Tall Building Security, Resilience & Protective Design

An output of the CTBUH Security Working Group

Sean A. Ahrens & Caroline Field
Tall Building Security, Resilience & Protective Design

An output of the CTBUH Security Working Group

Sean A. Ahrens & Caroline Field
Principal Authors

Sean A. Ahrens, Chair of the CTBUH Security Working Group, Chicago
Caroline Field, Arup, Bristol

Contributors & Peer Review Panel

Walter Adams, AECOM, New York City
Christopher Ballou, Patriot USA Inc., New York City
John Busch, Department of Homeland Security, Milwaukee
Louis Chavez, Underwriters Laboratories, Chicago
Seda Dogruel, Arup, London
Steven Fisher, JBA Consulting Engineers, New Orleans
Forrest Gist, CH2M Hill, Portland
Gez Hart, BuroHappold Engineering, Bath
Keith Johnson, Atkins, London
Brian Katz, Hinman Consulting Engineers, San Francisco
David Kimmerly, WSP Group, Dubai
Glen Kitteringham, Kitteringham Security Group Inc., Alberta
Robert Lomb, PositivEnergy Practice, LLC, Chicago
Patrick Markham, Guidepost, Dallas
Ronald Ronacher, Arup, New York City
Robert Smilowitz, Weidlinger Associates, New York City

About CTBUH Working Groups

CTBUH Working Groups report on specific aspects of the planning, design, construction, and management of tall buildings. They are not standing committees, but groups that form for a period of time, specifically around a need or important topic in the industry, with the aim of disseminating their findings through the publication of a technical guide.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.0</strong> Tall Building Interiors</td>
<td>72</td>
</tr>
<tr>
<td>6.1 Spatial Planning Considerations</td>
<td>74</td>
</tr>
<tr>
<td>6.2 Security Control Room</td>
<td>74</td>
</tr>
<tr>
<td>6.3 Planning Building Interiors</td>
<td>76</td>
</tr>
<tr>
<td>6.4 Entry Lobbies</td>
<td>78</td>
</tr>
<tr>
<td>6.5 Building Core</td>
<td>83</td>
</tr>
<tr>
<td><strong>7.0</strong> Tall Building Security Technologies</td>
<td>86</td>
</tr>
<tr>
<td>7.1 Emergency Communication</td>
<td>88</td>
</tr>
<tr>
<td>7.2 Surveillance Systems</td>
<td>89</td>
</tr>
<tr>
<td>7.3 Access Control and Alarm Monitoring</td>
<td>92</td>
</tr>
<tr>
<td>7.4 Locking Hardware</td>
<td>94</td>
</tr>
<tr>
<td><strong>8.0</strong> Precautions for Extreme Threats</td>
<td>96</td>
</tr>
<tr>
<td>8.1 Chemical/Biological and Radiological/Nuclear (CBRN) Threats</td>
<td>98</td>
</tr>
<tr>
<td>8.2 Elevated Ballistic Attack</td>
<td>99</td>
</tr>
<tr>
<td>8.3 General Blast Loading Considerations</td>
<td>99</td>
</tr>
<tr>
<td>8.4 Façade Blast Loading Considerations</td>
<td>105</td>
</tr>
<tr>
<td>Case Study: A Façade Designed for Blast Resistance</td>
<td>110</td>
</tr>
<tr>
<td><strong>9.0</strong> Narrative Summary and Future Considerations</td>
<td>114</td>
</tr>
<tr>
<td>9.1 Site Layout</td>
<td>116</td>
</tr>
<tr>
<td>9.2 Adjacency Planning</td>
<td>117</td>
</tr>
<tr>
<td>9.3 Future Lobby Design</td>
<td>119</td>
</tr>
<tr>
<td>9.4 Conclusion</td>
<td>121</td>
</tr>
<tr>
<td><strong>10.0</strong> Glossary of Relevant Terms and References</td>
<td>122</td>
</tr>
<tr>
<td>About the CTBUH</td>
<td>132</td>
</tr>
<tr>
<td>About the Authors</td>
<td>133</td>
</tr>
<tr>
<td>CTBUH Organization &amp; Members</td>
<td>134</td>
</tr>
</tbody>
</table>
Since September 11, 2001, government agencies and the private sector have endeavored to find an appropriate and sensible level of security in tall buildings that is proactive without being overly stringent or invasive to daily routines. Several executive branch agencies around the world, including Centre for the Protection of National Infrastructure (CPNI) and the Department of Homeland Security (DHS), have produced reports presenting risk-tiering systems or offering recommendations for improving building security, however to date, no such report has been tailored to meet the specific needs presented by tall buildings and their unique risk environment. This guidance aims to fill that void by providing a robust analysis of tall building security to empower building stakeholders to make risk decisions from an informed standpoint.

This document, developed by the CTBUH Security Working Group, was conceived as a response to these challenges, and is intended to provide practical, unobtrusive security guidelines for tall, supertall, and megatall buildings, with the hope of mitigating threats to personal welfare and business operations. This text offers a step-by-step approach to developing and implementing a protective design strategy for a tall building at the earliest phases of the project’s inception. By providing information on the concepts of tall building resilience and the risk assessment process, along with practical guidelines for increasing resilience through architecture, structure and critical equipment, this text offers design strategies to current and future security challenges, thus enhancing the resilience of tall buildings.

Objective

By providing a broad overview of protective design processes and resilience controls for high-rise buildings, it is the objective of this Guide to build a reference that can aid in deterring, delaying, detecting, mitigating, responding to and recovering from an event. These protective design processes will be explored across a variety of disciplines and contexts, including but not limited to architecture, siting, space planning, technology, lighting, interfaces, and other building elements.
The design of tall buildings must consider protective design and resilience measures holistically, to ensure that the correct level of protection is provided without compromising the ability to create aesthetic and functional spaces. It is a further objective of this Guide to relay that there is no “one size fits all” approach, as each environment and situation requires an informed and specific solution; rather, it aims to offer the conceptual framework so that each building stakeholder can forge a customized program that suits individual contexts.

The development of a security program must consider both current and future protective design and resilience measures, keeping in mind that threats can evolve and shift over time. Thus, this guide is intended to inform and educate the reader about the strategic benefits of a proactive, rather than a reactive approach. This guide provides an overview and a logical process for the evaluation and incorporation of building controls, and endeavors to provide controls that are intended to be adaptive towards a myriad of events that may occur in a changing environment. It also intends to increase the resilience of the asset, building, and habitat to a broad array of threats by enabling informed, proactive decisions about risk. Finally, this book promotes the integration of measures with holistic benefits, such as designing a secure space that is also functional and pleasant would attract people and various services and amenities.

The information presented in this Technical Guide is intended to be a reference for architects, owners, developers, consultants and planners, and aims to address proactive, value-driven planning in the protection of their respective assets. If incorporated during the planning stage, protective design costs are minimized, whereas the impacts of retrofitting can be far more financially restrictive, and in some instances, impossible or impractical to incorporate.
The threats of terrorism and malevolent events coupled with the increasing quantity of natural disasters due to climate change has made the field of tall building resilience more important now than at any other time in history (see Figure 1.1). These events are shifting how buildings are designed, accessed, perceived, and experienced by both building occupants and the public. The ability of tall building stakeholders and urban planners to successfully predict, identify and mitigate or eliminate these risk factors is directly proportionate to the early development of a resilience plan during building design.

1.1 Defining Tall Building Resilience

Resilience is the ability to prepare for, and adapt to, changing conditions, as well as the capacity to withstand and recover rapidly from disruptions. In the context of tall buildings, this means taking measures to not only increase the robustness and redundancy of buildings against identified risks, but incorporating the flexibility to adapt to future trends and technologies. It is also important to consider how best to minimize disruptions to the operation of the building, by having adequate situational awareness, response and recovery plans so that the building can resume normal operations within an appropriate time frame (see Figure 1.2).

As resilience strategies are implemented, the capability to prevent or mitigate identified threats improves, along with the ability to respond to those events that cannot be predicted or avoided. In summary, resilience is the capacity to recover from a crisis, learn from the event, and ultimately implement controls to preclude its occurrence in the future. This process includes understanding how to assess risks to a tall building, educating stakeholders on risk-mitigation options and their cost, and integrating protective design measures into the planning of the tall building to increase resilience.

1.2 Qualities of Tall Building Resilience

To build an appropriate resilience program for a tall building, it is useful to qualitatively understand the suggested attributes of a resilient system (see Figure 1.3). A resilient system should possess certain physical qualities, such as robustness, which in this context, refers to a structure’s hardness, or ability to resist the impact of an earthquake or blast. Sustainability is also crucial to the system’s successful operation. With respect to tall building resilience, sustainability indicates that the security program can be ongoing, supported and upheld over time. From
an environmental perspective, it should deplete a minimum of natural resources. A system with a high level of resilience should also include a high level of adaptability, which refers to its ability to anticipate disruptive technologies or emergent threats and controls, such as drones, robotics or other technological developments (see Figure 1.4). It should also be integrated, meaning that its constituent parts (architectural, technological and tactical/operational) work together in a coordinated manner to provide an outcome that solves multiple design requirements.

From a systems thinking point of view, a resilient building should be redundant, meaning that its infrastructure networks and resource reserves are well-distributed in case one is compromised during an event (see Figure 1.5). In this vein, a resilient building is also fail-safe, meaning that it anticipates and understands potential failure mechanisms and makes provisions to ensure failure is predictable, safe and not disproportionate to the cause. Active consideration is given to potential cascading failure situations so that the overreliance on a single asset is avoided.

Preparedness is also critical to building resilience, and more specifically translates to a building being responsive, or possessing a good awareness of a situation and the tools
This chapter addresses the preliminary stages of incorporating resilience into a tall building by assessing its organizational and design features at the outset of the design process, with the goal of introducing resilient elements into construction and supporting the tactical and operational aspects of the tall building after completion (see Figure 2.1).

2.1 Identify Building Stakeholders and Mission

The first step in establishing a building resilience approach is getting organized around goals with respect to building context, the parameters that define resilience goals, and identifying stakeholders. Tall building resilience is an inherent and interwoven part of the project either directly or indirectly. Much like any program, a top-down buy-in for the program should be implemented. Whereas resilience should not overpower the mission, goals and objectives of the tall building project, there must also be room in the mission statement for team input. For instance, typical mission statements for a tall building program can include, but are not limited to, values and qualities concerning conservation, outreach, welcoming, community experience, and icon-status. When considering the mission statement for a building, it is important to include wording that promotes the building’s protection ideals that could be applicable to the building context. The statement could read “to provide a welcoming and safe, secure environment that embodies and promotes interdisciplinary communication and dynamism.”

2.2 Prepare a TVRA

Prior to the initiation of the design process, goals and a security brief should be established, along with project stakeholders, the project team, and the data and document control considerations. During this phase, a Threat, Vulnerability and Risk Analysis (TVRA) would be performed to determine the project’s security requirements.

Project Requirements

Once determined, the security requirements for the buildings should be incorporated into the Owner’s Project Requirements (OPR), which is subsequently supported by the Basis of Design (BOD) and follow-on design phases. The following are suggested phases of exercises to integrate protective design and resilience planning into the overall process, thus providing the best Return-on-Investment for the project.

Owner’s Project Requirements (OPR)

The Owner’s Project Requirements (OPR) is a key project-planning document that broadly communicates the owner’s goals and objectives, so they can be implemented into the design. Ideally, architectural elements associated with security should be communicated via the OPR. The OPR can also detail the functional requirements and expected uses of a project, including how it is operated, which will inform what security controls are to be adopted into the building. The architect and owner/developer should utilize the OPR as a checksum to ensure that resilience/security controls are adopted successfully into the project.

Examples of typical OPR criteria may include: Vehicle Security Center (VSC), a lobby screening, air blast performance, mass notification systems, spatial requirements, telecommunication redundancy, MEP redundancy, structural and force protection performance requirements and similar. Ideally, security controls are not correlated under a common topic, but rather integrated into the OPR, subdivided and assigned to each respective design team member for inclusion into the project.

Basis of Design (BOD)

Typically compiled after the OPR, the basis of design (BOD) is a narrative or rendering provided by the design team and vetted by the owner, which outlines the project’s design approach. Whenever possible, risk decisions should
be evaluated, and controls and options should be presented for review by the owner. As many protective strategies may exceed building codes, this is an important part of the project planning process because if protective controls are not designed carefully at the outset, they can impact the user experience and inflate construction costs for the building. Vague protective design criteria can be misinterpreted; thus, the project brief should illustrate and identify standards or guides for the design team, so they can become part of the overall process. The BOD may provide detailed requirements for screening, setback and stand-off distances, protective barrier elements and ratings, among others (see Figure 2.2).

Once the TVRA has been evaluated, controls can be selected, and the risk decision, or the degree and nature of the mitigating measures to be implemented, can be communicated among building stakeholders.

**Data and Document Control Considerations**

As digital technologies are increasingly incorporated into the design, construction and operation of the tall building, the architecture, construction and engineering industries will encounter greater flexibility and an enhanced capability to collaborate. To take full advantage of these capabilities, openness and transparency will be required, as well as the sharing of detailed models and large amounts of digital information.

The lifecycle management of tall buildings is also evolving, which presents additional sensitive information, including product types, model numbers, surveillance footage, network internet protocols and other previously unavailable data. There is also a significant amount of information involved throughout the design process, which includes multitudes of copies, reproductions and other data. The increasing use of, and dependence on, information and communications technologies can also mean an increase in vulnerabilities that can compromise the controls and protective strategies implemented to reduce risk.

Data aggregation may arise from either accumulation (the volume of data that can be compromised) or association (the relationships between data sets that increase the sensitivity of any compromise), or from both. Data aggregation has the potential to provide an external party with a nuanced understanding of the built asset and the relationship of individual assets within it. For example, knowing
3.0 Assessing Security Risks

3.1 Approaching the Assessment Process

Assessing security risks to the resilience of a tall building requires a review of the tall building’s assets and the hypothetical threats that could occur and their relative impact to the asset. Determining impact and corresponding controls is a somewhat subjective process, but should ideally blend a quantitative and qualitative assessment process, which will each provide unique insights that will inform a comprehensive picture.

A quantitative assessment will offer hard numerical data, which can easily translate to different business and operational systems within the building. Because it measures and models, it also presents a finite objectivity or objective range for threat potential, if the risk scenario lends itself to such an analysis. Additionally, metrics are less likely to create disagreements during review, and can influence the degree of investment stakeholders are willing to make in a security program. An example of some quantitative data relating to tall building security would be the monetary value of a sensitive asset, and the costs that would be incurred to replace or repair it if there was a breach in security that caused it damage. Another example might be the average number of people that pass through a tall building over the course of a year.

A qualitative assessment offers additional scope and benefits, the most salient of which is that it can be performed more quickly and more easily (if the resources available are sufficiently prepared) than a quantitative assessment. Additionally, by moving away from hard data, a qualitative assessment provides an opportunity for the organization to modify the assessment process.

3.2 Threat, Vulnerability, and Risk Assessment Deliverables

Threats may range on a spectrum from a low to high likelihood. One goal of the threat, vulnerability and risk assessment (TVRA) is to classify these threats based on their probability, criticality, and the impact and severity of their consequences, so that informed business decisions can be made. Regardless of the process, the primary assessor team will gather data and information from the tall building and familiarize themselves with the anticipated function, use and vehicular and pedestrian circulation for both the exterior as well as the interior of the tall building with the subject matter expert (SME) team. It will be critical for the assessors to understand where public spaces end within each project, e.g., front of house (FOH) as opposed to back of house (BOH) in a restaurant or other hospitality venue within a skyscraper (see Figure 3.1).

This will greatly aid in security planning by informing where secure spaces begin, along with their associated egress routes.

Figure 3.1: A quasi-public space might be a lobby-level recreational area that allows public access, but is contained within a private building.
numerical value (i.e., the higher the number, the greater the residual risk). This data should be provided alongside an associative description of the impact on the assets, including people, building and business operations), which would include the estimated time required for restoration, rebuilding or recovery. Without a narrative identifying the associative score, or classification, the above criterion provides little value to the person reading the TVRA.

**Report Contents and Criteria**

The objective of a TVRA is to identify the design basis threat(s) (DBT) and ensure the design is scalable and flexible enough to address threats with operational and tactical procedures if the need arises.

The TVRA analysis should ultimately produce a narrative report that examines a broad number of natural disasters and man-made threats. The evaluation of natural disasters should be context-appropriate, taking into account location, weather patterns and climate. The level of threat these events present will vary depending on this contextual analysis, e.g., a tall building near or in a desert climate will place a higher risk on sandstorms than a building in an area affected by a monsoon season, which should be more concerned about and more prepared for flooding. Other events might include earthquakes, lightning strikes, fire, and snowstorms. Man-made events can exist on a large scale—such as the threat of an air blast that may be vehicle or pedestrian-borne, or on a more internal scale, such as workplace violence or personal property theft. Other man-made events could include the effects of civil unrest, cyber-attack, power failure, and insider (sabotage) attack.

While some of these events are minor in terms of the tall building’s overall risk, they can have negative impacts on staff, residents and visitors, which can have a commensurate effect on the owner’s reputation, litigation, insurance and leasing. While threats are evaluated, tall building vulnerabilities should also be examined, especially critical business items and the reduction of single points of failure.

The TVRA is a snapshot in time; it should be a narrative document in a draft format that has the following minimum components: executive summary, the methodology used, time-frame, sources, crime, terrorism concerns, identified threats and vulnerability review. It should also contain subdivided security elements, including technical, operational and architectural controls, and overall risk assessment and treatments that should be given the most consideration, as well as a conclusion and an appendix.

Vulnerabilities are different from threats in that vulnerabilities allow a threat to occur. For example, a vulnerability in the electricity supply could create an impact on other assets. With threats and vulnerabilities identified, the TVRA should also address potential controls through architecture, technology, and operations for inclusion into the project. Once the tall building is operational, these controls should be incorporated into policies and procedures.

The strategy should provide a layered approach to resilience and should also make suggestions toward proactive and reactive controls. For instance, the TVRA should examine egress, mustering points in the event of an evacuation, fire protection, armed attackers and emergency vehicle access.

Ultimately, the TVRA should introduce controls that would supplement an operational resilience program and should be broad enough to deter, delay, detect and respond to both opportunistic and determined attackers. For example, if a criminal were to use false emergencies to gain unauthorized access, or an attacker were to use muster points to proceed with secondary events.

The output of the TVRA documentation and client decisions should be supplied to the design team, so that informed decisions can be made regarding the level of risk assumed. That way, the desired controls for the project can be incorporated into the design process as soon as it is practically possible, saving time and resources.

### 3.3 Threat, Vulnerability, and Risk Assessment Challenges

There are a significant number of challenges that can arise during the TVRA process, and these mainly arise during scheduling, e.g., when to perform the TVRA in the design process, as well as coordinating it with changes that occur from concept to building completion. Other areas that tend to be challenging include environmental modifications and liability.

**Scheduling and Planning**

Completion time is one such challenge, as the TVRA can be a time-intensive process, and its completion may not align with the design schedule. A realistic and appropriate time frame should be allotted for in the design schedule, ideally before any major project steps have been taken because the TVRA can initiate changes in the design, which may require additional time. The timing is very important, as the TVRA is more impactful earlier in the design process, since opportunities in the design can be more easily incorporated as guiding strategies and controls in the Basis of Design (BOD) / Owner’s Project Requirements (OPR). Specifically, the concept design phase is a logical starting point for general threat analysis; however, explosive consequence analysis should occur.
A protective design should be economically viable and operationally practical in order to effectively mitigate identified threats, while retaining maximum building usability in all circumstances. The objectives of the overall security strategy, to be developed in conjunction with the protective design, are the protection of life, protection of properties and premises, and the protection of the client’s reputation and their core values. The strategy should also aim to prevent crime, reduce interruptions to business, and to preserve essential business services. Undesirable events can be mitigated by either minimizing or reducing the likelihood of the event, or by reducing its impact on the assets.

4.1: Design Phases: Deliverables and Tasks

Design flexibility will ensure a resilient tall building, securing the operational environment and applying international best practices to enable a successful operational capability, which maximizes the delivery of a tall building’s energy efficiency. The objective of a security strategy is ideally implemented throughout the tall building’s project life-cycle but ideally includes certain tasks and deliverables at each phase of design and construction.

Overall Goals

While the initial intent of the security strategy is to deter opportunistic or determined attackers, the architectural controls must offer opportunities to delay the aggressor from gaining access to their identified target, and these goals should be defined and included in the strategy. The longer someone who is attempting a criminal act can be delayed, the more opportunity there is to detect and respond to the incident, thus minimizing its impact.

Programming/Concept Design Phase

During this phase of design, the building’s functional programming and blocking for the anticipated uses is established. The programming phase should include a high-level internal self-assessment of the project and is generally the period where the TVRA is most likely to be implemented.

With threats and vulnerabilities identified, the TVRA should also address potential controls through architecture, technology, and operations for inclusion into the project. At this stage, the security plan should pursue a multipronged approach to resilience planning and should determine egress and muster points, as well as fire escape routes and entry points for emergency vehicles. For instance, the TVRA should examine egress, mustering, fire protection, and emergency vehicle access. Ultimately, the TVRA should introduce controls that would supplement an operational resilience program and should be broad enough to deter, delay, and detect someone in the opportunistic/determined attacker process. As mentioned, the TVRA should inform architectural controls by supplying a summary of potential threats, which include blast, theft, climate disasters and others. Blast threats should include the possibility of vehicle-borne improvised explosive device (VBIED) / person-borne improvised explosive device (PBIED) in relation to the result of workplace violence, civil unrest, cyber-attack, power failure or insider (sabotage) attack. Architectural controls and programming should take into account the risk of other threats to their reputation and the well-being of occupants, such as maintaining surveillance to avoid the risk of theft to personal property of staff and visitors. Natural effects such as inclement weather, flooding, lightning strike, earthquakes and sandstorms should also be accounted for (see Figure 4.1).

There are specific criteria that should be examined and considered during the implementation of any protective controls or countermeasures. These criteria should include the validity of the control’s function, and the reliability of the control, or examining whether the control will do as intended when active. Additionally, the control’s expense should be examined from several angles. Lastly, the control’s potential impact on the event, or the delay or elapsed time required to install the control, should be taken into account.

Depending on the overall design process, the BOD is likely completed at this phase, and has been given to representative design team members.
for inclusion into their respective parts of the project. At the end of the programming and design phase, several security action items should be reviewed. Principally, the tall building’s functional program and operational process should be established, and areas of use should be anticipated. The TVRA should be complete and ready to implement. After careful analysis, risk decisions about the management of the security risk by the client and stakeholders should be understood, at a minimum, before moving on to the next phase of design. The siting of traffic, architectural and other design modifications, such as setback/stand-off, and vehicle approaches and drop-offs should have been identified, as well as vehicular and pedestrian circulation routes and lobby areas. Consideration should also be given to assist in space planning, provision refuge areas, security control rooms, training rooms, crisis management rooms, security equipment storage and critical assets.

Critically, security zoning diagrams should be prepared, with components that include security zoning drawings, which are a two-dimensional plan view of what space is considered to be public, semi-public, semi-private, private and restricted by color code, so at a glance, it can be seen where non-public and sensitive areas/spaces or rooms abut to public areas. These zones are a guide to developing the tall building’s security plan, and they are generally linked to physical barriers and access controls that assist in graphically representing and evaluating these areas throughout the planning process, further supporting asset identification, while potentially incorporating security elements. Ideally color-coded zoning and strategy drawings should accompany the BOD to highlight public/quasi-public and other adjacencies, so life, safety, egress and usage conflicts can be readily evaluated (see Figure 4.2). Lastly, structural performance criteria requirements should be provided before moving on to the schematic design phase.

**Schematic Design**

This likely reflects the last opportunity to introduce architectural modifications to the program cost-effectively. At this phase, on-going consultation with the façade consultant, structural engineer, and all team disciplines should have occurred. The design team should be utilizing the BOD as an integral planning document for other facets of the building. At this phase, action items should include an updated BOD document, as required, as well as preliminary calculations for air blast effects, which, if required should be submitted to the structural and façade teams. Preliminary security systems drawings based on security zoning strategy drawings from the programming design phase should be completed. There should be a spatial allocation identified for security support, which can include a control center, locker room, roll-call room, training room, crisis management room, security equipment storage, and others, as required by the functional requirement for the project. The lobby and public amenity design should be identified in this phase, and coordination with lighting, landscape and traffic consultants should occur either at this phase or earlier, if possible. Additionally, the structural performance criteria that were provided during the programming/conceptual design phase should be reviewed and confirmed.

**Design Development**

The Design Development phase is when the introduction of architectural and operational security programming becomes more financially restrictive to implement. Architectural security programming elements, such as setback and stand-off; and vehicle and
This section refers to the infrastructure and roadways that surround a tall building, and emphasizes how to build resilience into these elements to maximally deter attackers before they are able to even access the building itself. By being judicious about avoiding certain landscape features (depressions, sunken areas) and leveraging others (berms, tree cover) buildings can increase the ability of occupants to naturally surveil the scenery, issuing a major deterrence to potential criminal activity (see Figure 5.1).
Avoid sunken/depressed areas

Call for assistance device

Demand Lighting

Fast-draining system minimizes attractive nuisances

Figure 5.1: Model of a tall building representing how exterior and landscape features can be designed to assist in protective design. © Affiliated Engineers, Inc.
6.0 Tall Building Interiors

6.1 Spatial Planning Considerations

Spatial planning requirements that are security and resilience specific can create significant issues in the design process, if not incorporated early on. The following is not an exhaustive list but is meant to catalogue certain areas that have created challenges for design teams in the past.

Direct Space Planning

Consideration should be given to both the space programming and planning for protective amenities within the building. At the beginning of the tall building planning, spatial areas for security/tall building resilience should be identified for inclusion into the project. Failure to incorporate these areas at the outset of the project may limit their ability to be included in the project later on. Items for consideration may include, but are not limited to, panic/safe rooms; dedicated, high-speed elevators; vehicle entrances; and roof-top access.

In many instances, tall buildings are owned through a corporate consortium or directly by a prominent VIP. These persons shall require additional security measures, which may necessitate dedicated high-speed elevators, hardened compartmentalization or the creation of individual panic/safe rooms.

Commonly these requirements are not discovered until the near-conclusion of the design, which can create significant challenges depending on the threat environment surrounding the high-worth individual. When high-worth individuals are involved, review programming elements to ensure structural and floor space requirements are incorporated into the design. If dedicated, high-speed elevators are required, determine the origin points and drop-off locations for these elevators. If protected spaces are required, consider shelter-in-place/panic rooms and the degree of protection that might be required. Additional vehicle entrances and storage should also be considered—if there may be a need to secure vehicles, consider how many can be accommodated, and where they would be located in the building. All entrances, including secure and public entrances should be accounted for early in the design as well. If the building is expected to need a place for helicopters to be stored or land, a “touch and go” and landing pad functionality should be explored and planned for.

6.2 Security Control Room

A Security Control Room (SCR) is required to monitor, control, communicate, coordinate and dispatch security services, as well as provide information and situational awareness to staff. The SCR should be isolated from all other activities and have a sound transmission class (STC), which is a rating of how well a wall diminishes airborne sound, of at least 55. The SCR is the command, Communication and Control (C2) for all criminal and emergency response and mitigation activities. Therefore, it should be designed to function during emergency, evacuation and threat scenarios. The control room should be designed with ergonomics in mind to limit repetitive stress injuries.

Typically, the control room would be located on a lower floor, away from primary or tertiary assets, to promote survivability, as well as to manage an incident away from egressing pedestrians. The control room should be placed in a location where column obstruction can be minimized, and clear view of monitors/video walls can be maintained. While natural light is advisable, it should not include floor to ceiling windows, and the room should generally be constructed with limited glazing. A backup/redundant control room may be beneficial depending on the security requirements of the building. Alternatively, a management space, such as conference room, could be utilized as a control room if adequate infrastructure is included in the design of the space. An SCR diagram identifies the relationships, and interdependencies necessary to determine the minimum spatial criteria for an SCR (see Figure 6.1).

These relationships and interdependencies may include equipment rooms, management offices, restrooms, security consoles, uninterruptible power systems, emergency power systems and locker rooms.

SCR Adjacencies

A properly designed and sized equipment room with adequate space and amenities will be required, not only for the current security technology, but for the expansion of these systems over time. Coordination of telecommunications, HVAC, and electrical is instrumental to the program’s ability to grow.

A security manager’s office allows law enforcement agencies to discuss items with discretion among themselves and away from other types of personnel; therefore, a minimum of two management offices should be provided near the SCR. One office would be dedicated to a security director and the second office would be utilized for all three shift supervisors. These areas are instrumental for writing reports and should be considered an operational base from which to service tall building projects. These offices should be in the same area, or within proximity to each other and should be designed with STC on par with that of the SCR. Additionally, having restrooms
and kitchenette facilities near the SCR prevents staff from being away from their duties for extended periods. Consider areas that could also be used for ad-hoc rest areas during crises.

**Security Console Sizing and Technology**

The console’s size should be commensurate with the duties and quantity of the staff required, as well as being planned to have the appropriate capacity for the identified technological elements that will optimize its function. As such, the design of the console will be best served with an early identification of these specifications. Items for consideration include the number and size of the monitors required for viewing, and whether a video wall or radio dispatch will be desired. The degree to which tall building operations are integrated should also be evaluated, as this may affect the design and location of the console. Consider whether facilities and information technology will share space, and if so, how this will affect the security of these locations and the sensitive information potentially shared there.

**Uninterruptible Power System (UPS)**

These systems are mission critical; therefore, to maintain operation, a standalone UPS system may need to be provided. The UPS shall hold electrical loads related to security equipment until which time the emergency generator can provide supplementary power for extended periods of time, which would be dictated by the OPR.

**Emergency Power System (EPS)**

Several critical building systems are connected to the emergency power system (EPS), including the fire alarm system, elevators, building management systems including HVAC, access control and any other system deemed critical by building owners and managers.

**Additional Security Areas**

An area should also be dedicated to the production and dissemination of identification badges (see Figure 6.2). Considerations should be given to a small satellite area within the tall building to offer convenience to tenants requiring an interface with security. Locker rooms, specifically for the use of security staff, offer facilities for staff to change, store clothing and shower, and would be an added convenience and measure of security. A multi-purpose room should also be provided where information, such as law enforcement reports and notices can be distributed to security staff. In addition, this area can serve as a conference area and, most importantly, an emergency operations center. Necessary systems such as satellite TV, a surveillance feed, a separate phone line, and storage for equipment should be provided in the event of an emergency. In some instances,
7.0 Tall Building Security Technologies

Technology complements operational resilience and can positively or negatively influence architecture. While technology is one of the easier things to incorporate into a tall building program, a well-coordinated design can support a more unobtrusive environment when considered in the planning phase. Technology is most beneficial in support of situational awareness when coupled with an effective physical and operational security program. In many circumstances, having a clear security strategy minimizes the overuse and reliance on security technology, and equally, reduces the burden of maintenance costs and equipment.

7.1 Emergency Communication

Mass Notification
The US National Fire Protection Association (NFPA) has introduced mass notification requirements within NFPA 72 which provide the opportunity to redirect egress routes, although other fire protection agencies can and should be referenced depending on project location. Consideration should also be given to how easily first responders are able to access the building during emergencies. Egressing persons should not impede first responder access to the building when gathering at muster points. A mass notification requires a robust integration via information and communications technology (ICT) systems to communicate to tenants, residents, and patrons during an emergency through a variety of interfaces. Mass notification systems intersect with planning for extreme threats, as the purpose of these systems is to redirect egress routes or provide alternate instruction such as lockdown, shelter-in-place and incident management messages, indicating the arrival of law enforcement or when it is safe to exit.

Mass notification can include simple overhead paging and voice evacuation audio systems or can be far more robust including phone / voice over internet protocol (VoIP) systems, which allow communication via an integrated speaker on a telephone handset. Messaging systems (televisions, clocks, or other text-based systems), could also be utilized. These systems would be integrated with ICT/audiovisual networks and display pre-written messages via static or scrolling screens and could be used in elevators, observation areas, cafés, screening areas or via interactive wayfinding. Exterior large format messaging boards could comprise interactive wayfinding, traffic signs, billboards, or LED walls, which are intended to communicate any emergency and other information, such as building closures, to minimize incoming traffic and pedestrian volume to tall buildings. These systems might indicate vehicle screening locations, roadways, and parking/dock information. Internet home pages can also be incorporated into a mass notification plan by leveraging an interface that can redirect web pages to communicate during an emergency event. It would also be possible to communicate to visitors and tenants through mobile phones by using simple messaging service (SMS), although this is contingent upon distributed antenna systems/bi-directional amplifiers (DAS/BDA) and repeatability throughout the building (see Figure 7.1).

Call for Assistance
Call for assistance (CFA) devices, also known as blue-light or "code-blue" devices, are free-standing structures that are designed to visually convey where assistance is needed (see Figure 7.2). When effectively designed, these devices can coordinate with wayfinding packages, and include maps and other orienting visuals. Typically, CFA devices are strategically placed near points of egress that can include elevator landings, stairwell access, ramp access and pedestrian pathways.

Figure 7.1: Mass notification systems can disseminate emergency information through intercoms, computer monitors and smartphones, depending on their configuration.
Once activated, CFA devices can alert authorities, as well as release a powerful strobe light with the intent of drawing attention to the area. All CFA devices should therefore be monitored with surveillance cameras. The location of these devices should be planned while considering the surrounding environment, inclusive of sightlines, landscape features, lighting and proximity to nearby buildings. Ideally, building occupants will have a clear line of sight or direct access (such as via an adjacent stairwell or exit point) to at least one CFA device, particularly in places that tend to be desolate at night, such as parking lots.

**Intercoms**
Intercoms can be cumbersome to incorporate for design teams, and their need is not typically evaluated until the end of the project. As it relates to the tall building, the primary concern is where to mount the intercom. Ideally, intercoms should be placed in accordance to ADA/MIP requirements, which precludes façade mounting. Considering whether intercoms are needed early in the process can allow the design team to identify an area for mounting, while maintaining aesthetics at the building entrance.

Separate/dedicated intercoms may be required and may necessitate special, protection interfaces and systems. These can include elevator intercoms, two-way voice intercoms, and area of refuge intercoms.

### 7.2 Surveillance Systems

**Field of View**
The field of view (FOV) for each camera will vary based on the camera type, inclusive of lens selection, video imaging, sensor/chip specifications, mounting height and surrounding lighting conditions. When considering camera fields of view, the design team security consultant should provide the camera’s purpose and scope which will inform the need for architectural modification. Surveillance images should always be evidential in nature, and the camera’s monitoring purposes and outcomes include monitoring, detection, recognition and identification.

To properly achieve these outcomes, consider the monitoring context when discussing the placement of the camera (see Table 7.1). Detection is more broadly defined as the ability to identify actions, such as someone climbing over a wall or breaching a door. Considering what needs to be detected will also help determine the appropriate field of view to capture. Detection should be as enhanced as possible to provide characterization, such as height, weight, complexion, clothing and other identifying characteristics. Facial recognition data can be used for subsequent forensic investigation. Identification also relates to the ability to read license plate information, which will typically require a camera to be mounted lower. The design team should incorporate architectural programs to support camera surveillance at all vehicular entry/exit points to include driveways, elevators and general lobbies, reception/security desks and other areas as described in the OPR. In these instances, the camera should not be mounted higher than 2.7 meters (9 feet), or similar regional code. Image quality is measured against the Rotakin test, which was developed to evaluate how accurately CCTV monitors could capture identifying features of intruders, and thus to develop screen height standards.

**Camera Technology and Placement**
Cameras are now able to capture higher-resolution images, and paramorphic, multi-lens and panoramic surveillance cameras can capture large...
8.0 Precautions for Extreme Threats

Extreme threats can either be man-made, accidental or natural, and proper controls need to be evaluated for their mitigation. As it relates to natural and accidental threats, building code will likely address the requirements for the project to some degree; however, it may not consider future trends or subsequently elevated performance requirements. As such, it is important that these threats are assessed and understood as early as possible through the threat, vulnerability and risk assessment (TVRA) process. Extreme threats are those that are singularly focused and require additional controls to manage, and include events such as chemical/biological, radiological/nuclear (CBRN) events, elevated ballistic attack, explosions and arson.

8.1 Chemical/Biological and Radiological/Nuclear (CBRN) Threats

The threat posed by CBRN materials encompasses a range of hazards to health and business continuity. Unlike an explosive event, it may not be immediately clear that a serious chemical, biological or radiological material event has occurred. A chemical threat consists of synthetic chemicals, referred to as toxic industry chemicals (TIC), which are used in legitimate manufacturing processes, and thus stored in large quantities (see Figure 8.1). Chlorine, for example, which is commonly used to disinfect pools and drinking water, poses a threat in its concentrated form. If exposed through accidental or purposeful means, these chemicals can present severe hazards to human health. Chemical warfare agents (CWA), are synthetic chemicals specifically used to harass, harm, incapacitate or kill humans, and which can disperse quickly, or linger and cause persistent or permanent damage, depending on their makeup and concentration.

Risk management for biological threats is rooted primarily in early detection, rather than prevention. However, foodborne biological threats such as ricin, naturally occurring in castor beans, and botulism, spread through the improper handling of perishables, can be managed through compartmentalization and control of food preparation and dispensing areas. Bioterrorism concerns the intentional deployment of hazardous bacteria or viruses, such as anthrax or plague.

Early adoption of the Owner’s Project Requirements (OPR) should communicate the intent to manage the threat to the architectural and mechanical team, and will require:

- Airtight façade/closed façade (operable windows not permitted)
- Airtight floor-to-ceiling partitions
- Airtight ducting/plenums
- Positively pressurized building
- Building zoning for shelter-in-place considerations
- Dedicated air handling units
- Negatively pressurized lobby, dock and mailroom.
- Hazardous materials located far from elevator banks
- Air louvers located as high as practically possible (see Figure 8.2)
- Dampers on air intakes
- Ability to recirculate air
- Ability to shutdown air handling system when threat is expected
- Carbon/MERV filtrations, requirements and accessibility for hazardous materials
- Capability to over-pressurize/ purge systems
Radiological/Radionuclide
Radiological/Radionuclide relates to the combination of an improvised explosive device (IED) with alpha, beta or gamma energy sources, with the purpose of irradiating a large area following an explosion.

Technology exists to detect unsealed radiological sources and can discriminate these from normal background radiation. While costly, these systems can provide early detection and directly relate to staff’s ability to respond quickly and efficiently, potentially reducing damage, business interruptions and injuries or casualties.

Nuclear Material Device
A nuclear material (NM) device is composed of weapons-grade uranium or plutonium, which creates a rapid release of energy via a fission or fusion reaction. The main threats to humans resulting from a nuclear explosion are blinding light, a blast of intense heat, a strong blast of air, and the resulting nuclear fallout, which consists of irradiated, airborne material that can cause severe illness and death.

NM material would typically be contained in a sealed source, so a specialized detector that identified gamma or neutron energy could be used. However, the detection range is limited, and the specific nature and severity of this threat makes the controls fiscally challenging to implement, and thus is outside the scope of this document.

8.2 Elevated Ballistic Attack
The mass shooting that occurred on 1 October 2017 from the 43-story Mandalay Bay Resort in Las Vegas, Nevada, shared similarities with the University of Texas tower shooting when an assailant fired 150 rounds at the public from an elevated position.

Protection for these types of events relies on comprehensive planning and precautions, and requires the consideration of several factors, including the immediate surroundings of the building and whether large occupancies are expected. Additionally, consider and account for any potentially prominent individuals that may be on-site.

While there are several controls that are possible, the most cost-effective methods affect the design of the building and its surrounding landscape, and thus benefit from early incorporation. These include obscuring the target with screening, such as tree canopies, and shading to make it more difficult for a potential shooter to take aim from an elevated height (see Figure 8.3). Hospitality areas should additionally be planned away from vantage points where people could congregate.

8.3 General Blast Loading Considerations
A blast load is created by an explosion and is unlike any other threat the project may experience. The characteristics of blast loads are very short in duration, but high in magnitude, and typically are localized to a small area of the building. These events differ from an earthquake in that earthquakes are of a lower intensity, but much longer in duration and affect the whole building, rather than a smaller portion of it (see Figure 8.4).

Establishing Risk Tolerance
Ascertaining the exposure of a blast will require, integral to the TVRA team, a blast consultant to evaluate the building’s vulnerability to blast effects. As part of this process, guidance to the design team regarding the level of protection/classification to be assumed for the project is necessary.
This final chapter features a narrative summary and restatement of the text, to serve as a concise overview for tall building stakeholders, and concludes with some future considerations as technology, architecture and other cross-disciplinary fields continue to evolve. Beginning with site planning and Crime Prevention Through Environmental Design (CPTED), which concerns how environmental features can deter crime, this summary then moves into the identification and protection of different asset classes against different threat levels and events. Finally, a section on designing the lobbies of the future discusses new challenges and opportunities that may arise for resilience planners due to increasingly sophisticated access control systems.

9.1 Site Layout

The process of site planning consists of functional programming first, followed by traffic planning and CPTED (see Figure 9.1). While not mutually exclusive, these comprehensive exercises can support more robust planning. First and foremost, applying the aspects in adjacency planning, the locations of entrances, parking, loading dock and critical infrastructure should be identified and coordinated with other design components and direction.

This security philosophy utilizes architecture to influence an aggressor’s behavior. One of the key components to modifying an aggressor’s mindset is to increase their perception of being detected during attack planning or decreasing their perceived level of success; the most beneficial is through enhancing witness potential. Witness potential can be enhanced by increasing lines of sight on the property, illuminating obstructions that could limit witness potential, and decreasing blind spots. Beyond witness potential, there are environmental factors that can also limit an opportunistic/determined aggressor’s activities. One such method is eliminating access to the underside of stairwells at grade or exit alcoves. Other attractive nuisances such as the use of water features and/or topography may increase the likelihood of misuse. Climate is an important factor to consider, especially in areas with extreme hot or cold. This may impact design considerations such as the distance between the vehicle drop off and lobby—with the need for stand-off distance balanced against user comfort. Less obvious may be the position or need for a smoking area. Should the latter be positioned in an inconvenient or unfavorable location (lack of shade or shelter from inclement weather), an alcove may invite unauthorized access. Other environmental concerns include the introduction of materials that could be used as weapons, such as river rocks within a water feature, or seating areas that are not secured or removed from patio areas or the layout of the building may facilitate scaling by urban explorers. Another component to modifying an aggressor’s behavior is to enhance property setback or stand-off distance. While many designers exclusively associate setback and stand-off to blast, there are other benefits. One of these key benefits is to increase the distance from the façade, however, it also can delay access to the tall building. The setback distance can be comingled with psychologically expected paths of travel, which if otherwise unused would appear suspicious, and increase a witness’s detection of a breach.

As it relates with blast, the site should maintain a finite set-back distance through an operable barrier system, which is controlled from a central location. These locations should include screening, parking, and most importantly a reject lane to redirect vehicles that are not expected at the site.
Lighting is one of the greatest aspects of limiting both opportunistic and determined attackers. Simply, if the attacker cannot be seen, nor can they see or perceive the witness, then the modification of the behavior is unlikely to occur. Current trends are moving towards the limitation of lighting to facilitate mood or maintain energy conservation goals. When considering lighting, the use of whiter types of LED lighting with a temperature between 4000K and 4500K should be evaluated. When there are mood aspects that need to be maintained, a lighting program can be developed that includes demand lighting to address higher threats. Demand lighting is lighting that is not normally used but can be turned on to supplement security during specific instances. Beyond lighting, other technologies, such as Forward Looking Infra-Red, infra-red lighting and thermal imaging can be used to supplement or manage challenging environments where lighting is not possible.

While lighting is important, witnesses need to know when, and when not to challenge someone that they think may not belong at the facility. The use of wayfinding can inform opportunistic and determined attackers about potential targeting, but signage such as “authorized personnel” can additionally support and enforce witness potential (see Figure 9.2). Wayfinding can get those that are unfamiliar with the tower to a desired location efficiently and effortlessly. This type of wayfinding can also assist in managing frustration, thus limiting negative interactions with on-site tall building staff that otherwise could unnecessarily escalate. Finally, and most importantly, wayfinding supports first responder access to the site by numbering doors, locations, and identifying how to access the site as efficiently as possible.

In many instances, fire access shall be required around the entirety of the building. Fire access can be supported through a variety of means inclusive of roadways to discreetly provide access. When planned early on, this access can be comingled with other services identified above for a more seamless integration of the roadway network.

9.2 Adjacency Planning

Adjacency planning relates to both exterior and interior aspects of a tall building. The key components of adjacency planning are the identification of assets, critical infrastructure and the functions and programming required to create an environment that promotes resilience. Architectural, site or functional planning rarely considers adjacency planning unless it is mandated by the owner or other local requirement. Adjacency planning, when completed early in the process, has limited impact on the project. Examples of adjacency planning for resilience include internal programming, people, and other elements. Internal programming deals with the relationship of different functions within the building. For instance, creating egress routes that pass through a compartmentalized/secured area can compromise existing security measures. When considering internal spaces, determine which areas are secured and where those areas intersect with required egress pathways.

An elevated garage that has centralized emergency stairwells that also service upper office floors is challenging. Ideally, tall buildings should separate exit stairs from inter-circulation stairs, but when this is not possible, additional stair compartmentalization may be required.

Another aspect of adjacency planning concerns people. Careful planning must be conducted to identify transportation and exit routes for large crowds. Whenever there are large groups of people, the potential for attacker targeting is possible. As such, areas
About the Authors

Sean A. Ahrens
Chair of the CTBUH Security Working Group

Sean A. Ahrens is a Security Market Group leader with expertise in access control and force protection systems. With over 23 years of security leadership experience, he has participated in many standard-setting panels at Underwriters Laboratories (UL), Security Industry Association (SIA) and most notably, the ASIS Commission on Guidelines. Ahrens has provided planning, design and construction administration for government, public, international and private entities. He is well-versed in the various trade and local authority issues impacting projects and has been responsible for providing security threat and risk analysis, contingency, site building configuration and anti-terrorism/force protection planning for some of the largest projects globally.

Caroline Field
Arup

Caroline Field has 25 years of experience designing and protecting the built environment, including the Millennium Dome (O2 Arena) in London, The California Academy of Sciences in San Francisco, and The National Geospatial Agency Headquarters in Virginia. She worked closely with the US Federal Government on projects that have mandated blast requirements before returning to the UK to lead the Risk and Resilience Team at BuroHappold Engineering. She recently re-joined Arup to lead one of their Resilience Advisory Teams as an Associate Director. Field is a Chartered Engineer with the Institute of Civil Engineers in the UK, a Principal Member of the Register of Security Engineers and Specialists, and a member of the American Society of Civil Engineers.

Dedication
Sean A. Ahrens

This document is dedicated to my loving family: in memory of Jerry, my father, who tirelessly taught me how to be a man of excellence, and about the “bell-shape” curve. To Anne, my mother, for always being there and fighting for my chance to do great things beyond the limitations that others had set for me. To Kathy, my mother-in-law; To Heather, my loving wife; and of course, my amazing children. Thanks for being ever-present—always cheering and patiently waiting for me to complete this effort.
The field of Tall Building Security has become increasingly important in recent decades—as the number of skyscrapers increase, so too do the nature of threats that must be considered when planning for their resilience. The effects of climate change have increased the frequency and intensity of storms, while advances in digital technology have created new opportunities for automation that simultaneously increase vulnerabilities to hacking and cyber-attacks. Globally, the threat of violence in both public and private arenas must also be planned and prepared for both structurally and with appropriate evacuation strategies.

To efficiently and adequately anticipate, prepare for, and execute tall building security plans, a complex roster of factors must be evaluated from the outset of the tall building's conceptualization. Within this guide to tall building security and resilience, factors including everything from site context to asset identification to access control restrictions and placement, are reviewed to offer a reliable reference for tall building stakeholders that wish to secure their building against a wide variety of threats.

This CTBUH Technical Guide is a product of the CTBUH Security Working Group which is composed of active professionals in the field, and aims to provide tall building architects, developers, contractors, occupiers, lighting consultants, security professionals, landscape architects and a wide variety of other tall building professionals with the resources to build a customized, step-by-step resilience plan for their respective projects that will empower them to understand, prepare for, and guard against context- and project-specific threats, with the ultimate aim of enhancing the security of the tall built environment in the most efficient and effective manner.