2.1 INTRODUCTION

As noted in the previous chapter, in the absence of prescriptive regulations that address man-made hazards and terrorist threats, the designer needs to understand on what threat the design must be based and what level of protection the owner desires. Threat implies both a method and scale of attack and the likelihood of its occurrence. The level of protection is a function of the degree of risk that the owner will tolerate – the "acceptable risk."

In every design or renovation project, the owner has three basic choices (Figure 2-1).

1. Do nothing and accept the risk.
2. Perform a limited risk assessment and manage the risk by implementing reasonable mitigation measures.
3. Implement a detailed risk assessment leading to major construction and operational measures to reduce a high risk to an acceptable level.

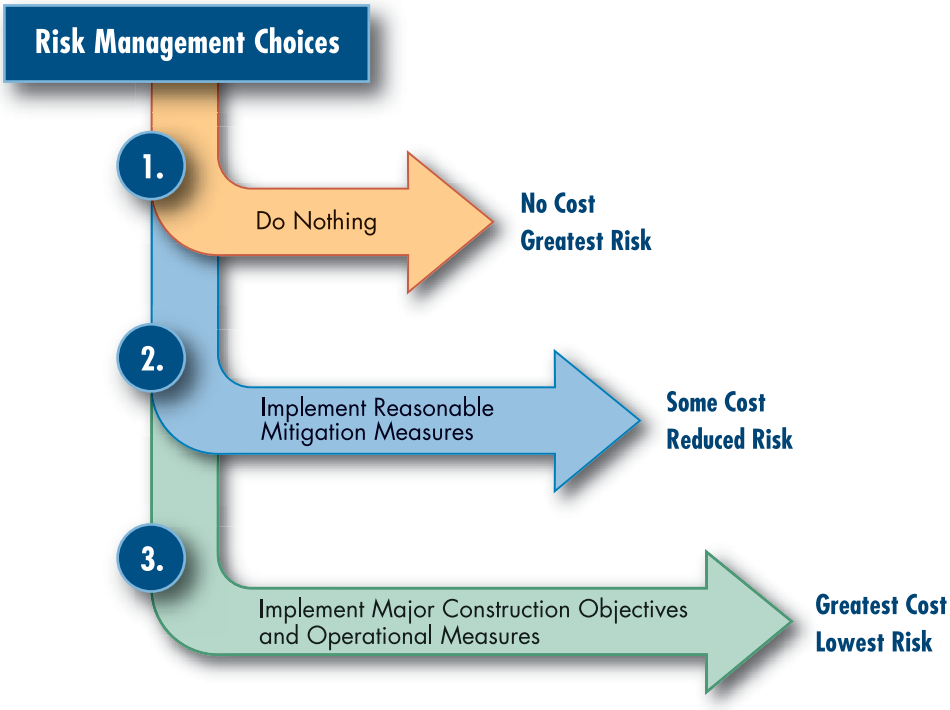


Figure 2-1:
The risk management choices.

SOURCE: FEMA 426

This publication focuses primarily on site design for assets at **high risk from vehicle-laden bombs**, because they have the capability of causing the maximum amount of damage and casualties. There are, however, design alternatives at this level, such as re-alignment of the approach to a building to slow down vehicles, or providing adequate stand-off distance between the bomb-laden vehicle and the building to reduce the explosive impact

These measures do not protect against lesser threats such as bombs carried in backpacks, briefcases, or letters. Protection against these depends on screening and inspection of pedestrians. CBR attacks involve a different set of mitigation measures that predominantly require modifications to the building itself and its utility systems. The Building Vulnerability Check List described in Section 2.2.4 covers CBR vulnerabilities, and some measures that apply to site planning are discussed in Chapter 5, Section 5-11. In a dense urban situation, methods may include street closure to prevent vehicles from approaching target buildings, or using advanced surveillance equipment and operational methods, together with building hardening, to limit the damage caused by vehicle-laden bombs. The designers may employ a number of these methods to develop an integrated strategy that provides cost-effective security. However, careful consideration must be given to the impact of these security measures on the operation and function of the city. These measures must also respect and enhance the environmental quality of the site, surrounding neighborhood and greater community.

This chapter focuses on three considerations that determine the design task:

1. The FEMA risk assessment process

This involves a five-step process that may be undertaken informally by an experienced team for a smaller project or be implemented as a formal recorded systematic process by a multi-disciplinary team that may involve extensive engineering and blast analysis. The latter procedure is exemplified by the detailed FEMA Risk Assessment outlined in section 2.2.

The basic model for establishing risk (which applies to natural hazards as well as physical attacks) consists of three factors that are related as follows:

Risk = Threat Rating X Asset (Consequences) Value X Vulnerability Rating

When the risk is established, consideration can then be given to alternative methods of mitigation. This model applies whether some consultants and the building owner are discussing security needs

at the outset of a project, or a full scale FEMA type risk analysis is undertaken. It also provides the basis for the FEMA five-step risk assessment process described in Section 2.2., The risk assessment provides essential information for the site security design strategy development.

2. Explosive forces and stand-off

Because this publication focuses on protection from bombs, the designers need to have a general understanding of the nature of explosive forces and the effects of blast on people and buildings. In particular, the relationship between blast loading and distance is fundamental to the way in which site design can assist in reducing risk.

3. The costs of protection

Because the protection of high-risk assets can be expensive, cost/benefit is an important element in developing an effective protection strategy. As the cost of a particular countermeasure (e.g., perimeter vehicle barriers) increases, the value of the measure decreases based on the relationship between performance and costs. Designers must become familiar with the performance of recommended measures and their cost considered over the building lifetime, with an initial cost governed by the owner's resources.

2.1.1 ACCEPTABLE RISK AND LEVELS OF PROTECTION

The concept of acceptable risk is based on the recognition that it is an unrealistic goal to attempt to eliminate risk altogether:
some damage from a terrorist attack must be anticipated, and the issue becomes that of determining how much and what kind of damage is "acceptable." For example, total building collapse will be unacceptable, but broken windows that result in minimal injuries may be acceptable.

The determination of "acceptable risk" is made by the building owner with the assistance of in-house security staff and/or security consultants, urban planners, designers and architects using risk management procedures and known building and site operations and city functions. Together, these professionals must evaluate and balance the economic and social tradeoffs between increased occupant safety, decreased

It may be difficult for some owners to determine "how much damage is acceptable" for the facility. Owners should realize that total protection is not possible for existing or even new facilities (short of designing a reinforced concrete bunker), and some acceptance of risk is unavoidable. Although this process may be difficult, owners should realize that it is a more thoughtful and conscientious way of designing perimeter security barriers than blindly following a prescriptive distance that may, or may not, be appropriate for the facility. The process also will ensure the most cost-beneficial solution for the site. In the unlikely event that cost is of no object to the owner, a systematic risk analysis is still essential to ensure that appropriate mitigation measures will be provided.

damage, repair cost, downtime reduction, construction cost, and effective function of the building and site.

An approximate way of defining the acceptable risk is to use the "Security Standards" or "Levels of Performance" issued by several government agencies to set minimum security standards for buildings constructed or leased by the agency or the General Services Administration (GSA). These standards and recommendations are not required for non-federal buildings; however, building owners can evaluate and select those standards that meet their specific needs and criteria.

The Interagency Security Committee (ISC) has issued the *ISC Security Design Criteria for New Federal Office Buildings and Major Modifications*, progressively updated since 2001. The application of the security design criteria is based on a project-specific risk assessment, similar to that outlined in the following sections, that looks at Threat, Assets and Consequences, Vulnerability, and Risk. Figure 2-2 reproduces the description of the three levels of protection used in the ISC.

Figure 2-2:
Levels of protection from the ISC Criteria.

SOURCE: *FEDERAL OFFICE BUILDINGS AND MAJOR MODERNIZATION PROJECTS*, INTERAGENCY SECURITY COMMITTEE, SEPTEMBER 29, 2004

PROTECTION LEVELS

Your entire building structure or certain portions of the structure will be assigned a protection level according to the facility-specific risk assessment The following are definitions of damage to the structure and exterior wall systems for each protection level.

Minimum and Low Protection – Major damage. The facility or protected space will sustain a high level of damage without progressive collapse. Casualties will occur and assets will be damaged. Building components, including structural members, will require replacement, or the building may be completely unrepairable, requiring demolition and replacement

Medium Protection – Moderate damage, repairable. The facility or protected space will sustain a significant degree of damage, but the structure should be repairable. Some casualties may occur and assets may be damaged. Building elements other than major structural members may require replacement.

High Protection – Minor damage, repairable. The facility or protected space may globally sustain minor damage with some local significant damage possible. Occupants may incur some injury, and assets may receive minor damage.

Note that each protection level gives a general description of expected damage that the building owner can use to help assess the acceptable risk. In addition, the ISC criteria provide more detailed performance

levels and damage state descriptions for a number of elements of the building. As an example, Figure 2-3, reproduced from the *ISC Security Design Criteria,* shows the protection levels and damage descriptions for glazing. The different levels of protection, for the building as a whole and its parts, will require different analysis techniques to verify that a design meets these various criteria.

Glazing Protection Levels Based on Fragment Impact Locations

Performance Conditions	Protection Level	Hazard Level	Description of Window Glazing Response
1	Safe	None	Glazing does not break. No visible damage to glazing or frame.
2	Very High	None	Glazing cracks but is retained by the frame. Dusting or very small fragments near sill or on floor acceptable.
3a	High	Very Low	Glazing cracks. Fragments enter space and land on the floor no further than 1 m (3.3 ft.) from the window.
4	High	Low	Glazing cracks. Fragments enter space and land on the floor no further than 3 m (10 ft.) from the window.
5	Medium	Medium	Glazing cracks. Fragments enter space and land on the floor and impact a vertical witness panel at a distance of no more than 3 m (10 ft.) from the window at a height no greater than 0.6 m (2 ft.) above the floor.
6	Low	High	Glazing cracks and window system fails catastrophically. Fragments enter space impacting a vertical witness panel at a distance of no more than 3 m (10 ft.) from the window at a height greater than 0.6 m (2 ft.) above the floor.

Figure 2-3: Glazing levels of protection and damages states.

SOURCE: *FEDERAL OFFICE BUILDINGS AND MAJOR MODERNIZATION PROJECTS,* INTERAGENCY SECURITY COMMITTEE, SEPTEMBER 29, 2004

2.2 THE FEMA RISK ASSESSMENT PROCESS

FEMA Publication 452: *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks against Buildings* provides a detailed process for the risk assessment of buildings and other critical structures. This section outlines the structure and concepts of the FEMA Risk Assessment approach in order to provide the reader unfamiliar with risk assessment an understanding of the FEMA process. The detail and thoroughness of the FEMA process is left to the building owner: the assessment process

guides the establishment of a desired level of protection by the owner and the development of mitigation measures by the multi-disciplinary design team. The FEMA process is also very effective in providing a uniform assessment for a large inventory of assets, such as an industrial park or the central business district of a city.

A risk involving an inventory of buildings begins with a Tier 1 assessment or a Rapid Visual Screening, described later, which will reduce the number of projects needing a more detailed assessment. The risk assessment can then proceed on successively more detailed levels, such that the most detailed level need only be investigated on relatively few projects. These three levels, or tiers, of assessment are outlined in more detail in Section 2.2.1.

The FEMA process consists of five steps; each step has a number of tasks (Figure 2-4).

Figure 2-4: The FEMA five-step process.

SOURCE: FEMA 452

2.2.1 TIERS OF THE RISK ASSESSMENT PROCESS

The level of the assessment for a given building or an inventory of buildings is dependent upon a number of factors, such as type of building, location, type of construction, number of occupants, economic life, other owner specific concerns, and available economic resources. *FEMA 452* provides procedures for increasingly detailed tiers of assessments. The underlying purpose is to provide a variable scale to meet benefit/cost considerations for a given building that meets the intent and requirements of available anti-terrorism guidelines, such as the *DoD Minimum Anti-Terrorism Standards and the DHS Interagency Security Criteria.*

A Tier 1 assessment is a screening process that identifies the primary vulnerabilities and mitigation options and is a "70-percent" assessment. This may involve a site visit and architectural, engineering, security systems, and operations staff and consultants.

A Tier 2 assessment is a full on-site evaluation that provides a robust evaluation of system interdependencies, vulnerabilities, and mitigation options; it is a "90 percent" assessment solution. This may involve the following professionals: site and architectural; structural and building envelope; mechanical, electrical, and power systems; site utilities; information technology (IT); telecommunications; security systems; and operations experts.

A Tier 3 assessment is a detailed evaluation of the building using blast models to determine building response, survivability and recovery, and the development of mitigation options. This assessment typically involves engineering and scientific experts and requires detailed design information, including drawings and other building information. Modeling can often take several days or weeks and is typically performed for high-value and critical infrastructure assets deemed at very high risk. This type of assessment may include the following professionals: site and architectural; structural and building envelope; mechanical, electrical, power systems, and site utilities; IT and telecom modeler; security system and operations; explosive blast modeler; CBR modeler; and cost engineer.

The depth and completeness on the assessment depends on the number of professional experts and the number of days devoted to prepare the assessment.

2.2.2 THE FEMA RISK ASSESSMENT STEPS

This section provides a summary of the five steps to show the structure and content of the assessment process. For each step the assessment results in a numerical value, on a scale of 1-10, as described in Section 2.2.6, that expresses the result of the assessment as a numerical importance rating (see Tables 2-1 and 2-2 for the scales used for these ratings).

Step 1. The **threat** is identified, defined and quantified. For terrorism, the threat is defined as any indication, circumstance, or event with the potential to cause loss of or damage to an asset. The threat can be qualified by the aggressors (people or groups) that are known to exist, and that have a known capability and history of using hostile actions, and includes the tactics and types of weapons that have been used. The outcome of the assessment is the definition of the **design basic threat – the types and capabilities of weapons against which the building must be protected** and the threat rating, which deals with the probability of the threat occurring and the consequences of its occurrence (Figure 2-5).

TASKS	KEY QUESTIONS DESIGNERS MAY ASK
❍ Identify the threats and collect information on them ❍ Determine the design basic threat ❍ Determine the threat rating	❍ What groups or organizations are known? ❍ Do they have a history of terrorist acts and what are their tactics? ❍ What are the intentions of the aggressors against the government, commercial enterprises, industrial sectors, or individuals? ❍ Has it been determined that targeting is actually occurring or being discussed?

Figure 2-5: Threat identification and rating tasks and issues.

Step 2. The **assets (consequences)** that need to be protected are identified. ("Assets" refer to the building, people, equipment and contents, and also the consequences of their damage or loss.) Assets can be categorized by the degree of debilitation impact that would be caused by their incapacity or destruction. Critical assets include identifying the core functions and processes necessary for the building to continue to operate and provide services after an attack, including infrastructure and utilities (Figure 2-6).

TASKS	KEY QUESTIONS DESIGNERS MAY ASK
❍ Identify critical assets (critical functions and infrastructure) ❍ Identify the building core and functions and infrastructure (see section 2.2.2.1) ❍ Determine the asset value rating	❍ How critical is this asset? ❍ What losses or damage may occur in case of a terrorist attack? Would the asset or building remain operational? ❍ What are the potential losses of life? ❍ What would be the social and economic impact of the attack?

Figure 2-6: Asset value assessment tasks and issues.

STEP 3 Vulnerability Assessment

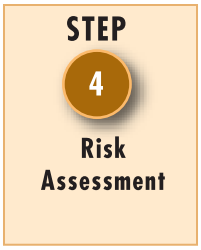
Step 3. A **vulnerability assessment** evaluates the potential vulnerability of the critical assets against a broad range of identified threats/hazards. Vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to damage or destruction.

As part of the vulnerability assessment process the layers of defense are identified. The layers of defense are described in detail in Chapter 3, Section 3.2. The layers of defense establish demarcation points for different security strategies, and establish where the assets being identified are located in relation to the property under the control of the owner. Typically, the first layer is outside the property line, the second layer is between the property line and the asset, and the third layer is the protection of the asset itself.

An important tool for defining vulnerability is the use of the Vulnerability Assessment Check List that is provided in *FEMA 452*; this is described in Section 2.2.4 in this publication. It consists of a list of questions and commentary that enables the assessors to develop a consistent and thorough picture of the asset's vulnerability. In and of itself, the vulnerability assessment provides a basis for determining mitigation measures for protection of the critical assets. The vulnerability assessment is the bridge in the methodology between threat/hazard, asset value, and the resultant level of risk (Figure 2-7).

TASKS	KEY QUESTIONS DESIGNERS MAY ASK
❍ Collect information about the site and building into a vulnerability portfolio that includes GIS maps and other pertinent information ❍ Identify the layers of defense ❍ Evaluate the site and building ❍ Determining the vulnerability ratin	❍ What are the major weaknesses identified that make the asset susceptible to an aggressor? ❍ Does the building lack redundancies or physical protection? Has continuity of operation been established? ❍ Is there an alternative site? ❍ Are redundancies for critical services and operations in place? ❍ When can the building be functional again?

Figure 2-7: Vulnerability assessment tasks and issues.



Step 4 . Risk assessment. In this step the values for the Threat, Asset, and Vulnerability are multiplied to arrive at the Risk. This step analyzes the threat (probability of occurrence) and asset value and vulnerabilities (consequences of occurrence) to ascertain the level of risk for each critical asset against each applicable threat. The risk assessment provides engineers and architects with relative risk profiles that define which assets are at the greatest risk against specific threats, thus enabling appropriate protection methods to be selected for further analysis. Thus, a very high likelihood of occurrence with very small consequences may require minimal mitigation measures, but a very low probability of occurrence with very grave consequences, such as large loss of life, may require costly and complex mitigation measures (Figure 2-8).

TASKS	KEY QUESTIONS DESIGNERS MAY ASK
❍ Prepare risk assessment matrices (see Section 2.2.2.1) ❍ Determine the risk ratings (Threat X Asset Value X Vulnerability) ❍ Beginning with highest risk ratings, prioritize observations identified as vulnerabilities to target potential mitigation measures	❍ How are priorities determined for observations identified as vulnerabilities using the Building Vulnerability Checklist/Database?

Figure 2-8: Risk assessment tasks and issues

Step 5. The consideration and selection of **risk mitigation options** are directly associated with and responsive to the major risks identified in Step 4. In Step 5 decisions are made as to where and how to minimize the risks and how to accomplish these tasks during the design and construction phase and, if appropriate, over the operational life of the building. In this process, general mitigation goals and objectives and the merits of each potential mitigation measure must be examined.

The building owner has to make the final decision as to which mitigation measures should be implemented based on the level of protection desired and the acceptable risk tolerated. However, engineers, architects, landscape architects, and other technical advisers and staff should be involved in this process to ensure that the results of the risk assessment are met with sound mitigation measures that will increase the capability of the building to perform to its selected performance level (Figure 2-9).

TASKS	KEY QUESTIONS DESIGNERS MAY ASK
❍ Identify preliminary mitigation options ❍ Review mitigation options for interaction and appropriateness in each layer of defense ❍ Estimate cost of mitigation options ❍ Select mitigation options to implement and timetable for each	❍ What mitigation options will reduce risk the most, especially for highest risks identified in risk matrices? ❍ Which options should be taken to detect, deter, or deny an attack in regard to available layers of defense? ❍ What regulatory criteria impact these options? ❍ What options have the greatest benefit (risk reduction or achievement of protection level) for cost? ❍ How do site and layout design protection and control measures balance against building hardening measures?

Figure 2-9: Mitigation options tasks and issues.

2.2.3 BUILDING CORE FUNCTIONS AND INFRASTRUCTURE

A key element for the preparation of a risk assessment is the identification of the core functions and infrastructure of the asset. The core functions establish what a building does, how it does it, and how various threats can affect the building operations. The core infrastructure consists of those characteristics of the building that support its functions and that are critical to its continued operation.

The functions and infrastructure analyses identify the geographic distribution within the building and interdependencies between critical assets. For example, a bomb or CBR attack entering through the loading dock could impact the telecommunications, data, uninterruptible power supply (UPS), generator, and other key infrastructure systems.

The reason for identifying core functions and processes is to focus the assessment team on the building functions, how they are accomplished, and how various threats can impact the building. After the core functions and processes are identified, an evaluation of building infrastructure should follow.

Figure 2-10 depicts the core functions and infrastructure. New functions can be added depending on the type and functions of a particular building. Building infrastructure is composed of fixed elements that are categorized in the next section of this chapter.

Figure 2-10:
Core functions and building infrastructure charts.

SOURCE: FEMA 452

Core Functions	Building Infrastructure
Administration	Site
Engineering	Architectural
Warehouseing	Structural Systems
Data Center	Envelope Systems
Food Service	Utility Systems
Security	Mechanical Systems
Housekeeping	Plumbing and Gas Systems
Day Care	Electrical Systems
	Fire Alarm Systems
	IT/Comminications Systems

2.2.4 BUILDING VULNERABILITY CHECKLIST

The Building Vulnerability Checklist, presented in full in *FEMA 452*, is intended to guide the preparation of the risk assessment. It is a screening tool for a preliminary design vulnerability assessment. The Checklist is organized into 13 sections: 1) site, 2) architectural, 3) structural systems, 4) building envelope, 5) utility systems, 6) mechanical systems, 7) plumbing and gas systems, 8) electrical systems, 9) fire alarm systems, 10) communications and IT systems, 11) equipment operations and maintenance, 12) security systems, and 13) security master plan.

To conduct a vulnerability assessment of a building or preliminary design, each section of the Checklist should be assigned to an engineer, architect, or subject matter expert who is knowledgeable and qualified to perform an assessment of the assigned area. Each assessor should consider the questions and guidance provided to help identify vulnerabilities and document results in the observations column. For an existing building, vulnerabilities can also be documented with photographs, if possible. The vulnerabilities of the facility are selected from the observations provided for each vulnerability question.

These vulnerabilities are then prioritized to determine the most effective mitigation measures. Prioritization is based on the greatest vulnerabilities that can be exploited by the aggressors and the largest risks in terms of loss of lives, building damage, and loss of operation.

2.2.5 ELECTRONIC DATABASE FOR RISK ASSESSMENT AND RISK MANAGEMENT

To facilitate the management of the large amount of information that comprises a thorough FEMA Risk Assessment process and use of the Building Vulnerability Assessment Checklist, FEMA has developed a software database with a graphical user interface to assist users in inputting data and producing reports presented in Microsoft Word© or Excel© documents. Security features protect data and provide search capabilities to find stored information.

The Risk Assessment Database is a stand-alone application that is both a data collection tool and a data management tool. Assessors can use the tool to assist in the systematic collection, storage, and reporting of assessment data. It has functions, folders, and displays to import and display threat matrices, digital photos, cost data, site plans, floor plans, emergency plans, and certain GIS products as part of the record of assessment. Managers can use the application to store, search, and analyze data collected from multiple assessments, and then print a variety of reports.

The Risk Assessment Database is continually evolving and is currently in its third version, with fourth and fifth versions already under development. The fourth version will add natural hazards vulnerability assessment checklist questions for earthquake (seismic), flood, and wind, following the same format as the original checklists – questions, guidance, and references for additional information, with color coding within the original Construction Specification Institute format.

The fifth version will add another type of assessment to the database called Rapid Visual Screening (RVS), which will follow the process in the soon-to-be-published FEMA 455, *Handbook for Rapid Visual Screening to Evaluate the Vulnerability of Buildings to Potential Terrorist Attacks*. The primary purpose of the RVS procedure is to prioritize the relative risk among standard commercial buildings in a portfolio, community, or region (urban and semi-urban areas), but it can also be used to develop building-specific vulnerability information. It can be performed using limited information from outside the building exterior, because interior inspections or interviews with key stakeholders are not always possible. Contrast this with a Tier 1 assessment in which the screening is performed with full access to the building and participation of key building occupants.

2.2.6 RANKING

For determining the threat rating, *FEMA 452* provides a methodology based on the consensus opinion of the building stakeholders, threat specialists, and engineers. Table 2-1 illustrates the 10-point numerical scales

(10 being the highest) that are used in this process. The key elements of these scales are the following:

- **For Threat Rating:** Likelihood of a threat (credible, verified, exists, unlikely, unknown), if the use of the weapon is considered imminent, expected, or probable

- **For Asset (Consequences) Value:** Loss of assets and/or people would have grave, serious, moderate, or negligible consequences or impact; economic impact due to the loss of functions

- **For Vulnerability Rating:** Number of weaknesses, aggressor potential accessibility, level of redundancies/physical protection, time frame for the building to become operational again

Table 2-1: Scale for Threat Value Rating,

Threat Rating		
Very High	10	Very High – The likelihood of a threat, weapon, and tactic being used against the site or building is imminent. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
High	8-9	High – The likelihood of a threat, weapon, and tactic being used against the site or building is expected. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium High	7	Medium High – The likelihood of a threat, weapon, and tactic being used against the site or building is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is credible.
Medium	5-6	Medium – The likelihood of a threat, weapon, and tactic being used against the site or building is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not verified.
Medium Low	4	Medium Low – The likelihood of a threat, weapon, and tactic being used in the region is probable. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is known, but is not likely.
Low	2-3	Low – The likelihood of a threat, weapon, and tactic being used in the region is possible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat exists, but is not likely.
Very Low	1	Very Low – The likelihood of a threat, weapon, and tactic being used in the region or against the site or building is very negligible. Internal decision-makers and/or external law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

SOURCE: FEMA 452

Table 2-2: Scale for Asset Value Rating

Asset (Consequences) Value		
Very High	10	Very High – Loss or damage of the building's assets would have exceptionally grave consequences, such as extensive loss of life, widespread severe injuries, or total loss of primary services, core processes, and functions.
High	8-9	High – Loss or damage of the building's assets would have grave consequences, such as loss of life, severe injuries, loss of primary services, or major loss of core processes and functions for an extended period of time.
Medium High	7	Medium High – Loss or damage of the building's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for an extended period of time.
Medium	5-6	Medium – Loss or damage of the building's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes.
Medium Low	4	Medium Low – Loss or damage of the building's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes.
Low	2-3	Low – Loss or damage of the building's assets would have minor consequences or impact, such as a slight impact on core functions and processes for a short period of time.
Very Low	1	Very Low – Loss or damage of the building's assets would have negligible consequences or impact.

SOURCE: FEMA 452

Table 2-3: Scale for Vulnerability Rating

Vulnerability Rating		
Very High	10	Very High – One or more major weaknesses have been identified that make the asset extremely susceptible to an aggressor or hazard. The building lacks redundancies/ physical protection and the entire building would be only functional again after a very long period of time after the attack.
High	8-9	High – One or more major weaknesses have been identified that make the asset highly susceptible to an aggressor or hazard. The building has poor redundancies/physical protection and most parts of the building would be only functional again after a long period of time after the attack.

Table 2-3: Scale for Vulnerability Rating (continued)

Vulnerability Rating		
Medium High	7	Medium High – An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/ physical protection and most critical functions would be only operational again after a long period of time after the attack.
Medium	5-6	Medium – A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection and most part of the building would be only functional again after a considerable period of time after the attack.
Medium Low	4	Medium Low – A weakness has been identified that makes the asset somewhat susceptible to an aggressor or hazard. The building has incorporated a fair level of redundancies/ physical protection and most critical functions would be only operational again after a considerable period of time after the attack.
Low	2-3	Low – A minor weakness has been identified that slightly increases the susceptibility of the asset to an aggressor or hazard. The building has incorporated a good level of redundancies/physical protection and the building would be operational within a short period of time after an attack.
Very Low	1	Very Low – No weaknesses exist. The building has incorporated excellent redundancies/physical protection and the building would be operational immediately after an attack.

SOURCE: FEMA 452

2.2.7 PREPARING THE RISK ASSESSMENT

To prepare the assessment, a number of matrices need to be completed, manually or through use of the database software. Multiplying values assigned for threat rating, asset (consequences) value, and vulnerability rating factors provides quantification of total risk. The total risk for each function or system against each threat is assigned a color code (Table 2-4). This table is an example of a completed matrix.

Table 2-4: Function and Site Infrastructure Pre-Assessment Screening Matrix

Total Risk Color Code			
	Low Risk	Medium Risk	High Risk
Risk Factors Total	1-60	61-175	≥ 176

Table 2-4: Function and Site Infrastructure Pre-Assessment Screening Matrix (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Administration	280	140	135	90
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	7	7	9	9
Engineering	128	128	192	144
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	2	4	8	9
Warehousing	96	36	81	54
Asset Value	3	3	3	3
Threat Rating	8	4	3	2
Vulnerability Rating	4	3	9	9
Data Center	360	128	216	144
Asset Value	8	8	8	8
Threat Rating	9	4	3	2
Vulnerability Rating	5	4	9	9
Food Service	2	32	48	36
Asset Value	2	2	2	2
Threat Rating	1	4	3	2
Vulnerability Rating	1	4	8	9
Security	280	140	168	126
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	5	5	8	9
Housekeeping	16	64	48	36
Asset Value	2	2	2	2
Threat Rating	8	4	3	2
Vulnerability Rating	1	8	8	9
Day Care	54	324	243	162
Asset Value	9	9	9	9
Threat Rating	3	4	3	2
Vulnerability Rating	2	9	9	9

Table 2-4: Function and Site Infrastructure Pre-Assessment Screening Matrix (continued)

Function	Cyber Attack	Armed Attack (single gunman)	Vehicle Bomb	CBR Attack
Site	48	80	108	72
Asset Value	4	4	4	4
Threat Rating	4	4	3	2
Vulnerability Rating	3	5	9	9
Architectural	40	40	135	20
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	9	2
Structural Systems	24	32	240	16
Asset Value	8	8	8	8
Threat Rating	3	4	3	2
Vulnerability Rating	1	1	10	1
Envelope Systems	84	112	189	112
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	2	4	9	8
Utility Systems	112	56	168	42
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	2	2	8	3
Mechanical Systems	42	56	105	126
Asset Value	7	7	7	7
Threat Rating	6	4	3	2
Vulnerability Rating	1	2	5	9
Plumbing and Gas Systems	40	40	120	70
Asset Value	5	5	5	5
Threat Rating	8	4	3	2
Vulnerability Rating	1	2	8	7
Electrical Systems	42	84	189	28
Asset Value	7	7	7	7
Threat Rating	8	4	3	2
Vulnerability Rating	1	3	9	2
Fire Alarm Systems	162	108	216	36
Asset Value	9	9	9	9
Threat Rating	6	4	3	2
Vulnerability Rating	3	3	8	2
IT/Communications Systems	512	64	192	32
Asset Value	8	8	8	8
Threat Rating	8	4	3	2
Vulnerability Rating	8	2	8	2

SOURCE: FEMA 426

The Risk Assessment procedure and the use of the matrix above provide a numerical ranking of risk that has been developed on a systematic basis. Note at the top of the matrix there is a "box score" for the low, medium, and high risk core and infrastructure functions. This provides a useful summary picture of the status of the facility, but the real value of the risk assessment process lies in the detail of the threat, asset and vulnerability assessments that provide the basis for the final selection of mitigation measures. Inspection and analysis of the results of the assessment are valuable in discerning patterns of vulnerability or asset value, for example, and establishing the relative importance of site, building, or other characteristics.

The ranking value provides a useful basis for prioritization when developing mitigation measures for an individual building or for prioritizing between a group of buildings. It is not intended that the ranking scoring system **on its own** be used for establishing absolute thresholds of mitigation.

2.3 EXPLOSIVE FORCES AND STAND-OFF

It is useful for designers involved in security design to have a general understanding of the nature of explosive forces and the effects of blast on people and buildings. This chapter presents a very brief discussion of explosives and blast. Fuller explanations will be found in FEMA 426 and FEMA 452. FEMA 427 provides further information on explosive weapons and specifically addresses their effects on four high-population, private-sector building types: commercial offices, retail, and multi-family residential, and light industrial. FEMA 453 provides useful information on explosive threat parameters.

An explosion is an extremely rapid release of energy in the form of light, heat, sound, and a shock wave. Explosive pressures encountered in design are typically much greater than other loads that are considered, but they decay extremely rapidly with time and space. As a rule of thumb, the pressures generated by the shock wave increase linearly with the size of the weapon, usually measured in equivalent pounds of TNT, and decrease exponentially with the distance from the explosion. The duration of the explosion is extremely short, measured in thousandths of a second, or milliseconds.

As the shock wave expands, the incident or overpressure decreases. When it encounters a surface that is in line-of-sight of the explosion, the wave is reflected, resulting in a tremendous amplification of pressure on the surface of the object: shock waves can reflect with an amplification factor of up to about 12. The magnitude of the reflection factor is a function of the proximity of the explosion and the angle of incidence of the shock wave on

the surface (with incidence normal to the targets resulting in the maximum pressure). Late in the explosive event, the shock wave becomes negative, followed by a partial vacuum, which creates suction behind the shock wave that can cause windows to fall outwards. For a specific type and weight of explosive material, the intensity of blast loading will depend on the distance and orientation of the blast wave relative to the protected space. These characteristics are aspects of the site size and placement of the building(s). Figure 2-11 shows the time-history of the blast in milliseconds.

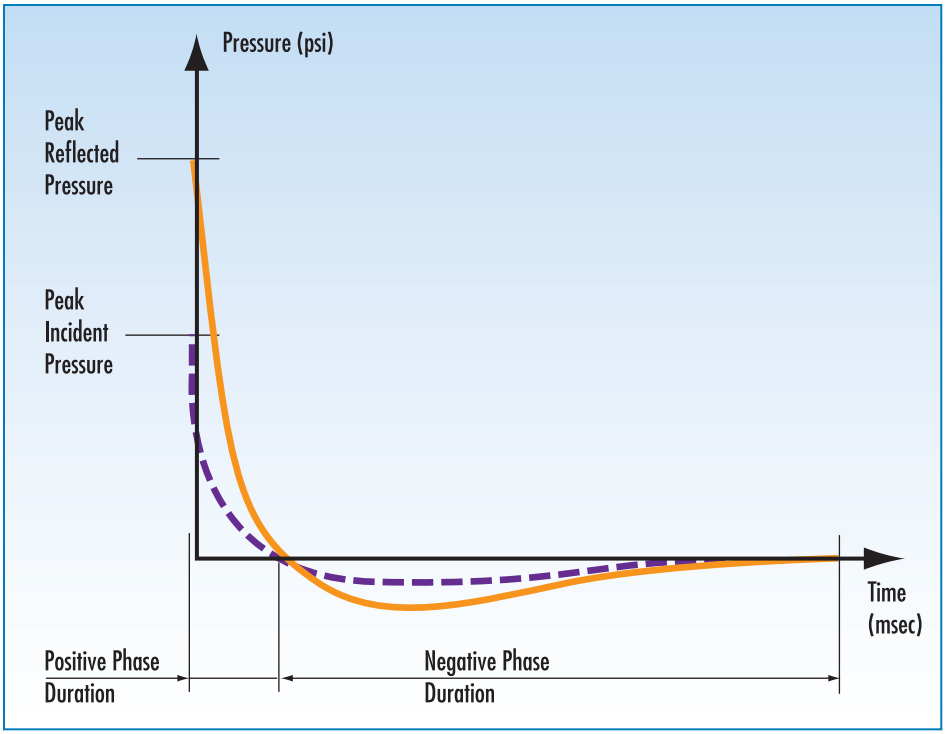


Figure 2.11: Air-blast time history (in milliseconds). The positive pressure greatly exceeds the negative pressure.

SOURCE: BASED ON FIGURE 3.2 IN *FUNDAMENTALS OF PROTECTIVE DESIGN FOR CONVENTIONAL WEAPONS, TECHNICAL MANUAL* TM5-855-1, HEADQUARTERS, DEPARTMENT OF THE ARMY, WASHINGTON D.C., 3 NOVEMBER 1986

Immediately following the vacuum, air rushes in, creating a powerful wind or drag pressure on all surfaces of the building. This wind picks up and carries flying debris in the vicinity of the detonation. In an external explosion, a portion of the energy is also imparted to the ground, creating a crater and generating a ground shock wave analogous to a high-intensity short-duration earthquake.

2.3.1 PREDICTING BLAST EFFECTS

Determination of blast loading is a specialized activity, and a blast consultant must be included as a member of the design team. He or she will have formal training in structural dynamics and demonstrated experience with acceptable design practices for blast-resistant design. The figures and tables in this section are also useful in providing non-specialist designers with an understanding of the relationships between blast loads, stand-off distance, and building damage (**stand-off** or setback is the distance be-

tween the explosive threat location and the nearest building element that requires protection).

The first step in predicting blast effects on a building is to predict blast loads on the structure. Because the damaging pressure pulse varies with stand-off distance, angle of incidence and reflected pressure over the building exterior, the blast load prediction should be performed at multiple threat locations; however, worst-case conditions are normally used for decision making. For complex structures requiring refined estimates of blast loading, blast consultants may use sophisticated methods such as computational fluid dynamics (CFD) computer programs to predict blast loads.

In essence, the blast consultant simulates an explosion based on the available or projected stand-off to determine the effect on the building. This provides information on the value a perimeter security system may have in protecting the available stand-off. Alternative stand-offs (including none) may also be simulated to compare the results to the required performance levels, so that tradeoffs between varying stand-off distances and levels of building envelope and structural hardening may be evaluated to obtain optimal costs.

2.4 THE IMPORTANCE OF STAND-OFF DISTANCE

The stand-off distance is the single most important factor in determining the extent of damage for a given-size weapon. This is because, as noted above, the blast loading decays rapidly with the distance. In general, if the distance is doubled, the blast loading is reduced by a factor of 3 to 8, based upon the distance to the building and the TNT equivalent weight, with the smaller reduction applicable to smaller distances.

Figures 2-12 and 2-13 and Table 2-3 illustrate the influence of stand-off on building damage and casualties. These graphics provide only a broad indication of the effects, which will vary considerably depending on the type of construction, age and quality of the building, its location, and its configuration.

Figure 2-12 represents the level of protection offered by conventional construction at a given stand-off. The green bars in the figure indicate that no significant protection from blast effects is readily attainable at these distances in a conventional building, without structural hardening for the bomb sizes indicated.

The blue bar indicates a low level of protection. At these distances, a conventionally constructed building will typically sustain moderate to heavy damage. Occupants in exposed structures may suffer temporary hearing loss and injury from the force of the blast wave and building debris fragmentation. Other building elements and contents may suffer damage from these effects.

The pale blue bar indicates a medium level of protection. At these distances, conventionally constructed buildings will generally sustain light to moderate damage. Occupants of exposed structures may suffer minor injuries from secondary effects such as building debris.

The violet bar indicates a high level of protection. At these distances, conventionally constructed buildings will generally sustain minor damage. Flying debris may also cause superficial injuries and minor damage to building elements and contents.

Note that for a 500-lb. bomb (carried in a car or light truck), a low level of protection begins only at a 200-foot stand-off. For a 50-lb. bomb (suitcase or suicide bomber), a low level of protection begins at about 80 feet.

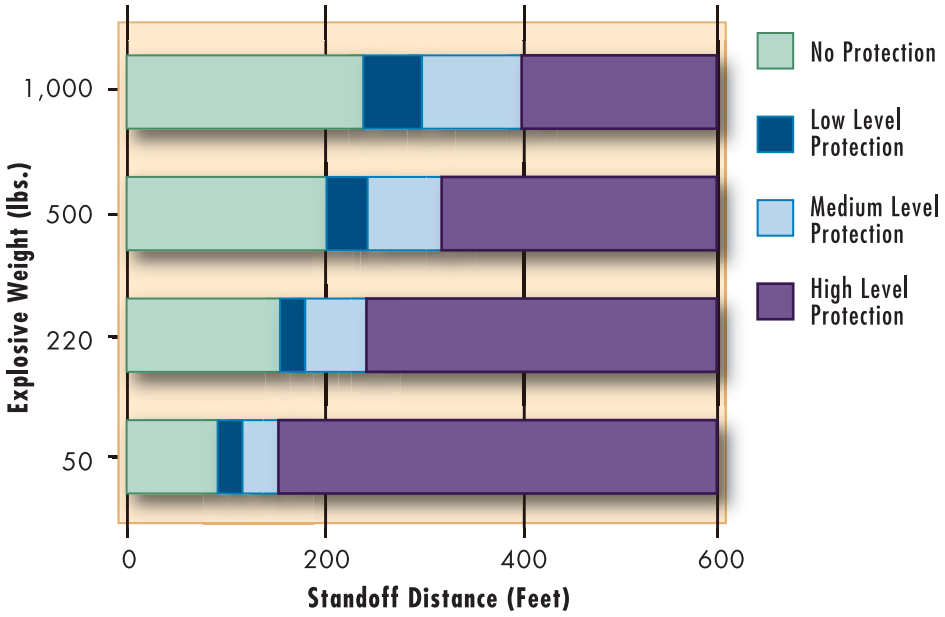


Figure 2-12:
Level of protection versus explosive size and stand-off.

SOURCE: APPLIED RESEARCH ASSOCIATES, INC

The thresholds of different types of injuries associated with damage to wall fragments and/or glazing are depicted in Figure 2-13. This range-to-effects chart shows a generic interaction between the weight of the explosive threat and its distance to an occupied building. These generic charts, for conventional construction, provide information to law enforcement and public safety officials that allow them to establish safe evacuation distances should an explosive device be suspected or detected. However, these distances are so site and building specific that the generic

charts provide little more than general guidance in the absence of more reliable site-specific information.

Based on the information in the chart, the onset of significant glass debris hazards is associated with stand-off distances on the order of hundreds of feet from a vehicle-borne explosive detonation while the onset of column failures is associated with stand-off distances on the order of tens of feet. Note also from inspection of the graphic figure (Figure 2-12), the threshold of potentially lethal injuries from a 50-lb. bomb is about 80 feet, considerably more than the stand-off available in typical urban settings.

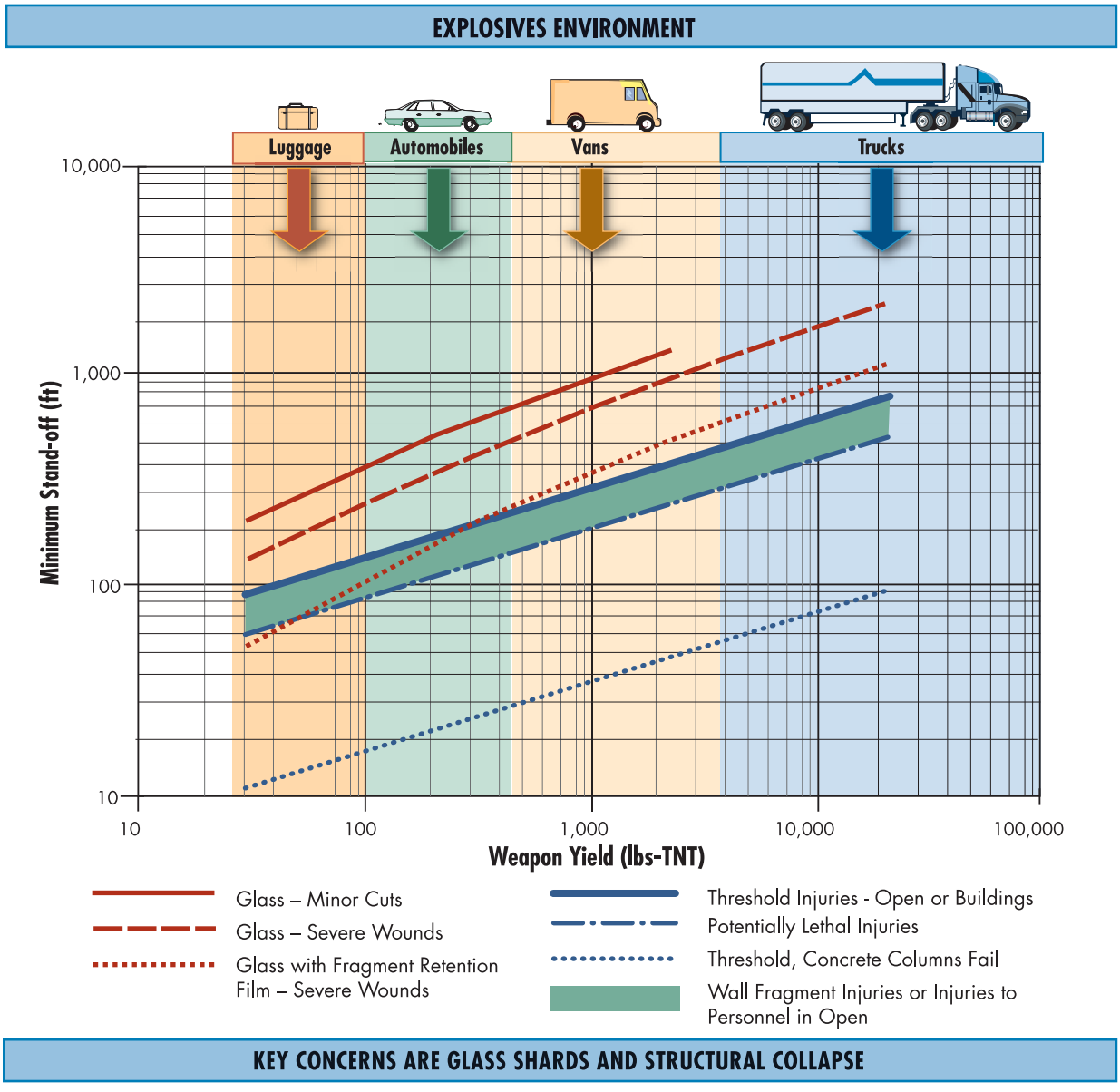


Figure 2-13: Explosive environments: stand-off versus injuries and damage.

SOURCE: FEMA 453

The performance graphically illustrated in Figure 2-13 can also be expressed as a range of stand-off distances in relation to increasing injuries and damage. Table 2-3 is derived from Figure 2-13 and shows injuries related to stand-off for a 500-lb. bomb carried by a car or light van compared to those of a 5,000-lb. bomb carried by a heavier truck. Again, as in the previous figures, the values are generic: the intent is only to illustrate the general benefit of increasing stand-off; they should not be used as design tools.

Table 2-5: Injury or Damage Related to Stand-off

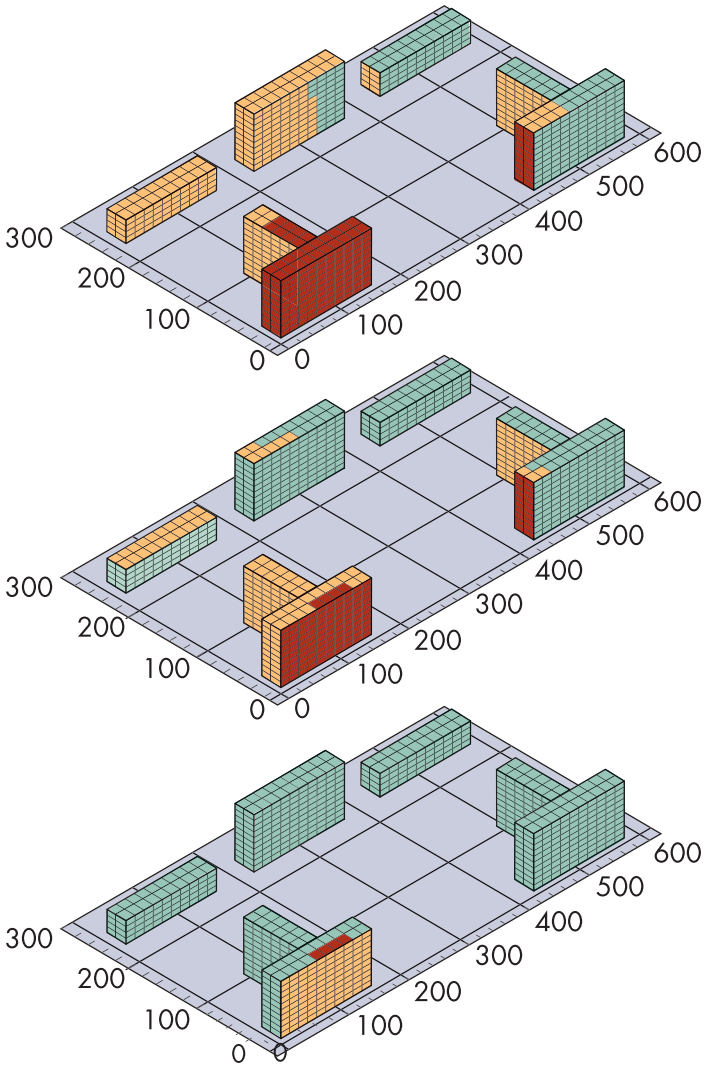
Injury and/or Damage	Stand-off (feet)	
	500-lb. Bomb	5,000-lb. Bomb
Threshold of failure, concrete columns	30	60
Potentially lethal injuries	150	350
Injuries from wall fragments or to people in open	150-250	350-500
Severe glass wounds (glass with applied film)	250	650
Severe glass wounds (unprotected glass)	500	1,000+
Minor cuts	800	1,000+

Figure 2-14 shows a blast analysis for the Khobar Towers incident of 1996. The 20,000-lb. bomb was exploded 80 feet from the closest building. Studies show that increasing the stand-off distance from 80 to 400 feet would have significantly limited the damage to the building and reduced casualties to the occupants (See Chapter 1, Section 1.5.2.8, for further information on this attack) .

The 20,000-lb. bomb was exploded in front of the building to the bottom left. Nineteen persons were killed. The Khobar buildings were constructed to prevent progressive collapse and were successful: the heavy casualties were caused by loss of the façade and glass damage. By contrast, the Murrah Building in Oklahoma City (see Section 1.5.2.6) was attacked by a truck-carried 4,000-lb. bomb that exploded 15-20 feet from the building, causing progressive collapse of much of the structure and most of the 168 deaths.

The critical location of a weapon is a function of the site, the building layout, and the security measures in place. For vehicle bombs, the critical locations are considered to be at the closest point that a vehicle can approach on each side, assuming that all security measures are in place. Typically, this is a vehicle parked along the curb directly opposite the building, or at the entry control point where inspection takes place. A curb is not a barrier to a terrorist vehicle with explosives. The Department

of State view is that if there is no effective anti-ram barrier, there is no setback. Achieving anti-ram setback is a most effective blast mitigation measure. For design and estimating purposes, stand-off is measured from the center of gravity of the charge located in the vehicle or other container to the building component under consideration (usually the building façade).



Detonation at 80 feet from Building 131

This is the actual stand-off that was provided at the Khobar Towers Complex

Detonation at 170 feet from Building 131

This is the minimum stand-off recommended by FM5-114 Engineer Operations Short of War

Detonation at 400 feet from Building 131

This stand-off distance would have prevented serious damage and reduced the extent of casualties

COLOR	DAMAGE DESCRIPTION	HAZARD TO OCCUPANTS
RED	Very severe damage, possible collapse	Very high hazard, widespread death and serious injury likely
YELLOW	Very unrepairable structural dmage	High hazard, death and serious injury possible
GREEN	Moderate repairable structural dmage	Medium hazard, limited casualties and injury possible

Figure 2-14: Stand-off distance related to blast impact as modeled on the Khobar Towers.

SOURCE: INSTALLATION FORCE PROTECTION GUIDE, USAF

It can be seen from the information above that even at stand-off distances of several hundred feet, a large weapon can inflict severe injuries, primarily through glass breakage. Building collapse can be prevented at much lower stand-offs, but in an urban situation, a curbside car or truck bomb presents a real threat of collapse to a conventional structure. Hence, every foot available to increase the stand-off is valuable.

Determination of minimum distances is specific for each building and is based on:

- Prediction of the explosive weight of the weapon
- Required level of protection: this may be specified in the case of a federal or other government building, but for a privately owned building, it is a determination of the "acceptable risk" made during the risk assessment process.
- Evaluation of the type of building construction, whether existing or new, including the building structure and nature of building envelope.
- Constraints or opportunities provided by the site.

If generous stand-off can be provided for an existing building, an evaluation of the building structure, façade, and the occupants at the perimeter may enable the elimination of protective solutions such as (in order of cost and effectiveness) installing blast-resistant glass and framing, additional reinforcing for some building supports (columns and walls) at the lower floors, and specific structural measures against progressive collapse. On the other hand, the relatively low cost of hardening the loading dock, other delivery areas, and the building lobby may be a good investment.

2.5 COST OF PROTECTION

Cost is a very demanding aspect of every design and construction project, and it particularly important when managing risk. As the cost of a particular protective measure (e.g., perimeter vehicle barriers) increases, the value of the measure decreases, based on the relationship between performance and cost. Achieving the maximum risk reduction for the minimum amount of money is one of the basic principles of risk management.

Life-cycle costing, economic analysis, and value engineering can be used to the extent that they suit the owner's economic goals. Clearly an agency or institution that expects to own a building for its entire useful life is well advised to budget on a life-cycle, and many government agencies now require that this be done. Private developers may have other aims, but the

ultimate building owners and operators will all benefit from a building in which life-cycle costs have been considered.

Three cost considerations specifically related to security measures need to be examined at the outset of project cost planning:

- Identification of elements that may not require additional cost if they are incorporated from the beginning of the design process and integrated with other requirements. These are items such as when the cost of construction can be substantially reduced by taking advantage of existing landscape or other elements that can perform as perimeter vehicle barriers and that fall within the acceptable range of distances. However, it is important to note that this approach is only acceptable after a detailed analysis by structural engineers to determine the landscape elements' ability to defend against the design threat vehicle. However, many barriers that have shown excellent simulated performance have failed crash tests, and validation testing for designs that do not have comparable test data available for correlation may be advisable. Owners must evaluate how much risk they are willing to accept by using existing unrated systems.

- Identification of elements that clearly represent additional cost for construction and installation, compared to a typical project, due to additional structural needs such as specially reinforced bollards, hardened street furniture, or reinforced entry gates.

- Identification of elements that may be installed in an incremental manner to minimize initial cost until final security needs are determined. For private-sector projects that will be leased, the occupants and their security requirements may not be finalized until after construction is complete. Provision of pits for active or passive barriers, conduit for security systems, and the preliminary negotiation of approvals for perimeter security enable these elements easily to be added later, when and if tenants require them. The developer will carry a portion of the initial cost for construction, while the tenants will be responsible for the remaining costs as part of their leases.

The cost/performance of the perimeter barrier must be evaluated in relation to the entire protection system, both for the site and the building. (The major cost evaluation in protection is that between the impacts of stand-off distance and building component costs). Thus cost reduction achieved by decreasing stand-off and perimeter length must be evaluated against the comparative increased cost of other solutions, such as hardening the building, providing more guards, increasing camera surveillance, relocating the facility, or relocating key building occupants to interior locations. These evaluations must be conducted with respect to achieving an acceptable level of risk.

Figure 2-15 shows how stand-off affects various structural and nonstructural components of a facility. The figure generally illustrates, at no specific scale, the general trends and relationships between stand-off and cost of protection to implement a typical set of federal agency criteria, such as the ISC Security Criteria. A number of components of incremental security are shown, including structural and nonstructural components contributors. The relative magnitude and scale of these relationships will vary from project to project.

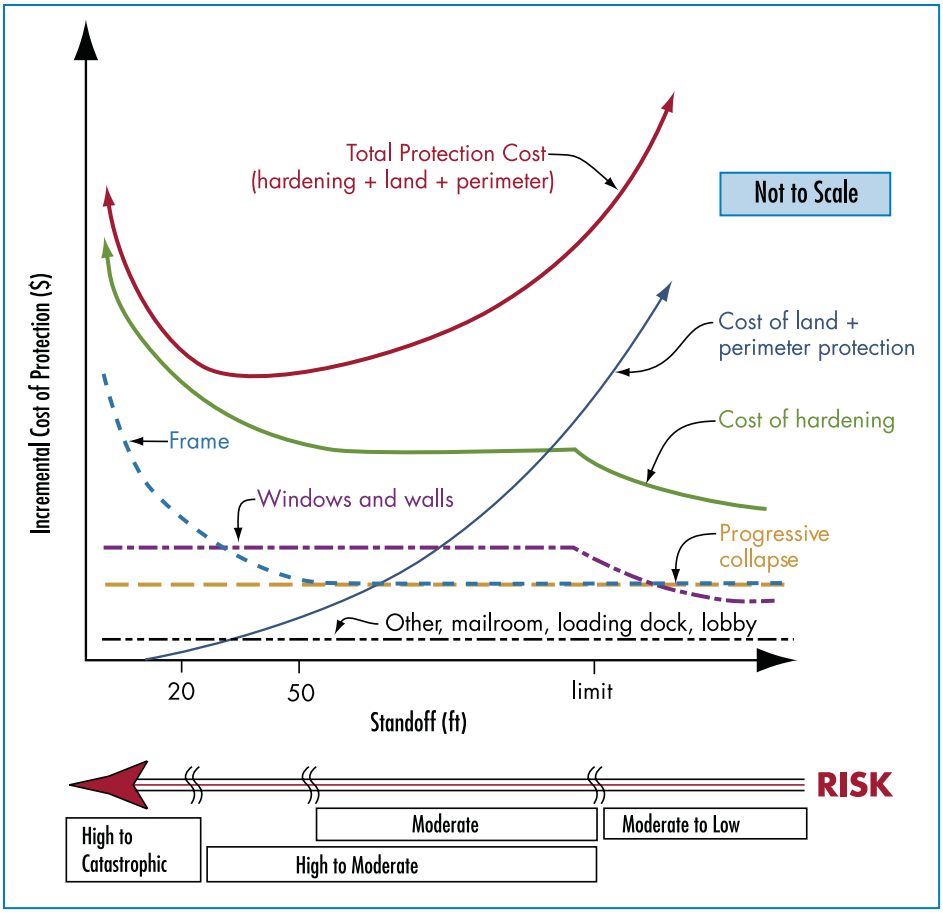


Figure 2-15:
Impact of stand-off distance on component costs.

SOURCE: L. BRYANT, J. SMITH, APPLIED RESEARCH ASSOCIATES, INC.

As can be seen, the cost associated with hardening the mailroom, loading dock, and lobby is usually small compared to the total project cost, and does not vary with available stand-off to a vehicle-delivered bomb. The cost associated with progressive collapse consideration is also constant with stand-off, since it is normally treated as threat-independent. There is a point at smaller stand-offs where the structural design is further impacted by the blast loading on the frame, resulting in larger framing members and additional cost. This issue occurs in close-in regions, particularly within about 50 feet. As the stand-off gets very small (as in a central business district alley) costs increase exponentially, and reasonable strat-

egies are to accept the risk, or to increase stand-off by street closure, together with active barriers and screening, if vehicular services to the building must be maintained, as discussed in Chapter 6.

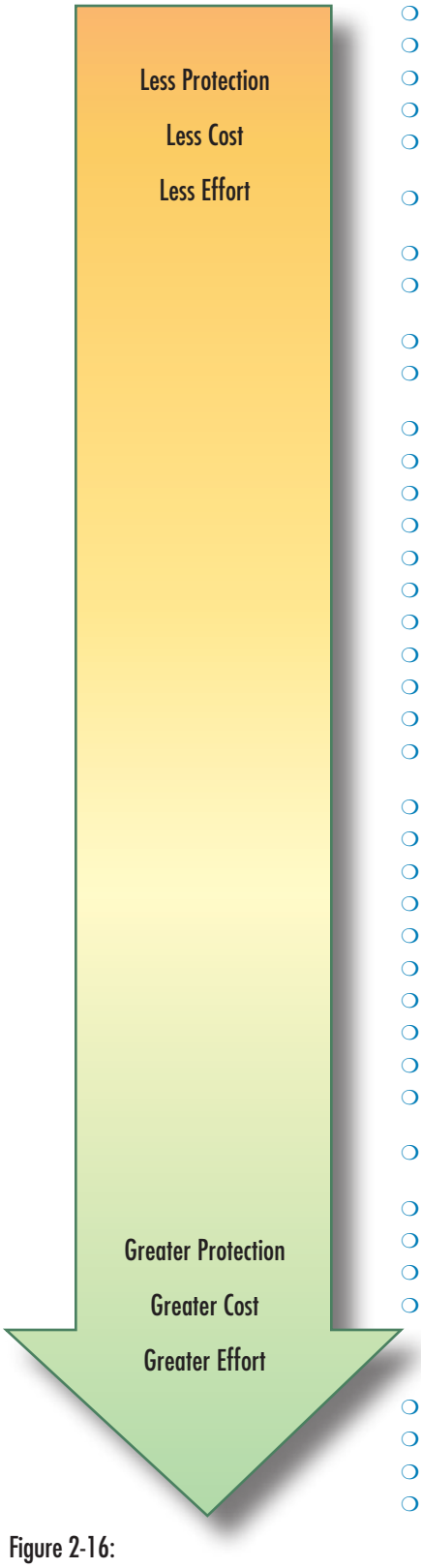
The requirements for walls and windows are a function of stand-off, as indicated for larger stand-off. However, most federal criteria place limits on the maximum levels for which various components must be designed. The limits placed on the design blast pressure and impulse for the medium and higher levels of protection cap the cost at a particular stand-off (limit), such that the cost for walls and windows does not increase within this limit. It must be noted that this limitation in blast resistance increases the inherent risk accepted with decreasing stand-off.

The sum of costs of hardening for the various components result in the "cost-of-hardening" curve indicated on Figure 2-15. This function has a plateau between about 50 feet stand-ff distance and the limit value for the relevant level of protection. At stand-off less than 50 feet, costs will increase very rapidly due to increased structural framing requirements to achieve acceptable risk. At larger stand-off values, costs decrease to a plateau where conventional design requirements may govern.

The cost components that may increase with increasing stand-off are those for land (site area) and perimeter protection. As noted above, the provision of increased stand-off results in increases in the distance to the defended perimeter, the area of the site, and the length of the perimeter that must be protected. Evaluation of the additional costs of hardening versus the costs of land and perimeter protection results in a general function of "Total Protection Cost." At stand-off values within the "limit," the risk continues to increase with decreasing stand-off.

Figure 2-15 illustrates the general characteristics of the cost and risk functions. Actual relative magnitudes and significance of individual cost components will vary for each case considered; i.e., these relationships will be different for each building and site considered. Also, the figures shown represent trends for more modern "conventional construction" and do not necessarily apply to existing construction. Although the general trends may be the same, the optimum stand-off distances will vary substantially based upon the myriad types and qualities of construction techniques that have been used for an existing building.

Although it is difficult to assign costs to different upgrade measures because they vary, based on the site-specific design, some generalizations can be made. A general spectrum of site mitigation measures ranging from least to greatest protection, cost, and effort is provided in Figure 2-16. The intent of this figure is to give a broad sense of the potential correlation between protection, cost, and effort.



- Place trash receptacles as far away from the building as possible.
- Remove any dense vegetation that may screen covert activity.
- Use thorn-bearing plant materials to create natural barriers.
- Identify all critical resources in the area (fire and police stations, hospitals, etc.).
- Identify all potentially hazardous facilities in the area (nuclear plants, chemical labs, etc.).
- Use temporary passive barriers to eliminate straight-line vehicular access to high-risk buildings.
- Use vehicles as temporary physical barriers during elevated threat conditions.
- Make proper use of signs for traffic control, building entry control, etc. Minimize signs identifying high-risk areas.
- Identify, secure, and control access to all utility services to the building.
- Limit and control access to all crawl spaces, utility tunnels, and other means of under building access to prevent the planting of explosives.
- Utilize Geographic Information Systems (GIS) to assess adjacent land use.
- Provide open space inside the fence along the perimeter.
- Locate fuel storage tanks at least 100 feet from all buildings.
- Block sight lines through building orientation, landscaping, screening, and landforms.
- Use temporary and procedural measures to restrict parking and increase stand-off.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much stand-off distance as possible from potential vehicle bombs.
- Separate redundant utility systems.
- Conduct periodic water testing to detect waterborne contaminants.
- Enclose the perimeter of the site. Create a single controlled entrance for vehicles (entry control point).
- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed circuit television cameras.
- Mount all equipment to resist forces in any direction.
- Include security and protection measures in the calculation of land area requirements.
- Design and construct parking to provide adequate stand-off for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Do not site the building adjacent to potential threats or hazards.
- Locate critical building components away from the main entrance, vehicle circulation, parking, or maintenance area. Harden as appropriate.
- Provide a site-wide public address system and emergency call boxes at readily identified locations.
- Prohibit parking beneath or within a building.
- Design and construct access points at an angle to oncoming streets.
- Designate entry points for commercial and delivery vehicles away from high-risk areas.
- In urban areas, push the perimeter out to the edge of the sidewalk by means of bollards, planters, and other obstacles. For better stand-off, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or through street closings.
- Provide intrusion detection sensors for all utility services to the building.
- Provide redundant utility systems to support security, life safety, and rescue functions.
- Conceal and/or harden incoming utility systems.
- Install active vehicle crash barriers.

Figure 2-16:
Mitigation options for site and layout design arranged in approximate order (top to bottom) of least to greatest protection, cost, and effort.

SOURCE: FEMA 426

Cost control is an area where the limited experience of security design and implementation presents a current problem. Comprehensive cost data is hard to obtain due to the relatively recent status of security design. Relatively little work has been published on the analysis of the comparative costs of alternative solutions, such as land costs for stand-off versus hardened structures, or the cost of physical solutions versus security operations. Non design options such as the comparative risks (and cost to mitigate) of different locations and tenant mixes, and the amount of increased rent that tenants are willing to pay for increased security improvement, must be subject to analysis and evaluation to enable a comprehensive risk management plan to be developed.

Cost management should be based on local cost information procured before the design process for budgeting purposes and during the design process for cost management purposes. Construction costs fluctuate and rapidly become out of date. Published indices attempt to ameliorate this problem, but they tend to be very broad in scope and are not very useful in application to a specific project. The state of the local market at the time of bidding and construction often has a major effect on cost.[1]

2.6 CONCLUSION

This chapter has provided a summary of the FEMA Risk Assessment procedure, which has been successfully used on many hundreds of buildings that belong to various government agencies.

The summary is intended to explain the general concepts of the procedure; for implementation of a complete risk assessment process, the reader should use the detailed guidance in FEMA 452. In addition, the reader is referred to FEMA 455, *Handbook for Rapid Visual Screening*. This procedure has been developed for use in assessing the risk of terrorist attack on standard commercial buildings in urban or semi-urban areas, and is intended to be applicable nationwide for all conventional building types. It can be used to identify the level of risk for a single building, or the relative risk among buildings in a portfolio, community, or neighborhood as a prioritization tool for further risk management activities.

Similarly, the sections on explosive forces and cost have presented an introduction to these issues as a background to the design of risk mitigation measures. Designers involved in security design need to have a general understanding of the concepts behind these two important topics of analysis.

1 Some portions of this section are based on a paper by Douglas Hall, Smithsonian Institute, entitled " *A Performance Based Design Methodology for Designing Perimeter Vehicle Barriers for Existing Facilities Using the ISC Security Design Criteria*"