Protecting against terrorist attacks for urban transportation projects

G. Katzman
*Arup Risk Consulting, New York*

Abstract

Arup has undertaken security risk assessments for designs and analyses of major infrastructure projects. As part of engineering team efforts, Arup Risk Consulting performs risk assessments and supports decision analyses for threats of explosives and chemical, biological or radiological agents for buildings, urban transit centres, bridges, public bus systems and airport facilities. The work is timely because of attacks in recent years on buildings in New York City and Istanbul, and on transportation systems in Madrid and Tokyo. This paper will describe the challenges of protecting public infrastructure against terrorist attacks, and the approach taken by Arup for performing threat and risk assessments and interacting with clients and team members. The assessments lead to risk rankings and to the creation of lists of cost-effective mitigation measures recommended to the design team and client. These measures can have minimal impact on design principles and budget if the studies are performed early. The efforts can be most successful if they engage the team of designers, and if the client makes security a priority for the overall effort.

*Keywords: threat and risk assessment, protective design, infrastructure protection.*

1 Introduction

The tragic events of September 11, 2001 (9/11) changed building design forever. Balancing aesthetics, openness and other design goals with safety and security is now a common challenge. The comprehensive understanding of risk is crucial to achieving this balance.

Pre-9/11, local and national building codes had evolved to ensure protection for building occupants against known hazards. Specific code requirements were
often developed in response to behaviour observed in extreme natural and technological events like fires, earthquakes, high winds or floods. For example, measures to make tall buildings safer under strong corner winds were first added to codes after dangerous performance was predicted for the Citicorp Center in New York City (see Katzman et al. [1]).

Post-9/11, owners, tenants and the public globally are concerned with new hazards: deliberate attacks of bomb blasts, vehicle impacts, and delivery of chemical, biological or radiological agents (CBR). These attacks have low probability of occurrence, yet potentially catastrophic consequences. Many developers and owners today are weighing the costs and benefits of safeguarding their buildings against these extreme events. Most have little incentive to improve protection because codes do not specifically require it, and because return on investment through insurance premium savings is not guaranteed. Market-place benefits for security are not yet clear. A roundtable discussion was organised in New York City by Katzman and Meacham [2] in 2004 to get input from the real estate community on incentives for adding protection measures for buildings.

Meacham [3] describes the practice of design today as evolving to incorporate uncertainty about extreme event occurrence in addition to architectural and functional goals and in light of limited financial resources. A risk-informed performance-based approach provides a method for balancing these various competing objectives when designing for low probability, high consequence events. This paper outlines an approach for balancing objectives, using the design of an urban transportation hub in New York City as a case study.

2 Threat and risk analysis

A terrorist attack on a transit system can affect passenger life safety, system owners through lost revenue and cleanup expenses, and the community through loss of key infrastructure. Other groups can also be adversely affected by an attack. A threat and risk analysis (TARA) aims to safeguard against these negative outcomes in a cost-effective manner. The process allows for consideration of values and safety goals of multiple stakeholders.

Engineers define risk as the product of the probability of an extreme event occurring and the severity of the event consequences. Risk analyses can be quantitative or qualitative, relative or absolute depending on the level of analysis desired and availability of relevant data. Semi-quantitative methods are commonly used for transit system risk analyses on terrorist attacks when there is minimal historical data available to estimate the occurrence of attacks modes being studied.

Figure 1 outlines a framework for a risk analysis. The process consists of two main phases: risk assessment and risk management. The first step, risk assessment, requires an estimate of the probability of the external hazard occurring and a measure of consequence severity, or criticality, should the event occur. Criticality depends on both the desired performance of the facility, and the inherent resistance of its systems to the threats.
Once risk is understood, it can be managed. The decision of what level of risk to accept is made by stakeholders. If the outcome of the event is unacceptable, measures to avoid, mitigate or transfer risk are considered. To combat risks of terrorist attacks on a facility, options include both efforts to reduce likelihood of an attack, and to reduce criticality by improving the resilience of the facility. The current paper focuses primarily on engineered solutions that can be integrated into design.

Figure 1: Risk analysis framework for threats to buildings or infrastructure.

2.1 Risk assessment

According to Kaplan and Garrick [4], the risk assessment phase begins by asking three questions about the facility: What can happen? What is the likelihood that it will happen? What are the consequences of it happening?
2.1.1 Probability of threat
This first step in risk assessment is to determine the type of events, and their potential magnitude, to consider. For terrorist threats, it can be difficult to pinpoint type of attack to consider because new surprise tactics are possible and even likely. Probability of an attack is also challenging to estimate because there is limited historical data on terrorism occurrence. A list of threats and their relative likelihood however, can be put together based on review of previous attacks on similar facilities, and knowledge of potential aggressors. Factors such as symbolic meaning of the building, the ease of access to the facility, desirability or centrality of its location, number of people potentially affected, and nature of the commercial functions, can contribute to making the estimate.

For urban transit centres, the threat may be considered to be particularly high. In recent years blasts shook transportation infrastructure at the Atocha train station in Madrid and hazardous materials were released in the Tokyo subway system. Sites in Lower Manhattan were also targeted, which disrupted several subway stations.

2.1.2 Criticality of threat consequences
The second step is determination of criticality to the facility for the threats of concern. Criticality is a measure of both the desired performance of the facility by its stakeholders and its ability to perform as desired following an attack. Performance definitions may be set for the structural response to an explosive attack, the ability of mechanical systems to isolate a CBR release, or other criteria. Newly constructed areas can be designed with performance criteria, and existing components in renovation projects can be studied for their performance when subjected to the established threats.

**Performance** U.S. building codes aim to ensure occupant life safety. They prescribe design criteria to prevent substantial loss of life when subjected to natural and technological hazards like hurricanes, earthquakes, floods or fires. For terrorist attacks, codes offer little guidance on protection for people and against building damage or economic loss. Performance objectives established during the risk assessment can therefore focus on other considerations in addition to life safety, including: building structure and systems; neighbouring buildings and occupants; business operations; the environment; facility and surrounding access; and protection of key assets or historic fabric. Many stakeholders can help set performance objectives, such as owners and primary users, the community, and alternate transportation systems.

**Resilience** Resilience describes the ability of the physical facility to meet the performance criteria established for the agreed threats. It takes into account physical systems and occupant vulnerabilities. Familiarity of occupants with layout and means of egress, and certain design characteristics such as degree of structural redundancy or mechanical isolation, contribute to the resilience measure.

The various measures described in this section can be estimated quantitatively using an agreed metric, or qualitatively using careful terminology. Extent of structural damage, repair cost, likelihood of injuries or fatalities, and business
disruption time can be used as measures for performance. Various reference documents produced by U.S. government agencies provide guidance on establishing metrics for criticality determination, with some described in this paper.

2.1.3 Risk measure
Probability and criticality combined provide a measure of risk. When assessed for an entire facility, the risk measure reveals which components are most vulnerable and should be targeted for mitigation.

2.2 Risk management
Kaplan and Garrick [4] pose a second set of questions for risk management. What can be done to address risk? What options are available, and what are their associated tradeoffs? What are the impacts of current decisions on future options?

Risks can be accepted, avoided, mitigated or transferred, depending on stakeholder tolerance. For unacceptable risks, three main methods to reduce risk are possible: engineered design options; operational procedures; and financial methods such as insurance policies.

To determine which engineered solutions to incorporate, risk management efforts should lead to a prioritized list of recommended countermeasures. Measures for a transportation facility can cover almost all design disciplines, including: security systems; architectural layout; life safety planning; structural materials and schemes; mechanical and electrical building systems; and specialties of lighting design and acoustics.

Designs that incorporate risk-reduction measures almost always result in increased cost. The measures that are identified and incorporated early in the design process will likely be less intrusive and have lower financial impact. A life-cycle cost analysis allows owners to compare the cost to do nothing with the cost of countermeasures over the lifetime of the facility. A cost-benefit analysis provides a framework for prioritizing funding amongst various mitigation options.

3 Sample threat and risk analysis for a New York City transit facility
Infrastructure facilities are particularly challenging to protect against terrorist attacks because they are by definition open and accessible to the public. Densely populated urban areas are of concern because public transportation is most likely to be available there, making it a desirable target while also critical to the functionality of a region. These areas can also have many obstacles to adding protection, from street and geotechnical congestion to high real estate value. Multiple building types within dense urban areas further complicate a risk analysis because new, existing and protected historic buildings can have different
requirements. For an urban transportation hub, like in downtown New York City, many of these issues are critical.

Transportation security is a high priority for government agencies today. Yet benchmarking performance and design loads for terrorist attacks is difficult because the U.S. does not have a singular building code that covers protection for non-federal buildings. Various reference documents sited in this paper however, do provide some guidance in this arena.

Designs can successfully provide some level of safety to occupants if they incorporate protection measures, make riders aware of security concerns, and keep critical areas closed off from the public. A recent transportation facility in New York City designed by Arup included a comprehensive threat and risk assessment for the entire site, following the procedures described in this paper. The TARA considered threats to the facility not covered by building codes, primarily explosive attacks and releases of CBR agents. It led to a risk ranking and resulted in a list of cost-effective mitigation measures recommended for the design team to incorporate. Coordinating the effort with overall design goals and team activities was ongoing, with strong client support.

A similar TARA can be performed by following eight steps described below.

3.1 Outline current guidelines and best practices

Several U.S. government agencies produce documents that give direction for designing to protect against terrorist attacks. A report by the Department of Justice (DoJ) [5] provides levels of security based on factors such as occupant load and functions of a facility. Standards developed by the General Services Administration (GSA) [6] and the Department of Defense (DoD) [7] contain levels that reflect target performance for different loading conditions. Each report uses its own definitions and methodologies.

There are however, common trends between these documents: the protection level increases as the performance level increases; the highest level of protection is targeted at mission critical facilities; and protection against all possible terrorist attacks cannot be assured. Table 1 summarizes the performance levels outlined in the three documents. It does not imply equivalence between levels. Rather it serves as a comparison between the definitions used by each agency.

Table 1: Comparison of security / performance levels in U.S. references.

<table>
<thead>
<tr>
<th></th>
<th>DoJ</th>
<th>DoD</th>
<th>GSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>below standard</td>
<td>very low</td>
<td>low</td>
</tr>
<tr>
<td>II</td>
<td>low</td>
<td>medium low</td>
<td>medium</td>
</tr>
<tr>
<td>III</td>
<td>medium</td>
<td>medium</td>
<td></td>
</tr>
<tr>
<td>IV</td>
<td>high</td>
<td>higher</td>
<td></td>
</tr>
</tbody>
</table>
Reports by the Interagency Security Committee [8], Federal Transit Administration [9], National Institute for Occupational Safety and Health [10], Army Corps of Engineers [11], American Society for Heating Refrigeration and Air-Conditioning Engineers [12], and others should also be included as relevant.

3.2 Identify threats of concern and associated design loads

Blast and CBR scenarios are not covered by building codes and therefore often considered in TARA efforts. They should be developed with associated design loads based on site layout and other considerations in consultation with the client. The TARA should not aim to duplicate the work of other groups on the design team, and therefore will likely not address in detail normal fire and security system design issues.

Details of the threat scenarios and design loads should be discussed only with approved client representatives. They should be kept confidential from most of the design team. Representatives from each specialty can sign non-disclosure agreements in order to be able to coordinate with TARA efforts.

3.2.1 Explosion scenarios and loads

Design loads will likely need to be established for the threats of internal and external explosions. Loads should be formalized but not published in any drawing or specification that could become publicly available.

Blast loads are established so that structural performance can be analyzed. Specifically, engineers should check for disproportionate damage such as progressive collapse given the explosive loads. They should also analyze behaviour and potential fragmentation hazard for glazing at the explosion design loads if the architecture includes a large amount of glass.

3.2.2 CBR scenarios

Enclosed spaces like buildings, tunnels and subway stations are vulnerable to CBR attack because they have distribution systems for air and water that can be used to deliver agents to areas beyond those which were attacked. The Japan Sarin attacks for example, caused much damage when released in the Tokyo subway.

Current TARA efforts generally focus on measures to isolate and minimize the potential spread of CBR agents. There are few mechanisms to prohibit agents from entering a facility, and detection technology is in its infancy.

3.3 Agree on target performance level for the facility

The concept report should also recommend performance levels for design in accordance with DoJ (FTA applied), GSA, DoD and other documents. Levels should be reviewed with the client and other important stakeholders as appropriate. Recommendations should cover structural and glazing performance, mechanical system response, capabilities of fire protection systems, capacity of egress routes, physical and electronic security systems, and other systems as
appropriate. The performance can be described either qualitatively or quantitatively.

3.4 Undertake initial threat and risk assessment, and risk ranking

The threat and risk assessment should aim to understand how the facility will respond to a threat, discover what are the potentially vulnerable systems and features, and to identify what components can be cost-effectively upgraded to reduce risk. A semi-quantitative risk ranking, supported by design team analyses of resilience that are quantitative (such as analysis of blast waves on structure and glazing) and qualitative (including an assessment of CBR distribution) can be useful and not require extensive research on historical data. A relative risk-ranking approach can use a five-point ranking system to indicate relative values.

Arup summarizes analyses in a matrix format. When semi-quantitative methods are used, each numeric entry described below is either assigned on a scale of one to five, or calculated based on the assigned inputs. Thirty or more components of a facility can be assessed individually for each threat scenario. The first section in the matrix documents the component and scenario, with the headings of Area / System, Location, and Threat Scenario. The next section records the probability of occurrence estimate through Attack Potential, followed by the calculation of criticality in Concern Level, Threat Ranking, a Potential Consequence description, and the Consequence Ranking. The Risk Ranking is derived from the various input values as a single number representative of the risk level for that component.

Risk acceptance decisions should be made in consultation with the client or other important stakeholders. Where risks were intolerable, mitigation measures should be explored or avoidance can be considered through elimination of the program element.

3.5 Develop a list of potential mitigation strategies

A broad range of mitigation measures should be considered for incorporation into the design to mitigate the effects of the threats considered. Mitigation measures aim to either reduce probability of attack or increase resilience of the facility. Measures can cover the work of most disciplines. Typical mitigation options are listed in table 2.

3.6 Assess relative costs and benefits of strategies

The matrix format from the risk analysis can be extended to include a cost-benefit analysis, using the inputs of Relative Mitigation Effectiveness and Relative Mitigation Cost to arrive at a Relative Cost Effectiveness. This value is combined with the Risk Ranking for each component to arrive at the Relative Risk-Cost Ranking. The design team architects and engineers, as well as cost estimators can aid the evaluation of costs and benefits of options. Done in the early stages of design and with ongoing input of the team, this effort aims to seamlessly integrate measures with aesthetic goals and design assumptions.
Table 2: Typical mitigation measures to protect against threats.

<table>
<thead>
<tr>
<th>Blast mitigation options:</th>
<th>CBR mitigation options:</th>
</tr>
</thead>
<tbody>
<tr>
<td>video monitoring through CCTV</td>
<td>air intakes inaccessible</td>
</tr>
<tr>
<td>intrusion detection and alarm</td>
<td>tightly seal areas</td>
</tr>
<tr>
<td>adequate lighting</td>
<td>airlocks at entrances to critical areas</td>
</tr>
<tr>
<td>presence of security personnel</td>
<td>separation by air curtain</td>
</tr>
<tr>
<td>package screening machines</td>
<td>minimal entrances to plant areas</td>
</tr>
<tr>
<td>call ahead procedures for deliveries</td>
<td>controlled access to water storage</td>
</tr>
<tr>
<td>protected and redundant egress paths</td>
<td>remote closing of air intakes</td>
</tr>
<tr>
<td>redundant load paths, harden structure</td>
<td>filters on air intakes</td>
</tr>
<tr>
<td>restrict access to critical areas</td>
<td>CBR agent detection</td>
</tr>
<tr>
<td>secure inventory systems</td>
<td>critical rooms isolated from public</td>
</tr>
<tr>
<td>bollards or other barriers</td>
<td>HVAC zones controlled</td>
</tr>
</tbody>
</table>

3.7 Recommend specific mitigation measures

The final Relative Risk-Cost Ranking results can be colour-coded to emphasize measures that are both beneficial and cost-effective for the highest risks. While all measures contribute to risk reduction, those with the largest Rankings highlighted in green are clearly strongly recommended for incorporation into design. Measures in yellow with next highest ranking should also be considered. Measures in red are lowest in the priority ranking, but may be further explored upon client or design manager request.

3.8 Work with the design team to incorporate measures

Many decisions about the transit complex will be influenced by the TARA, including structural measures, glazing design, use of bollards, security in public and private areas, and compartmentation between facilities. The strongest green recommendations should be audited internally to ensure the client of their inclusion. A database can easily be created to store the analysis summary for each component of the facility, from which audit forms are created. These audit forms derived from the database should include sign-off by design managers, confirming incorporation of the measure.

4 Conclusions

Transportation facilities are normally designed to withstand technological and natural hazards according to building code requirements. They can also be designed to protect against terrorist blast and CBR attacks through a site-specific TARA. A TARA produces a risk ranking for components of the facility, and leads to recommendations for cost-effective mitigation measures. If the client
and designers from all disciplines on the design team help brainstorm measures, and estimate their costs and benefits, mitigation options can align with aesthetic and functional project objectives with minimal cost.

The TARA work should be kept private. Design criteria for blasts should not be published in drawings or specifications that might become publicly available, reports should be treated as confidential, and designers coordinating with the TARA should sign non-disclosure agreements.

Protecting public transit facilities in New York City and other densely urban areas against terrorist attacks is a serious challenge. A TARA performed during design can help improve protection of the passengers, the site and its operations.

References


