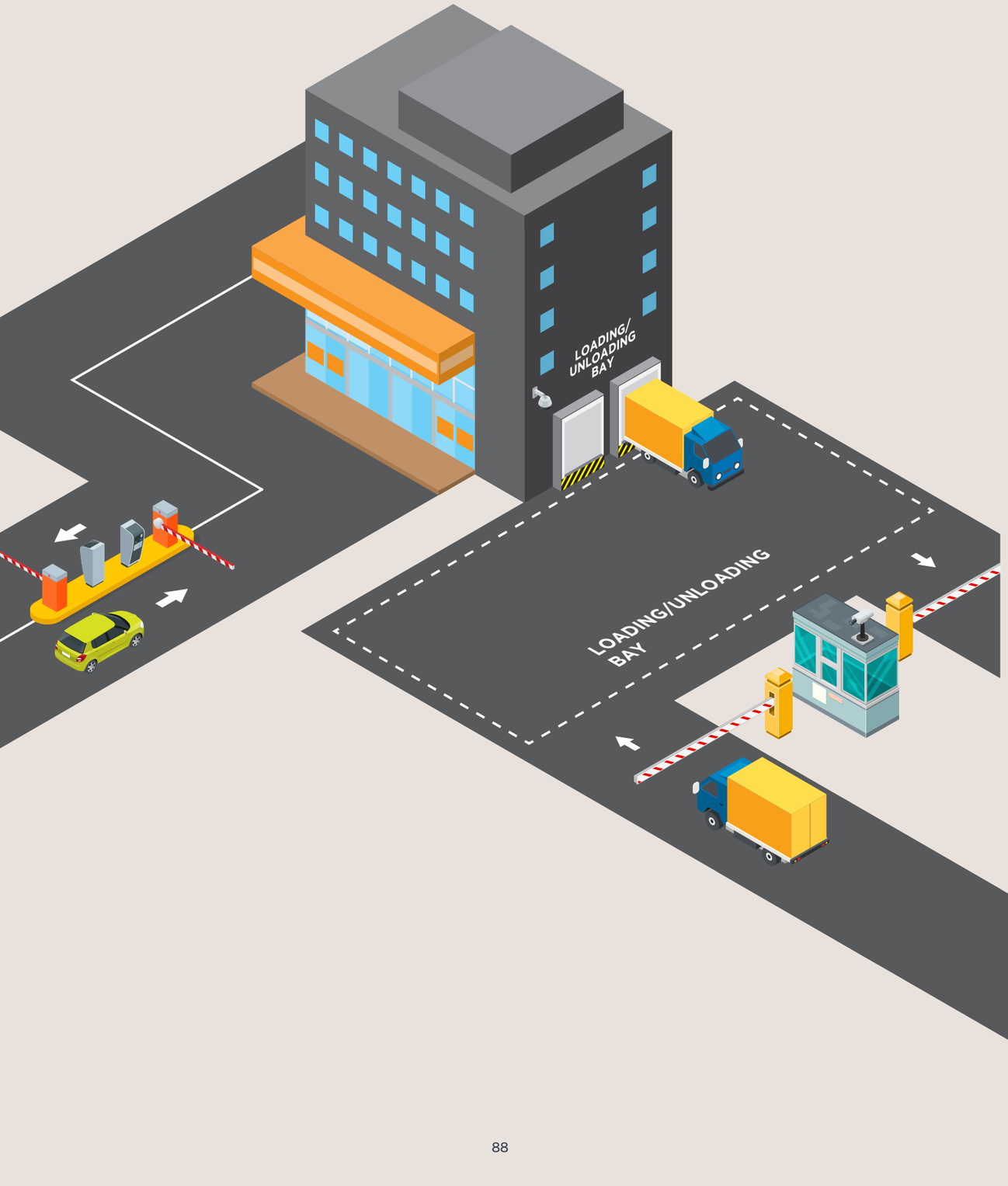
Figure 15: Typical interlocking system entry point

Figure 16: Pedestrian access point

DELIVERY/SERVICE VEHICLE ACCESS CONTROL

Loading docks and service access areas are a necessity for a building. The specific requirements may vary according to the characteristics of the building, its environment and traffic regimes. In many cases, loading docks are positioned either inside the building itself or in an underground car park. Therefore, careful attention should be given to these service areas in order to avoid undesirable intrusions and infiltrations of explosive charges.

If a delivery or service access control point is planned, it should be equipped with an active VSB that is crash-rated to the same performance criteria as the anti-ramming perimeter line. It should be noted that the vehicles accessing the loading dock are expected to be significantly heavier than those at the regular vehicle access point. Reference should be made to the section on “Vehicle Security Barriers” for the design considerations and possible designs used in a delivery/ service access control point.



Design of Delivery/
Service Vehicle Access Control

When designing the delivery/service vehicle access control point of a building, the following recommendations apply:

Driveways leading to the loading docks and the loading docks should be positioned away from the building so that vehicles will not be allowed to access near or under the building. If this is not possible, the area should be hardened for blast and under no circumstances should the location be close to major structural elements.

- Keep the delivery entrances separate from main vehicle entrances with clear signs.

- Loading docks and shipping/receiving areas should be kept away from rooms housing critical building services such as utility mains, electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.

- Use an interlocking vehicle entrance for the delivery/service entrance, or at least have the ability to upgrade to one in case of elevated or high threat levels.

- Locate the security screening area on the exterior of the barrier. Consider infrastructural needs of the screening equipment (e.g. underground pits, extra lighting, underground cameras), and whether space is needed for delivery vehicles to queue at peak hours.

- The screening process and equipment must detect relevant threats. For example, undercarriage screening cameras need to be used together with physical inspections of the vehicle interior if concealed explosive devices are a concern.

- Design of the loading dock should limit damage to adjacent areas and vent explosive forces to the exterior of the building.

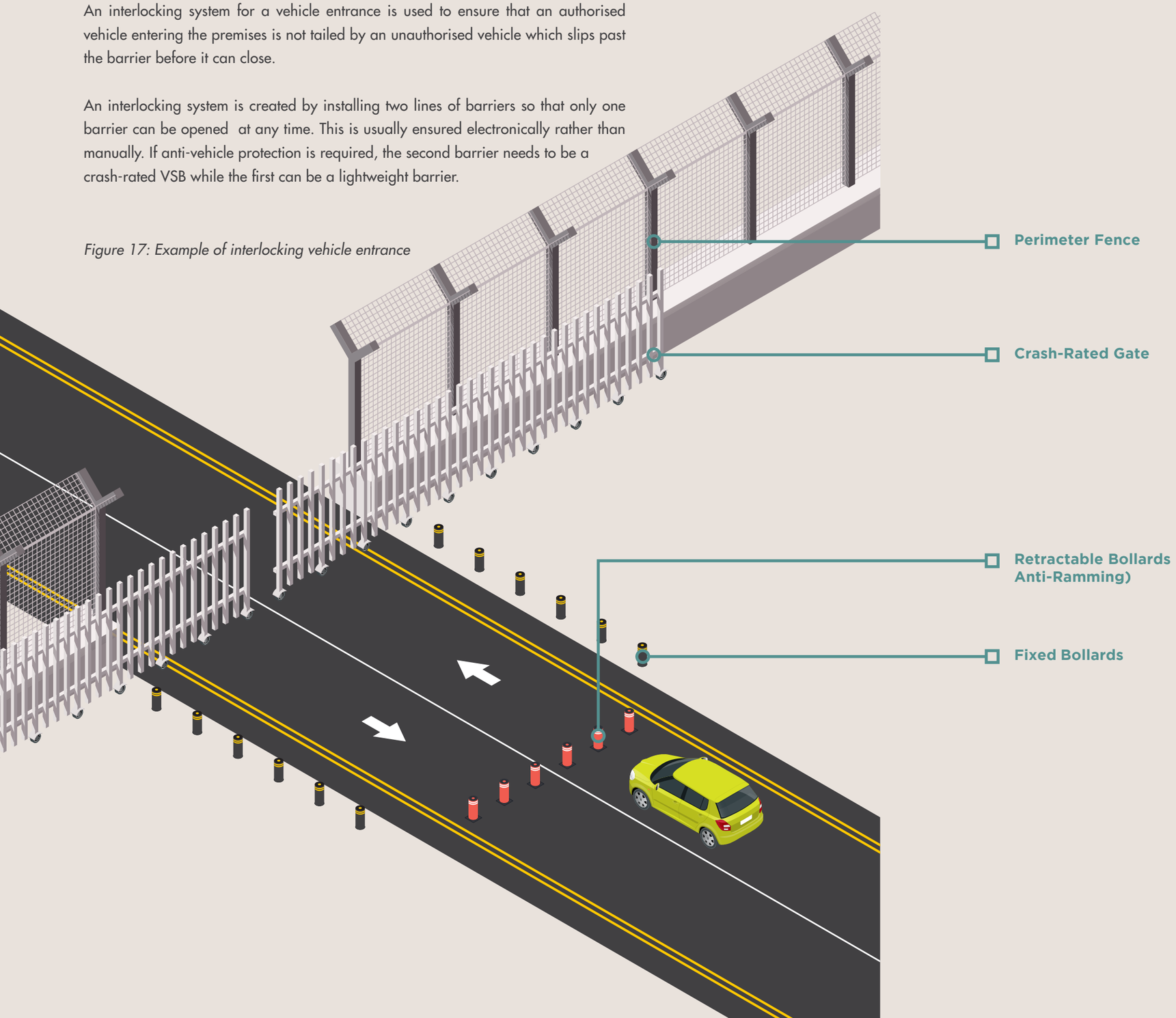
- Ideally, delivery/service vehicle bay should have its own Air-Handling Unit and should be zoned independently from the rest of the building. It should also be kept at a negative pressure compared to the rest of the building but positively pressured with regards to the ambient atmosphere.

INTERLOCKING VEHICLE ENTRANCE

An interlocking system for a vehicle entrance is used to ensure that an authorised vehicle entering the premises is not tailed by an unauthorised vehicle which slips past the barrier before it can close.

An interlocking system is created by installing two lines of barriers so that only one barrier can be opened at any time. This is usually ensured electronically rather than manually. If anti-vehicle protection is required, the second barrier needs to be a crash-rated VSB while the first can be a lightweight barrier.

Figure 17: Example of interlocking vehicle entrance



Design of Interlocking Vehicle Entrance

An interlocking vehicle entrance is one where one of the barrier lines also forms part of the perimeter fence.

It is recommended that the sliding gate be the lightweight barrier (i.e. non-anti-ramming). It will open and close faster, and be less costly. The second barrier should be the anti-ramming line. The distance between the two barrier lines should fit the maximum size of vehicles that use the entrance. The entrance should be designed to prevent a vehicle from bypassing the second line once it has been allowed through the first line. Sufficient lighting as well as space and power for screening equipment should be provided.

The interlocking system is required at both entrances and exits. Both barriers should be operated by the same system controller. The area between the barriers should be used as the security screening point and preferably be outside the perimeter line. This area should not be under populated or vulnerable parts of the building. If there is no choice but to locate the screening area under parts of the building, the whole area must be strengthened in such a way to contain any possible attack that could take place there. It is recommended to try to allocate necessary space in case such a procedure is required in the future for higher threat levels.

SECURITY POSTS

The security post is meant to enhance the ability of the security guard to perform his duties by being well positioned and well equipped regardless of the weather or light conditions.

Security posts are built when there is a security need to man a static location on the building's perimeter line or at critical positions for long periods of time. The security post is meant to enhance the ability of the security guard to perform his duties by being well positioned and well equipped regardless of the weather or light conditions. It can also be used to improve his survivability in case of an attack aimed at breaching the building's perimeter.

Security posts can be designed and built as part of the development or in certain situations, be bought as a ready-made product when only a small booth is required (usually at vehicle entrances).

ENTRANCE SECURITY POSTS

The entrance of a facility is one of the most vulnerable and critical locations within a site because it performs three main functions:

i. Administrative admission / information.

ii. Access control.

iii. Security screening.

For these reasons, an entrance security post, guarding the vehicle and pedestrian entrances, would likely be the first point of attack so that the perpetrator can gain access into the facility. Sufficient consideration should be given to the balance between aesthetics, functionality and protection since the entrance often gives the visitor his first impression of the building.

As the entrance is usually on or close to the building lot line, design mistakes are very difficult to correct, especially if the desired stand-off distance is not achieved. Due to their critical role in providing protection to the assets by keeping unauthorised vehicles away, a certain protection level is required for the entrance security post itself.

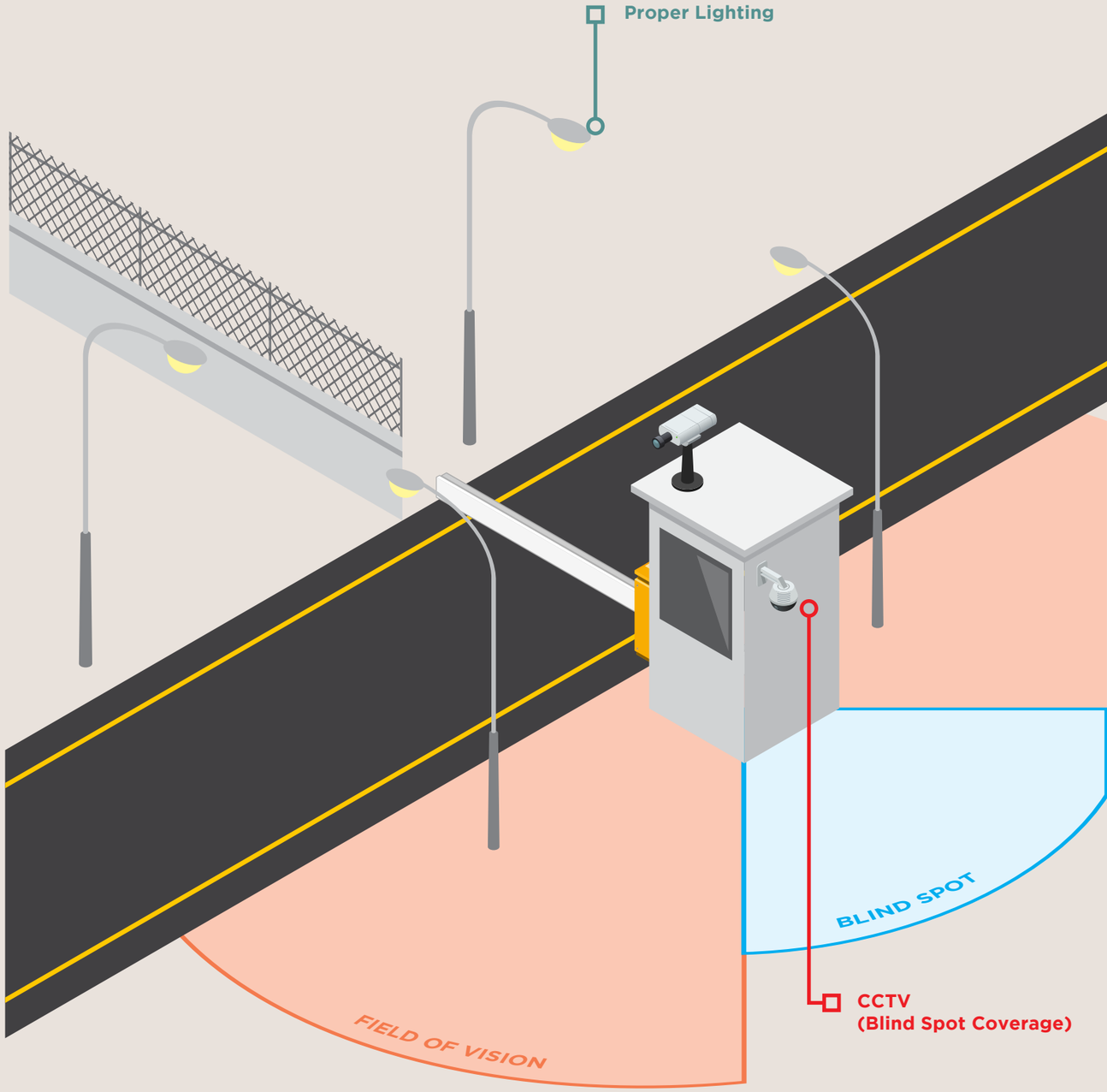
Design of Security Posts

Entrance security posts should provide a good field of vision and tactical control of the area under their responsibility. The area under observation should also have proper lighting and be covered by cameras. Blind spots should be monitored using cameras.

The security post positioned on the perimeter which are securing the entrances should be designed to give the guards a good field of vision and tactical control of the area under their responsibility. Where necessary, the observation of the area under responsibility should be augmented by proper lighting and cameras. Blind spots should be prevented and backed up by CCTV monitoring or mirrors if they cannot be avoided. No critical controls for any building security system should be placed in the perimeter or entrance security post. Exceptions can be made only if the security post has an adequate protection level. The systems in the security post should be fail-secure to ensure the site remains secure if the post is breached.

If the post is not in an area secured from the potential threat on the exterior side, the line between the security post and the inner side of the building should be protected to prevent any potential perpetrator from moving into the building. The entrance to the security post should be from the inner area and not from the outside. If the security post is on the building line, it should be carefully considered if access is needed both between the security post and the screening area and between the security post and the inner building area. This should be avoided, but if it is unavoidable, forced-entry protection should be considered to deny or delay entry to the perpetrators.

A security control room, if it exists, should be able to override the access control systems operated by the entrance security post. The entrance security post should have enough allocated space to house all screening equipment for both currently planned and future options. The entrance security post should be equipped with a duress button to allow guards to alert the security team /local security monitoring centre in the event of an attack.



LANDSCAPING

The clear zone is the area between the buildings and the perimeter line. Unrestricted visibility is required in order to ensure that no intrusion will be unnoticed and package-sized objects cannot be abandoned without detection. A clear zone can be achieved by using a combination of civil and architectural elements with exterior landscaping. Certain types of intrusion detection systems (e.g. video analytics or infrared detectors) require clear lines-of-sight to the area marked out for detection, and this should be noted when designing the landscape for the clear zone.

POSITIONING OF CAR PARKS AND CRITICAL UTILITIES

Addressing security issues during the initial stages of a development project has an enormous impact on the ability to implement cost effective protective solutions. By eliminating or limiting the possibility of carrying out an effective attack, the need to harden the building or vulnerable areas can be reduced.

The following can make a critical difference to the outcome of a terrorist attack:

i. Stand-off distance between potential threat areas and either critical areas or areas where people gather.

ii. Good positioning of the buildings or vulnerable areas within the lot.

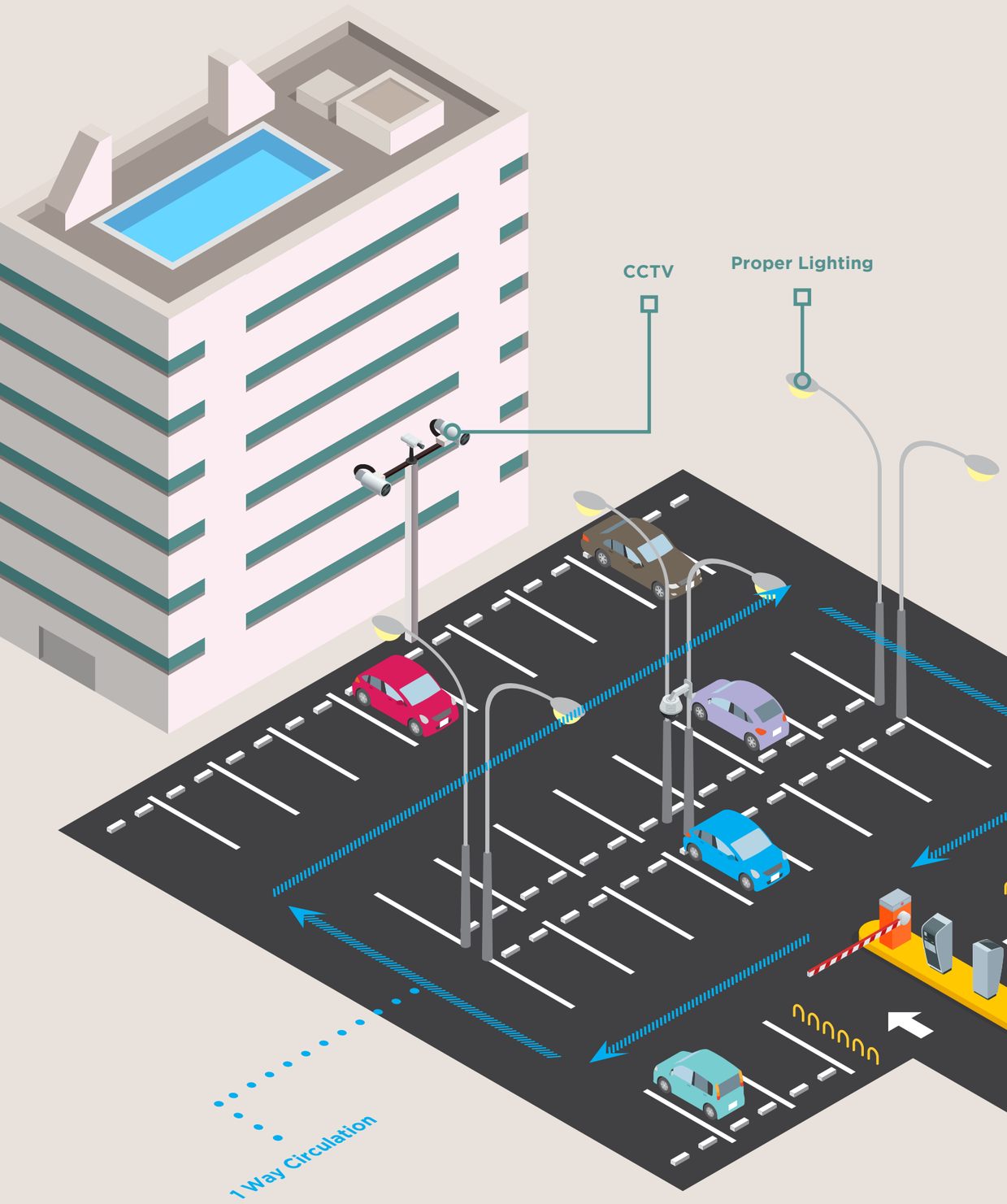
If sufficient stand-off distance is difficult to achieve because of land scarcity or other architectural considerations, the right positioning of the building will be able to compensate considerably for this.

For example, if the building's lot has a public road that runs along it, the structure positioning should try to maximise the distance between the road and the structure or areas where people gather.

The congregation of a large number of people behind large glass façades in public areas poses a great risk. The internal positioning of the various functional areas within the site has a critical influence on the cost and the ability to protect them.

This section will focus on two main areas whose positioning is particularly sensitive:

i. Car parks
ii. Critical Utilities



POSITIONING OF CAR PARKS

Car parks can provide a relatively simple opportunity to introduce large quantities of explosives to a building's vicinity or to its sensitive and vulnerable areas. Limiting or restricting parking can help to keep threats away from a building. However, in a dense urban environment like Singapore, parking spaces in close proximity to the building, and underground parking are common. Mitigating the risks caused by parking in close proximity can be achieved by creative design measures, including parking regimes, perimeter buffer zones, barriers, structural hardening and other architectural and engineering solutions. Operational measures may also be implemented to inspect or screen vehicles entering car parks.

Design of Car Parks

Vehicle parking areas should be sited as far as possible away from

- Highly populated areas.
- Rooms housing critical assets, and critical building services such as utility mains, electrical, telephone/data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.

Parking areas under the building and having vehicle access roads close to key structural elements should be avoided. If this is not possible, the building and key structural elements should be hardened against blast. The design of the car park should limit damage to adjacent areas. If it is enclosed, explosive pressure build-up within the enclosed car park should be vented to the exterior of the building. If possible:

- Resident and visitor parking should be separated.
- Visitor or general public parking areas should be located near, but not on or below, the site itself.
- Parking lots should be designed with one-way circulation of traffic.

There should be adequate lighting and with CCTV surveillance of the parking areas. Height limits should be imposed to limit the size of vehicles allowed into the car park or to highly vulnerable areas. The management of traffic flow and queue of traffic heading to the car park must be considered carefully when planning the location of a car park.

POSITIONING OF CRITICAL UTILITIES

Utility systems can suffer significant damage when subjected to the shock of an explosion. Some of these utilities may be critical for safely evacuating people from the building or to the emergency response to an attack. Their destruction could cause damage that is disproportionate to other building damage resulting from an explosion. For example, if a fire breaks out as a result of an explosion, the consequences of the fire extinguisher or smoke ventilation systems not functioning can be much higher than the direct results of the explosion.

Design of Critical Utilities

As much as possible, the critical utilities should be located underground, concealed, and protected. There should be redundancy to life saving utility systems. Water treatment plants and storage tanks should be protected by limiting and securing access points, such as manholes.

The main fuel storage should be located away from areas that can be easily accessed. For utilities that need to be refilled, they should be located at areas that can be accessed from the outside of the building thereby limiting the need for service vehicles to enter.

Garbage containers should be located as far away from the building as possible. Incoming utility systems should be concealed within building and property lines. Critical or fragile utilities should be routed such that they are not located on exterior walls or on walls shared with mailrooms, loading docks etc.

To limit opportunities for aggressors to place explosives underneath buildings, ensure that access to crawl spaces, utility tunnels, and other means of under building access is controlled. Such means by which utility services can penetrate a site's perimeter barrier, including through fences, walls, or other perimeter structures, should be sealed or secured to eliminate openings large enough for an intruder to pass through the barrier. Typical means include storm sewers, water, electricity, or other site utility services. Please refer to the section on "Standards for Protection of Infrastructure Pipes" for more advice.

BUILDING FACADE

This section describes construction methods, solutions and protection elements relating to the building's envelope including façades and openings. The façades at the building's envelope walls are the main protection against most criminal and terror related threats including silent or forced entry, shootings and explosions.

The objective of this section is to provide basic protection design guidelines enabling architects and engineers to make decisions regarding doors, windows, envelope walls and building materials.

The level of detail provided is at an introductory level. It provides basic knowledge to assist in specifying requirements for suppliers and/or protection engineers to provide further advice.

These decisions should be based on knowledge and understanding of the relevant design criteria, protection requirements and the building's characteristics.

In the event of an explosion, protected façades will transfer part of the blast load to the building's structure. This transferred force must be calculated and considered when designing the structure. Some products will transfer more energy than others. Their performance must be proven by the manufacturer in test conditions or by calculations. The failure mechanism of the protection element must be provided to the design team and studied in order to ensure that it will not cause more damage than an unprotected façade.

Pre-fabricated wall elements and curtain wall systems are the dominant construction systems in modern countries. In Singapore, the trend towards industrial construction of prefabricated walls, beams and column is prevalent. These guidelines will focus on these construction systems.

The guidelines cover basic design principles and materials that are commonly used in Singapore. If a proposed building system or product design is not mentioned in the guidelines, refer to the recommended protection level for the closest relevant system or design whilst applying engineering best practices. The developer should also consult a qualified protective design/blast consultant.

BUILDING WALLS

Figure 18: Example of external wall with exposed column line - poor design

Envelope walls play many architectural and functional roles. In some cases they form the main structural support for the building. In this section, the protection roles of the building envelope walls and the need for the addition of special protection elements will be discussed.

The main protection and security functions of the envelope walls are:

i. Securing the interior of the building against silent or forced entry.

ii. Protecting critical assets and occupants inside the building against blast loads, bullets and shrapnel.

iii. Concealing activities inside the building from external hostile surveillance.

Good design principles for envelope walls include the following:

- External walls should not be designed with recesses, as recesses may amplify blast loads (Fig 19 and 20).
- Columns should be oriented so the stronger axis will resist the likely direction of the blast.
- Avoid exposed external columns or transfer beams as they are easily targeted (Fig 21 and 22).
- Avoid tying**?** the external walls with the columns as they will transfer blast loads to the columns and may cause progressive collapse of the building.

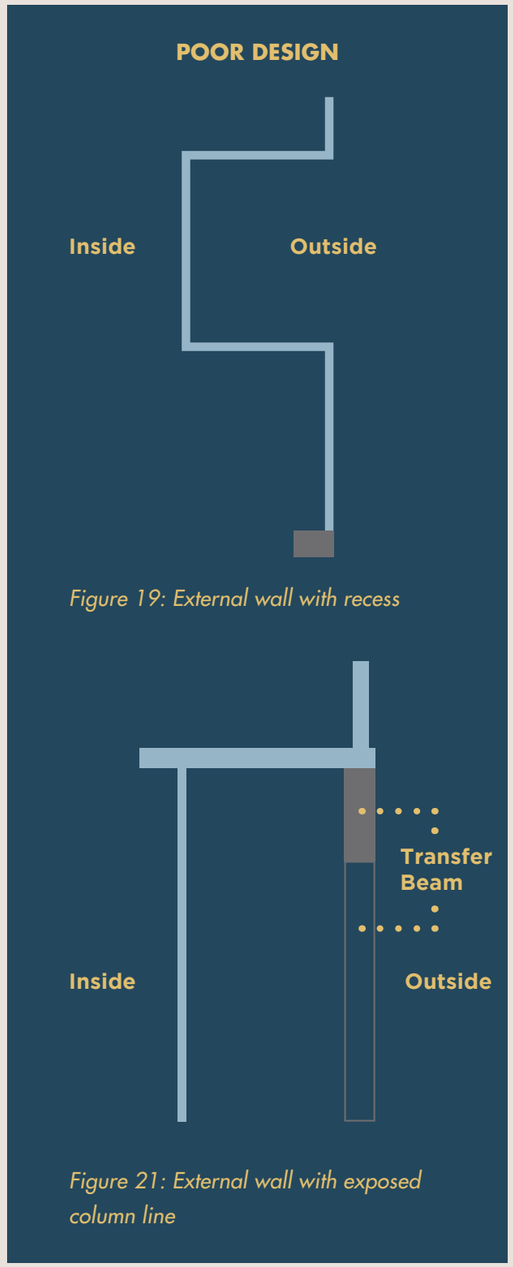


Figure 19: External wall with recess

Figure 21: External wall with exposed column line

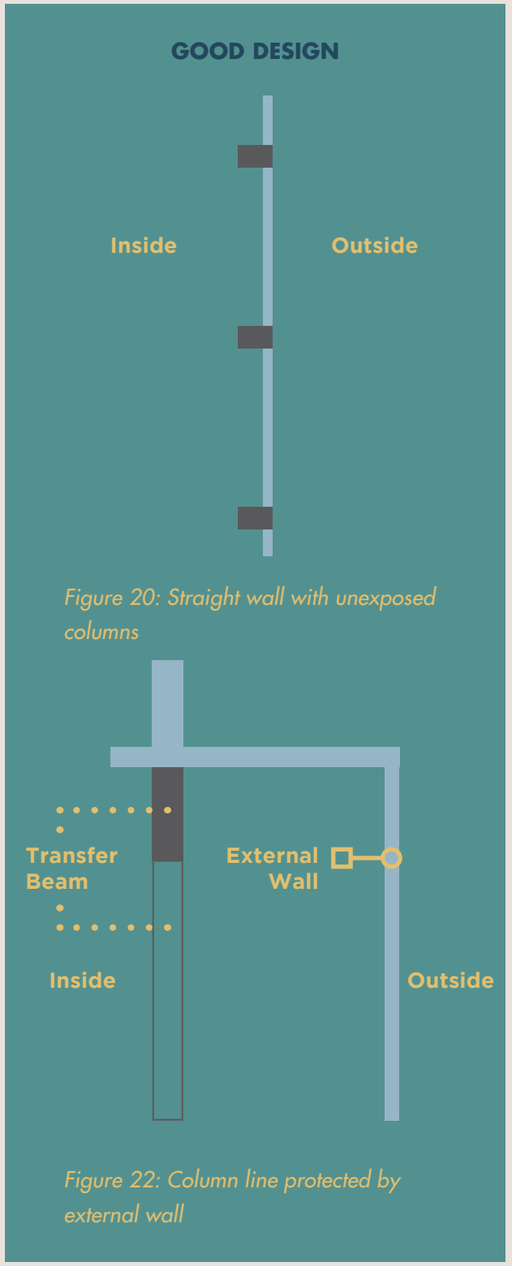


Figure 20: Straight wall with unexposed columns

Figure 22: Column line protected by external wall

LOAD BEARING WALLS

In-situ reinforced concrete walls are the most cost-effective method of protection against blast loads in the building industry. While modern construction methods favour the use of pre-cast over cast-in-situ reinforced concrete walls, pre-cast walls are comparatively weaker at resisting blast loads at the joins where they connect with other pre-cast elements. It is therefore preferable to go for cast-in-situ construction where protection for high blast loads is required.

Figure 23: Building constructed from pre-cast elements

Design of Load Bearing Walls

The recommended general design criteria for load bearing walls should include the following:

BLAST RESISTANCE

The load bearing wall must be able to withstand the expected blast load, and preferably in excess of the expected load. The structural engineer should work with a professional blast consultant / engineer to design structural components that meet the project's requirements.

FORCED ENTRY

If the connection details and the section properties are planned correctly, a load bearing wall can provide a high level of forced entry protection. The most vulnerable parts of the wall are the openings for windows, doors and utilities where the forced entry protected coverings should be considered.

CURTAIN WALLS AND GLAZING

Curtain walls and glass windows are important architectural and functional components of a building. However, in the event of an accident, natural disaster, or terrorist attack, they can fragment and cause serious injuries. A professional protective design/blast consultant/engineer should be engaged if the design needs to resist blast loads.

Good design principles for curtain walls include the following:

- Use fully framed curtain walls. Non-fully framed walls (e.g. point-supported walls) concentrate blast loads on support elements, which are more likely to fail.
- If a non-fully framed curtain wall is used, mitigating measures like laminated glazing and a catcher system will reduce fragmentation and hence casualties.

FULLY FRAMED GLASS CURTAIN WALL

Glass is relatively fragile compared to other building materials. In the event of an explosion, attempt at forced entry or small arms fire/fragmentation, flying glass debris from the damaged façade can cause many casualties. This is known as secondary fragmentation. It can be effectively controlled by using protective glazing materials.

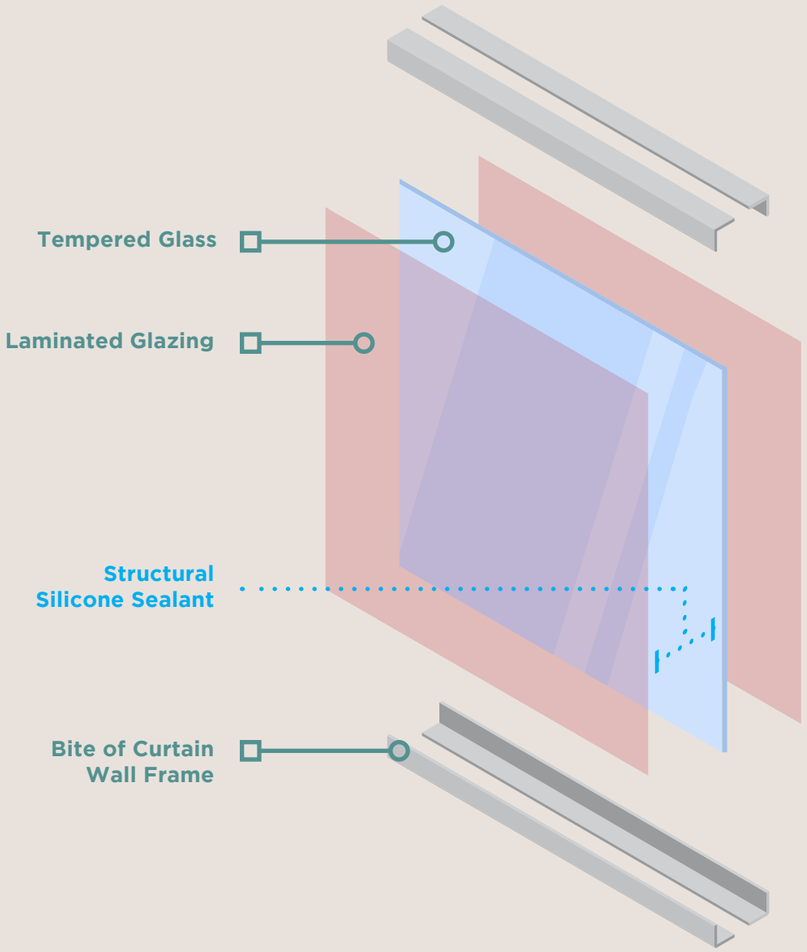
Protective glazing should be considered for all exterior windows/curtain walls where blast overpressures, shrapnel and projectiles could be of concern. For example, skylights and key locations such as the ground floor/lobby, and other densely populated areas.

This can dramatically reduce the risk of secondary fragmentation, depending on the type of glazing used.

Figure 24: Example of fully framed curtain wall

Design of Fully Framed Glass Curtain Walls

Laminated glass is recommended over other types of glass for its resistance to blast loads and its ability to hold the glass fragments in in a single sheet after the glass fractures. Good design practices include to:



- The overlap between the glass and its frame should be as large as possible. This will prevent the damaged laminated glazing sheet from flying free and becoming a large projectile.

- Glue the laminated inner glass to the framing members with a four sided structural silicone adhesive, preferably a two-part “shop glazed’ application of structural silicone. This will enable the polyvinyl butyral (PVB) laminated membrane to act as a blast shield and prevent the shattered outer glass from flying into the inside of the building. It will also prevent the glazing from detaching from the frames and allow the system to fully realise the energy absorbing capacity of the glass.

- Insulated glazing panels (thermo-panels) can also be very effective if interior laminated glazing is used and fixed to the mullions of the curtain walls with structural silicone sealant. The laminated glazing should be made out of heat strengthened glass. With thermo panels, the outer pane is considered a sacrificial element and adds to combined protection level of the glazing.

- Using non-laminated glass is not recommended when resistance to fracturing is needed. Fully-tempered glass fractures into pebble-sized pieces which pose a fragmentation risk at high velocities resulting from a blast. Annealed or heat-tempered glass is weaker than fully-tempered glass and shatters into sharp fragments when it fractures.

POINT SUPPORTED OR OTHER CURTAIN WALL SYSTEMS

Figure 25: Example of a point supported curtain wall

Figure 26: Example of a point support

Glass facades which are not fully framed are attached to the building structure with metal hangers that are connected to the glass by point supports.

These systems provide relatively poor protection levels. Point supported systems are not capable of withstanding high blast pressure loads. The supports concentrate the blast forces at the four corners of the glazing. As a result, there are large stress concentrations in the glass corner supports. Instead of absorbing energy (by bending), the components of point supported systems can detach and become large, high-energy projectiles. These types of glass facades do not provide a high level of protection against forced entry.

Design of Point Supported Curtain Wall Systems

If the use of a non-fully framed glass curtain cannot be avoided where higher levels of protection are needed, it must be complemented with special designs and glass systems.

For example, using laminated glass with a catcher system installed behind the glass, which will stop fractured panels and corner supports from becoming flying projectiles.

STONE OR METAL FINISHED LIGHT WALLS

Figure 27: Stone wall design

Translucent or decorative walls, constructed of light stone, metal or other similar finishes, are often used in modern buildings. These wall systems are relatively weak and provide little protection against most threats including blast or forced entry. There are two major ways to enhance its protection capabilities:

i. Choosing stronger materials and connection details.

ii. Add an extra layer of protective material behind the outer façade. This can be designed to look like a decorative feature (e.g. wooden bars or steel mesh).

Design Considerations of Stone Finished Light Walls

A stone or metal panel façade can withstand blast or forced entry by installing a steel or concrete backing together with appropriate connections. This system can be designed to withstand an expected blast load, and should be tested either by a laboratory or using calculations/simulations. As the protection elements can be installed on the interior of the façade, it will not interfere with the exterior aesthetics of the building.

If material which can easily fragment is used (e.g. stone panels), the backing elements should also serve to catch any fragments created by a blast. In general, such materials are not recommended for locations where large numbers of people gather.

BLAST PROTECTED WINDOWS

Protective windows and glazing can reduce (or prevent) casualties and damage if an explosion occurs outside the building. Glass can shatter into secondary fragments which can be hazardous due to their velocity and shape. This can be effectively controlled by means of protective glazing materials. Typically, as the level of blast protection increases, so does the level of forced entry resistance and ballistic protection, in addition to the expected life span of the product.

Good design considerations for windows include:

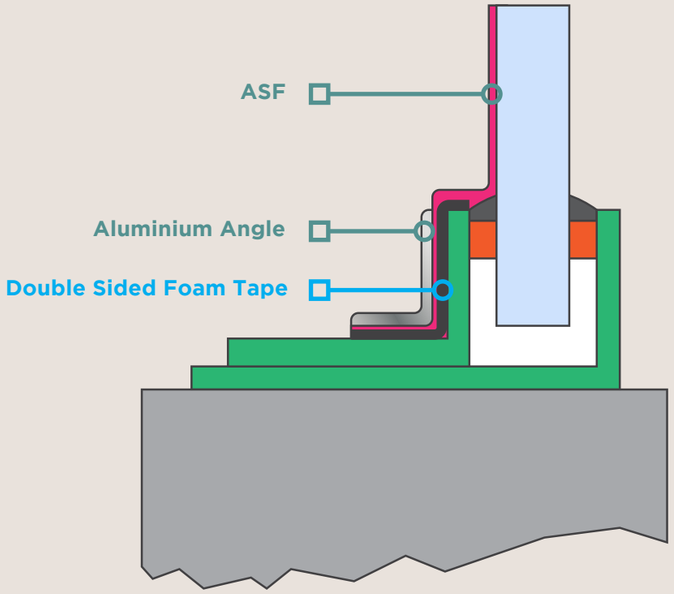
- Minimise the number of windows that can be opened, except when required for emergency or maintenance use. Fixed windows provide a higher level of protection, and could be designed as an integral part of a curtain wall system, a glass façade between slabs, or applied as an integral part of pre-fabricated wall panels.
- Windows that can open should be installed in areas that are not easily accessible from the outside. They should also be locked with a key-operated locking device from the inside. A good locking mechanism includes multiple locking and anchoring points.
- Avoid externally exposed hinges, pivot fixing screws and window frames. If used, they should be non-removable from the outside. BS 8220-2 provides recommendations on general security of windows including specific instructions on the installation of locks and bars to the window structure.
- Bars or grilles fixed to the window structure can provide additional security against forced entry. They can also serve as debris catchers for fractured laminated glass panels in an explosion.
- If blast resistant windows are used, they must be certified and installed according to the certified method, using clear and approved construction drawings. Windows on lower floors are generally subjected to higher blast loads which are likely to originate from the ground level. Although most blast protected commercial windows are fixed, some can be opened for maintenance or in case of emergency.

Standards for Glazing Protection

The U.S. General Services Administration (GSA) blast protection criteria have been adopted by the Interagency Security Committee (ISC) and are the most widely recognised classifications of design levels for glazing hazard protection (see table below).

Table 1: GSA/ISC performance conditions for windows system response

Performance Condition	Protection Level	Hazard Level	Description of Window Glazing Response
1	Safe	None	Glazing does not break. No visible damage to glazing or frame.
2	Very High	None	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a	High	Very Low	Glazing cracks. Fragments enter space and land on floor no further than 1 metre from the window.
3b	High	Low	Glazing cracks. Fragments enter space and land on floor no further than 3 metres from the window.
4	Medium	Medium	Glazing cracks. Fragments enter space and land on floor and impact a vertical witness panel at a distance of no more than 3 metres from the window at a height no greater than 60 cm. above the floor.
5	Low	High	Glazing cracks and window system fails catastrophically. Fragments enter space impacting a vertical witness panel at a distance of no more than 3 metres from the window at a height greater than 60 cm. above the floor.



Design of Blast Protected Windows

The ability to resist loads is a function of:

i. The connection of the window to the supporting frame.

ii. The connection of the glazing to the frame of the window.

iii. The type of glazing.

The supporting frame can be a reinforced concrete wall element or equivalent. The window frame can be constructed from materials including aluminium, HPVC or steel. If a window can be opened, the ability to transfer loads from the frame of the window to the supporting frame of the building depends on the locking mechanism. In most commercial windows, the ability of the locking mechanism to resist blast loads is very limited.

Laminated glass is recommended over other types of glass for its resistance to blast loads and its ability to hold the glass fragments in in a single sheet after the glass fractures. The panels should be adhered to the frame of the window with structural silicone sealant.

Insulated glazing panels (thermo-panels) can be very effective if interior laminated glazing is used and fixed to the frame of the window with structural silicone sealant. In this case, it is recommended that the laminated glazing will be made out of heat strengthened glass. With thermo panels, the outer pane is considered a sacrificial element but testing has proven that the external glass adds to the protection level of the glazing

If it is not feasible to install windows which are designed or tested against blast, anti-shatter film (ASF) may be used to retrofit existing windows. This can reduce the hazard resulting from a blast by holding glass fragments together if the glass fractures. Securing the anti-shatter-film to the frame with a mechanically connected anchorage system further reduces the likelihood of the glazing system becoming a projectile. Mechanical attachment includes anchoring methods that employ screws and/or batten strips that anchor the film to the frame along two or four sides.

Examples of Design

Figure 28: Cable protected window for low blast levels (before explosion)

Figure 29: Cable protected window for low blast levels (after explosion)

Figure 30: A window protected by mechanically anchored ASF for basic blast level (before explosion)

Figure 31: A window protected by mechanically anchored ASF for basic blast level (after explosion)

BALLISTIC PROTECTED WINDOWS

Figure 32: Ballistic window cross section

There are many commercially available ballistic protected windows which meet different protection levels. Only windows which have been successfully tested and certified by an official laboratory should be used. They must be installed according to the certified method, using clear and approved construction drawings. This includes both the glazing and frame. Special care should be taken at the connection of the ballistic protection, the wall and its supporting frame.

Figure 33: Tested sample of framed window for high level of ballistic resistance

Figure 34: Ballistic windows

Design of Ballistic Protected Windows

The most common method of providing ballistic protection in windows is by combining thick glazing with steel plates which are used to protect the connecting details to the supporting frame. Some commercial windows use aluminium or ceramic materials instead of steel plate.

Most commercially available ballistic protected windows are fixed. Some can be opened either for maintenance or in an emergency. Fixed windows are recommended because the connection detail to the supports only requires one frame. Windows which can be opened usually require two frames – one for the glazing and one for the connection to the supporting element. While tilt, tilt/turn or sliding windows are available, such windows will only provide full protection when the windows are closed and locked.

Ballistic protected windows can be used as an integral part of a curtain wall or a pre-fabricated wall system.

Where possible, it is recommended to use them as part of a pre-fabricated concrete panel or in-situ reinforced concrete wall. The connection detail between a ballistic protected window and a reinforced concrete opening is relatively simple, with minimal gaps/holes. The connection detail to a structural steel frame is also straightforward. However, designing an appropriate connection detail for a standard curtain wall is difficult and in general not recommended.

Standards for Ballistic Protected Windows

International standards for testing ballistic resistant windows include EN 1063 European Standard for Testing Bullet Resistant Glass, and NIJ Standard – 0108.01 Ballistic Resistant Protective Materials.

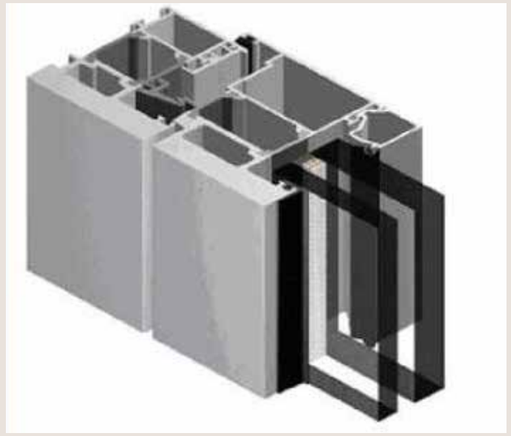


Figure 35: Bullet-resistant window and door construction

FORCED ENTRY RESISTANT WINDOWS

Forced entry resistant windows are necessary to secure a building. Especially if the windows are easily accessible from the outside (e.g. on the ground level). Modern forced entry resistant windows can be designed with no visible bars or protection elements by using glass (laminated or polycarbonate) with specially designed frames and locking mechanisms.

There are many commercially available forced entry resistant windows that are certified to various protection levels according to established international standards. The windows must be installed according to the certified method, using clear and approved construction drawings. Special care should be taken at the connections between the wall and its supporting frame, and between the window frame and the wall frame.

Design of Forced Entry Resistant Windows

The most common method of providing forced entry resistance in windows is by combining the glazing itself, the connection details between the glazing and the sub-frame, and the locking mechanism to the frame of the wall (in the case of opening windows). The protective components of the forced entry windows should be tested and approved by an accredited laboratory. The test report must include certificates for the glazing and the locking mechanism (in the case of opening windows) and the wall connection of the frame.

Forced entry resistance is tested in accredited laboratories, by professional technicians with a predefined set of tools (manual and electric). Each protection level is defined using a set of tools and time limits which the technicians have to breach a window of a predetermined size.

Forced Entry Standards

The required level of forced entry resistance should be determined based on the following considerations:

i. Accessibility of the window in terms how long an intruder can work to gain entry without being disturbed, and how easily it can be accessed.

ii. Importance of the site.

iii. Time taken for first responders to arrive.

International test standards for forced entry resistant products include European Standards EN 1627, EN1628, EN 1629, EN 1630 and EN 356; and American Standards ASTM F476, ASTM F588, ASTM F842, ASTM F1233 and ASTM F3038. Another standard, the US DOS SD-STD-01.01, is intended for use by US Department of State in its facilities throughout the world.

The Fire Code stipulates that for buildings (except residential buildings) exceeding 10m in habitable height, access openings on the external wall shall be provided for external fire-fighting and rescue operation. If the access opening is in the form of window, door, wall panel or access panel, one must be able to readily open the access opening from the inside and outside. Please advise the QP/owner to seek waiver from SCDF if the above requirement cannot be complied with.

Most commercially available forced entry resistant windows are fixed. Some can be opened either for maintenance or in an emergency. Fixed windows are recommended because the connection detail to the supports only requires one frame. Windows which can be opened usually require two frames – one for the glazing and one for the connection to the supporting element. While tilt, tilt/turn or sliding windows are available, such windows will only provide full protection when the windows are closed and locked.

Forced entry protected windows can be used as an integral part of a curtain wall or a pre-fabricated wall system.

Where possible, it is recommended to use them as part of a pre-fabricated concrete panel or in-situ reinforced concrete wall. The connection detail between a ballistic protected window and a reinforced concrete opening is relatively simple, with minimal gaps/holes. The connection detail to a structural steel frame is also straightforward. However, designing an appropriate connection detail for a standard curtain wall is difficult and in general not recommended.

Forced entry protected windows can be used as an integral part of a curtain wall or a pre-fabricated wall system.

STEEL GRILLE

It is common to protect windows against forced entry by adding steel grilles. Although it may not be aesthetically pleasing, they are a cost effective solution that provides protection when the window is open. The grille including its connection details should be designed in accordance with the forced entry standards.

Figure 36: Window before forced entry testing

Figure 37: Testing of 15 minutes forced entry resistant window

Figure 38: Testing of 15 minutes forced entry resistant window

Figure 39: Inside view of window after test

COMBINED PROTECTION OF WINDOWS

Windows can be designed to provide any combination of ballistic, blast and forced entry protection. They must be specifically designed for the combination required. It should not be assumed that protection against one kind of threat also offers protection against others.

For example, windows on the ground floor can be designed to resist blast loads as well as forced entry and ballistics. Another example of a combined system is a forced entry grill installed behind blast protected windows. The grill provides both forced entry protection and can be used as a catcher system against high blast loads.

Most protected windows can be designed with all three protection capabilities. In some cases, for comparable cost and aesthetics as compared to options that protect against fewer threats. Therefore, it is advisable at the design stage to explore multi-protection windows, even if only one protection type is needed.

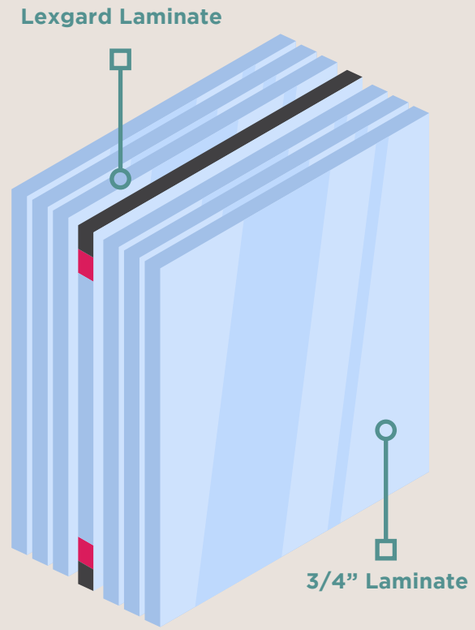


Figure 40: Bullet and blast resistant glazing system

Figure 41: Window before explosion

Figure 42: Window after explosion

DOORS

External doors are used mainly for pedestrians, cars and cargo to enter the building. They can be transparent (made of glass or other material), single or double and in any shape or size. Doors are an important factor in the overall protection of the building, especially against forced entry threats. Doors are less important for envelope protection against blast or ballistic threats, since they cover only a very small percentage of the façade. They do, however, have a major role in the protection of the most vulnerable locations of the building. The main protection and security roles of doors are:

i. Protecting the inner parts of the building against silent or forced entry.

ii. Protecting the inside of the building against blast loads, bullets and shrapnel.

iii. Preventing splinters or shrapnel from building materials from hitting people inside.

iv. Controlling access to the building.

In general, the number of external doors should be minimised to restrict potential intrusion points subject to emergency egress requirements.

Good design considerations for doors include:

- Solid wood core or metal doors provide greater security than those containing glazed viewing panels.
- Doors should open outwards towards the direction of the possible threat. The frame can then support the door against forced entry or blast effects from the outside. With this design, the hinges need to be hardened against tampering as they will be outside.
- The frame and wall attachments should be hardened to the same level as the door.
- Doors should be secured from the inside rather than outside where possible. This protects the locking devices from tampering.

Standards for Security of Doors

BS 8220-2 and UFC 4-010-3 provides guidelines in the security of doors including construction, installation and locking configurations.

BLAST RESISTANT DOORS

There are many commercially available blast doors that are tested to various blast loads according to established international standards. The blast resistant doors must be installed according to the certified test method, using clear and approved installation drawings.

Blast resistant doors should be considered for all exterior doors where blast overpressures may produce conditions hazardous to people behind them. As blast protected doors are relatively costly and difficult to design, that should only be installed at rooms or spaces requiring protection from blast (e.g. rooms holding critical assets or areas of mass congregation). Otherwise, a catcher system could be used to prevent the non-blast resistant doors from becoming flying projectiles and causing injuries or fatalities in the event of an explosion.

Blast resistant doors may be hinged, sliding, double-leaf or other accepted designs. Doors can be set in concrete walls, installed as part of a curtain wall design (typically made of glass), installed as part of a special steel wall, or used in many other ways to complete the overall protection of the façade.

Blast resistant doors should be considered for all sensitive locations such as the security control room, safe areas and VIP rooms as they will substantially reduce the risk to occupants and equipment in the facility.

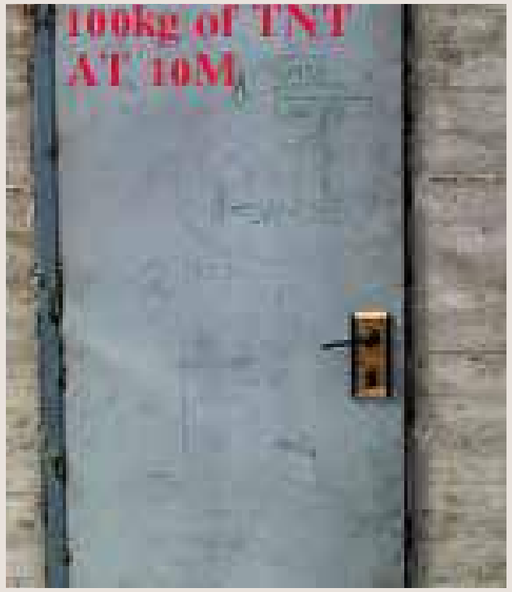


Figure 43: Blast resistant door after a 100kg explosion at 10m

Blast protected doors should be considered for all sensitive locations such as the security control room, safe areas and VIP rooms as they will substantially reduce the risk to occupants and equipment in the facility.

Design of Blast Resistant Doors

Blast resistant doors typically open outwards and are supported by the frame against positive pressure from a blast. The blast resistant door must include installation details on how the door should couple with the wall design. The wall and door connection systems should be designed to be able to withstand the same or greater blast loads as the door.

Figure 44: Steel bars used as a catcher for the doors

BALLISTIC RESISTANT DOORS

Ballistic resistant doors are typically used at the entrances to special locations in a building, or at specially protected buildings which may come under armed attack. Typical locations for ballistic resistant doors include the external guard's booth, security control room, treasury room and interlocking room at the entrance to a secured area or building.

There are many commercially available ballistic doors that are tested to various protection levels according to established international standards. The test report should include detailed installation drawings so that the doors could be installed properly and work as intended. Special care should be taken with the ballistic protection at the connections between the wall and its supporting frame. If the installation is not done in accordance to the detailed installation drawings that include clear details of the protected connections, the door may not performed as well as intended. This should also include the handles, peep hole and others, which should be tested and approved by a certified laboratory.

Ballistic doors can be used as an integral part of a curtain wall or a pre-fabricated wall system. In general, it is recommended to use them as part of a pre-fabricated concrete panel. The connection detail between ballistic protected doors and a reinforced concrete opening is relatively simple, with minimal gaps/holes. The connection detail to structural steel frame is also straight forward.

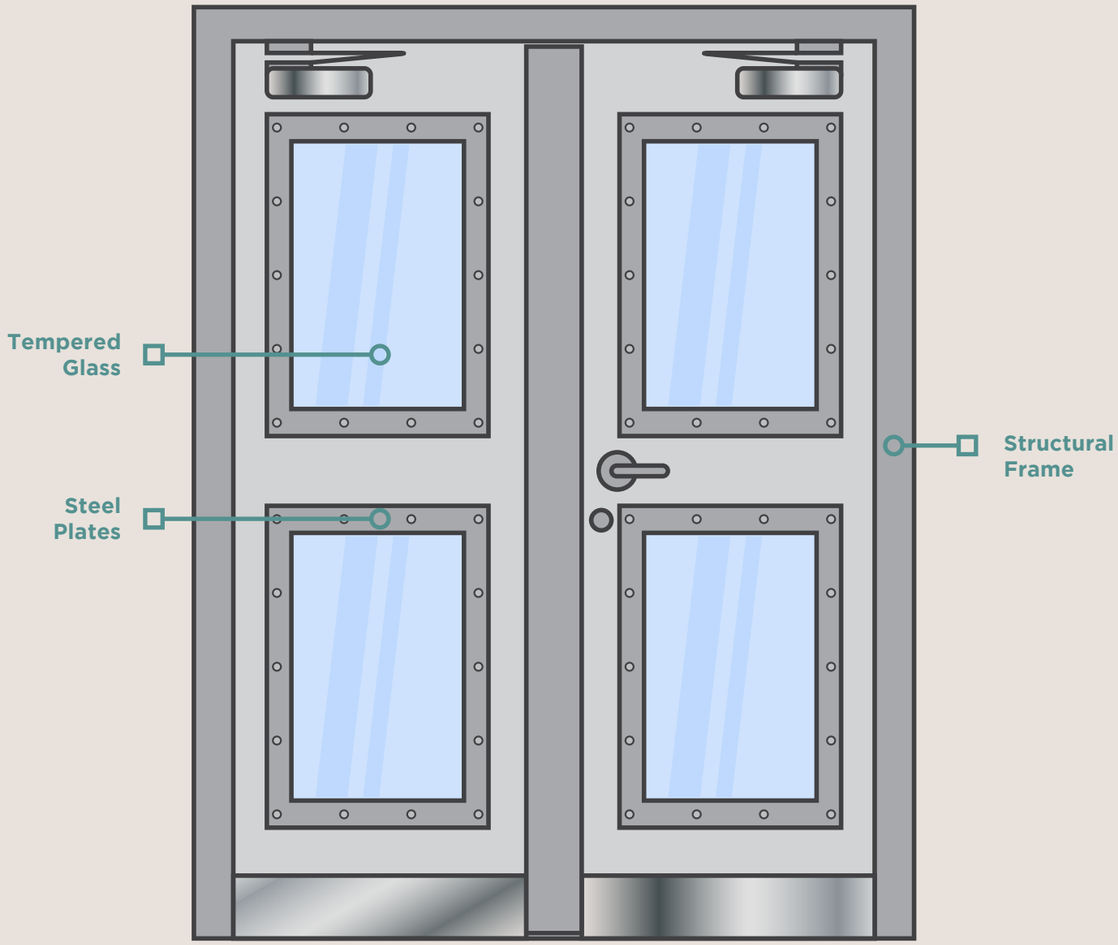
Design of Ballistic Resistant Doors

The ballistic door must be supplied by the manufacturer with the complete instructions for installing it in the designated wall.

The most commonly used protective material in ballistic doors is steel plates. The test report must include certificates for the steel and the frame to ensure that the same products are installed in the site. Ballistic protected doors with glazing should be treated like ballistic protected windows.

Standards for Ballistic Resistant Doors

International standards for testing ballistic resistant doors include EN 1523 and NIJ Standard – 0108.01 Ballistic Resistant Protective Materials.



FORCED ENTRY RESISTANT DOORS

Every door offers some level of forced entry resistance. In general, a higher protection level will be required at the outer envelope doors or at special locations (e.g. those which contain critical assets). The required level of protection may be lower for doors contained deeper in the building after many layers of security.

There are many commercially available forced entry resistant doors that are tested to various protection levels according to established international standards. The forced entry resistant doors must be installed according to the certified test method, using clear and approved installation drawings. Special care should be taken at the connections between the walls and the door's supporting frame.

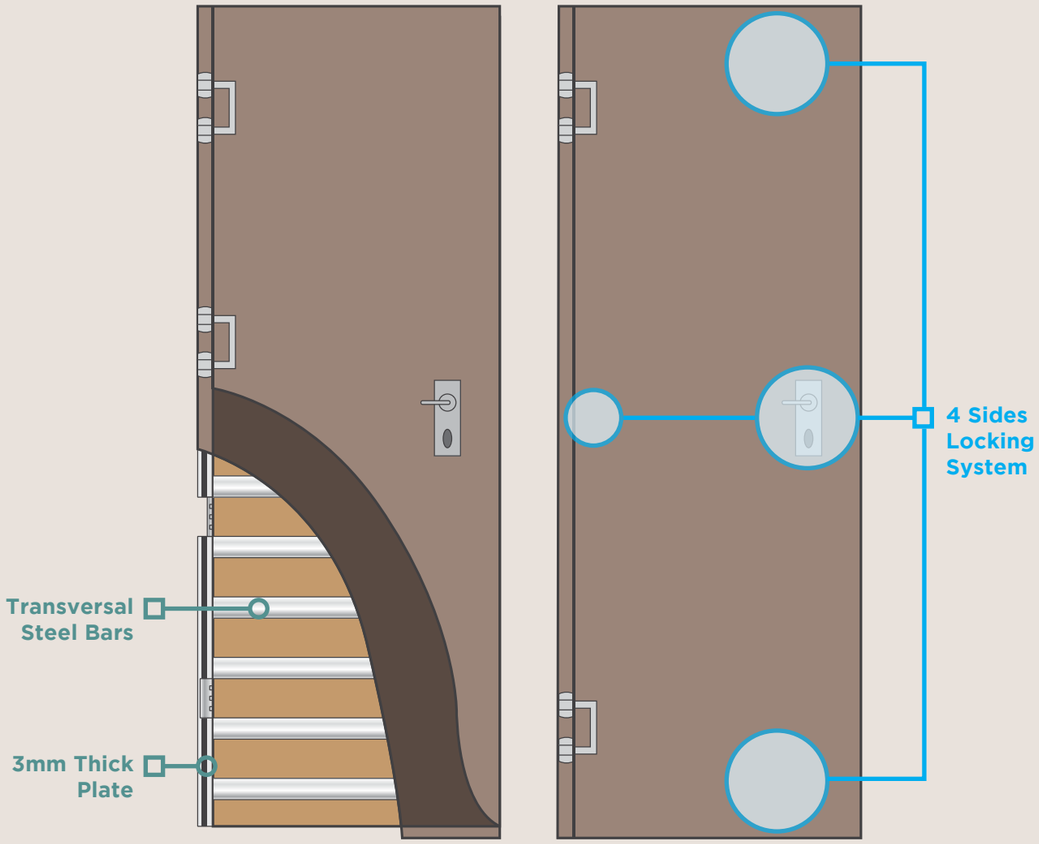


Figure 45: 15 minutes forced entry resistant door

Design of Forced Entry Resistant Doors

The most common material used to protect a door against forced entry is steel which is extensively used in the plates, ribs and frame. The strength of the connection between the door panel and the supporting frame is achieved by the locking mechanism. The test report must include certificates for the steel components and the locking mechanism.

Forced entry resistance tests are conducted in accredited laboratories, by professional technicians with a predefined set of tools (manual and electric). Every protection level has a different set of tools and time limits by which the technicians have to create an opening of a predetermined size.

Forced entry protected doors can be used as an integral part of a curtain wall or a pre-fabricated wall system but in general it is recommended to use them as part of a solid concrete wall panel. The connection detail between forced entry protected doors and a reinforced concrete opening is relatively simple, with minimal gaps. The connection detail to a structural steel frame is also straight forward but the connection detail to a standard aluminium curtain wall is difficult and in general not recommended.

Standards for Forced Entry Resistant Doors

International test standards for forced entry include European Standards EN 1627, EN1628, EN 1629, EN 1630 and EN 356; and American Standards ASTM F476, ASTM F588, ASTM F842, ASTM F1233 and ASTM F3038. Another standard, the US DOS SD-STD-01.01, is intended for use by US Department of State in its facilities throughout the world. Also, BS 8220-2 and UFC 4-010-3 provides guidelines in the security of doors including construction, installation and locking configurations.

Figure 46: Test of door

COMBINED PROTECTION FOR DOORS

Figure 47: Ballistic and force entry resistant doors

Most protected doors can be designed with all three protection capabilities. Therefore, it is advisable at the design stage to explore multi-protection doors, even if only one protection type is needed.

Doors can be designed to meet combined levels of protection, for example entry doors in a secured building will typically be required to withstand forced entry, blasts and ballistics. They must be specifically designed for the combination required. It should not be assumed that protection against one kind of threat also offers protection against others.

Figure 48: Ballistic and force entry resistant doors

OTHER ACCESS POINTS

Apart from the protection of walls, windows and doors, the security of other access points in the building façade or protected office within a mixed use building needs to be considered to prevent intruders from gaining access through these points. Examples are roofs, ceiling, floors and infrastructure pipes.

ROOF

Access to the roof should be restricted. Service openings should be secured by bars or grilles and locked from the inside if possible. Roof glazing or skylights should be avoided where possible as they present weak points that an intruder can exploit for unauthorised entry or to introduce other threats into the building.

BUILDING ENVELOPE AIR TIGHTNESS

An airtight building envelope protects against unfiltered infiltration of contaminated air into the building. An airtight building also results in greater energy-efficiency and cost savings, as less cooled air is lost through the building façade.

Buildings designed with a continuous air barrier restrict air leakage into or out of the air-conditioned space. The air barrier materials for each assembly should be joined and sealed to the air barrier materials of adjacent assemblies while allowing for the relative movement of these assemblies and building components. The air barrier should form a continuous barrier around the building, with all gaps in the air barrier assembly sealed. The air barrier should be supported to withstand the maximum positive and negative air pressures that the building will be subjected to, and to last the anticipated service life of the building.

THE FOLLOWING TEST STANDARDS CONTAIN RELEVANT INFORMATION ON TESTING FOR BUILDING ENVELOPE AIR TIGHTNESS:

- ASTM E779
- ASTM E1827
- CIBSE TM23
- USACE
- NEBB
- British ATTMA
- ASHRAE 189.1

SECURITY SYSTEMS

Professional security consultants can perform a risk assessment and recommend a holistic security solution which combines technological systems, design and manpower solutions. This section provides a basic introduction to security systems for prospective clients and built environment professionals, so they can be well-informed when procuring and planning for security systems.

Security systems are usually used for the following purposes:

i. Detect illicit activities or intrusions.

ii. Warn designated security personnel of hostile activity and/or breaches of security to the building.

iii. Monitoring of activity in sensitive or vulnerable locations.

iv. Recording activities for future investigations.

v. Deterrence.

vi. Replacing or supporting human security resources for cost effectiveness.

vii. Assuring the proper function of physical security elements.

Security systems, unlike physical protection elements, have a relatively short life span before they become technologically obsolete (usually not more than 10 years). The building's infrastructure should be designed to allow security systems to be upgraded easily and in a modular way.

Security systems, in the context of the building's overall security plan, should be planned at the design-phase of the building. This will:

- Allow for coordination between design, manpower and technology. This can reduce operating costs of the building by using less security manpower, improve security by designing-out risks, and deliver better cost efficiency by reducing the need for retrofitting later.

There are a large number of security systems available. While it would provide an added level of assurance, it may not be necessary for projects with lower security demands to use systems that have been tested and approved by national laboratories or military institutions. There are a limited number of such certified systems available, and they are relatively costly.

Security systems, unlike physical protection elements, have a relatively short life span before they become technologically obsolete (usually not more than 10 years). The building's infrastructure should be designed to allow security systems to be upgraded easily and in a modular way.

The most common security systems are CCTVs and alarm systems. These should be incorporated in every modern building. These systems usually consist of:

i. End points, which are the systems' data gathering sensors (e.g. detectors, cameras, etc.).

ii. Base points, which receive and process all the input gathered by their system's end point (e.g. CCTV matrix, alarm system).

iii. Cabling, infrastructure and wireless channels.

Security systems can also be integrated with the facilities management systems of the building for greater efficiency.

SECURITY CONTROL ROOM

The security control room is the nerve centre of security operations for a building. It 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 a security incident has occurred.

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 monitoring capabilities only.

APPLICABLE STANDARDS FOR CONTROL ROOMS INCLUDE:

- SS 558:2010
- BS EN 50518-3:2013
- UL 827
- AS 2201.2—2004

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

System	Level
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 (with overriding authority)
Intercom	Sub-station
Fire Detection	Sub-station
Air-conditioning and Mechanical Ventilation	Sub-station (with overriding authority)
Security Lighting	Sub-station (with overriding authority)
Lift System	Sub-station

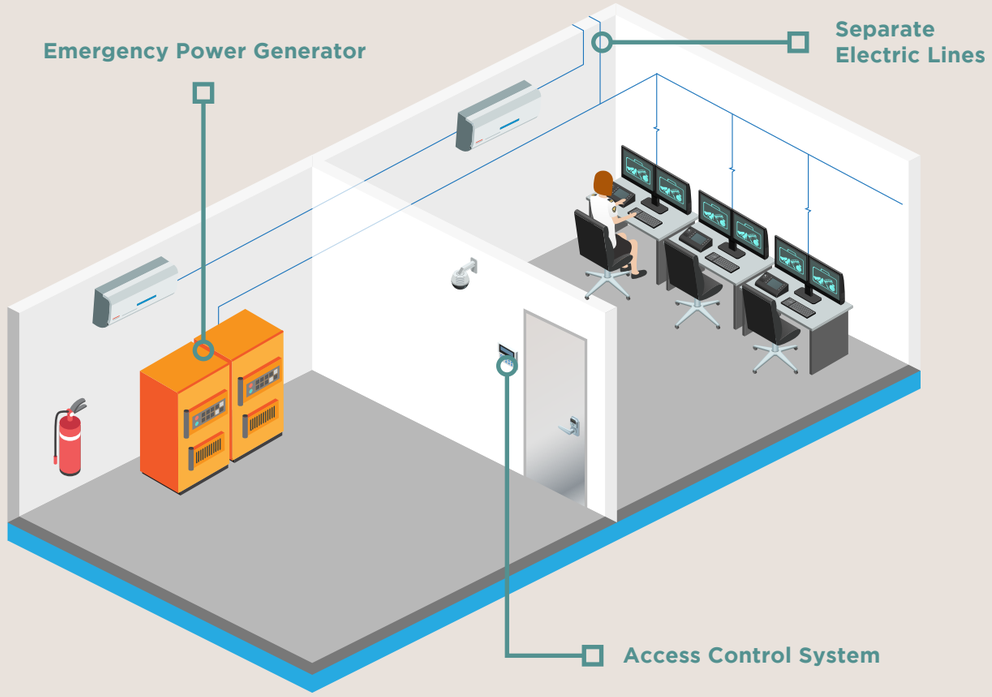
The security control room design must allow it to effectively manage both routine security and emergency situations. To do this, the security control room needs a clear situational picture. It needs access to data on any regular and irregular activities, crowd concentrations and security related incidents. The security control room must also prioritise and filter relevant information by prioritising inputs received from the security cameras and the alarm system in a way that can effectively differentiate real incidents from false alarms.

Additional functions of the security control room include:

a. Communicating information to staff and visitors in emergency situations.

b. Assisting and monitoring the evacuation of the building's occupants when necessary.

c. Supporting commanders and decision makers and first responders while they are performing their respective responsibilities.



Design of Security Control Room

The security control room is critical to a building's security and must be adequately protected against expected threats (e.g. forced entry, ballistics and explosives). The entrance to the security control room should be equipped with an access control system and forced entry protection.

Good design principles include:

- Designing the control room as a dedicated facility. It should not serve a dual function (e.g. also as an access control guard post).

- Having a direct connection to the building's management systems that are considered to be critical or security related (e.g. air conditioning and mechanical ventilation systems). This allows security control room staff to override or control these systems when the situation requires it.

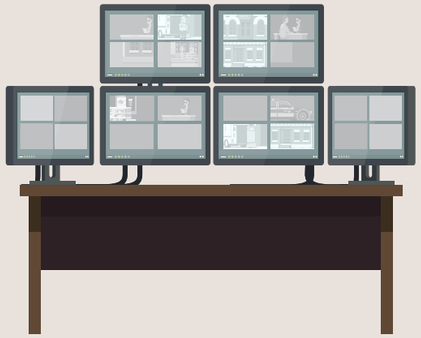
- Emergency power, lighting and backups of all critical systems to allow the security systems to continue operating during emergency situations (e.g. when the security control room is damaged or during a power failure).

- Lighting should not cause glare on monitor screens.

- Working surfaces should be positioned to allow operators to have a good view of the monitors.

- At least two separate power lines, with one dedicated to security systems while the other for administrative equipment.

- Dedicated phone line with a direct external line.
- Designate an area for administrative uses which should not interfere with the security control room's operations.
- Avoid water pipes running near the security control room and (where applicable) the adjoining equipment room.
- Raised floor to allow cabling.
- Fire extinguishing measures installed in the security control room and its adjoining equipment room (where applicable) must be designed for use in such facilities, and not cause damage to the electrical equipment.
- Electrical equipment used by the security control systems that are located in the security control room should be in an adjoining but separate room with appropriate climate control.



CCTV MONITORS & RECORDERS

Please refer to "Video Surveillance System (VSS) Standard for Buildings (dated 5 Nov 13)" published by Singapore Police Force for details on VSS requirements, video storage and other requirements.

ALARM

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.

INTERCOM & COMMUNICATION SYSTEM

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:

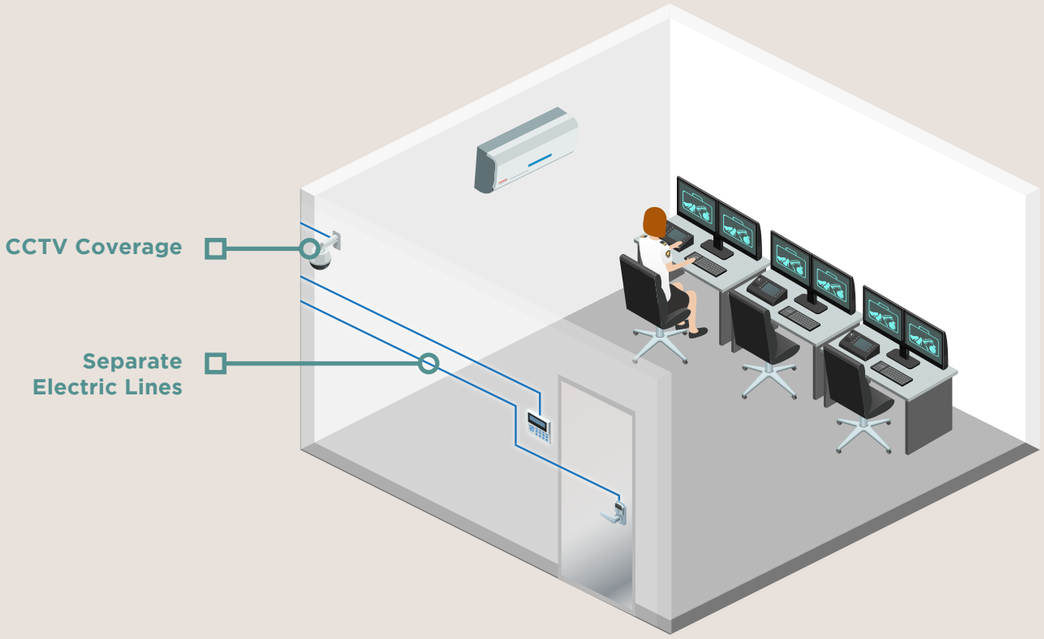
i. Standard point to point intercom system (party line systems).

ii. Matrix systems.

iii. Videophone systems.

iv. Wireless systems.

v. Telephone based systems and others.



Design of an Intercom & Communication System

The system's volume and background noise filtering levels should be set after taking into consideration:

- Noise levels of the operating environment (e.g. street vs a room).

- Average distance that the users will be from the unit while operating it (e.g. drivers in their cars vs at a pedestrian entrance).

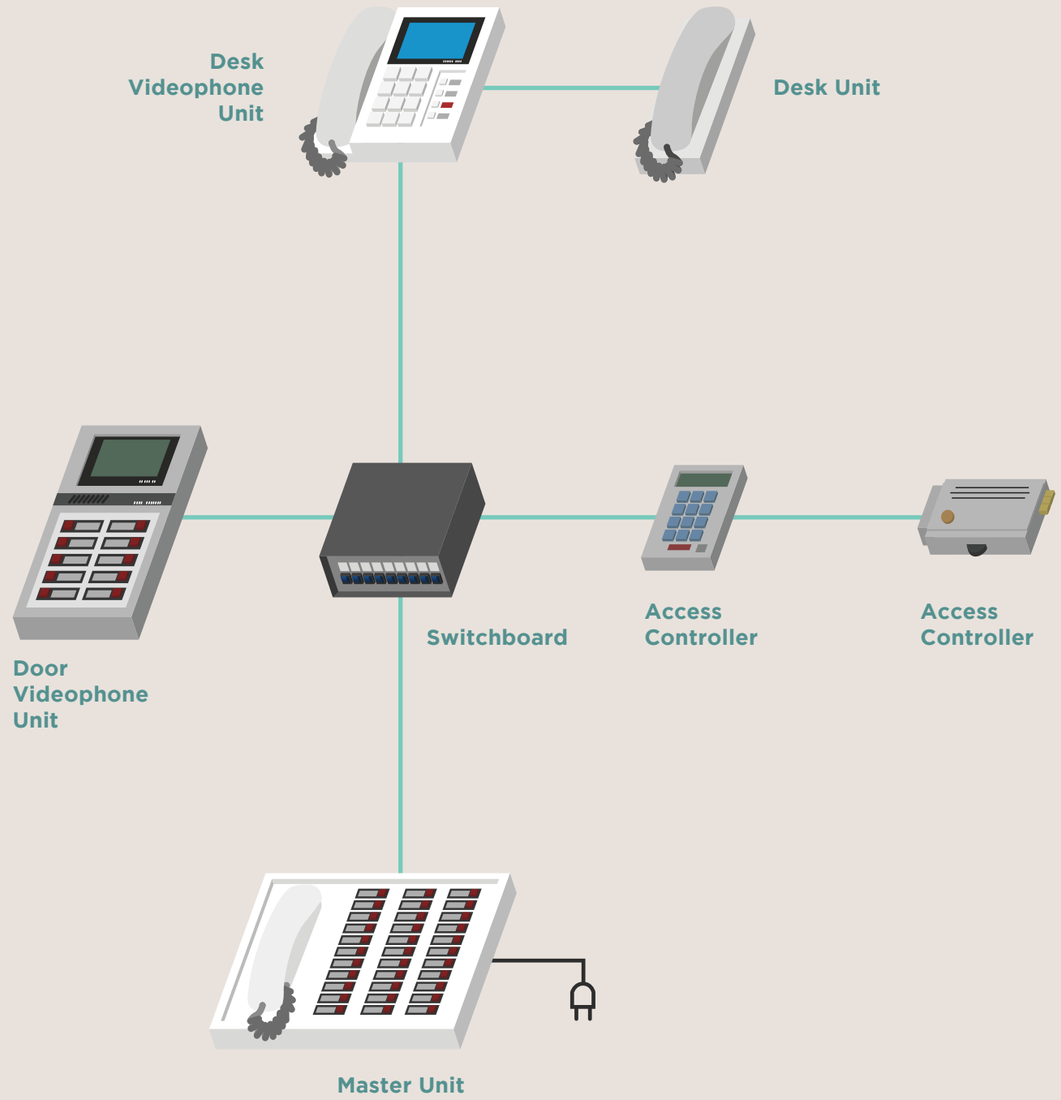
Combine intercom units employed for use in access control with CCTV coverage, and proper lighting. This will enable the security personnel to screen incoming persons in a more effective manner. Prior to deciding whether to use a specific intercom system for security purposes, it is important to check whether the levels of amplification and noise filtering are suitable for the building's environment.

Maintain proper separation between intercom lines and other electric lines to prevent interference. Ensure that all intercom systems installed are compatible with each other.

Most intercom systems need to be regularly maintained. Install them where this can be done conveniently. Exterior intercom units should be protected against environmental conditions such as temperature, humidity and rain, and should also include anti-vandalism measures.

Intercom units 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.

Figure 51: Typical point to point intercom system layout



PUBLIC ADDRESS SYSTEM

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:

i. Indoor / outdoor speakers

ii. Amplifier

iii. Microphone

iv. Area division panel (to be able to address parts of the building individually)

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 various scenarios.

The speaker coverage should be complete and cover every room. The system should be easy to operate in an emergency.

INTRUSION DETECTION SYSTEM

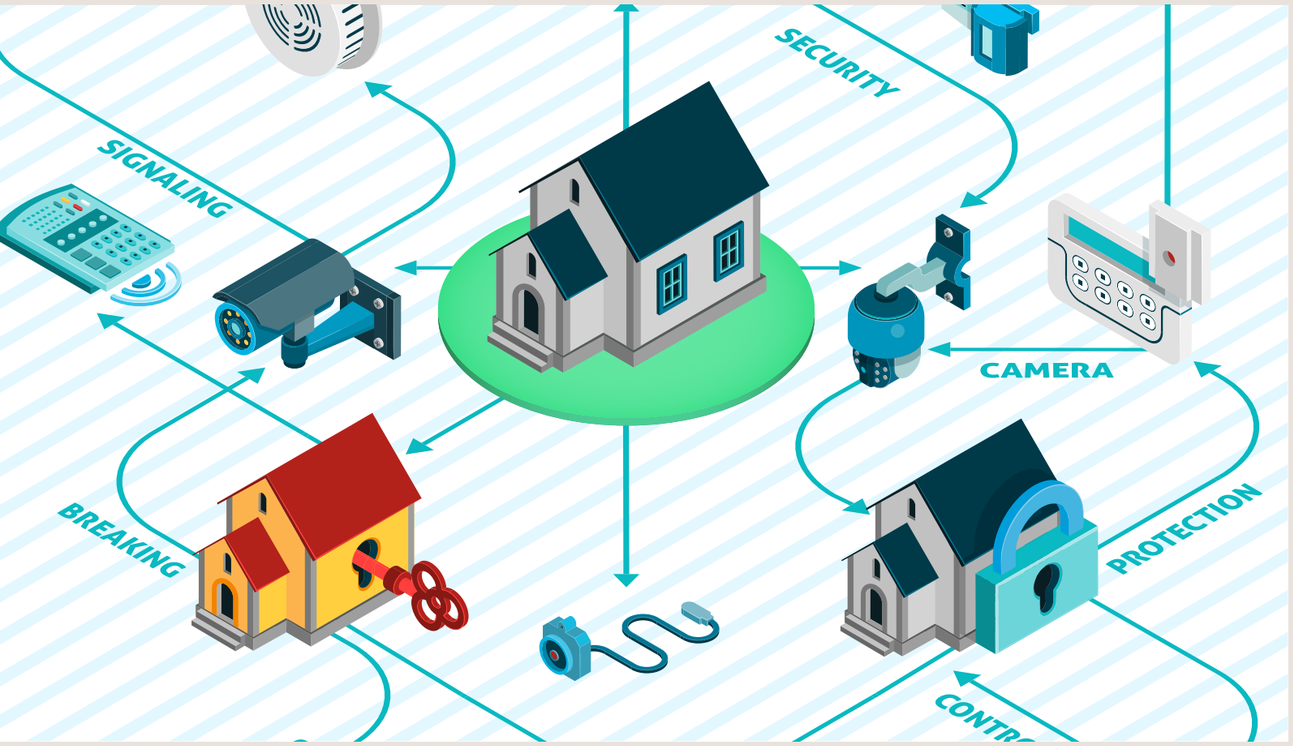
AN IDS WILL USUALLY CONSIST OF:

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

Intrusion detection systems (IDS) installed in buildings and/or complexes detecting both unlawful intrusion and lawful entry. These systems can be programmed to monitor various parameters such as opening of doors and/or windows; crossing of lines; movement in defined areas; shifts in temperature; change in lighting etc. The following are some examples of the various detector types:

Detector Technology	Description
Interior Detectors	
Balanced magnetic switch	Balanced magnetic switches use a magnetic field or mechanical contact to determine if an alarm signal is initiated (for example, if an access portal such as a door, window, or roof hatch has been opened). Compared to standard magnetic switches, balanced magnetic switches is more secure as it is resistant to tampering with magnetic field.
Glass break detectors	Glass break detectors can be deployed on components with glass such as windows and doors with glass panels. Technologies include acoustic detectors (listens for an acoustic sound wave that matches the frequency of broken glass), shock detectors (feels the shock wave when glass is broken), and dual technology detectors (senses acoustic and shock vibrations).
Passive infrared detectors	Passive infrared detectors pickup heat signatures (infrared emissions) from intruders by comparing infrared receptions to typical background infrared levels and are suitable for interior deployment.
Exterior Detectors	
Active infrared detectors	An infrared signal is transmitted via a transmitter and received by a receiver located elsewhere. Interruption of the normal IR signal indicates an intruder or object has blocked the path. These detectors can be installed in such a way as to be almost completely unobtrusive.
Microwave detectors	Microwave detectors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is received, and a base level "no intrusion" signal level is established. Motion by an intruder causes the received signal to be altered, setting off an alarm.
Interior/ Exterior Detectors	
Infrared beam detectors	Infrared beams can create an invisible line or lattice that when crossed, triggers an alarm in the command centre. These detectors are usually noticeable.
Step detectors	Step detectors are used to detect someone stepping on the top of a wall or laying a ladder against it. They are based on covered coils running along the top of the wall. When the cover bends as a result of the weight of someone climbing onto the wall, the detectors will send an alarm to the command centre.

Detector Technology	Description
Interior/ Exterior Detectors	
Step detectors	Step detectors are used to detect someone stepping on the top of a wall or laying a ladder against it. They are based on covered coils running along the top of the wall. When the cover bends as a result of the weight of someone climbing onto the wall, the detectors will send an alarm to the command centre.
Video Motion Detectors	Video motion detection is a video surveillance based system which analyses video footage and sends an alarm when intruders are detected.
Fence Line	
Taut wires	Taut wires are stretched along a fence and sound an alarm if the wires are cut, pulled or bridged (electrically). In some cases they can also provide a non-lethal electric shock. The taut wires may come be installed in a variety of configurations such as on the top, inside or outside of a wall.
Vibration detectors	Vibration detectors can be deployed on the fence line by installing sensors along the fence line to detect any vibration. An intruder trying to climb the fence will cause an alarm to be triggered in the command centre.
Coaxial Strain-Sensitive Cable Systems	Coaxial strain-sensitive cable systems use a coaxial cable woven through the fabric of the fence. The coaxial cable transmits an electric field. As the cable moves due to strain on the fence fabric caused by climbing or cutting, changes in the electric field are detected within the cable, and an alarm Is triggered.
Time Domain Reflectometry systems	Time Domain Reflectometry systems send an induced radio-frequency (RF) signal down a cable attached to the fence fabric. Intruders climbing or flexing a fence create a signal path flaw that can be converted to an alarm signal. When the conductor cable is bent or flexed, a part of the signal returns to the origination point. This reflected signal can be used to determine the intrusion point.
Fibre-optic strain-sensitive cable systems	Fibre-optic strain-sensitive cable systems are similar to the coaxial strain-sensitive cable systems. The fibre-optic system uses a fibre-optic cable woven through the fence fabric. Strain on the fence fabric causes micro-bending of the fibre cable, which is monitored by the control panel and triggers an alarm.



Design of an Intrusion Detection System

An IDS consists of several types of detectors. The type of detector to be used should be determined after all location (e.g. indoors, outdoors etc.) and environmental (e.g. humidity, temperature etc.) issues have been taken into consideration. Detectors with a relatively high false alarm rate should be avoided. A high false alarm rate makes it probable that a real alarm will be ignored. The input received from the detectors (e.g. different alarms for different amount of weight applied to weight sensors) should be calibrated in the alarm system. The display unit should provide clear information as to which zone and detector were set off.

IDS 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 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 different types of alarms at different situations (e.g. a buzzer during the day and siren at night). A dialler should be included so that it would be able to alert response forces in case of a breach. A siren or other alarm elements should be considered.

Magnetic or mechanical switches that are installed on window and door frames are effective tools to detect the unauthorised opening of windows and doors. However, they are not able to detect situations where the intruder gains entry by breaking the window glazing or creating a hole through the door. Cabling for alarm detectors should always be protected.
All external doors and external openings that can be accessed by the public should be fitted with detectors, including ground level openings and openings that can be reached by climbing.

A professional security consultant should advise the design of a building's IDS.

Standards for Intrusion Detection Systems

RELEVANT STANDARDS FOR IDS INCLUDE:

- BS EN 50131-1:2006 + A1:2009
- PD 6662:2012
- SS 558:2010
- AS/NZS 2201.1:2007
- UL 1076
- UL 609
- UFC 4-021-02

ACCESS CONTROL SYSTEMS

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. Key considerations are:

i. The number of entrances to the building/ installation should be minimised.

ii. Identifying and deciding areas to which access should be limited.

iii. The employed measures should not interfere with fire protection and safety systems.

iv. 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. The access control system (ACS) must be designed together with the other security systems.

Design of an Access Control System

All external doors that are used on a regular basis by authorised persons only require access control.

All access controlled doors should be equipped with an automatic door closing mechanism.

Main entrance doors should be equipped with an automatic locking mechanism that allow external guards to lock the doors if an emergency situation occurs outside. A door that is supposed to be protected against forced entry should be equipped with an electric lock that is fail-secure.

Standards for Access Control Systems

Relevant standards for ACS include BS EN 60839-11-1, UFC 4-021-02 and UL 294.

ACCESS CONTROL IS A COMBINATION OF PHYSICAL ELEMENTS AND SECURITY PROCEDURES, CONSISTING OF BUT NOT LIMITED TO THE FOLLOWING COMPONENTS:

- 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
- Automatic door closing mechanism

VIDEO SURVEILLANCE SYSTEM AND SECURITY LIGHTING

The primary purpose of a Video Surveillance System (VSS) is to support and enable the overall management of a building's security. VSS are an aid to security monitoring, especially of vulnerable or sensitive areas. VSS 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, VSS 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.).

Security lighting must be deployed to increase the visibility around perimeter lines, buildings, and sensitive locations. Proper lighting can greatly improve the combined operation of other security systems, particularly CCTV and other surveillance measures. It must be designed to complement these systems.

For guidelines on VSS and security lighting, please refer to "Video Surveillance System (VSS) Standard for Buildings published by Singapore Police Force. This Standard has been developed to provide a uniform and consistent approach to the specification, installation, operation and performance of VSS across buildings in Singapore.

As there are many VSS options available on the market, it is recommended to employ a professional consultant when designing VSS systems.

REGULATORY REQUIREMENTS

All relevant Singapore building codes, regulatory controls and standards must be followed. If there is a contradiction between these guidelines and the building code, the latter should prevail.

The Singapore Civil Defence Force should be consulted on the following during the planning stage of the building project so that:

i. Perimeter Line: Fire engines have to make use of public roads or internal access ways/ roads to conduct fire-fighting operations. Building facades where fire access openings are located shall not be more than 10m from the nearest edge of a public road or internal fire engine access way/road.

ii. Vehicle Security Barriers: VSBs should be placed such that they do not affect the access and manoeuvrability of fire engines during fire emergency.

iii. Fence & Blast Shielding Wall: should be placed such that they do not affect the access and manoeuvrability of fire engines during fire emergency.

Approval should be sought from all relevant government authorities including the Singapore Land Authority, Urban Redevelopment Authority, Land Transport Authority and National Parks Board before vehicle security barriers are installed.