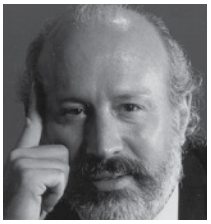
Title:	**Securing Iconic Structures**
Authors:	Sean Ahrens, Practice Leader/Manager, Aon Fire Protection Engineering Corporation Stephen Yas, Design Principal, Mulvanny G2 Architecture
Subjects:	Architectural/Design Security/Risk
Keyword:	Security
Publication Date:	2012
Original Publication:	CTBUH Journal, 2012 Issue II
Paper Type:	1. Book chapter/Part chapter 2. **Journal paper** 3. Conference proceeding 4. Unpublished conference paper 5. Magazine article 6. Unpublished

Securing Iconic Structures

Sean Ahrens



Stephen Yas

Authors

Sean A. Ahrens, Practice Leader/Manager

Aon Fire Protection Engineering
Security Division
1000 Milwaukee Avenue, 5th floor
Glenview, IL 60025
United States

t: +1 847 461 9359
f: +1 847 953 7793
sean.ahrens@aon.com
www.aonsecurity.com

Stephen Yas, Design Principal

MulvannyG2 (Shanghai) Architecture
Ciro's Plaza Suite 1905
388 Nanjing Xi Road
Shanghai 200003
China

t + 86 21 6032 0100
f + 86 21 6217 8525
e: Stephen.Yas@mulvannyg2.com
www.mulvannyg2.com

Sean A. Ahrens
Sean leads the security consulting practice at Aon FPE with over 19 years of experience, a majority of which has been in a security consulting function. He has been responsible for providing security threat and risk analysis, contingency planning, loss prevention, and force protection design and planning. Sean has provided design and construction administration for government, public, and private entities that encompass telecommunications, security, surveillance, and access control systems. He is well versed in the various trade and local authority issues impacting projects, and has specialized professional competence in security, access control systems, and force protection systems.

Stephen Yas
Stephen has over 35 years experience working internationally. He specializes in architecture, urban design and interior design for large mixed-use projects. As design principal in the Shanghai office of MulvannyG2 Architecture, he is the design leader in China for the firm. Prior to MulvannyG2, Stephen led his own firm in Chicago for 22 years. Prior to that he was a senior designer at SOM Chicago and Lohan Associates, as well as having worked in England and the Middle East.

"In sophisticated urban planned environments, security should be subtle, but allow for the potential for heightened threats. The key is to find a suitable balance between security and preserving the designer's vision. A security program for any structure should employ a variety of controls to deter, delay, detect, deny and respond to threats, as well as mischievous or potential accidental acts."

This paper emphasizes the importance of integrating security programming into building design, allowing for different uses and threat levels for the life of the building. Security strategies will be evaluated that can be applied to any building, as well as review procedures to address concerns early in the design process, especially in politically and economically charged international environments. General concepts and approaches to building security will be examined, demonstrating the benefit of collaboration between architects and security professionals at an early stage to meet the project's goals without detracting from the planner's vision for the project.

The "Fortress"

To the untrained eye, this graphic (see Figure 1) may appear "fortress" like. However, in its most basic format, the diagram describes the security program for building at any security level. Early dialogue between security professionals and the designer can limit the fortress or bunker aesthetic by careful placement of technical security, including cameras, setbacks, gates, fencing and spatial provisions for security staffing.

In many cases, consideration is not given to the potential for a future modification to the building, such as the addition of a casino, parking garage, skate park or theater, which may increase the potential for malevolent acts. The addition of new tenants, such as a dignitary or VIP, may require a change in the security status not considered in the original design process. The modification of the physical and architectural security component is the most important, most expensive and, therefore, most difficult to modify post-design. Done early in the design process there is significant indirect and direct return on investment that can be achieved by pre-planning.

When planning a facility, design professionals need to think outside-the-box. Although fear of terrorism typically drives the mindset for iconic building security, there are other more likely threats, including workplace violence, domestic spill-over issues, intellectual theft, property theft and other malicious acts against persons or property that can affect the building and its occupants. Unforeseen dangers can create significant security challenges for building owners post-design and may detract from the marketing, image and status of the project. Planning for a single threat may not be effective and may miss potential threats in the future. The best approach is to create generalized controls designed to address a broad range of threats.

Unlike other building elements, there are no standards for the provision of security based on building occupancy. As a result, the evaluation and development of security controls is purely based on a quantitative risk and consequence analysis which evaluates all aspects of the proposed building, not simply such critical assets as electrical and telecommunications systems. Conducting a risk and consequence analysis will assist the

designer with understanding the exposure to threats. For example, a building near a proposed or existing mall will make criminal incidents more likely. In similar fashion, integrating a train or metro into a large high-rise project could increase exposure to chemical or explosive attacks, while the creation of a building near a government facility or embassy may escalate the tertiary terrorism risk.

The type of building and its tenants may also affect risk rating, which can change over time. Understanding the risks early in the process will assist organizations in making decisions. The planner should ensure that the security analysis provides specific guidance and recommendations on vehicular access, security placement of cameras, access control and the overall security compartmentalization program.

From a security perspective, designers need to think about the "what-ifs." They need to have a vision. That does not necessarily mean implementing controls from day one, but designing provisions into the architecture so security controls can be easily and quickly adopted in the future if higher threat scenarios arise.

The downside of shortsighted preplanning is evident in the airports built 20 years ago. The functions and usage of airports have changed dramatically. The free flowing public environment of yesterday is now a series of mazes and security compartmentalization which could have been avoided, if only designers had taken a more open-minded approach during the design process.

Preparing for the Future

To prepare for tomorrow's uncertainties, today's international planners should start by evaluating the site and potential setbacks and standoff distances from the façade of the building. Even with constricted site layouts, there are opportunities that can be explored. Setback can be achieved through a number of programming elements. To increase the affect of clear space, the perception of setback can be somewhat masked through architectural programming, such as the creation of multi-tiered planting areas, water features, structures and natural boulders. The proposed US Embassy in London employs an enveloped glass façade and a water feature to support security. The water feature provides a visual element to the project, but it also creates a defined perimeter and clear zone.

When developing building placement, roadways should be carefully evaluated. Centralized or limited roadway access is preferred, while incorporating standards and requirements for emergency access. In some cases, emergency access roadways will need to be secured and may create a conflict with first responders. Proper signage and clear access routes can limit frustration by people who are not familiar with the site, which could be a key to minimizing negative interactions with security. Site confusion can lead to anger. Roadways are integral to the project, but simple and cost effective techniques, such as using a serpentine access road, can create elegant and effective solutions to reduce the potential for a vehicle to approach a building at high speed.

Counter terrorism and counter surveillance techniques are extremely beneficial to identifying an aggressor. For this reason, building layout, whenever applicable, should afford natural sight lines to allow the detection of an intruder. As a result, landscaping is extremely important. Trees and other foliage that can obscure sight lines should be discouraged. Lighting, the number one deterrent to crime, may become obscured by growing tree canopies. As a result, lighting plans and photometrics should take into account tree growth over the life of the tree and the effect on the light distribution. By doing this, more effective light placement can be identified.

Hotels will often employ a *porte cochere,* which can expand setback from the primary structure while providing continuity in architecture and limit the perception of distance from the entry to the building. Setback is more than just maintaining vehicle proximity. Setback increases natural lines of sight as well as the area that must be traversed prior to accessing a facility, while supporting the potential for early detection of an aggressor. Designs should limit components that may be used by aggressors for criminal acts. Loose rocks of substantial size could be used to break windows to gain entry to a building or be picked up as a makeshift weapon in an ambush scenario. If rocks are integral to design, they should be kept small or be large enough that they can't be easily picked up.

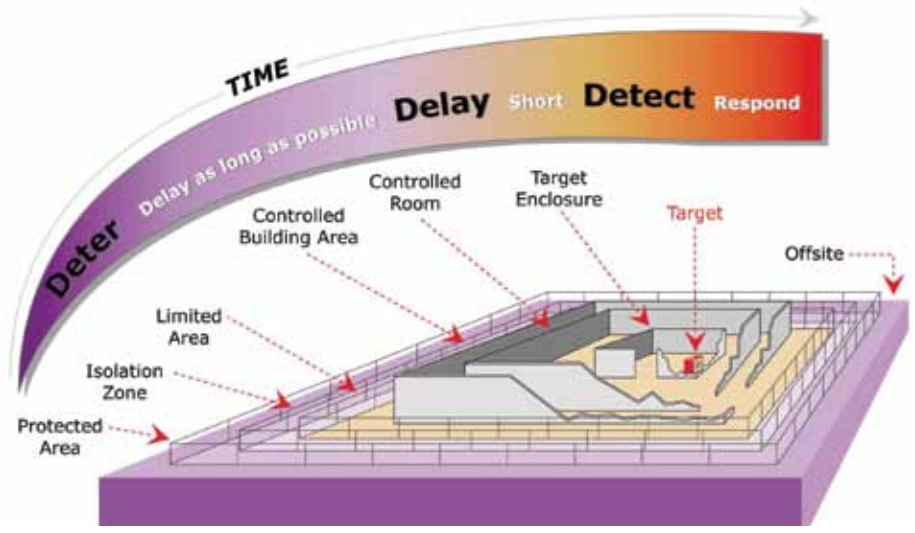


Figure 1. The "fortress" © Aon

The Worst Case Scenario

When designing setback and site placement, consideration should be equally afforded to the planning for emergency vehicles and muster points for evacuating tenants. Muster points need to account for the expected mass of people and should be as far away from

the building as possible, typically not less than 30.5 meters. At the same time they need to be located in areas where they will not encumber or block first responders. Planners should also recognize that some muster points may be unusable during an emergency, and alternatives will have to be developed. Unresolved, these conflicts can reduce first responder times, which can lead to loss of life.

To develop muster points, designers should plan for the population density by using 1.2-square meter per person as a worst case scenario. When considering fire department access, especially in international markets, planners should identify areas for the large turning radius required of first responder vehicles. In addition, multiple access points to the facility should be considered, some roads may not be accessible. One innovative approach used in the past is to employ sub-surface materials to support the weight of first responder vehicles. These subsurface materials allow vegetation to grow while masking a roadway. This is especially beneficial when working with one-way roads and congested thoroughfares.

Beyond accommodating first responders, planners should also take into account prevailing winds to minimize potential chemical exposures. This information should also be included in the security design and, whenever possible, muster points should be located upwind to prevent mass casualties as a result of a primary or secondary event.

Secondary events are commonly utilized by terrorists to inflict additional loss, such as a chemical release in muster areas after a primary attack.

Coordination of exit routes for the interior of the building is equally important. The design should identify secure areas and ensure that paths of egress do not conflict with security provisions. In coordination with egress requirements, the building core should be evaluated to ensure the application of security does not clash with the life safety code. For example, in a fit out program that uses the elevator vestibule as an exiting corridor, security technology might be easily defeated by activating an automatic sprinkler or emergency pull station, which would allow access to the building from the elevator vestibule. Additionally, the elevator corridor itself is a potential entrapment area, and must include provisions for unimpeded egress. Although a dedicated corridor could be provided, a secondary approach would be to encapsulate a stairway within the elevator or building core. Horizontal and vertical access, especially in a high-rise, should be carefully evaluated. Where applicable, in high risk environments, considerations should be given to further controlling the core of a building.

This diagram (see Figure 2) describes an approach used for a high-security financial enrollment. The creation of an egress corridor that surrounds the core eliminates life-safety code impacts, and still provides a high degree of security. In these instances, the elevator core and stairwells are secured, but egress onto the floor or access from the elevator lobby is still permitted. In the event either of these doors are breached, an alarm is sent to security. This offers significant delay because this is only the first control measure being used to delay access to the fit out area beyond the emergency corridor that we created.

Thinking about Space

Lobby designs should also take into account the possibility of higher threats in the future, and the potential for additional equipment. The use of X-ray and magnetometers are more common for large sophisticated international projects and can take up significant space and increase pedestrian queuing times. Planners should identify pedestrian throughputs and design the space to accommodate this equipment and expected pedestrian traffic.

Space allocations vary, but for one magnetometer and X-ray device, planners should accommodate 6.7 square meters for both equipment and a minimum of two operators (see Figure 3). With a minimum of two X-rays and magnetometers, space can be allocated quite quickly. These devices can make a lobby extremely congested if plans are not properly designed to accommodate the equipment. When considering pedestrian

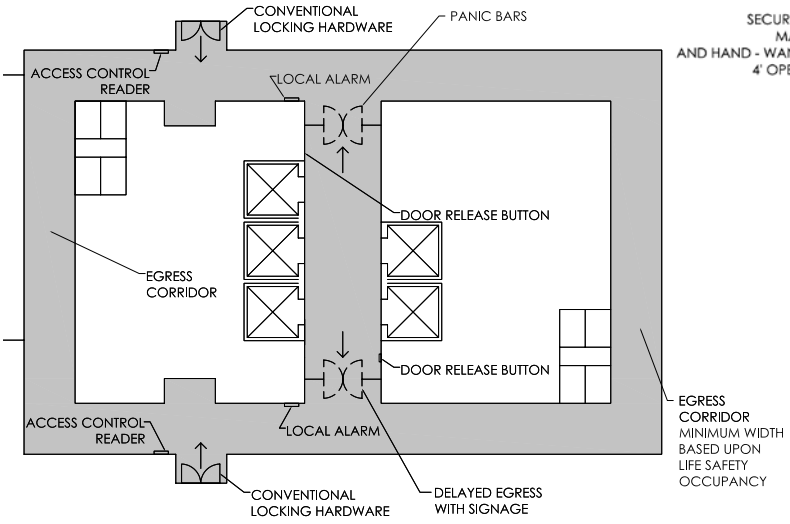


Figure 2. Typical diagram of a secured egress

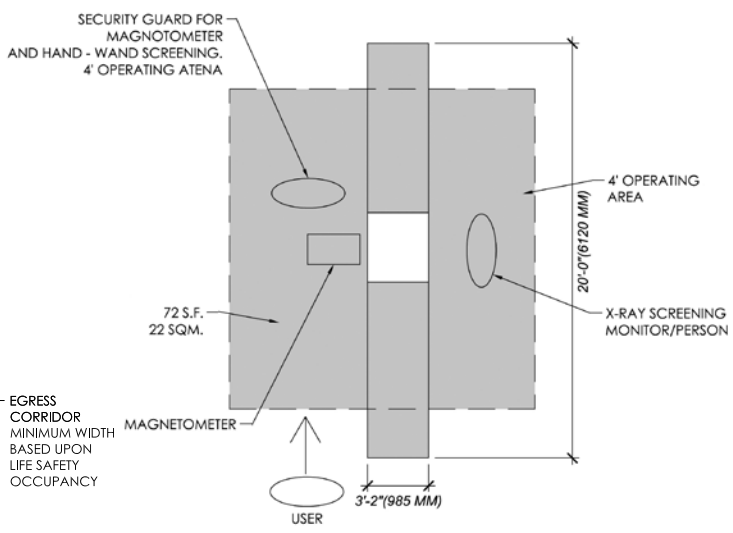


Figure 3. Space allocations for a typical security point

Figure 4. Faro Monarca, Medellin, Colombia © Yas Architecture

queuing times recognize that X-ray and magnetometers can differ from manufacturer to manufacturer. However, as a worst case scenario 25 seconds per person for one screening point should be considered in determining the total space required to limit queuing issues.

Another commonly overlooked aspect of a security program is the staffing and operations space required for the security program. It is possible for an international project to employ more than 80 people in a dedicated security function. Sizing for these support areas is dependent on the preparation of the security strategy. In the case of a very large mixed use project in Asia, the security operations required 55.6 square meters for a control room, 12.9 square meters for an equipment room, 8.9 square meters to accommodate an uninterruptable power system, 3.0 square meters for toilets, 18.5 square meters for a break room, 10.1 square meters for two management offices, and 5.8 square meters for badging rooms. In addition to spatial allocation, adjacencies need to be evaluated and incorporated into the design. If this is not done early in the process, then these security elements will have to be segregated, which limits the effectiveness of the program, especially in an emergency.

These elements should be addressed early in the design. International projects, especially those in the Middle East, are more likely to carry requirements for security and third-party review. Security-specific presentations and multi-tiered, multi-organizational reviews of the security plan are common. The process can be somewhat confusing, time-intensive and it varies from location to location. Some international projects might also require a formal review by the military or local law enforcement. But a design team addressing security compliance issues later on in the design process could be met with resistance, potential modifications to the design and delays in obtaining approval permits for construction.

For example, in Abu-Dhabi the Urban Planning Council (UPC) is one of many third parties with a formalized review process which includes an analysis of threats and vulnerabilities specific to the property, as well as a review of proposed security measures and controls. Beyond the UPC, supplementary requirements can be mandated based on the building type and location within a specific region. UPC recognizes that terrorism is a potential threat, but requires measures to deal with other threats, such as sabotage or riots. The process is not subjective or exclusive; it is the designer's requirement to reflect a security program for the project.

UPC is one of several planning bodies using Crime Prevention Through Environmental Design (CPTED) reviews, calling for architecture and landscaping to integrate with security. For a project in the Middle East the security team worked with the architect to define acceptable and legitimate paths of travel on to the site. These predictable patterns were marked with flowers on either side of a path, which was emphasized with lighting during evening hours. This approach allowed the designers to concentrate surveillance on these predictable traffic patterns, and made it easier to detect illegitimate activity, which would have to occur in landscaped areas outside of the pathways.

Some may attempt to circumvent the third party approval process in international projects by indicating controls on their submission plan, but later change the design as part of a value engineering exercise. This approach can backfire on the design team, resulting in more serious complications and costs. Some reviewing entities are verifying the installation to ensure that the elements submitted and documented were actually implemented.

Case Study: Faro Monarca, Medellin, Colombia

To maintain the design goals, meet third-party requirements and prepare for tomorrow's uncertainties, designers need to develop a security strategy, much like any other component in the design process. The security strategy establishes the program in narrative format, prior to the development of drawings, which allows planners to adapt more readily to the security threats and implementation of controls.

When developing a security strategy, it is important to consider the use of a zoning diagram, similar to that employed in space planning, to describe the functions and types of occupancies as they relate to security. Zoning diagrams should clearly convey functions, and describe generally the security for the area. Zones of security start with minimal controls, and then increase with complexity and proximity to a core asset. Increasing controls facilitates detection and response to an in progress event.

As an example, let's examine the Faro Monarca Tower in Medellin, Colombia, a multi-use facility designed to stand more than 300 meters tall, including 217 hotel rooms, 476 condominiums and an 850-car underground parking structure (see Figure 4). The Faro Monarco is unique in that it incorporates a variety of functions that could create security issues. Specifically, there is a metro-cable car station connecting the project to the city, as well as the foothills of Medellin. In addition, the project includes a religious sanctuary, which is expected to be frequented by 3,000 people or more. When the sanctuary is not in use it will serve as an auditorium to host rock concerts and pavilion-type events. A casino is planned for the site opposite of the

mixed-use religious sanctuary. The Faro can be seen as a sophisticated building, but it is – first and foremost – a building of and for Medellin; a symbol of promise and rebirth for the future of the Colombian Republic after 40 years of war. When built, the Faro has the potential of being one of the tallest buildings in South America and an icon for the country's economic growth and prosperity.

For the Faro Monarca Tower the security team worked closely and collaboratively with the designers on every aspect of the project, from basic site layout to pedestrian and vehicular circulation, and other movement systems on the perimeter grounds. It was recognized that this building could be a potential symbolic target, prompting planners to embrace security holistically in its design. For this project, country and local risks were analyzed to identify broad threat exposures. Considering these findings, the focus was narrowed to the building and surrounding area, the proposed tenant clientele, overall usage of the facility and the evaluation of surrounding buildings and tertiary exposures. The location of mass transit was also reviewed for the potential for criminal incidents.

Security risks were then internally evaluated, white-boarded and prioritized. With no standards specifically for security planning,

...cheaply

> "Southwark would have been selling itself very cheaply… and [it] would have set an awful precedent. It would also have sent a signal that Southwark is anyone's."
>
> *Allies & Morrison Director Graham Morrison on a proposal to drape advertisements on the Kings Reach Tower in Southwark, London. From "Council Rejects Proposal for 60-meter High Adverts on Richard Seifert Tower," www.bdonline.co.uk, April 20, 2012.*

Figure 5. Security strategies implemented on Faro Monarca Tower © Yas Architecture

the white-boarding process was a collaborative effort, maintaining the goals of openness, usability and function. This process utilized a cause and effect analysis, which looked at specific risks and threats and implemented broad recommendations, such as increasing the defined perimeter around the building, which could then be incorporated with the designer's goals.

For the Faro Tower, a primary risk was the perception of the building and the impact of previously experienced high crime rate in the area. The building's functions were anticipated to draw a variety of aggressors. At the same time, the need for openness, transparency and the overall tenant/guest experience was not to be overshadowed by the perception of security. The builder required that security had to be built in and unobtrusive.

Using these goals as a benchmark, a holistic security program was developed that began with a recommendation for setback distances, as well as predefined vehicular routes and predictable pedestrian entries to the property (see Figure 5). Setbacks were based on Federal Emergency Management Agency (FEMA) guidelines identifying the minimum stand-off distance, at 30.5 meters. First responder requirements for vehicular access and equipment availability were reviewed in interviews with local representatives to minimize confusion and conflict during an emergency. The security program was supplemented with psychological and visual barriers through landscaping, which highlighted signage along a predetermined path, making it easy to identify illegitimate access to the property.

As the facility is envisioned as mixed-use, with a wide variety of pedestrian and vehicle circulation, security compartmentalization needed to be evaluated from a fresh perspective. A building core was developed that permitted unimpeded egress from the elevator vestibule/lobby, and floor plate exclusively. Typically, this compartmentalization is already built into the program. However, in multi-use facilities, egress can be shared between functions, and conflicts between life safety code and security can arise.

For the Faro, the building core and the relation of service elevators and emergency exits were examined and, whenever possible, integrated to further support security while maintaining the life safety code and exiting requirements by eliminating the need to utilize the elevator vestibule as an exit path.

During a joint team meeting, it was determined that there were tertiary risks from surrounding buildings that would create additional targeting dangers to the primary structure. The proposed metro/cable car line and the planned religious multi-purpose sanctuary and casino would draw thousands of pedestrians and vehicle traffic on a daily basis. These tertiary risks, in combination with a lack of local law enforcement and fire services, dictated the need for a fairly robust security and traffic staff. They had to be accounted for in the architectural planning process by creating space for a dedicated

security force and fire brigade for the project. The security facility was positioned near the building core to support situational awareness, centralization and survivability.

In the lobby, systems were integrated with the interior design to address the security requirements. Space was allocated for metal detectors and X-ray equipment and the security function itself. Pedestrian circulation was examined and controlled through the use of turnstiles that blended into circulation patterns. Screening equipment was blended into architectural elements by cladding the equipment with non-metallic materials. Designs were rendered to create enclosures, which would be completely devoid of metal screws. As a result, these enclosures need the use of wood dowels as a method to construct them. This approach created an open atmosphere that can quickly adapt to a changing environment or higher threat scenarios, such as a visiting dignitary or VIP.

Landscape and sitting elements were another important architectural component to the project. As a result, in accordance with US best practices, barriers were needed to inhibit accidental or deliberate vehicle ingress through the proposed lobby, which would be encircled by a glass curtain wall. The placement of the below-grade parking structure was another key element of the joint security and design plan. Following US guidelines, it was not located directly under the tower due to the potential for vehicle bombs. Additionally, the property was raised to provide clear lines of sight in the area leading up to the entrances, creating a clear zone between the hardened perimeter and the façade. These barriers were designed using local large, rough, natural stone slabs, covering large steel tubes secured to the ground. To the untrained eye, the barriers are part of the landscape and emphasize the lobby entrance.

The perimeter encompassed dual purpose retaining walls, which acted as physical barriers and vehicle arresters. These retaining walls sloped down into more formalized vehicle barriers systems, which are typically seen in iconic buildings. In other areas, landscaped terraces and earth berms were utilized as deterrents and natural vehicle arresters. Roadways were introduced to the property and incorporated curves and speed bumps as a natural method to controlling vehicle speed and approach to the property. The applicability of a welcome center building extension was also reviewed (see Figure 5), allowing planners to incorporate screening further from the primary building structure. Roadways were designed with slip lanes to minimize vehicle queuing and identify higher threat scenarios.

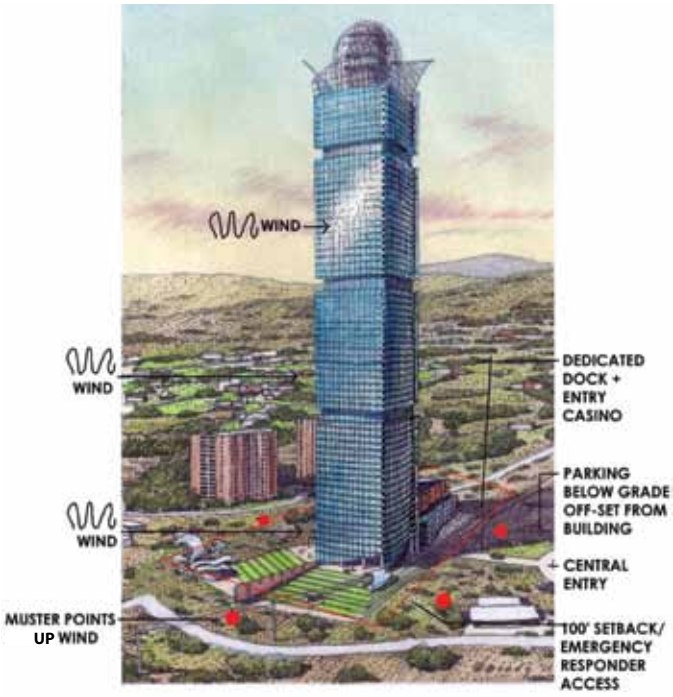


Figure 6. Allocating the muster points © Yas Architecture

Careful consideration was also given to the muster points, in case of an emergency (see Figure 6). Muster locations too close to the building can create conflicts with first responders, delaying response, which could create loss of life. The designer also needed to evaluate prevailing wind as it relates to the structure. When possible, muster points should be upwind, and should additionally be at elevated areas. The possibility of a chemical attack cannot be ruled out. Many chemicals are heavier than air, and can remain in depressed, sunken areas of the site. Potential chemical exposure can be mitigated by utilizing the wind to the designers' benefit.

Conclusion

Absent of standard security guidelines, developing security for an international building can be a moving target. But best practices and team collaboration including the owner, architect and security professionals can be a process-driven exercise. Done early and in collaboration with the team, commensurate controls can be identified and incorporated with no impact on the design, if the true risk appetite is understood and appreciated. The real value of security planning is realized when the architectural vision and aesthetics are preserved without detracting from the function and adaptability of a security program at any threat level.

Depending on the level of security required, a project typically allocates one to two percent of its budget for the security equipment. By all estimates, the total security program is miniscule in comparison to the other elements that make up a project. However, mismanaged security programming can become a stumbling block when not considered in the design. Recognizing what is to be designed and the potential future environmental impacts will provide a baseline for informed decisions. This will assist in streamlining the third-party review process, drive client value and innovation, minimize headaches for architects and planners, limit conflicts, and maintain the aesthetic vision for the project. This process incorporates the potential for changes as the building's usage and function changes over time. But, most importantly, this process makes the buildings safer for the people that will work and reside in them. ■