Safety and Security Planning Manual
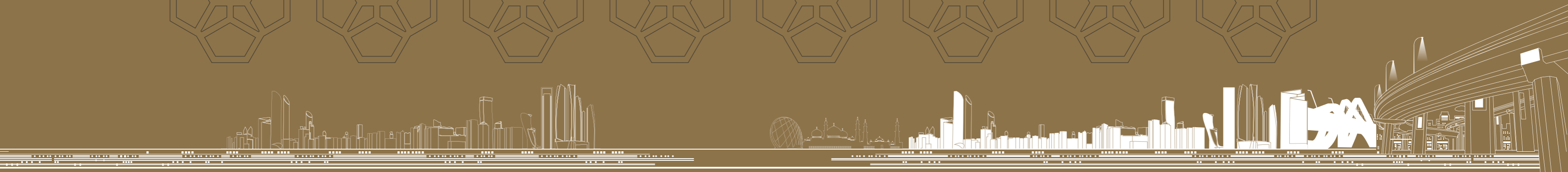
Abu Dhabi Safety and
Security Planning Manual
Version 01

His Highness Sheikh Khalifa bin Zayed Al Nahyan

President of the United Arab Emirates and Ruler of Abu Dhabi

His Highness General Sheikh Mohamed bin Zayed Al Nahyan

Crown Prince of Abu Dhabi, Deputy Supreme Commander of the UAE Armed Forces
and Chairman of the Abu Dhabi Executive Council

Contents

Mandate of the Abu Dhabi Urban Planning Council

The Abu Dhabi Urban Planning Council (UPC) was created by Law No. 23 of 2007 and is the agency responsible for the future of Abu Dhabi's urban and regional environments, and the expert authority behind the visionary Abu Dhabi 2030 Urban Structure Framework Plan published September 2007. Chaired by His Highness General Sheikh Mohamed bin Zayed Al Nahyan, Crown Prince of Abu Dhabi, Deputy Supreme Commander of the UAE Armed Forces and Chairman of the Abu Dhabi Executive Council, the Abu Dhabi Urban Planning Council defines the shape of human settlements in the Emirate, ensuring factors such as sustainability, infrastructure capacity, community planning and quality of life, by overseeing development in the cities and in the Emirate as a whole. The Abu Dhabi Urban Planning Council ensures best practice in planning for both new and existing settlements.

The Abu Dhabi Urban Planning Council's primary purpose is to deliver upon the vision of His Highness Sheikh Khalifa bin Zayed Al Nahyan, President of the United Arab Emirates and Ruler of Abu Dhabi, for the continued fulfillment of the grand design envisaged by the late Sheikh Zayed bin Sultan Al Nahyan, Father of the Nation, and the ongoing evolution of the Emirate of Abu Dhabi. By drawing on urban planning expertise from local Emiratis, throughout the Arab States of the Gulf, and around the world, the Abu Dhabi Urban Planning Council strives to be a global authority on the future of urban planning and design.

Building on the success of the Abu Dhabi Urban Planning Vision 2030, the Abu Dhabi Urban Planning Council is pleased to issue the Safety and Security Planning Manual (SSPM) for the Emirate of Abu Dhabi.

The Manual Vision:

To ensure the creation of safe and secure communities that enhance quality of life and reflect the Emirate's unique identity

The Abu Dhabi Safety and Security Planning Manual (SSPM) was commissioned by the Abu Dhabi Urban Planning Council (UPC) to guide the development of safe and secure communities.

Reassuringly, Abu Dhabi is a safe and secure place for its UAE Nationals, residents and visitors. The purpose of the Manual is to ensure that Abu Dhabi remains safe, secure and welcoming as it continues to grow and attract a range of diverse activities, people and opportunities.

Good planning and design of the built environment are central to community safety and protective security, yet crime and security issues rarely receive sufficient attention early in the development process. The purpose of the Manual is to ensure that safety and security are embedded in development proposals and this is best achieved using an Integrated Development Process. This process will be used to implement safety and security planning and design principles that are bespoke to Abu Dhabi Emirate. It will ensure that neither the development community, nor those tasked with safety and security enforcement, lose sight of the Vision 2030 overarching principles. The vision for the Manual is to ensure the creation of safe and secure communities that enhance quality of life and reflect the Emirate's unique identity.

Work on the initiative that produced the Manual included a series of workshops over a nine month period with senior representatives of Federal Ministries, Abu Dhabi Government departments, representatives of the private sector and Higher Education institutions. The initiative included a major benchmarking study, that for the first time, examined both community safety and protective security practices at an international, regional and domestic scale. Where good practices were observed, these have been amended to take into account the following Abu Dhabi factors: Culture & Religion, Climate, Pace of Development and Built Form.

Eight Principles are presented in the Manual (Chapter 2):

- P1 Access and Connectivity
- P2 Structure and Spatial Layout
- P3 Ownership
- P4 Surveillance
- P5 Activity
- P6 Physical Security
- P7 Public Image
- P8 Adaptability

They are universal, regardless of the type, size or location of development. However, they need to be applied differently according to context.

Guided by the Principles, specific policies have been developed under the following topics:

- Planning Culture
- Risk Assessment
- Balancing Act
- Working Together
- Owner Pays

The Integrated Development Process presented in Chapter 3 of the Manual will ensure that the Principles are applied early in the development process. This will allow professionals to use their skills and imagination to incorporate unobtrusive measures into the built environment. This is certainly more cost effective than retrofitting and will ensure design quality.

The Manual is supplemented by an online Decision Support Tool, that is both simple and user friendly. It may be used during the pre-planning stage of a project to gain an appreciation of how much influence safety & security will have on the development proposals. There are only two outcomes from the Decision Support Tool. Projects will either be identified as 'Low Priority' projects or 'High Priority' projects.

It is anticipated that the majority of projects will be identified as Low Priority Projects and applications submitted as part of the municipal planning and Building Permit process will need to demonstrate the implementation of the Principles. The Manual does not introduce any new deliverables for these types of projects. High Priority Projects, which will typically be larger in size or include land uses that attract particular security risks, will be required to submit additional deliverables as part of the municipal planning and Building Permit process. The recommendation is that these are completed by specialists, working as part of the multidiscipline project team, who are best placed to balance competing development objectives. In these instances, a Government safety and security advisor will work together with the project team to provide advice and support during the planning and design stages of development. They will be present at workshops and will review the proposals submitted to the UPC or relevant Municipality.

The Manual contains a toolkit of planning and design guidance that may be used to address safety and security risks. Decisions relating to which tools to adopt and to what extent they are applied are to be made as part of the Integrated Development Process. Neither the Planning Toolkit (Chapter 4) or the Design Toolkit (Chapter 5) prescribe any particular solutions. Best practice and experience shows that safety & security risks differ from one place to another and that the solutions that work in one place might not work in another. There is a need to take into account the local situation and for all those involved in developing, managing and maintaining the built environment, to work collaboratively and holistically to address safety and security risks.

The constraints present in the existing built environment justify the Manual's focus on the planning stage of development. However, even though Vision 2030 is ambitious and involves significant development, much of Abu Dhabi is existing and there is an equal need for community safety and protective security in existing areas. As such, the Planning and Design Toolkits present a wide range of options that will be useful for owners of existing buildings.

An implementation programme coordinated and funded by the Government will be used to identify any improvements needed at existing buildings for national security reasons. Owners will be contacted if their building is deemed 'High Priority' and if improvements are required, an action plan will be agreed.

Whether this Manual is being used during the early stages of the development process, or to make improvements at existing buildings, it is intended to inspire innovative and aspirational solutions that are in-keeping with the local context. The Manual does not provide detailed guidance, as it is a starting point, covering a large geographic area and a wide range of projects with varying safety and security requirements. With further advances and by working together to implement its Principles, it will create a solid foundation for safe, secure and sustainable communities.

1

Introduction
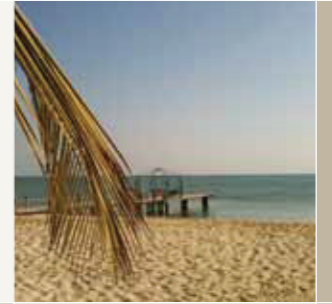
The Abu Dhabi
Safety and Security
Planning Manual
was commissioned
by the Abu Dhabi
Urban Planning
Council to guide
the development
of safe, secure,
and sustainable
communities.

This Manual is part of the UPC's development regulations and is approved by the Emirate of Abu Dhabi Executive Council for use across Abu Dhabi Emirate.

It constitutes one of many related planning and design initiatives in the Emirate of Abu Dhabi and shall be used in conjunction with other adopted standards and guidelines as applicable. The Manual integrates the needs of different agencies and its content will inform developers, owners and a range of professionals, including urban planners and designers, transport planners and safety and security specialists.

The Manual shall be used by all agencies involved in the approval of all new development in the Emirate of Abu Dhabi, and in assessing the appropriateness of community safety and protective security arrangements at existing developments. For the first time, the role of owners and the development community in maintaining Abu Dhabi's excellent record on crime has been documented.

The Abu Dhabi Safety and Security Planning Manual will be updated regularly as new data and experience with best practices become available. Please check the UPC's website for the latest version before using this Manual.

Safety and Security Definition

Good planning and design of the physical environment are central to community safety and protective security. Freedom from crime and the fear of crime lead to social, economic and environmental success and make a significant contribution to the fulfillment of Vision 2030.

The causes of crime and disorder are many and complex. For a crime to occur, the following are required:

- An offender who is motivated and resourceful;

- A target or victim; and

- A favourable place where the crime is likely to go unnoticed, unchallenged or even be promoted.

Through planning and design, it is possible to reduce the number of occasions when all three components are in place.

When discussed within this document, safety and security refers to the following:

Community Safety – comprises strategies and measures that seek to reduce the risk of crimes occurring and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes.

Protective Security – is an organised system of protective measures implemented to achieve and maintain security. It combines the three disciplines of personnel, information and physical security in a manner to create 'defence in depth', where multiple layers work together to deter, delay, detect and deny an attack.

Central to the planning efforts in Abu Dhabi are the 2030 Plans which establish a vision for the future development of the Emirate. The 2030 Plans include:

- Plan Capital 2030: Urban Structure Framework Plan
- Plan Al Ain City 2030: Urban Structure Framework Plan
- Plan Al Gharbia 2030: Regional Structure Framework Plan

The 2030 Plans regulate the pattern of urban expansion to balance economic, social, cultural and environmental priorities in a sustainable manner. The Plans seek to establish a planning culture and introduce best practice principles for both new and existing development. A series of overarching principles within the Plans are supported by specific policies to guide implementation. The development of the Abu Dhabi Safety and Security Planning Manual (SSPM) is informed specifically by Urban Design Policy VII – U23 Crime Prevention, which states:

"Complete a set of guidelines for crime prevention through building and landscape design and henceforth manage development to facilitate the safety of environments and maintain Abu Dhabi's excellent record on crime."

The preparation of this Manual has also been guided by subsequent UPC planning regulations, policy and guidelines that have been prepared to ensure the continued sustainable development of the Emirate.
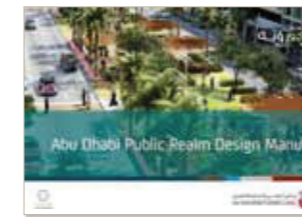
A selection of planning policy and guidelines issued by the UPC

Reassuringly, Abu Dhabi is a safe and secure place in which to live. The purpose of the Manual is to ensure that the Emirate remains safe and secure as it continues to grow rapidly and to attract a range of new and diverse activities, people and opportunities.

Crime
An extensive benchmarking effort conducted in the preparation of the Manual concluded that crime is very low in the Emirate of Abu Dhabi, but rising at a rate exceeding the population growth rate.

Crime statistics supplied by Abu Dhabi Police GHQ show that while personal crime is higher as a proportion of total recorded crime than in the benchmark countries, there is an exceptionally low level of property crime. As such, the primary focus for the Manual is to reduce crimes against the person through changes to the built environment. Essentially, this includes all crimes apart from those that occur within private properties.

Terrorism
As is the case across the world, the United Arab Emirates faces a real, evolving and increasingly complex threat from international extremism. To this day, there has not been a successful terrorist attack within the United Arab Emirates, although terrorist activity both globally and regionally is significant and its impact extensive.

Given the need for national security and the target-rich environment that will be created as a product of the ambitious development plans set out in Vision 2030, the Emirate of Abu Dhabi has established a Higher Committee for Crises and Terrorist Acts Management (HCCTAM). The HCCTAM leads the Emirate's efforts to counter terrorism and is the owner of the Counter Terrorism Strategy. This Strategy is organised around a series of work streams, one of which is 'Protection', which seeks to increase the resilience of the UAE against an attack.

Terrorism is a crime, and with the agreement of the HCCTAM, the Manual presents planning and design guidance that will embed counter-terrorism protective security in our built environment, reducing vulnerabilities and increasing the resilience of our communities.
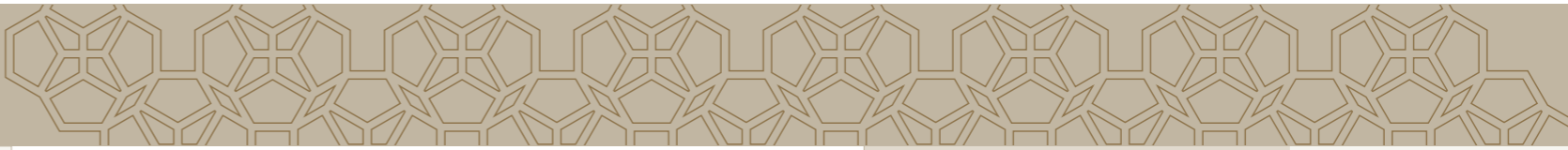
The Manual outlines eight Principles that are guided by a vision for safe and secure communities:

P1: Access and Connectivity
P2: Structure and Spatial Layout
P3: Ownership
P4: Surveillance
P5: Activity
P6: Physical Security
P7: Public Image
P8: Adaptability

The Principles need to be applied carefully as there is no such thing as a universal planning and design solution. This explains why the Manual has a strong focus on the process of implementing the Principles, rather than outlining a set of prescriptive standards that may never fulfill the vision.

Best practice and experience show that safety and security risks differ from one place to another and that the solutions that work in addressing these risks in one place, might not work in another. There is a need to take into account the local situation and for all those involved in developing, managing and maintaining our built environment to work collaboratively and holistically to address safety and security challenges. The following policies support and guide the decision-making process and will be adopted to ensure positive implementation outcomes.

Policy Statement 1

'Planning Culture'

Community safety and protective security shall be a core planning consideration in all new development.

Policy Statement 2

'Risk Assessment'

Community safety and protective security arrangements, in new and existing developments, must be fit-for-purpose, appropriate and proportionate to the risks.

Policy Statement 3

'Balancing Act'

Decisions relating to community safety and protective security must be balanced with other development objectives.

Policy Statement 4

'Working Together'

Appropriate advice, information sharing, transparency and rigour must be present to support community safety and protective security decision-making.

Policy Statement 5

'Owner pays'

Costs associated with community safety and protective security fall where responsibility for safety and security lies: with the owner.

New Development

Following the release of the Manual, all new development shall implement the Abu Dhabi Safety and Security Planning and Design Principles (Chapter 2). Chapter 3 of the Manual illustrates a simple Integrated Development Process (IDP) that describes how safety and security is to be integrated in a project. It highlights who will be involved, when they will be involved and their roles and responsibilities.

A simple, user-friendly Decision Support Tool (DST) has also been prepared for use by developers during pre-planning.

The DST can be used to gain an appreciation of how much influence safety and security may have during planning and design. For the majority of projects, which are likely to be defined as 'Low Priority Projects', this will mean that, whilst safety and security is important, it is unlikely to have significant influence on development proposals. There will be no safety and security specific deliverables required in planning and Building Permit Submissions made to the Abu Dhabi Urban Planning Council or the relevant Municipality. However, the content of the normal submissions will be expected to demonstrate the application of the Manual's Principles.

For projects defined as 'High Priority Projects', safety and security is likely to influence spatial use, spatial layouts and spatial design and Government safety and security advisors will be involved in decision making for each project. The developer is also advised to appoint a competent safety and security specialist to assist them in the preparation of safety and security deliverables required as part of planning and Building Permit Submissions. These deliverables are discussed in more detail in Chapter 3, which includes a section on 'Getting the Right Advice'.

Projects within this category will also be referred to the Planning Toolkit (Chapter 4) and Design Toolkit (Chapter 5) to assist developers implement the Principles.

The Government acknowledge that 'designing-out crime, and designing-in safety' will be new to many developers, planners, designers and operators. As such, the development community will have access to specialist advice from Government community safety and protective security advisors during the development review process.

Before seeking advice, the project team should read Chapter 3 (Process) of the Manual and complete the Decision Support Tool (DST). Using project-specific information, the DST will assign the development a Low Priority or High Priority classification.

Those projects assigned as High Priority Projects should consult with an advisor. Contact details are available from the UPC and the relevant Municipality Town Planning department.

Existing Development

In the existing built environment, certain constraints will reduce opportunities for owners to make community safety and protective security enhancements. This explains why the Government is focusing on ensuring that developers integrate safety and security early in the development process. However, the Principles outlined in the Manual are universally applicable and the Design Toolkit (Chapter 5) will be useful to owners wishing to install retrofit measures. The Toolkit will help them achieve design quality and fit-for-purpose solutions.

Government safety and security advisors will be initiating a programme of site vulnerability assessments across the Emirate, although these will be restricted to 'High Priority' sites. A notification will be received if the site is to be subject to an assessment. In the spirit of transparency and fairness required by Policy Statement 4 'Working Together', the advisors will explain why the site has been selected and will share the results with the owner. The cost of any protective security improvements will be the responsibility of the owner.

Crowded Places

There will be a focus on crowded places during the early stages of the implementation of this Manual.

A crowded place is a location to which members of the public can gain access and, by virtue of its crowd density and known terrorist attack methodology, may be considered potentially liable to terrorist attack. They may be buildings or open air public spaces and they may be permanent or temporary.

Whilst there have been attacks against well-protected targets around the world, the trend is for terrorists to attack these crowded public places, where crowd density and the difficulty in controlling access make them both attractive and vulnerable targets.

Previous attacks on crowded places include the bombings on the London Underground (UK), at hotels and restaurants in Egypt and armed assaults in Mumbai (India).

The guidance contained in the Manual should be used to reduce vulnerabilities at crowded places in Abu Dhabi. A Government safety and security advisor will assess safety and security at crowded places in one of the following categories:

1. Restaurants and cafes

2. Hotels and resorts

3. Shopping malls, markets and traditional souk

4. Health establishments

5. Recreation and leisure clubs

6. Exhibition, commercial and media centres

7. Visitor and tourist attractions

8. Sports and entertainment stadia

9. Special events

10. Religious sites and places of worship

11. Transport stations and hubs

12. Cinemas and theatres

13. Education establishments

14. Celebration halls
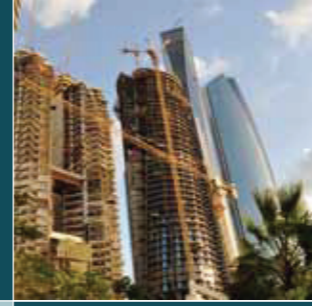
2

Abu Dhabi Safety and Security
Planning and Design Principles

Introduction

This Manual is based on eight Abu Dhabi Safety and Security Planning and Design Principles (each with sub principles). All development in Abu Dhabi will now be expected to follow these Principles.

The Manual uses a legend to demonstrate the Principles or guidance presented

✓ A positive illustration of the Principle or guidance presented

✗ An illustration of an environment that will benefit from the Principle or guidance presented

The Principles are universal — they are relevant everywhere, regardless of development type, size or location. They are however, to be applied differently, according to context.

Applying these Principles will help to ensure that Abu Dhabi residents and visitors can continue to enjoy a high quality of life in a low crime environment. The Principles will not just help to keep the Emirate safe and secure; they represent the best of good planning and design and they will be central to the implementation of Vision 2030.

This chapter sets the context for the Principles by introducing how good planning and design contributes to safety and security, before explaining how the Principles have been generated. It concludes by presenting the eight Principles one by one.

Principles

P1: Access and Connectivity
P2: Structure and Spatial Layout
P3: Ownership
P4: Surveillance
P5: Activity
P6: Physical Security
P7: Public Image
P8: Adaptability

The Role of Planning and Design in Safety and Security

A well-planned and designed built environment can do much to reduce the likelihood of an incident occurring or its impact if it does. This can be expressed in a number of ways, such as:

- Reducing opportunities for crime and terrorism by controlling access to vulnerable places;

- Empowering people to contribute to the safety and security of their communities by providing welcoming places to visit that encourage use and promote a sense of ownership;

- Increasing natural surveillance so that offenders are discouraged from wrong-doing due to the increased perception of being observed;

- Providing clues to how people are expected to behave in an area or building;

- Constructing buildings and other elements of the built environment so that they are less susceptible to crime or terrorism;

- Arranging buildings and facilities so that adjacent uses do not lead to conflicts; and

- Allowing the emergency services to respond quickly and effectively in the event of an incident.

This approach is sometimes referred to as Crime Prevention through Environmental Design (CPTED).

Adopting such an approach has been very successfully demonstrated elsewhere alongside other objectives of planning and design, such as sustainability, attractive environments and economic success.

Indeed, it enhances sustainability by making a place more popular, better used and with good community cohesion. These measures form the basis of the Principles introduced in this chapter.

The Manual is part of the Abu Dhabi Vision 2030 suite of documents and its Principles sit alongside those in the existing documents.

These Principles were considered alongside the most common principles from guidance and practice uncovered in international benchmarking. This involved a review of more than 50 documents from around the world, with a particular emphasis on reviewing guidance from those countries which share characteristics with Abu Dhabi. Whilst most formal planning for safety and security guidance is found in the UK, USA, Australia, New Zealand and the Netherlands, information was also sourced from countries such as Egypt, Pakistan, Singapore and Turkey.

Finally, to ensure that the Principles are bespoke to Abu Dhabi, a set of issues that set the Emirate apart from the benchmark nations were identified. These Abu Dhabi Factors can be summarised into culture and religion, climate, pace of development and built form. These are presented in the following pages.

Abu Dhabi Factor 1:
Culture and Religion

The importance of privacy means that surveillance, overlooking and screening need to be handled carefully so that residents do not feel uncomfortable.

The importance of family and notions of 'homeliness' mean that the focus of management and maintenance can be more on the upkeep of the home than the public realm.

The gifting of plots can result in plots that remain vacant for a period of time.

To ensure privacy UAE Nationals' homes are typically surrounded by a high boundary wall

Abu Dhabi Factor 2:
Climate

The climate of the region means that:

- Public areas such as parks and plazas are quiet during summer time;

- People are more likely to drive rather than walk during the summer months;

- Streets are often aligned with prevailing winds to gain cooling breezes; and

- Buildings are aligned and narrow paths created for increased shading.

A sikka offers shading to protect people from the summer sun and extreme heat

Abu Dhabi Factor 3:
Pace of Development

The current pace of development presents an opportunity to address macro safety and security needs using planning and design solutions early on in Abu Dhabi's advancement towards Vision 2030.

The scale of development means that safety and security principles can be applied as part of a master plan, rather than being restricted to individual plots.

The scale and pace of the development allows safety and security to be addressed earlier and on a wider scale

Abu Dhabi Factor 4:
Built Form

The layout and design of many urban and rural settings introduces long, narrow and uninhabited spaces that can be unsafe and vulnerable to misuse. Whilst there are many landmark buildings, the uniform grid structure of Abu Dhabi City can make it difficult to orientate oneself.

Cities have been designed around the needs of the car user, rather than those of pedestrians. Plot sizes are small, particularly in urban areas, making it more difficult to introduce stand-off or secure perimeters.

Underground parking is common in central areas and any constraints on such parking for safety and security reasons will inevitably exacerbate existing surface parking issues.

The built form in Abu Dhabi can present particular challenges to safety and security

Following discussions at the SSPM preparation workshops, the eight Abu Dhabi Safety and Security Planning and Design Principles were agreed.

Before they are introduced, it is important to make the following points about these Principles:
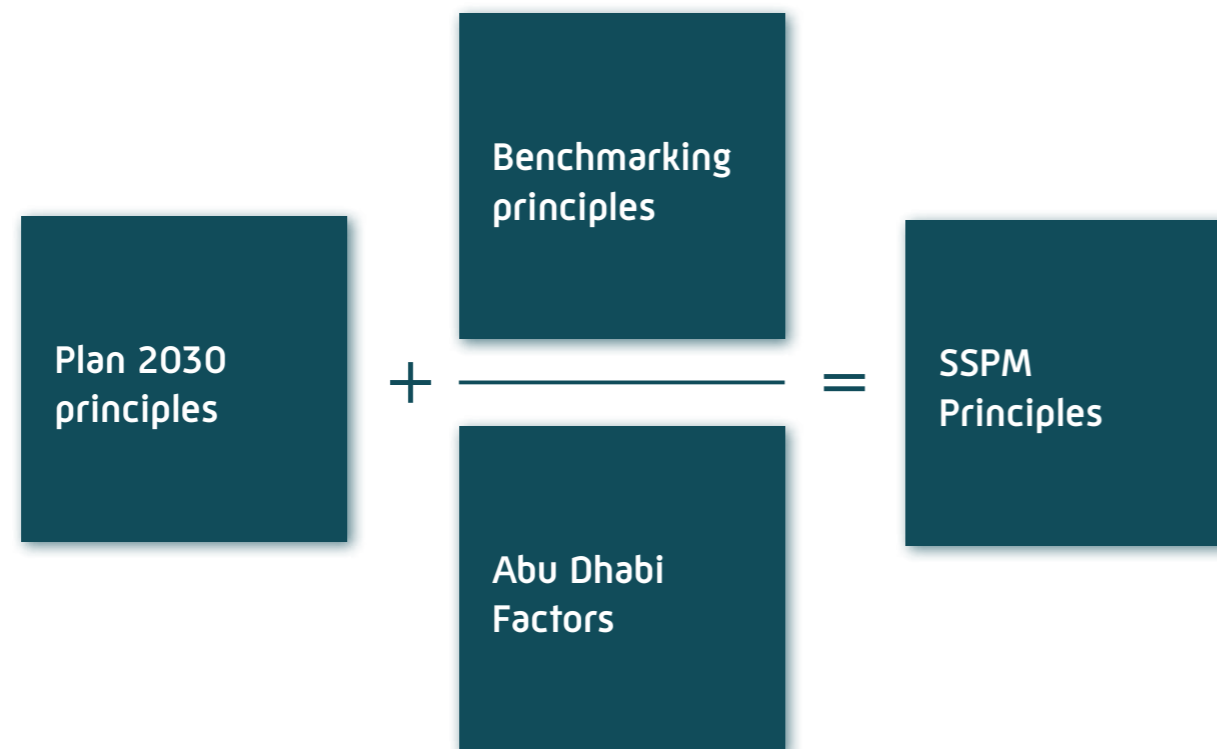
- They equate with good planning and design in a general sense. The Principles should be applied to all development in Abu Dhabi, regardless of type, scale or perceived safety and security risk; and

- The Principles relate to planning and design outcomes in the built environment. They do not cover the process of achieving these outcomes. There are some assumptions underlying how the Principles will be applied. For example, responses will be: different according to context; proportionate to risk; based on the sharing of information; and part of a holistic strategy. This process is explained in Chapter 3.

The remainder of this chapter introduces each of the Principles in more detail, including the rationale behind them. This is achieved by presenting a list of features that can compromise safety and security and extracts of evidence from benchmarking that can be published publicly. Each Principle concludes with a useful checklist to help users of the Manual to apply the Principles.

To Summarise:

The Abu Dhabi Safety and Security Planning and Design Principles were generated through these three steps:

1. Examining the existing Vision 2030 principles.

2. Exploring the principles that stem from international best practice in planning for safety and security.

3. Amending the international principles so as to take account of the unique Abu Dhabi factors.

Plan 2030 principles + Benchmarking principles / Abu Dhabi Factors = SSPM Principles

The Principles

P1 Access and Connectivity

P2 Structure and Spatial Layout

P3 Ownership

P4 Surveillance

P5 Activity

P6 Physical Security

P7 Public Image

P8 Adaptability
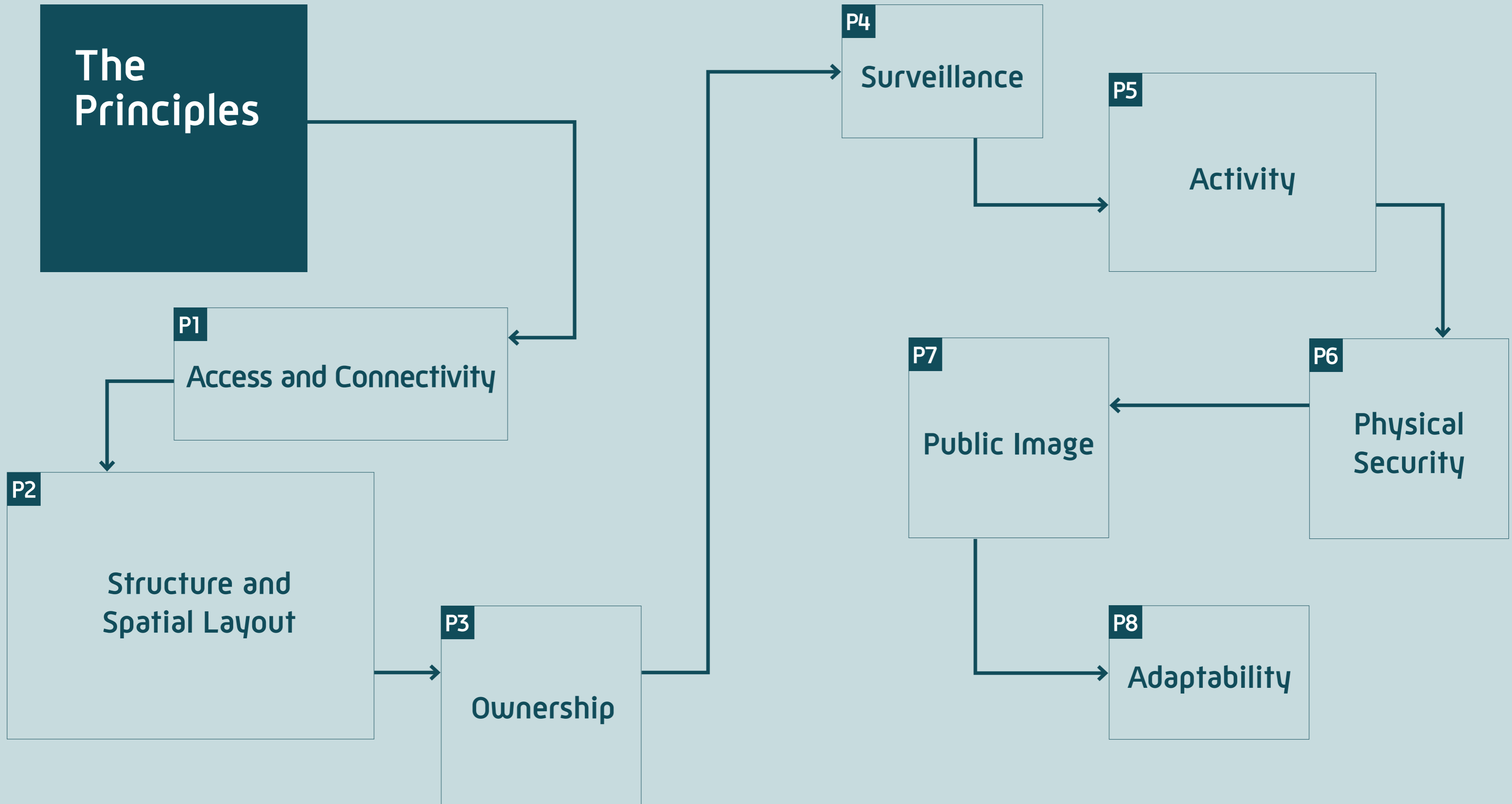
P1 | Access and Connectivity

Safe and secure places balance the need for access control with connectivity and circulation

Safety and security can be compromised if:

- Pedestrian routes are poorly lit, indirect and segregated from traffic;

- There is easy, anonymous access to targets, buildings and plots;

- There is no means of controlling who can enter a development;

- There are several uncontrolled escape routes from an area; and

- There is inadequate access for emergency vehicles.

From the evidence base:

A recent detailed study of crime patterns in 12 housing developments showed that "crimes are consistently clustered around alleyways and footpaths. Properties are particularly vulnerable when footpaths allow access to the rear or side of the dwelling, where footpaths are not overlooked by surrounding dwellings and where footpaths are not well used."

Armitage, R. (2011) "The Impact of Connectivity and Through-Movement Within Residential Developments on Levels of Crime and Anti-Social Behaviour," University of Huddersfield

Temporary pedestrian routes are commonly unsafe places
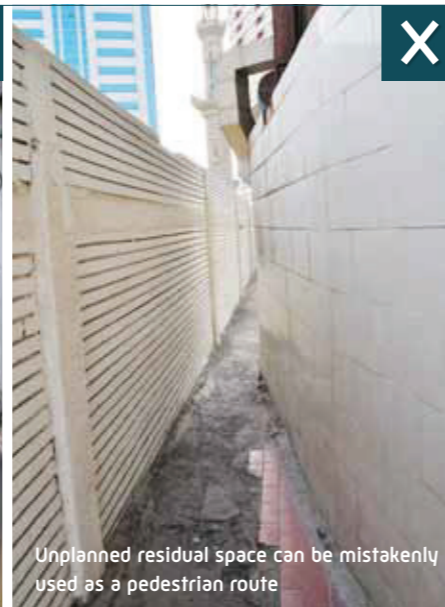
Unplanned residual space can be mistakenly used as a pedestrian route

Poorly lit and segregated pedestrian routes can be unsafe and misused

P1A — Connectivity is to be encouraged in Abu Dhabi unless it would result in inappropriate safety and security risks

Maximising connectivity will be the aim in most situations, but vulnerable sites will need to be protected where the risks of crime and terrorism are high. Restricting access, either by foot or vehicle, will sometimes be needed. The Planning Toolkit in Chapter 4 covers this in more detail.

Well connected neighbourhoods with convenient access to local facilities are full of life and frequented by members of the community

P1B — Places should have a well-defined movement framework that is tailored to the local context

Places rely on the right connections being put in place. The most appropriate movement frameworks have direct routes that lead to where people want to go.

Well-defined routes and destinations will help users orientate themselves as they move from place to place.

Well designed parks are welcoming and make it easier for people to orient themselves

P1C
Pedestrian-only routes need to be planned, designed and managed with care

It is important that pedestrian routes have a defined purpose as an integral part of a movement network to avoid them being abandoned by the community for whom they were intended.

Pedestrian routes need to be planned and designed to aid public image and proper use

Carefully planned and designed sikkak are safe and support community use

P1D
Vehicle access and circulation routes need to be planned, designed and managed with care

Vehicle access and circulation routes need to be planned, designed and managed with care. Criminals may use a vehicle as a means of forcing entry into a site, causing vandalism or even facilitating a terrorist attack. Vehicle-borne attacks can be sophisticated, involve high speeds and offer the criminal manoeuvrability even when delivering or removing large payloads.

The Abu Dhabi Urban Street Design Manual provides specific guidance for the planning and design of streets in the Emirate of Abu Dhabi.

Well-designed vehicle approaches reduce the risk of forced vehicle entry

Checklist:
- Has a coherent movement framework been set out?
- Are all routes necessary?
- Where safety and security risks are high, has access been controlled for vehicles and pedestrians?
- Are routes for different users segregated when they could be integrated?
- Do all sikkak or alleyways lead directly to a defined destination?
- Are sikkak clear of obstacles, straight and well lit?
- Does the planning and design of streets comply with the Abu Dhabi Urban Street Design Manual?

The movement framework should consider safety and security alongside other planning objectives

P2 | Structure and Spatial Layout

Safe and secure places are structured in a way that manages risk and conflict

Safety and security can be compromised if:

- The designated use of space is unclear;
- Places are under used and derelict;
- Conflicting user groups congregate in the same places;
- Public spaces are not overlooked;
- Areas of concealment and entrapment exist; and
- Places at risk of vehicle attack do not benefit from stand-off.

From the evidence base:

In most vehicle-borne explosive attacks, the impact is worsened by terrorists being able to drive vehicles next to, or even underneath / within, vulnerable buildings. Examples include:

- Alfred P. Murrah Federal Building, Oklahoma City, US, 1995 (169 Killed, 1000 injured)
- World Trade Centre, New York, US, 1993 (6 Killed, 1000 injured)
- Hilton Hotel Taba, Egypt, 2004 (34 Killed, more than 100 injured)
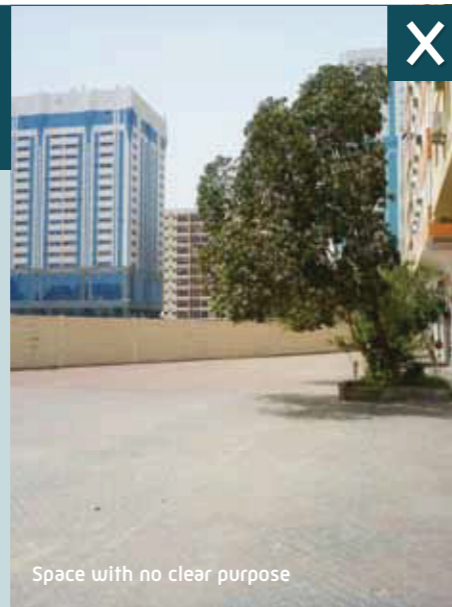
Space with no clear purpose

Area of concealment and entrapment

A lack of stand-off contributed to the large number of fatalities and injuries in the Alfred. P. Murrah Federal Building, (Oklahoma City, USA)

P2A — Spaces should have a designated purpose

If space either has no intended use or if the intended use of a space is not clear to the community, then there will inevitably be conflict, where individuals within the community have differing views on what is and is not appropriate within the space. It is difficult to encourage community ownership of a space that offers no benefit to the community.

Poorly planned and managed spaces with no clear function can become unsafe

P2B — Spaces should be planned and designed to support intended use

A space should lend itself to the intended use. If the space is the wrong size, is adjacent to conflicting uses or its design is not high quality, then the intended users are less likely to use the space.

Aesthetics, cost and function compete with safety and security when determining how a site is planned. Talented planners and designers will find an appropriate compromise when planning circulation routes, placing buildings, infrastructure and parking.

The same space is transformed by programming of space and public realm design improvements

Active and visible frontages encourage users to visit a space and observe the public realm, which contributes to community safety and security

Poor spatial planning can present areas of concealment and entrapment

Stand-off can be achieved using attractive and creative landscaping

Checklist:

- Does every space have a clear purpose?
- Are all spaces fit for their designated purpose?

P3 | Ownership

Safe and secure places are those over which occupants and users have a sense of ownership and responsibility

Safety and security can be compromised if:

- It is unclear whether space is public or private;
- Private space is open to the public;
- There is limited communal interest or supervision over a space; and
- Offenders are not afraid of being seen or reported.

From the evidence base:

The Dutch Police Label Secure Housing initiative, which seeks to ensure that residents have a sense of ownership and responsibility over spaces by insisting that all spaces in a neighbourhood are carefully planned and defined (alongside other measures), has seen burglary rates plummet since it was introduced in 1994 – by 98% in new housing schemes and 80% in existing environments.

Jongejan, A (2011) "The Dutch Police Label Secure Housing: a successful approach", Working Paper

Public space being used as private space

Poor public image

Clear evidence of the absence of communal interest

P3A The ownership of space should be clearly defined

The built environment consists of spaces over which different users have varying degrees of access rights and ownership. What is deemed acceptable behaviour in one space may be deemed unacceptable in another. It is very important that there is clear definition of space so users know who owns a space, where they can go, when they can go there and the permitted use of the space.

Ownership and responsibility can be facilitated by making it clear where public space ends and where semi-private or private space begins.

A change in texture, colour and style of paving can be used to define space

Physical barriers can be used to define a change in ownership

P3B Instil a sense of ownership over space

The community can be encouraged to contribute to safety and security when they have a sense of ownership over space.

By empowering members of the community as observers, people are more comfortable and encouraged to report suspicious behaviour, misuse and crime.

Well designed parks encourage use

Checklist:

- Is public and private space clearly defined?
- Is the means of defining space appropriate to context and other planning objectives?
- Is the space welcoming and encouraging of positive behaviour?
- Will the development have an identity of its own that will encourage community development?

Well designed parks are welcoming

A lack of ownership or communal interest over a space increases the likelihood of crime and misuse

A sense of ownership over space helps to bring activity to the public realm

P4 | Surveillance

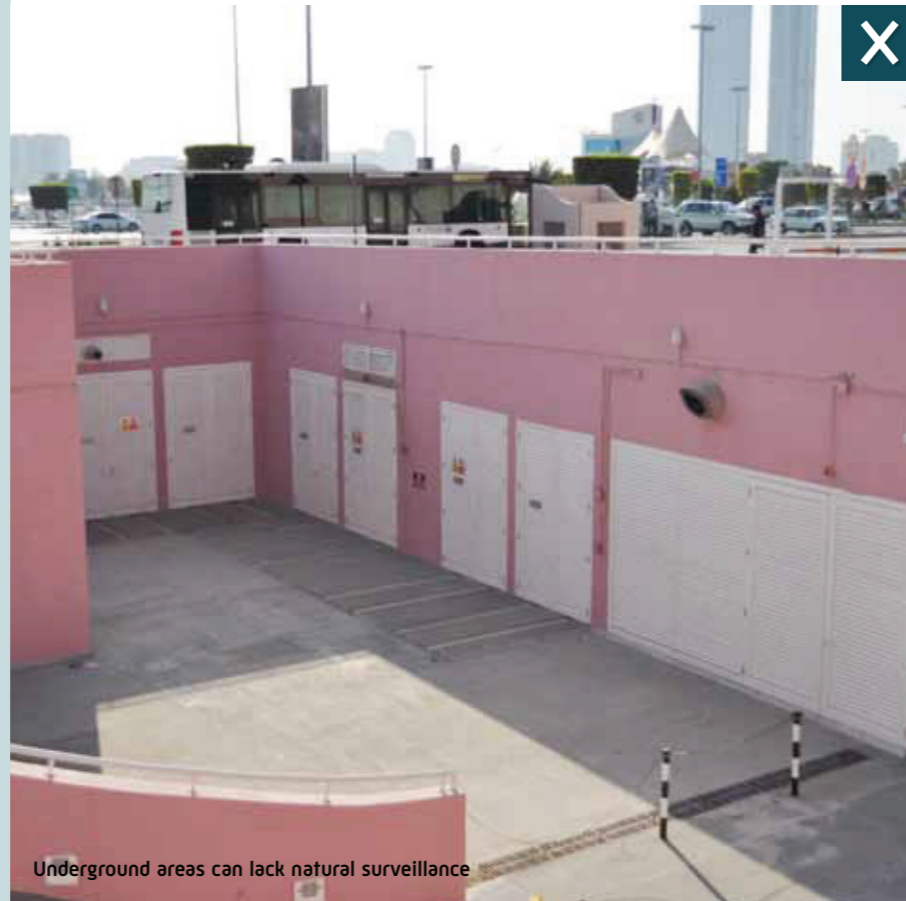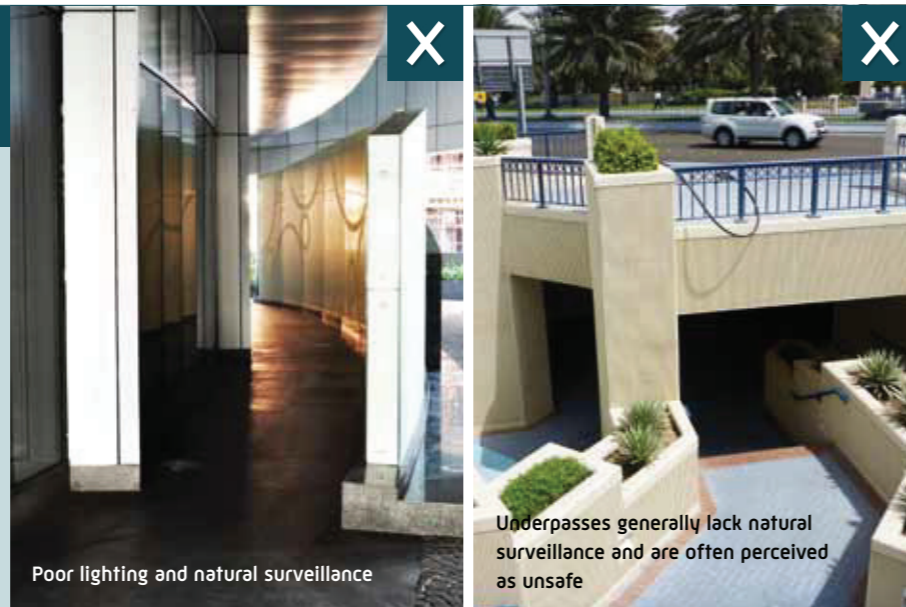## Safe and secure places have appropriate levels of surveillance

Safety and security can be compromised if:

- The balance between surveillance and privacy is not achieved;
- The balance between surveillance and the need for shading is not achieved;
- Offenders are not afraid of being seen or reported;
- There is restricted natural surveillance of the public realm;
- Vulnerable areas do not have active surveillance systems; and
- Places are not well lit.

From the evidence base:

Maximising surveillance is one of the central aims of the Secured by Design initiative (UK).

There have been five published evaluations of 'Secured by Design', all of which conclude that it has led to significant reductions in crime. For example, burglary rates are typically four or five times lower in Secured by Design based developments than comparable ones.

Poor lighting and natural surveillance

Underpasses generally lack natural surveillance and are often perceived as unsafe

Underground areas can lack natural surveillance

P4A — Balance the need for surveillance with the need for privacy

Surveillance needs to be achieved sensitively to reflect the cultural and religious factors in Abu Dhabi, as well as the value placed on privacy.

An innovative approach to balance the need for privacy while enabling residents to watch over the public realm from the balcony. Transparent materials enable observation of the elevator from the public realm and vice versa

P4B — Balance the need for surveillance with the need for shading

Shading of public realm space encourages activity (which is especially important – Principle P5). However, it can impede natural and active surveillance. There is a balance to be struck between shading and surveillance.

Shading and natural surveillance are carefully balanced at the Abu Dhabi Corniche

P4C Adopt natural surveillance before relying on active systems such as CCTV

Natural surveillance is where users of a space provide 'eyes on the street' that act as a deterrent to crime and the misuse of space.

In most situations, good natural surveillance will be more of a deterrent than active systems (meaning those that rely on technology and/or manpower). It is more important to get the basics of planning and design right in the first place, rather than resorting too quickly to active systems.

Spaces that offer good natural surveillance will generally have clear sight lines that will offer benefits to active system designers later in the development process.

Operators may choose to incorporate active surveillance to meet operational needs such as public transport safety, traffic monitoring and crowd management.
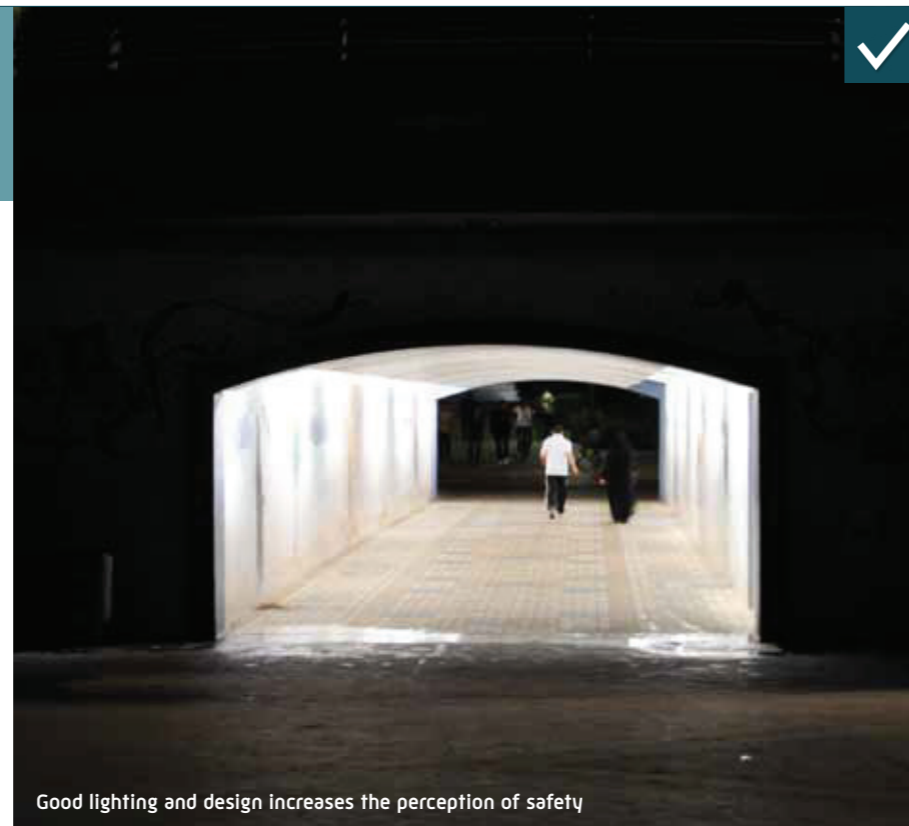
Good lighting and design increases the perception of safety

Good landscape design enables people to see what is happening around them and empowers them as observers over space

Residential streets that lack natural surveillance can feel unsafe, particularly at night

Natural surveillance can be enhanced by the placement of doors, windows and balconies to overlook the public realm

P4D — Concentrate active surveillance systems in areas that are more prone to crime and misuse

In addition to deterring the misuse of space and criminal acts, active surveillance systems can afford a number of additional benefits to management and enforcing authorities. These include incident monitoring and investigation.

An operational requirement should support the use of active systems and this can be developed following a safety and security risk assessment.

This service area would benefit from the application of video surveillance technology

P4E — Support natural and active surveillance with good landscape, urban and architectural design

Design decisions, ranging from building orientation and shape through to plant species selection and shading structure design, will influence the effectiveness of surveillance systems. Practitioners will need to adopt a holistic approach to address site-specific requirements and project objectives.
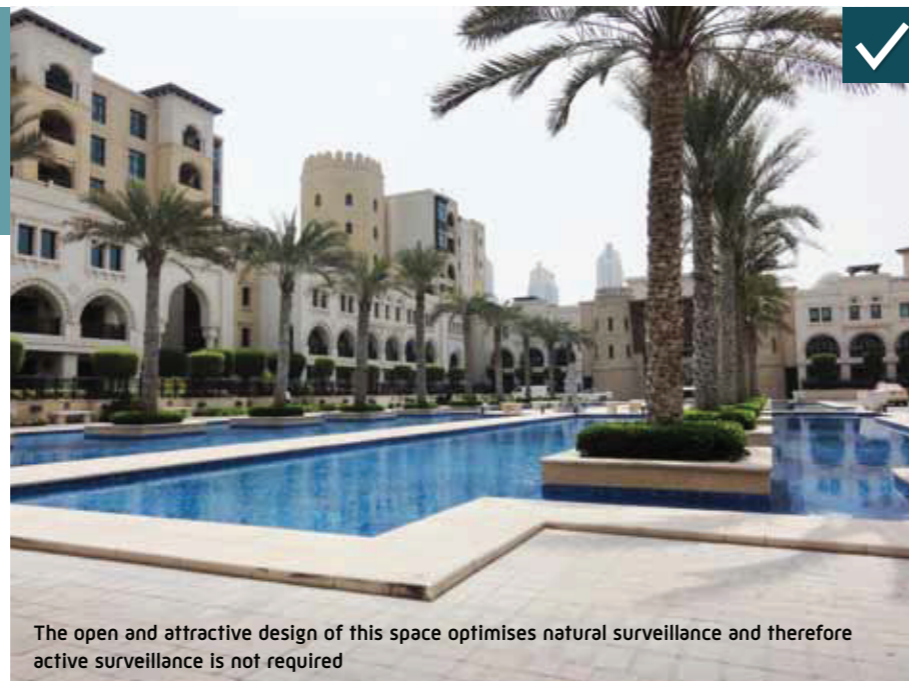
The open and attractive design of this space optimises natural surveillance and therefore active surveillance is not required

P4F — Support natural and active surveillance with appropriate lighting

Lighting may be provided to aid in the detection of intruders, to deter intruders, or in some cases simply to increase the feeling of safety. A holistic approach is required to ensure lighting supports effective surveillance.
To ensure lighting elements are fit-for-purpose, their design and specification should include anti-vandalism and anti-tamper features.

Good lighting supports natural surveillance

Checklist:

- Has a balance been struck between the needs for surveillance and privacy?
- Does the approach to surveillance take account of local context?
- Are there opportunities for overlooking of spaces from surrounding buildings?
- Does the layout and landscaping allow clear lines of sight?
- Are surveillance opportunities available at all times of the day and night?
- Are CCTV and other systems focused on the most vulnerable areas?
- Does CCTV supplement, rather than replace, natural surveillance?
- Is lighting provided everywhere that needs to be lit?
- Is lighting robust and energy efficient?

Good lighting makes it easier for people to see what is happening around them while also aiding wayfinding

P5 | Activity

Safe and secure places are active and welcoming to legitimate users

Safety and security can be compromised if:

- An area is very quiet (for most crime types);

- An area is very crowded (for terrorism and pick-pocketing);

- Communities are not supported by the facilities they need;

- Opportunities are not provided for comfortable walking and cycling; and

- Operators are unprepared for sudden changes in activity levels.

From the evidence base:

"There is a growing body of research on activity support and mixed use neighbourhoods where it is found that opportunities for crime are reduced by increasing the range of activities in public spaces."

Western Australian Planning Commission (2006) "Designing Out Crime Planning Guidelines"
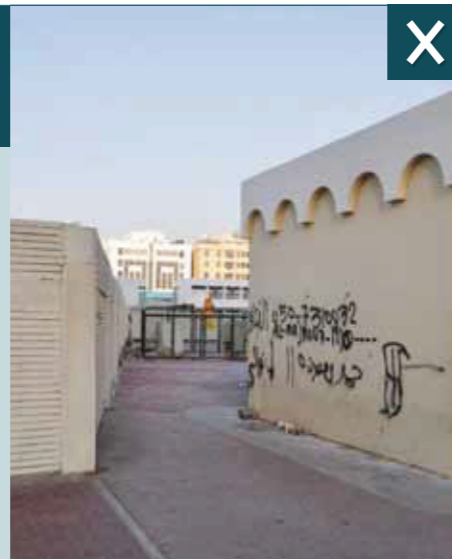

Very quiet areas allow vandalism to go unnoticed
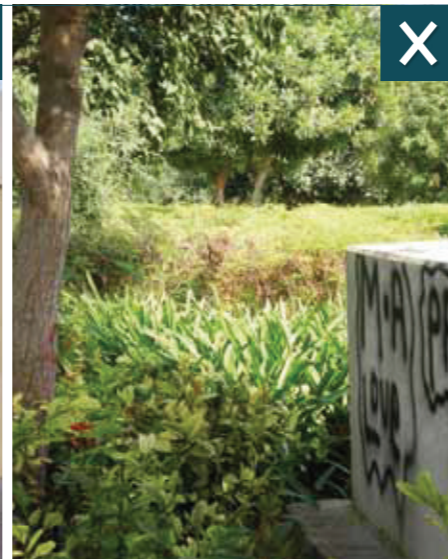
Inactive areas attract crime and misuse

P5A — Plan for a rich mix of compatible uses

A mix of uses can bring activity to an area at all times of day or night, offering 'eyes on the street'.

A mix of uses can make places more economically and socially successful, as well as safer. However, care should be taken to ensure the compatibility of different uses. This will be different from one site to another and there is no 'one-size fits all' solution.
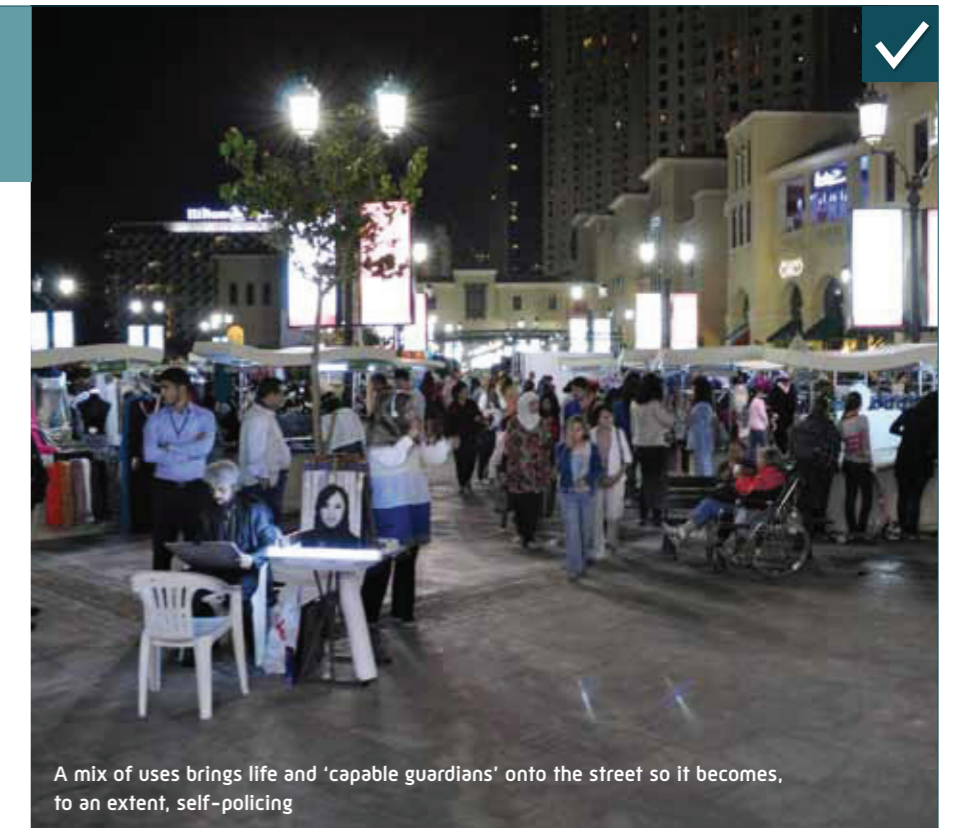

A mix of uses brings life and 'capable guardians' onto the street so it becomes, to an extent, self-policing

P5B — Provide the right type of facilities to support the local community

Providing facilities that match the needs of the community will generally increase the level of activity in a community.

The Abu Dhabi Urban Planning Council provides guidance to developers on the appropriate provision and placement of community facilities.
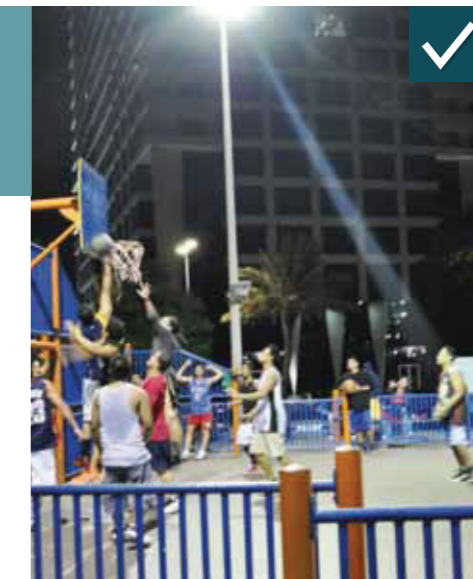
Recreational use helps to activate areas in the evening
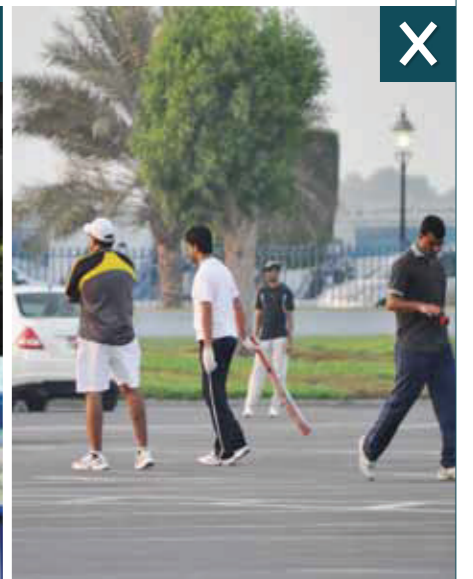
A lack of community facilities has led to an impromptu game of cricket in an unsuitable space

P5C — Ensure that opportunities exist for safe and comfortable walking and cycling

The Abu Dhabi Public Realm Design Manual and Abu Dhabi Urban Street Design Manual both provide very useful information on how to develop environments that support pedestrians and cyclists.

Cyclists and pedestrians are a sign of successful, safe streets and spaces

P5D — Pay particular attention to safety and security risks at crowded places

Abu Dhabi is developing a range of tourist attractions, transport facilities and commercial centres as part of Vision 2030. In addition, particularly in the winter months in all regions of the Emirate, there is a range of special events and exhibitions.

These crowded places are accessible to members of the public and are associated with high crowd densities. This level of activity represents an attractive target for criminals and terrorists. If poorly planned, crime is hard to detect or may go unchallenged. Innovation is required to address safety and security risks at crowded places.

The planning of crowded places should address safety and security needs

Checklist:

- Is there an appropriate mix of complementary uses?
- Will public places have legitimate activity throughout the day and evening?
- Is the community supported by the facilities it needs?
- Are people encouraged to walk and cycle?
- Is there a safety and security plan for crowded places?

The planning and design of this Abu Dhabi bus station promotes natural surveillance

P6 Physical Security

Safe and secure places are appropriately and proportionately protected

Safety and security can be compromised if:

- Physical security is not appropriate or proportionate to risks;
- Physical security components are not fit-for-purpose;
- Defence in depth is not achieved; and
- Risks have not been assessed when determining physical security needs.

From the evidence base:

Studies have shown that total housebreaking crime fell by 60% in residential areas that have fitted secure doors and windows to houses and apartments.

Teedon, P et al (2010) "Evaluating Secured by Design door and window installations: effects on residential crime" Crime Prevention and Community Safety, Vol. 12, 4, 246–262

Easy to climb

Inappropriate to context

An ineffective vehicle access control point that is easily circumvented

P6A Use risk assessment to identify and justify physical security needs

Physical security includes tactics to deter, delay, detect and deny inappropriate and/or criminal behaviour. There is no one size fits all solution to physical security and therefore proposals must be based on an assessment of the local situation and project risks.

Physical security should be appropriate given the context, proportionate to the safety and security risks and balanced with other development objectives.


This ornate wall has been specifically designed to provide hostile vehicle mitigation and to match the context of the surrounding environment (London, UK)

P6B Integrate physical security to result in design quality

Physical security needs to be considered as part of the Integrated Development Process (IDP) (Chapter 3) to result in fit-for-purpose solutions. Innovation should be used to ensure the delivery of design quality, to seek 'dual purpose' installations and cost effective physical security.

Natural and built physical security elements such as ditches, walls and gates can be used to meet other development objectives e.g. privacy, sound attenuation; as well as performing a safety and security function.
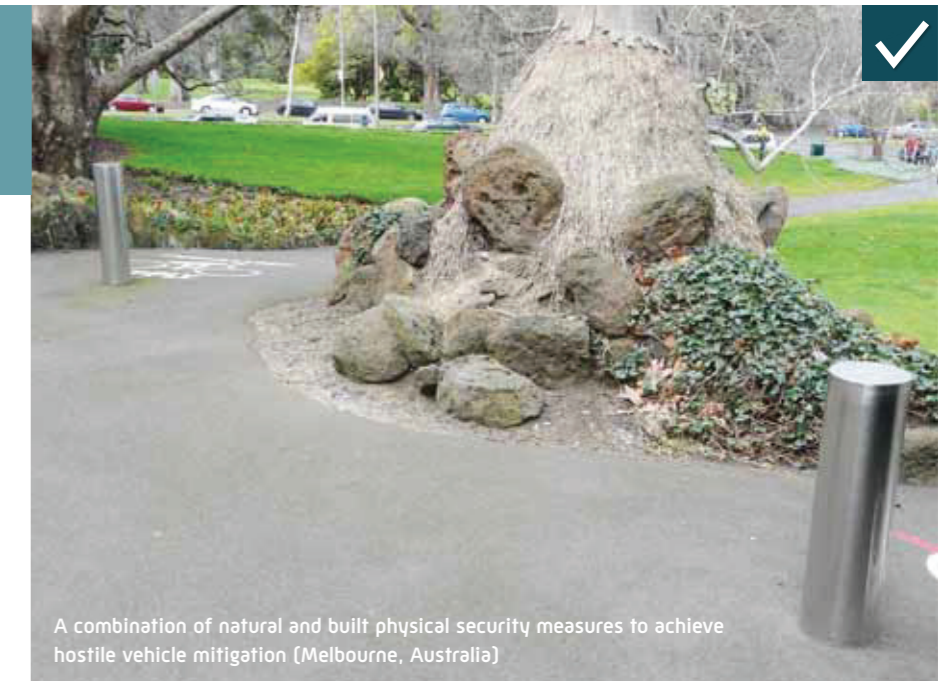
A combination of natural and built physical security measures to achieve hostile vehicle mitigation (Melbourne, Australia)

P6C
Physical security must be part of a balanced security programme

Physical and technical and operational security should be integrated to offer defence in depth.

Security should be integrated into the landscape design and grounds maintenance strategy

P6D
Both natural and built physical security elements can be used to reduce safety and security risks

Natural elements, such as topographic features, can be used for physical security. These elements can be enhanced or combined with built elements if they do not meet the operational requirement.

Built physical elements must be tested and certified to ensure they meet the security function.

Water features can be used as a natural barrier

Checklist:

- Has a risk assessment informed planning decisions on physical security?

- Is there an appropriate emphasis on physical security?

- Are physical security components fit-for-purpose?

- Is the physical security plan consistent with the wider protective security assumptions?

- Are security measures in keeping with the wider built environment?

- Is access and connectivity balanced with physical security?

- Is access maintained for emergency vehicles?

P7 | Public Image

Safe and secure places are well maintained and managed, and promote a positive public image

Safety and security can be compromised if:

- There is no sense of place;
- Places are untidy or unattractive;
- People think that they can commit offences with little risk of people caring;
- Signs of disorder and neglect are not dealt with at the earliest opportunity;
- Management and maintenance is not considered during planning and design; and
- Vacant or disused plots are left in poor condition.

From the evidence base:

Several empirical studies have shown that the presence of disorder such as vandalism, rubbish or graffiti leads directly to more inappropriate behaviour. These studies support the broken windows theory, which states that "if a window in a building is broken or left unrepaired, all the rest of the windows will soon be broken...One unrepaired broken window is a signal that no one cares...Untended property becomes fair game".
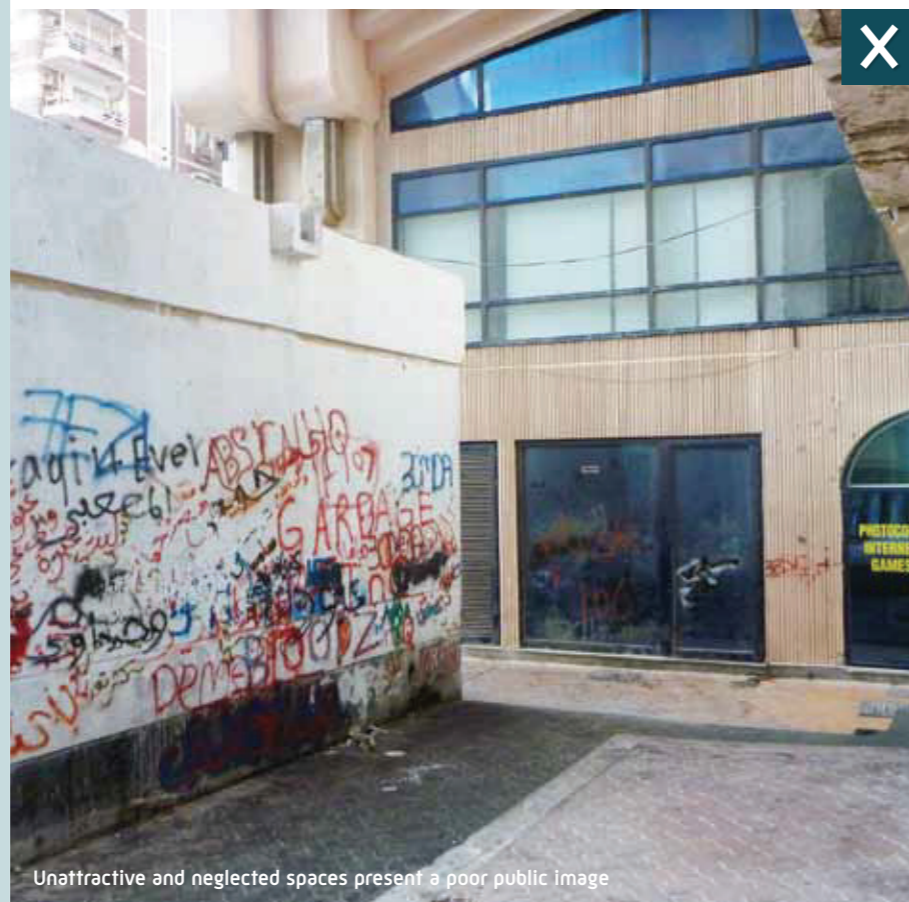
Wilson, J.Q. and Kelling, G.L. (1982) "The Police and Neighbourhood Safety", The Atlantic Monthly

A vacant site left in a poor condition

Evidence of neglect and poor maintenance

Unattractive and neglected spaces present a poor public image

P7A — Promote a sense of place and the legitimate use of space

If a place has its own identity, its community will feel a sense of place. This promotes ownership over space, encourages legitimate use and deters offenders.

A well designed pedestrian route helps to establish a sense of place

A neglected space receives little attention and detracts from a sense of place

P7B Plan and design with management and maintenance in mind

A place that appears to be abandoned or uncared for will signal to offenders that their actions are likely to go unnoticed and unchallenged. This can even promote crime and discourage the intended use of a space.

Decisions taken during the planning and design stages to create quality spaces that are easy to manage and maintain will have a positive impact on safety and security and lead to sustainable communities.

A highly maintained landscape sends out a positive message and pleasant street environment in Ruwais

P7C Hold owners responsible for managing and maintaining their plots

Whether a plot is vacant because development has not yet commenced, construction is underway or is awaiting clearance, a plot must be managed and maintained by its owner to avoid misuse and criminal behaviour on private land.

Due to the pace of development in Abu Dhabi, both the Government and plot owners shall work together to ensure appropriate development phasing and plot allocations.

Management and maintenance of vacant plots, construction and demolition sites offers Environmental, Health & Safety benefits as well as a reduction in crime and inappropriate use of space.

Checklist:

- Does the development have its own sense of identity?

- Can design quality be demonstrated?

- Is it easy to maintain high standards of upkeep?

- Are non-occupied plots well maintained and secure?

- Does a phasing strategy avoid vacant plots that may become problematic?

Dhu Al Qida 8, 1432

400 empty buildings set for demolition

Places neglected by owners often suffer from crime and misuse

P8 | Adaptability

Safe and secure places are adaptable to change

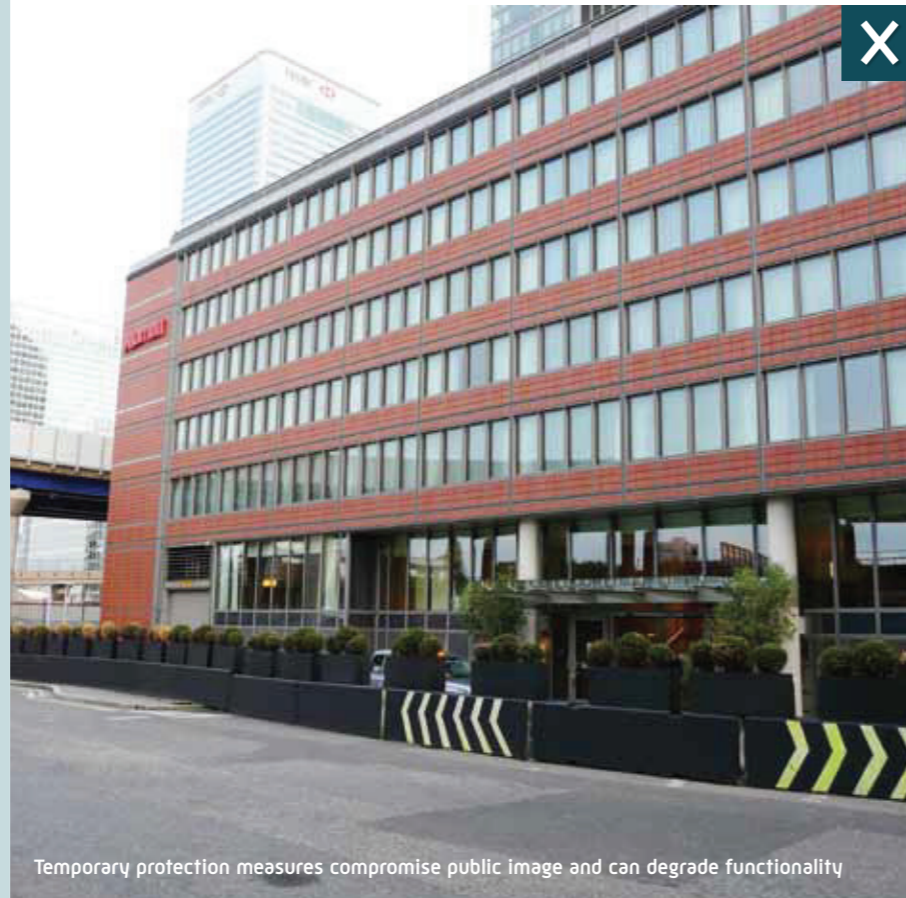### Safety and security can be compromised if:

- Places cannot respond to changes in use or users;
- Places do not respond to changing threats;
- Places cannot respond to special events;
- There is no planning for incident management; and
- Places cannot adapt to different modes of operations.

From the evidence base:

CONTEST, the UK counter-terrorism strategy, places changing threats and responses to them at its heart. The 2011 updated strategy commences by reviewing how threats have changed in the previous years. It continues to outline how strategies have been altered in response. It also explains how counter-terrorism efforts are responding to specific major events, most notably the Olympic Games.

Temporary protection measures compromise public image and can degrade functionality

Temporary protection measures compromise public image and can degrade functionality

P8A — Plan for changes in owner, occupiers and users

Significant changes in use or the users of space can be associated with changes in safety and security risks. The Principles should be adopted even where initially risk may be seen as low.


The planning and design of this building has enabled both commercial and Government use

P8B — Plan for changes in threat

Criminals are constantly evolving their tactics, weapons, tools and targets. The challenge for planners and designers is to systematically anticipate, identify and prepare for these changes before they occur.

Effective adaptable measures to control access of vehicles (Downing Street, London, UK)
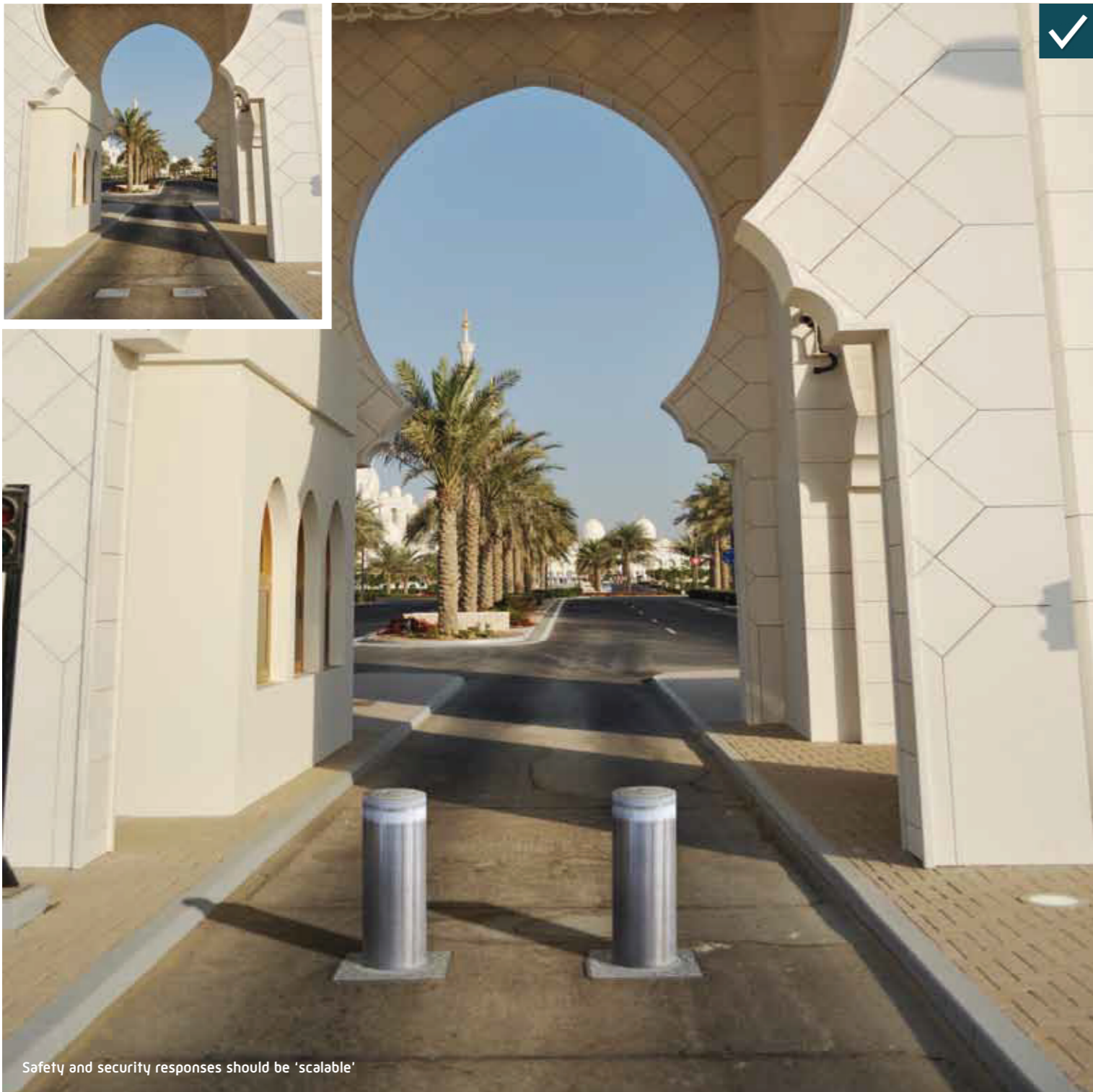
Safety and security responses should be 'scalable'

P8C Plan for special events

Safety and security plans should be able to accommodate special events, such as visits by VIPs and crowded places associated with celebrations.

Temporary safety and security elements may be introduced if they are readily available, there is space for their deployment and they can be integrated within an existing safety and security programme.


Temporary security measures for a special event held in Abu Dhabi

P8D Plan for all modes of operation

In many developments there are changes in safety and security needs at different times of the day, month or year. In some places these changes may be subtle, while for certain uses there are clear differences in the safety and security requirements between working hours and out-of-hours operations.

At certain places, typically at crowded places such as public plazas, shopping malls, stadia and public transport facilities, there are extremes of activity and calm.

A good safety and security plan will adapt to each mode of operation.
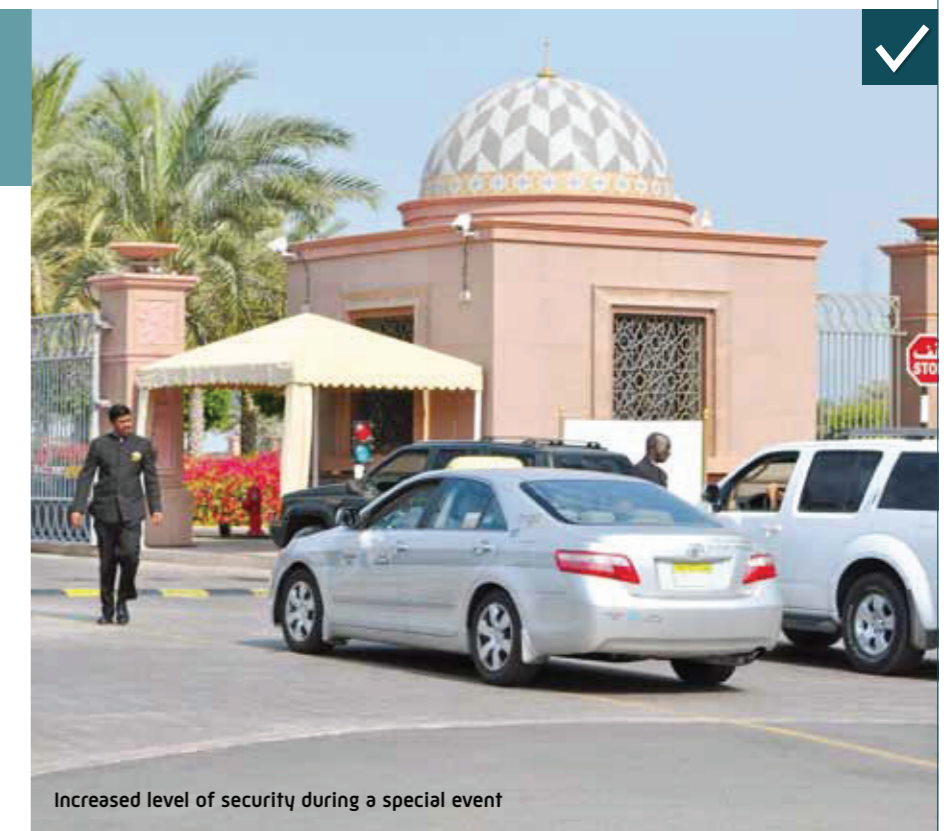
Increased level of security during a special event

P8E Plan for incident management as well as normal operations

Additional pressure will be placed on management systems in an emergency situation. A good safety and security plan will incorporate elements that support effective operations and the work of the emergency services such as the Abu Dhabi Police and Civil Defence.

Basic utilities such as electrical power, water and communications become even more important in an emergency situation. Open space can be put to very good use during an emergency, such as decontamination areas, assembly points and for evidence collection.

Checklist:

- Have changes in use or users been considered during planning and design?
- Have attempts been made to anticipate and plan for changing threats?
- Can the development accommodate special events?
- Does the safety and security plan respond to changing levels and types of activity?
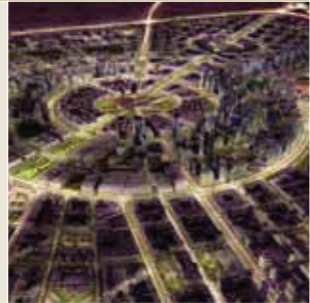- Is there space, facilities and infrastructure for use in an emergency situation?

A fire at Al Raha Gardens, Abu Dhabi

3
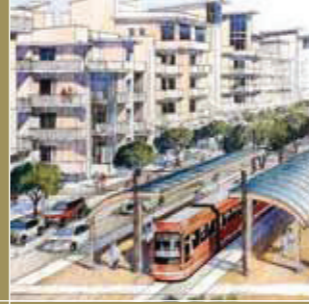
Safety and Security within an Integrated Development Process

Introduction

The purpose of this Chapter is to describe how the Manual will be integrated and implemented within the existing planning and design framework of the Emirate of Abu Dhabi.

"Thankfully, safety and security measures are rarely called upon. However, this can often lead to planners and designers underestimating their importance"

"It is rarely possible or cost effective to implement every security countermeasure for every conceivable scenario. However integrating security throughout the planning and design process enables the project team to strike a responsible balance between the level of risk, available resources and appropriate mitigation measures"

This Chapter outlines:

- How safety and security fits into the existing development process; and

- Who will be involved, when they will be involved and their roles and responsibilities.

The Integrated Development Process (IDP) aims to ensure that the right people are involved in projects at the right time. This will facilitate:

- The development of appropriate and proportionate safety and security solutions;

- Safety and security solutions that are balanced with other Vision 2030 planning objectives; and

- Innovation and collaboration between developers and the Government.

Decision Support Tool

The Decision Support Tool (DST) has been prepared for developers. The DST can be used at pre-planning to gain an appreciation of how much influence safety and security may have during planning and design. The DST is available online. Visit www.upc.gov.ae for more details.

DST Outputs:

| 'High Priority'	'Low Priority'
Safety and security is likely to influence spatial use, spatial layouts and spatial design. Government safety and security advisors will be involved in the decision making on the project.	Safety & security is important, but is unlikely to have significant influence on the development proposals.

Integrated Development Process Stages

There are several sequential stages within the normal development process, each building on the foundations of the previous stages. Safety and security must be part of this process and balanced with other objectives.

At each stage there will be inputs, tasks and deliverables that are performed to meet the safety and security objectives of the project. The four stages of an Integrated Development Process are shown below.
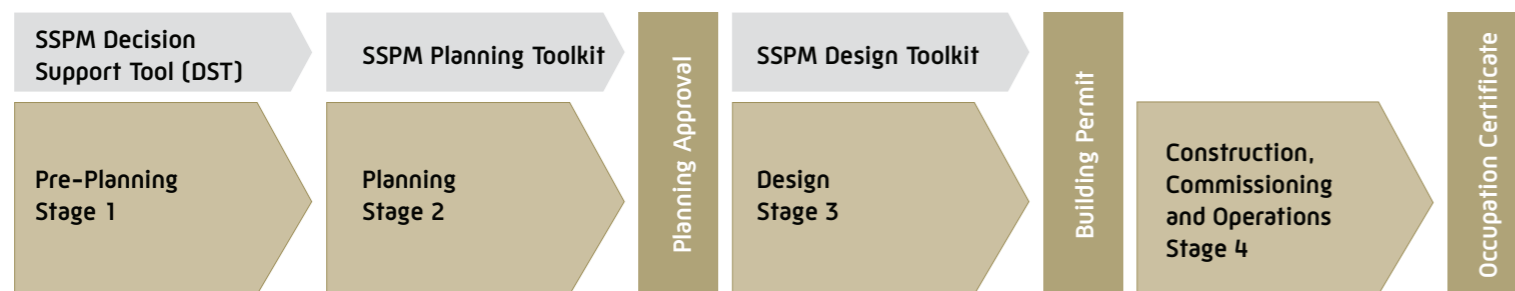
Project Scheduling

The aim of the Manual is to encourage the development community to consider safety and security early in the development process so that planning can be used to reduce safety and security risks.

Commencing design, in parallel with planning or prior to planning, clearly runs contrary to this aspiration and greatly reduces the opportunities for innovative, cost effective planning solutions. Scheduling this way is likely to push safety and security solutions further along the development process, resulting in greater emphasis on design solutions, or if not possible, placing a heavier reliance on operations security. Residual risk is likely to be higher, assurance levels are likely to be lower and aesthetic compatibility is likely to be reduced. For High Priority Projects this may be deemed unacceptable.
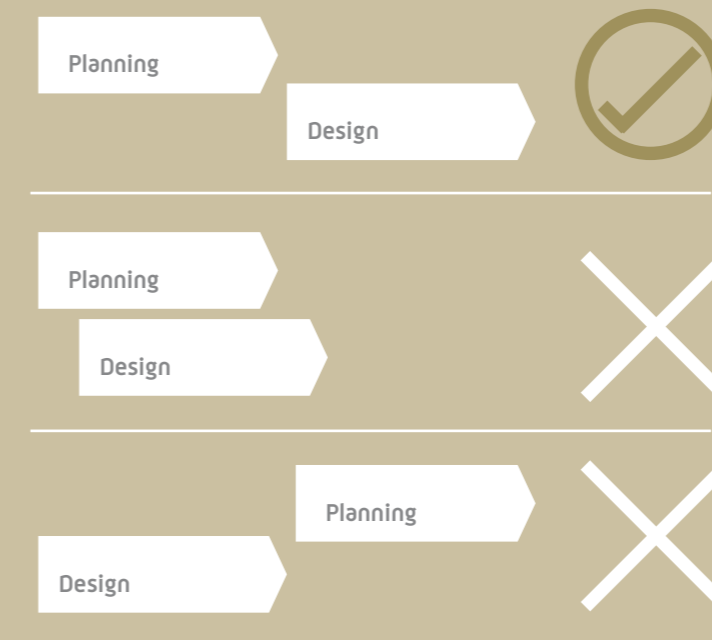
Planning for Safety and Security: A Balancing Act

There are few organisations that have the resources or mandate to mitigate every plausible threat scenario.

The Manual's Principles and process are based upon the principles of risk management. The highest risks should be tackled first, as the sooner the intervention, the bigger the impact on reducing risk and the lower the impact on design quality and cost.

Invariably this involves compromise which will need to be clearly identified, understood and recorded. The level of risk also sets the level of compromise possible with regard to the specific safety and security requirement. For higher risk projects, the security requirement will not change, however there should always be sensible discussion and agreement on how much protection is to be afforded and flexibility on how that protection level is to be achieved.

SSPM Decision Support Tool (DST)

SSPM Planning Toolkit

Planning Approval

SSPM Design Toolkit

Building Permit

Occupation Certificate

Pre-Planning Stage 1

Planning Stage 2

Design Stage 3

Construction, Commissioning and Operations Stage 4

Planning

Design

Planning

Design

Planning

Design

Stage 1: Pre-Planning

This stage focuses on setting up the project and identifying the right people for the project team. If specialist safety and security input is required, then it is at this stage that the expertise should be identified and sourced.

Whether or not specialist input is required will depend on the complexity of the development project. Clearly, each project is different, with proposed land use, development location and scale of development determining safety and security needs. In addition, stakeholder and regulatory requirements should be fully understood and documented at this stage.

The Manual should be read and understood and in particular, the function and application of the Decision Support Tool (DST).

SSPM Decision Support Tool

This tool is not intended to be a substitute for a development specific safety and security risk assessment undertaken by a specialist, but its output will help to determine whether safety and security should be a high or low priority for the project team.

'Low Priority'

If the DST identifies the project as low priority, the project team will be required during later planning and design approvals to demonstrate that the Manual's Principles have been implemented. The project team will not be expected to have appointed a specialist, although they may wish to do so if the project team is unfamiliar with safety and security planning and design.

'High Priority'

If, either the DST indicates safety and security to be a high priority, or the project brief incorporates specific safety and security objectives, the developer should seek to appoint a safety and security specialist (See 'Getting the Right Advice').

Projects identified as 'High Priority' must undertake a comprehensive, development specific safety and security risk assessment. Projects identified as having business or organisation specific risks may also want to undertake a development specific risk assessment (which will be much more comprehensive than the output of the DST).

The Government is only concerned with protecting the public interest and it may be necessary to consider corporate level safety and security risks. The DST cannot take this into account and if unsure, always seek advice and consult the project owner.

Pre-Planning Summary Sheet

High Priority and Low Priority Projects	
Input	
• Project brief • Planning policy and guidance documents • Abu Dhabi Safety and Security Planning Manual	
Task	
• Read the SSPM • Use the Decision Support Tool (DST) to gain an understanding of the importance of safety and security during planning	
Output/ Deliverables	
• Appointment of a safety and security consultant (if specialist support is required)	

Checklist
1. Do you understand the SSPM Principles?
2. Have you used the Decision Support Tool?
3. Do you need a specialist as part of your project team?
4. Do you know what you have to submit for safety and security as part of the Planning Submission?

Crowded Places

Crowded places are locations where the public can gain access and, by their nature, attract high crowd densities. Examples include but are not limited to, shopping malls, stadia, hotels and transport premises. Unfortunately, evidence from around the world shows that these locations are often targeted by terrorists. As such, developers of these projects will be expected to pay particular attention to safety and security and these projects will often require specialist input and review.

Stage 2: Planning

Within the context of Abu Dhabi, 'Planning' covers all those aspects of planning and design that lead the project towards a detailed planning approval. After planning approval, the project will be developed to obtain a building permit.

Initially, a project will be assessed by the whole project team, whereby various disciplines seek to analyse the existing site and its context. The project team will identify, explore and evaluate a number of planning options to ensure that the right concept is selected for further development. The Planning Toolkit (Chapter 4) outlines a series of planning tools that can be used in Abu Dhabi to reduce safety and security risks.

From the selection of the preferred concept, the project team moves forward to detailed planning, which requires a holistic approach to realising the project's safety and security objectives.

Low Priority Projects

Once confirmation has been received that a project is Low Priority, the project team should address the Principles (Chapter 2) alongside other planning objectives. There is no specific safety and security deliverable for inclusion in the Planning Submission, but the development review officer at the UPC or Municipality will assess compliance of all planning policy and guidelines, including the SSPM, in their review of the Planning Submission.

Collaboration

Team collaboration is best achieved through structured workshops that recognise the importance of safety and security. IDP records should be kept as evidence of this effort.

High Priority Projects

For the safety and security specialist, this is perhaps the most important stage in influencing the strategic outcome of the project. Good communication and information sharing will remain of paramount importance throughout.

It is at this stage that the specialist will interface for the first time formally, with Government safety and security advisors as part of the development review process. Initial discussions will focus on the project-specific safety and security risk assessment. The risk assessment, discussed in more detail in Appendix 1, should result in a Risk Summary Graphic that identifies the key risks to the project. A typical example is shown (opposite), and consists of marked up plans identifying vulnerabilities, site constraints and critical areas.

Following the consultation, the project safety and security brief can be developed and recorded. This document sets out safety and security priorities to be addressed during the remainder of the project development process. This should include any regulatory requirements, best practice (local, regional and international) and any requirement stemming from the owners project brief. It is important for this stakeholder group to reach consensus on the focus for safety and security and appropriate levels of protection. How well the project team address these priorities through planning and design will be evaluated using the safety and security components of the Planning Submission and the Building Permit Submission.

At this point the brief will be in place and the safety and security specialist, as an integrated member of the project team, will participate and lead workshops (as necessary), to find innovative and appropriate planning solutions. Invariably, this will involve compromise between the needs of safety and security and other planning objectives.

Once planning objectives have been balanced, a set of Safety and Security Plans should be produced to demonstrate how safety and security will be achieved for the project. The deliverables for the Planning Submission include:

Deliverable 1:
Risk Summary Graphic

Deliverable 2:
Access and Circulation Zoning Plan

Deliverable 3:
Safety and Security Plan

An illustrative set of deliverables are shown on the following pages.

Elements shown in the Safety and Security Plans must be fully integrated with the remainder of the Planning Submission. For example, elements relating to access and connectivity should be captured within the associated transportation plans, while urban design and Estidama proposals should be consistent with the Safety and Security Plans. If this is not clearly evidenced in the Planning Submission, the Government safety and security advisor may request IDP records and to see the project safety and security brief.

Deliverable 1: Risk Summary Graphic
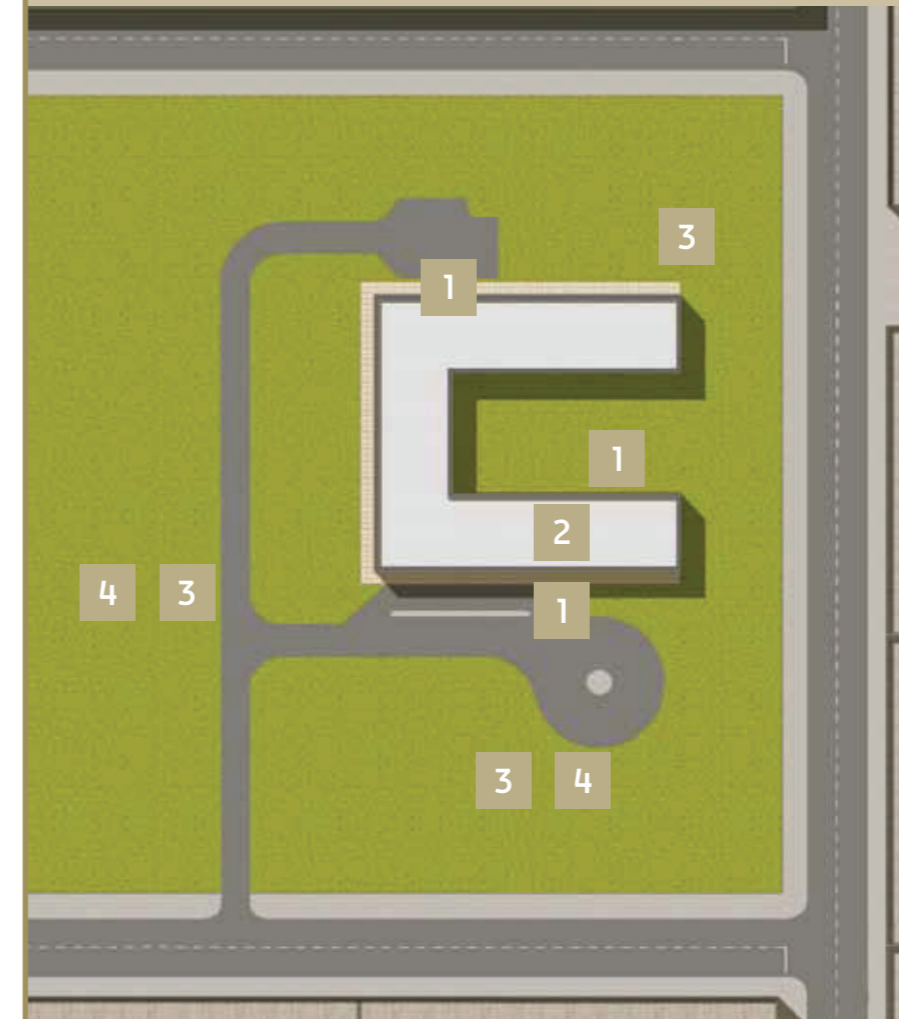
Consequence	Rare	Unlikely	Credible	Likely	Certain
Catastrophic			Risk1		
Major			Risk2		
Moderate					
Minor				Risk3	Risk4
Insignificant					

Likelihood

This risk matrix gives a representation of the identified safety and security risks to inform prioritisation.

Risks associated with concept plans

1

Risk 1:
vehicle-borne explosive attack on building

- No hostile vehicle mitigation treatment – vehicles can drive up to the building on all sides
- No stand-off distance between building and vehicular circulation areas
- Uncontrolled/unscreened access
- Parking and deliveries under the building
- U-shaped building would worsen impact of a blast

2

Risk 2:
person-borne explosive attack on building

- Free, unscreened access to site and building

3

Risk 3:
crime against person in public realm
- No features to encourage activity for natural surveillance
- Poor private / public space definition

4

Risk 4:
inappropriate behaviour and damage
- No distinction between public and private space
- No features to encourage activity for natural surveillance
- No sense of identity

Deliverable 2:
Access and Circulation Zoning Plan

Restricted zone		VACP = Vehicle Access Control Point
Private zone		PACP = Pedestrian Access Control Point
Semi-private zone		V_{Auth} = Vehicles (Authorised)
Public zone		V_{S+V} = Staff and visitors
		V_C = Vehicles (Commercial)

Deliverable 3:
Safety and Security Plans

Submitted as part of the Planning Submission for High Priority Projects.

	Rare	Unlikely	Credible	Likely	Certain
Catastrophic					
Major		Risk1			
Moderate		Risk2			
Minor			Risk3		
Insignificant		Risk4			

Consequence (vertical axis label)

Likelihood

This risk matrix identifies residual risks following the application of planning tools outlined in Chapter 4 of the Manual.

Planning tools used to reduce risks

1. Building located at centre of site to increase stand-off and reduce impact of security measures in public zone

2. Secure perimeter treatment

3. Building shaped to dissipate energy from blast

4. Stand-off distance (min 30m), also serves as gardens for site staff and visitors

5. Raised podium for vehicle access control

6. Critical infrastructure and connection within the site secure perimeter

7. Planting and shading to encourage appropriate activity in public areas

8. Pedestrian access control, just two entry points

9. Direct route funnels users to single building entrance

10. Controlled parking, outside HVM line

11. Vehicle access control with HVM measures, single entry point at secure perimeter site

12. Drop-off area for VIPs only

13. Indirect vehicle approach to building

14. Pedestrian access control and screening to building entrance

15. Clear sight lines to aid surveillance

16. Infrastructure (e.g. HVAC) placed away from possible interference

17. Back-of-house delivery area and screening, linked to building by foot tunnel

18. Emergency only access point (HVM line maintained)

Planning Summary Sheet

Input

- Project brief
- Planning policy and guidance documents (including SSPM)
- Site context
- External stakeholders (including Government safety and security advisors for High Priority Projects)

High Priority Projects	Low Priority Projects
Task	**Task**
Implement the SSPM Principles - Multi-disciplinary workshops - External stakeholder meetings - Conduct a project safety and security risk assessment - Preparation of a project safety and security brief - Development of deliverables 1–3, using the Planning Toolkit - Maintain IDP records of meetings and decisions	Implement the SSPM Principles
Output/ Deliverables	**Output/ Deliverables**
Planning Submission including: - Risk Summary Graphic - Access and Circulation Zoning Plan - Safety and Security Plans Other outputs - IDP records - Project safety and security risk assessment - Project safety and security brief	Planning Submission demonstrating implementation of the SSPM Principles
Checklist 1. Have you appointed your safety and security specialist? 2. Has the consultant led a series of safety and security focused workshops? 3. Do you know the key security risks to be addressed by the project? 4. Has the team consulted with a Government safety and security advisor? 5. Does the planning application demonstrate that safety and security risks have been addressed appropriately? 6. Have safety and security been balanced with other planning objectives? 7. Has the safety and security plan been integrated throughout the submission application?	**Checklist** 1. Have you implemented the SSPM Principles? 2. Does your submission show evidence of this?

Stage 3: Design

Following detailed planning approval, the project enters the Design Stage, which will culminate in a Building Permit that allows construction work to commence on the development site. The first design task in any project is to ensure that the detailed planning approval is read and understood, so that any conditions are addressed during design development.

The Building Permit process is led by the Municipality: Abu Dhabi, Al Ain or Western Region. Safety and security review by Government advisors (High Priority Projects only) will be captured as part of the existing review process.

During design development, the project moves towards increased design detail with safety and security elements captured in architectural design, urban design and system design solutions. The Design Toolkit (Chapter 5) includes a range of safety and security tools that can be considered for use in Abu Dhabi.

Low Priority Projects

As with the planning review for Low Priority Projects, there is no safety and security specific submission within the Building Permit Submission. However, the project team should be able to demonstrate that the project design implements the SSPM Principles alongside other design objectives.

The Municipality development review officer will assess compliance with the Principles alongside all design policy and guidelines, such as the Building Code and Estidama. They will seek evidence of implementation and integration in the construction documentation e.g. drawings and specifications.

High Priority Projects

The project team will continue in consultation with Government safety and security advisors. An advisor will provide the project safety and security specialist with inputs, offer advice and conduct a review of the Building Permit Submission.

Value Engineering

If a project goes through a value engineering exercise during design, safety and security objectives must still be achieved. It is an opportunity to reassess design decisions, but this should be done in line with the safety and security risks and objectives.
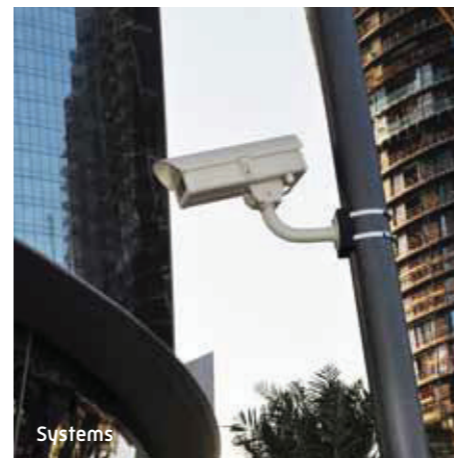
The project safety and security specialist will need to participate and lead a series of workshops to ensure safety and security design proposals are coordinated with other project team disciplines.

The safety and security specialist will employ a range of design tools from the Design Toolkit in order to achieve the project objectives. They will work holistically with other design disciplines to find innovative solutions. They are likely to provide marked-up drawings and design notes throughout design development.

Operations

Physical
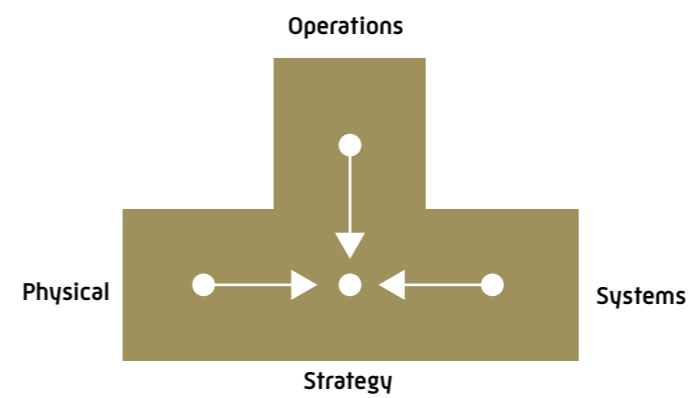
Systems

Strategy

The design effort will culminate in a Safety and Security Strategy Report which outlines the balance between physical, systems and operational elements that need to be incorporated to meet the project safety and security design objectives. This report will need to demonstrate that the key concept of defence in depth has been achieved and that the design solutions are appropriate and commensurate with the project risks. On this basis, the project risk assessment should be updated to identify residual risks following integration of planning and design solutions. The design stage concludes with a Building Permit Submission incorporating those outputs listed in the Design Summary Sheet.

Strategy

Physical

Systems

Operations

Design Summary Sheet

High Priority Projects	Low Priority Projects
Input	**Input**
• Planning approval (with/without conditions) • Project brief • Planning policy and guidance documents (including SSPM) • Design advice from Government safety and security advisor • Risk Summary Graphic • Safety and security brief • Safety and Security Plans • Access and Circulation Zoning Plan	• Planning approval (with/without conditions) • Project brief • Planning policy and guidance documents (including SSPM)
Task	**Task**
• Develop the design to address any planning conditions • Multi-disciplinary workshops • External stakeholder meetings • Develop the design referencing the SSPM Design Toolkit • Prepare the safety and security element of the Building Permit Submission	• Develop the design to address any planning conditions • Design with the SSPM Principles in mind
Output/ Deliverables	**Output/ Deliverables**
Building Permit Submission demonstrating implementation of the SSPM Principles, including: • Risk Summary Report • Safety and Security Strategy Report (Concept and detailed design) • Design drawings and specifications (Construction documentation) • IDP Records	Building Permit Submission demonstrating implementation of the SSPM Principles

Checklist
1. Have you addressed the planning conditions (if any)?
2. Have you conducted a series of safety and security focused workshops?
3. Have you consulted with external stakeholders?
4. Does your Building Permit Submission include evidence of how the SSPM Principles and Planning Toolkit and Design Toolkit have been implemented?
5. Is safety and security balanced with other design objectives?
6. Is safety and security integrated as part of the overall design?
7. Does your safety and security strategy have an appropriate balance between physical, systems and operational security elements?

Checklist
1. Have you addressed the planning conditions (if any)?
2. Does your Building Permit Submission include evidence that the SSPM Principles have been implemented?

Stage 4: Construction, Commissioning and Operations

During construction, the contractor's role is to build what is set out in the Building Permit. Unanticipated site conditions, value engineering or preferred construction materials and techniques can all lead to variations which may compromise the safety and security strategy.

Information Handover

After significant time and effort has been carried out in planning and designing the project with safety and security in mind, it is important that the operator is made aware of:

• Residual safety and security risks; and

• The safety and security features of the development.

This will ensure appropriate management and maintenance programmes can be put in place

Low Priority Projects

The contractor must work with the architect and engineers of record to ensure that any proposed variations do not contradict the Principles outlined in the Manual.

High Priority Projects

It is important at this stage that the safety and security specialist remains on hand to deliver support and evaluate any proposed design changes. This would typically involve scrutinising shop drawings to ensure design compliance and that the original safety and security objectives are met.

As in all other stages of the IDP, regular workshops with the contractor and project team will improve design quality and implementation of the design.

Upon completion of the project, there will be a need to commission safety and security systems to check that they are fit-for-purpose. The operator will need to receive all as-built drawings, Operations and Maintenance (O&M) Manuals and introductory training to ensure effective operation.

Construction, Commissioning and Operations Summary Sheet

High Priority Projects	Low Priority
Input	**Input**
• Building Permit (with construction drawings and Specifications) • Safety and Security Strategy Report • Risk Summary Report (updated)	• Building Permit (with construction drawings and Specifications)
Task	**Task**
• Ensure 'as-built' condition conforms to Building Permit • Check any on-site led deviations do not diminish safety and security objectives • Commission systems • Prepare O&M manuals for 'as built' • Prepare update Risk Summary Report (if required) • Prepare update Safety and Security Strategy Report (if required)	• Ensure 'as built' conforms to Building Permit • Check any on-site led deviations do not diminish safety and security objectives • Commission systems • Prepare O&M manuals for 'as built'
Output/ Deliverables	**Output/ Deliverables**
• 'As-Built' drawings • O&M manuals • Commissioning certificates • Updated Risk Summary Report (if required) • Updated Safety and Security Strategy Report (if required)	• 'As-Built' drawings • O&Ms manuals • Commissioning certificates

Checklist

1. Does the contractor have a copy of the safety and security information included in the Building Permit approval?
2. Does the contractor understand the safety and security requirements?
3. Has the construction deviated from the Building Permit design?
4. Has the project safety and security brief been achieved?
5. Has evidence of installation been provided to the future operator?
6. Are the safety and security measures 'fit-for-purpose'?
7. Are the safety and security systems managed, operated and maintained appropriately?

Getting the Right Advice

It is now necessary for all developers to consider safety and security as part of the development process and for some projects, this will require the appointment of specialists.

"The best collaboration occurs early in the project, when planners, designers and safety and security specialists sit down together to consider the problem"

Seasoned, multidisciplinary expertise is critical for fostering innovation. Well informed project teams develop strategies that successfully integrate safety and security with planning, architectural and site design and work well with operations and maintenance programmes. Team members who are aware of the latest techniques can take advantage of opportunities during the early planning and design stages to innovate and explore new concepts.

Project managers should expect and require that specialists and stakeholders actively contribute to planning and design workshops/ meetings and provide deliverables that facilitate decision making as early as possible in the IDP.

Safety and security specialists within a project team must collaborate with planners and other design disciplines in order to:

• Identify and determine which safety and security risks should be addressed;

• Develop strategies to manage those risks; and

• Create an effective planning and design solution that balances safety and security with project budget and client vision.

Safety and security roles and responsibilities need to be assigned as follows:

If a realistic budget or integrated process are not in place early in the project, then the opportunities for creativity and innovation are severely restricted.

Project Manager

- Selects safety and security specialists with sufficient and relevant expertise

- Sets realistic budget and schedules (incorporating safety and security)

- Is practical about managing risk

- Supports collaboration

- Understands the opportunities and orchestrates the team to achieve a holistic solution

- Leads the team to innovative and successful solutions

Planners & Designers

- Develop a holistic project plan and design

- Work closely with safety and security specialists to create flexible alternatives and innovative solutions

- Support collaborative teamwork

Client/Owners

- Support a long term strategy and comprehensive site design for the project

- Support long term management and maintenance

- Advocates realistic and innovative solutions that serve the property and the neighbourhood

- Shares expertise on the detailed operation and everyday functionality of the building and site

Safety & Security Specialists

- Conduct a site specific risk assessment

- Support development of innovative solutions

- Collaborate with other stakeholders and disciplines

- Seek and implement creative and flexible safety and security measures

- Advise on the balance between safety and security assurance, the level of risk and cost

Although the planning and design community has focused on safety and security for many years, there remains a limited number of completed projects that illustrate best practice. As a result, most companies do not have the background needed to lead successful, well-balanced projects. Project leaders must be selective to ensure that the chosen consultants possess the right expertise.

The level of involvement of each safety and security specialist will vary, depending on the type of project and the stage of the IDP. The chart on the following page outlines specific safety and security roles and responsibilities at each stage in the IDP.

In reality, a group of specialists may work together throughout the planning and design process to provide the highlighted deliverables. For example, it is appropriate for an engineer to be involved in early design to ensure that the safety and security strategy is achievable in engineering terms; equally it is important for a strategist to review the engineering designs to ensure the integrity of the strategy has been maintained.

Specific Safety and Security Roles and Responsibilities

Roles	Responsibilities		
	IDP Stage	Tasks	Outputs / Deliverables
Risk Analyst	Planning	Conduct a safety and security risk assessment	Risk Summary Graphic
	Design	Update the safety and security risk assessment	Risk Summary Report
Safety and Security Strategist	Planning	Formally captures any stakeholder requirements (including Government agencies) Conducts benchmarking research Develops a project safety and security brief Application of the Planning Toolkit Explore a range of solutions which meet the brief Develop the Safety and Security Plans	Safety and Security Plans Access and Circulation Zoning Plan Project safety and security brief IDP records
	Design	Application of the Design Toolkit to develop a holistic strategy	Safety and Security Strategy Report IDP records
Security Engineer	Design	Implementation of the strategy through engineering solutions	Specifications Design drawings Construction documentation

In general, most safety and security specialists are likely to be sourced from consultancy practices with relevant experience of the development process and the built environment.

These split into the following general categories:

- Specific safety and security risk consultancy practices;

- Management consultancy practices with an in-house safety and security capability; and

- Architectural and engineering consultancy practices with an in-house safety and security capability or appreciation.

In the future, Abu Dhabi will be considering the introduction of a system that will enable developers to better source and guarantee the level of service provided by consultancy companies working in the safety and security industry. This will involve benchmarking against systems employed internationally and regionally to determine what is most appropriate for Abu Dhabi. However until that system is developed, project managers should look at the knowledge, expertise, qualifications and relevant experience of potential candidates to ensure that they are capable of fulfilling the role required.

It is recommended that anyone requiring safety and security specialist services obtains the Curriculum Vitae for each specialist to ascertain their relevant level of expertise and competency; this should be verified against references where possible.

A Government safety and security advisor can provide further guidance if required.
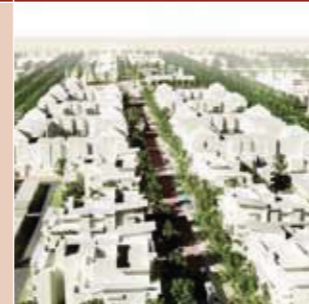
Institute Memberships & Vocational Qualifications

Selecting specialists that are registered with independent institutions or professional associations will provide confidence that the consultant is involved in continuous professional development activities and up-to-date with developments and advances in safety and security.

4

Planning Toolkit

Introduction

Chapter 4 presents a series of planning tools that may be used to implement Community Safety & Protective Security in a development project. The guidance contained here will assist developers and owners to implement the Abu Dhabi Safety and Security Planning and Design Principles presented in Chapter 2.

The Planning Toolkit includes international best practice, examples of innovation and draws on good existing examples from around the Emirate of Abu Dhabi. Decisions relating to what planning tools need to be applied and to what extent they are applied, are to be made as part of the Integrated Development Process (Chapter 3).

The Safety & Security Plans submitted as part of the planning application for High Priority Projects should demonstrate an integrated design solution and highlight the planning tools that have been adopted by the project.

Private and Public Ownership

Planners designate space for different uses. These spaces within the built environment are either public, such as parks and streets, or private land which is defined by a development plot. These two zones preserve land ownership rights and define roles and responsibilities for planning, designing, managing and maintaining space. A good planner will ensure design integration between public and private spaces while maintaining a clear distinction between the two. The assumption made in the 2030 Plans is that as much space as is practically feasible will be public.

This public and private land (development plots) can be viewed as a series of spatial layers, as shown in the figure below.

Asset | Building | Plot | District

Facade | Plot Boundary
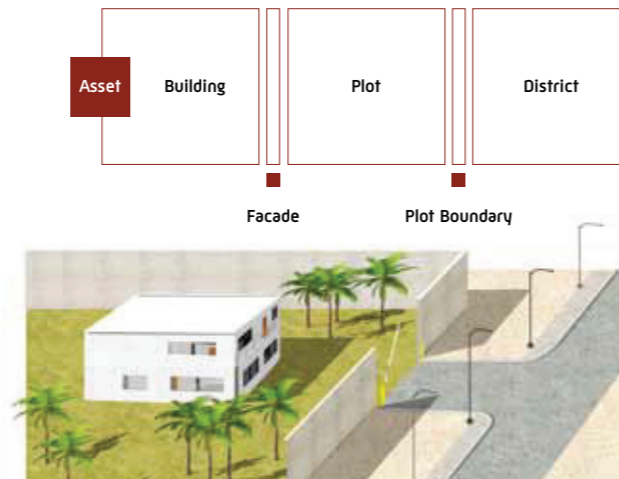
It is important to be familiar with these layers as they are used throughout the remainder of the Planning and Design Toolkits to highlight where spatially, the guidance presented in each tool can be applied. Equally important, the plot boundary is usually the constraint on where it is possible to implement access control and physical security for a project. That is unless an agreement is reached that allows the sharing of security measures with neighbouring plots or the placement of security measures outside the plot boundary.

Navigating the Planning Toolkit

There are ten planning tools provided in the Planning Toolkit. They are:

PT1 Site Selection

This tool highlights the importance of selecting the right use for the right place. It deals with land use compatibility, scale of development and how to deal with constrained sites where, because of gifting or competing development objectives, it is not possible to develop at a different location.

PT2 Access & Circulation Routes
PT3 Vehicle Access Control
PT4 Pedestrian Access Control
PT5 Service Access Control
PT6 Parking Placement

Tools PT2–PT6 are all directly related to a project's movement framework. High Priority Projects tend to require increased levels of access control and physical security to mitigate security risks. This requirement can influence spatial layout and, if these tools are ignored or not used correctly, can have a significant impact on the movement of people, vehicles and services at a development.

PT7 Infrastructure Planning
PT8 Topography
PT9 Building Orientation & Shape

Tools PT7 – PT9 deal with other safety & security planning requirements that will likely influence space allocation and site spatial planning.

PT10 Development Delivery

Tool PT10 highlights how important it is to consider development phasing at the project planning stage, particularly for larger developments where there is likely to be partial occupation before a development is complete.

100   4. Planning Toolkit

4. Planning Toolkit   101

A useful concept for all those involved in developing High Priority Projects is 'defence in depth'. This describes how obstacles can be arranged in multiple layers to make it harder for a criminal or attacker to reach a target. At each transition between spaces, there is an opportunity to establish a layer of security and implement access control. A safety and security specialist can use these layers to deter, delay, detect or deny intruders.

The level of protection afforded is only as effective as its weakest link. Therefore, care must be taken to ensure the layers of protection are balanced. The time to penetrate a layer and the probability of detection should remain constant; equally the transition or access control process at each point between layers should be consistent. No matter how many layers are in place or how well constructed they are, they are unlikely to be one hundred percent effective for one hundred percent of the time.

Best practice dictates that the higher the risk, the more layers are required and the more robust each layer should be.

Defence in Depth

A traditional example of defence in depth (Edinburgh Castle, UK)

Urban Context
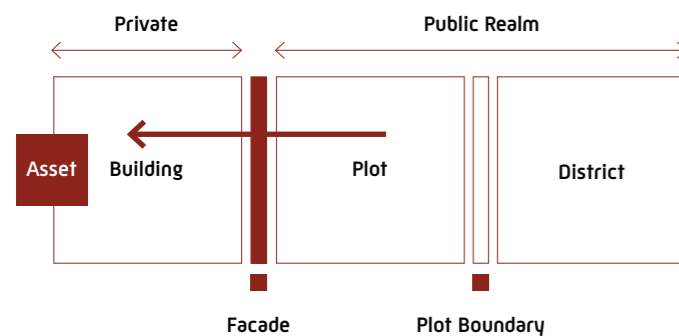
Only two layers of defence are afforded at the building facade and asset level

Open Site
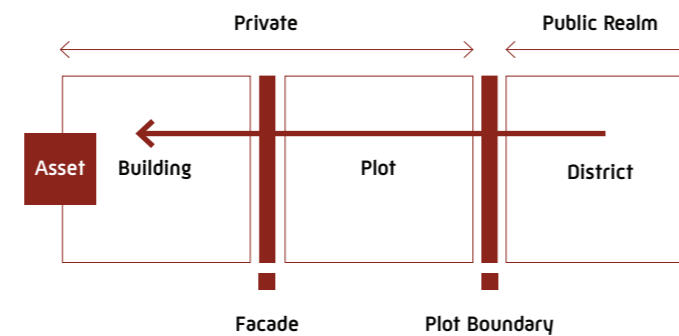
Here it has been possible to implement access control at the development boundary, again at the building facade and again at the asset

Access Control Zoning

The simplistic spatial model on the previous page does not address how to achieve defence in depth where there are multiple user groups who have different access rights to spaces, or how to deal with access control where there are multiple dispersed assets to be protected i.e. a single set of layers cannot be defined.

In this common scenario it is necessary to introduce a more sophisticated access control model to define the level of access control for different spaces within a development plot (private space).

Access control zoning involves the following stages:

1) Defining a series of zones with differing degrees of access control

Zone	Description & Examples	
Public	Public zones are normally accessible to everyone at all times with no automatic ability to impose access control measures.	Examples: Sidewalks, pavements, roadways, pedestrian links and tram ways.
Semi-public	Access to these areas is typically restricted outside normal business hours. Visitors are considered guests of the facility and their access may be limited at any time. For example, a retail mall is open to the public during normal operating hours. The mall may choose to restrict access to some individuals or choose to close at any time.	Examples: Retail, hotel lobbies, restaurants, bank lobbies, community facilities and public transit facilities (prior to ticket line).
Semi-private	Semi-private areas are predominantly for the use of a limited, authorised population. Visitors may enter, but are either invited or screened prior to entry. Semi-private facilities usually employ electronic or procedural access control measures that limit free public access to a lobby or reception area.	Examples: Sports events with accreditation checks on entry, office buildings, bank service areas, hotel guest areas and public transit facilities (beyond ticket line).
Private	Private areas are limited to access by authorised individuals and their guests. In commercial environments, guests are normally escorted within private areas.	Examples: Individual residences, internal offices and executive parking.
Restricted	Restricted areas are private areas that contain critical, essential or sensitive assets or are areas reserved for very exclusive groups (VIP). Access is usually limited to a very small group of people within an organisation. Access control measures to these areas may include biometrics, access token, etc. Guests are allowed entry but are always screened and escorted.	Examples: Data centres, IT rooms, security command centres, bank interiors and essential and critical infrastructure facilities.

Increasing access control →

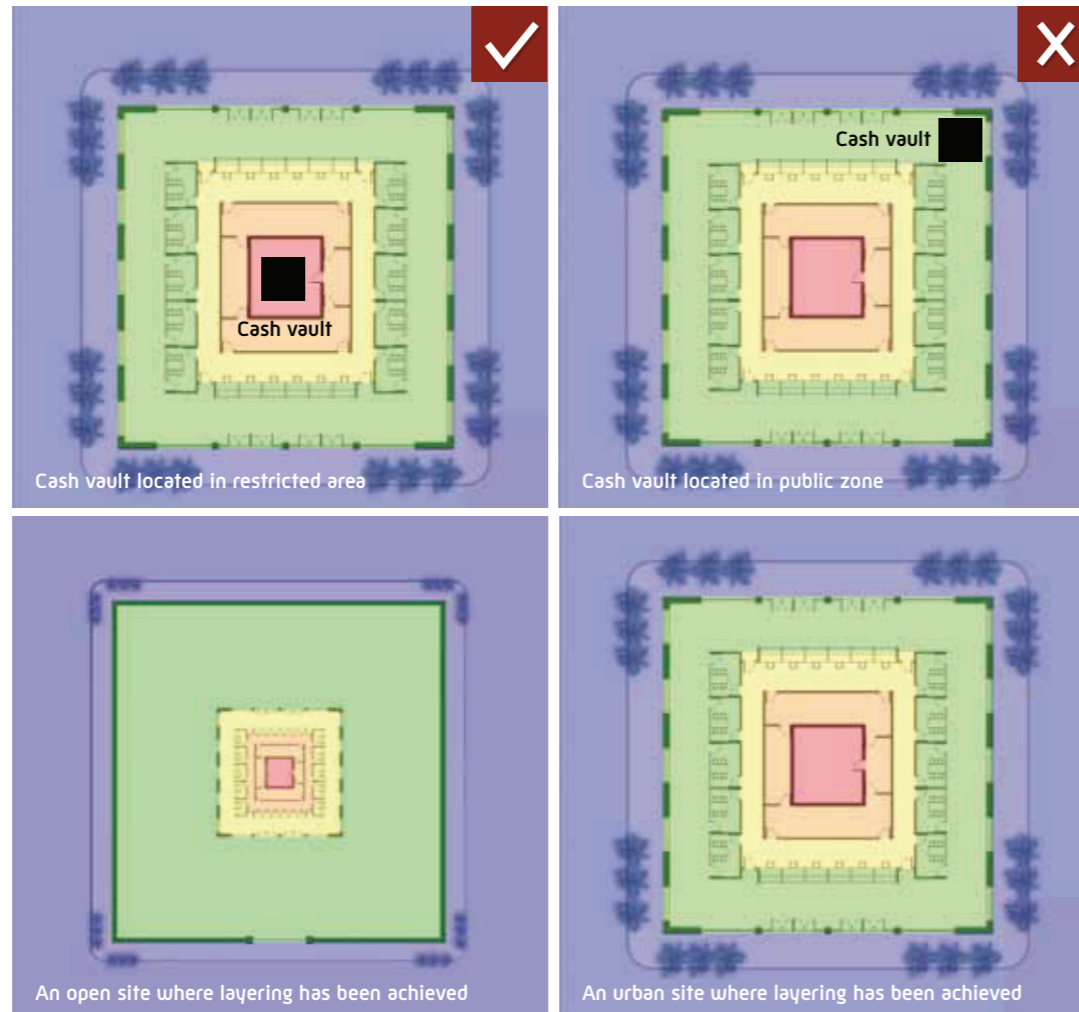**2) Locating assets that need protecting within an appropriate zone category**

3) Organising the zones in layers where practical

a) The layers should be organised so there is increasing access control

b) Wherever possible, avoid placing zones with extremes of access control adjacent to one another e.g. public next to restricted

4) Determining which users have access rights to these spaces and when they can have access

This effort will require a safety & security specialist to work with the project team and mark up plans and general arrangement drawings. This collaborative approach will avoid spatial conflicts, maximise opportunities to achieve defence in depth and forms the basis of an effective access control strategy.

Cash vault located in restricted area

Cash vault located in public zone

An open site where layering has been achieved

An urban site where layering has been achieved

Restricted zone		Semi-public zone	
Private zone		Public zone	
Semi-private zone			

Case Study – Mixed-use Development

In this virtual example, the access control zones show that there are different access control requirements for the office, public plaza and commercial areas. The office space is semi-private in the day and restricted at night, while the plaza remains publicly accessible 24 hours a day.

One of the retail units operates 24 hours a day, while access is to be restricted to the other, a bureau de change, out of hours.

Two years later, a Federal Government Agency moves into the development and this changes the access control requirements. The previously public zone spaces surrounding the offices must be restricted for security reasons. Initially, the Government Agency wanted the public plaza to be restricted access 24 hours a day. However, a compromise was achieved to allow the plaza to remain a public zone during office hours, allowing access to the commercial facilities. This required minor design modifications to the ground floor areas of the office block. This is a good example of the need for adaptability and the balancing of objectives between safety and security and other development objectives.
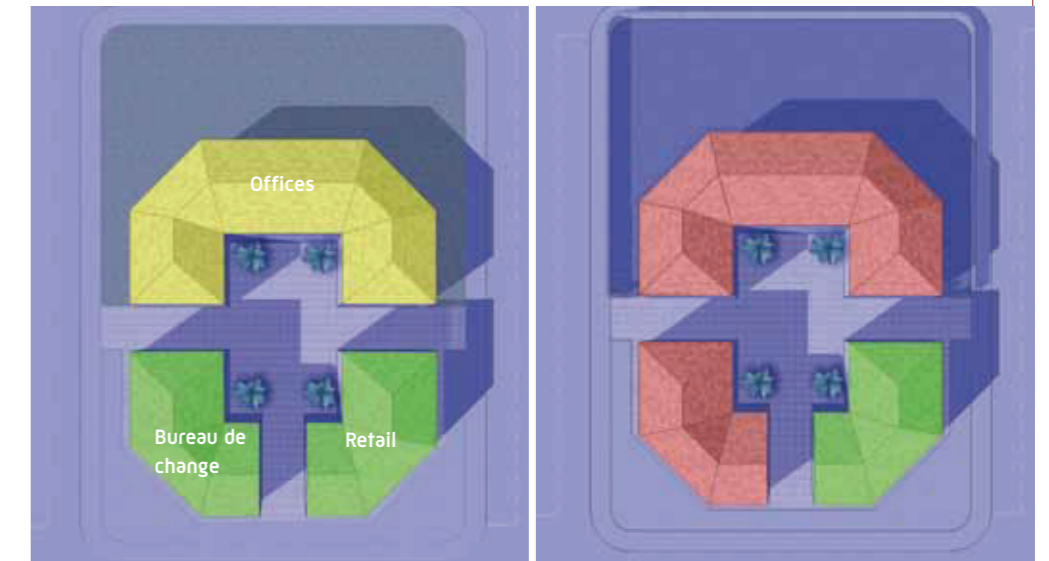
**Office hours
08.00 – 18.00**

**Night hours
18.00 – 08.00**

**Office hours
08.00 – 18.00**

**Night hours
18.00 – 08.00**

Restricted zone		Semi-public zone	
Private zone		Public zone	
Semi-private zone			
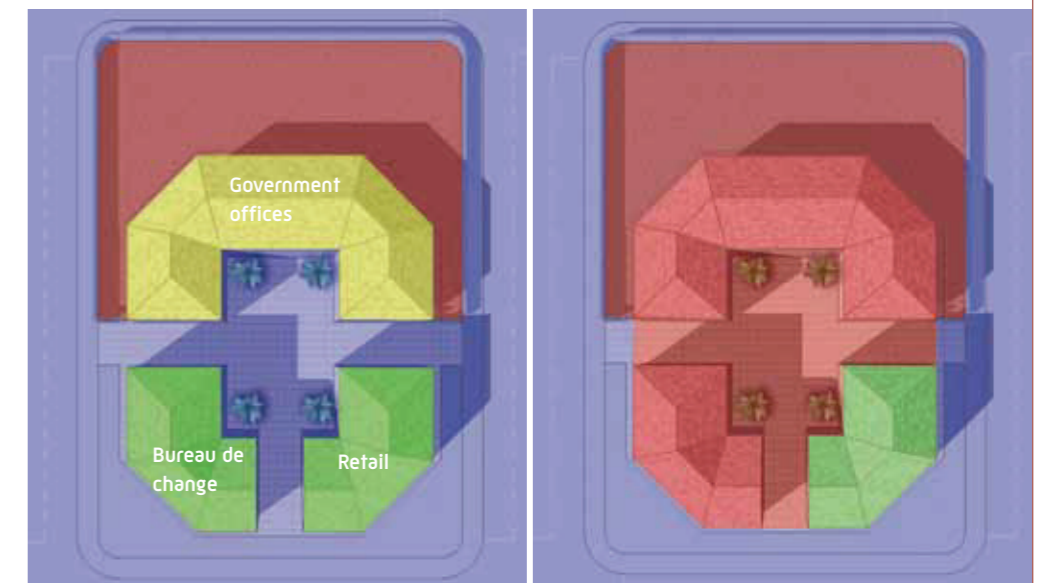
Introduction

The need to develop the right uses in the right places, away from conflicting uses, is at the heart of good urban planning and is equally important for safety and security. If a development is badly located, community safety may be negatively affected and it may be difficult or even impossible to achieve effective protective security. Mistakes in choosing the location of a development cannot usually be corrected in design or subsequent operations.

Planning Tool 1 (PT1) provides guidance for selecting an appropriate site for a development.

For those developers that are gifted land or for those with existing plots, the guidance contained here can be used to identify possible vulnerabilities that may need to be addressed using other tools in the Planning and Design Toolkits.

The challenge is to maximise the safety & security advantages that new development can bring to a community.

Land Use Compatibility

The Abu Dhabi Urban Planning Council has developed Urban and Regional Structure Framework Plans for each of the three municipal regions of the Emirate. These Plans, along with supplementary planning policy and guidance, are used to determine permitted land use for development plots. There are many land use dimensions that are considered in this decision-making process, including transportation needs, growth
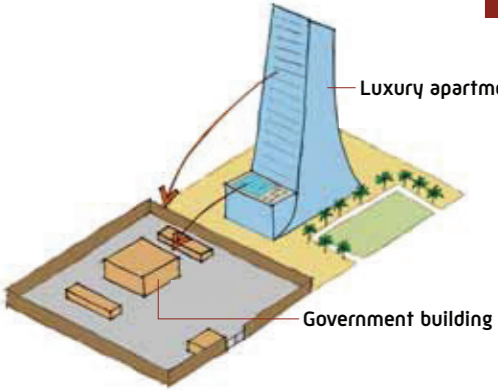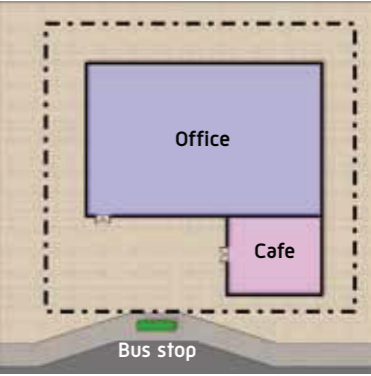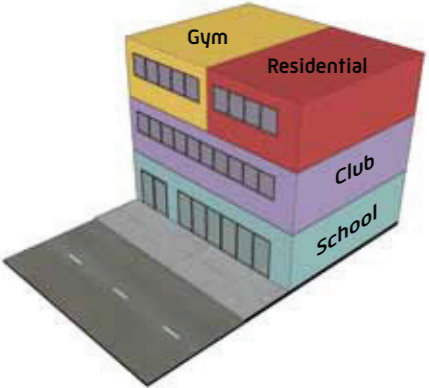
demands, Estidama principles and of course, safety and security. For obvious reasons, project-specific safety and security needs cannot be taken into account when allocating a permitted land use for a plot. For example, it may be appropriate for a commercial office to be located directly adjacent to a hotel but not for a Government office. In both cases, the intended use is office but the protective security needs are very different. This observation highlights the importance of the project owner and their development team working with a Government safety and security advisor to consider whether the proposed development location is appropriate for their project.

The types of questions that planners should ask when assessing land use compatibility include:

1. Would the relationship between the project and the community increase safety and security requirements?

2. Could the project introduce uses and users that will conflict with the existing community?

3. Would the level of activity associated with the new development be appropriate?

4. Could the project increase the local community's exposure to crime and inappropriate behaviour?

5. Could access control be achieved without disrupting the surrounding community?

Land use compatibility should be considered at all development scales, whether the project is a master plan involving numerous plots, a single plot development, or even when spatially planning a single building within a plot.

Land use compatibility at different scales

Master Plan	It is necessary to consider the relationships between the types of land use, their locations and their adjacencies to determine if they create any significant safety and security vulnerabilities. Particular care is required when considering the placement of land uses that tend to generate higher levels of risk e.g. royal palaces, military bases, heavy industry, hazardous material storage and group labour accommodation. As well as land use, the design of buildings on a plot may also create vulnerabilities. For example a high rise building such as luxury apartments immediately adjacent to a restricted Government building or military camp, may create line of sight issues. Development controls may be required to address this type of issue.	Luxury apartments — Government building
Site	The same principles also apply at a site level. The placement of buildings and their functions should enable effective site-level zoning. In this example, the commercial office, cafe and public transport location are compatible land uses.	Office — Cafe — Bus stop
Building	At a building level, as with the site level, spatial use and adjacency must enable effective internal zoning. In this example, a publicly accessible gymnasium is located on the top floor alongside residential apartments. This may be more appropriately located on the ground or first floor, enabling the upper floors to remain private.	Gym — Residential — Club — School

Scale Compatibility

If a development project is out of scale with the surrounding community uses, it can cause nuisance to existing residents and stimulate the fear of crime. An example is shown opposite.

In a constrained site, it can be difficult to implement access control and physical security. Therefore, if a project risk assessment identifies security as a high priority, then it will be important to select a plot that is sufficiently large to achieve defence in depth.

It is important that developers understand the development constraints on their plot. These are set out in planning policy and regulations and should be discussed with the UPC or the Municipality. For example, it may be possible in some cases to increase building height in order to decrease the footprint of a building while maintaining the desired Gross Floor Area of the project, This may offer additional space for the introduction of access control but whether this is permitted will be dependant on the regulations governing the particular plot proposed for development.
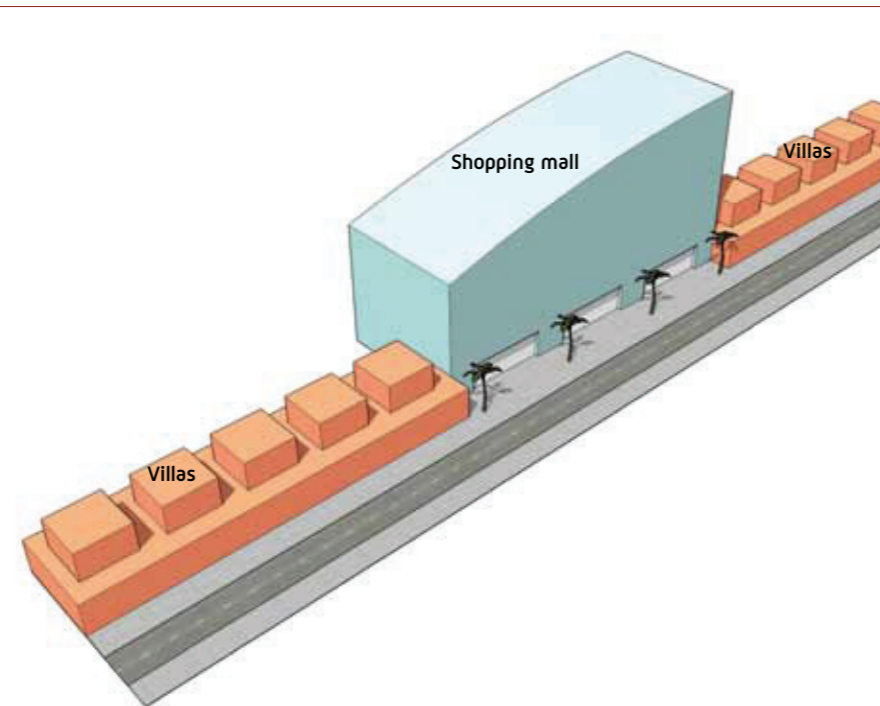
Out of scale facility may cause crime and nuisance for neighbouring residents

'Although rare, a project with high security needs may be required to develop in an alternative location where there is more space and a secure perimeter can be established'

Case Study –
US Embassy London

Due to an increased terrorist threat, the US Embassy in London needed to introduce additional physical security. Their constrained plot within Central London could not accommodate the new measures.

Ultimately this resulted in the Embassy moving to an alternative plot where security can be achieved.

An insufficient plot means that temporary physical measures have been erected in the public zone

Innovation –
Constrained plots

If a project is constrained by a small plot and physical security and access control improvements are required, it may be possible to implement measures at the district layer.

This involves the use of public land, and as the existing US Embassy example shows above, it is not always feasible to adopt space to respond to a changing threat. This will require innovation, careful consideration and consultation with stakeholders. Here, two plots share an access control point to facilitate increased stand-off.
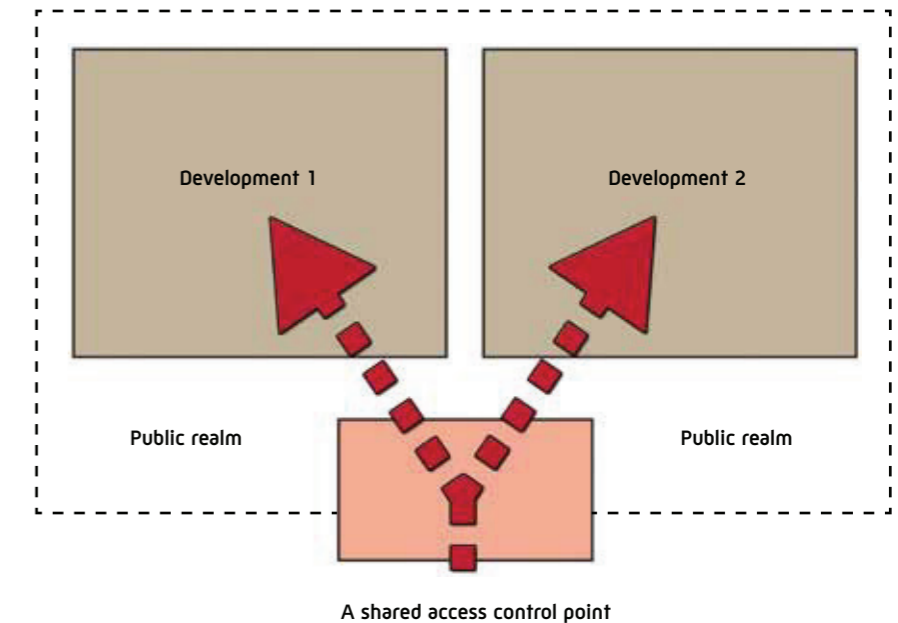
A shared access control point

Balancing Act – To Cluster or Disperse Buildings?

The pace of development in Abu Dhabi means that many projects will involve large-scale master planning and campus developments where it is possible for safety and security to influence plot allocations.

One of the required planning decisions will be whether to cluster or disperse buildings of similar risk profile. Do you put 'all your eggs in one basket' and protect them well or do you scatter them to reduce the probability of attack?

A concentration of buildings, physical assets, people and business operations in one location creates a target-rich environment for criminals or terrorists. An attack against one building is more likely to result in collateral damage to others and it presents the terrorist with multiple targets to attack simultaneously. However clustering of assets allows for a 'collective security solution' that can be more concentrated, more efficient and effective; response should be quicker and costs should be lower. Also as buildings have similar security requirements, entry points can be minimised and security measures and procedures can be more readily standardised. Clustering of buildings also allows them to be located further from public space i.e. the plot boundary; this should make it easier to implement defence in depth and help to maximise stand-off distance. By contrast, dispersal across a site (or multiple sites) reduces the risk that an attack on any one part will impact on the others and enables a less obtrusive security profile to be adopted. Both patterns have compelling strengths and weaknesses. There is no 'one size fits all' solution and planners should take advice from their safety and security specialist and external stakeholders.

Dispersed
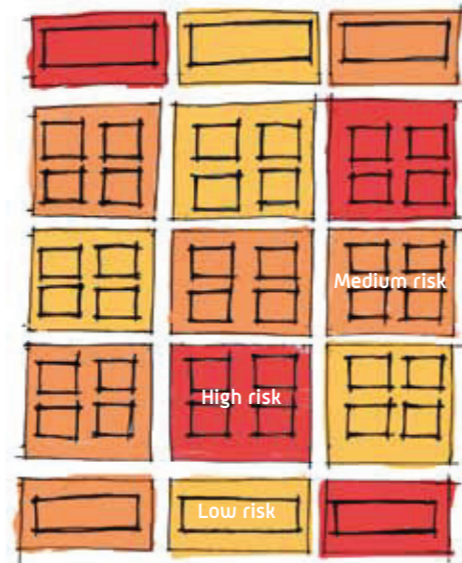
Clustered
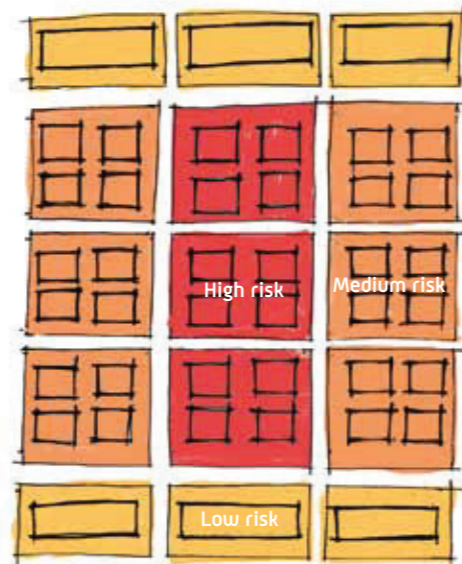
Examples of dispersal approach adopted (top image), and a clustered approach (bottom image)

Checklist

- Have safety and security needs been considered in the decision to develop on this site?

- Do safety and security needs suggest that the development would be better located elsewhere?

- Are neighbouring uses compatible?

- Does the development introduce safety and security risks for neighbours?

- Have buildings been clustered or dispersed depending on the safety and security risks?

PT2 | Access and Circulation Routes

Introduction

Principle P1 (Access & Connectivity) requires connectively to be maximised in projects, subject to this not compromising safety and security. It also highlights the need to plan pedestrian and vehicular routes with safety and security in mind. This section of the Planning Toolkit provides implementation guidance for urban planners and transport planners.

Access Control – Permeability

The project movement framework is used in planning to define how freely vehicles, people and materials can move into, out of and around a development. If a project-specific risk assessment identifies a need to introduce access control, this requirement should be integrated into the project movement framework. Any access control within the movement framework is expressed in the degree of connectivity in the layout of streets and pathways. Where risks dictate that the number of through routes should be reduced, the rectilinear block structure prevalent in much of Abu Dhabi can be easily amended. This is illustrated in the images (right).

Urban Street Planning & Design

The Abu Dhabi Urban Street Design Manual (USDM) should be used when designing streets in the Emirate of Abu Dhabi. The findings of the SSPM Benchmarking Report support its guidance for designing pedestrian orientated streets, where pedestrians and vehicles share streets, rather than isolating pedestrians.
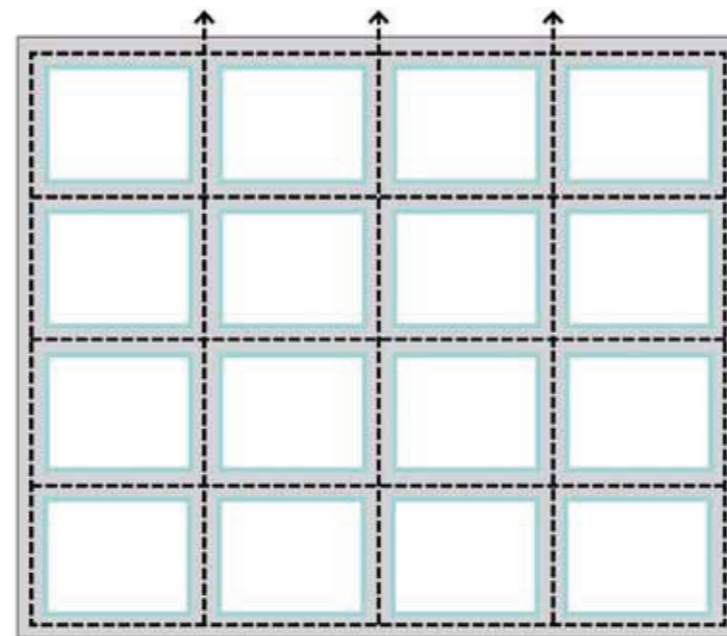
Permeable block structure suitable for a low risk site
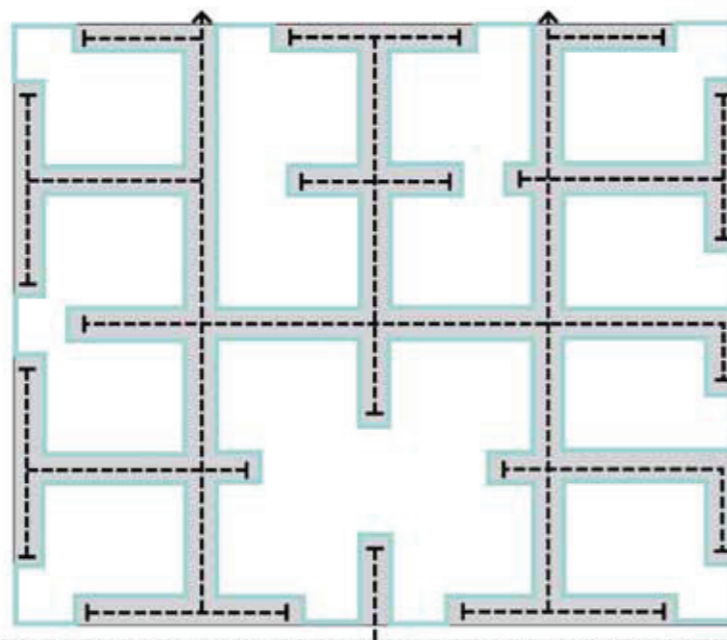
Where risks are higher, permeability may be curtailed by incorporating no-through-routes

Facade   Plot Boundary
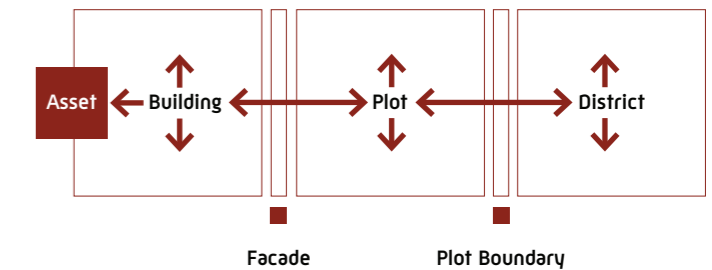
There are safety & security advantages of permeable and impermeable structures, these are identified below and should be compared with the findings of the risk assessment.

Safety and security advantages of well-connected layouts

- Clear views and easy orientation
- Easier to bring life to streets and improved natural surveillance
- Local facilities will be more accessible and so more viable
- Better emergency access

Safety and security advantages of layouts with fewer connections

- Easier to control access and create 'defensible space'
- Less chance of opportunistic crime
- Activity is directed towards certain routes and spaces
- Fewer escape routes for criminals
- Easier to monitor potential offenders

Pedestrian Route Planning

Segregated pedestrian-only footpaths and subways can lead to problems of crime and inappropriate behaviour. Isolation of users can make them vulnerable, as an offender is less likely to feel they will be seen or caught committing a crime.

The movement framework should establish a hierarchy of pedestrian routes and shared spaces. An emphasis should be placed on designing out or removing existing pedestrian routes, including sikkak, that are under-used because they do not connect to a specific destination. These can be problematic if they allow secluded access to the rear of plots.
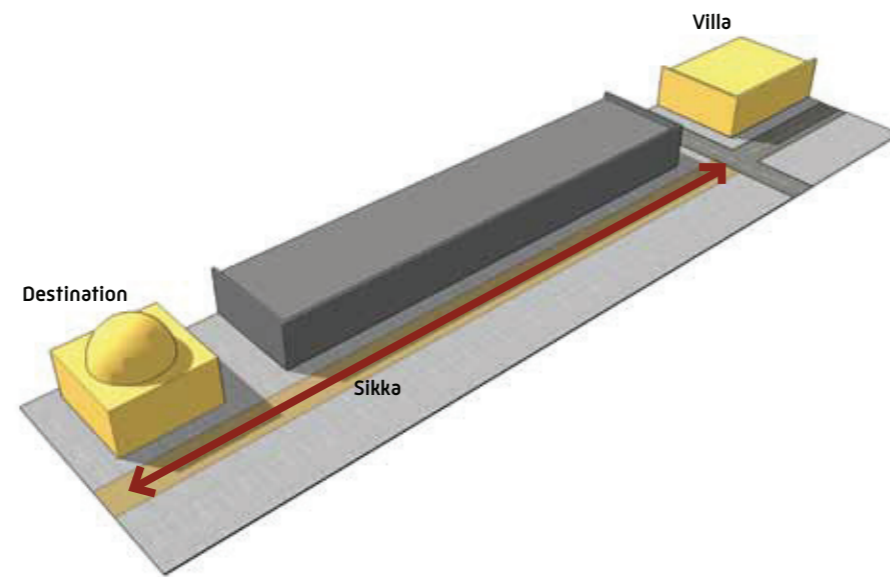
Here a Sikka provides a connection to a specific destination

Grade crossing - natural surveillance provided
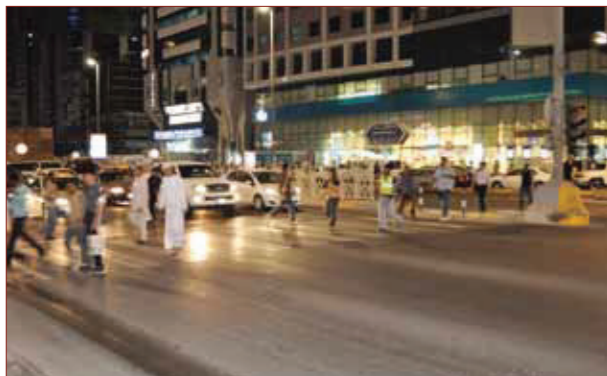
Subway

The use of subways are a last resort where other planning objectives cannot be met with at-grade crossings

Vehicular Route Planning

Planners highlight that the most efficient movement framework will take users on the most direct route to their destination. However, it is sometimes necessary for safety and security reasons, to use horizontal deflections to limit vehicle speeds in the vicinity of buildings deemed to be vulnerable to penetrative vehicle attack. This is discussed in more detail in Planning Tool PT3 'Vehicle Access Control'.

Even small reductions in speed on the approach to a target building will significantly reduce the impact on the building or the Hostile Vehicle Mitigation barriers installed to protect it. This can reduce the design specification and associated cost of the barriers presented in the Design Toolkit (Chapter 5).
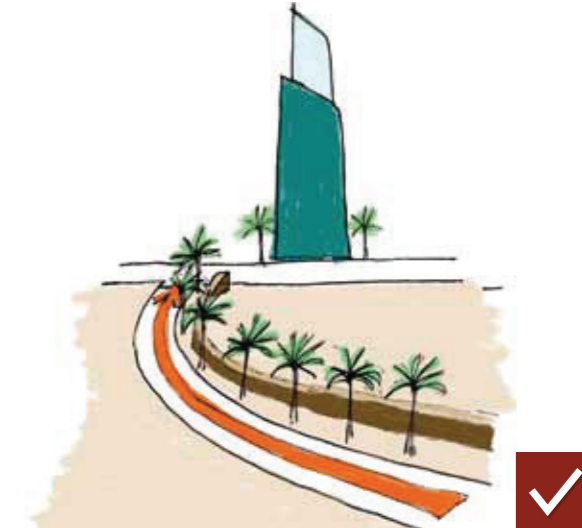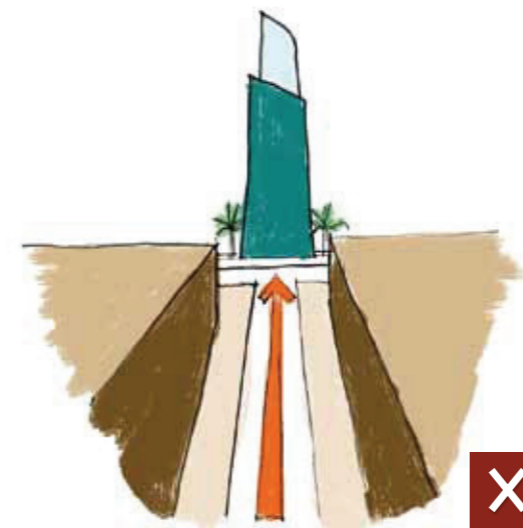
Emergency Access & Circulation Routes

The General Directorate of Abu Dhabi Civil Defence, in cooperation with the Municipalities, regulates and enforces minimum standards for emergency access.

These access and circulation standards are often more onerous than those for other vehicles, due to the need for large vehicles to gain access to buildings. Developers are responsible for addressing these access needs within the project movement framework plan.

There are two important planning criteria to be addressed when planning a project that has protective security needs:

1. Any proposal to introduce Vehicle Access Control (refer to PT3 Vehicle Access Control) shall be integrated into the movement framework to ensure appropriate emergency access is maintained.

2. Minimum access and circulation route standards may be insufficient to address the project-specific response requirements dictated by the risk assessment.

Desert Islands Civil Defence Station, Abu Dhabi

A vehicle borne improvised explosive device created a large crater at the only entrance to this embassy compound. This hampered emergency response vehicles attending the incident

Case Study 1 – Emergency Access during Construction

As a result of ongoing construction and phased occupation of a master planned community, emergency access and circulation routes for Civil Defence would change on a regular basis. Civil Defence were called on numerous occasions and their response was delayed due to changes in access points, new road layouts and a lack of wayfinding signage.


Construction Stage – Week 1

Construction Stage – Week 20
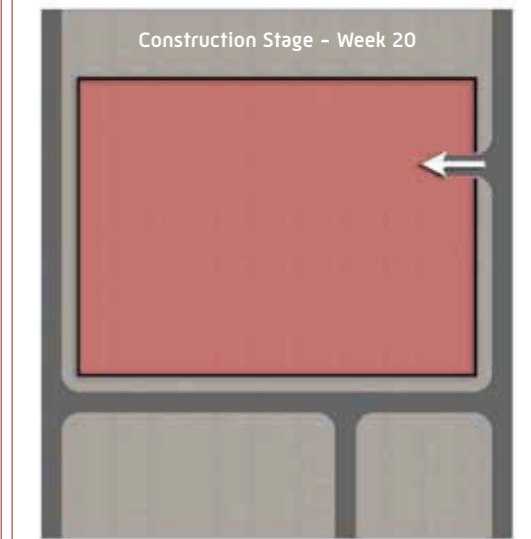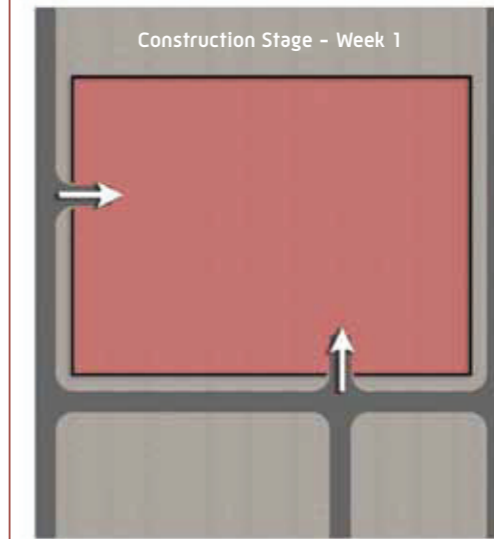
Changes to emergency access and circulation routes may change during construction effecting emergency response

Case Study 2 – Emergency Access

A development in Abu Dhabi had considerable difficulty obtaining Civil Defence approval after proceeding directly to design without planning for appropriate emergency access to high rise buildings.

Inappropriate project scheduling resulted in:

• Additional plot access which reduced achievable Gross Floor Area (GFA);

• Impaired emergency response; and

• Increased infrastructure costs.

Limited access
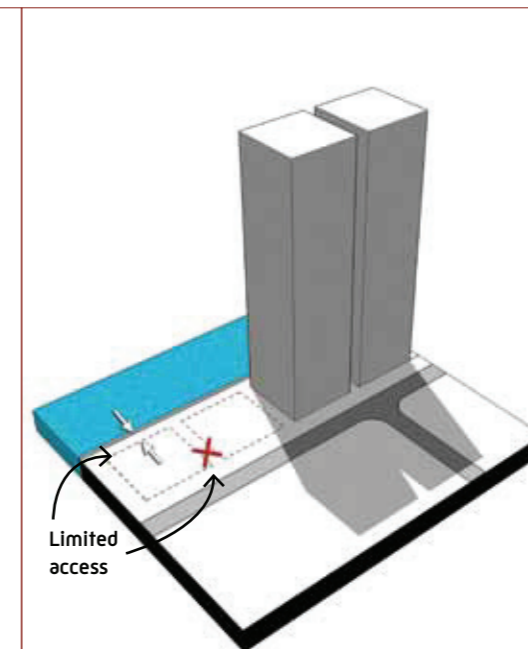
Inadequate access to high rise waterfront plots

Inadequate clearance heights under bridge structures

Vehicle Access Control – Movement Framework Integration

If it is necessary to close public streets for vehicle access control, which could be avoided by selecting an appropriate development site, the impact of such measures must be taken into account when testing a project's movement framework. Temporary road closures introduce significant disruption. They can result in significant transport delays including delaying emergency responders. They are not a sustainable solution and project teams should collaborate with stakeholders to find aspirational and innovative solutions.

Access control induced delays at Wembley Stadium, London UK

Case Study – Canary Wharf, London

A vehicle borne terrorist threat from the Provisional Irish Republican Army (PIRA) against this London financial district led to the development of a security zone.

Neighbouring sites with similar security needs share vehicle access control and physical security arrangements.

This allows security to be 'scaled-up' in response to increased threat. An appropriate amount of stand-off would not have been possible without a collaborative approach.

Vehicle entry control

Vehicle entry control

Vehicle entry control

Vehicle entry control

- - - - Area with restricted vehicle access
⚠ Warning signage
🛑 Anti-ram road blocker
🚫 Vehicle boom barrier
🚌 Public transport route
🏠 Guard house / check point
🚶 Footpath – No vehicle access
📹 CCTV monitoring
🌿 Planter

A plan of Canary Wharf, London, UK

Signage & Wayfinding Systems

A well-planned movement framework will create a development that requires few wayfinding signs. Signage can supplement cues from the built environment that support wayfinding by pedestrians and drivers.

Signage should make navigation easy for first-time visitors. Signage should be part of a hierarchy of wayfinding elements. It should be consistent, using a unified visual language of fonts, colours, scales and symbology. It is good practice to consult with the Municipality during the development of a wayfinding plan. The Abu Dhabi Public Realm Design Manual should be referred to, and conformed with, if any form of signage is inserted into the public realm.

Checklist

- Do footpaths run alongside streets, as opposed to being segregated?

- Do segregated paths have a defined function, such as leading to a specified facility?

- Is the movement framework structured to reduce the risk of vehicle attack of vulnerable buildings, spaces and assets?

- Have the implications of access control on the remainder of the wider movement framework been assessed?

- Is access controlled for all people and vehicles or just some? How will this be achieved?

- Do user groups need to be separated?

- Are the mandatory standards for emergency access met?

Well planned spaces require few wayfinding signs

Signage should make navigation easy for first time visitors

Vehicle Access Control

Introduction

Criminals may use a vehicle to force entry into a site, cause malicious damage or as an aid in a terrorist attack. These attacks can be sophisticated and past incidents indicate that vehicles are a preferred means for delivering Improvised Explosive Devices (IEDs) due to the speeds, manoeuvrability and payloads offered by vehicles.

Vehicle access control is used to prevent unauthorised vehicle access and to reduce vulnerabilities to attacks involving vehicles. This section of the Planning Toolkit provides guidance for implementing vehicle access control where justified by risk assessment. It highlights a full range of access control options, ranging from high to low security. It offers innovative ideas for constrained developments and outlines the additional benefits of introducing the most aspirational form of vehicle access control;'Total Vehicle Exclusion'.

Vehicle Attack Tactics

Vehicles may attack a target using one or a combination of the following tactics:

1. Parking underneath or next to a building

2. Encroachment into a site by bypassing or breaching access control measures without force

3. Penetration – using the vehicle to forcibly breach access control measures, the site perimeter, or building facade

Attackers may also resort to the following tactics where access control measures are installed:

4. Duress – such as forcing the driver of a legitimate vehicle to carry an explosive, or a guard to grant access, through a vehicle access control point

5. Deception – such as the use of a Trojan (disguised) vehicle or cloned ID

It is important that the threat to a project is clearly defined and understood. This will require consultation with stakeholders.

Vehicle Exclusion or Vehicle Inclusion?

From a security perspective, the best way to deal with vehicle attack threats is to exclude vehicles from a site altogether. However, at most buildings, especially crowded places, other planning objectives such as access and parking requirements will require compromise.

Total vehicle exclusion is more likely to be appropriate and proportionate where the risk of a vehicle attack is high. It may be neither possible nor necessary to adopt this approach at low risk sites.

Where vehicle inclusion is adopted, access for authorised vehicles, such as the emergency services and approved delivery vehicles, will need to be controlled at Vehicle Access Control Points. Even where the very best operational security regime is in place, a project adopting vehicle inclusion will remain vulnerable to attacks using Duress and Deception tactics.

Vehicle exclusion

Vehicle inclusion

Asset   Building ← Plot ← District

Facade   Plot Boundary

Stand-off

'Stand-off' is the distance between a structure and a physical barrier designed to protect it. If a risk assessment concludes that there is a high risk associated with a Vehicle Borne Improvised Explosive Device (VBIED) attack, then it is important to use stand-off to reduce the impact of an attack. This is best achieved at the planning stage of a project.

In new developments, if the right site has been selected, it should be possible to introduce adequate blast stand-off distance or enhance the structural design of a building to make it more resilient to blast loading (See Chapter 5 – Design Toolkit).

Vehicle Access Control – Planning Options

Four vehicle access control planning options are presented here. They range from an aspirational vehicle exclusion scheme, through to a scheme that affords no access control. The latter would leave a project vulnerable to any form of vehicle attack.

It is important to remember that even if a risk assessment identifies a low risk for this type of attack at present, changes in threat, occupiers, and special events may warrant protection in the future. Planners should consider future adaptability.

Whichever of the options is adopted, there is a need to integrate emergency access and circulation routes in accordance with minimum standards.

EVERY METRE MATTERS

10m   20m   30m   40m

Stand off
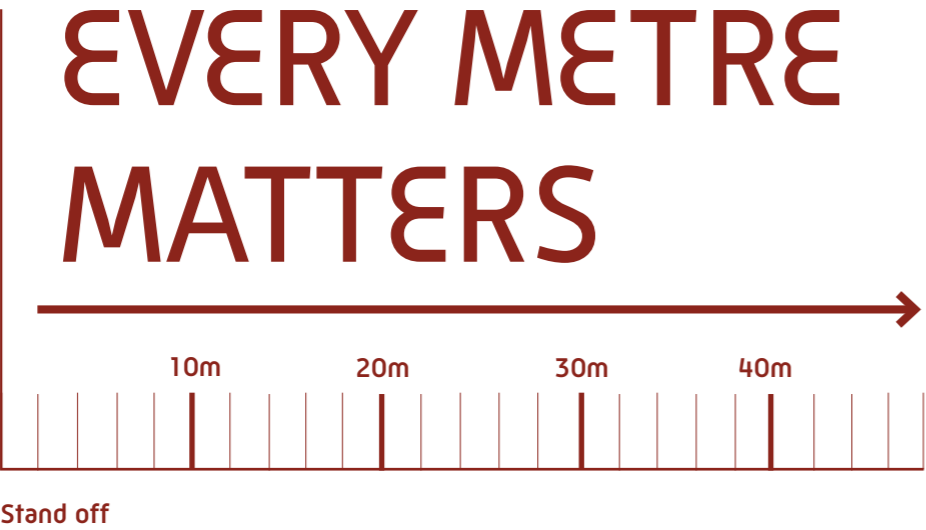
Option 1:
Total vehicle exclusion zone

Maximum protection from vehicle-borne attack and can make for welcoming pedestrian environment. A good example is the Washington Monument (USA) pictured above
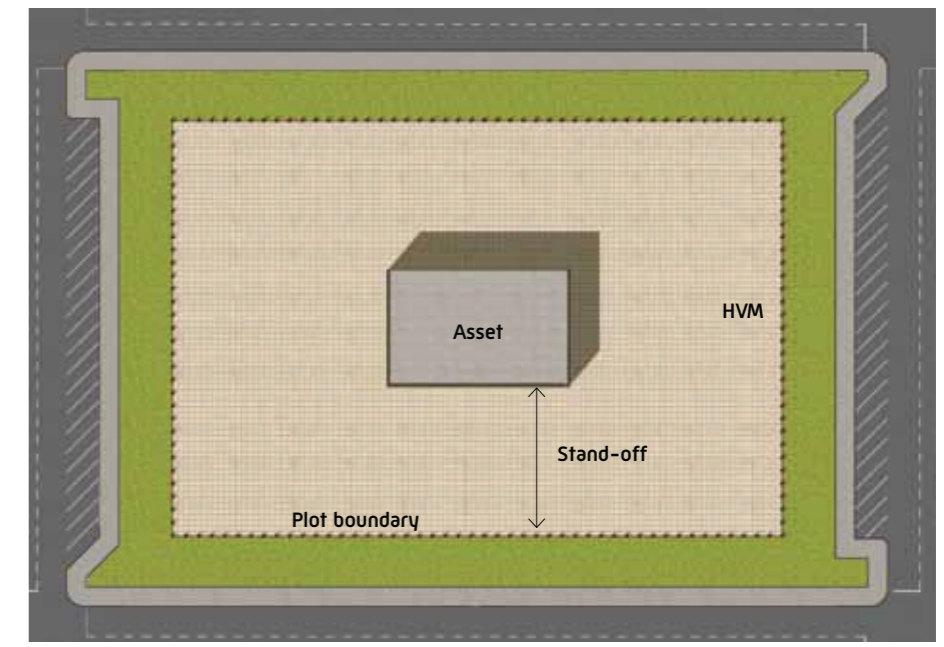
Option 2:
Asset vehicle exclusion

Continuous HVM Line

Continuous HVM Line

Excellent protection from vehicle-borne attack, and other forms of attack

+ Security −

Asset

HVM

Stand-off

Plot boundary

+ Security −

Parking

Asset

Parking

HVM

Stand-off

Plot boundary
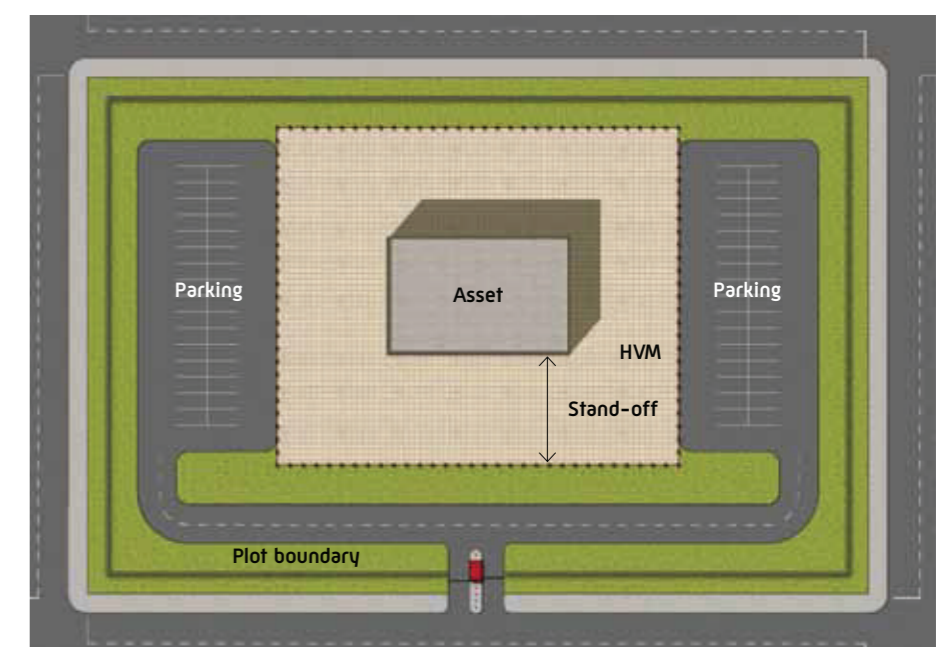
Option 3:
Vehicle inclusion

Access is possible using vehicle attack tactics 4 and 5 even if a 360^0 HVM line is installed and operated effectively

+ ——— Security ——— −

HVM

Asset

Parking

stand off

Plot boundary

Option 4:
Vehicle inclusion,
no secure HVM perimeter

In this option, urban design and architecture have complete freedom but the site is very vulnerable to all vehicle attack tactics

+ ——— Security ——— −

Asset

Parking

No VACP
No HVM

Plot boundary

This existing building is set-back from the street. It would be relatively simple to introduce stand-off if deemed necessary
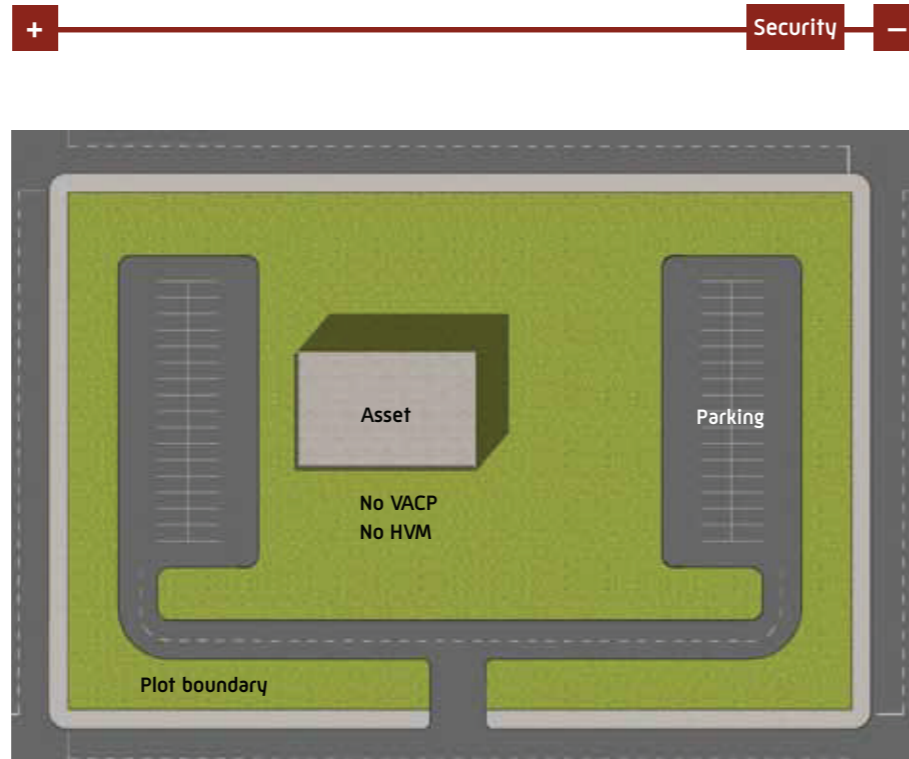
These existing buildings are constrained and if stand-off is required, it will be a significant challenge to implement

Complementary Planning Objectives

An innovative planning team will identify complementary planning objectives that increase the likelihood that stand-off and vehicle exclusion will be implemented for a project.

A series of benefits and examples of developments that have introduced vehicle access control for non security reasons are presented here.

Masdar City is an emerging global hub for renewable energy and clean technologies. This modern Arabian city is car-free. High-tech driverless pods transport users into the city. This introduces major security advantages for the city, even though this was not the principal planning objective

At the Al Forsan Club (Abu Dhabi), vehicle access to the club is controlled, with only VIPs and club members able to utilise on-site parking. Visitors park outside the site boundary and gain access on a courtesy bus. Although this access control is primarily for exclusivity, it benefits security and access could be controlled further or excluded altogether if there was an increase in threat (adaptability)

This park has been planned to exclude vehicles

Pedestrian-only public realm (Sheikh Zayed Grand Mosque, Abu Dhabi)

Public realm spaces within a vehicle exclusion area can be used to create public plazas, outdoor souks, a park, or similar uses that contribute to the community

District-wide Vehicle Access Control Solutions

Every metre matters when it comes to the protection of buildings from a vehicle borne improvised explosive attack. In constrained urban areas, publicly owned land (space outside the development plot) may be used to reduce blast vulnerability subject to the following planning conditions:

- Risk assessment justifies blast protection and the most appropriate solution is additional stand-off;

- Relevant stakeholders, including the Municipality, issue a 'No Objection Certificate'; and

- Demand analysis confirms that any proposed road closures can be accommodated by the local movement framework.

Two options for enhancing security for projects constrained by their urban setting are presented below.

(1) The Security Zone – Collective Vehicle Access Control

A cluster of buildings with similar security needs may share vehicle access control facilities by creating a district security zone. This collective approach is often most feasible for master planned developments, although the potential for large stand-off distances and cost savings brought about by shared access control facilities, might make this an attractive option.

Vehicle access is controlled to this campus of Government buildings in Melbourne (Australia)

The 'Ring of Steel' surrounding the City of London (UK), Is an example of a district-wide solution to mitigate the risk of VBIED

(2) Planned Street Closures

A planned closure of streets surrounding a vulnerable building may be an option where traffic demand is low and even welcomed if it creates new public realm space for use by the local community.

Street closure, Central London, UK

Shopping Mall   Hotel
Vehicular route (via public road)

Shopping Mall and Hotel
Vehicular route (via public road)
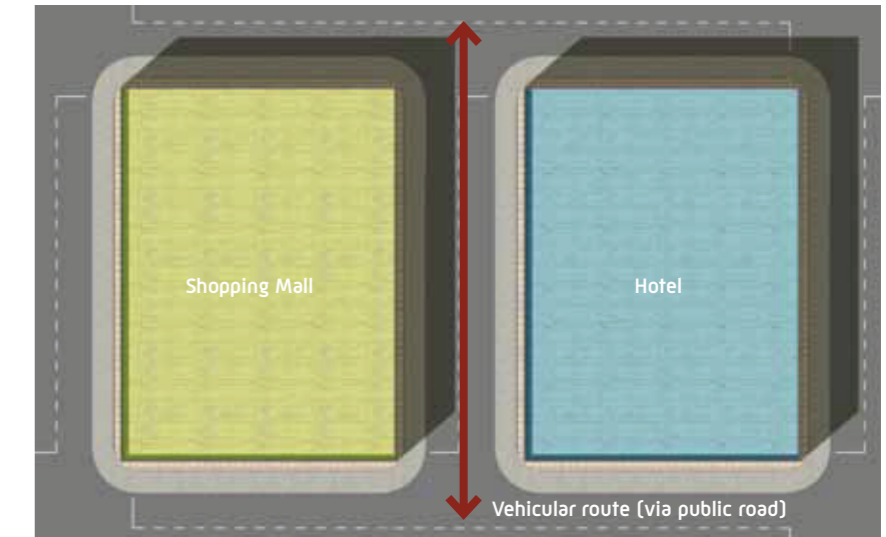
A pedestrian-only public realm space has been created between the hotel and shopping mall

Vehicle Access Control Points

Where vehicle access control has been introduced and vehicle inclusion is required, then it will be necessary to introduce one or more access control points.

These points are used to ensure that only authorised vehicles can gain access to the access controlled zone. A well planned and designed access control point will deliver effective security checks while maximising the rate of entry for authorised users based on a demand analysis.

Typical attributes of Vehicle Access Control Points:

1. Placed such that the surrounding road network can handle the traffic demand and minimum processing rate.

2. Spatial requirement determined by demand and required security checks. These could range from credential checks or include full search and screening regimes.

3. Planned so that any queuing does not impede the traffic flow on the surrounding road network.

4. Planned so that vehicles do not need to reverse or enter the site to be rejected.

5. Placed either in a location offering a level approach or preferably where there is a gentle rise to offer reduced approach speed and clear sight of approaching vehicles from the control point.

The access control strategy may identify different access control needs for different user groups. For example, it may be necessary at a football match to search normal ticket holders while allowing VIPs or the players to enter the stadium without a security search. At industrial and commercial buildings it is common for trusted staff to be given different access rights to visitors.

At the planning stage this is likely to have implications on the number of access control points, the amount of space allocated for access control and the location of access control points.

Typical vehicle access control points at existing developments in Abu Dhabi
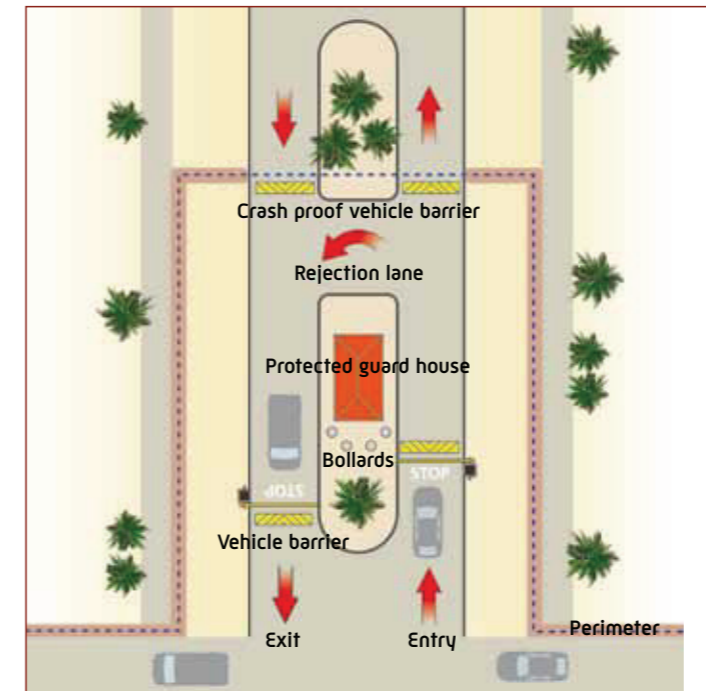
A typical high security vehicle access control point

Emirates Palace Hotel, Abu Dhabi

Checklist

- Is there a threat from vehicle attack?

- Does the risk associated with a vehicle attack warrant vehicle access control?

- Is vehicle exclusion or vehicle inclusion more appropriate?

- Does the movement framework accommodate access control?

- How much stand-off is appropriate?

- Have any associated benefits of incorporating stand-off been identified?

- Are vehicle access control points required?

- Have vehicle access control points been planned to accommodate the anticipated vehicle demand?

PT4 Pedestrian Access Control

Introduction

If a risk assessment has determined that pedestrian access control is required for security reasons, then there will be a need to determine whether to control access at the plot boundary, at the facade of the building, or after pedestrians have entered a building. An appropriate solution will balance access and connectivity with the level of security needed.

Unlike vehicle access control, pedestrians cannot be excluded from buildings, and in crowded places in particular, introducing excessive access control will not only disrupt normal operations but could discourage visits by legitimate users.

This section of the Planning Toolkit outlines a series of planning options for pedestrian access control, along with advice for developers and owners of constrained development plots. Design guidance for pedestrian access control is presented in the Design Toolkit (Chapter 5).

Pedestrian Access Control – Planning Options

Four planning options are presented for pedestrian access control. They range from an aspirational high security plan, where space is allocated at the plot boundary, to the lowest level of security, where no provision of space has been made, with multiple entry points around a building facade.

It is important to remember that even if risk is assessed as being low at present, changes in threat, the occupiers of the development or special events may warrant additional protection in the future. It is often difficult to allocate additional space for pedestrian access control post construction and therefore planners should be considering adaptability.

Whichever option is adopted, there is a need to integrate pedestrian access control with the vehicle access control and service access control strategies.

Asset ← Building ← Plot ← District

Facade   Plot Boundary
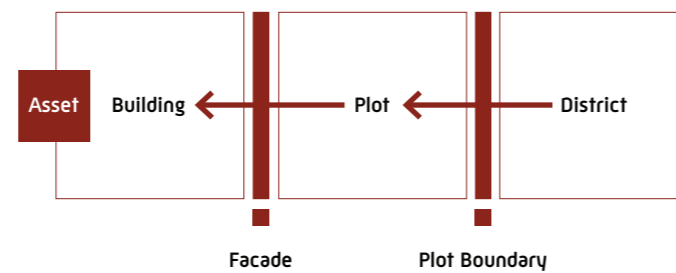
Option 1: Plot boundary pedestrian access control

Access control and searching occurs at or near to the plot boundary, enabling less control and more flexibility at the building entrances

+ Security −

Secure perimeter
Primary entry
PACP
Lobby
Asset
Secondary entry
Parking

Practical at special events, high security facilities and industrial premises where most visitors are staff or approved contractors

Option 2: Building extremity pedestrian access control

Access is controlled at the building facade in a dedicated lobby. The remainder of the facade is secured to prevent circumvention
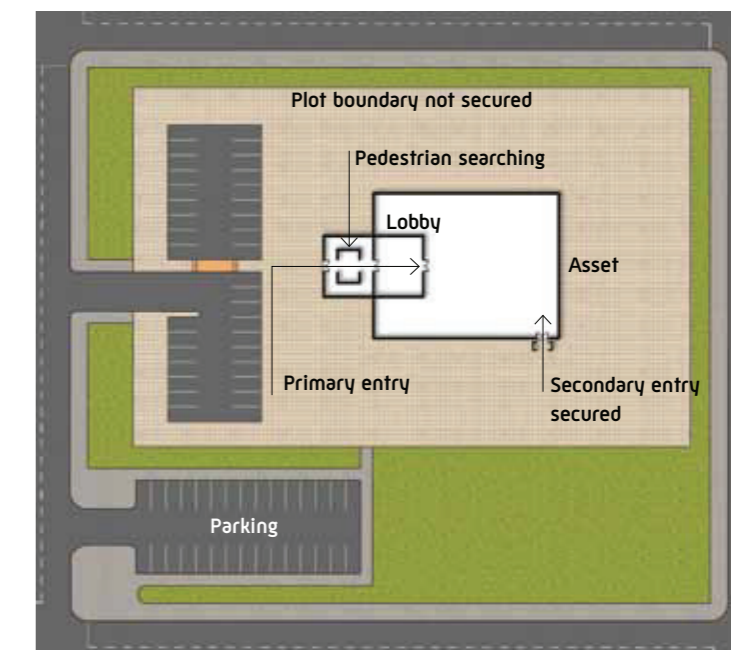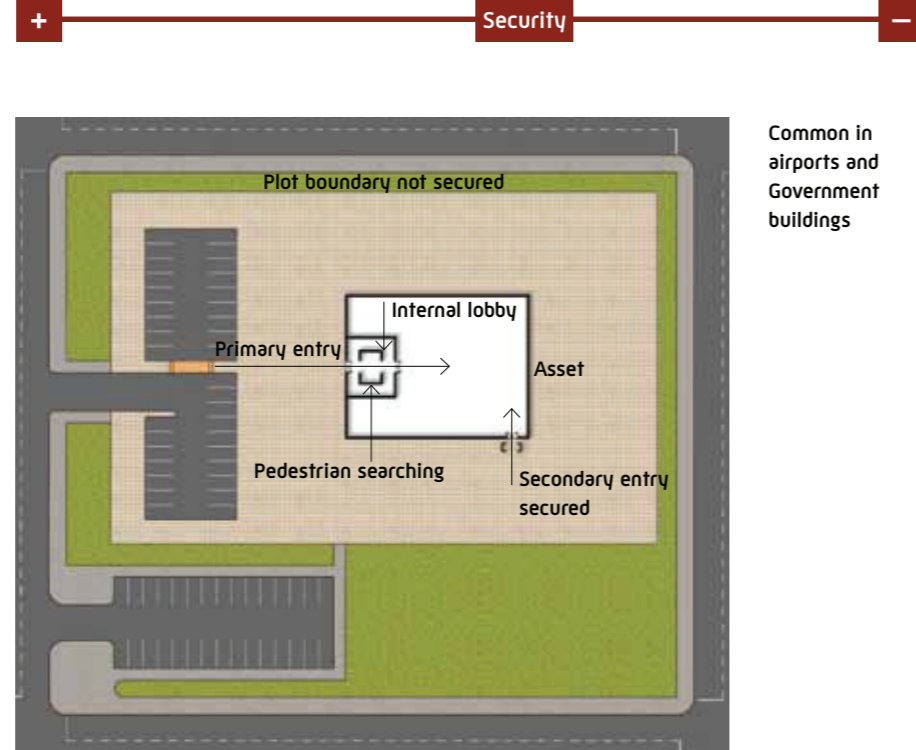
+ Security −

Plot boundary not secured
Pedestrian searching
Lobby
Asset
Primary entry
Secondary entry secured
Parking

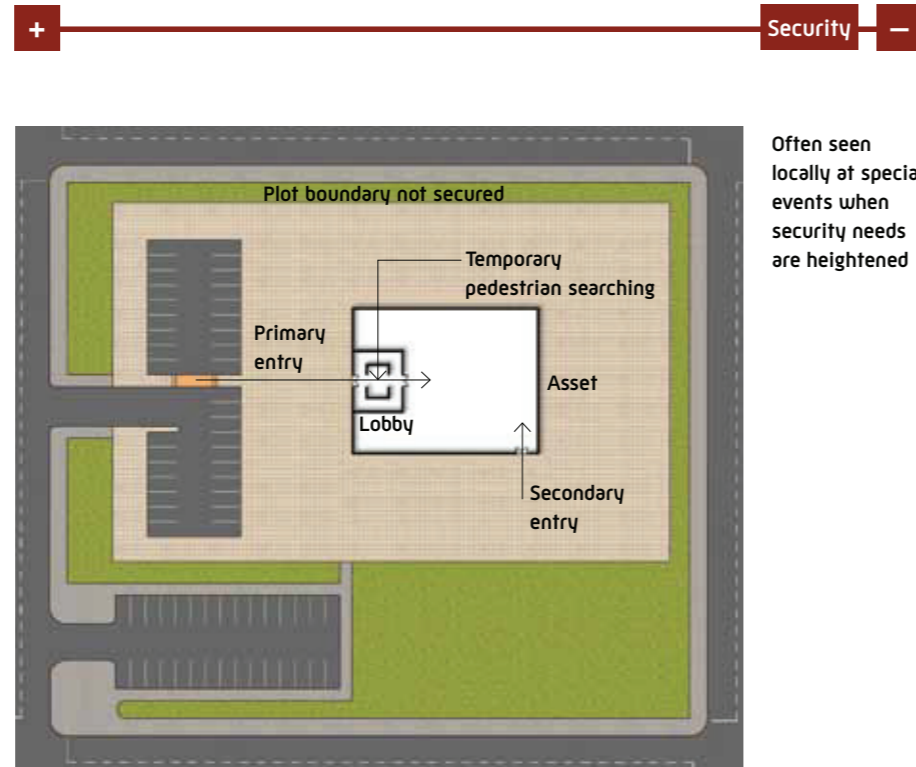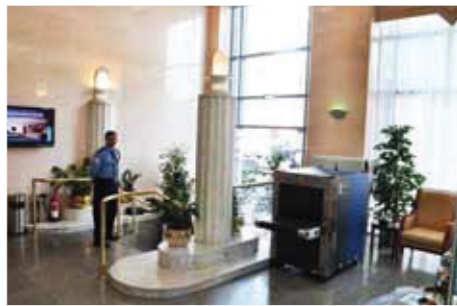Good practice often seen in US Federal buildings

Option 3:
Internal lobby pedestrian access control

Access is controlled at the main entrance. There is space allocated for search capability if required

Security

Plot boundary not secured

Internal lobby

Primary entry

Asset

Pedestrian searching

Secondary entry secured

Common in airports and Government buildings

Option 4:
Limited access control and temporary searching

Facilities for access control and screening are deployed on a temporary basis, typically in a main reception area

Security

Plot boundary not secured

Temporary pedestrian searching

Primary entry

Asset

Lobby

Secondary entry

Often seen locally at special events when security needs are heightened

Pedestrian Access Control Points

The number and amount of space to be allocated for access control points will be project-specific e.g. size of the plot, the anticipated numbers of legitimate users, the number and location of connections to surrounding transport infrastructure and the security checks required.

If a plot has a number of different user groups with different access rights and privileges, this will result in different access control regimes and may even change the number of entry points to allow for user group separation.

Where screening is required in addition to access control checks, there will be an increased spatial requirement at access control points due to longer processing times and additional security equipment.

Constrained Sites 'Urban Context'

In dense urban areas, it is rarely possible to have multiple layers of defence. This is often the case in downtown Abu Dhabi due to small plot sizes. This means that it is difficult to implement access control before people reach the building facade as they are in public space.

A combination of planning interventions may be adopted to improve access control without compromising connectivity:

1. Establish a well-defined movement framework and minimise the number of access points around the building.

2. Use topographic features, landscaping and urban design to celebrate 'main entrances', define transition from public to privately owned space and improve wayfinding.

3. Optimise sight lines surrounding the building to increase awareness of misuse and crime and to detect hostile reconnaissance.

This entrance is used for staff access only

A well defined movement framework helps channel people through designated access points

Checklist

- Is access control needed or will monitoring of access be sufficient?

- Is it appropriate to implement access control at the plot boundary or at the building?

- How many access control points are required and where will they be located?

- How much space is required for access control points?

- Can vehicle and pedestrian access control points be integrated?

PT5 | Service Access Control

Introduction

Service access, loading bays and mailrooms are required for receipt and dispatch of goods and mail, including replenishment of on-site consumables. These areas are typically kept out of sight in 'back of house' areas for aesthetic reasons. Service areas are often targeted by criminals due to the value of goods they contain. Also, because there is a need to allow large service vehicles to access these areas, they may introduce vulnerability to vehicle borne attack. Given that these areas are the location where unsecure deliveries are received, they are also the location where an Improvised Explosive Device (IED) or Chemical, Biological or Radiological (CBR) agent is most likely to be discovered.

The guidance contained in this section of the Planning Toolkit should be used to reduce vulnerabilities associated with service access. It highlights the importance of planning for service access and deliveries to prevent mail and deliveries entering a building unchecked.

A series of planning options ranging from high security to low security are outlined below. The project-specific risk assessment will help developers and owners to determine which option is most appropriate for their project.

Plan for Service Access

Project planners should assess how a project will be serviced and allocate appropriate space in the development plan for service access and facilities. This will ensure there is a location and adequate space for secure storage of valuable goods / mail and will allow a service access control strategy to be developed.

The amount of space required will not only depend on the anticipated volume of incoming and outgoing goods, but whether there is a need to screen deliveries before allowing internal dispatch.

Service Access Control – Planning Options

Five planning options are presented for service access control. They range from an aspirational high security plan where deliveries are received and processed off-site, to the lowest level of security where there is no provision of space for security.
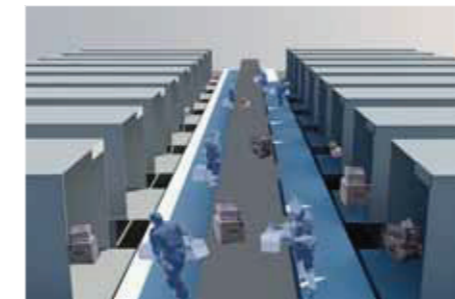
It is important to remember that even if a project is assessed as being low risk at present, changes in threat, the occupiers of the development or special events may warrant additional protection in the future. It is often difficult to allocate additional space post construction and therefore planners should be considering adaptability.

Whichever option is adopted, there is a need to integrate the service access control strategy with the vehicle access control strategy and the pedestrian access control strategy.
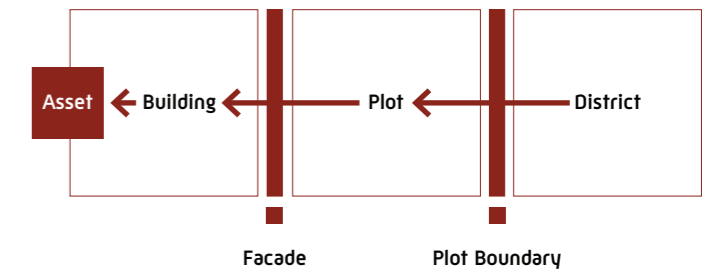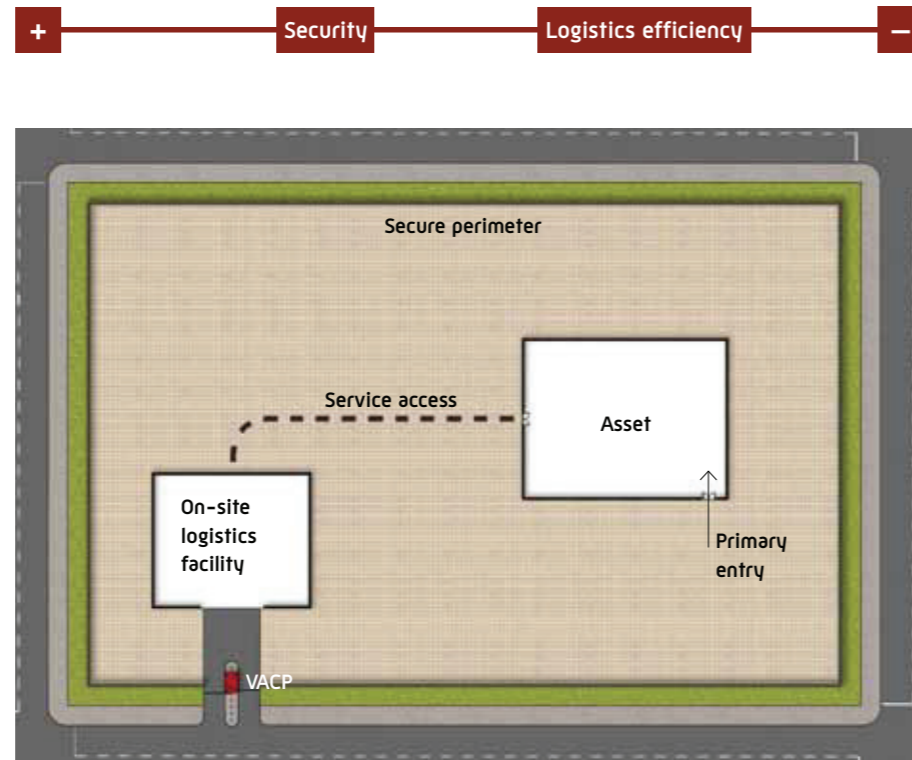
Option 1: Remote secure logistics system

Off-site facilities with a secure logistics chain for maximum security

Asset ← Building | Plot ← District

Facade | Plot Boundary

+ Security — Logistics efficiency —

Remote logistics facilities | Secure perimeter | Service entry | Asset | VACP | Parking | Secondary entry secured
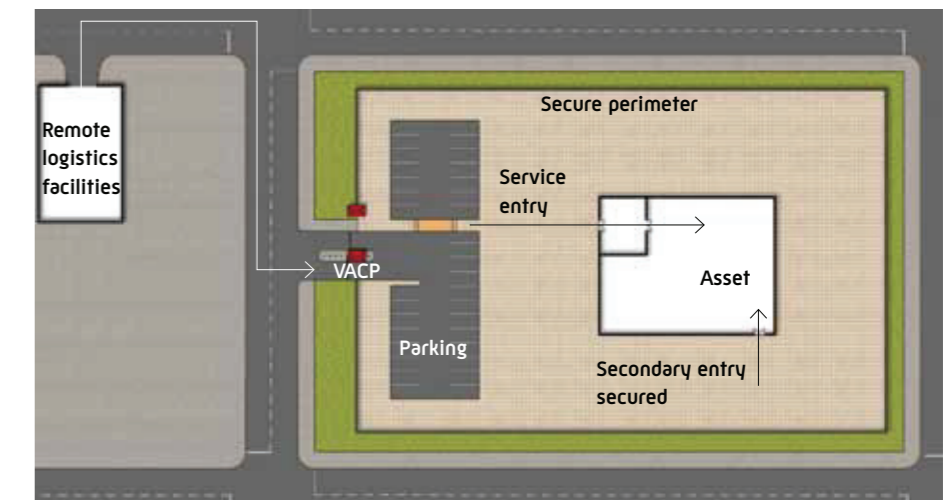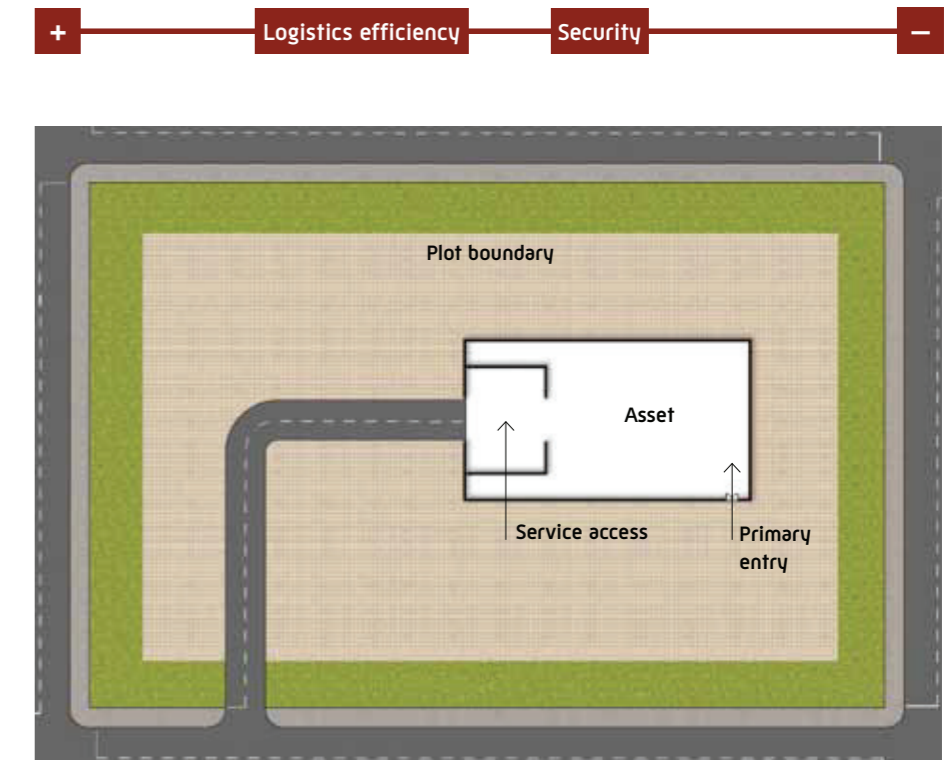
Option 2:
Dedicated on-site delivery reception area

Allows delivery vehicles onto the plot but screening of goods before entry into the main building

Secure perimeter

Service access

Asset

On-site logistics facility

Primary entry

VACP

Option 3:
Dedicated building delivery reception area

Secure facility enables secure storage of goods and a screening regime to prevent entry of suspicious packages

Plot boundary

Asset

Service access

Primary entry

Option 4:
Standard building delivery reception area

Space is allocated within the building for storage of goods, allowing a degree of protection. A suspicious package is likely to go unnoticed or, if opened, could cause contamination or damage

Plot boundary

Asset

Service access

Primary entry
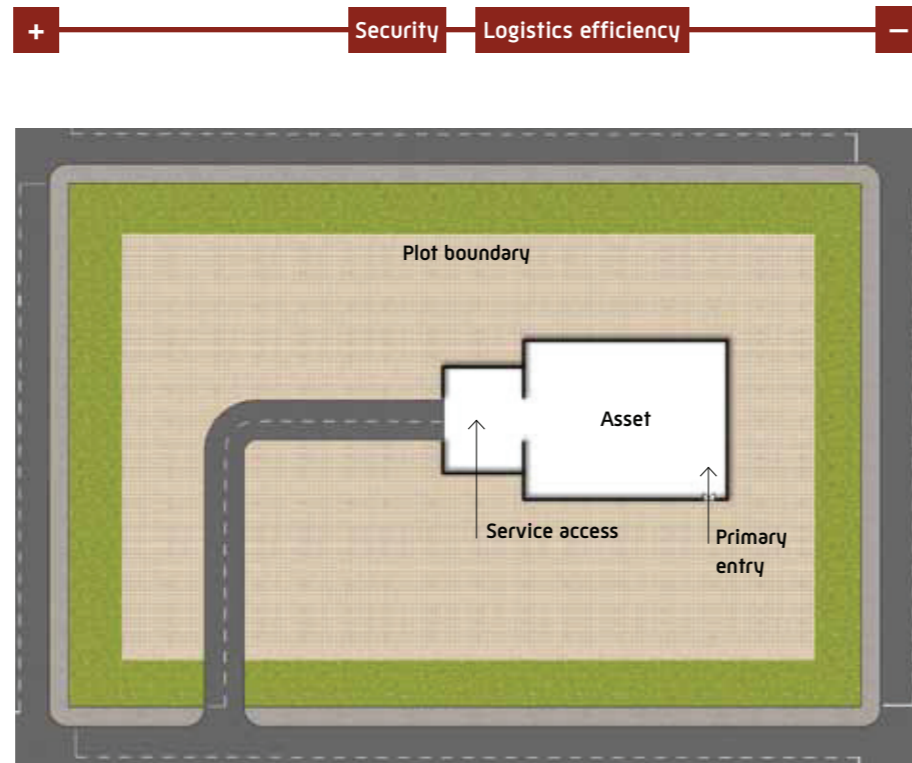
Option 5:
No delivery security regime

Building may potentially be vulnerable as items can be delivered directly into the building and cannot be held securely

Plot boundary

Asset

Primary entry
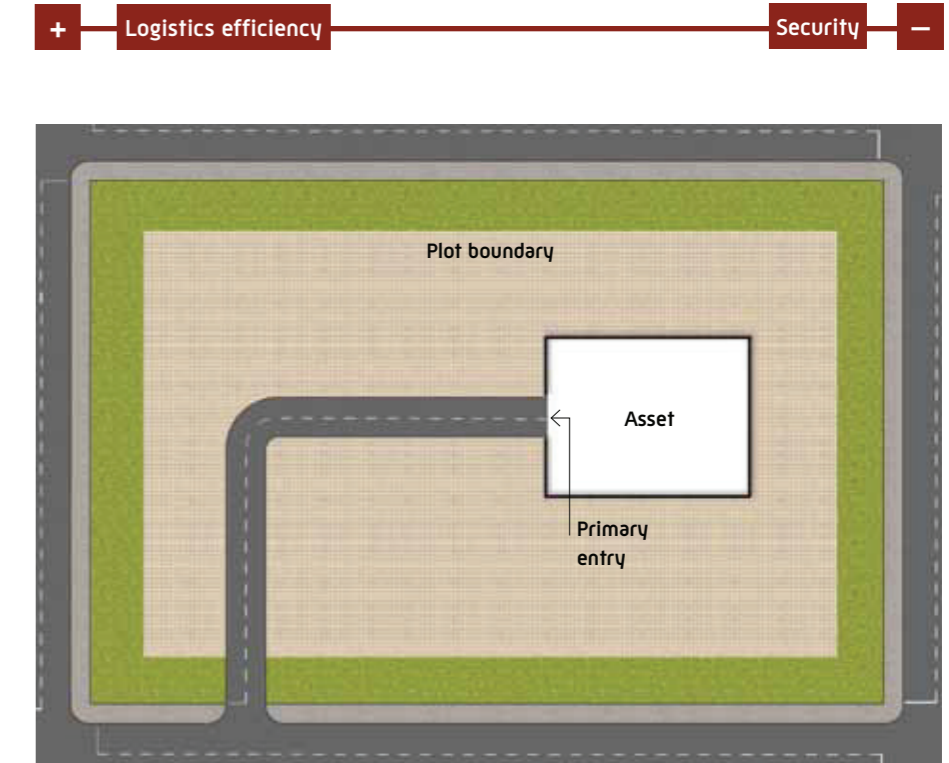
Innovation –
Service Access Control

The proposed Guggenheim Abu Dhabi and Louvre Abu Dhabi, planned for the Cultural District of Saadiyat Island, are to incorporate an underground shared remote logistics facility. This greatly increases security as all deliveries will be received and processed off-site before entering the museums. On-site service vehicles will be used to transport artwork, via secure connections, directly to art storage areas and galleries for public viewing.

Shared logistics centre, Cultural District, Saadiyat Island, Abu Dhabi
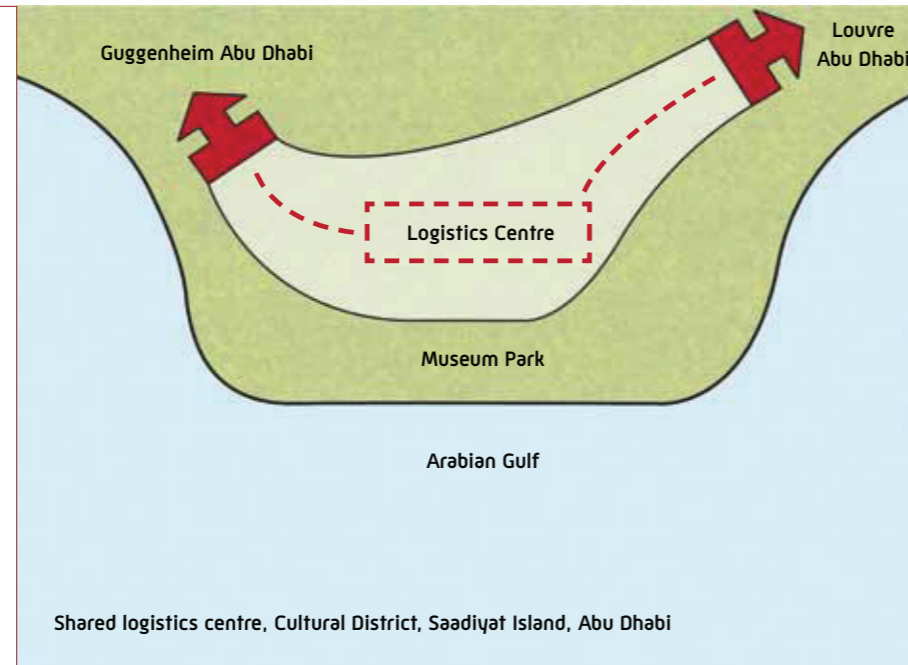
Checklist

- Has appropriate space been allocated for service access and deliveries?

- Which planning option is most appropriate given the results of the risk assessment?

- Can facilities be shared or located off-site as part of a secure logistics chain?

Typical service areas and processing operations

Parking Placement

Introduction

An important consideration in site planning is the allocation of adequate and appropriate space for vehicle parking. There are many competing objectives which influence whether to adopt on or off street surface parking, a dedicated parking structure or parking within a building. Underground parking within buildings is common in Abu Dhabi, particularly in dense urban areas where plot sizes are limited and demand for parking spaces is high. The use of basements is often seen as the most economic option and there may be other benefits of this approach, such as the removal of cars from the public realm.

The guidance contained in this section of the Planning Toolkit, will assist a project team in determining which approach is most appropriate given the safety and security risks identified for their project.

Safety and Security Risks

In many countries, car parks can become crime 'hotspots'. Often poorly designed, dark, inactive and lacking in natural surveillance, criminals target people and vehicles in these vulnerable areas. Crime rates for assault, theft of vehicles and theft from vehicles are often high along with users fear of crime. In addition, terrorists have used underground car parks as a means to attack target buildings. For example, in February 1993, terrorists detonated a large truck bomb in the car park below the North Tower of the World Trade Center in New York City, USA, resulting in six fatalities and over 1,000 casualties.

Fortunately crime in Abu Dhabi is low and terrorist attacks have not occurred. However, it is still necessary for the project team to assess the risks and ensure that car parks are appropriately located and well-designed to minimise such risks.

| Asset | Building | Plot | District |

Facade   Plot Boundary

Balancing Act

Much can be done to reduce car crime through the use of Situational Crime Prevention measures, such as designing cars to make them less vulnerable e.g. the fitting of steering locks, secure door locks and car alarms. The public should also be encouraged to remove attractive items from sight where possible. However such as, planners and designers also play a role in reducing car crime through the placement and design of car parks.

There is no 'one size fits all' solution to parking placement when it comes to safety and security. Firstly, every project is different and will need to balance any safety and security requirements with other planning objectives. Secondly, solutions that may address low level crime concerns may not be the most appropriate for buildings at risk from hostile vehicle attack. Different security solutions are required to mitigate different security risks and in some cases, mitigation advice can be contradictory. The risk assessment should help to determine which solution is most appropriate.

Parking within the plot for
CRIME PREVENTION

Parking away from the plot for
COUNTER – TERRORISM

World Trade Center Bombing, February 1993, New York City, USA
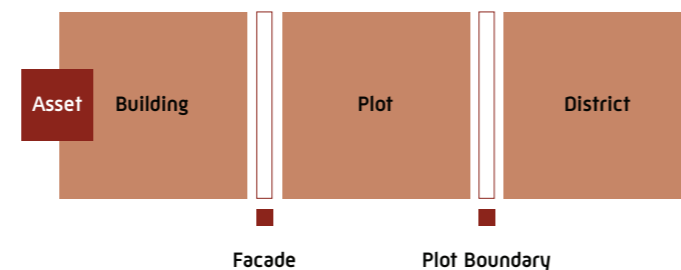

UAE | Crime

Car theft haunts Abu Dhabi residents

21 vehicles were broken into and their valuables stolen in the capital's Khalifa City

By Iman Sherif, Staff Reporter
Published: 00:00 September 7, 2011

GULF NEWS

Reader comments (15)

Local media reports on car crime in September 2011

Parking Placement Options

Planners have several options available to them when placing car parking. Each option offers advantages and disadvantages from a community safety and counter terrorism perspective.

Approach	Less favourable ← Crime Prevention → Favourable	Advantage	Disadvantage	Favourable ← Counter Terrorism → Less favourable
Surface – On street		Maximum stand off distance can be achieved Activity in public realm and surrounding buildings affords natural surveillance Premises owners do not take responsibility for the vehicles left unattended	Long distance to walk from vehicles to buildings. This may not be practical for certain uses or comfortable due to the hot climate	
Surface – Off street		Users have reduced distance between their car and their destination Users' vehicles can be parked within access controlled private spaces Natural surveillance can be achieved from surrounding uses	Vehicle inclusion to the site means reduced stand-off against vehicle borne attack A degree of access control, traffic management and enforcement will be required on site More difficult to detect illegitimate users as there is less open space	
Dedicated Structure		The walk from the vehicle to the users' destination can be within access controlled space Users vehicles can be parked within access controlled space	A degree of access control, traffic management and enforcement will be required on site Natural surveillance from surrounding uses may be difficult to implement. This may increase reliance on CCTV	
Within a Building (Basement parking)		Users' vehicles can be parked within controlled private space The walk from the vehicle to the users destination can be within access controlled space. This might be particularly important for VIPs	Increased requirements for access control are likely, along with traffic management and enforcement Natural surveillance is not available from other uses. This may require active surveillance solutions to be introduced If vehicle borne attack is likely, spatial layouts may be constrained, especially the placement of crowded places and critical functions. If vehicle borne attack is likely, then significant design changes may be required	

Innovation

If underground parking is necessary in order to meet other planning objectives, other treatment options exist to reduce the risks associated with terrorism:

1. Spatial Planning
Consider off-setting the underground parking so that parking is not located directly below critical structural elements, functions or crowded places.
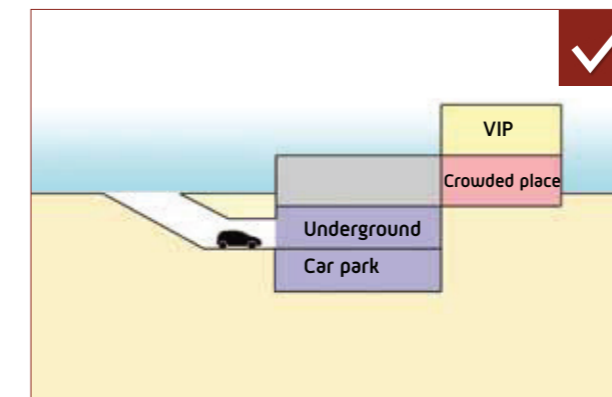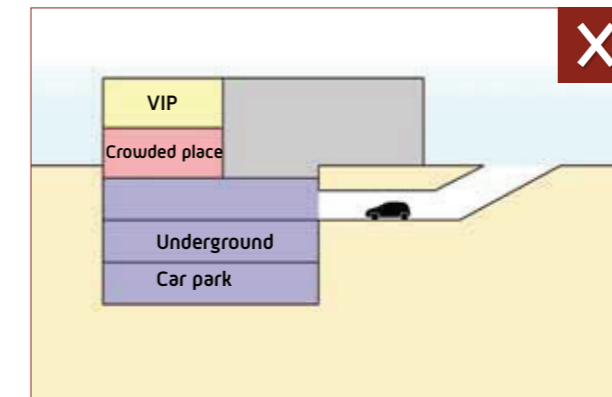
2. Hardening
Within the car park, the stand-off distance from vehicles to critical structural elements should be maximised. This can be achieved through the placement of non-essential plant or other building functions immediately surrounding columns.

Other innovative solutions include the design of column shrouds. These may only provide a small degree of stand-off distance but may be sufficient to prevent collapse. Ultimately, the structure can be designed to withstand blast loading, as discussed in Chapter 5.

3. Access Control
A more operationally focused solution is to incorporate screening and an access control regime. Screening should be applied prior to entering the basement car park. However this may be difficult to achieve in buildings with large peak flow rates, such as shopping malls. This approach also requires additional space. Access control offering higher levels of trust to certain user groups is a viable consideration, but it must be remembered that operations are prone to human error and are reactive rather than preventative.

If parking is required within a building, try to place critical functions and crowded places away from the parking entrances and exits

Checklist

- Is the type and placement of parking influenced by safety and security requirements?

- Is parking planned to take account of counter- terrorism or general crime prevention needs?

- If terrorism is a concern, can parking be accommodated outside of the building?

- If underground parking is necessary, has it been offset from critical areas?

- If underground parking is necessary, has vehicle access control and screening been considered?

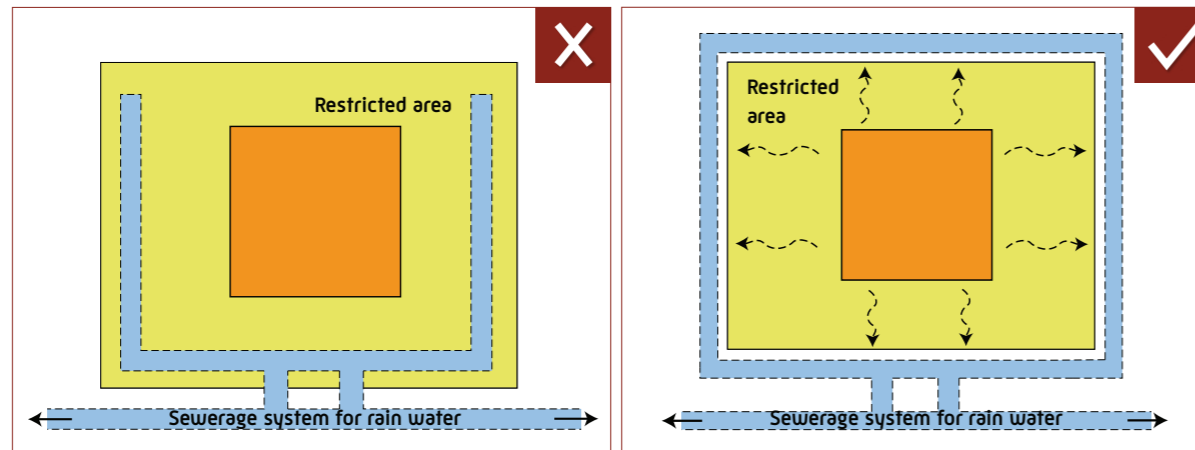# PT7 Infrastructure Planning

Introduction

This section of the Planning Toolkit presents infrastructure planning guidance that will increase resilience, reduce the likelihood of access control circumvention and the misuse of infrastructure as a means to attack a building. Utilities and infrastructure design guidance can be found in the Design Toolkit (Chapter 5).

Although the focus of the guidance contained here is not business continuity, if the guidance is followed, it will increase resilience and in doing so, improve business continuity as part of a comprehensive business continuity plan.

Access Control Circumvention

Infrastructure routes can be used as a means of circumventing access control measures. Reducing the number and size of large aperture openings at transitions between zones with different levels of access control is the most basic means of reducing opportunities for circumvention.

The infrastructure plan on the right avoids routing the rainwater collection within restricted space. This removes all openings from the restricted space
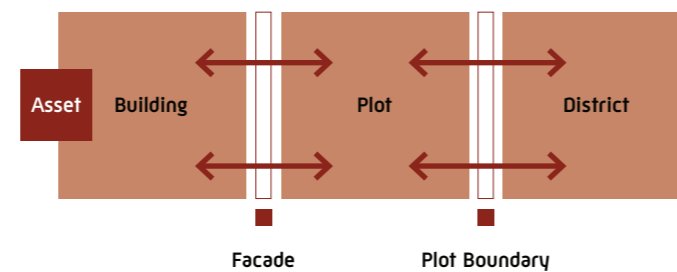
Supply Resilience – Connection Placement

Locating utility connection points within an access controlled area reduces opportunities for tampering or malicious damage. Such placement of connections allows access to be controlled and monitored. In some cases, access may be required for utility providers 24 hours a day. Therefore, it is important to consult with these providers during the planning stage.
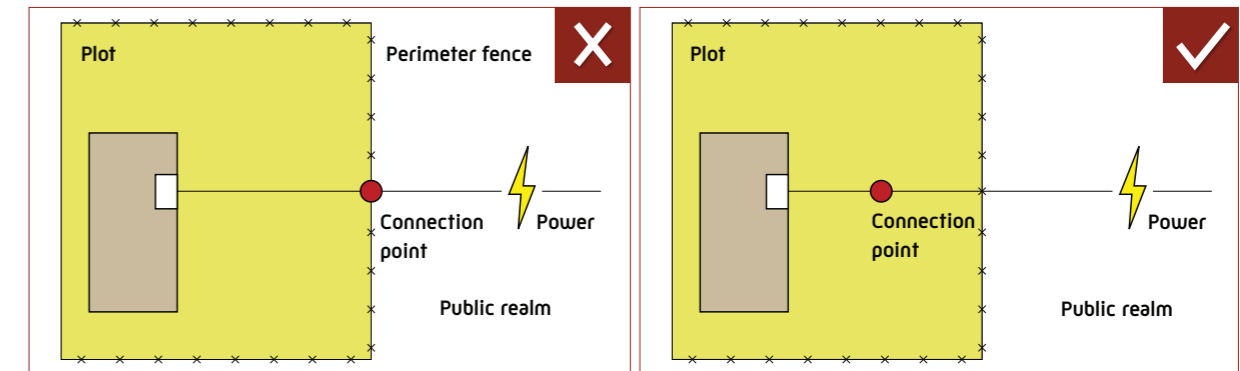
The infrastructure plan on the right places the above ground electrical connection and substation within the plot boundary

Supply Resilience – Infrastructure Routing

Routing utilities and infrastructure remotely from access control points reduces the likelihood of consequential damage in the event of a hostile attack.
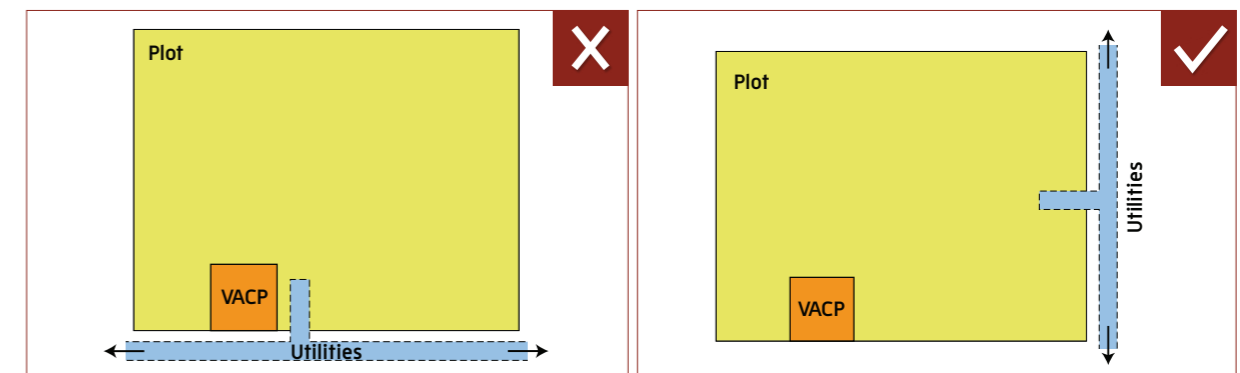
The infrastructure plan on the right places the utility connection away from the Vehicle Access Control Point

Supply Resilience – Redundancy

Determine whether it is necessary to designate space for redundant infrastructure. There is often a requirement for emergency power supplies for fire safety but there may be a need in some projects for redundant communications, water supplies, cooling and ventilation systems. Avoid placing duty and standby systems in close proximity where they could be subject to simultaneous failure.
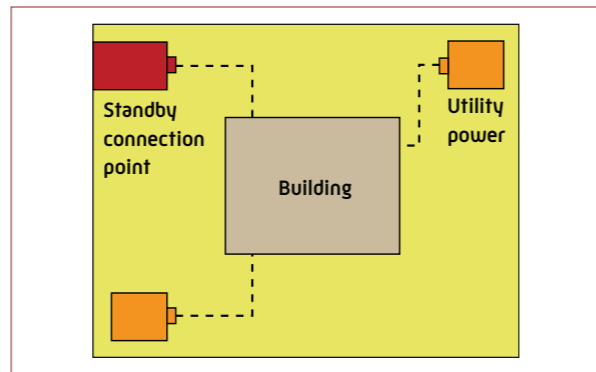
This building requires dual and standby power connections, to enhance resilience

Command and Control Infrastructure

Appropriate allowances should be made within plans for command and control infrastructure and operational support facilities. This includes, but not limited to, command and control rooms, storage facilities and rest facilities for on-duty personnel. Exact spatial requirements will be project-specific and determined in consultation with the project owner and stakeholders.
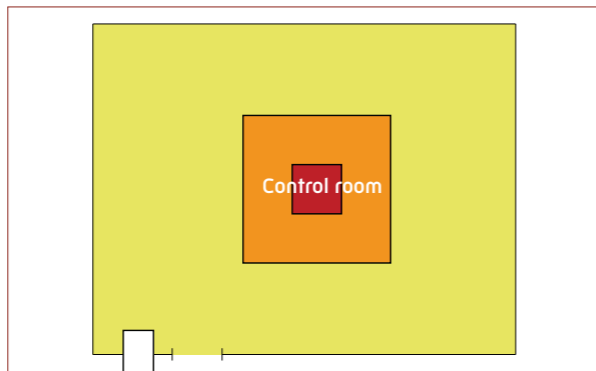
Space should be allocated within a building or master plan for command and control facilities

Infrastructure Hazards – Infrastructure Placement

Place hazardous installations within access controlled space to deter, delay, detect and deny unauthorised access as required.

Where plot constraints allow, crowded places, critical infrastructure and other assets should be placed remotely from hazardous infrastructure installations. This includes on-site infrastructure and off-site hazards such as pipelines.
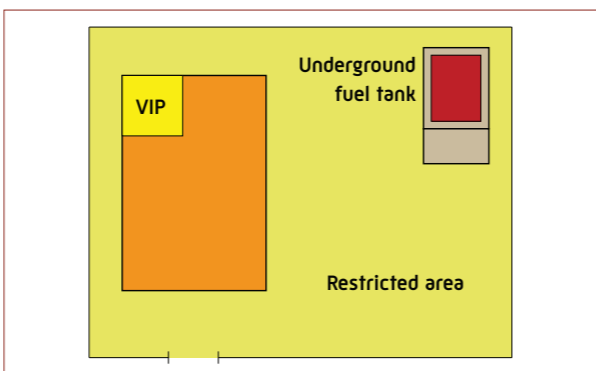
The fuel tank supplying this facility is underground, within the access controlled plot boundary and remote from the main building

Attack Vulnerabilities – Openings

Reduce the number of openings to infrastructure systems and place them remotely from publicly accessible areas. Where possible, place water tanks and ventilation openings on rooftops or within the access controlled perimeter of a plot where CBR agents cannot be introduced.
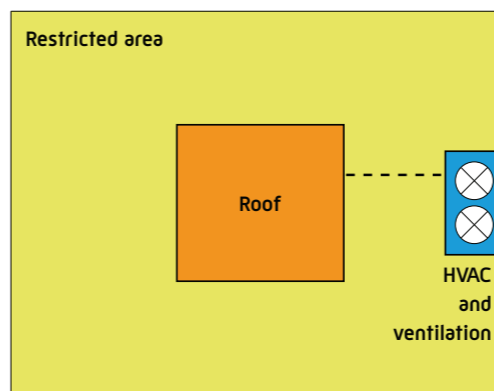
Inaccessible infrastructure opening

Access to roof mounted HVAC systems can be controlled and unauthorised access easily detected for efficient response
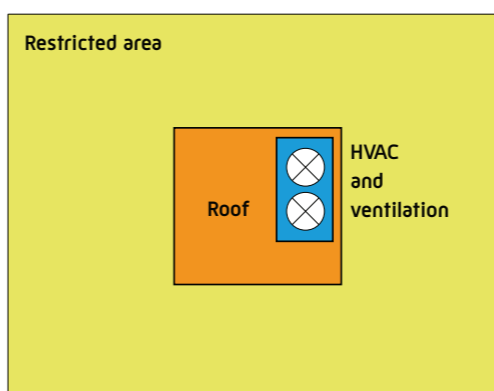
During the planning stage of this Government building, CBR attack risk was identified and HVAC openings were relocated to the building roof

Checklist

- Does the type, quantity and placement of infrastructure take account of safety and security risks?
- Will systems still function in an emergency?
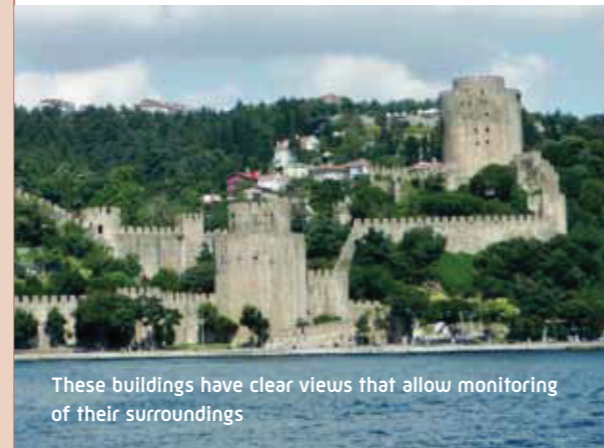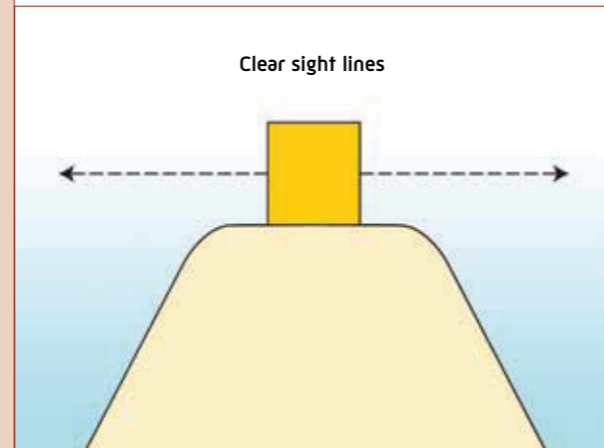
PT8 | Topography

Introduction

This section of the Planning Toolkit describes how topography and topographic features can be used to influence surveillance, define space, support access control and mitigate the impact of different types of malicious attack.

The topography of a plot describes its grade and natural and/or built topographic features, such as banks, hollows and bodies of water. These features will have a significant impact on development proposals, construction costs and 'buildability'. There will be trade-offs between safety and security objectives and those of other disciplines. For example, while a step change in grade may offer benefits in preventing vehicle borne attack, it might also reduce pedestrian accessibility. Planners must compromise to reach an appropriate solution, rather than dismissing one objective in order to meet another.

Later in design, it is normal practice for developers to employ landscape and urban designers to develop public and private realm spaces. This often involves the introduction of changes in grade, slopes and water features to add variety and texture to external spaces. The Design Toolkit (Chapter 5) provides design guidance for practitioners involved in projects where there is a need to mitigate safety and security risks.

Natural Surveillance

Natural surveillance, where clear sight lines are optimised to provide viewing opportunities, plays an important role in both community safety and protective security. This is particularly important where there are public realm spaces such as parks and surface parking surrounding a development.

Clear sight lines

These buildings have clear views that allow monitoring of their surroundings

Privacy

Topographic features can be used to hide a building from public view where privacy is required. Such features also shield sensitive use or users from view, reducing opportunities for hostile reconnaissance or a malicious attack.


Landscape

High-rise building

Sight lines obscured

High security building
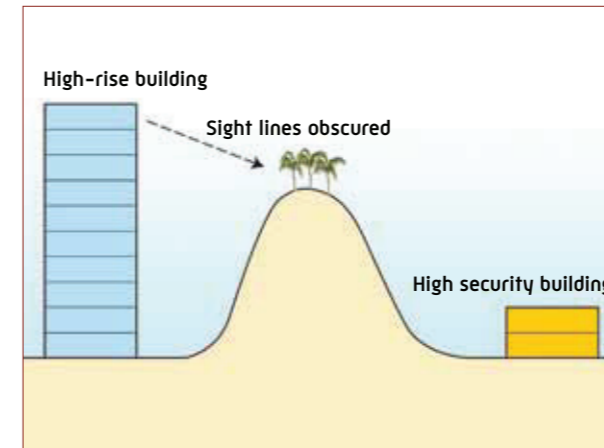
A ridge maintains privacy for this high security building, allowing a high-rise building on the neighbouring plot

Space Definition

A simple change in grade, a berm, ditch or water body can be used to define the transition between public and private space where access control is not required.

Water feature

Topographic features used to demarcate spaces and deter unauthorisead access

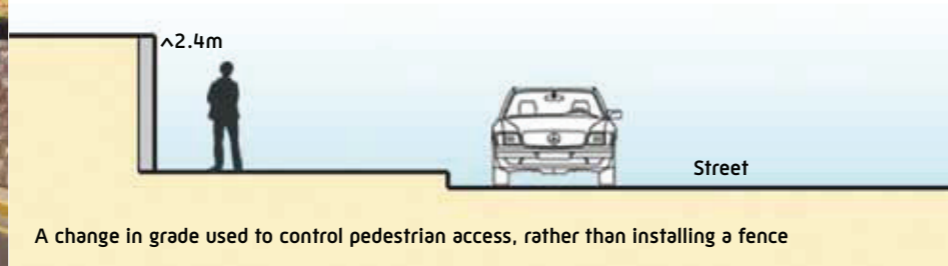Asset | Building | Plot | District

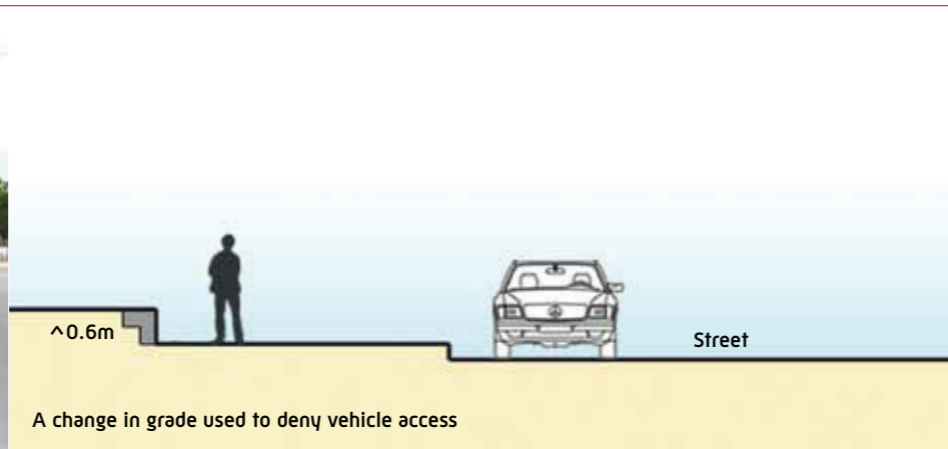Facade | Plot Boundary
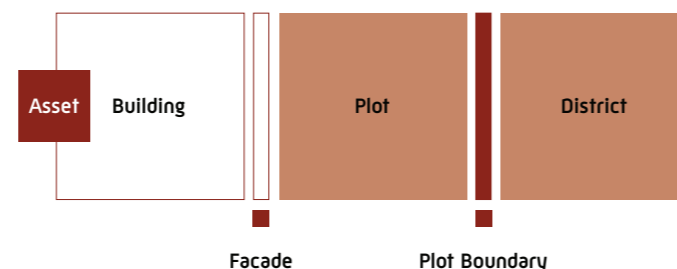
Access Control

Topographic features used for access control will be more pronounced than those used for space definition and they may be a significant feature on a plot. It might be necessary to supplement such features with security design elements to deny access.
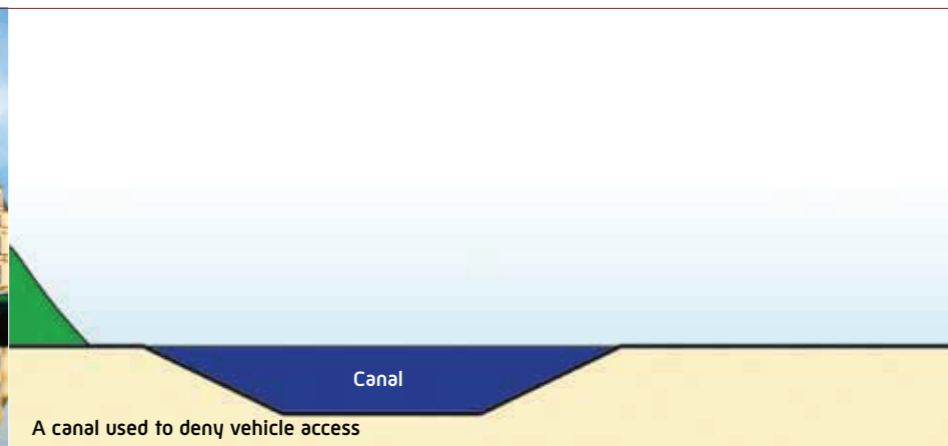

Intercontinental Hotel Abu Dhabi

^2.4m

Street

A change in grade used to control pedestrian access, rather than installing a fence

Abu Dhabi Investment Authority, Abu Dhabi

^0.6m

Street

A change in grade used to deny vehicle access
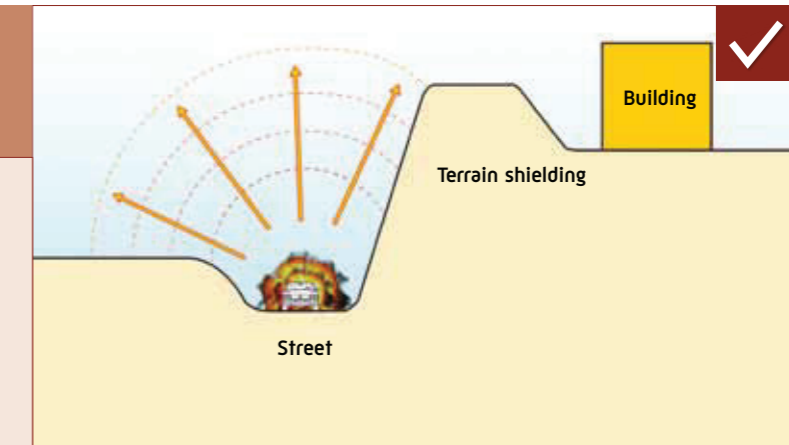

Chambord, France

Canal

A canal used to deny vehicle access

Blast Effects Mitigation

If a project risk assessment determines that a building is at risk of explosive attack, topography can be used to reduce the impact of an attack.

Building

Terrain shielding

Street

This Government building is shielded from blast effects and fragmentation

Chemical, Biological & Radiological (CBR) Attack Mitigation

Topography can be used to protect a building against CBR attack. The range of possible agents, their attributes and behaviour in different atmospheric conditions means that specialist advice is required to address this type of attack.

CBR agents

Building

CBR agents collect in the depression
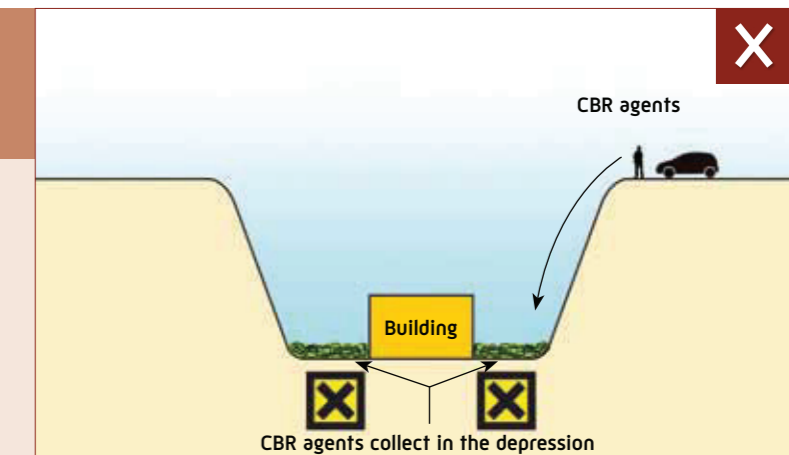
This Government building was located in a hollow for privacy reasons, this left it vulnerable to CBR attack involving heavier than air agents.

Checklist

- Have the existing topographical and landscape features of the plot been used in the safety and security plan?

- Have all opportunities to alter topography to increase safety and security in an unobtrusive way been exploited?

- Should sight lines be obstructed or unobstructed?

PT9 | Building Orientation and Shape

Introduction

Taking time during the planning stage to consider how building orientation and shape may reduce safety and security risks will often reduce vulnerabilities and the need for physical security.

The guidance outlined in this part of the Planning Toolkit can be used to influence surveillance, avoid the creation of spaces and features that can be used by criminals and reduce the impact of an attack involving explosives.

The climate of the Emirate means that building shape and orientation plays an important role in reducing solar heat gains, in channeling cool breezes and providing shade of the public realm. On each project it will be necessary to balance these competing planning objectives.

Clear line of sight

Recess creates an entrapment area out of sight

Original   Option 1   Option 2   Option 3
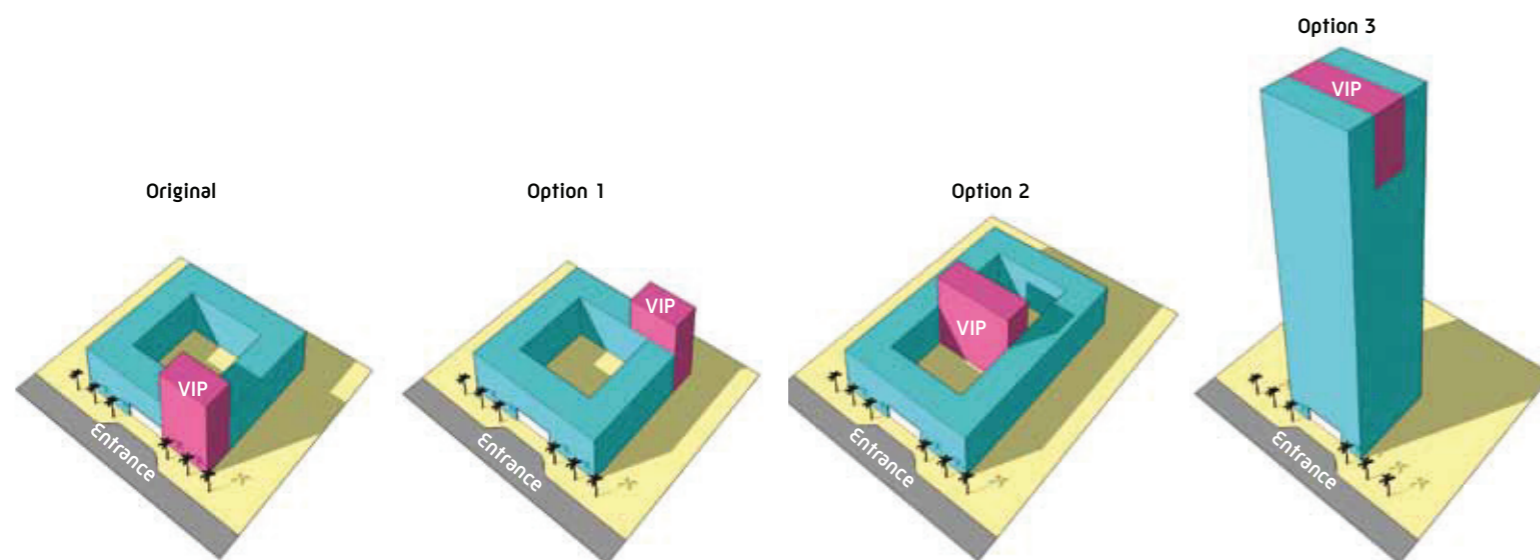
Changes of shape and building orientation, along with spatial planning, have been used to improve privacy and protection for the VIP area

Natural Surveillance

Natural surveillance, where clear sight lines are optimised to provide viewing opportunities, plays an important role in both community safety and protective security.

On projects where there are community safety concerns, building shape and orientation should be used to create a building that is seen to 'open up' to its surroundings, rather than turn its back. This will not only enhance surveillance but make a building more inviting to legitimate users.

The creation of active frontages and the use of glazed facades for regularly occupied spaces, provides 'eyes on the street'. This is particularly important where there are public realm spaces such as parks and surface parking surrounding a development.

Using building orientation and shape to optimise natural surveillance around a building perimeter is important for projects that need to address security risks, particularly on constrained sites where the facade is the first line of defence. Introducing clear sight lines will improve:

- Detection of suspicious activity such as hostile reconnaissance; and

- Effectiveness of active surveillance systems.

As highlighted in the Principles (Chapter 2), there is always a need to balance surveillance with the need for privacy. Building shape and orientation can be used to create a building that 'turns its back' on public space where there is a need for privacy, for example to shield sensitive use or users from view.


Asset   Building   Plot   District

Facade   Plot Boundary
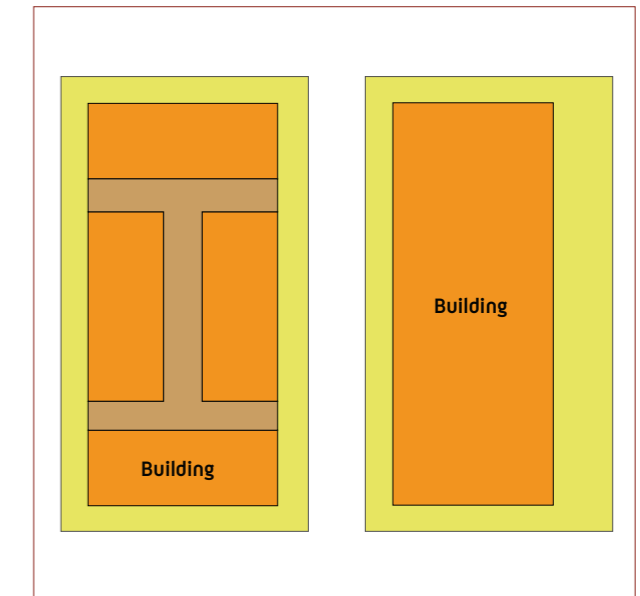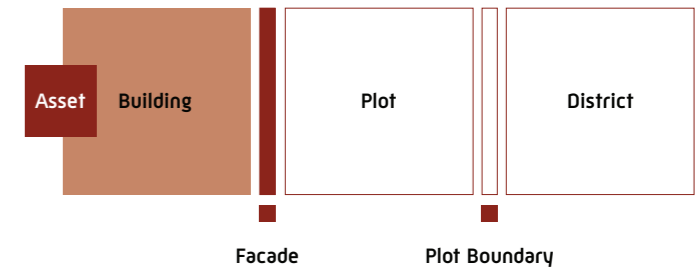
Buildings have been located very close together, limiting natural surveillance
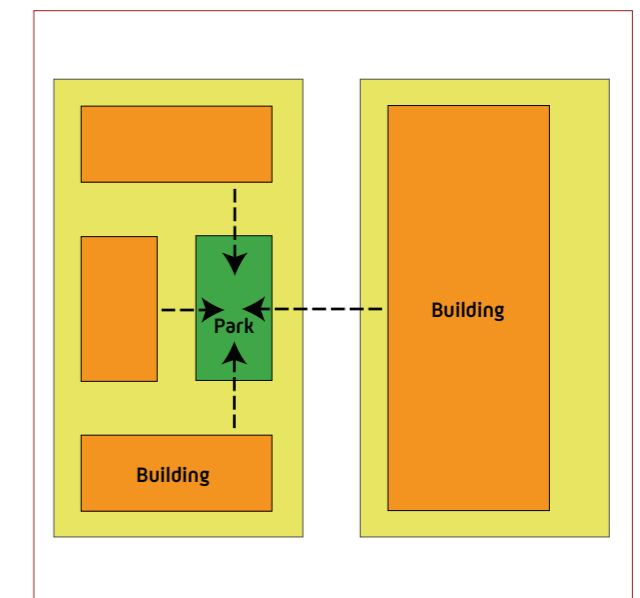

More open space improves surveillance

Blast Effects Mitigation

If a project risk assessment determines that a building is at risk of explosive attack, its shape can be used to reduce the impact of an attack by dissipating blast overpressures. Shapes that accentuate and dissipate air blast are presented below. Rarely will a building conform exactly to any one of these shapes and even where it does, specialist advice should be sought. A specialist can evaluate vehicle exclusion, stand-off and design treatments alongside building orientation and shape to reduce blast vulnerabilities.
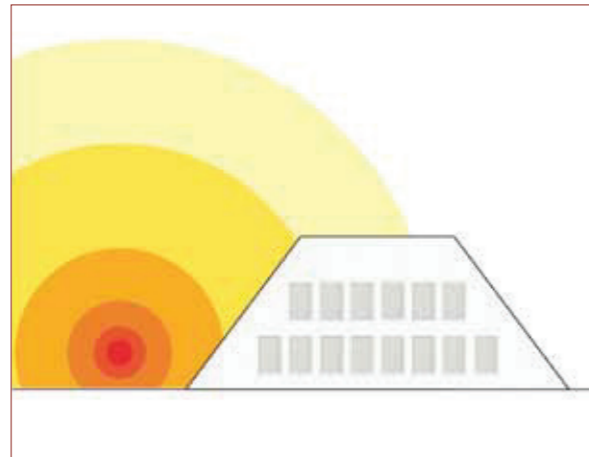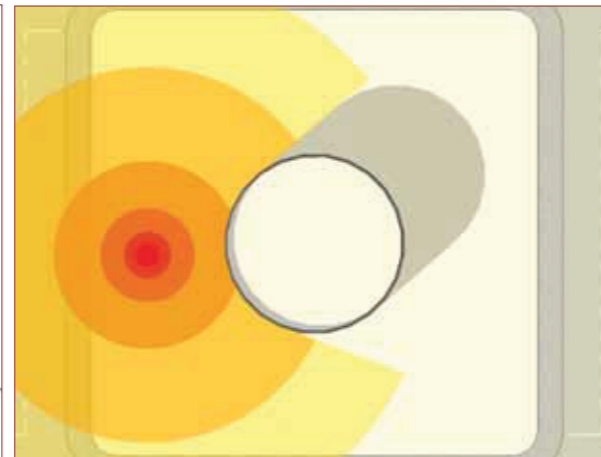

Shapes that dissipate blast
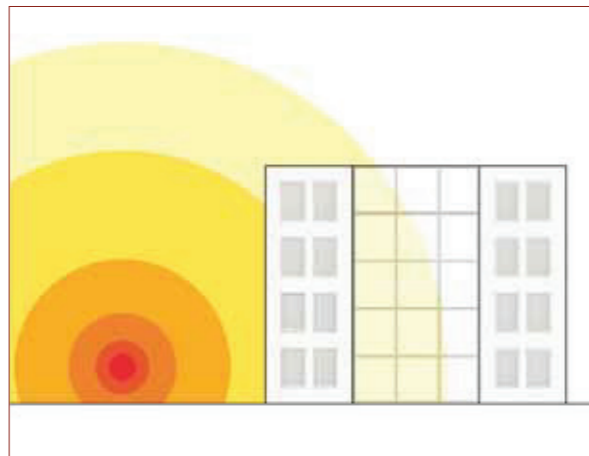
Shapes that accentuate blast

Innovation – Case Study

The shape of the US Embassy in Abu Dhabi has been heavily influenced by the need to protect it from terrorist explosive attack.

US Embassy, Abu Dhabi

Building Features

There are a number of features that can make buildings and users more vulnerable to crime. Examples are provided below and planners and architects should avoid these features that aid criminals and enable inappropriate behaviour.

Features that inadvertently aid intruders

These recesses provide hiding places and places for entrapment

Checklist

- Do building shapes and orientation support natural surveillance?
- Have buildings been orientated so that sensitive spaces are away from vulnerable or overlooked facades?
- Will the shape of buildings minimise the impact of a blast?
- Has the development been planned bearing in mind that criminals may use features in unintended ways?

PT10 | Development Delivery

Introduction

The pace and scale of development associated with Vision 2030 is considerable. This often means that project delivery is phased, with partial occupation of early phases to fund ongoing development.

This also means that projects are often incomplete for prolonged periods. Therefore, it is very important that development delivery is considered at the planning stage of a project to ensure community safety and protective security is implemented not only for the end state of a project, but during phased occupation.

This section of the Planning Toolkit provides guidance intended to ensure vulnerabilities are not introduced when formulating development delivery plans.

Phasing: Community Safety

The creation of complete communities should be promoted through appropriate development phasing. Phasing that clusters occupied plots rather than dispersing them will ensure that occupants of early phases do not spend the early years of the project living in a construction site.
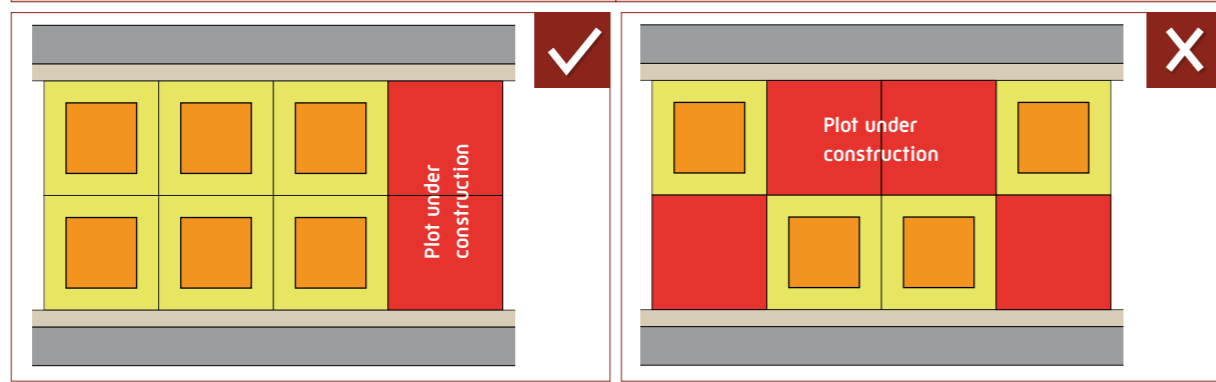
A fully developed community

Khalifa City A has many undeveloped plots

Construction: Community Safety

SSPM Principle 7 (Public Image) highlights that plot owners and developers are responsible for the management and maintenance of their plots. This is true even during construction and sites should be made safe and secure to stop misuse, theft of property and access to hazardous materials and areas.

The Municipality has powers under the Emirate of Abu Dhabi Environment, Health & Safety Management System (EHSMS) to monitor and enforce good practice.

Phasing: Physical Security Integrity

Although the Planning Submission for a project will primarily focus on the final build out of a project; the safety and security 'end state', development phasing should not undermine the Safety and Security Plan.

If physical security elements intended to protect occupied buildings are not in place as planned, as a result of being delivered in later development phases, occupants may be left vulnerable to security threats.

This is particularly relevant where security planners are looking to use innovative solutions such as natural barriers and topography to create continuous HVM barriers, and 'collective solutions' that provide a security zone to protect several plots or a district.


Construction can affect the security of neighbouring occupied buildings

Phasing:
Community Facilities

During the planning stage, master developers, in consultation with Government stakeholders, are tasked with allocating appropriate community facilities.

Included within this task is the need for the master plan to make provision for facilities for the emergency services e.g. Civil Defence, Police and Ambulance stations.

These decisions will be based on each safety and security agency's estates strategy and assumptions relating to emergency response targets. It is important that master developers have an understanding of their development phasing to ensure they do not leave early phases without sufficient emergency cover.
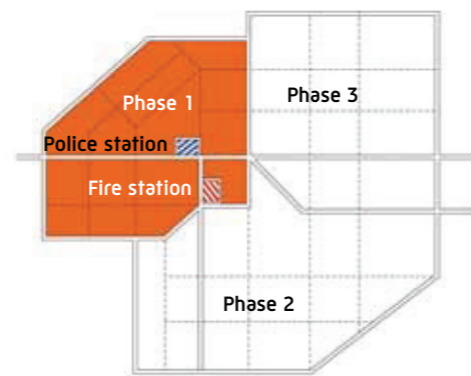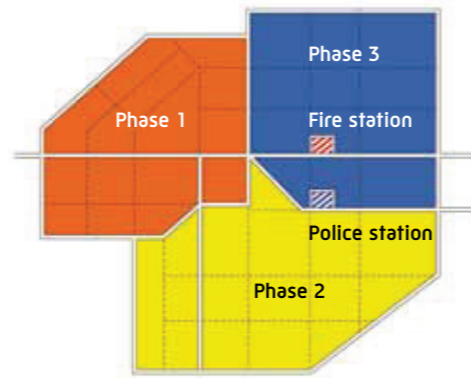
The impact of phasing on emergency cover

Phasing:
Safety & Security Infrastructure

Planning assumptions made in relation to utilities and infrastructure supply should remain valid after development delivery decisions are made. Safety and security systems, including firefighting water, emergency power supplies and communications may be required in early phases. Utilities and infrastructure phasing should be aligned to avoid unintended vulnerabilities.

Safety infrastructure

Checklist

- Does phasing promote community development?

- Are construction sites appropriately secured?

- Are physical security elements in place and complete prior to occupation?

- Are community facilities delivered in the correct phases of development?

- Is infrastructure delivery aligned with development phasing?

5

Design Toolkit

Introduction

Chapter 5 presents a series of design tools that may be used to implement Community Safety and Protective Security in a development project. The guidance contained here will assist developers and owners to implement the Abu Dhabi Safety and Security Planning and Design Principles presented in Chapter 2.

The Design Toolkit builds on the solid foundation established by the Planning Toolkit (Chapter 4) and includes international best practice, innovative design ideas and draws on existing good practice from around the Emirate of Abu Dhabi.

Decisions relating to which design tools need to be applied and to what extent they are applied are to be made as part of the Integrated Development Process (Chapter 3). The documentation submitted as part of the Building Permit Submission for High Priority Projects should demonstrate an integrated design solution and highlight which design tools have been adopted.

Existing Buildings

Use of the Design Toolkit is not restricted to new development projects. Owners of existing buildings will find the Design Toolkit useful for assessing options for retrofitting safety and security measures.

The built environment can be viewed as a series of spatial layers. It is important to be familiar with these layers as they are used throughout the Design Toolkit to highlight where the guidance in each tool can be applied.

The plot boundary is usually the limit for implementing access control and physical security for a project, that is unless agreement is reached to share security measures with neighbouring plots or to place security measures outside the privately owned plot boundary.

Asset	Building	Plot	District

Facade   Plot Boundary
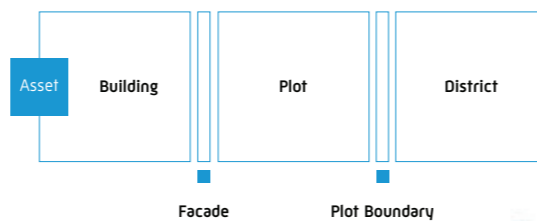
Navigating the Design Toolkit

For ease of use, the Design Toolkit is presented in three sections, each highlighting how members of the project team who are working on different design aspects can contribute to safety and security.

DT1: Landscape & Urban Design

This section deals with exterior design elements at the plot level, plot boundary and within the surrounding district.

DT2: Architectural Design

This section outlines the role of architectural design in asset protection and reducing safety and security vulnerabilities. It covers design decisions relating to interior space, structure and the envelope of the building (facade).

DT3: Systems Design

This section provides design guidance for infrastructure protection and the deployment of safety and security systems.

Appropriate design for safety and security relies on an analysis of the local situation and must take into account competing design objectives.

DT 1 Landscape and Urban Design

Landscape architects and urban designers create and implement a vision for outdoor spaces. They connect buildings with the wider built environment, they facilitate access and connectivity and importantly it is their design that implements the Safety and Security Principles in these spaces.

Specialist Advice

The lead design disciplines should seek specialist advice where elements are used to address specific safety and security risks, such as hostile vehicle attack. These specialists can ensure physical security elements are cost effective and fit-for-purpose. Where practical, any elements used for safety and security should serve a dual purpose.

In Abu Dhabi, it is common for plot boundaries to feature high walls. This is often primarily for reasons of privacy, rather than to deter, delay or deny unauthorised access

Abu Dhabi Public Realm Design Manual

The Abu Dhabi Public Realm Design Manual is part of the UPC's development regulations and is to be used in all public realm designs across the Emirate of Abu Dhabi. The guidance provided in this Manual will assist designers and safety and security specialists in selecting appropriate design solutions.

Abu Dhabi Public Realm Design Manual

This section includes five design tools

DT 1.1: Boundary Treatment
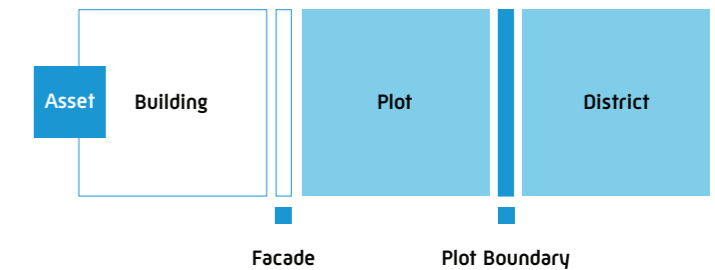
DT 1.2: Hostile Vehicle Mitigation

DT 1.3: Vehicle Access Control Points

DT 1.4: Pedestrian Access Control Points

DT 1.5: Materials Selection and Planting

Asset | Building | Plot | District

Facade | Plot Boundary

To date, few places in Abu Dhabi benefit from Hostile Vehicle Mitigation. It is anticipated that its use to **deny** vehicle borne attack will become more common-place, particularly in crowded places and Government buildings, so there is a need for integrated design solutions

DT 1.1: Boundary Treatment

A boundary treatment is often the most visible element of any security plan. Urban designers will be looking to maximise permeability, while security specialists will be looking to reduce permeability, minimise the number of entrances and determine the level of access control

required. This challenge frequently requires resolution at the plot boundary. Therefore the design team is required to provide the desired level of protection without turning the building or plot into a fortress. The aspiration for boundary treatment is for subtle and aesthetically pleasing security measures to be used, particularly in the urban environment, with the use of specifically designed security products limited to those developments that have been identified as having higher security requirements.

Security Strategy

A security specialist will look to create and embed the concept of 'defence in depth' into a holistic security plan. The plot boundary is normally the outermost layer of defence in higher risk developments. Using the plot boundary maximises the distance between the first layer of security and the building or asset to be protected. This may be difficult to achieve in the urban environment; which may inform other design elements, such as the strength of the facade and its openings.

A secure perimeter is used to create a 'controlled zone'. It defines the physical boundaries of a space and helps to restrict, channel or impede access. The degree of access control will vary considerably from project to project; it may be achieved through territorial reinforcement, by operational or electronic means, or through the deployment of a physical barrier.

Some plots are designed so that their security is obvious and imposing, others employ a more subtle approach that blends in better with the urban environment.

Ultimately, boundary treatments provide definition and deterrence, and offer differing levels of delay and denial. The choice of boundary treatment should be based on the risk assessment and which of these characteristics are required. For low risk sites, low levels of deterrence are sufficient. As risk levels increase, boundaries will need to incorporate increasing levels of delay while for some, denial may be a requirement.

The role of a secure boundary is to:

- Define legal property boundaries;
- Control plot access;
- Provide maximum distance between potential threats and assets to be protected; and
- Provide opportunities to assess and respond to intrusion.

A bright, colourful and effective boundary treatment defines the play area, keeps children safe and maintains natural surveillance

Planting along the pedestrian walkway maintains sight lines while demarcating and deterring unauthorised access to the private family beach

Natural Boundary Treatments

Boundary treatments can be natural or man-made. Natural barriers, such as wadi's and steep terrain can be used, especially where they are difficult to traverse. Topographical changes, which are required in many projects for site shaping, drainage and roadways, also present opportunities to unobtrusively enhance security and define the plot boundary. Berms, steep slopes, ridges, decorative landscape elements and vegetation can all serve to reinforce territorial ownership and act as barriers. Sharp leaved and thorny plants and dense hedges can also create natural barriers. They integrate well into the landscape design and are relatively inexpensive but irrigation needs to be considered.

Man Made Boundary Treatments

Man-made boundaries such as walls and fences are common means of establishing a secure boundary. Fences can provide high levels of security, and can be constructed in a range of materials and styles to suit the project security requirements. They should be used only in high security environments where individual intruders, rather than vehicles are a threat. Walls offer a greater opportunity for compatibility with the architectural context; they may also provide higher levels of privacy and if designed appropriately, enhanced protection against ballistics and blast.
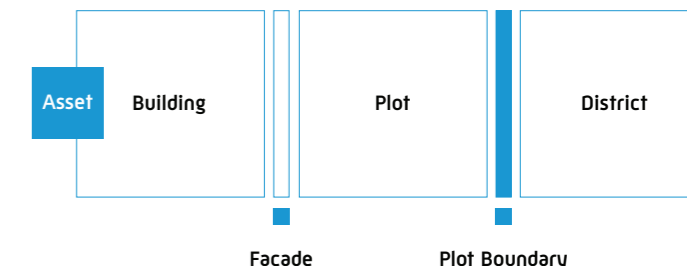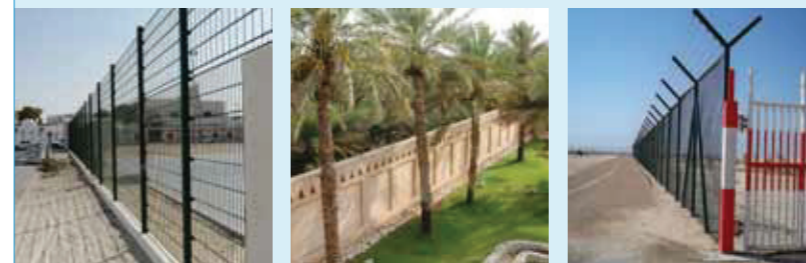
Design Factors

Design must start with an evaluation of the project context including:

- Adjacent properties and neighbours;
- Existing building codes and design guidelines;
- Surrounding street network, entry points and parking requirements;
- Extent of vehicle and pedestrian access;
- Level of protection required;
- Aesthetics;
- Cost;
- Topography and vegetation;
- Sight lines and visibility;
- Material selection and construction techniques;
- Finish and durability;
- Height, length and alignment; and
- Infrastructure e.g. power, alarms, lighting and CCTV.

Low risk environment

Medium risk environment

High risk environment

Vehicle Denial Perimeters

Boundary treatments may also need to incorporate specific measures to deny vehicle access – see HVM (Design Toolkit).
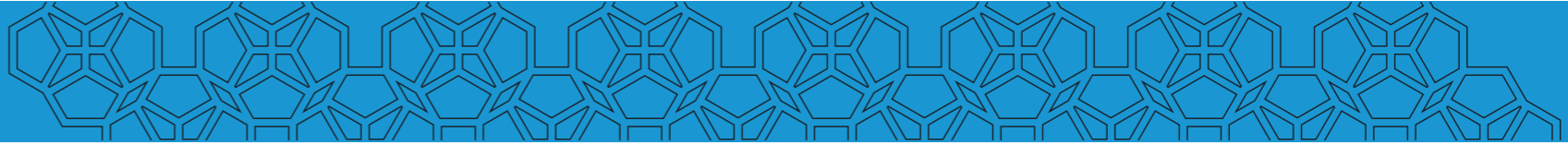
Security Systems

In high security environments, sensors can be applied to a boundary treatment to detect unauthorised entry. If someone attempts to cross the terrain, or attempts to climb, cut through, or dig under the treatment, an alarm is triggered. With a fully integrated system, this can automatically trigger monitoring and recording by a CCTV system.

Design Factors

1. Dense planting close to a building can screen illicit behaviour and conceal items such as weapons and contraband. Vegetation must not block important sight lines or create attractive hiding places.

2. Plants, trees and shrubs can be used to 'soften' or screen security elements.

3. Walls may restrict surveillance into and out of a site.

4. A clear zone should exist between the boundary treatment and exterior structures or trees that may serve as climbing aids.

5. Barriers can be compromised through deliberate breaching (cutting through) or by natural elements (overhanging trees, sand movement, etc.) and therefore should be inspected and maintained regularly.

6. Painting fence fabric and structures can minimise visual impact. Different types and heights minimise their presence and prevent monotonous, negative visual perspectives.

7. If increased deterrence and delay is required, topping can be placed on a fence or wall.

8. Clear zones should be maintained on both sides of a high security barrier to provide an unobstructed view of the barrier and the ground adjacent to it.

9. For long boundaries, a road should be provided on the secure side of the boundary for security patrols.

Maritime Boundaries

Many of the developments in Abu Dhabi have waterfront boundaries. In most circumstances no form of security treatment will be required and projects have the design freedom to focus on safety, functionality and aesthetics.

However, where security risks have been identified, additional measures may need to be incorporated. This is a difficult challenge and requires a multi-disciplinary approach to ensure that access, safety and the maritime environment is not compromised.
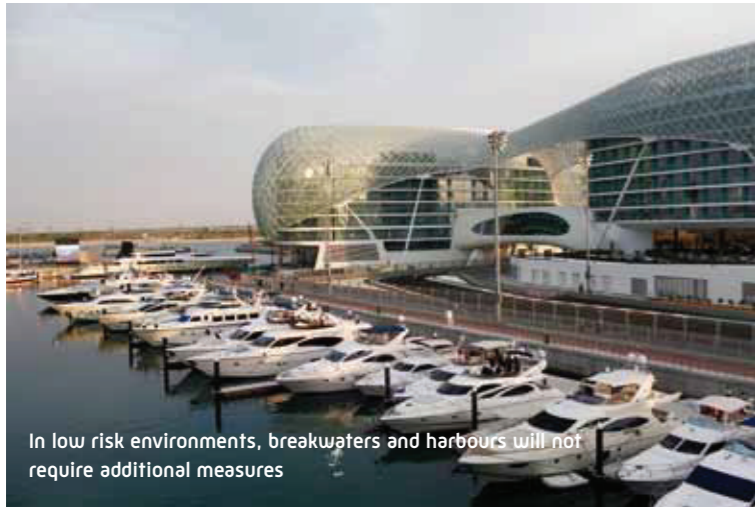
In low risk environments, breakwaters and harbours will not require additional measures
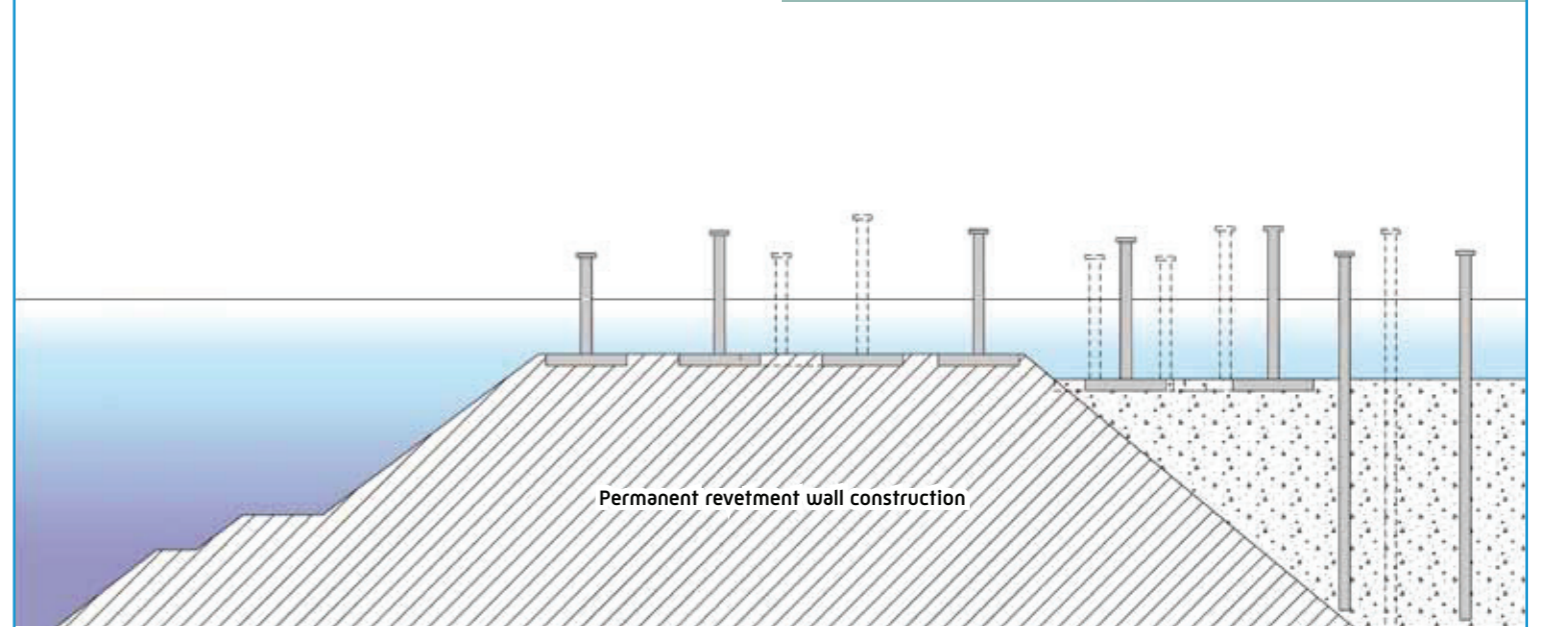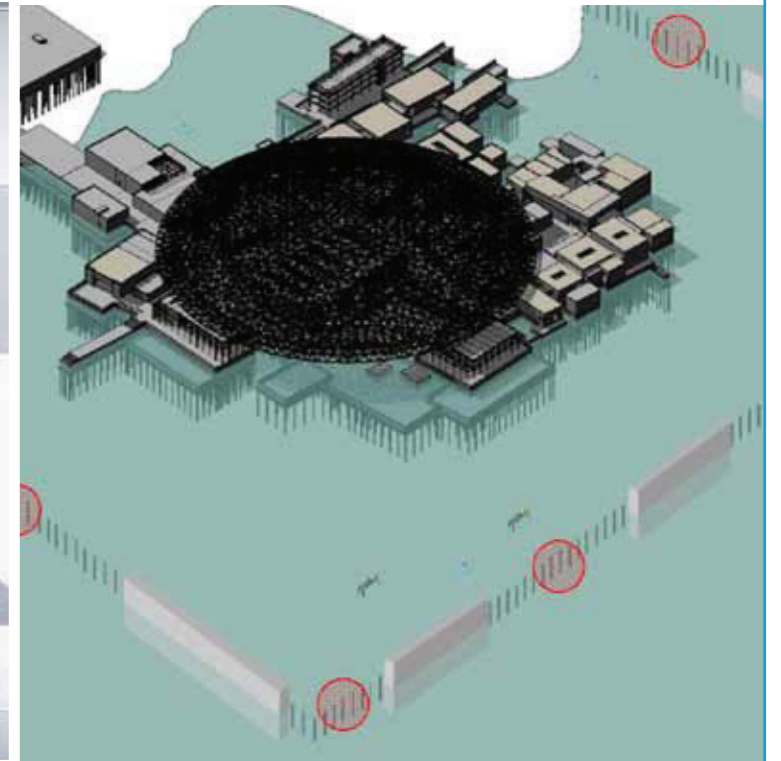

Maritime security can be achieved operationally through the deployment of law enforcement maritime patrols

In high risk environments, such as critical national infrastructure, maritime security measures may be necessary

## Innovation

Permanent revetment wall construction

Where maritime protection is required without impacting the architectural vision for a project, innovation is required. In this example, water piles have been designed to deny access to maritime craft but allow access to sea life and enable natural flushing, preventing stagnation

DT 1.2: Hostile Vehicle Mitigation

Hostile Vehicle Mitigation (HVM) measures will be necessary wherever there is a requirement to deny a determined attacker from using a vehicle to access a space. These measures are primarily deployed to maintain stand-off distance and reduce the risk from a VBIED. However they may also be necessary to deny close vehicle access to buildings assessed to be at risk from crimes such as armed robbery. During planning, stand-off should be maximised and in some circumstances, particularly for crowded places, this requires HVM to be placed in the public realm, which is a significant challenge. In these circumstances, HVM measures should be seamlessly integrated into the urban fabric. The guidance contained below will help designers to achieve this aspiration.
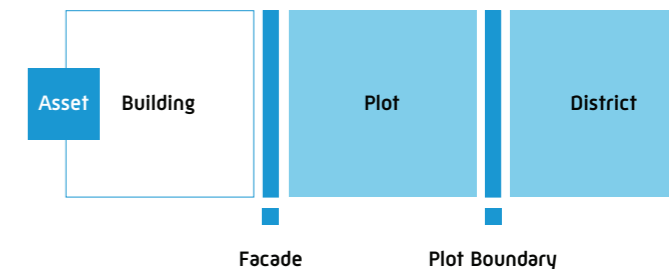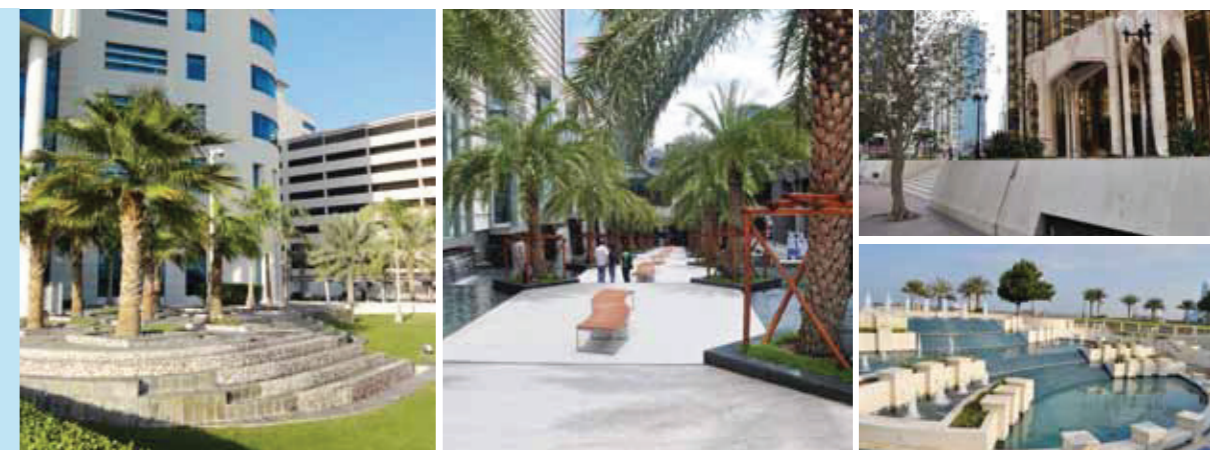
Design Factors

1. If a site does not totally exclude vehicles, it will be necessary to include active HVM and access points at the HVM line.

2. A HVM line must be continuous and integrated with other elements to provide 360 degree vehicle denial around the asset to be protected.

3. Designers should aspire to provide HVM through natural and topographical features, or through dual purpose elements that are already part of the public realm.

4. Walls and fences used as a boundary treatment can be hardened to resist the impact of a vehicle. However, other more innovative methods can be used that achieve the same objective in a much more aesthetically pleasing manner, as well as enhancing pedestrian connectivity.

5. There is no 'one size fits all' response to HVM as every situation requires a well-informed, tailored solution.

A fresh approach is required from public realm designers to ensure that HVM measures are integrated seamlessly into the environment to provide appropriate security whilst also creating beautiful places. This Design Toolkit explores design thinking and provides technical information to demonstrate ways of addressing this challenge.

Emirates Stadium, UK, employs a range of innovative and standard systems to create a continuous HVM line

Asset	Building	Plot	District

Facade   Plot Boundary

Landscaping and Level Change

Water Features

Public Art and Street Furniture

Design Factors

6. The maximum clear distance between adjacent HVM elements should be no greater than 1,200mm. This dimension is designed to prevent encroachment of vehicles beyond the HVM line, whilst maintaining access for pedestrians, wheelchairs and pushchairs.

7. The 1,200mm clear distance should be measured between elements at a height of 600mm above ground level.

8. The minimum height for fixed vertical structures is 500mm, however an increased height of 900mm or more will make the measure more noticeable, assist the visually impaired and typically reduce penetration of a hostile vehicle attack.

9. When located alongside a highway, HVM should be located at least 450mm from the kerb edge to prevent conflict with road users.

10. All elements of HVM should be fit-for-purpose and successfully tested to either BSI PAS 68 'Impact test specifications for vehicle security barriers' or CWA 16221 'Vehicle security barriers –performance requirements, test methods and application guidance'.

$$\text{Kinetic Energy} = \tfrac{1}{2} MV^2$$

(where m is the mass of the vehicle and v is the velocity or speed)

A small decrease in speed = a large decrease in energy = reduced impact = smaller and less intrusive HVM measures and possibly reduced costs

(Refer to PT2: Access and Circulation Routes)

Where it has not been possible to adopt natural, landscape or dual purpose elements for HVM, then purpose built measures will need to be considered. In these circumstances, projects should aspire to use elements specifically designed to blend in with the local context. Standard security products should only be used as a last resort, as lines of bollards can be monotonous and degrade the public realm. In some circumstances, particularly with existing built environments, HVM measures will not have been considered from the outset and solutions may need to be retrofitted. Unless carefully planned and designed, these solutions may be less effective, be more costly and have a negative aesthetic impact. Temporary measures should be avoided as they impact on aesthetics and site functionality – it is far better to design for adaptability and consider the long-term use of the building and changes in threat.

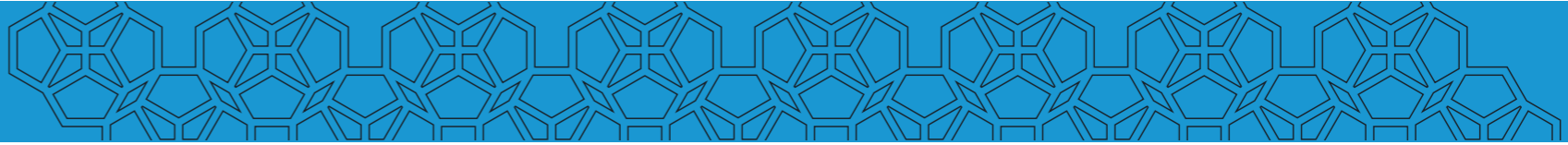Contextual

Security Furniture

Temporary

Visitor attractions and crowded places
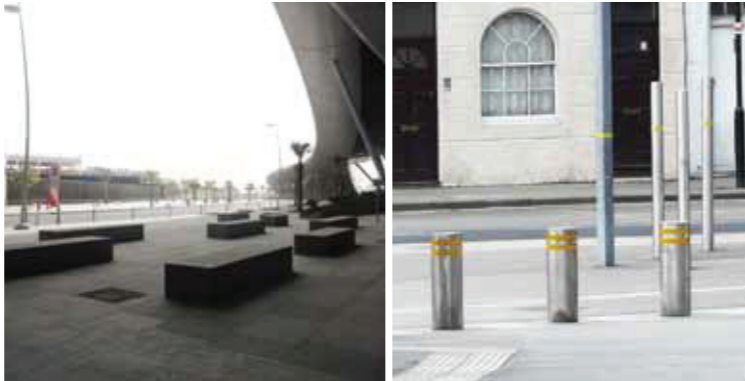
Business districts

Government buildings

Transport locations
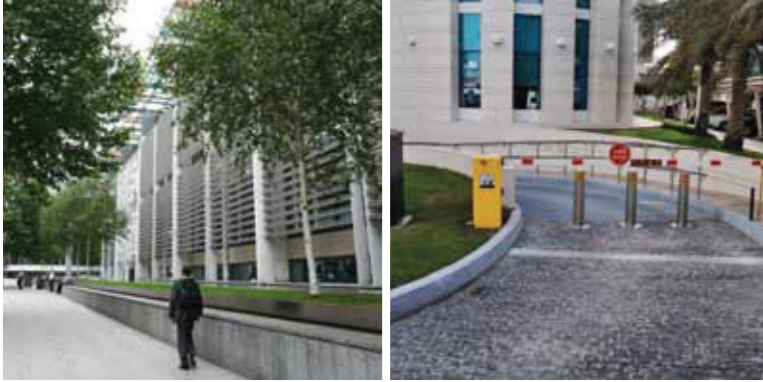
DT 1.3: Vehicle Access Control Points

Vehicle access control points provide legitimate vehicles with access through a secure perimeter or HVM line where vehicle inclusion is required.

For low risk projects where stand-off is not required, projects may decide to introduce a degree of vehicle access control for traffic management purposes. Reasons could include restricting access to reserved parking areas or simply to monitor what vehicles are on site at any given time. This type of system may be used to detect suspicious activity or theft of property from a site.

If during project planning it was determined to be necessary to protect the building from hostile vehicle attack, then active HVM measures will be required to control vehicles at entrances. At these entrances there will be a series of measures deployed to deny unauthorised access and implement any screening deemed necessary to protect assets. These measures will need to maximise the rate of entry of authorised vehicles to prevent excessive delay to users. A safety and security specialist should be appointed to ensure any installation is fit-for-purpose.

This section shows how the types of access control components differ depending on the degree of access control and denial required at a project.

Design Factors

1. Vehicle access control points used to deny vehicle access should be located along the 360° HVM line. They must offer the same security performance against vehicle attack as the fixed (static) HVM barriers located around the vehicle perimeter.

2. To deny access, the specification of the barriers must take into account vehicle size and velocity of attack. This is influenced by the vehicle approach route e.g. gradient, direct or indirect approach and the terrain.

3. Adequate space should be allocated between the point of challenge and the deployable barriers. This space is determined by approach speed and allows the device to be fully deployed before impact.

4. Vehicle access control point design and procedures should be tailored to the different user groups e.g. staff, visitors, VIPs and deliveries. This may necessitate the provision of different access control infrastructure and facilities at each vehicle access control point.

5. Some entrances may be used infrequently or for access by fewer users. This may affect the type of vehicle access control barrier used e.g. gates versus wedges or rising bollards.

6. Most high security access control points will incorporate guard facilities to allow vehicles and occupants to be assessed. The design of these facilities should provide a safe environment for the occupiers in the event of an attempted ramming incident and should maintain the integrity of the HVM line against the design vehicle and velocity.

7. Where vehicle inspection is required at high throughput entrances, there should be a separate vehicle inspection area or lane to prevent blocking of subsequent vehicles. These areas are often best screened from public view where space is available. Vehicles should be inspected on the non-secure side of the HVM line.

8. It is important that the design of the access control point provides for vehicle rejection without needing a vehicle to enter the secure side of the HVM line.

9. Infrastructure is required for guard post facilities, access control and screening systems at vehicle access control points.

10. For the highest level of vehicle access control and denial, a 'Sally Port' of interlocking barriers may be required.

Asset | Building | Plot | District

Facade | Plot Boundary

Rejection lane
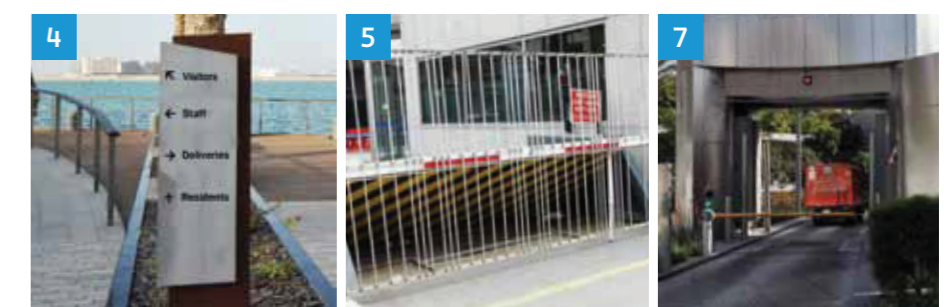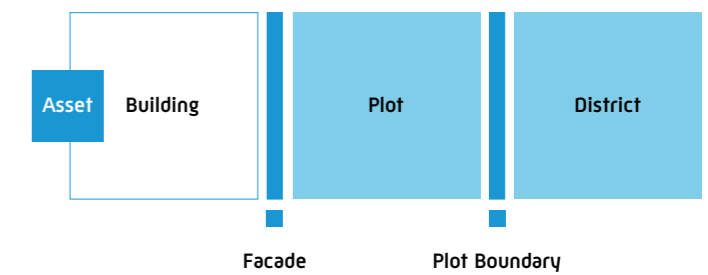
Access control points should integrate dedicated lanes for pedestrians and bicyclists. If this is not feasible, try to use bollards rather than rising wedges or gates, if these can accommodate the security function

Traffic Management
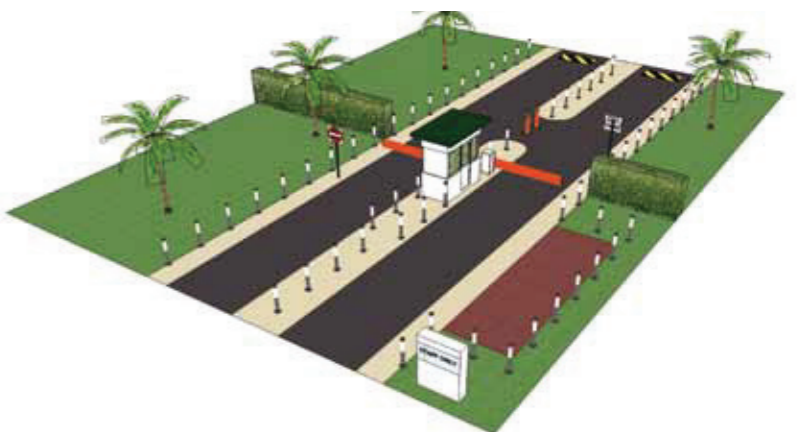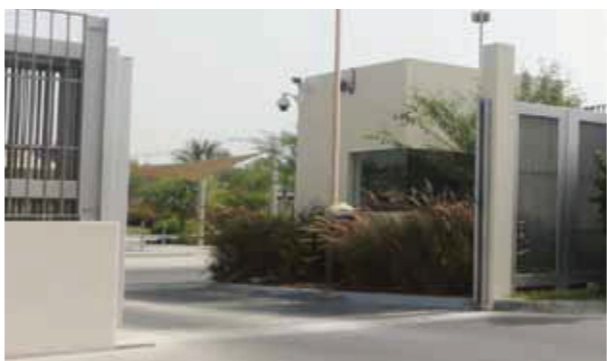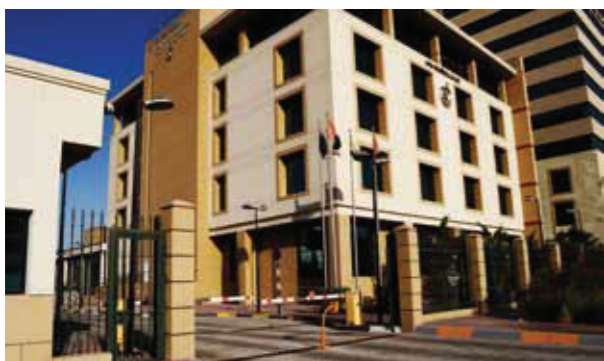
Typical local examples of traffic management measures

Road Signs

Integration

A well-designed system of signage and markings will increase legitimate and consensual drivers' awareness when approaching VACPs. However, they will not prevent or even influence a determined vehicle borne attacker

Innovative architectural design can transform otherwise mundane control and search locations into visually appealing site design elements

Vehicle Denial

Typical examples of vehicle access control points for higher risk environments

Innovation
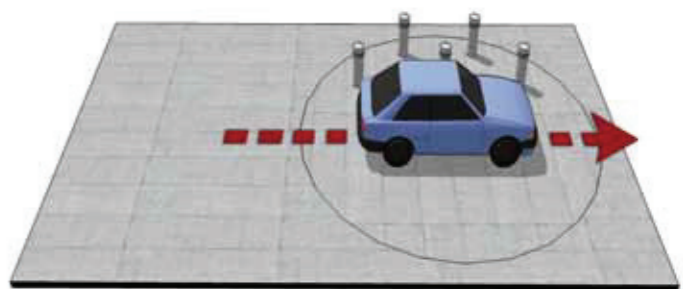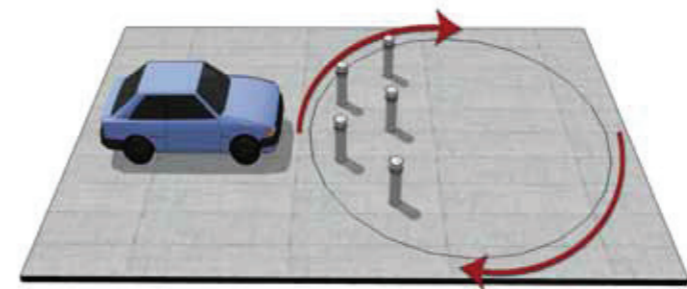
Incorporation of a turntable can provide access through a HVM line and allow greater use of public art and other street design elements

DT 1.4: Pedestrian Access Control Points

Asset

For a project featuring a secure perimeter at or near the plot boundary, pedestrian access control points will function to monitor or control access. In a high risk environment, these access points will feature a series of measures deployed to deter, delay, detect or even deny unauthorised access and will facilitate any screening and searching deemed necessary to protect assets within the secure perimeter. The design of each access control point will need to maximise the rate of entry of authorised users to prevent excessive delays, while meeting the security requirements. A safety and security specialist should be appointed to ensure any installation is fit-for-purpose.
In low risk projects, an access control point is more likely to be integrated into the perimeter to deter and/or detect unauthorised access or simply to monitor who and how many people are on site at a given time. This can be useful at business premises to monitor hours worked by employees, detect suspicious activity or attempted theft and to verify that occupants have evacuated safely in an emergency situation. In addition, if there is an increased security threat, access control can be 'scaled-up' at these locations.

Asset | Building | Plot | District

Facade | Plot Boundary
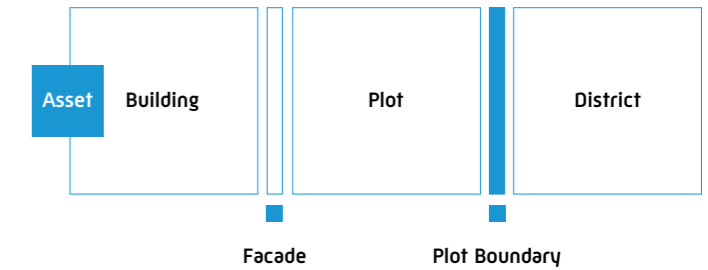
Design Factors

1. Each entry point represents a security vulnerability and increases demands on operations. The number of access control points should be minimised while meeting emergency access and evacuation requirements.

2. Highlight the main access points and use wayfinding signage so that visitors, staff and commercial visitors use appropriate entrances.

3. Determine the security access control requirement. Is it necessary to control access to the site or is monitoring access to the site sufficient?

4. Access control starts with determining if a user is legitimate and should be allowed access. This typically requires reception facilities for visitors or can utilise automated systems.

5. A manual or automated system may be used to deter, delay, detect and deny attempted unauthorised access.

Low Access Control

Typical examples of low control pedestrian access points

Medium Access Control

Typical examples of pedestrian access control points that offer medium levels of control

High Access Control

Typical examples of pedestrian access control points offering high levels of control

DT 1.5: Material Selection and Planting

Landscape and urban designers can draw on a palette of materials and plants when designing outdoor spaces. The elements used should be designed for the intended use and be appropriate, given the context. Certain attributes can be used to serve a specific safety and security function. Designers should note that in many cases planting may not reach maturity for many years and will require ongoing management and maintenance.

The design specification of all elements should take into account the impact of local environmental conditions. The impact of dust, sand, humidity and salinity need to be considered when designing in Abu Dhabi.

| Asset | Building | | Plot | District |

Facade   Plot Boundary
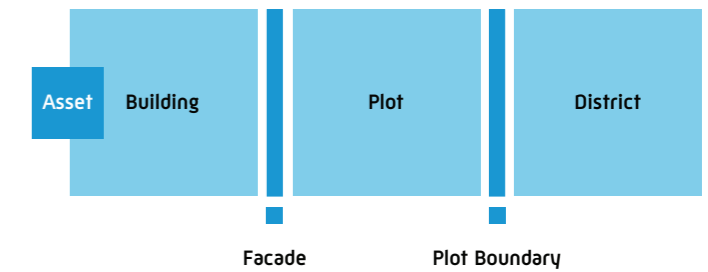
Robust materials used in an area subject to constant use

Elements selected exhibit design quality, attract users and instil ownership over the space

The designers choice of glazing could result in secondary fragmentation risk in a crowded place

Trees act as a climbing aid for intruders
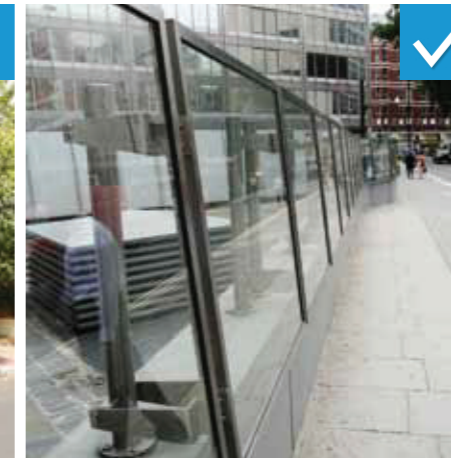
This boundary wall offers both natural surveillance and is shatter resistant, so avoids secondary fragmentation
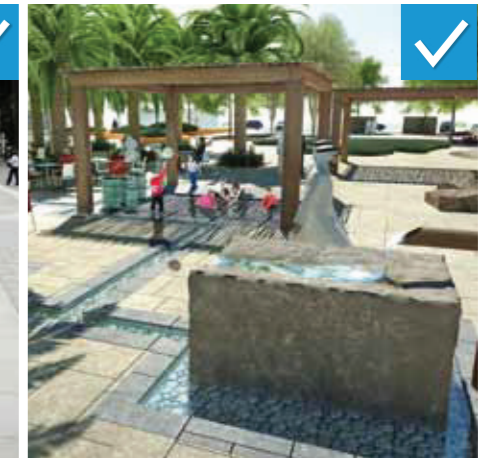
Elements selected are attractive to users

Transparent materials used to improve natural surveillance
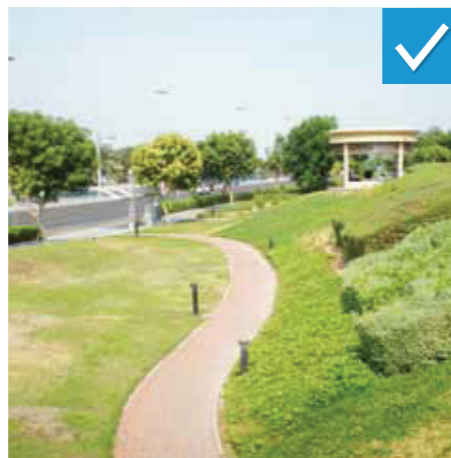
Planting creates clear sight lines for pedestrians and avoids the creation of hiding places
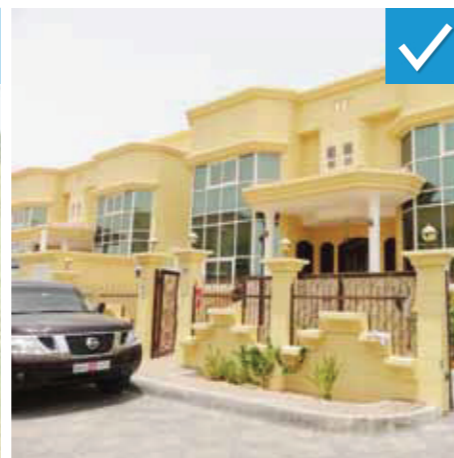
Perimeter sight lines have been maintained around this residence through the use of ornamental fencing
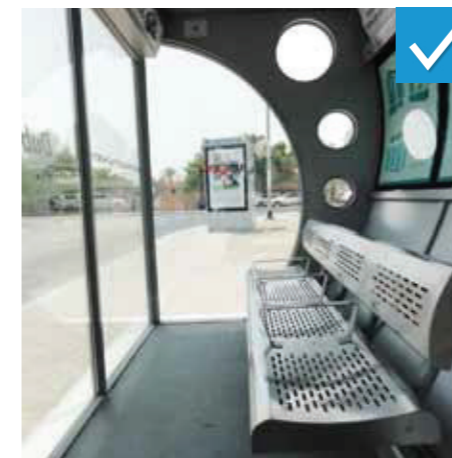
Transparent materials can be used to improve community safety

Ongoing maintenance is required due to poor design integration between active surveillance and landscaping
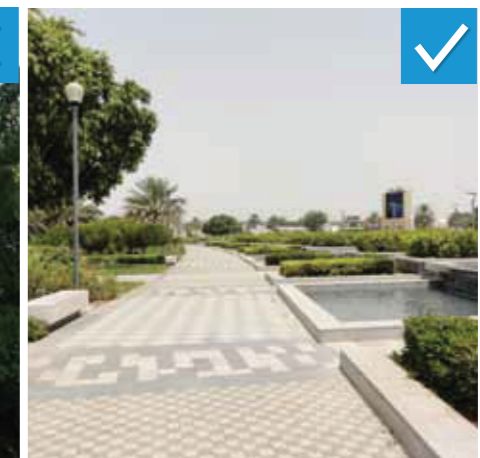
A simple change of material is used to demonstrate change of use

The use of natural materials is encouraged but they do require management and maintenance

All metallic elements are painted to avoid corrosion

Tamperproof lighting design

These bollards are used for parking management but would not be effective for hostile vehicle mitigation

Innovation – Transport Premises

After Improvised Explosive Devices were left within trash bins at transport stations in London, the initial reaction of many station owners and operators was to remove these bins. This operational response soon led to issues of littering and complaints of poor management and maintenance at stations.

A simple and effective solution was the use of transparent plastic refuse bags that allow a suspicious device to be easily detected by staff or members of the public.

Abu Dhabi Bus Station

The bright and colourful street furniture makes this plaza attractive and welcoming to users

Planting along the pedestrian walkway in this plaza allows users to be aware of their surroundings

DT2 | Architectural Design

Architects create and implement the vision for a building project. Architects are familiar with the importance of life safety as it is fundamental in the design and construction of buildings. Although, many architects are unfamiliar with the Principles of community safety and protective security.

"In June 1996, a terrorist truck bomb explosion at the Khobar Towers, in Dharan, Saudi Arabia, caused 19 deaths and hundreds of injuries. A Government report estimated that flying glass shreds from the blast caused up to 90% of the fatalities."

(Building Security, Barbara A. Nadel FAIA)

This part of the Design Toolkit focuses on the application of physical security to reduce vulnerabilities to intrusion, blast and ballistic attack.

An architect should seek specialist advice regarding elements used to address a specific security risk, such as hostile vehicle attack. A specialist can ensure physical security elements are cost effective and fit for purpose.

Abu Dhabi International Building Code

The Abu Dhabi International Building Code adopted by the Department of Municipal Affairs does not contain minimum security requirements for buildings. This is because risks are project and context specific.

To avoid conflicting requirements, this Design Toolkit does not mandate any particular solution, it simply presents guidance to assist in design decisions.

It is important that these design decisions are made using a holistic approach to ensure integrated security.

There are three design tools presented in this section

Asset | Building | Plot | District

Facade | Plot Boundary
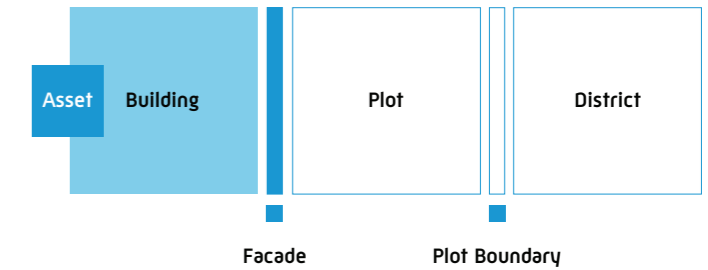
DT 2-1: Facade Design

DT 2-2: Building Entrances
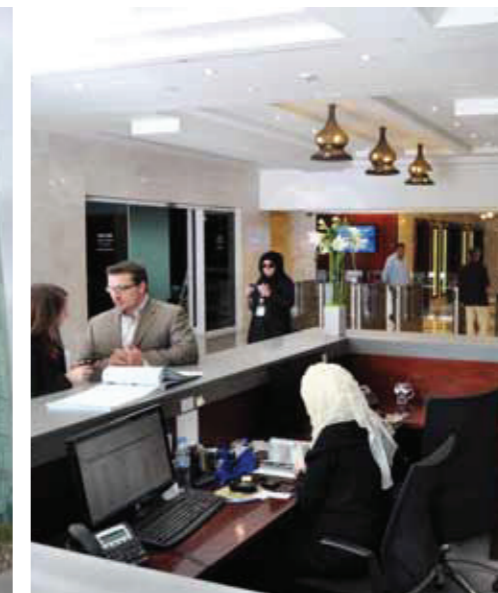
DT 2-3: Structural Design

Crowded Places

Many of the design elements presented here will be required at crowded places such as shopping malls, transport premises and exhibition centres.

These locations, to which members of the public can gain access, may be considered a terrorist target. The Abu Dhabi Urban Planning Council or the relevant Municipality Town Planning department can direct the project team to Government safety and security advisors if further advice is required.
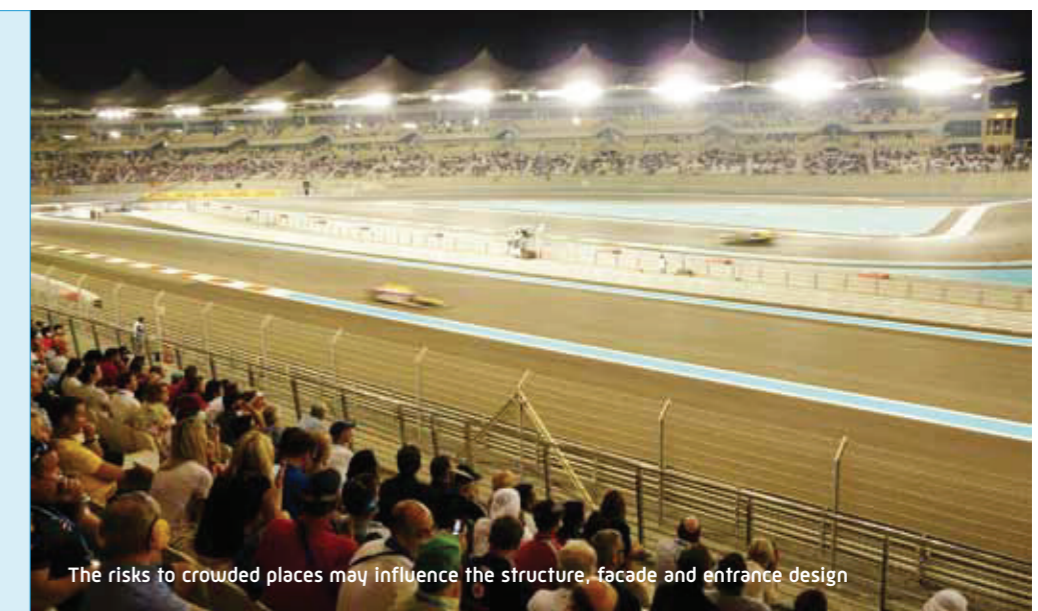
The risks to crowded places may influence the structure, facade and entrance design

DT 2.1: Facade Design

The skin of a building contributes to energy performance, aesthetics, fire safety, internal comfort and safety and security. The four aspects to consider from a safety and security perspective are the facades role in surveillance, its ability to deter or deny access to the building, the protection it offers against blast and the protection it offers against ballistic attack.

In many buildings, the facade is the first line of defence between public and private space. In buildings at risk of terrorist attack, it is critical that the facade does not contribute to injuries or fatalities by producing large quantities of glass shards (secondary fragmentation). The design of the facade should be influenced by the risk assessment findings.

Design for privacy

Design for natural surveillance

Innovation

The mashrabiya is used in this case to delay unauthorised access through this window. It is aesthetically pleasing and was specifically designed by the architectural team to meet the minimum specified criteria set by the project owner.

Intruder Protection

The first step in reducing the likelihood of unauthorised entry is to reduce the number and size of openings.

Khalidiya Police Station, Abu Dhabi
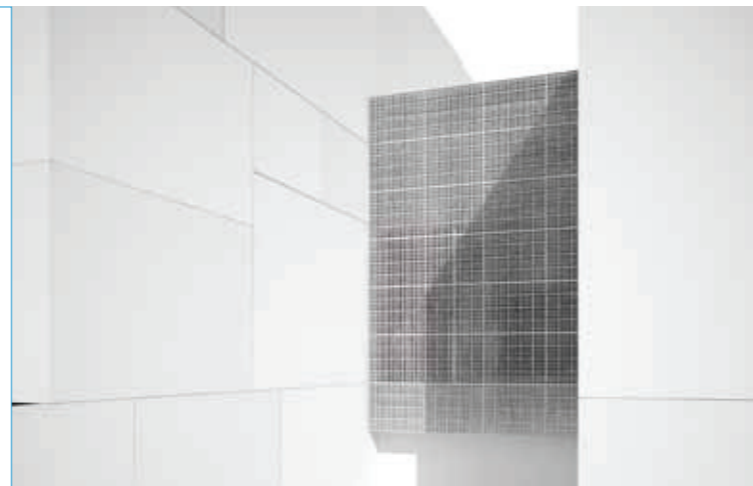
Facade Openings

Openings in facades are a popular point of unauthorised entry to a building. Access may be gained either by breaking through a door, window or other aperture; or simply gaining access where the aperture has been left open. A range of protection options are presented below.

Low Security → High Security

Windows	Openable windows	Glazed curtain wall	Window grilles
Doors	Glass door	Steel door	Blast doors
Other openings	Unsecured air intake	High level air intake	Roof mounted HVAC
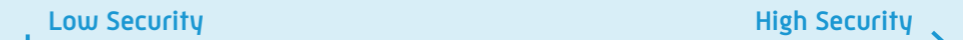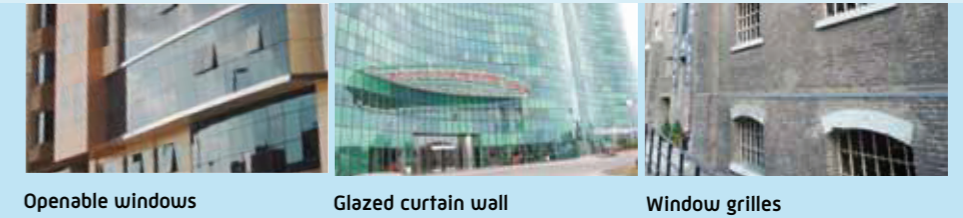
Blast Resistance

Glass has widespread use in facade design. If a facade is subject to blast loading, shards of glass can result in severe injuries to occupants and those in the proximity of the building. It is widely accepted that in the majority of explosions in urban areas, it is glass that causes more injuries than the explosive blast itself.

Start with the Basics

If the glass must offer a certain level of protection eg. it must not break, the project team should consult a specialist, as these systems can be expensive, heavy and must be designed as an integrated part of the facade and structural design.

1

Sheikh Zayed Grand Mosque, Abu Dhabi

Use non-glazed facade systems if blast is a concern. This will reduce secondary fragmentation

2

Masdar, Abu Dhabi

Limit the size and number of glazed elements

3

Place glazing closer to the floor to reduce the distance that glass shards will fly within perimeter rooms

4

Glass

PVB film
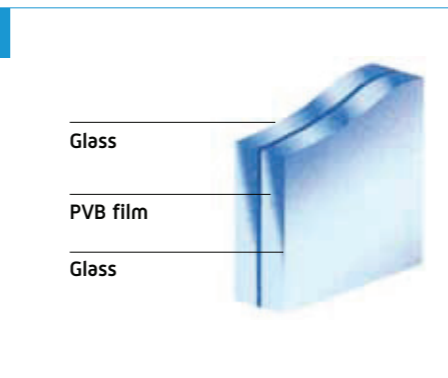
Glass

Use laminated glazing, appropriately anchored to its frame, as its PVB interlayer will reduce secondary fragmentation

Existing Buildings

It is possible for blast protection to be enhanced without replacing float or annealed glass windows. Anti-shatter film, sometimes referred to as security film, is placed on the internal surface of glazing and acts in the same way as a PVB layer in laminated glass, to hold together glass fragments if the glass is attacked or experiences blast loading.

It is not as effective as laminated glass and does not prevent glass from leaving the frame as this will be determined by the anchorage of the existing glazing system. In addition, it is necessary to replace the film at periodic intervals determined by the supplier, as the film degrades over time in ultra-violet light.

Ballistic Resistance

If a facade is required to offer protection against ballistic attack, then it is wise to consult a specialist. Normally, ballistic glazing is used to protect a particular individual or user group from an attack. It is rarely practical or cost effective to protect an entirely glazed facade. If protection is required for an entire building, it would make sense to avoid transparent materials in the cladding system or use other elements of the Planning Toolkit and Design Toolkit, such as topographic features or planting to hide potential targets from sight.

Asset | Building | Plot | District

Facade | Plot Boundary

Special Applications

VIP Area

Guard post featuring ballistic rated glazing

Innovation

The security function of these shutters is only required at night when the Museum is closed.

The shutters are hidden in this facade during the day; this was possible through the integrated approach adopted by the structural engineer, facade engineer, architect and the safety and security specialist.

Rodin Museum, Paris (France)
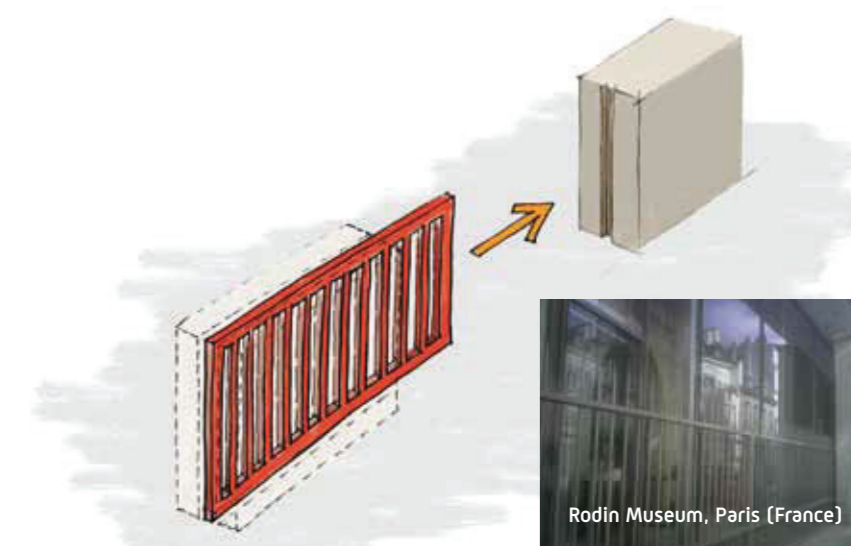
DT 2.2: Building Entrances

Each building entrance represents a security vulnerability. As such, the design of each entrance must address any needs to monitor or control access to a building.

In many buildings, the facade and its associated entrances will be the first point of access control from public to private space. It is therefore of primary importance that the access control needs of the project are understood by the architect.

Interlock Doors

Purpose built interlock doors are used in high security facilities to prevent tailgating through access control measures at entrances. They significantly reduce throughput and are typically viable only where access is highly controlled to a small user group.

Asset | Building | Plot | District
Facade | Plot Boundary
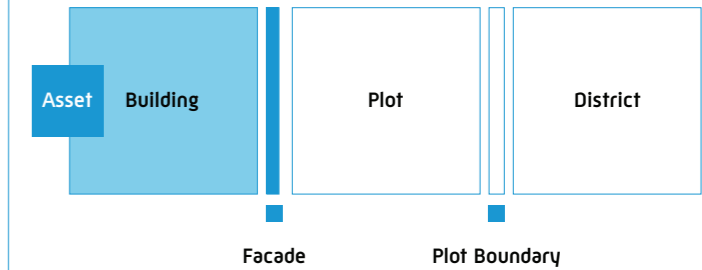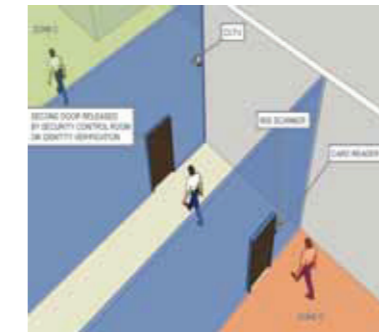
Design Factors

1. The number of entrances should be minimised having regard for fire safety requirements.

2. Highlight the main building entrances so that visitors and staff use appropriate entrances.

3. Determine whether it is necessary to control access, such as in an office, or if monitoring access only is appropriate e.g. in a shopping mall.

4. If there is a need to control access, it is likely that more space will be required to avoid increased entry time delays for users.

5. If there is a need to control access, there may be a need to separate user groups as certain groups will be more trusted than others e.g. staff vs. visitors.

6. Access control starts with determining if a user is legitimate and should be allowed access. This typically requires reception facilities for visitors.

7. A manual or automated system may be used to deter, delay, detect and deny attempted unauthorised access.

8. Search & screen capability may be required as part of the regular entry procedure for all pedestrians or limited to certain user groups.

9. Search & screen capability may be required only temporarily e.g. special events or increased threat. It is important to design for adaptability.

Low Access Control

Low control measures are primarily intended to deter unauthorised users and welcome or direct legitimate users
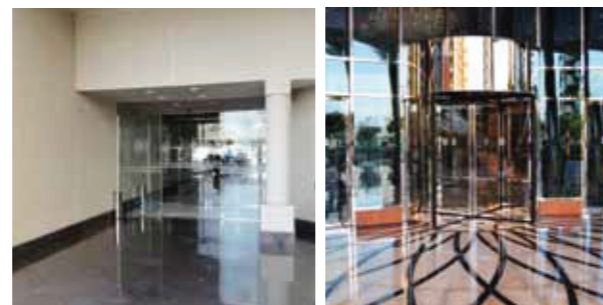
As well as providing environmental protection, doors also offer deterrence and delay unauthorised access when locked

Medium Access Control

Low height turnstiles usually used in industrial or back of house areas help to prevent tailgating but can be easily vaulted

Speedgates are less industrial and help to prevent tailgating

High Access Control

Searching and screening equipment will be required where banned items need to be detected such as at stadia or secure Government facilities

Full height turnstiles do not allow passage until the user has been verified. The risk of tailgating is reduced considerably

DT 2.3: Structural Design

Whereas it is standard practice in Abu Dhabi for a structural engineer to design for wind and seismic loading, it is unlikely that they will have designed a structure to resist blast loading. That is unless they have been instructed to do so following a risk assessment and a decision by a client or stakeholders to enhance protection.

Structural design plays an important role in protecting buildings against blast loading, particularly where a building benefits from limited stand-off. Structural hardening is expensive and should be considered after the basic design guidance provided here has been incorporated to make the structure more resilient.

Specialist Advice

Structural design for blast loading can be complex and requires specialist advice, particularly for innovative structural forms that are commonly seen in new signature developments in Abu Dhabi.

- Blast wave breaks windows
- Exterior walls are blown in
- Columns may be damaged
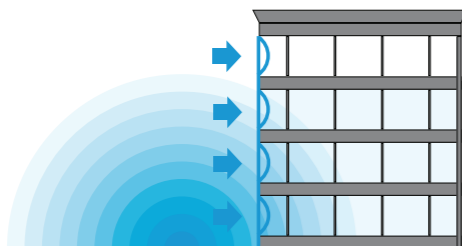
- Blast wave forces floors upward
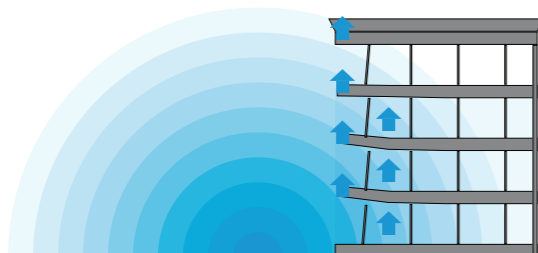
- Blast wave surrounds the structure
- Downward pressure on the roof
- Inward pressure on all sides
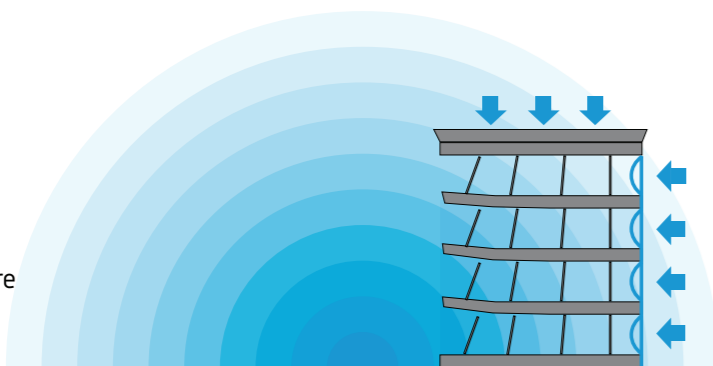
Explosive Blast Loading

An explosive blast is associated with extreme but very short duration loading of a structure. The pressure acting on the structure can be orders of magnitude above wind loading but is experienced for a much shorter duration. Unfortunately, history shows us that building damage can range from glazing failure through to disproportionate or complete collapse.

Glazing failure resulting from a large VBIED, Canary Wharf, London, UK

Progressive collapse resulting from a large VBIED, Oklahoma City, USA

Prevent Disproportionate Collapse

This situation arises where the local failure of primary elements of structure leads to progressive failures of elements more remote from the initial cause. This leads to damage that is disproportionate to the original cause. Regardless of how well a building needs to be protected to meet the client and stakeholders objectives, the most important job of the structural engineer is to prevent disproportionate collapse.

A resilient structure will exhibit the following attributes to reduce the likelihood of disproportionate collapse.

Asset	Building	Plot	District
	Facade	Plot Boundary	
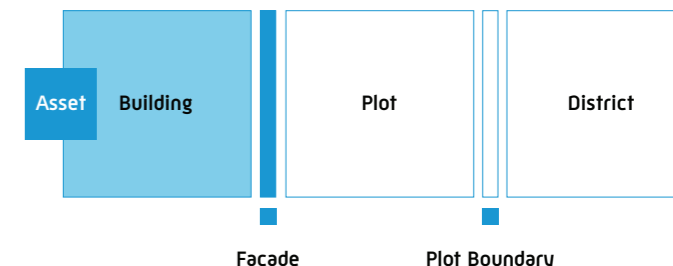
Redundancy	Multiple load paths to accommodate abnormal loads
Load reversal	Primary and secondary elements and connections that can accommodate reversal of loads
Ductility	The ability of elements to deform without collapse. Cast-in-place reinforced concrete exhibits this attribute and sees widespread use in Abu Dhabi.
Shear load capacity	Elements have sufficient strength and ductility not to fail in shear.

Start with the Basics

The guidance below may conflict with other design objectives so it is imperative that the design team work collaboratively and holistically.

1. Concentrate on the most important elements first

2. Avoid large floor to floor heights, while complying with minimum building code standards

3. Avoid direct exposure of primary structural elements e.g. architectural shroud

4. Design with regular, limited structural spans

1 — Primary structure → Secondary structure → Non-load bearing elements

2

3 — Concrete column — Metal shroud to provide stand-off

4
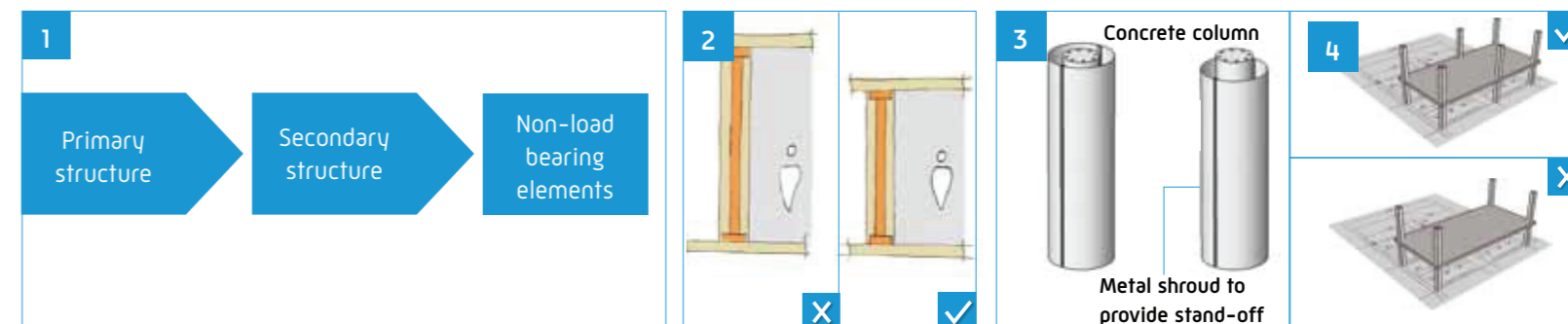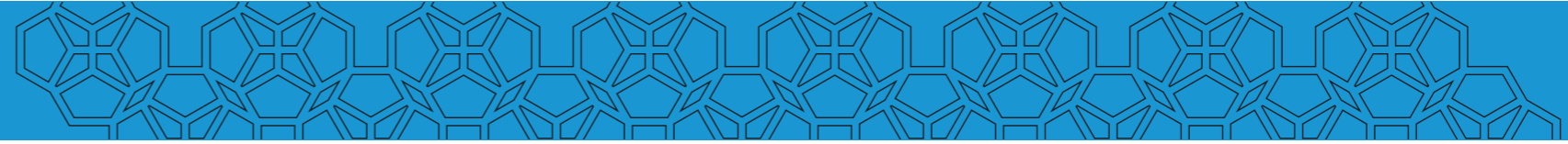
DT3 | Systems Design

Engineers design, construct and maintain the systems that support communication and provide energy, cooling and clean running water. This Design Toolkit includes guidelines for the protection of these systems against malicious attack. It also highlights the role of security systems in achieving defence in depth.

Architects, urban designers and landscape designers should seek specialist advice to ensure security systems are cost effective and fit-for-purpose.

'CCTV ...remains one of the most effective tools to combat crime and anti-social behaviour provided the installation, operation and management are of a high standard'

UK Home Office Online Report 15/05: the Impact of CCTV, Fourteen Case Studies

Asset | Building | Plot | District
Facade | Plot Boundary
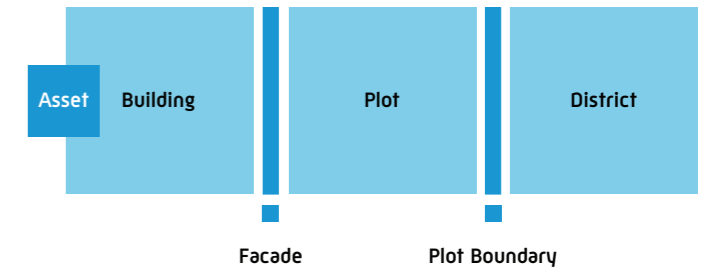
There are three design tools presented in this section

DT 3.1: Utilities and Infrastructure

Case Study –

Not fit-for-purpose

A high risk project developed a security solution that was not-fit-for purpose. Key failings included:

- Unbalanced solution – omission of physical security as the developer's consultant was only contracted to provide technical systems;
- No strategy to justify or inform system deployment;
- No operational requirements for systems; and
- Inappropriate selection of technologies for building environment and security objectives.

The result for the client was:

- Project delay as numerous iterations of design development were required to reach a viable solution;
- Difficulty in obtaining insurance; and
- Over AED 2 million wasted on systems procured that could not be used.

The safety and security specialist is tasked with developing a strategy that integrates all three aspects of a security programme

Operations

Physical — Systems

Strategy
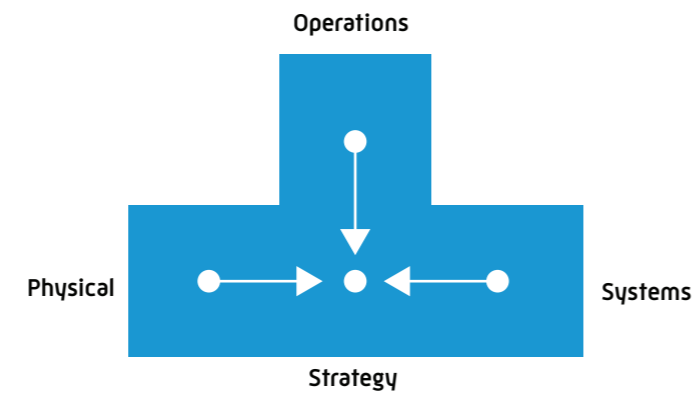
Selection of equipment must take into account the local weather conditions. Temperatures in the summer can exceed the maximum operating temperatures of many products. Sandstorms can also degrade areas of coverage and dust can create additional maintenance requirements

Abu Dhabi Environmental Factors

Shaded areas are not covered by surveillance ✗

Placement of cameras allows for effective surveillance ✓

Large areas of the public realm in Abu Dhabi require shading. This can drastically impair surveillance coverage unless coordinated during design.

DT 3.2: Plot Security Systems

DT 3.3 Building Security Systems

At these buildings in Abu Dhabi, CCTV cameras have been installed below shading canopies

DT 3.1: Utilities and Infrastructure

The Planning Toolkit highlighted how appropriate infrastructure placement can reduce loss of supply and unauthorised access vulnerabilities at a site. 'Designing-in' protection of utilities and infrastructure will improve business continuity, prevent circumvention of physical security installations and support life safety and site security functions.

Utility and infrastructure protection requirements are project-specific and should be assessed as part of the Integrated Development Process. It is important that designers follow applicable Regulations and guidance of utility providers. Any proposed deviations for safety and security reasons shall be subject to a utility provider's 'No Objection Certificate'.

Asset | Building | Plot | District

Facade | Plot Boundary

'Utilities and infrastructure can be vulnerable to attack within the district, at the plot boundary, within the plot and at building entry points'
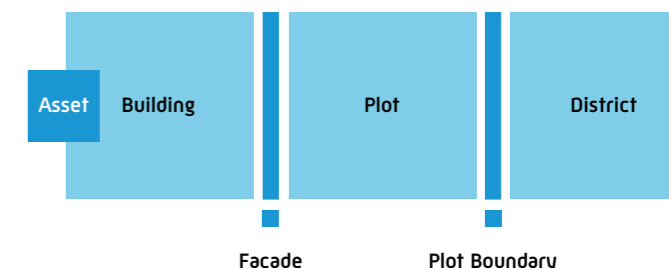
Start with the Basics

1. As part of the risk assessment process, determine what infrastructure is critical to normal, life safety and security operations.

2. Minimise access openings to infrastructure. Where possible bury infrastructure or hide it.

3. Where access is required to meet utility provider or system installation standards, incorporate appropriate access control and intruder detection where justified by risk assessment.

4. Minimise or close infrastructure openings to prevent unauthorised access to the site or building (security circumvention) using utility and infrastructure routes.

5. Harden critical infrastructure from malicious attack where resilience is not afforded by dispersed, redundant supplies i.e. there remains a risk of simultaneous failure of primary and back-up supply.

Case Study –
Manufacturing Plant (Abu Dhabi)

The proposed vehicle access control point for a manufacturing plant was located adjacent to the only electrical substation and all feeds to the site were routed along the same service road. This created a single point of failure. The utility feeds were fixed by the utility provider, and the options for reducing the supply vulnerability were constrained to:

- Removing the entry road;
- Re-planning the site entrance;
- Repositioning the electrical substation; and
- Hardening the utilities.

Manufacturing Plant

VACP

Substation
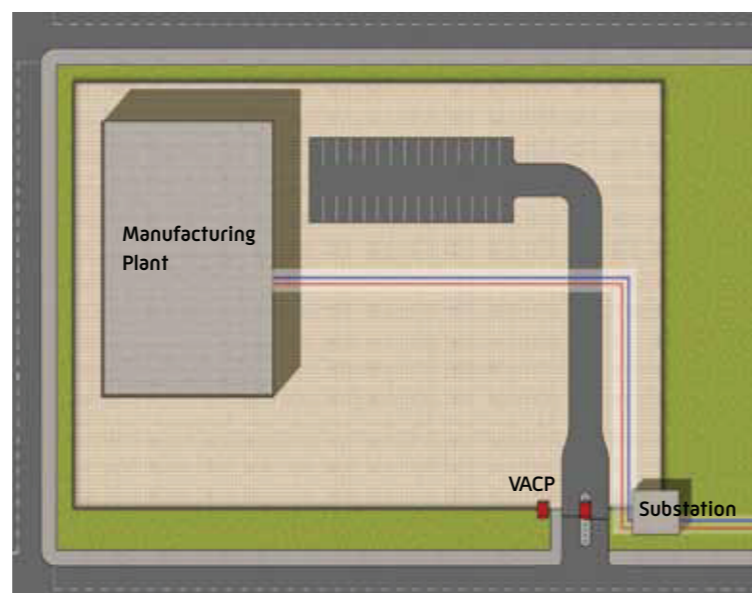
Case Study –
Virtual National Bank Data Centre
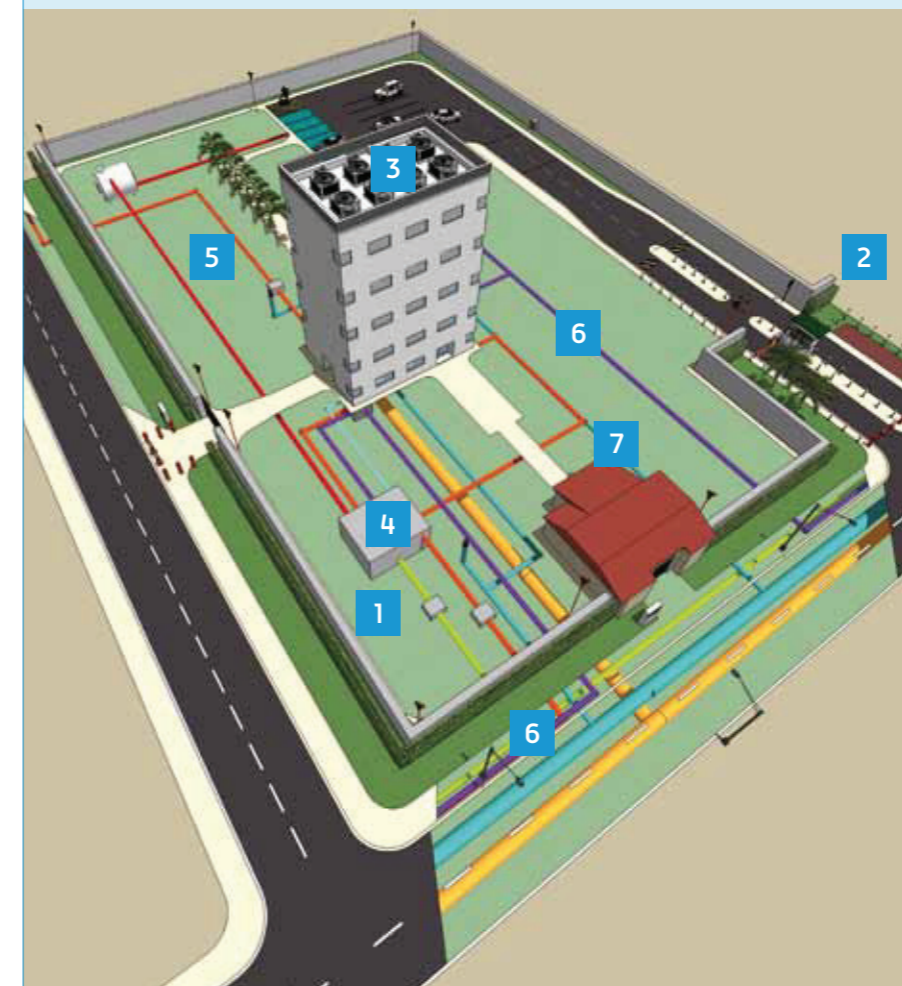
This data centre handles all debit and credit card transactions for Virtual National Bank and business continuity was identified as a key component of the safety and security brief. The design of utilities and infrastructure included:

1. Utility connections – Located within the plot secure boundary and accessible under 24 hours a day supervision.

2. Vehicle access control point - Located remotely from utility lines.

3. Roof mounted HVAC and chillers – Decreasing the vulnerability of operations to tampering and intake of hazardous materials.

4. Remote energy centre – Located within the plot secure perimeter, the energy centre houses generator sets for back-up power supplies and life safety systems.

5. Sewerage and drainage pipes features lockable manholes and grilles.

6. Redundant and diverse ICT fibre infrastructure.

7. Site-wide fire fighting standpipe system in addition to automatic sprinkler and gas suppression systems.

DT 3.2 Plot Security Systems

The best performing security sensor is a highly trained, dedicated human being. Human senses cover all the necessary operations – sight, hearing, smell, touch, taste, feeling and a voice to sound an alarm. The human brain is also able to quickly process inputs from all senses simultaneously and make decisions – a truly integrated system. However, putting a sufficient number of the right people in place to monitor and secure facilities is an expensive proposition. Humans are also prone to error and therefore security systems are deployed as an alternative. As with all other security elements, technology should be

deployed in a layered system to achieve defence in depth. The technology layers should tie in directly with the other physical layers, being used to control access or detect unauthorised access through each layer. The number of technology layers and the type of systems employed should be based on the risk assessment and result in an integrated security strategy.

For low risk projects, there is unlikely to be a requirement to deploy security technology to the external areas, except perhaps for lighting and minimal surveillance. However, high risk projects may require a significant number of systems, including active surveillance, lighting, intrusion detection and access control.
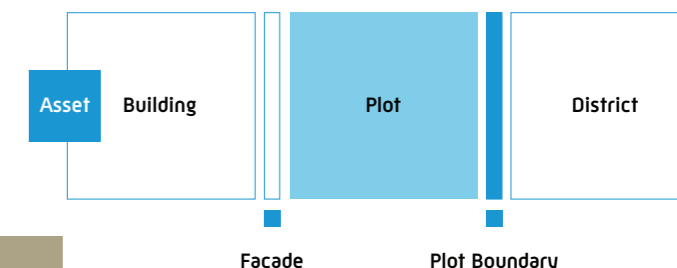
Design Factors

1. The security strategy should reflect an appropriate balance of physical, technical and operational measures.

2. Increased reliance on security systems is likely to result where planning and other design tools have not adequately addressed safety and security risks.

3. Security systems should not be deployed without a technical strategy, based on a documented Operational Requirement (OR).

4. Project teams should appoint a specialist to provide an unbiased assessment of the technical requirement and the most appropriate solutions based on system capability, cost and project needs. System suppliers may over specify as a means of selling their equipment.

5. System design must take into account operational measures. The presence of an on-site security team greatly reduces response times and alarm configuration. Conversely, in order to trigger a police response, many countries now mandate a minimum specification of alarm system (to reduce false call-outs).

6. Technical security solutions must be integrated so that they work together in an effective and coordinated manner and enhance the operational response. Where possible, they should also integrate with other building systems.

7. Security systems should be discrete to reduce the risk of tampering and should fit the architectural and urban design context.

District-Wide Systems

Master developers should consider the deployment of systems on a district-wide basis to increase defence in depth. In the future, private developers may be asked to contribute to public safety and security by installing and operating public realm safety and security systems including surveillance, communication and dynamic signage. This will be determined on a project-by-project basis with stakeholders.

Abu Dhabi wide surveillance system

Asset	Building		Plot		District
	Facade		Plot Boundary		

3 Active Surveillance Systems

Active surveillance is primarily used to monitor the plot boundary, access control points, approach routes, any exclusion areas and activity. Camera selection varied considerably depending on location and function. Surveillance systems are monitored in real time and recorded.

1 Lighting Systems

Well lit spaces improve natural surveillance and reduce the fear of crime. In this case, security lighting is deployed around the plot, building facades and plot boundary to allow security personnel to monitor during darkness. Security lighting has been designed for sensitive areas such as loading bays and the utility compound. High levels of illumination are used at entrances. Where practical, high mast lighting was incorporated as it provides a broader, more natural and uniform light distribution. Motion activated lighting is provided in vulnerable areas and this illuminates when an alarm is triggered, providing deterrence and facilitating a quick response.

2 Automatic Access Control Systems

Access control systems have been deployed at entry points alongside other physical and operational control mechanisms to ensure that only authorised personnel gain access to critical areas. All control systems use one or more of three basic forms of verification:

- 'Something you have' eg. card;
- 'Something you know' eg. password; and
- 'Something you are' eg. fingerprint.

4 Intruder Detection System (IDS)

Exterior Intrusion Detection Systems are used to detect an intruder crossing a boundary of protected areas. In this high risk environment, it is provided at the plot boundary and around other critical areas. A range of systems are used including infrared, seismic, microwave and video motion technologies. Due to the nature of the outdoor environment, exterior sensors are more susceptible to nuisance alarms than interior sensors. The use of dual technology sensors and a thorough site assessment was vital to the delivery of a viable solution for the bank.

DT 3.3 Building Security Systems

The design factors for the deployment of security systems within a building mirror that at a plot level. They should still form part of a holistic, balanced solution and be applied in accordance with the 'defence in depth' concept. The deployment of access control, surveillance and intrusion detection technologies should accurately reflect the internal zoning of a building. Technology solutions should become more stringent as users transition through the building from public to private and then restricted areas. For low risk projects, there may still be a need for several layers of technical security in internal areas – as minimal or no layers exist in external spaces. It would be normal in low risk commercial buildings to see the deployment of active surveillance, access control and intrusion detection systems. For high risk security environments such as Government buildings or research facilities, best practice would dictate a multiple layered solution, with different access control technologies at each layer and multiple layers of intrusion detection using complementary technologies to provide early warning of intrusion and monitoring of intruder movement.

How Much is Enough?

With so many choices of equipment on the market, a challenging issue facing project teams concerns is selecting and installing appropriate technology and determining how much is enough. Specifying appropriate systems is essential to meeting facility needs and safety and security objectives. In some cases e.g. hotels in Abu Dhabi, minimum regulatory requirements must be observed.

Asset Building Plot District

Facade Plot Boundary

Projects are often quick to resort to a heavy deployment of CCTV as a total security solution. However, CCTV is not the panacea to safety and security. Research has proven that it is most effective when combined with other measures

Active Surveillance: Surveillance systems may be used to conduct access control, surveillance and video motion detection. They are normally deployed to monitor building entrances, movement corridors and points of alarm such as emergency exits and critical areas. Video motion detection can generate an alarm when an intruder enters a selected section of the cameras view and trigger recording or prompt other actions.

Access Control Systems: Access control technologies are also deployed to building entrances and at transition points through other internal zones. At the main entrance they are likely to be associated with turnstiles, whereas for other internal areas, they are more likely to be associated with normal door locking mechanisms.
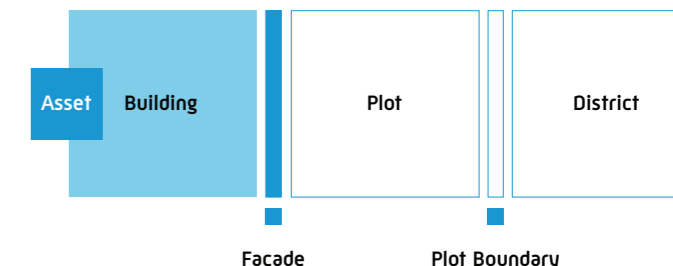
Intruder Detector Systems (IDS): Interior intrusion detection systems are designed to detect penetration or attempted penetration through a facade or other zone boundary. IDS technologies include structural vibration, glass breakage, passive infrared, video motion, microwave and dual technology sensors.
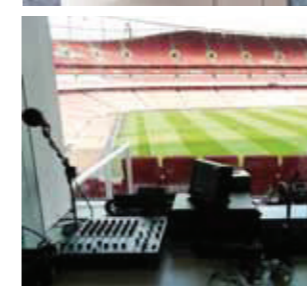
Communication Systems: These systems are designed to enable communication on-site and off-site during normal and emergency operations. Applications include: public address / voice alarm which uses broadcasting to offer mass notification, and emergency voice communication systems used for duress and incident management by staff, visitors or the emergency services.

Search and Screening Systems: Walk-through metal detectors and baggage screening equipment are intended to detect the presence of concealed weapons or other prohibited items. They are normally deployed at the entrance to the building and will require power and space for queuing and further searching.

Deterrence

Technology can deter intruders by being visible or by creating the perception of a security presence. Highly visible detection devices suggest that other devices are also present – prompting an intruder to look elsewhere. However this does not apply to a determined terrorist who is willing to sacrifice his or her life

Security systems must be integrated to maximise efficiency and effectiveness

An ergonomically designed control room allows security personnel to monitor security systems on a 24 hour basis

6

Case Studies

Al Bandar

Context

Al Bandar is located at the eastern end of Al Raha Beach, within close proximity to Abu Dhabi International Airport, Etihad's headquarters and the main Abu Dhabi-Dubai Highway.

The developer's intention was to create a living community in Al Raha Beach, and Al Bandar forms one part of it, fostering a multi-cultural community and encouraging a sense of place.

Within the development there is a full-service marina, supermarket, beverage store, laundry, tennis court, swimming pools, dining areas, an optician, pharmacy, nail salon as well as other retail, plus a residents' clubhouse with multi-purpose facilities.

To Dubai

Al Bandar

Abu Dhabi Airport

To Abu Dhabi

Al Bandar demonstrates the implementation of the Principles, Planning Toolkit and Design Toolkit outlined in this Manual.

Al Bandar, a high-quality waterfront mixed-use development, exhibits many of the traits of a safe and secure development.

Principles and Toolkit in Practice

Al Bandar consists of spaces to which different users have varying degrees of access rights and ownership. The plan below broadly divides the types of spaces open to users into four zones - Private, Semi-Private, Semi-Public and Public. The scheme benefits from clearly defined boundaries and transitions between each zone.

Combined with good access control, landscape design and features, these measures help to create a safe and secure environment.

Single Vehicle Access Control Point

Zones	Access
■ Private	→ Residents' parking
■ Semi-private	→ Visitors' parking
■ Semi-public	⇢ Delivery & emergency access
■ Public	

Spatial Definition

Throughout the development, there are clearly defined spaces.

In the example to the right, psychological and physical cues are used to deter unwanted access, without resorting to physical barriers.

Vehicle Access Control

Designers have introduced a single access control point to the development. By minimising entry to the development via a singular route, it is easier to prevent and monitor unauthorised vehicular access.

Vehicle movement is also restricted to the edges of the development, the exception being for deliveries and emergency response. Residents and visitors' parking areas are located in underground basements, again these are accessed near the entrance of the development, away from the main residential and commercial buildings.

Ownership

In the example to the right, changes in paving and signage have been used to define ownership of space. Where physical barriers have been used, they are attractively designed, blending in with the streetscape. It is clear to different users where Semi-Public and Semi-Private areas begin and end; in this case the space beyond the gate is for residents' use only.

Public Image

The decision taken during the planning and design stages to create high-quality spaces throughout the development (that are easy to manage and maintain) has had a positive impact on safety and security. In addition, the open spaces offer opportunities to enhance natural surveillance and are also adaptable and can be utilised to support emergency response and special events.
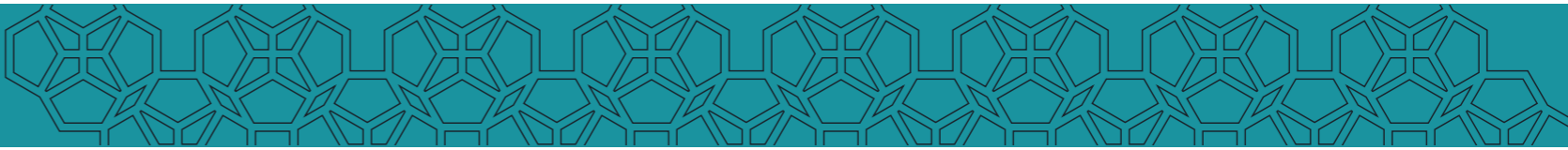
Signage and Wayfinding

The movement framework is well-defined, offering convenient movement between public destinations and discouraging use of more private areas.

Routes and destinations are clearly signed and oriented, helping users move from place to place safely. Evacuation routes and emergency meeting points are well-planned.

The high-quality signage and street furniture contribute to community and place identity.

Activity

The variety of uses, shops, cafes, marina, housing and other leisure facilities helps create a mixed-use community. As a result more people are around at all times, keeping more eyes on the street.

Surveillance

There are high levels of natural surveillance throughout the development. Public spaces, facilities and movement routes can be observed by residents. In the context of this mixed-use community, this is highly desirable as good natural surveillance is more of a deterrent than active systems.

Emirates Palace Hotel

Context

The Emirates Palace Hotel is one of the world's most distinguished hotels and is one of Abu Dhabi's most celebrated iconic structures.

It is frequented by world leaders, celebrities and other members of elite society and regularly hosts significant special events such as the 31st GCC summit and Queen Elizabeth II's 2011 State Visit. As a result, protective security was a key planning and design requirement.

The Emirates Palace Hotel in Abu Dhabi exemplifies a number of the safety and security planning and design interventions outlined in the Manual. Elements of the hotel's physical security programme are apparent to the public and are captured in this case study to illustrate how protective security can be achieved in balance with aesthetics and function. Their visibility acts as a deterrent, as much as to detect, delay and deny intruders.

Principles and Toolkit in Practice

The Emirates Palace security operation has employed an exemplar physical security programme across the site that is holistic and balanced. Key strategies that are transparent from the public domain include:

- Scalable multi-layer defence system to respond to a change in threat or to accommodate a special event;

- Deployment of HVM measures to protect against vehicle borne attack.

Stand-off

The Emirates Palace Hotel benefits from a large open site. The size and layout of the development helps manage the risk of VBIED attack by providing sufficient stand-off between the hotel and plot boundary.

Topography

The topography of the development contributes to HVM by offsetting approaches to the hotel and to naturally reduce the speed of advancing vehicles. It also contributes to crime prevention by enhancing natural surveillance.

Movement Framework

The development has a well-defined movement framework plan for vehicles and pedestrians that benefits access control, wayfinding and traffic calming. Traffic is funnelled into the development through separated entry points that serve different functions and user groups.

Service Access Control

All deliveries for the development are processed through a dedicated on-site delivery reception area, located away from the hotel. The location provides sufficient stand-off between the facility and the hotel to help manage the risk of VBIED attack via a service vehicle.

On-site delivering reception area

Access Control Points

Vehicles and people are funnelled into the development through designated entry points which are actively monitored and controlled using a combination of physical and operational measures.

Each vehicle control point is fit-for-purpose to enable vehicle searching and entry or rejection based on the security operator's findings.

The actual control operation is scalable and designed to allow the security operator to quickly respond to change; lowering or raising the level of control based on threat or a special event.

Boundary Treatments

A wrought iron ornamental fence, designed for HVM, is applied around the development's boundary, with exception to the northern boundary. On this boundary, the maritime domain acts as a natural barrier while patrolling by CNIA vessels controls access to the marina.

The fencing creates a secure perimeter around the Emirates Palace and it is well-maintained and creates a good public image. The fence and urban design of the surrounding area promotes natural surveillance between the public realm and hotel grounds and prevents quick circumvention of the fence via tunnelling and climbing.

Adaptability

A number of physical solutions, all appropriate and proportionate, are employed in combination with natural barriers to define and enforce each layer. This helps achieve the development's security requirements while maintaining a welcoming and functional hotel operation.

Scalable physical solutions, like the active bollards and wedge pictured, are installed to enable access (when necessary) through each layer at a designated entry point. Permanent solutions like the perimeter fence and fixed bollards are employed to funnel traffic to the entry point.

Lowered operation

Heightened operation

Wasat Madinat Abu Dhabi (Sector E4-01)

Introduction

The Wasat Madinat Abu Dhabi (Sector E4-01) revitalisation project is featured as a case study in this document because it:

- Is a master plan project for an existing community;
- Demonstrates the value of integrated planning;
- Illustrates the benefits of applying the safety and security planning and design Principles in an existing environment;
- Is a large mixed use community in a downtown setting; and
- Shows signs of crime and misuse.

When tested against the Decision Support Tool, the project would be assigned a "Low Priority". As such, safety and security is important, but is unlikely to have significant influence on development proposals and counter terrorism is not a primary planning or design consideration.

This case study will provide evidence that the safety and security planning and design principles have been applied to this project and helped to improve community safety and security.

The Wasat Madinat revitalisation project is part of a wider revitalisation master planning initiative intended to help sustain the northern portion of Abu Dhabi Island as newer, significant master planned communities become available in and around the Island.

Context

The development is comprised of a dense population and a rich mix of uses; a few of which are not compatible. Certain groups of people are not active in the community because there is a lack of the right type of community facilities. Others are forced to misuse available space to sustain their interest, such as playing cricket in the car parks.

Pedestrian circulation across the development is not based on an effective movement framework plan and pedestrian routes are of poor quality. This offers little distinction between where a person should and should not walk, and people can be seen frequently using utility corridors to reach their destination. Consequently, some pedestrian routes are under used and more likely to experience misuse and crime.

The image of the existing environment is not positive and unlikely to instill a sense of ownership or encourage people to contribute to community safety and security.

Signs of misuse and crime are evident across the development but are predominately concentrated in areas that have no apparent purpose.
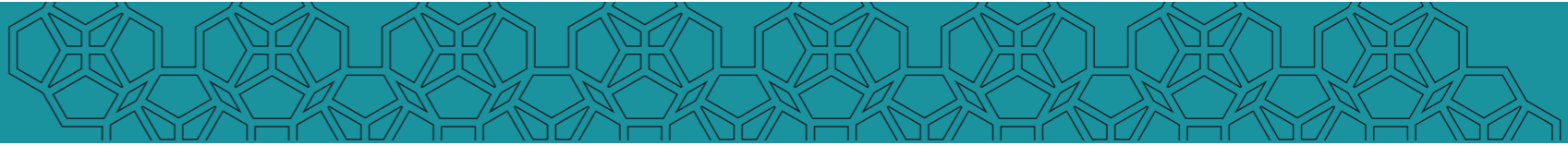
Key Problem Areas

Natural Surveillance

The space pictured has limited natural surveillance from the surrounding community, is poorly lit and is a long narrow pedestrian route.

Public Image

The cemetery wall shows strong evidence of crime and misuse.
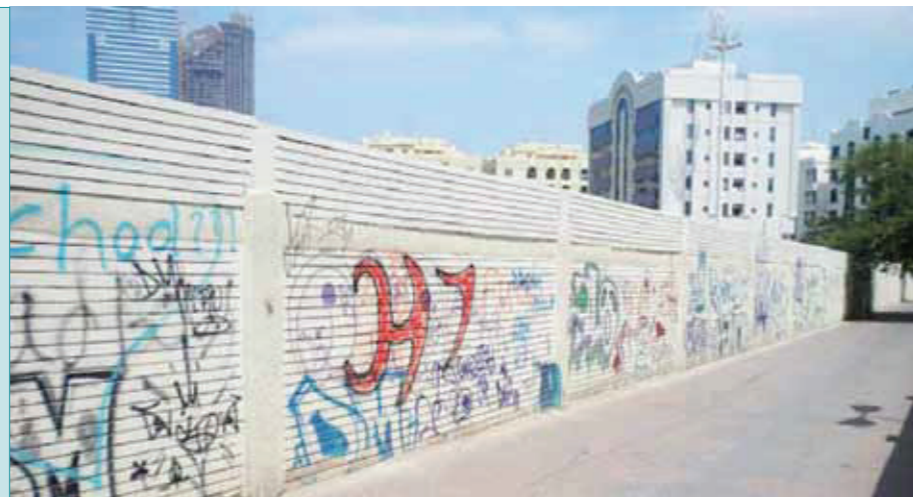
Ownership

This space has no defined purpose and as a result lacks ownership.

Process

The master plan was developed as part of an integrated planning and design process and the project was led by a multi-discipline team, including safety and security specialists.

The team was first briefed about the vision of the wider North Island revitalisation initiative, then carried out a site inspection to observe existing conditions that contribute to crime and misuse.

A planning and design charrette was hosted by the team to interview a number of local residents. Information obtained during the interviews was then cross analysed with the site inspection findings.

Once the project's safety and security needs were identified, the project team identified, explored and evaluated a number of planning options to ensure that the right concept was selected for further development.

The selected safety and security concepts were then integrated in the master plan alongside other planning objectives.

Multi-discipline planning and design charrette

Principles and Toolkit in Practice

Key elements of the project vision that are integrated into the master plan include:

- A public realm that expresses traditional Arab culture while serving the diverse, multicultural population;

- A broad array of community facilities within walking distance of most residents and businesses;

- Access to public transport options; and

- Efficient vehicular access and parking facilities

The master plan contributes to safety and security by:

- Introducing the right types of community facilities in the right places to balance activity across the development;

- Establishing a well defined movement framework that offers convenient movement between places while discouraging use of more private places;

- Improving the public realm to restore public image and compelling people to take an interest and become active in their community; contributing to community safety and security as observers; and

- Adopting designs that make it clear where public space ends and where communal, semi-private or private space begins.

Implementation

The master plan will be constructed over the course of many years.

"Quick wins" will be employed today to help improve areas that experience more crime and misuse. This will help establish a foundation for development as delivery continues in the future.

Quick win suggestions include:

- Additional tamper proof lighting; and

- Replacement of cemetery and school boundary walls.

1 Cemetery / School

Visually permeable fencing will replace existing walls around the cemeteries and school; improving natural surveillance. The plan also proposes to redevelop the school to include shared facilities with the community; this will help activate the area around the school and southern cemetery, and promote ownership.

2 Community Facilities

Parks and leisure areas are provided for the local community.

3 Public Realm

Existing space with no apparent purpose will, in many cases, be programmed as a series of new open spaces (i.e. linear parks, community parks, family parks, Meyadeen parks).

4 Parking

The development's parking requirement was addressed innovatively using a number of strategically placed parking structures, to limit surface parking. This was instrumental in freeing space to enable the introduction of more community facilities and open space across the development.

Saadiyat Island Cultural District
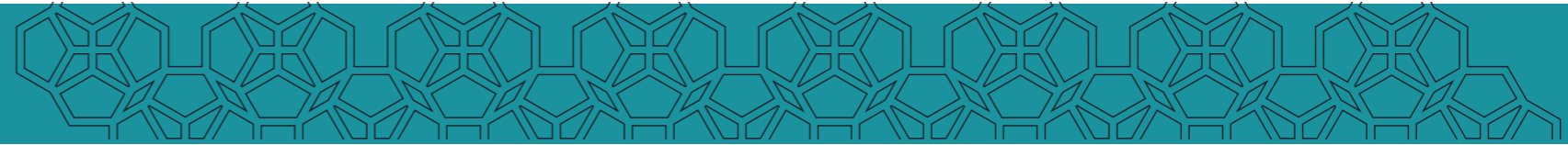
Introduction

The Saadiyat Island Cultural District Master Plan project is featured as a case study in this document because it:

- Is a new master plan that includes four high profile, iconic, cultural buildings requiring protective security;

- Demonstrates the advantages of early project engagement and integrated planning; and

- Illustrates the benefits of addressing safety and security requirements using the tools presented in this Manual.

Context

The development is predominantly mixed use but will be home to the Zayed National Museum (ZNM), Louvre Abu Dhabi (LAD), Guggenheim Abu Dhabi (GAD) and Performing Arts Centre. Each museum is considered a crowded place and will require protection against terrorism and specific types of crime, particularly art theft.

Co-location of the four museums is an example of clustering buildings of similar risk profile.

The Cultural District on Saadiyat Island is to be devoted to culture and the arts. It aims to be a centre for global culture drawing local, regional and international visitors with unique exhibitions, collections and performances at iconic institutions housed in buildings, which constitute a statement of the finest architecture.

The Louvre Abu Dhabi

The Cultural District

The Zayed National Museum

The Guggenheim Abu Dhabi

The Performing Arts Centre

The Process

An integrated development process was adopted by the Tourist Development Investment Company (TDIC). This approach was successful for several key reasons:

- Security was identified by the client as a primary planning and design requirement;

- A safety and security specialist was included as part of the multi-disciplinary team in the earliest stages of planning to help identify and balance requirements for the project;

- The project adopted a risk based approach to identify and address safety and security needs;

- Early involvement enabled each design team to achieve the security objective through very different, innovative solutions;

- The master plan resulted in a significant reduction in risk through planning and design; and

- Security requirements were achieved without negatively impacting on aesthetics or function.

This process resulted in the following five solutions:

1. Realignment of the canal
2. Maritime boundary treatment
3. Remote logistics delivery
4. Pedestrian screening
5. Movement framework enhancements

Cultural District, Saadiyat Island

Solution 1:
Realignment of the Canal

The canal was realigned and the ZNM relocated to create a natural protective barrier around the museums. This natural barrier was later supplemented by the deployment of HVM measures at the bridge locations crossing the canal, which will enable the establishment of a security zone during times of heightened threat or special events.

Original canal layout

Modified canal layout

Distinct security zone
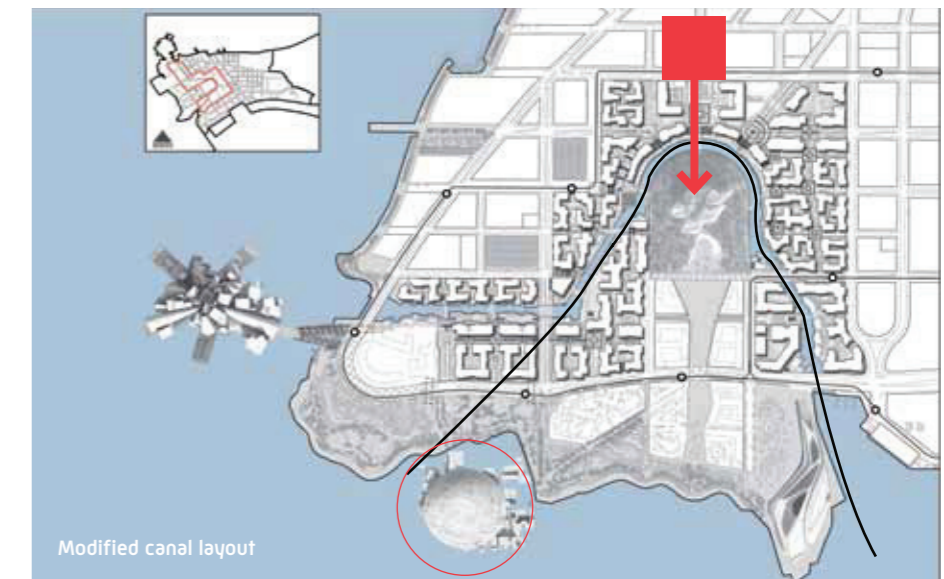
Solution 2:
Maritime Boundary Treatment

Both the LAD and GAD have extensive maritime boundaries that make them vulnerable to boat borne terrorist attack and high value art theft. The security requirement to achieve maritime denial and access control was achieved through two different but equally innovative solutions.

Museum maritime boundaries
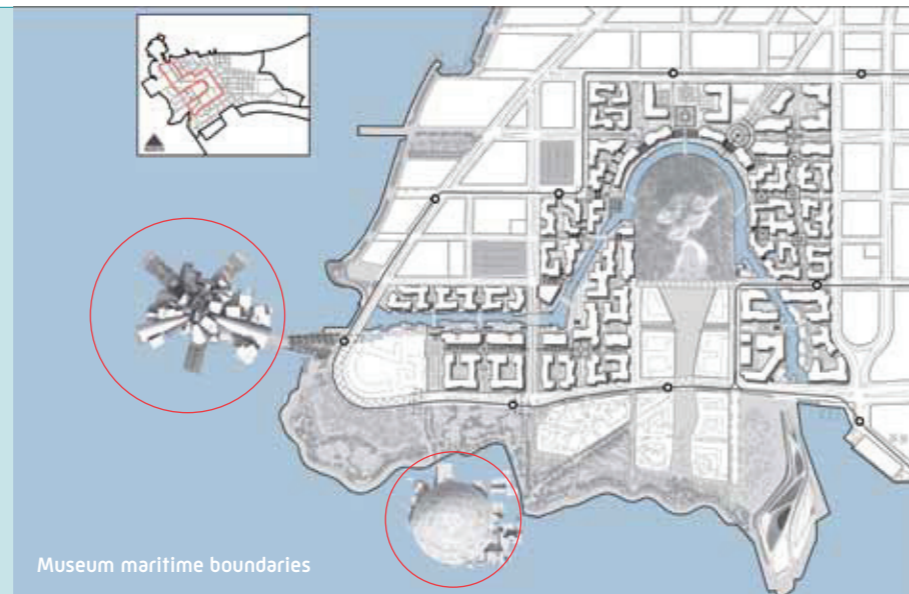
The LAD design team achieved maritime access control through the development of a concept based on Venetian piles. The piles of different heights and sizes were reinforced to security specifications, and deployed in an apparently random pattern of layers to prevent an unappealing 'stockade perimeter'.

Louvre Abu Dhabi 'Venetian pile design'
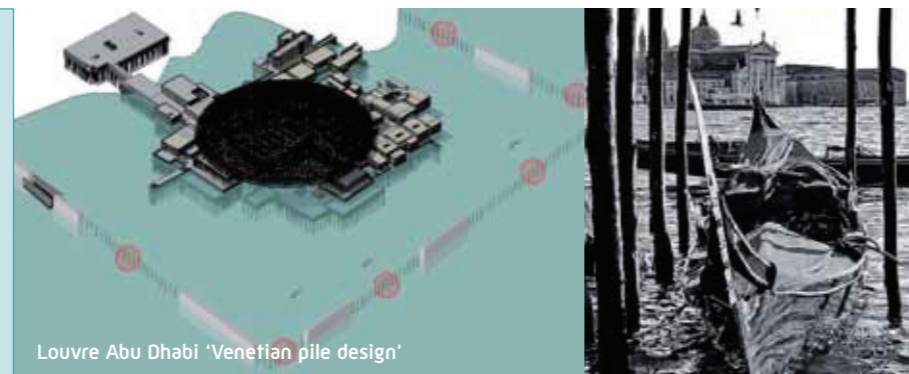
The GAD design team achieved maritime access control through the incorporation of the security requirement into the design of their wave attenuation barriers. The specification and alignment of the barriers was amended to satisfy both requirements. In addition the large platforms surrounding the museum served a dual purpose, providing a secondary layer to keep vessels away from the museum facade, while enabling visitors to walk around the outside of the museum.

Guggenheim Abu Dhabi combined wave attention and security barriers

Solution 3:
Remote Logistics Delivery

Delivery vehicles and loading bays present significant vulnerabilities in the design of a museum, potentially facilitating a terrorist attack in the form of large VBIEDs and providing a location for high value art theft. In order to address these risks, innovative solutions were developed for the three museums.

Remote logistic delivery Centres

A shared remote logistics system is to be incorporated into the design for the Museum Park between the LAD & GAD museums. This below grade facility will provide secure, dedicated delivery to the two museums, as well as providing below-grade public parking. This design greatly increases the level of deterrence and protection afforded to the museums, enabling vehicle exclusion zones to be maintained on each site.

Combined LAD and GAD museums logistic delivery centres below the Museum Park
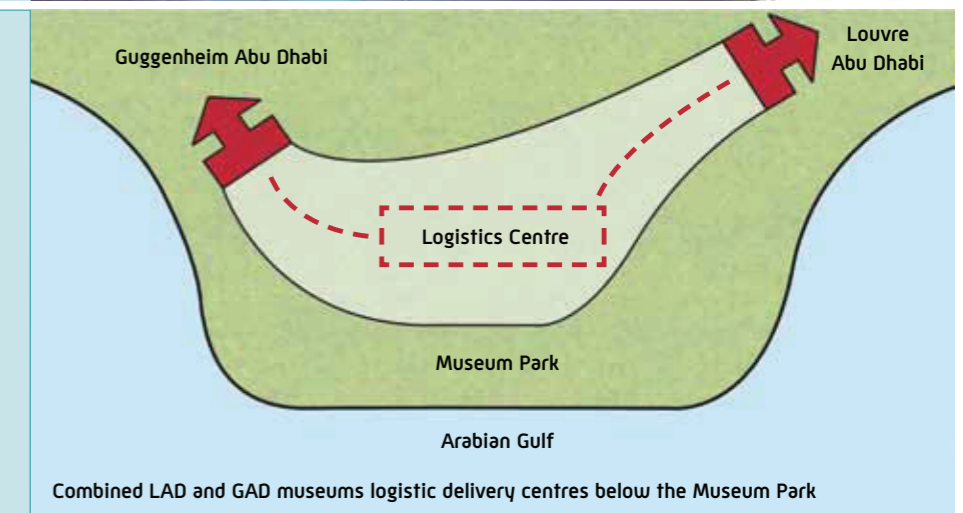
Deliveries for the ZNM are processed through a dedicated delivery reception area on the plot of the ZNM. The facility is located a considerable distance from the museum, with internal movement through tunnels on electric vehicles. This design also provides high levels of deterrence and protection and enables a vehicle exclusion zone at ground level to be enforced.

Proposed logistics delivery centre for the ZNM
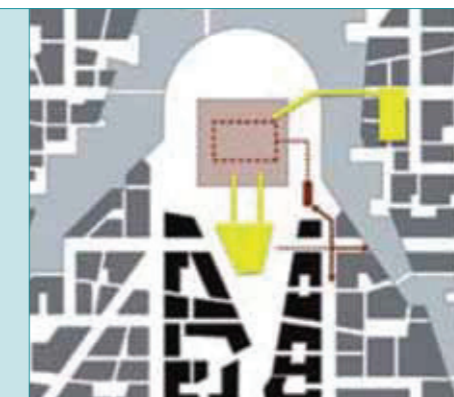
Solution 4:
Pedestrian Screening

The museums were directed to incorporate screening of visitors into their designs, to mitigate against terrorist attack (particularly PBIEDs and armed attack) as well as crimes such as armed robbery, theft and vandalism.

For the LAD, the screening locations were pushed to the extremities of the development area on the pedestrian approach bridges. These are located a considerable distance from the museum gallery and public spaces and independent of the main structures of the museum buildings.

Screening
Locations
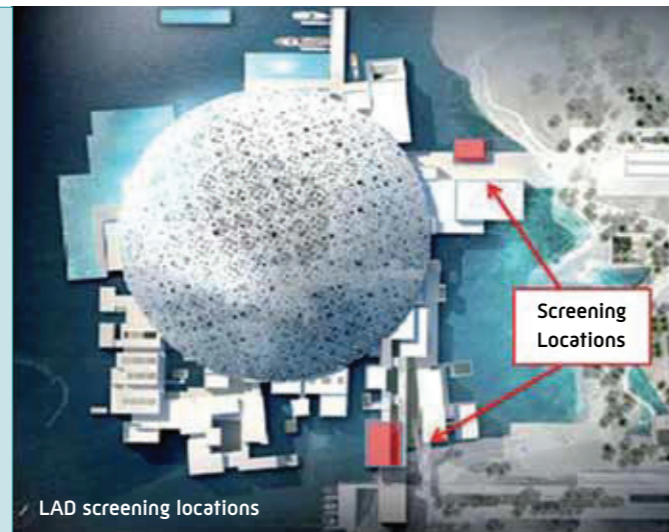
LAD screening locations

The GAD project team have created a security control point for pedestrian screening that achieves a high level of protection without impacting on the aesthetics of the museum entrance. During design the screening location was moved away from its initial location at the heart of the museum to its new position below grade, independent of the main structure.
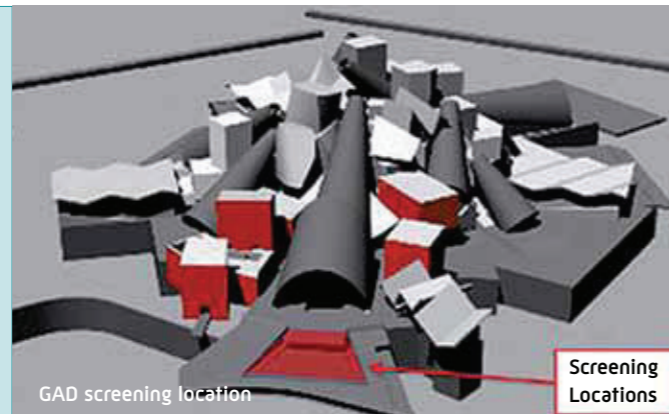
GAD screening location

Screening
Locations

Solution 5:
Movement Framework Enhancements

Main entrances present significant vulnerabilities in the design of a museum, being susceptible to both terrorism, in the form of large VBIEDs, and high value art theft, particularly armed robbery.

Several options for adapting the vehicle movement framework for the ZNM were considered, each offering differing levels of access control from vehicle inclusion through to exclusion schemes. An inclusion scheme was taken forward and the design team elected to close the approach road with access limited to a small number of invited users only.
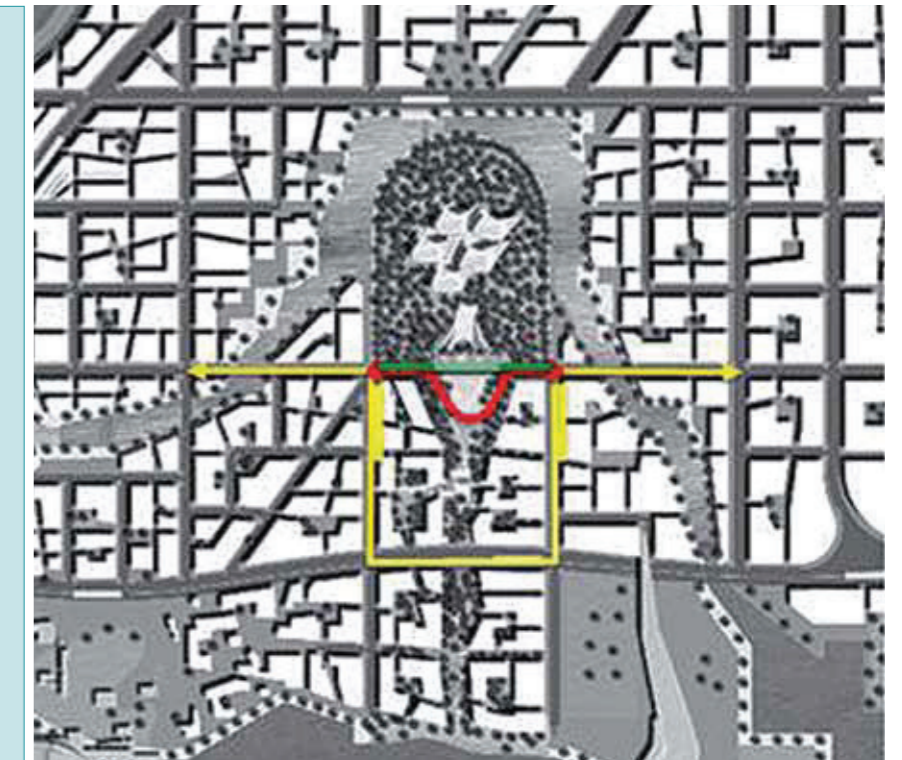
Vehicle access control options

Legend

Option 1:
Re-route traffic along the existing roads which run parallel to the garden

Option 2:
Flip the "U"shaped entry pathway to the south and divert the road around it

Option 3:
Drop the road below grade level as it passes the front of the museum

A1
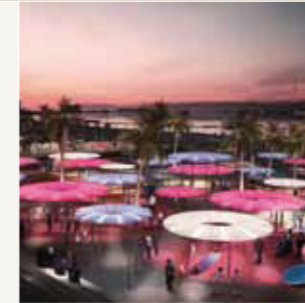
Risk Management

Introduction

This section of the Manual is not designed to be a definitive guide to safety and security risk management; there are many excellent standards and best practice documents that serve that purpose. Its purpose is to outline the fundamental elements of the risk management process and to set an expectation for the decision making process within a project. One of the key weaknesses in the safety and security development review process to date has been the quality of risk assessment documentation supporting planning applications. Therefore this section aims to inform planners and designers of what to expect from their consultants.

The Manual will be supported by a Decision Support Tool (DST) that will broadly determine if projects are Low Priority or High Priority. If assessed to be low priority, additional risk assessments will not be necessary as part of planning and design approvals process. Project teams will only be required to adhere to the Principles of the Manual. If assessed to be high priority, projects will be directed to complete a risk assessment. This should be conducted by a competent specialist and should follow the guidance given in this section. No specific methodology is mandated, however process and documentation must conform to an international recognised risk management standard, such as:

- ISO 31000 (2009) Risk Management – Principles and Guidelines;

- BS 31100 (2008) Risk Management – Code of Practice;

- HB 167 (2006) Security Risk Management

- HB436 (2004) Risk Management Guidelines; Companion to AS/NZS 4360: 2004; and

- FEMA Risk Management Series.

The various stages of the risk management process detailed below should be incorporated into the wider Integrated Development Process; it should form part of the main decision making process at each stage of the project. Ultimately, the identification, analysis and evaluation of risk will form the foundation for the treatment options, which will be developed in planning and design.

What is risk and risk management?

Risk is widely defined as the potential for a course of action or activity to result in an undesirable consequence (or a loss). Risk is inherent in everything we do, whether it be riding a bicycle, managing a project, dealing with clients, taking decisions about the future or deciding not to take any action at all. We manage risks continuously, sometimes consciously and sometimes without realizing it – deciding what to do and when to make sure life continues as smoothly as possible with as few unpleasant surprises as possible.

In a business context, risk should be directly linked to its impact on business objectives. This is an important definition because it exposes the increasing maturity in thinking about risk that has occurred over recent years.

Applying this approach within the safety and security discipline helps to move the focus of thinking away from threat alone to a wider consideration of safety and security risk.

The need to manage risk systematically applies to all organisations and individuals and to all functions and activities within an organisation. The alternative to risk management is risky management, or making reckless decisions, or decisions that are not based on a careful consideration of the facts. This is unlikely to result in a desired outcome. The need for sound and systematic risk management applies to the development process as much as any other business or industry.

Certain land uses, adjacencies and occupancies can result in the creation of safety and security risks. Equally, the type of business activity of a particular owner/tenant, or the people that work or visit that site, can result in additional risk. These risks can greatly impact on our daily quality of life. This fact is acknowledged in the UPC's vision to plan Abu Dhabi as a safe and secure environment that promotes quality of life, preserves local values and culture and contributes to economic sustainability and the overall welfare of the Emirate.

Many developers and users feel that crime and terrorism risks are the responsibility of others e.g. Governments, police. Many believe they cannot be controlled or treated by an individual. This is not always the case and it is incumbent on every project development, however large or small, to consider these risks, how they impact on people and their quality of life, and to ensure that they are appropriately addressed.

Often balancing risks is difficult as they share causal relationships and dependencies. Striking this balance is a challenge and requires a continual thought and decision making process. Within that context, different people all have different perceptions of, and attitudes towards risk. Some people actively seek adventure and take greater risks in their lives – participating in adventurous sports such as skydiving and mountaineering, where the chances of injury or even fatality are higher. Equally, others prefer to lead a more sedentary lifestyle, choosing not to take any more risks than absolutely necessary. The challenges of balancing risk and differing risk appetites are two of the key elements in project decision making.

Internationally, attitudes have changed significantly in recent times, with a major focus on, and acceptance of the need for, an increased attention to safety and security. In some instances this can be driven by misinformed perception, fuelled by an overly dramatic media. The result is that security investment may be misdirected to where the 'noise' is, not where it is really required. This not only applies in terms of risk but also in relation to 'favoured' treatments, such as a heavy reliance on the deployment of CCTV cameras. Therefore the project risk management process must assess and review information for its relevancy, accuracy and credibility to ensure that the process identifies the relevant risks and results in the implementation of the most effective solutions; in short it must enable appropriate decision making.

"Risk management is a more realistic term than safety. It implies that hazards are ever present, that they must be identified, analysed, evaluated and controlled or rationally accepted."

Jerome Lederer, Director of the Flight Safety Foundation for 20 years and NASA's first director of Manned Flight Safety, quoted in his 9 February 2004 obituary, the New York Times.

All risk methodologies require a systematic and rigorous process with clear stages, responsibilities and outcomes or deliverables.

The following diagram shows the fundamental stages of a general risk management process. Compatible with this, refined models have been developed for security risk management, such as that offered by HB167, as shown opposite:

Communicate and Consult

Establish the Context

Risk Assessment

Identify Risks

Analyse Risks

Evaluate Risks

Treat Risks

Monitor and Review

Communicate and Consult

Establish the Context

Strategic Context

Organisational context

Security risk management context

Threat Assessment

Vulnerability Assessment

Criticality Assessment

Identify the Risks

What? When? Where? How? Who?

Assess the Risks

Likelihood

Consequence

Evaluate the Risks

Tolerance

Acceptability

Treat the Risks

Avoid

Accept

Exploit

Share

Reduce

Monitor and Review

Communicate and consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

Establish the context

Establish the external, internal and safety and security risk management context, structure and activities in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the analysis defined.

Identify risks

Identify where, when, why and how events could prevent, degrade, delay or enhance the achievement of project/business objectives. In a security context this includes determining the threats, the assets under threat, the vulnerability of those elements to the threats identified and identifying specific events and scenarios

Analyse risks

Identify and evaluate existing controls if appropriate. Determining the consequence should the risk be realised and the likelihood of such a risk with that consequence occurring. Defining a level of risk based on a combination of consequence and likelihood.

Evaluate risks

Compare estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. Determining the tolerance to identified risks. Enable decisions to be made about the extent and nature of treatments required and about priorities.

Treat risks

Develop recommendations and implement specific cost-effective strategies for the treatment of priority risks. Assign accountabilities, responsibilities and budget for risk treatment activities. Analyse and evaluate residual risk.

Monitor and review

It is necessary to monitor the effectiveness of all steps of the risk management process. Monitoring of the external and internal security environments to detect change. Reviewing of the risks and their treatment strategies for effectiveness and efficiency.

Fundamentally, safety and security risk management requires those involved to have a thorough understanding of the principles and practice of risk management as well as a thorough understanding of safety and security.

The process of mitigating risk is part of a continuous and ongoing process throughout the lifecycle of the planning, design, construction, commissioning, occupation and operation of the building. Planners and designers play an important role at the beginning of this process and should think innovatively to remove vulnerabilities whenever an opportunity arises.

Although this process commences at the earliest stages of planning it must consider the lifecycle of the project. Key requirements for the process are

- Long term strategic planning;
- Holistic approach;
- Performance criteria; and
- Risk focus.

Within planning and design, the objective of risk management is to reduce safety and security risks to an appropriate level, while balancing them with other planning and design objectives. Risk management solutions should satisfy the risk appetites of both the development owner (client) and any Government stakeholders.

"Risk management does not mean finding 100 safeguards that are missing and drumming up a $1million budget to address them all. Risk management means making informed decisions about which risks to mitigate and which risks to accept"

A White Paper for Health Care Professionals, HIPAA Security Risk Analysis and Risk management Methodology, 2010

"From a practical perspective, what one ultimately seeks to develop by completing a risk analysis is a prioritised list of security risks that need to be addressed with a risk mitigation action based on an informed decision"

A White Paper for Health Care Professionals, HIPAA Security Risk Analysis and Risk management Methodology, 2010

Like the wider development process, risk management also requires effective communication and consultation throughout. Effective internal and external communication is important to ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and why particular actions are required.

Effective communication and consultation will improve participants' understanding of risks, ensure that the varied views of stakeholders are considered and ensure that all participants are aware of their roles and responsibilities. It is vital in 'getting buy-in' from stakeholders and should begin at the earliest stages of the security risk management process.

Communication and consultation should focus on engagement, participation, information transfer between parties, the perceptions of individual parties involved, comprehensiveness and clarity of information for making decisions and agreement between the parties involved on the expected deliverables.

Establishing the context is the principal activity in developing the scope for safety and security risk management. This includes establishing both the internal and external context of the development as well as the safety and security risk management context (objectives, structure, processes, structure, stakeholders).

External Context
The term 'external context' refers to gaining an understanding of the external environment in which the organisation is operating or may be operating in the future.

The key objective is to identify factors in the external environment that are going to have an effect on the organisation, the manner in which it does business and ultimately, those factors that will have safety and security risk implications for the organisation. It is necessary to place some boundaries on the exercise to ensure that it remains relevant to the risk management objectives for the planning and design process.

Internal Context
The focus of developing the internal context is to create an agreed understanding of the organisation's internal environment and issues that may influence the nature of the safety and security risk exposures. The key elements of the internal context and areas around which questions should be posed in its establishment include:

- The organisation's objectives, plans and strategies;

- Key business functions and processes;

- The type, extent and interaction of operations;

- Historical crisis, disruption, disaster, emergency, safety and security incidents and trend information;

- Locations of business sites, accommodation, and other operations;

- Internal hazard locations (e.g. dangerous goods storage); and

- Presence of 'sensitive targets' (e.g. high profile individuals, sensitive information, attractive assets, business critical assets and cash).

Risk identification is concerned with creating a well thought out and comprehensive determination of the sources of risks and potential events that will have an impact upon the individual's, organisation's, or community's objectives. In the safety and security context, identification of risk normally involves the consideration of threat, asset criticality and vulnerability assessment as primary inputs into the identification process.

The words 'threat' and 'risk' are often used interchangeably. However, risk is not a synonym of threat, although closely related, the two are significantly different. In many circumstances a 'threat' will provide a source for one or more risks. It is the interaction between the threat and someone or something, at a particular instance or over a period of time that will create the risk. Threats may exist, but not pose a risk. For example, a protestor/activist may present a threat. However, the risk only emerges if there is some chance (no matter how small) that the threat will interact with something (structure, person, etc) to cause an event resulting in certain consequences (unauthorised entry, assault, criminal damage, vandalism).

THREAT is a function of Capability and Intent

In undertaking risk identification, a list of risks should be developed by considering the following questions :

- How it could happen (a source of risk – for example a potential threat)?

- Why it could happen (a cause: actions, incidents or other underlying factors that create the source of risk)?

- What could happen (a potential event or incident, where the source of risk interacts with some aspect of the entity with an associated consequence)?

- Where it could happen (the physical locations and assets where the event could occur or where the consequences may be experienced)?

- When it could happen (specific times or time periods when the event is most likely to occur or the consequences realized)

- Who could be involved (individuals or groups that may be associated with the threat or may impacted by the risk)?

Identifying risk is therefore about understanding the nature of the threat (the source of the risk), interacting with important elements such as the community, development assets, etc (with importance expressed through criticality) and in what manner the nature of these elements will facilitate or inhibit this interaction (expressed through vulnerability).

RISK is a function of Threat and Vulnerability

The full identification of safety and security risks normally involves separate processes:

- The Criticality Assessment – 'what' and 'where' answers;

- The Threat Assessment – 'who', 'why' and 'when' answers; and

- The Vulnerability Assessment – 'how' answers.

Information to support these processes can be gained from a wide range of sources including:

- Organisational loss and incident data;

- Local incident/crime data;

- Industry/Sector loss and incident data;

- Open source information: media, internet, public reports;

- Intelligence assessments (from national security agencies, industry associations etc); and

- Comparative analysis with other organisations or developments that may have similarities in size, character, operations and locations.

Asset and Criticality
The criticality assessment (or 'asset assessment'), involves the identification of the critical assets (people, property, information and the processes that support them) that may be exposed to, or harmed by the threat. The criticality assessment is a vital step in the identification of risk as it provides the starting point for a consideration of the pertinent threats, and the development's or individual user's vulnerability to those threats. In many circumstances it would be difficult and costly to conduct a thorough risk assessment for all assets, locations and people.

The criticality assessment should focus on those assets that are of most importance to the development, community or individual.

Threat
The aim of the threat assessment is to clearly identify the range of potential threats arising from the external and internal security environments, and their relevance to the development. The threat assessment is concerned with identifying those events, aggressors or adversaries that can cause losses to the development, organisational, or individual assets (as identified in the criticality assessment above).

Intentional threats, which are based on the notion of an attacker or adversary, include an assessment of the intent and capability of an individual or group to undertake actions that will result in harm or the expectation of harm to another individual, group, organisation or community.

This includes:

- identifying the range of potential threats to an individual, organisation or community;

- examining the possible ways in which these threats may interact with the critical asset, either directly or indirectly, and understanding the specific impacts that could arise; and

- determining how likely these threats are to occur within a defined time frame or locality.

Intent and Capability

Threat is often expressed as a function of intent and capability. Intent is represented by the expressed aims, objectives, desires, or directions of the threat and includes the motivational factors for such individuals or groups. Capability considers factors such as skills, experience, resources, numbers of attackers, supporting networks and their overall ability to conduct criminal or terrorist operations. As assessment of intent considers the question "will they attack" while capability considers the question of 'how effective will they be if they do attack".

Threat assessments can range from quite general to very specific, depending on the level of information available. Within the development context, where information is limited, particularly during the earlier stages, assessments are more likely to veer towards the general scale, providing general threat levels against types of land use, industries or tenants.

If possible, the threat assessment should culminate in the development of a range of credible threat scenarios or Design Basis Threats (DBT'S). These express more specifically how the threat is likely to manifest. For example while assessments may identify a general threat from terrorism, it is more helpful, particularly in the planning and design process, for a range of DBTs to be considered e.g. a large Vehicle Borne Improvised Explosive Device, a Person Borne Improvised Explosive Device and a Coordinated Small Arms Attack. This helps project teams to better understand how the threat may apply to the development and what the vulnerabilities are; this in turn can be used to inform a more specific treatment plan. These scenarios should be based on historical trend data, previous incidents, intelligence (from local police crime advice/intelligence).

Specific Threat — Hotels — Abu Dhabi — UAE — UK, USA, France — Tourists — General Threat

Assessing Vulnerability

The first step in the vulnerability analysis considers how each of the credible threats can be realised against each of the critical assets. This involves determining two elements:

- How a successful 'attack' against the asset could be carried out (based on the DBTs); and

- The effectiveness of each of the layers of defence in preventing this event from happening.

Many safety and security controls will exist in a 'layered' or 'defence in depth' structure. No matter how many layers are in place or how well constructed they are, they cannot be one hundred percent effective for one hundred percent of the time. Borrowing a safety model developed by James Reason, each of the layers of security controls or countermeasures) will resemble a slice of Swiss cheese, with holes of varying number and size through it. Under normal circumstances the holes are covered by subsequent layers of controls. However, under certain circumstances the holes in all layers will line up and all defences can be penetrated. The aim of the vulnerability analysis must not only be to identify and characterise holes in each of the layers; it must also consider the potential for these holes to align.

Deter   Detect   Delay   Respond Recover
———— The Attack ————

This vulnerability model is of less value in the early planning stages of the IDP, when security controls have yet to be considered. Therefore vulnerability is more likely to consider 'generic' vulnerabilities associated with certain land uses and building types. However this model is useful when considering the treatment of risks in order to determine how many layers of defence are required and what should be in each layer. Best practice would dictate that the higher the risk, the more layers are required and the more robust each layer should be.

Summary
For the identification of risks, it is necessary for all of the above elements to be combined.

Threat
Who or what will potentially cause harm (informed by the threat assessment).

Asset
What site, area, person, entity, process, or other assets will be affected (informed by the criticality assessment).

Vulnerability
What controls or other operational parameters could be exploited (informed by the vulnerability assessment).

Event
In what manner or circumstances will the harm be realized (informed by considering threat, asset and vulnerability).

For example, the following description may be useful: 'there is a risk that terrorists could deliver a large VBIED in a private car to the porte corchere of the hotel, resulting in considerable damage, fatalities and injuries to guests and staff.
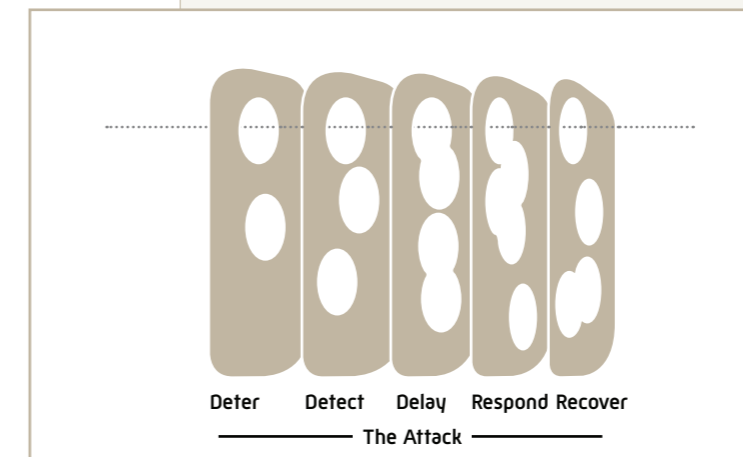
Risk analysis should provide decision makers with sufficient information to make an informed decision on the need for increasing or decreasing the investment being made for protection across the spectrum of assets under consideration. The risk analysis involves the consideration of the risk description, developed in the previous identification step, along with the combined outputs of those analyses (threat, criticality, and vulnerability analyses) that contributed to its formulation. The risk analysis should examine how these factors interact to determine an overall level of risk through a consideration of the consequences of the event occurring combined with the likelihood of the event with that consequence. These risks should be prioritised so that project teams can readily identify which risks require the greatest level of consideration during planning and design and ultimately, how much 'weight' will be afforded to them as 'design drivers'.

Methodologies

Many methodologies exist, quantitative versus qualitative, subjective versus objective, some are general while others are very detailed in their approach. No single approach is regarded as absolutely correct or wrong, all models have implicit flaws to a larger or lesser extent. Also methodologies should not be rejected out of hand because they appear to be overly simplistic. Some highly sophisticated and complex mathematical models can, depending upon the context, be of less utility than much simpler models.

However it is important that a known methodology is identified and followed. In the IDP context, particularly during the early planning and design stages, little information is known and therefore detailed analysis may not be possible. Equally specific analysis may not be necessary – the primary aim of the risk analysis should be to inform planning and design decision making.

A sensible approach

A security consultancy working for a major developer delivered an 'all hazard' risk analysis that applied all threats to a full range of assets. The formulaic approach allocated a numerical value for threat, vulnerability and consequence with additional weighting factors to create overall numerical risk values. The process resulted in 2350 individual risk scenarios of largely irrelevant or inappropriate analysis – such as the 'risk of storm surge to a cash point' and 'solar radiation against a road'. The complicated and long-winded process failed in its primary objective – which was to inform the development process and facilitate security decision making.
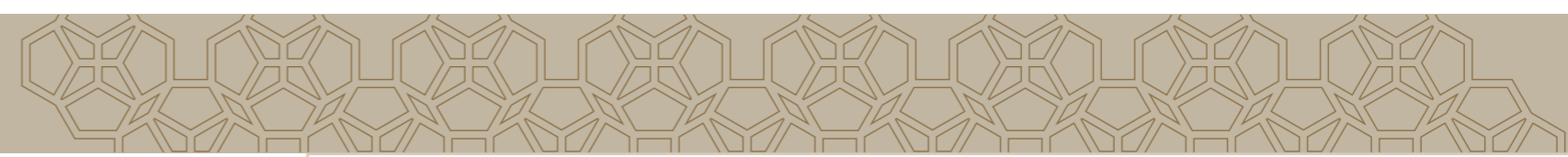
Example Criteria

Likelihood	Criteria
Almost Certain	• Over 99% Probability, or • 'Happens often', or • Could occur within 'days to weeks'
Likely	• >50% Probability, or • 'Could easily happen', or • Could occur within 'weeks to months'
Possible	• >10% Probability, or • 'Could happen, has occurred before', or • Could occur within 'a year or so'
Unlikely	• >1% Probability, or • 'Has not happened yet, but could, or • Could occur 'after several years'
Rare	• >1% Probability • 'Conceivable but only in extreme circumstances' • Exceptionally unlikely, even in the long term future • a '100 year event' or greater

Risk analysis requires a careful consideration of both likelihood and consequence. The likelihood refers to the chance or probability of an incident or event. The likelihood can be estimated as an absolute probability (e.g. occurring with a probability of between 0 and 1), as a percentage chance of occurrence, as the chance that something will occur over a defined period (e.g. 'over the next two years') or as a general statement of likelihood (e.g. certain, unlikely).

The consequence of safety and security risks can usually be expressed as a measure of financial loss, stakeholder/community impact, reputational damage, loss of operational capability, or health and safety implications. Impacts derived as part of the criticality assessment are used to inform the determination of overall risk consequence. Care should be taken to consider the indirect consequences, such as loss of reputation, loss of revenue during recovery and so on.

Consequence Rating	Financial Rating (AED)	Reputational Rating	Project/Business Rating
Catastrophic	>350,000,000.00	Extreme negative coverage causing public outcry appearing consistently over weeks Majority of stakeholders severely disadvantaged (months)	Serious process breakdown that prevents the achievement of mission official objectives Multiple severe injuries, including fatalities
Major	>20,000,000.00 <350,000,000.00	Negative significant coverage, appearing consistently over weeks Multiple stakeholders severely disadvantaged (weeks-months)	Serious process breakdown that substantially impedes the achievement of a core objective Multiple severe injuries, or a single fatality
Moderate	>200,000.00 <20,000,000.00	Negative coverage lasting for several days, and/or frequent occurrence for several weeks Multiple stakeholders experience significant disadvantage (weeks)	Process breakdown that impedes the achievement of an important objective or causes extensive inefficiencies in key processes Multiple casualties requiring hospital attention
Minor	>8,000.00 <200,000.00	Minor negative coverage, limited circulation for one day Minority stakeholders experience disadvantage (days-weeks)	Process breakdown that impedes the achievement of one or more objectives or some inefficiencies in key processes Minor injuries requiring hospital attention
Minimal	<8,000.00	Isolated brief coverage, single media outlet Stakeholders experience minimal disadvantage (days)	Process breakdown or inefficiencies that have a limited impact on the achievement of an objective Minor injury requiring first aid only

Small losses rarely present a problem to an organisation unless the frequency becomes so high that their aggregate effect approaches that of a single medium loss. However, large losses present the most serious problem; they rarely happen but if realised, the impact could be catastrophic.

There are two concerns about focusing on such risks. Firstly, the obvious danger is that the far more likely lower consequence events can be missed or given insufficient attention.

Secondly, there is also an inherent difficulty in conceptualising these low likelihood high consequence events. By their very nature they are outside of the experience of the majority of people, they are difficult to subjectively analyse and should they occur, they can rapidly overwhelm most coping mechanisms. Human perception being what it is, these types of events either receive unwarranted attention or fall outside of usual consideration processes.

"There is evidence to indicate that we are generally not very effective at responding to low probability high impact risks such as terrorism, until it is too late".

Then, S.K. and Loosemore, M. (2006), Terrorism Prevention, Preparedness, and Response in Built Facilities. Facilities Journal, Volume 24, Number 5/6, pp 157–176, Sydney Australia: Faculty of the Built Environment, University of New South Wales.

Most Credible Worst Case Scenario

In safety and security risk assessments (particularly when focused on national security issues) the consequence of the worst case scenario is often adopted. The ultimate worst case scenario of any safety and security risk could potentially be a catastrophic loss to any project, organisation or community, involving mass fatalities and destruction. However, such extreme worst case scenarios are not those that are experienced by the vast majority of organisations that are the victims of such security incidents. Instead it may be more prudent to consider the concept of **'most credible worst case scenario'**, which introduces a degree of practicality and plausibility into the analysis.

For example in a worst case scenario, a small bump of the head could result in delayed concussion later whilst driving, causing a serious road accident involving multiple vehicles, resulting in a significant number of fatalities and injuries. The most credible worst case would result in the victim suffering concussion possibly requiring hospital treatment. Therefore, it is usually appropriate in looking at high consequence (and usually low likelihood) events to use available historical precedent to determine realistic worst case losses that could be expected from a particular risk (hence the 'most credible' scenario). For both crime and terrorism related risks, a large database of previous incidents is available to determine realistic consequences.

Overall Risk Rating

The overall level of risk or 'risk rating' is determined through combining the consequence and likelihood estimations. The example table right, provides one example of a matrix approach for estimating a risk rating. Risk rating in this manner allows the risks to be prioritised in order of decreasing relative risk level from 'Extreme' to 'Low'. It also provides an aid to decision making regarding the tolerability of risk which is determined during risk evaluation.

Scales and formula
A cautionary note on the use of scales in the measurement of risk:

A number of methodologies attempt to perform feats of quantitative analysis that are mathematically unsound, because of the very nature of the rating scales that they are trying to use. There are certain mathematical things that you just cannot do with certain types of scales. For example, ordinal scales, where data is sorted into comparative scales ('High', 'Medium' and 'Low' or where numbers – 1,2, 3,4,5 etc – are assigned for relativity but not magnitude) mathematical treatment is likely to be arbitrary in the absence of zero points. With the interval scale, where there is a constant interval between numbers (but where the zero point may be arbitrary) for example the Fahrenheit temperature scale: numbers can be added and subtracted but cannot be multiplied/divided: e.g. 20°F is not twice as hot as 10°F.

Example Table

	Consequence				
	Minimal	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	Significant	High	Extreme	Extreme
Likely	Medium	Medium	Significant	High	Extreme
Possible	Low	Medium	Significant	High	High
Unlikely	Low	Low	Medium	Significant	High
Rare	Low	Low	Medium	Significant	Significant

(Likelihood — row label for left axis)

"Remember, there are just some things you cannot do with some types of scales, If you do, the products could be nothing short of nonsense".

HB 167 (2006) Security Risk Management

The 4 Ts:
Terminate
Transfer
Treat
Tolerate

The crux of risk management is this forth stage in the process, the decision making related to the identified and analysed risks. The aim of risk planning is to select and implement measures to minimise the expected loss by either reducing the likelihood, impact or both. However some risk will always remain, especially with intentional risks such as terrorism, which cannot be totally eliminated. This is a critical message to consider during the development of the built environment, in particular for developments such as hotels and tourist destinations, where the standard 'defence in depth' model with multiple layers of robust security cannot be adopted.

The 4 Ts
It is widely accepted in the risk management discipline that there are four 'options' available for reducing identified risks, sometimes referred to as the 4 Ts:

Terminate
Eliminate, withdraw from or not become involved in an activity associated with the risk e.g. prevention of personal safety risk by not undertaking overseas travel to a specific location at that time. In a development context this is rarely achievable, although relocation should be considered if the risks are assessed to be very high and treatment makes the project less financially viable.

Transfer
Share, outsource or insure the risk, e.g. request that a Government agency deals with the risk, especially during high profile, international events. In reality only part of the responsibility for managing the risk can be transferred, some responsibility and all accountability for the risk remains with the first party.

Treat
Mitigate the risk, e.g. install protective security measures such as HVM barriers (this is the main focus of the Safety and Security Planning and Design Toolkit).

Tolerate
Accept and plan for risk occurring e.g. allow vehicles into a development but ensure that emergency vehicles can respond effectively to any incident. If this option is chosen then stakeholder agreement needs to be sought and the level of residual risk (the remaining risk that has not been treated) carried over into later stages of the project must be clearly articulated.

Security risk decision making will depend on the project evaluation criteria, which may vary depending upon a range of factors including:

- Prevailing political, stakeholder or community sensitivities and expectations;
- The nature or types of the incident involved;
- Existing or emerging incident trends;
- Strategic or business priorities;
- Resource availability for treatment and other project planning and design constraints; and
- The ability of the organisation, community or individual to absorb losses.

Decisions on the tolerability of risk can be based upon straightforward decision criteria that divide risks that require treatment (intolerable) from those that do not (tolerable) e.g. any risk with potential safety or reputational consequences above 'Moderate' is intolerable. In reality, tolerance is more likely to be exhibited as a gradient, where the risk may become increasingly less tolerable as the risk level is elevated and where a range of other contextual factors, such as a decreasing capacity to manage the risk will influence the decision on risk tolerance. This degree of flexibility is particularly relevant to development projects, where the application of additional layers of defense may inhibit other design opportunities, which may be unacceptable for lower risks.

Therefore the decision may focus not so much on whether to treat/not treat but rather it will focus on how much safety and security to put in and at what stage of the project cycle.

The decision making will certainly require consultation and agreement with all relevant stakeholders. In early planning this decision is particularly difficult as information is incomplete. However developers should look to reduce the risk through planning and design where possible; treatment measures should be proportionate and appropriate. These decisions should be captured in the project safety and security brief, which should identify the priority risks to be treated, the overall approach to deciding how those risks are to be treated, as well as highlighting those risks that are to be tolerated.
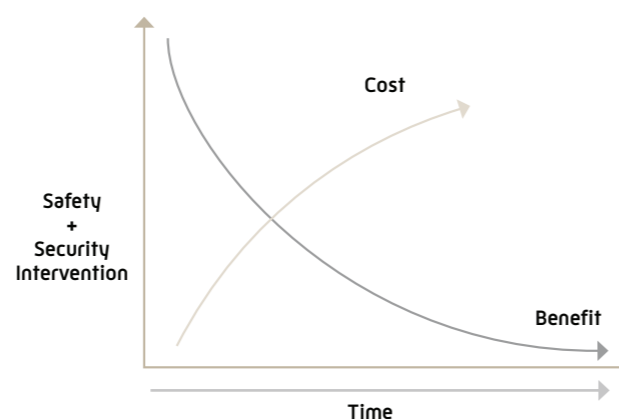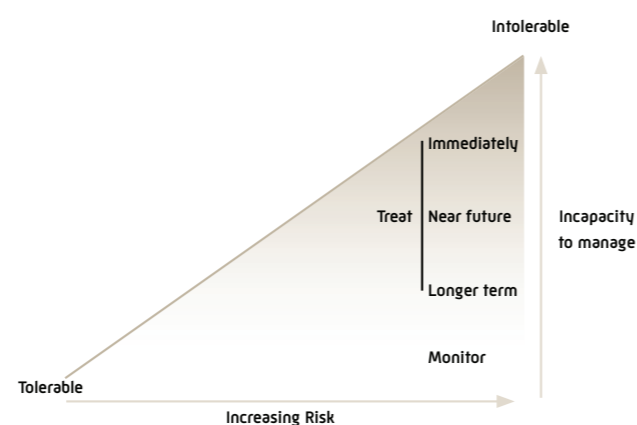
While reducing risks later through operations is a sensible option, developers should avoid the easy and cheaper option of passing the responsibility for risk treatment to later in the project life cycle – risks should be treated as early as possible and where the measures can be most appropriate and effective.

Where a security risk has been determined as intolerable (during the risk evaluation stage), some form of treatment will be required to manage the risk. It will never be possible to completely remove risk. The aim is to manage the level of risk to a tolerable level. Such treatment will usually involve some form of improvements to controls already in place, or the introduction of new controls.

In the safety and security environment, risk treatment often results in an unhealthy focus on one particular mitigation to the exclusion of other types of control measure e.g. an over reliance on technology such as CCTV, or conversely, an over reliance on purely physical measures. As part of the IDP, it will be necessary to offer a balanced and holistic solution, applying the most appropriate and effective package of measures at the most appropriate stage of the project life cycle. Also, projects should be able to show a direct link between the measures being proposed and the vulnerabilities that are being addressed to lower the level of risk. As the development process is iterative, it would be appropriate for projects to discuss options for the treatment of these key vulnerabilities, which should be accompanied by an assessment of safety and security and cost benefit, as well as the impact of introducing the measure on other project disciplines.

Safety and security can be an emotive subject as invariably parts of a development or some buildings will not receive as much treatment as others. It is not possible to protect all assets against all plausible threats. They must therefore be prioritised to maintain a balance between competing planning and design objectives.

Risk treatment is the main focus of the Manual, in particular reducing the vulnerabilities within the project plan and design. The Planning Toolkit and Design Toolkit include a suite of guidance to reduce these vulnerabilities and consequences. The approach of reducing the risk will vary depending on project opportunities, constraints and level of risks, however the focus should be on the innovative use of planning to minimise safety and security risks. Throughout the design process, projects should also seek innovative solutions, such as landscaping, street furniture, and public, art before resorting to standard security treatment options.

"There is no such thing as zero risk"

"Rarely it is possible to protect all assets against all plausible threats."

The safety and security risk environment is not constant. Organisations, communities and individuals are also in continual flux, sometimes discretely, often dramatically over short periods of time. Perhaps more importantly in the IDP, the project environment is extremely dynamic, with continual changes in plans and designs that all have an impact on risk. Monitoring of risk provides the capability to respond effectively to these changing environments. Far too many risk management activities finish with the monitor and review step – it is a continuing cycle, and should be completed at each and every step of the project process.

In particular, the concept of 'monitor and review' requires project teams to:

- Continuously examine the external and internal environments and reconsider the context and its effect on safety and security risk management;

- Redevelop the analytical outputs of the safety and security risk management process to reflect the changing context;

- Assess the efficiency and effectiveness of treatment plans in mitigating the risks identified; and

- Re-evaluate the appropriateness of treatment activities to manage a dynamically changing risk and project environment, including changes in the plan or design and value engineering exercises.

IDP

The Integrated Development Process (IDP) is a continuous, iterative process. Equally, the safety and security risk management process is dynamic and cyclical in nature. While these two processes are completed in parallel, they also need to interface and interact regularly. This is primarily achieved through the involvement of the safety and security specialist, who constantly updates the assessment and treatment plan as the plan and design unfolds.

It is the role of the safety and security specialist to ensure that a risk management process is adhered to and the following requirements are met at each stage of the IDP:

- Take ownership of the safety and security risk management process with regular assessment of risk and identification of residual risk;

- The approach to risk management is tailored to the development and the requirements of stakeholders;

- Key safety and security decision directly relate to the reduction in likelihood or consequence of a risk;

- Any transferring, sharing or acceptance of residual risk is clearly articulated; and

- Changes to the development or removal of safety and security measures have an associated 'risk cost' identified.
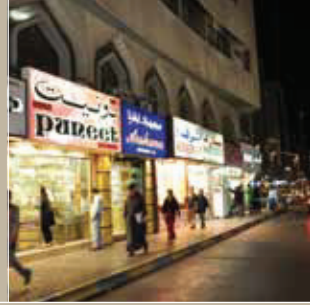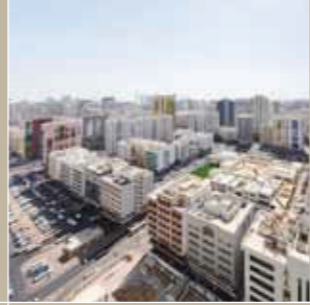
A2
Appendix 2: Glossary

Glossary
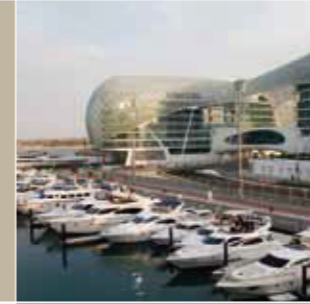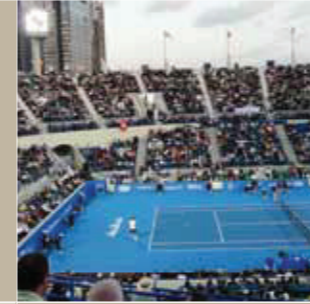
Accessibility: The ability for people to move round an area and to reach desired destinations, including 'mobility impaired individuals' (elderly, disabled people, those with small children or encumbered with luggage or shopping).

Access Control: The control of persons, vehicles, and materials through the implementation of security measures for a protected area.

Active frontage: An active frontage is an area where frequent use or adjacency to windows, mezzanines etc. provides a high degree of natural surveillance.

Alarm System: Combination of sensors, controls, and annunciators (devices that announce an alarm via sound, light, or other means) arranged to detect and report an intrusion or other emergency.

Asset: Any tangible or intangible value (people, property, information) to the organisation.

Barrier: A natural or man-made obstacle to the movement/ direction of persons, animals, vehicles, or materials.

Boundary Treatment: Safeguarding of a boundary or limit of responsibility.

Building Facade: The separation between the interior and the exterior environments of a building. It serves as the outer shell to protect the indoor environment as well as to facilitate its climate control. Building envelope design is a specialised area of architectural and engineering practice that draws from all areas of building science and indoor climate control.

Chemical, Biological, Radiological and Nuclear (CBRN): CBRN materials can be used in terrorist attacks. There have so far only been a few examples of terrorists using CBR materials, most notably a sarin gas attack on the Tokyo subway mass transit system and anthrax letters in the United States.

Closed-Circuit Television (CCTV): See video surveillance system.

Collapse – Progressive: A building undergoes progressive collapse when a primary structural element fails, resulting in the failure of adjoining structural elements, which in turn causes further structural failure.

Collapse – Disproportionate: The structural collapse of a building, disproportionate to the cause; it is often, though not always, progressive. A building should be constructed so that in the event of an accident or intentional attack, it will not suffer collapse to an extent disproportionate to the cause.

Community Safety: Strategies and measures that seek to reduce the risk of crimes occurring and their potential harmful effects on individuals and society, including fear of crime, by intervening to influence their multiple causes.

(UN Economic and Social Council, resolution 2002/13 of 24 July 2002, Annex)

Crime: An action or omission which constitutes an offence and is punishable by law.

Crime Prevention Through Environmental Design (CPTED): A theory that when a development is appropriately designed it can reduce the likelihood of crimes being committed. By introducing such measures it is anticipated that this will assist in minimising the incidence of crime and contribute to perceptions of increased public safety.

Crime Reduction: Any action to reduce the frequency and seriousness of criminal events.

Crowded Place: A Crowded Place is a location to which members of the public can gain access and by virtue of its crowd density and known terrorist attack methodology may be considered potentially liable to terrorist attack. They may be buildings or open air public spaces and they may be permanent or temporary.

Decision Support Tool: A web based 'on-line' facility to be used by developers at the pre-planning stage to gain an appreciation of how much influence safety and security may have during planning and design. At the end of the process there will be only two outcomes, High Priority or Low Priority.

Defence in Depth: The strategy of forming layers of protection for an asset (see assets).

Deter, delay, detect and deny: Key prevention principles in designing out the opportunities for crime:

Deter – This constitutes a visible deterrent to dissuade the opportunist; measures may include physical obstructions such as doors, the presence of security personnel and technical security systems e.g. CCTV.

Delay – Measures designed to provide an adequate delay to an intruder for other measures to respond.

Detect – Having delayed the intruder, measures must be sited to detect and identify the incident. These measures can either be covert or overt depending on the response available. The longer the delay the more successful the detection layer will function.

Deny – Denies intruders access to vital assets. Denial is the final chance to defeat an intruder / attacker and usually involves measures known as 'target hardening'.

Facility: One or more buildings or structures that are related by function and location, and form an operating entity.

HVAC: Heating, ventilation and air conditioning system.

Hostile Vehicle Mitigation (HVM): Design principle to protect an asset from a range of vehicle borne threats ranging from vandalism through to sophisticated attacks by determined criminals or terrorists.

Improvised Explosive Device (IED): An IED is a bomb constructed by the maker to allow someone to detonate it effectively at the time and place required. Some of the components, including the explosive, may have been homemade. IED's incorporate destructive, lethal, noxious, pyrotechnic, or incendiary chemicals, designed to destroy and incapacitate. IED's have been the most commonly used method of attack by terrorists in recent years.

Integrated Development Process: A process that brings together an interdisciplinary team to work collaboratively and iteratively, in pursuit of a single integrated safety and security

solution to new developments during the phases of Pre-planning, Planning, Design and Construction, Commissioning & Operation.

Intrusion Detection System: A system that uses a sensor(s) to detect an impending or actual security breach and to initiate an alarm or notification of the event.

Lighting: Degree of illumination; also, equipment, used indoors and outdoors, for increasing illumination (usually measured in lux or foot-candle units).

Natural Surveillance: A design concept to facilitate observation and help create an increased perception of risk to an offender thereby discouraging wrongdoing. Natural surveillance occurs by planning and designing the placement of physical features, activities, and people in such a way as to maximise visibility.

Operational Requirement (OR): A statement of need based upon a thorough and systematic assessment of the problem to be solved, and the hoped for solutions.

Opportunity: Describes the ability of a potential 'attacker' to conduct or carry out acts to aid an attack

Pedestrian Access Control Point (PACP): A facility specifically designed for controlling pedestrian access to a premises or location.

Personal Borne Improvised Explosive Device (PBIED): Bombs made small in size and less conspicuous, so they can be placed closer to the intended target, e.g. within a building or structure, carried or delivered by a person. The term is often used to describe deadly and determined suicide bombers however this is not always the case.

Physical Security: Physical security addresses actions taken to protect buildings, property and assets against intrusion or attack. It includes physical measures designed to safeguard personnel and prevent unauthorised access to equipment, installations, material, and documents etc.

Physical Security Measure: A device, system, or practice of a tangible nature designed to protect people and prevent damage to, loss of, or unauthorised access to assets (see assets).

Policy: A general statement of a principle according to which an organisation performs business functions.

Procedure: Detailed implementation instructions for carrying out security policies; often presented as forms or as lists of steps to be taken prior to or during a security incident (see security incident).

Proprietary Information: Valuable information owned by a company or entrusted to it, which has not been disclosed publicly; specifically, information that is not readily accessible to others, that was created or collected by the owner at considerable cost, and that the owner seeks to keep confidential.

Proprietary Security Organisations: Typically, a department within a company that provides security services for that company.

Protective Security: An organised system of protective measures implemented to achieve and maintain security. It combines the disciplines of personnel, information and physical security to create 'defence in depth', where multiple layers work together to deter, detect, delay and deny an attack.

Public Realm: The public realm includes all exterior places, linkages and built form elements that are physically and /or visually accessible regardless of ownership. These elements can include, but are not limited to, streets, pedestrian ways, cycleways, bridges, plazas, nodes, squares, transportation hubs, gateways, parks, waterfronts, natural features, view corridors, landmarks and building interfaces.
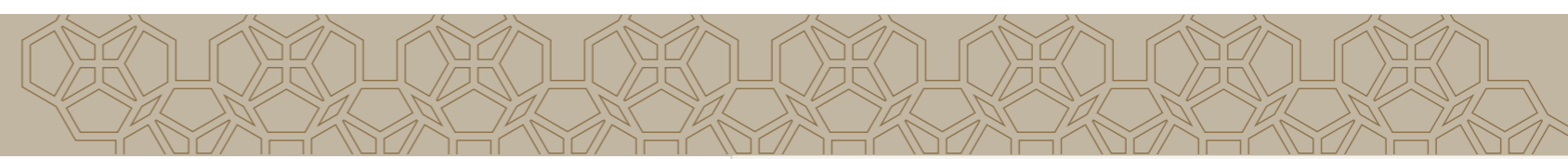
Risk: The effect of uncertainty on objectives. It includes both positive and negative impacts on objectives.

Risk Assessment: The process of assessing security-related risks from internal and external threats to an entity, its assets, or personnel.

Risk Management: The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects (HB167: 2006 Security Risk Management).

Safety and Security Advisors: Government officials, who will liaise with the development project team to offer advice, provide specialist inputs on safety and security and conduct the review of Planning Submissions and Building Permit Submissions from a safety and security perspective.

Safety and Security Specialist: A suitably experienced and qualified professional who, as part of the interdisciplinary development project team, advises the project client and manager on safety and security issues. Within the context of the SSPM, this person has specific functions to undertake during the Integrated Development Process for High Priority projects.

Sally Port: A secure, controlled entry point that usually incorporates the use of doors or barriers either side of a secure middle space (airlock). Can be used for controlling access for both vehicles and pedestrians.

Security Incident: An occurrence or action likely to impact upon assets.

Security Measure: A practice or device designed to protect people and prevent damage to, loss of, or unauthorised access to equipment, facilities, material, and information.

Security Vulnerability: An exploitable security weakness.

Setback: Setback in terms of land use is the distance of a structure from the boundary of the development plot. This is not the equivalent of 'stand-off' distance.

Site Hardening: Implementation of enhancement measures to make a site more difficult to penetrate.

Stand-off Distance: The distance between the asset and the threat, typically regarding an explosive threat.

Surveillance: Observation of a location, activity, or person.

Tailgating: The act of or attempt by one or more individuals, to enter a controlled area by immediately following an individual with proper access. Also referred to as 'piggy-backing'.

Target Hardening: A term used in security referring to the strengthening of the security of a building in order to reduce or minimise the risk of attack or theft.

Terrorism: Terrorism is the threat or use of action, calculated to create an atmosphere of fear and alarm. These acts are designed to influence the Government or to intimidate the public or a section of the public, and made for the purpose of advancing a political, religious or ideological cause. This often involves serious violence against a person or serious damage to property. Terrorism can come in many forms, not just a physical attack on life and limb. It can include interference with vital information or communication systems, causing disruption and economic damage.

Threat: A potential source of loss, harm or disruption.

Throughput: The average rate of flow of people or vehicles through an access point / portal.

Token: An electronically encoded device (i.e., a card, key-fob, etc.) that contains information capable of being read by an electronic device placed within or at the entry and exit points of a protected facility.

Uninterruptible Power Supply (UPS): A system that provides continuous power to an alternating current (AC) line within prescribed tolerances; protects against over-voltage conditions, loss of primary power, and intermittent brownouts (darkness resulting from the extinction of light). Usually utilised in conjunction with an emergency generator.

Vehicle Access Control Point (VACP): A facility specifically designed for controlling vehicular access to a premises or location.

Vehicle Borne Improvised Explosive Device (VBIED): Bombs transported by vehicles, one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target and can cause a great deal of damage.

Urban Design: The art of making places. Urban design involves the design of buildings, groups of buildings, spaces and landscapes, in neighbourhoods, districts, cities and municipalities, and the establishment of framework and processes which facilitate successful development.
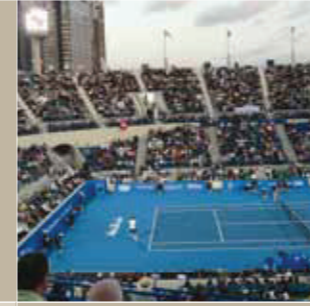
Video Surveillance Systems (VSS): A surveillance system in which a signal is transmitted to monitors / recording, and control equipment. Includes CCTV and network based video systems.

Vulnerability: The susceptibility of a target to be effected by a threat.
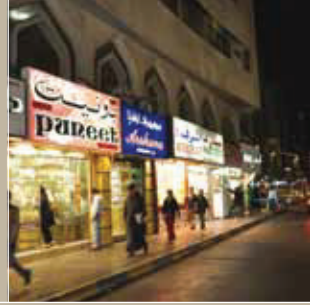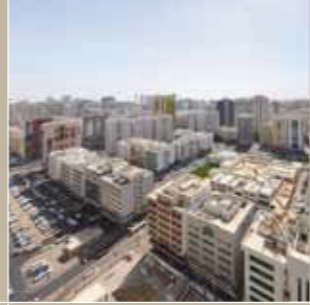
A3

Appendix 3: Further Reading

Further Reading

Abu Dhabi Public Realm Design Manual: Commissioned by the UPC to guide the development of a world-class public realm (Abu Dhabi)

Abu Dhabi Urban Street Design Manual: Commissioned by the UPC to address the needs of a growing population and a desire to create more walkable communities (Abu Dhabi)

Estidama (Pearl Rating System): Creating a new sustainability framework that will help preserve and enrich Abu Dhabi's physical and cultural identity, improve the quality of life for residents and reduce the Emirates's carbon footprint by encouraging developers to adopt a more sustainable approach to construction (Abu Dhabi)

Plan Capital 2030; Plan Al Ain City 2030; Plan Al Gharbia 2030; Structure framework plans to guide the Emirate's urban and regional development, planning strategies (Abu Dhabi)

ACT Crime Prevention and Urban Design Resource Manual: Australian Capital Territory, Advisory document to assist in incorporating crime prevention through environmental design principles into planning and development activities (Australia)

Contest: The United Kingdom's Strategy for Counter Terrorism (UK)

CPTED Essentials: Crime Prevention Through Environmental Design: Participant Workbook (Australia)

Crime Prevention Through Environmental Design: Applications of Architectural Design and Space Management Concepts, National Crime Prevention Institute (USA)

Crime Prevention Through Environmental Design: Guidelines for Queensland, Queensland Government (Australia)

Crime Prevention Through Environmental Design Guidebook: National Crime Prevention Council (Singapore)

Crowded Places: the Planning System and Counter Terrorism, Department for Communities and Local Government / Home Office (UK)

Department of Defence Minimum Anti-terrorism Standards for Buildings: Unified Facilities Criteria (UFC) system for application of anti-terrorism standards and recommendations (USA)

Designing Safer Places: A manual for crime prevention through planning and design (South Africa)

Does Regulation of Built-in Security Reduce Crime: Evidence from a Natural Experiment, Ben Vollard and Jan C van Ours (Holland)

Engineering Security: Protective Design for High Risk Buildings: New York City Police Department (USA)

FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, Federal Emergency Management Agency (USA)

FEMA 430: Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks Against Buildings, Federal Emergency Management Agency (USA)

Guidelines for Human Settlement Planning and Design Volume 1: Compiled under the patronage of the Department of Housing, by CSIR Building and Construction Technology (South Africa)

Integrated Security: a Public Realm Design Guide for Hostile Vehicle Mitigation, Centre for the Protection of National Infrastructure (UK)

National Guidelines for Crime Prevention Through Environmental Design in New Zealand Part 1: Seven Qualities of Safer Places (New Zealand)

Planning and Designing Urban Space, Community and Crime Prevention: The Case of Arab Countries - Policy Brief Series No 16, Dina Shehayeb (Egypt)

Protecting Crowded Places: Design and Technical Issues, Home Office (UK)

RIBA Guidance on designing for Counter Terrorism: (UK)

Safer Design Guidelines for Victoria: Principles facilitating the planning of safer urban environments, Department of Sustainability and Environment (Australia)

Safer Places: Planning System and Crime Prevention, Office of the Deputy Prime Minister (UK)

**Safer Places**: Counter Terrorism Supplement, Office of the Deputy Prime Minister (UK)

Safety Toolbox: Working Together to Build Safer Communities, Winnipeg Committee for Safety (Canada)

Secured by Design: New Homes 2010 (UK)

The Site Security Design Guide: US General Services Administration (USA)
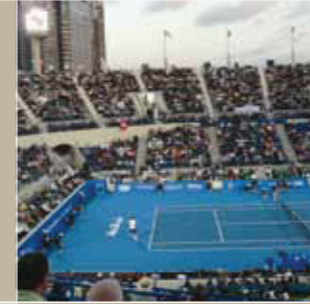
Think Thief: A Designer's Guide to Designing Out Crime, Design Council Guide funded through the Home Office Crime Reduction Programme (UK)

Working Together to Protect Crowded Places: Home Office (UK)
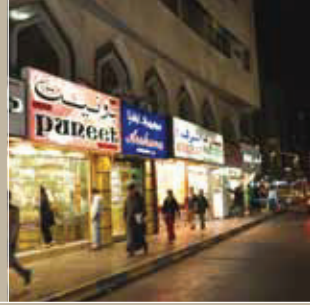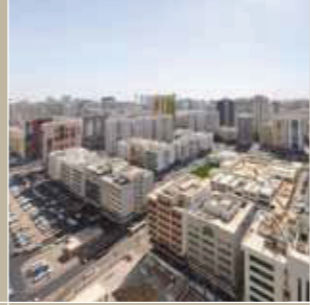
A4

Appendix 4:
Acknowledgements

Acknowledgements

Abu Dhabi Urban Planning Council

- H.E. Falah Mohammed Al Ahbabi
  General Manager, Abu Dhabi
  Urban Planning Council

- Amer Al Hammadi,
  Director, Planning and
  Infrastructure

- Hasan Al Mehairi
  Manager, Safety & Security

- Gavin W Jones
  Safety and Security Specialist
  (SSPM Project Manager)

- Stuart Williams
  Safety and Security Specialist

- Hunter Burkall
  Safety and Security Specialist

Higher Committee for Crises and Terrorist Acts Management

The Abu Dhabi Urban Planning
Council extends special thanks
to the Chairman and members
of the Higher Committee, who
have provided wise leadership
throughout the development
of the Manual.

Steering Committee

- Col Salem Al Zaabi
  Office of the Deputy
  Supreme Commander of the
  UAE Forces

- Col Saif Hamdan Al Kaabi
  Engineering Projects
  Adminstration
  Abu Dhabi Police GHQ

- Jasem Al Darmaki
  Department of Municipal
  Affairs

- Abdulla Al Shamsi
  Abu Dhabi City Municipality

- Abdulla Al Amiri
  Al Ain City Municipality

- Mubarak Al Hajeri
  Western Region Municipality

- Captain Mansour Al Dhaheri
  UAE Armed Forces

Implementation Working Group

- Abu Dhabi Urban Planning
  Council

- Abu Dhabi City Municipality

- Al Ain City Municipality

- Western Region Municipality

- Abu Dhabi Police GHQ

- Environment, Health and Safety
  Management System Centre

Technical Advisory Committee

- Abu Dhabi Urban Planning
  Council

- Department of Municipal Affairs

- Abu Dhabi City Municipality

- Al Ain City Municipality

- Western Region Municipality

- Abu Dhabi Police GHQ

- Department of Transport,
  Abu Dhabi

- Critical National Infrastructure
  Authority

- National Crisis & Emergency
  Management Authority

- Ministry of Interior
  (State Security)

Technical Advisory Committee Sounding Board

- Tourism Development and
  Investment Company (TDIC)

- Aldar Properties PJSC

- Abu Dhabi National Exhibition
  Centre (ADNEC)

- Musanada Abu Dhabi
  General Services

- Khalifa University of Science &
  Technology

- CBRn Advisor, Higher Committee
  for Crises and Terrorist Acts
  Management

- University of Huddersfield

Ministry of Foreign Affairs European Affairs Department

The Abu Dhabi Urban Planning
Council extends special thanks
to the Ministry of Foreign
Affairs for their support during
the development of the Manual.

UAE Embassy to the United Kingdom

The Abu Dhabi Urban Planning
Council extends its special
thanks to the Embassy and
H.E. Ambassador Abdulrahman
Ghanem Al Mutaiwee

HM Government, United Kingdom of Great Britain & Northern Ireland

The Abu Dhabi Urban Planning
Council extends special
thanks to the UK Foreign and
Commonwealth Office, National
Counter Terrorism Security
Office (NaCTSO) and the Centre
for the Protection of National
Infrastructure (CPNI) for
participation in workshops and
hosting benchmarking visits to
the United Kingdom.