Buildings and Infrastructure Protection Series

Reference Manual

to Mitigate Potential Terrorist Attacks Against Buildings

FEMA-426/BIPS-06/October 2011
Edition 2

Homeland Security

Science and Technology

Buildings and Infrastructure Protection Series

Reference Manual

to Mitigate Potential Terrorist Attacks Against Buildings

FEMA-426/BIPS-06/October 2011
Edition 2

Homeland Security

Science and Technology

FEMA

This publication was produced by the Department of Homeland Security, Science and Technology Directorate, Infrastructure Protection and Disaster Management Division.

The views, opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the official policy or position of the Department of Homeland Security (DHS) or other Federal agencies. The publication of these views by DHS does not confer any individual rights or cause of action against the United States. Users of information in this publication assume all liability from such use.

Hyperlinks to Web sites do not constitute endorsement by DHS of the Web site or the information, products, or services contained therein. DHS does not exercise any editorial control over the information on non-DHS Web sites. Users must adhere to any intellectual property rights contained in this publication or in material on hyperlinked Web sites.

All photographs and illustrations in this document were taken or created by DHS or a DHS contractor, unless otherwise noted.

Foreword and Acknowledgments

Background

This manual, part of the new Building Infrastructure Protection Series published by the United States (U.S.) Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Infrastructure Protection and Disaster Management Division (IDD), serves to advance high performance and integrated design for buildings and infrastructure. This manual was prepared as a component of the S&T program for infrastructure protection and disaster management; the overall goal of this program is to enhance the blast and chemical, biological, and radiological (CBR) resistance of our Nation's buildings and infrastructure to meet specific performance requirements at the highest possible level.

This manual revises and expands the original 2003 edition with updated risk assessment techniques, infrastructure resiliency standards, protective measures, and emerging technologies. Readability has been enhanced,

The U.S. Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) first developed FEMA 426, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, in 2003 to provide information on how to mitigate the effects of potential terrorist attacks against buildings. The intended audience included the building sciences community: architects and engineers working for public and private institutions; Federal, State, and local government officials; first responders (police, fire, and emergency services); and building owners.

and the reader is provided with a straightforward approach to find answers to pertinent questions. This revised manual provides guidance that will help design professionals translate a multitude of security concerns into solutions to make buildings more resilient to hazards and terrorist attacks. Security design goals are introduced as an integral part of the overall approach to building design.

Objectives and Scope

One of the objectives of this manual is to provide the tools and guidance to reduce physical damage to structural and nonstructural components of buildings and related infrastructure and to reduce resulting casualties caused by conventional bomb attacks and attacks using CBR agents. Although the material and the risk assessment methodology in this manual can be applied to most building types, it is intended to assist with the design and management of facilities in eight designated sectors outlined in the DHS 2009 *National Infrastructure Protection Plan* (the NIPP):

- Banking and Finance
- Commercial Facilities
- Communications
- Critical Manufacturing
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Postal and Shipping

The protective techniques described in this manual may not be applicable to lower occupancy buildings, such as single-family homes. Protective measures applicable to many critical facilities and other NIPP sectors (e.g., chemical plants, nuclear power plants) are addressed through existing sector-specific regulatory agencies and requirements (e.g., Nuclear Regulatory Commission) and are not included in this manual.

The purpose of this manual is to provide guidance to designers and decision makers in these sectors, to building professionals working for public and private institutions, and to first responder communities.

The purpose of this manual is to provide guidance to designers and decision makers in these sectors, to building professionals working for public and private institutions, and to first responder communities.

communities. It presents tools to help assess the performance of buildings and infrastructure against terrorist threats and to rank recommended protective measures.

A primary objective of this manual is the establishment of a common framework of terminology to facilitate the transfer of information.

A primary objective of this manual is the establishment of a common framework of terminology to facilitate the transfer of this information. For example, a basis for design is established by identifying the threat or hazard to which a building may be vulnerable. Within the military, intelligence, and law enforcement communities, the term "threat" is typically used to describe the potential threat elements (personnel) and their tactics for creating terrorism or manmade disasters. Within FEMA and other civil agencies, the term "hazard" is used in several different contexts. "Natural" hazard typically refers to a natural event, such as a flood, wind, or seismic event. "Human-caused" (or manmade) hazards are "technological" hazards and "terrorism." These are distinct from natural hazards, primarily, in that they originate from human activity. Furthermore, "technological" hazards are generally assumed to be accidental, in that their consequences are unintended. For the sake of simplicity, this manual uses the terms "threat" to describe terrorism or intentional attacks and "hazard" to describe accidental manmade or technological hazards.

Another objective of this manual is the transfer of design concepts that have been in use by DHS [these include concepts of the Interagency Security Committee (ISC) Standards and Best Practices, the General Services Administration (GSA), the U.S. Department of Veterans Affairs (VA), the U.S. Department of State (DOS), U.S. Department of Defense (DOD), Unified Facilities Criteria (UFC), and the military services] to commercial practice. Several valuable risk assessment methodologies are used by both the public and private sectors; however, this manual focuses on the methodology described in FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks* (2005), which has been used extensively by Federal agencies, along with State and local governments and the private sector.

Natural hazard typically refers to a natural event, such as a flood, wind, or seismic event. "Human-caused" (or manmade) hazards are "technological" hazards and "terrorism."

Building owners and managers must be the ones to determine their level of risk to each threat and decide from which threats to seek protection. Decisionmakers who consider their buildings to be at elevated risk may be able to use this guidance to mitigate the potential risks from hazards or terrorist attacks against their buildings.

The information contained in this manual is:

- Not mandatory,
- Not applicable to all buildings, and
- Not applicable when the recommended measures interfere with design measures adopted to reduce risk from other hazards, such as fire.

This manual presents techniques that can be implemented incrementally over time to increase resiliency as well as decrease the vulnerability of a building to hazards and terrorist threats. Many of the recommendations can be implemented quickly and cost effectively.

Overview of Changes from FEMA 426 and the National Infrastructure Protection Plan

Since 2003, when FEMA 426 was published, the country has focused increased attention on and gained substantial knowledge about the security of our built environment. The Federal Government has articulated its strategy for protecting people and assets against terrorist attacks in much greater detail. Many existing programs and initiatives were brought together through the formulation of the NIPP in 2009 by DHS and the following sector-specific agencies (SSAs): U.S. Department of Agriculture (USDA), DOD, U.S. Department of Education (ED), U.S. Department of Energy (DOE), U.S. Department of Health and Human Services (HHS), U.S. Department of the Interior, U.S. Department of Transportation (DOT), U.S. Department of the Treasury (Treasury), U.S. Environmental Protection Agency, and U.S. Coast Guard (USCG) (DHS 2009b; p. 19, Table 2-1).

The NIPP establishes a national framework for prioritizing protection initiatives and investments across 18 sectors to ensure that both public and private sector resources are used judiciously to minimize risk by lessening vulnerabilities, deterring threats, and reducing the consequences of terrorist attacks and other manmade and natural disasters in the most cost-effective manner. The NIPP risk management framework builds on many existing protective programs and initiatives, including those that were used to produce FEMA 426.

This manual presents techniques that can be implemented incrementally over time to increase resiliency as well as decrease the vulnerability of a building to hazards and terrorist threats.

USDA is responsible for agriculture and food (meat, poultry, and egg products). HHS is responsible for food other than meat, poultry, and egg products. Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over DOD, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures. The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities. The Water Sector includes drinking water and wastewater systems. The USCG is the SSA for the maritime transportation mode. As stated in Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection (DHS 2003), DOT and DHS will collaborate on all matters relating to transportation security and transportation infrastructure protection. ED is the SSA for the Education Facilities Subsector of the Government Facilities Sector.

To achieve its goals, the NIPP relies on all public and private agencies and other security partners to implement a variety of tasks. One such task is "enabling education, training, and exercise programs to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future" (DHS 2009b; p. 6). DHS S&T has undertaken the task to update and enhance the highly regarded *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings* (FEMA 426) to promote and distribute the latest information on security protection of buildings to professionals and organizations interested in enhancing the resiliency of the Nation's built environment.

The updated FEMA 426 delivers the following NIPP-defined and prioritized activities:

- Provide owners and operators of buildings and facilities timely, analytical, accurate, and useful information on a variety of threats to their assets.
- Articulate to corporate leaders, through education, training, and private communications, both the business and national security benefits of investing in security measures.
- Provide a rationale for creating a program of incentives for companies to adopt widely accepted and sound security practices voluntarily.
- Help private sector industry develop and clearly prioritize key missions, and enable their asset protection or restoration.
- Contribute materially to the emerging network for time-sensitive information sharing, restoration, and recovery support to facilities and services in the aftermath of incidents.

The NIPP provides a unifying structure for the integration of critical infrastructure and key resources (CIKR) protection efforts into a single national program. It describes an overall framework for integrating programs and activities that are underway in the various sectors, as well as new and developing CIKR protection efforts. The NIPP includes 18 sector-specific plans that detail the application of the overall risk management framework to each specific sector.

To facilitate the development or evolution of methodologies that allow cross-sector comparisons, the NIPP sets forth some basic risk management principles. Chief among them is the principle that assessing risk involves assessing three separate components: threat, consequence, and vulnerability.

Replacing "Asset Value" with "Consequences"

In FEMA 426, risk scores were calculated by multiplying asset value, threat, and vulnerability. To make this manual more compliant with the NIPP, the "asset value" component of the risk equation is being replaced with "consequences," which are defined as the effects of a terrorist attack or other hazard event that reflect the level, duration, and nature of the loss resulting from the incident. This concept and its relationship with asset value are discussed in more detail in Section 1.5.

Resilience and Continuity of Operations

This manual supports the concept of resilience and continuity of operations after an event. The NIPP defines resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions (DHS 2009b; p. 11). The 2009 National Infrastructure Advisory Council (NIAC)[1] report, *Critical Infrastructure Resilience Final Report and Recommendations*, defines infrastructure resilience as "the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event" (DHS 2009a; p.8).

The NIPP defines resilience as the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions.

When the building owner can maintain continuity of operations or has taken steps to ensure that key

1 www.dhs.gov/niac

functions will not be significantly affected by an event, then the owner will have increased resilience and lowered the overall risk. The definitions of consequences and vulnerability both have a time component to them to incorporate resilience into this risk assessment process (see Sections 1.5 and 1.6).

Making high-occupancy buildings resilient against terrorist attacks is a challenging task. It is difficult to estimate the risks or even predict how, why, and when the terrorists may strike. A successful protection strategy must establish a firm risk management framework that defines the processes for combining threat, consequences, and vulnerability information to produce a comprehensive, systematic, and rational assessment of risks. The risk assessment provides the basis for prioritizing protective activities for reducing the risk by improving the performance of buildings and their operations. Protection can include a wide range of activities, such as hardening facilities, increasing redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety programs, and implementing cyber security measures, among various others.

A successful protection strategy must establish a firm risk management framework that defines the processes for combining threat, consequences, and vulnerability information to produce a comprehensive, systematic, and rational assessment of risks.

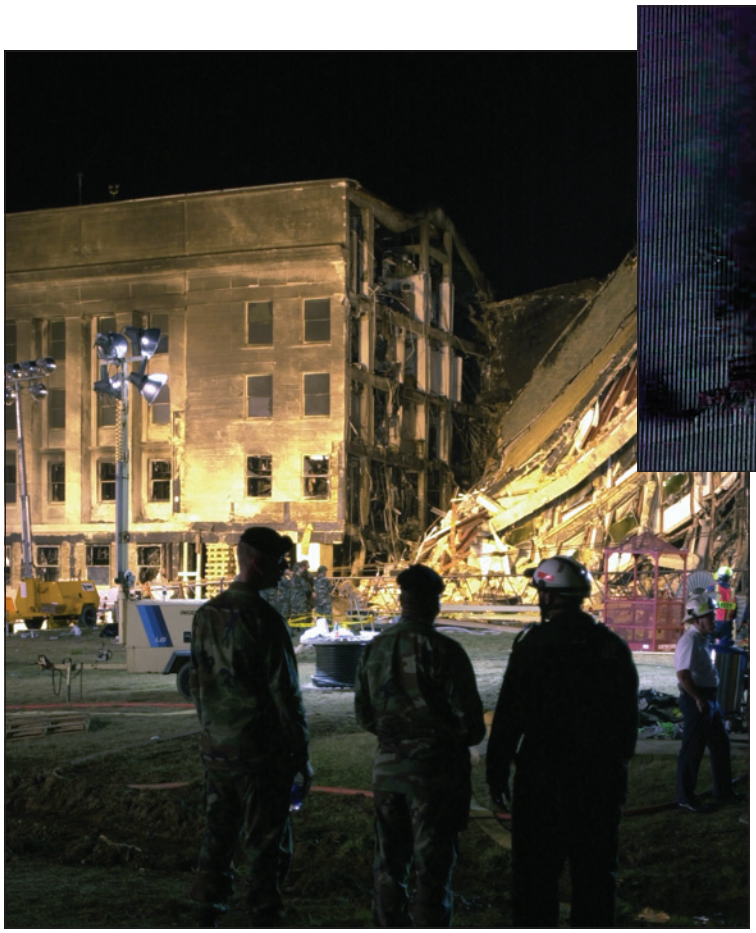
This manual presents a NIPP-compliant methodology that can be used for new buildings during the design process, as well as for existing buildings undergoing renovation. It discusses the components of the risk assessment process—threat or hazard assessment, consequences assessment, and vulnerability assessment—and the principal risk management concepts to introduce architects and engineers to the methodology that will help them identify the best and most cost-effective terrorism protective measures for each building's unique security needs.

Importance of Protecting the Building Stock

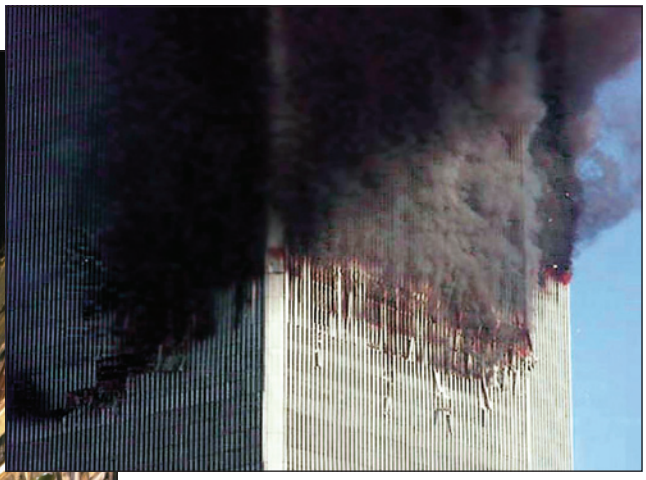
Traditionally, terrorist have selected buildings as a preferred target for their malicious attacks. This preference can be easily understood: there is a large inventory of vulnerable buildings throughout the Nation. Buildings are largely built in accordance with building codes lacking substantial design considerations intended to prevent or minimize the impact caused by CBR attacks. The collapse or failure of these buildings can have a severe effect on the all sectors of the economy and key resources, and can result in significant loss of life. For the U.S., the rise of terrorist attacks as a significant problem began with

the attacks of military installations and DOS embassies and consulates. An example of these terrorist attacks include the U.S. Embassy, Beirut, Lebanon, April 1983; Marine Barracks, Beirut, Lebanon, October 1983; World Trade Center, New York City, February 1993; Murrah Federal Building, Oklahoma, April 1995; the U.S. Embassy, Kenya, August 1998; U.S. Embassy Dar es Salaam, Tanzania, August 1998; and the World Trade Center in New York City and the Pentagon in Washington D.C., September 2001.

Since the World Trade Center attack, it has been recognized that terrorism has become a dominant domestic concern and that security can no longer be viewed as a standalone capability, but must be part of National strategy for protecting critical infrastructure. Building designs must include both physical security measures and resilience as objectives of an integrated design process to reduce the wide range of risk from terrorist attacks.



FEMA



FEMA

U.S. AIR FORCE

Figure 1:
Recent acts of terrorism (clockwise left to right, U.S. Pentagon, Arlington, VA; World Trade Center (WTC), New York City, NY; Murrah Federal Building, Oklahoma City, OK.

Protective Measures

When starting the design process for any new building or the renovation of an existing one, various owner, statutory, and building use inputs are required. These inputs must be integrated to ensure that mandatory building code requirements are met, as well as the owner's functional needs, and that the risks from natural and manmade hazards are mitigated to an acceptable level. In some cases, protective measures to enhance security may be in conflict with other design intentions. The assessment process helps to ensure an understanding of risk, so that it can be consciously addressed within the design process in accordance with available resources.

For natural hazards (e.g., earthquakes, floods, winds, grassland and forest fires) and building fire hazards (technological accidents), information is available in building codes, industry standards, and FEMA guidelines. For manmade hazards, the suggested course of action is less well defined. The U.S. has not yet developed unified building standards to address security concerns for private-sector buildings, similar to those developed for Federal facilities by DOD, DOS, ISC (Interagency Security Committee Standards), or the British Standard structural design code, which was developed because the United Kingdom has a long history of contending with repeated terrorist attacks on its home soil.

A challenge for the designer is to present appropriate information in a manner that allows the building owner or decision maker to make a rational, informed decision. For this purpose, this manual uses the concept of vulnerability-based threats, which, ideally, will be identified and agreed upon at the earliest stages of design (no later than preliminary design). The reason for this early identification is twofold. First, the designer must have a defined problem that will inform the final design. Second, by considering all threats or hazards early in the design, potential synergies among mitigation actions can be achieved to protect against both. One strategy may be beneficial against more than one threat or hazard; for example, designing moment frame connections between floors and columns and reinforcing exterior walls can mitigate risks from winds, explosive blasts, and earthquakes. To design protective measures and assist the building owner or decision maker, the designer must have some appreciation of the process of assessment of threats or hazards, consequences, vulnerability, and risk.

Many tools, techniques, and products are available for the development of new solutions for the design of new and renovation of existing buildings to minimize vulnerabilities and increase building performance. Advances in commercial satellite imagery, geographic information system (GIS) imagery (see Figures 2 and 3), structural hardening, agent

sensors, glass fragmentation films, ventilation protection, physical security systems, and many other building-related technologies and products provide the design professional with numerous tools to design buildings to better protect occupants from terrorist acts.

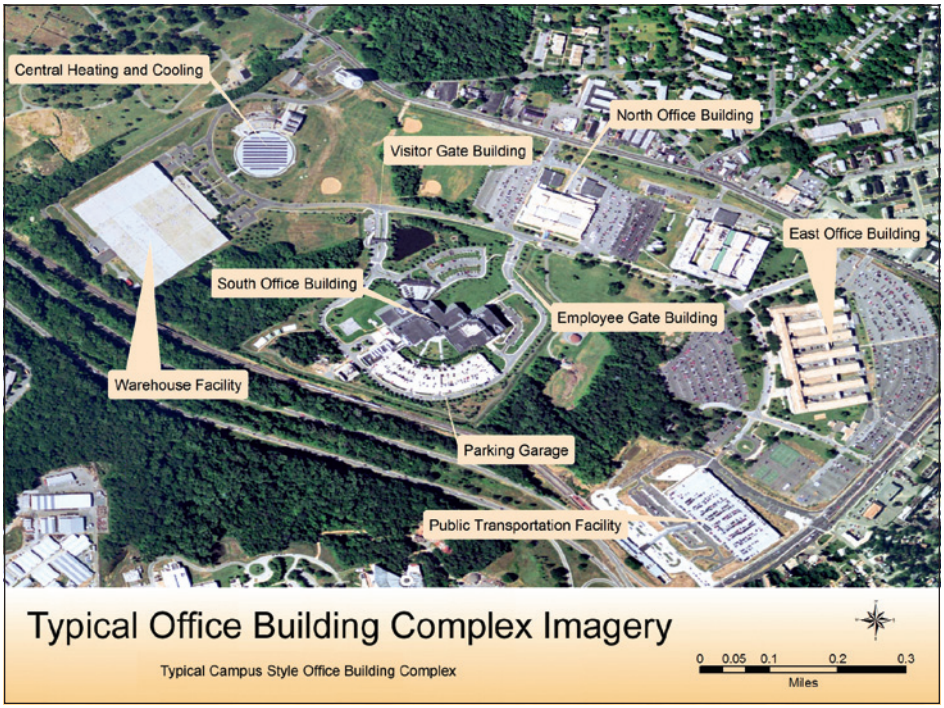


Figure 2:
GIS image of office building complex

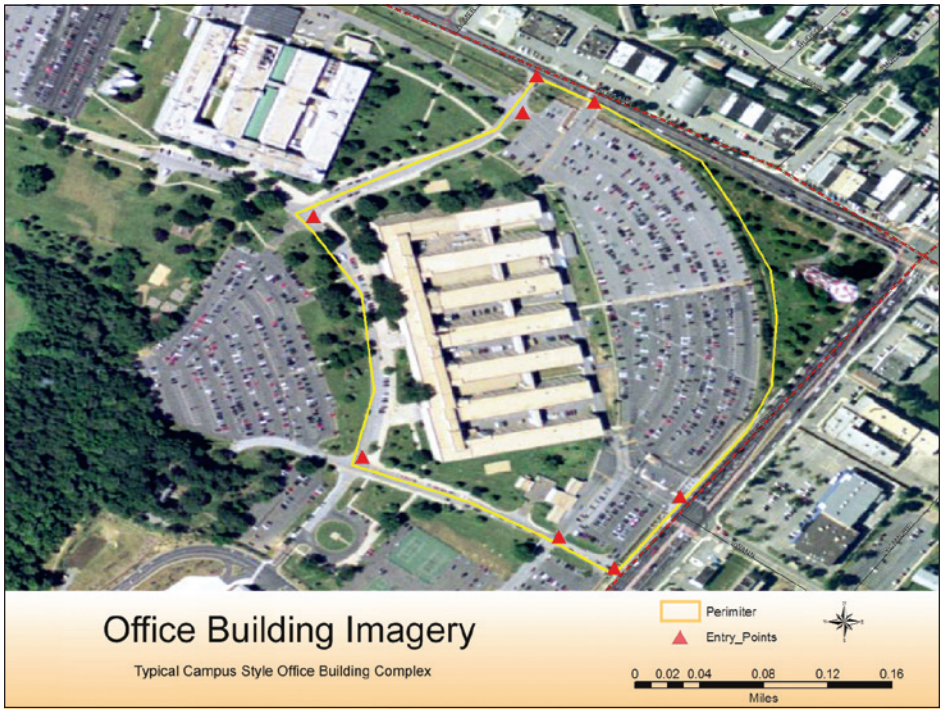


Figure 3:
Satellite imagery of East Office Building showing potential controlled perimeter and entry points

Organization and Content of the Manual

This manual contains many concepts that are based on current information contained in publications written by DHS, the Department of Commerce (Commerce), DOD (including Army, Navy, and Air Force), the U.S. Department of Justice, GSA, VA, the Centers for Disease Control and Prevention (CDC), the National Institute for Occupational Safety and Health (NIOSH), ISC, and others. It is intended to provide the user with an understanding of a methodology for assessing threats or hazards, consequences, vulnerability, risk, as well as the design considerations needed to improve protection of new and existing buildings and their occupants. This manual should be supplemented with more extensive technical resources, including the advice of experts when necessary.

The manual is organized as follows:

- Chapter 1 presents the method for calculating risk for a building by assessing the threat or hazard, and determining the vulnerability and consequences.
- Chapter 2 presents guidance for site layout and design. In addition, it provides security design guidance for a number of site functions, such as access controls, gatehouses and security screening, parking, loading docks, and service areas.
- Chapter 3 discusses the risks from attacks with explosives and presents guidance for integrating protection techniques into building design, including structural, architectural, building envelope, and nonstructural aspects.
- Chapter 4 discusses the risks from attacks with CBR agents and presents guidance for integrating protection techniques against CBR hazards into the building design.
- Chapter 5 provides security systems design guidance, as well as concepts for integrating various security subsystems to create an effective integrated protective system approach. This chapter highlights electronic security.

Acknowledgements

As with FEMA 426, the risk assessment methodology presented in this manual is based in part on work completed by VA. The DHS S&T acknowledges the Federal partners that assisted in the development of this manual, with revisions to concepts and methodologies based on FEMA 426 and 452, as well as FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* (2009). Federal partners include FEMA, the DHS National Protection and Programs Directorate, and the National Institute of Standards and Technology (NIST).

This publication was prepared under contract to DHS. It will be revised periodically, and comments and feedback to improve future editions are welcome. Please send comments and feedback to bips@dhs.gov.

Project Officers

Milagros Kennett, Senior Program Manager, Lead High Performance and Resilience Program, Department of Homeland Security, Science and Technology Directorate.

Paul Tertell/Civil Engineer, FEMA Risk Reduction Division, Department of Homeland Security.

Principal Authors

Robert Smilowitz, Weidlinger Associates, Inc.

Christopher Arnold, Building Systems Development, Inc.

Mohammed Ettouney, Weidlinger Associates, Inc.

Mark Hankewycz, The Protection Engineering Group, Inc.

William Blewett, Battelle Eastern Science and Technology Center

Mike Kaminskas, Raytheon UTD

Eric Letvin, URS Group, Inc.

Review Committee Members

Gwainevere Hess, Department of Homeland Security

Andrea Schultz, Department of Homeland Security

John Sullivan, Jr., PE, Portland Cement Association

Steve Cauffman, National Institute of Standards and Technology

Fred Krimgold, Virginia Polytechnic Institute and State University (Virginia Tech)

Arturo Mendez, New York Police Department

Lloyd Siegel, Department of Veterans Affairs

Mary Ellen Hynes, Department of Homeland Security

Jim Rossberg, American Society of Civil Engineers

Doug Hall, Smithsonian Institution

Michael Chipley, PMC Group

Earle Kennett, National Institute of Building Sciences

Technical Editors

Bogdan Srdanovic, APS Consulting

Nanne Eliot, National Institute of Building Sciences

Richard Walker Jr., URS Group, Inc.

Ivy Porpotage, URS Group, Inc.

Graphic Designer

Wanda L. Rizer, Design4Impact

Learn More:

http://www.dhs.gov/files/programs/high-performance-integrated-design-program.shtm

http://www.dhs.gov/files/programs/scitech-bips-tools.shtm

Table of Contents

Appendices

Figures

Chapter 1

Chapter 2

Chapter 3

Chapter 4

Chapter 5

Appendix C

Tables

Chapter 1

Chapter 5

1

Threat, Consequences, Vulnerability, and Risk

In this chapter:

The primary function of this chapter is to provide the methodology for risk assessments for existing buildings, the tools presented here can be used during the design process for new buildings as well as existing buildings undergoing renovation. This chapter also presents the risk management tools that design professionals can use to evaluate the advantages and costs of increased occupant safety, construction, operations and maintenance, resilience (the ability to anticipate, absorb, adapt to, or rapidly recover from an event), and decreased damage repair costs and downtime.

Since the attack on the World Trade Center (WTC), terrorism has become a dominant domestic concern. Security can no longer be viewed as a disassociated pursuit, but must be part of a national strategy for protecting CIKR. The protection of buildings has become one of the most important components of this strategy, not only because buildings have been the preferred targets of terrorist attacks, but also because they are the central venue of the Nation's economic life, the embodiment of its wealth and culture.

Buildings are constructed today in accordance with building codes that lack any substantial design considerations intended to prevent or minimize the impact caused by explosive blast or CBR attacks. Building collapse or failure of other building systems can have a severe effect on all sectors of the economy and key resources, and can result in significant loss of life. Building design today must integrate the traditional code guidelines with safety and security measures, and other environmental and economic considerations.

Buildings are constructed today in accordance with building codes that lack any substantial design considerations intended to prevent or minimize the impact caused by explosive blast or CBR attacks.

The protective function of integrated building design seeks to reduce the risks from hazards and threats that may cause building damage and thereby harm occupants, or passers-by, impair critical functions, and inflict economic and other losses. Integrated building design must, therefore, rely on the best available information about prevailing risks and the best protective measures that can be deployed against these risks. The objective of this chapter is to outline methods for (a) identifying the principal components of risk, (b) assessing their relative magnitude, and (c) ordering the risks in accordance with their significance. The methods presented in this chapter provide building owners and building professionals with tools to make benefit-cost-based decisions for risk reduction.

The protective function of integrated building design seeks to reduce the risks from hazards and threats that may cause building damage and thereby harm occupants, or passers-by, impair critical functions, and inflict economic and other losses.

This chapter also presents the risk management tools that design professionals can use to evaluate the advantages and costs of increased occupant safety, construction, operations and maintenance, resilience (the ability to anticipate, absorb, adapt to, or rapidly recover from an event), and decreased damage repair costs and downtime. While the primary function of this chapter is to provide the methodology for risk assessments for existing buildings, the tools presented here can be used during the design

process for new buildings as well as existing buildings undergoing renovation. The methodology presented in this chapter is based on the methodology for assessing risk described in FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks* (2005).

1.1 The Concept of Risk

The concept of risk is commonly used to characterize the likelihood of the occurrence of an unwanted outcome or event. It is commonly associated with terrorist threats, especially if the intelligence or past experience indicates that terrorists target a particular type of facility. Analysis of terrorist goals and motivations reveals that domestic and international CIKR are potentially the prime targets for attack (DHS 2009b; p. 11).

On the other hand, terrorists also take into consideration the level of protective measures employed at the target site. For example, the Murrah Federal Building in Oklahoma City became the target of an attack only when the aggressor realized that it was too difficult to get the attack vehicle close to his primary target, the Federal Bureau of Investigation (FBI) building. The attack on the Murrah Federal Building succeeded because it was possible to park the vehicle with a bomb immediately adjacent to the target—the office of the Bureau of Alcohol, Tobacco, and Firearms. However, even if the available information does not indicate that a particular critical infrastructure or facility is the potential target of attack, its vulnerabilities may warrant serious consideration of its exposure to terrorist risk.

Finally, the potential consequences of a successful attack greatly influence the level of risk. Minor potential consequences may have a low-risk rating even with a potentially high likelihood of occurrence. Considering that terrorists always seek maximum impact for their attacks, the risk of a catastrophic event with grave consequences may have higher risk rating, even with a low likelihood of occurrence, thereby requiring more costly and complex protective measures.

Infrastructure, or asset-based, resilience is closely aligned with the way modern businesses manage strategic, operational, and financial risks and the way governments absorb societal shocks from disasters. For businesses, the need to be resilient is driven by competitive market forces because customers and shareholders expect products and services to be delivered despite disruptive events. In certain sectors, leading companies have incorporated risk management, which includes risk assessment and risk acceptance, into their corporate culture, and many consider it a competitive differentiator. This sophisticated risk management includes protection, i.e. reduced vulnerabilities, which is a critical component of risk management in asset-based sectors.

Simply stated, risk is influenced by the nature and magnitude of a threat, the vulnerability to that threat, and the consequences that could result from a successful attack. The risk assessment process analyzes the probability of occurrence of each particular threat for each asset. The potential losses are determined based on potential consequences and vulnerability of the asset.

Risk is influenced by the nature and magnitude of a threat, the vulnerability to that threat, and the consequences that could result from a successful attack.

The concept of "acceptable risk" is based on the recognition that eliminating risk altogether is an unrealistic goal. Some damage from a terrorist attack must be anticipated. The goal is to determine how much and what kind of damage is acceptable. For example, total building collapse may be unacceptable, but broken windows that result in minimal injuries may be unavoidable and therefore acceptable. The determination of acceptable risk is made by the building owner or principal decision makers with the assistance of design professionals, in-house staff, or security consultants.

The goal of the risk assessment process is to determine which protective measures are required to achieve the level of protection sought in a particular building. See Section 3.1.4 for discussion of levels of protection. Protective measures may reduce risk by deterring or detecting the potential terrorist, preventing the damage and injury sought by that terrorist, or devaluing the asset or resulting consequences of loss to reduce the building's attractiveness to the terrorist prior to or during the execution of an attack. Protective measures may also reduce risk of damage or injury by providing a certain level of protection if the attack does occur, which may also serve to further deter an aggressor.

The goal of the risk assessment process is to determine which protective measures are required to achieve the level of protection sought in a particular building.

The application of any security design criterion is based on a project-specific risk assessment, similar to that outlined in the following sections, which looks at threats, assets and consequences, and vulnerabilities as the components of risk.

1.2 DHS/FEMA Risk Assessment Overview

To reduce the risks and increase safety and security, many factors must be considered. Figure 1-1 depicts the assessment process used to identify the best and most cost-effective terrorism protective measures for a building's unique security needs. The building's risk is calculated based on assessments of the threat/hazards unique to the building, the consequences of an attack or hazard event on the building, and the building's vulnerability to threat/hazards. The risk assessment provides engineers and architects with a relative risk profile that defines which assets are at the greatest risk against specific threats.

This approach is based on a three-step process. The first step is to conduct a threat assessment to identify, define, and quantify the threats or hazards (see Section 1.4). A terrorist threat derives from aggressors (people or groups) known to exist and to have the intent and capability of using hostile actions to achieve their goals. A measure of threat is the probability that a particular type of attack will be mounted against a particular target.

The second step of the assessment process identifies the potential consequences of an attack, and the resulting loss of lives or building functions (see Section 1.5). A consequences assessment looks at the value of a building's critical assets, identifies those that need to be protected, and considers the importance of the building's operations within a wider network of public or private activities. A measure of consequences is the potential magnitude of losses resulting from a successful attack of a specific type on a specific target.

The third step identifies potential vulnerabilities of critical assets against a broad range of identified threats or hazards (see Section 1.6). A measure of vulnerability is the probability that damages or losses will occur as a result of a successful attack of the specified type. The vulnerability assessment provides a basis for determining the type of protective measures required to protect the critical assets. The vulnerability assessment is the

DHS has developed several manuals to facilitate assessment of risk in buildings. These are: FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks* (2005), and FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risk* (2009). DHS has recently released the Integrated Rapid Visual Screening for all hazards (Building and Infrastructure Protection Series [BIPS] 04) . BIPS 04 allows the users to assess the risks from explosive blast, CBR incidents, earthquakes, floods, winds, and fire in a fast manner using a friendly methodology and software.

bridge in the methodology between threats or hazards, consequences, and the resultant level of risk.

As the data are assembled and processed, assessors are able to identify and quantify the risks (see Section 1.7). Risk assessment involves analyzing the threat or hazard, consequences of a successful attack, and vulnerabilities to determine the level of risk for each critical asset that may represent a legitimate target against each applicable threat. The purpose of risk assessment is to provide information to the building owner and the design community that enables them to decide which protective options are the most feasible and cost effective against which threats.

After risks are quantified and ordered, assessors identify and prioritize protection measures that reduce these risks.

After risks are quantified and ordered, assessors identify and prioritize protection measures that reduce these risks. When the risk assessment process is completed, stakeholders are frequently left with the awareness that the number of assets that may require protective measures exceeds the available resources. Thus, decisions must be made to prioritize and focus the available resources on the most important and most effective mitigation activities. Chapters 3, 4, and 5 describe a variety of protective measures and discuss their relative merits with respect to asset resilience.

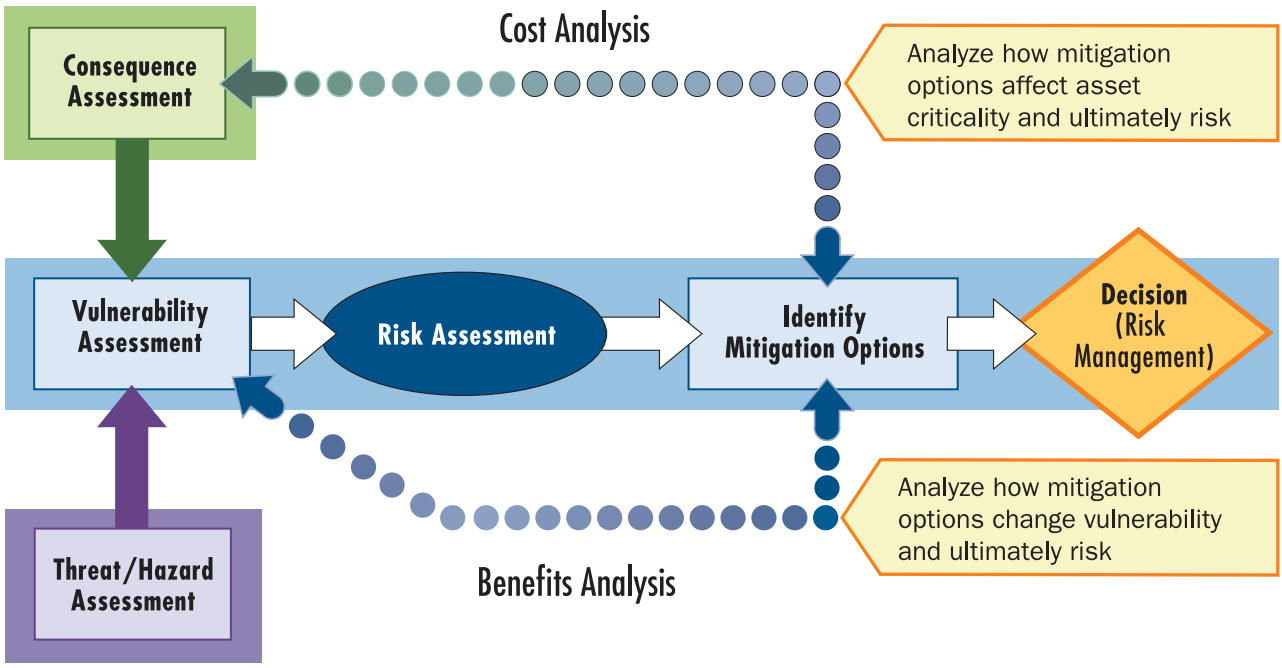


Figure 1-1: Risk assessment process model

1.3 DHS/FEMA Risk Assessment Types and Processes

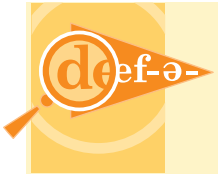
The level of assessment for a building depends on a number of factors, including building type, location, method of construction, number of occupants, economic life, and other owner-specific concerns. The different levels of assessment in FEMA 452, FEMA 455, and BIPS 04 are described as a tiers (See 2.3.1). A tiered assessment process includes successively more refined analysis when more detailed information is needed. FEMA 452, FEMA 455, and BIPS 04 provide risk scores for each threat, consequence, and vulnerability to an asset. FEMA 455 and BIPS 04 methodology calculates the scores automatically based on the information provided by the assessor. FEMA 452 relies on the assessor's judgment in determining the scores. The risk score helps to prioritize protective measures by identifying those that have the greatest benefit-cost ratio for reducing the risks. Knowing the risk score helps decision makers prioritize and select the most appropriate set of protective measures.

"Infrastructure resilience describes the ability to reduce the magnitude and/or of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potential disruptive event." (DHS 2009a).

Detailed vulnerability evaluations of facilities are technically complex and expensive procedures that require substantial mobilization of experts, resources, and time. They should be performed only when risks are very high or when lower level assessments confirm that a higher level investigation is required. Consequently, using simpler procedures (i.e., FEMA 455 and BIPS 04) initially to rapidly provide the vulnerability profile of different types of buildings or facilities is important. Initial assessments may uncover vulnerabilities or indicate that more complex evaluation procedures (i.e., FEMA 452) are warranted for the most critical assets.

1.3.1 FEMA 452 Risk Assessment Methodology

- **Tier 1** (FEMA 452 Risk Assessment Methodology) assessment is a screening phase that identifies the primary vulnerabilities and protective options; it is a "70 percent" assessment (see Table 1-1). In most cases one or two experienced assessment professionals can conduct a Tier 1 assessment in approximately two days with the building owner and key staff. It involves a "quick look" at the site perimeter, building, core functions, infrastructure, drawings, and plans. A Tier 1 assessment will likely be sufficient for the majority of commercial buildings and other non-critical facilities and infrastructure.



Tier 1 assessment is a screening phase that identifies the primary vulnerabilities and protective options.

Table 1-1: Tier 1 Screening Phase

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	Standard commercial office buildings	1 Site and Architectural 1 Security Systems and Operations	1 day	• Review technical area and general site analysis.
On-Site Evaluation			1 day per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports. • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings. • Receive input on the assessment process.
Develop Mitigation Options			Typically 1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures.

- **Tier 2** (FEMA 452 Risk Assessment Methodology) assessment is a full onsite evaluation by assessment specialists that provides a robust evaluation of system interdependencies, vulnerabilities, and protective options; it is a "90 percent" assessment solution (see Table 1-2). A Tier 2 assessment, typically conducted by three to five assessment specialists, can be completed in three to five days and requires

significant key building staff participation (e.g., providing access to all site and building areas, systems, and infrastructure) and an in-depth review of building design documents, drawings, and plans. A Tier 2 assessment is likely to be sufficient for most high-risk buildings, such as iconic commercial buildings, government facilities, schools, hospitals, and other designated high-value infrastructure.

Table 1-2: Tier 2 Full Onsite Evaluation

Task	Building Type	Team Composition	Duration	Activity
Information Gathering and Review	High-risk or iconic buildings Commercial buildings, government facilities, schools, and hospitals Designated high asset value infrastructure	1 Site and Architectural (recommended as Team leader) 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 Landscape Architect 1 IT and Telecommunications 1 Security Systems and Operations	1 day per assessor	• Review technical area and general site analysis collected during the Tier 1 assessment.
On-Site Evaluation			2 to 4 days per assessor	• Complete the Critical Function and Critical Infrastructure matrices; perform a limited technical review using the Building Vulnerability Assessment Checklist; input site, vulnerability, and mitigation information into the database; write reports. • Prepare a verbal or PowerPoint presentation with key findings to review with building owners' and stakeholders' major findings. • Receive input on the assessment process.
Develop Mitigation Options			1 to 3 days per assessor	• Prepare a Preliminary Report, including findings and feedback from stakeholders. This report should include concept and cost mitigation options. • Prepare a written Final Report that lists the vulnerabilities, observations, and mitigation options. Very rough order of magnitude cost estimates may be developed using standard unit costs for blast, CBR, and physical security infrastructure and equipment. • Prepare a Vulnerability Portfolio with recommendations for incorporation into Emergency Operations, Disaster Recovery, and other plans or procedures.

- **Tier 3** (FEMA 452 Risk Assessment Methodology) is the third type of rapid assessment methodology. Tier 3 assessments provide a detailed evaluation of the building using blast and weapons of mass destruction models to determine building response, survivability, and recovery, followed by the development of protective options. Tier 3 methodology is typically performed for high-value and critical infrastructure assets. A Tier 3 assessment (see Table 1-3), typically conducted by engineering and scientific experts, requires detailed design information, including drawings and other building information. Modeling and analysis can take several days or weeks. The assessment team, while not defined for this tier, may be composed of eight to 12 people.

Table 1-3: Tier 3 Detailed Evaluation

Building Type	Team Composition	Activity
High value and critical infrastructure assets	1 Site and Architectural - Team leader 1 Structural and Building Envelope 1 Mechanical, Electrical, and Power Systems and Site Utilities 1 IT and Telecommunications Modeler 1 Security Systems and Operations 1 Explosive Blast Modeler 1 CBR Modeler 1 Cost Engineer 1 Landscape Architect	• A typical Tier 3 Assessment Team will use the results of the Tier 2 assessment and involve modeling and analysis of the building and related systems using advanced blast and WMD models and applications. Blast analysis will include structural progressive collapse, glazing, and effects of building hardening. CBR analysis should evaluate the effects of the agents released externally and internally to provide the dispersion, duration, and exposure of the building systems and occupants. The IT and Telecommunications Modeler should evaluate effects on all IT systems assuming cascading equipment failure and long-term access denial to critical equipment, data, and on-site administrative capability. • The Tier 3 assessment will provide detailed building response, survivability, and recovery information used to develop enhanced and accurate costing of mitigation options.

1.3.2 DHS Integrated Rapid Visual Screening of Buildings (BIPS 04)

DHS S&T has developed IRVS procedures for assessing risks to a building from natural and manmade hazards with the potential to cause catastrophic losses (fatalities, injuries, damage, and business interruption).

This procedure is an enhanced version of FEMA 455 and includes improvements to the methodology, updates to the catalog of building characteristics, and updates to the forms that incorporate natural hazards, building types, and critical functions. The Method is detailed in DHS BIPS 04, *Integrated Rapid Visual Screening of Buildings.*

IRVS is a Tier 1 assessment tool, a quick procedure for obtaining a preliminary risk-assessment rating. The natural and manmade hazards considered in the tool include: internal and external explosive attacks, external CBR releases, earthquakes, high winds, floods, landslides, and fires. Risk is determined by evaluating key building characteristics for threats, consequences, and vulnerabilities. The screening process can be conducted by one or two screeners and completed in one to five hours. The procedure is designed to be a flexible tool to identify the level of risk for a single building, to identify the relative risk among buildings in a community or region, or to prioritize for further risk management activities. Experts can use the information from the visual inspection to support higher level assessments and analysis of mitigation options. The tool also computes a resiliency index for the above hazards, as well as a multihazards index matrix.

The latest improvements to the IRVS database software have made the IRVS methodology completely digital.

The latest improvements to the IRVS database software have made the IRVS methodology completely digital. The software facilitates data collection and functions as a data management tool. Assessors can use the software on a tablet computer or laptop to collect, store, and report screening data systematically. The software can be used during all phases (pre-field, field, and post-field) of the IRVS procedure. Similar methodologies have also been prepared and released for the risk assessment of mass transit and tunnels.

FEMA 455 describes a rapid visual screening procedure, effectively a "Pre-Tier 1" assessment. It is designed to be conducted by one or two screeners and, depending on the level of effort and access to building information, can be completed in as little as few hours or as much as two days. DHS S&T is currently expanding FEMA 455 to include natural hazards.

BIPS 04 is an enhanced version of FEMA 455 and includes improvements to the methodology, updates to the catalog of building characteristics, and updates to the forms that incorporate natural hazards, building types, and critical functions.

FEMA 452 outlines methods for identifying the critical assets and functions within buildings, determining the threats to those assets, and assessing the vulnerabilities associated with those threats. Tier 1 is a "70 percent" assessment, while Tier 2 represents a "90 percent" assessment solution.

1.4 Threat and Hazard Assessment

The NIPP defines threat as any "natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property" (DHS 2009b). FEMA 452, on which the following threat assessment methodology is based, defines threat as any indication, circumstance, or event with the potential to cause loss of, or damage to, an asset.

Hazard is defined in several contexts: natural, manmade, or technological. Natural hazard typically refers to a source of harm or difficulty created by a meteorological, environmental, or geological phenomenon or combination of phenomena. Manmade or technological hazards and terrorism are distinguished from natural hazards in that they originate from human activity. Technological hazards are generally assumed to be accidental and their consequences unintended.

This manual, while focused on mitigation of risk associated with terrorist threats, promotes an integrated assessment approach that combines all hazards (natural and manmade). For example, the Tier 1 IRVS integrates assessments for vulnerability to threats as well as to earthquakes, floods, high winds, and fire.

In the context of individual buildings, threats are defined in terms of specific types of attack on a specific set of targets. Law enforcement and intelligence agencies are more concerned with identifying and stopping the individuals and groups who may pose a threat, but for the purpose of protecting structures and buildings, identifying the attack types for specific targets may be more important than the potential perpetrators.

Assessing the threats or hazards that may affect an asset involves:

- Identifying the threat type and hazard
- Determining the threat rating

1.4.1 Threat Type and Hazard Identification

To facilitate the identification of potential threats that may affect an asset, a myriad of sources with threat/hazard assessment information are available at the local, State, and Federal level of government, as well as numerous quasi-government and private entities. Assessments of threat/hazard are routinely disseminated at the local and State level by law enforcement and emergency management agencies, by State Homeland Security Offices, and by numerous Federal agencies such as DHS, the FBI, and the CDC.

Other good sources of information include the National Counterterrorism Center (NCTC) and the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). NCTC is the primary organization in the Federal Government to integrate and analyze all intelligence pertaining to terrorism and counterterrorism and to conduct strategic operational planning by integrating all instruments of national power. HITRAC assesses the overall threat to a sector and individual assets whenever specific information is available.

Experience tells us that potential threat elements or aggressors often seek publicity for their cause, monetary gain, or political gain through their actions.

Unlike historical and quantitative data available on natural hazards, data for manmade hazards may be scarce and are often largely subjective. This is especially true for terrorist threats, which are by nature very volatile and unpredictable. Identifying all the possible ways in which a variety of aggressors may harm a facility may require very a complicated and detailed analysis of every possible type of attack. In reality, risk assessment usually focuses on a limited number of probable attack types, mainly those using various explosive devices, or CBR agents.

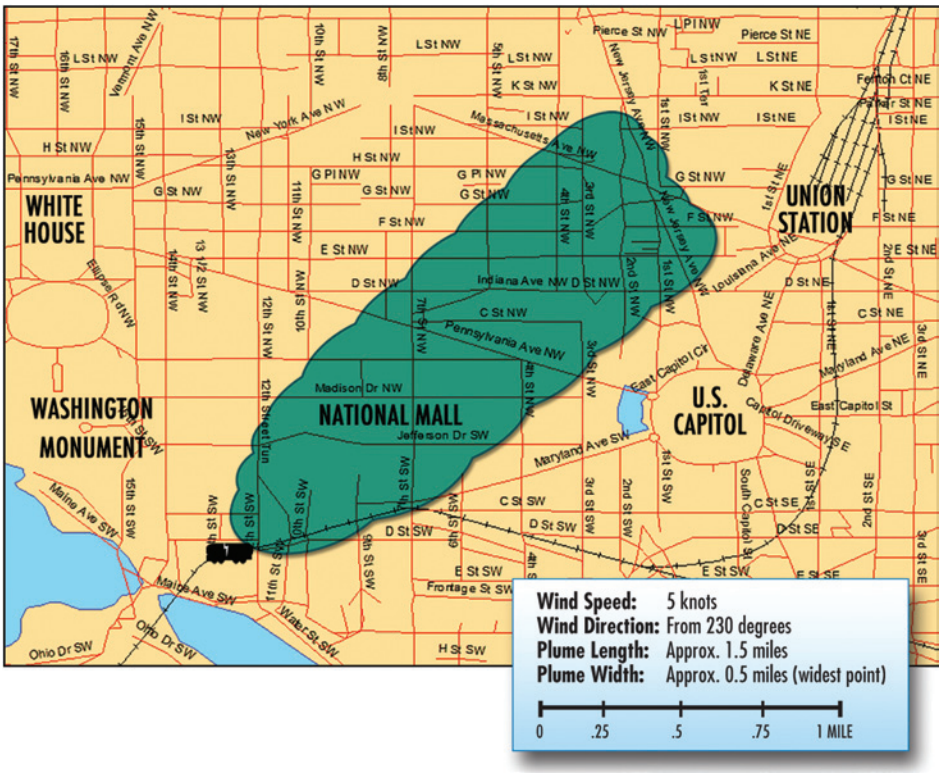
Experience tells us that potential threat elements or aggressors (those people with intent to do harm) often seek publicity for their cause, monetary gain (in some instances), or political gain through their actions. These actions are intended to injure or kill people; destroy or damage facilities, property, equipment, or resources; or gain advantage or cause damage by stealing equipment, material, or information. The attacks usually include surveillance (visual/audio, standoff, or planted), forced entry, in secrecy or by an open attack, or remote activation of a variety of weapons. The attack weapons can include incendiary devices, small arms (rifles and handguns), standoff military-style weapons (rocket propelled grenades or mortars) (see Figure 1-2), explosives, and CBR agents, individually or combined with explosives to aid in dispersion.

Figure 1-2:
Aggressor weapons

Explosives include homemade and stolen industrial and military varieties, and can be packaged as small to very large devices (e.g., mail bombs to vehicle bombs). Aggressor tactics run the gamut: moving vehicle bombs; stationary vehicle bombs; exterior attacks (thrown objects such as rocks, Molotov cocktails, hand grenades, or hand-placed bombs); standoff weapons attacks (military or improvised larger direct- and indirect-fire weapons); ballistic attacks (small arms handled by one individual); covert entries (gaining entry by false credentials or circumventing security with or without weapons); mail bombs (delivered to individuals); supply

bombs (larger bombs processed through shipping departments); airborne contamination (CBR agents used to contaminate the air supply of a building as hypothetically demonstrated in Figure 1-3); and waterborne contamination (CBR agents injected into the water supply).

Figure 1-3:
Estimated plume from a 1-ton chlorine spill in Washington, DC



For technological hazards, gathering information about the presence of hazardous materials (hazmat) and procedures from the local fire department and hazmat unit, Local Emergency Planning Committee (LEPC), and State Emergency Response Commission (SERC) is important. LEPC and SERC, the local and State organizations established in accordance with the requirements of the Emergency Planning and Community Right-to-Know Act of 1986, identify critical facilities in vulnerable zones and generate emergency management plans. Additionally, most fire departments are aware of which industries in the local area handle the most combustible materials and the hazmat unit knows who handles materials that could have a negative effect on people and the environment. In many jurisdictions, the hazmat unit is part of the fire department.

Table 1-4 provides the design professional with a general profile of events associated with the spectrum of manmade threats/hazards and can be used as a tool for threat assessments. Figure 1-4 illustrates how a terrorist or aggressor might analyze the building or target to determine the type of attack, type of weapon, and tactics to employ to defeat the building or critical mission/business function. Chapter 2 provides additional

information on manmade hazards, and Appendix C provides a complete list of CBR agents. More information about identifying primary threats can be found in Task 1.1 of FEMA 452.

Identifying technological hazards is especially important, not only to help protect communities against technological accidents but, more importantly, to protect against the intentional use of these hazards for terrorist attacks.

Table 1-4: Event Profiles for Terrorism and Technological Hazards

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Improvised Explosive Device (Bomb) • Stationary Vehicle • Moving Vehicle • Mail • Supply • Thrown • Placed • Suicide Bomber	Detonation of explosive device on or near target; via person, vehicle, or projectile.	Instantaneous; additional secondary devices may be used, lengthening the duration of the threat/ hazard until the attack site is determined to be clear.	Extent of damage is determined by type and quantity of explosive. Effects generally static other than cascading consequences, incremental structural failure, etc.	Blast energy at a given stand-off is inversely proportional to the cube of the distance from the device; thus, each additional increment of stand-off provides progressively more protection. Exacerbating conditions include ease of access to target; lack of barriers/ shielding; poor construction; and ease of concealment of device.
Armed Attack • Ballistics (small arms) • Stand-off Weapons (rocket propelled grenades, mortars	Tactical assault or sniper attacks from a remote location.	Generally minutes to days.	Varies, based upon the perpetrator's intent and capabilities.	Inadequate security can allow easy access to target, easy concealment of weapons, and undetected initiation of an attack.
Chemical Agent • Blister • Blood • Choking/ Lung/ Pulmonary • Incapacitating • Nerve • Riot Control/ Tear Gas • Vomiting	Liquid/aerosol contaminants can be dispersed using sprayers or other aerosol generators; liquids vaporizing from puddles/ containers; or munitions.	Chemical agents may pose viable threats for hours to weeks, depending on the agent and the conditions in which it exists.	Contamination can be carried out of the initial target area by persons, vehicles, water, and wind. Chemicals may be corrosive or otherwise damaging over time if not remediated.	Air temperature can affect evaporation of aerosols. Ground temperature affects evaporation in pools of liquids. Humidity can enlarge aerosol particles, reducing the inhalation hazard. Precipitation can dilute and disperse agents, but can spread contamination. Wind can disperse vapors, but also cause target area to be dynamic. The micro-meteorological effects of buildings and terrain can alter travel and duration of agents. Shielding in the form of sheltering in place may protect people and property from harmful effects for a limited time.

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
Biological Agent • Anthrax • Botulism • Brucellosis • Plague • Smallpox • Tularemia • Viral Hemorrhagic Fevers • Toxins (Botulinum, Ricin, Staphylococcal Enterotoxin B, T-2 Mycotoxins)	Liquid or solid contaminants can be dispersed using sprayers/ aerosol generators or by point or line sources such as munitions, covert deposits, and moving sprayers. May be directed at food or water supplies.	Biological agents may pose viable threats for hours to years, depending on the agent and the conditions in which it exists.	Depending on the agent used and the effectiveness with which it is deployed, contamination can be spread via wind and water. Infection can be spread via human or animal vectors.	Altitude of release above ground can affect dispersion; sunlight is destructive to many bacteria and viruses; light to moderate winds will disperse agents, but higher winds can break up aerosol clouds; and the micro-meteorological effects of buildings and terrain can influence aerosolization and travel of agents.
Radiological Agent • Alpha • Beta • Gamma	Radioactive contaminants can be dispersed using sprayers/ aerosol generators, or by point or line sources such as munitions, covert deposits, and moving sprayers.	Contaminants may remain hazardous for seconds to years, depending on material used.	Initial effects will be localized to site of attack; depending on meteorological conditions, subsequent behavior of radioactive contaminants may be dynamic.	Duration of exposure, distance from source of radiation, and the amount of shielding between source and target determine exposure to radiation.
Cyber Attacks	Electronic attack using one computer system against another.	Minutes to days.	Generally no direct effects on built environment.	Inadequate security can facilitate access to critical computer systems, allowing them to be used to conduct attacks.
High-Altitude Electromagnetic Pulse (HEMP)	An electromagnetic energy field produced in the atmosphere by the power and radiation of a nuclear explosion. It can overload computer circuitry with effects similar to, but causing damage much more swiftly than a lightning strike.	It can be induced hundreds to a few thousand kilometers from the detonation.	Affects electronic systems. There is no effect on people. It diminishes with distance, and electronic equipment that is turned off is less likely to be damaged.	To produce maximum effect, a nuclear device must explode very high in the atmosphere. Electronic equipment may be hardened by surrounding it with protective metallic shielding that routes damaging electromagnetic fields away from highly sensitive electrical components.

Threat/Hazard	Application Mode	Duration	Extent of Effects; Static/Dynamic	Mitigating and Exacerbating Conditions
High Power Microwave (HPM) EMP	It is a non-nuclear radio frequency energy field. Radio frequency weapons can be hidden in an attaché case, suitcase, van, or aircraft. Energy can be focused using an antenna, or emitter, to produce effects similar to HEMP, but only within a very limited range.	An HPM weapon has a shorter possible range than HEMP, but it can induce currents large enough to melt circuitry, or it can cause equipment to fail minutes, days, or even weeks later. HPM weapons are smaller-scale, are delivered at a closer range to the intended target, and can sometimes be emitted for a longer duration.	Vulnerable systems include electronic ignition systems, radars, communications, data processing, navigation, electronic triggers of explosive devices. HPM capabilities can cause a painful burning sensation or other injury to a person directly in the path of the focused power beam, or can be fatal if a person is too close to the microwave emitter.	Very damaging to electronics within a small geographic area. A shockwave could disrupt many computers within a 1-mile range. Radio frequency weapons have ranges from tens of meters to tens of kilometers. Unlike HEMP, however, HPM radiation is composed of shorter wave forms at higher-frequencies, which make it highly effective against electronic equipment and more difficult to harden against.

Note: Cyber attack focuses on denial of service, worms, and viruses designed to attack or destroy critical infrastructure related systems such as energy management, supervisory control and data acquisition systems, security, control valves, and voice over internet protocol telephones, which are critical systems that support multiple functions and are becoming increasingly connected to the internet.

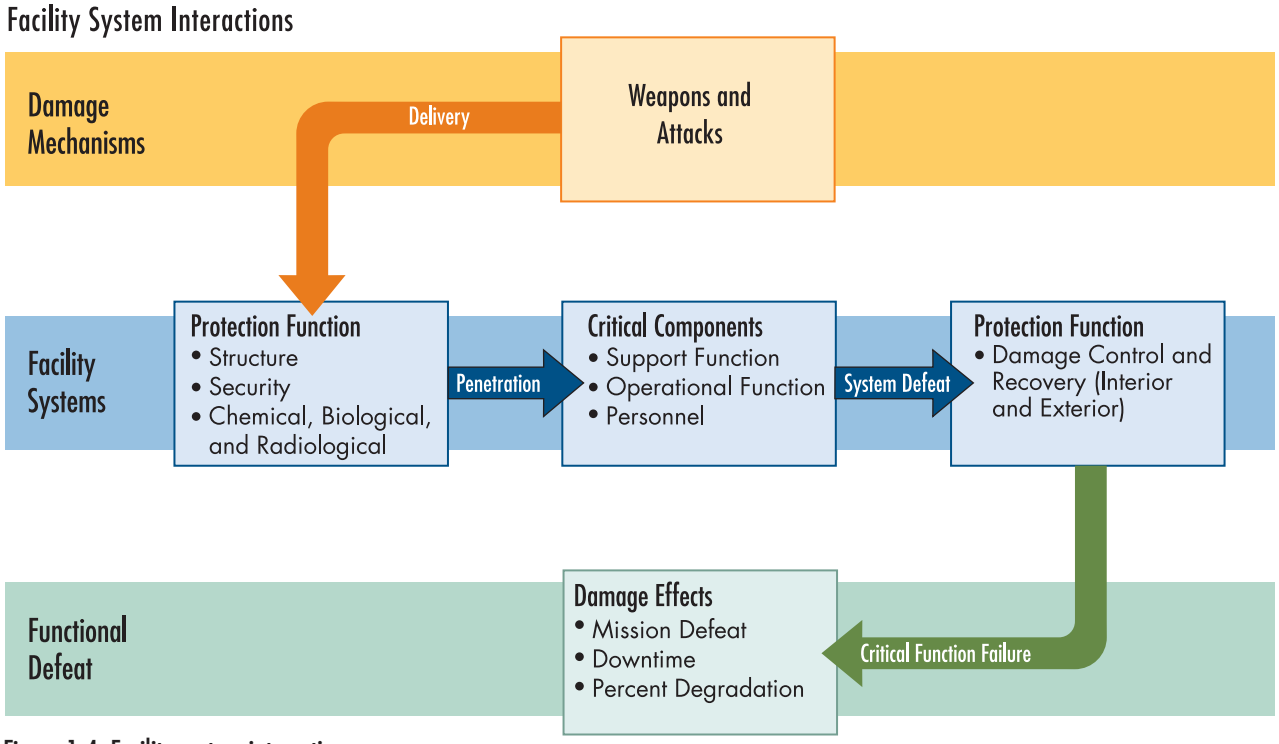


Figure 1-4: Facility system interactions

1.4.2 Determining the Threat Rating

Once potential and primary threats have been identified, based on the available information, the next task is to estimate the threat rating. The threat rating is a measure of the likelihood or probability that a specific type of attack will be mounted against the selected target. This is an integral part of the risk assessment.

Once potential and primary threats have been identified, based on the available information, the next task is to estimate the threat rating.

The recommended threat assessment methodology from FEMA 452 involves evaluating the probability of an attack by examining potential threats to a specific facility and its associated components or assets. Threat assessment includes an analysis of historical and quantitative data on threats, hazards, and actual incidents, as well as real-time situational awareness. The data collected most likely will indicate that the magnitude and frequency of incidents and attacks vary widely and are very difficult to estimate. This unpredictability in the threat assessment represents the greatest source of uncertainty in the risk assessment process, because a specific determination of a level of threat, (i.e., the likelihood of intentional attack on any particular facility, is difficult to quantify and may be largely subjective in nature). In certain sectors, especially those that operate in highly dynamic threat environments, the infrastructure owner/operator will likely have to take continuous actions to reduce vulnerability and increase resiliency.

The recommended threat assessment methodology involves evaluating the probability of an attack by examining potential threats to a specific facility and its associated components or assets.

Table 1-5 provides a scale to help with this determination. The scale is a combination of a 7-level nominal scale and a 10-point numerical scale (10 being the greatest threat). The key elements of the scale are the likelihood/credibility of a threat, potential weapons to be used during a terrorist attack, and information available to decision makers.

Table 1-5: Threat Rating Scale

Threat Rating		
Very High	10	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	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	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	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	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	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	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. Law enforcement and intelligence agencies determine the threat is non-existent or extremely unlikely.

1.5 Consequences Assessment

Consequences are the adverse effects of a terrorist attack (or a hazard event) and reflect the nature and severity of losses sustained as a result of such an incident. The assessment of the consequences is the process of estimating the probable damage or loss that a target may sustain as a result of a successful attack of a specific type or a hazard event. Consequences are usually expressed in terms of fatalities, injuries, property damage, economic losses, or other types of adverse

effects, such as psychological or social impacts. In the wake of some incidents, the immediate losses reverberate through the society, triggering indirect or secondary losses, which can be far-reaching and sometimes even more devastating than the direct losses. This is particularly true in cases where large areas, or sites/facilities with critical functions or significance, are affected. Catastrophic disasters and terrorist attacks, such as Hurricane Katrina and 9/11, affect society as a whole and require a much more comprehensive analysis of potential consequences. The consequences assessment in relation to risk to an individual facility or building (opposed to a region), as described in this manual, is usually limited to direct or immediate consequences, (i.e., the effects on human health and safety and effects of the direct physical impact of an attack on the targeted facility or asset).

Identifying a building's critical assets is accomplished using a two-step process: 1) define and understand the building's core functions and processes, and 2) identify site and building infrastructure and systems. Functions include primary services or outputs and critical activities; critical infrastructure includes critical support lifelines and critical/sensitive information.

The sources of uncertainty in estimating consequences mainly deal with the situation and conditions at the target at the time of an incident. The direction and strength of the wind, for example, will greatly affect the spread and, therefore, the impact of any accidental or intentional toxic agent release. The considerable knowledge base that exists today and the well-developed engineering and statistical tools for estimating consequences of various types of incidents make these types of uncertainty much easier to manage than they once were.

Experts have studied the effects of many types of weapons on people and structures, under different conditions, and this information is particularly useful in the risk assessment process. Some of the specific information on potential effects of threats on people and buildings is provided in the chapters of this manual that deal with individual types of threats.

Consequences primarily relate to the use, occupancy, and importance of the asset from the owner's or the assessor's perspective. Estimating the direct consequences of an event is accomplished by performing the following steps:

- Identify potential targets.
- Identify the effects on people and buildings or assets.
- Identify physical and environmental conditions at the target.
- Quantify the potential losses.

These steps are further discussed in the four sections that follow.

1.5.1 Identifying Potential Targets

Terrorists usually choose their targets to maximize the impact of their attack, or rather its consequences, and minimize the effort. They rarely attack "hard" targets, i.e., those that are fortified or defended, such as military installations. They prefer so-called "soft" targets, such as commercial shopping malls or football stadiums, where a successful attack might produce the greatest effect. This effect may involve anything, from massive casualties or physical destruction intended as symbolic acts to induce psychological shock, demonstrate a community's vulnerability, and instill fear.

Risk reduction, therefore, requires the identification and prioritization of potential consequences of a successful attack on a building. This identification is a vital first step in the process that will lead to determining the best protective measures prior to a terrorist attack. Potential consequences will depend on which specific building-related asset is the primary target. The asset can be tangible (e.g., occupants and visitors or building systems and equipment that support specific activities or operations) or intangible (e.g., a building's symbolic value or its importance for the owner's reputation).

Risk reduction requires the identification and prioritization of potential consequences of a successful attack on a building.

The nature of the target and, therefore, the magnitude of potential losses as a result of an attack or hazard event are determined by importance or criticality of the asset's function. This approach to identify targets by importance or criticality of the asset's function provides a better understanding of vulnerability and consequences and should consider the following factors:

- What are the building's primary services or outputs?
- What critical activities take place at the building?
- Who are the building's occupants and visitors?
- What inputs from external organizations are required for the building's operation?

After the core functions and processes are identified, an evaluation of building infrastructure should follow. To help identify and value-rank infrastructure, the following factors should be considered, keeping in mind that the most vital asset for every building is its people.

- The number of people that may be injured or killed during a terrorist attack that directly affects the infrastructure.
- The effects on occupants if a specific asset is lost or degraded. (Can primary services continue?)
- The impact on other organizational assets if the component is lost or cannot function.
- The possibility that critical or sensitive information may be stored or handled at the building.
- Whether backups exist for the building's physical assets.
- The availability of replacements for critical physical assets.
- The presence of any critical building personnel whose loss would degrade or seriously complicate the safety of building occupants during an emergency.
- Whether the building's physical assets may be replaced and at what cost.
- The locations of key equipment and the impact of their loss during an event.
- The locations of personnel work areas and systems.
- The locations of any personnel operating outside a building's controlled areas.
- The physical locations of critical support systems:
  - Communications and information technology (IT) (i.e., the flow of critical information)
  - Utilities (e.g., facility power, water, air conditioning, steam)
  - Infrastructure that provide access to external resources and provide movement of people (e.g., road, rail, air transportation)
- The location, availability, and readiness condition of emergency response assets and the state of training of building staff in their use.

1.5.2 Identifying the Effects of Threats and Hazards

Information on the effects of blast and CBR attacks on buildings and occupants may be readily available, because government agencies and many private organizations have long studied the effects of toxic and other noxious substances, as well as weapons, on people and buildings. For example, a known quantity of explosive material detonated at a certain known distance will produce air pressures sufficient to kill people and cause damage to structures. Similarly, information on the effects of exposure to various toxic substances or radiation is also available and may be used in estimating the potential consequences of an attack with a particular type of weapon.

In terms of explosives, concern about improvised explosive devices (IEDs) and vehicle-borne improvised explosive devices (VBIEDs) has increased since 9/11. An IED attack is conducted with a homemade bomb and/or destructive device to destroy, incapacitate, harass, or distract. Criminals, vandals, terrorists, suicide bombers, and insurgents use IEDs. Because they are improvised, IEDs can come in many forms, ranging from a small pipe bomb to a sophisticated device capable of causing massive damage and loss of life. IEDs and can be carried or delivered in a vehicle (VBIEDs); carried, placed, or thrown by a person; delivered in a package; or concealed on the roadside. Many commonly available materials, such as fertilizer, gunpowder, and hydrogen peroxide, can be used as explosive materials in IEDs (see Table 1-6). Explosives must contain a fuel and an oxidant, which provides the oxygen needed to sustain the reaction. (Blast/explosive effects are discussed in Chapter 3.)

Table 1-6: Examples of Explosives

	Common Uses	Common Form	Known IED Use
High Explosives			
Ammonium nitrate and fuel oil (ANFO)	Mining and blasting[1]	Solid	Oklahoma City bombing, 1995
Triacetone Triperoxide (TATP)	No common uses; mixed from other materials	Crystalline solid	London Bombings, 2005
Semtex, Composition 4 (C4)	Primarily military	Plastic solid	Irish Republican Army Manchester, bombing, 1996
Ethylene Glycol dinitrate (EGDN)	Component of low-freezing dynamite	Liquid	Millennium Bomber, intended for Los Angeles airport, 1999
Urea nitrate	Fertilizer	Crystalline solid	World Trade Center, 1993
Low Explosive			
Smokeless powder	Ammunition	Solid	Olympic Park bombing, 1996

1 Ammonium nitrate (without fuel oil) is used as fertilizer.

1.5.3 Identifying Conditions at the Target

The gravity of consequences of an attack on a particular target is influenced by the type of attack (threat), or hazard event, and the physical and environmental conditions at the target at the time of an attack. For example, a toxic release near a building located downwind will have different consequences on a windy morning than during a still night. Worst case physical and environmental conditions should be considered when analyzing potential scenarios in risk assessment. Consider the following factors when identifying the conditions at the target that may affect the consequences of an event:

- **Timing:** Most buildings are occupied and operate on a fixed schedule, usually during the regular working hours, which means that attacks at different times of the day will have different consequences. Also, seasonal conditions determine the type of heating and cooling systems that may affect the consequences of releases of toxic substances.
- **Environment:** Wind speed and direction, stability, air humidity, and other environmental conditions affect the duration and severity of exposure to toxic substances in the air and may aggravate the consequences of a CBR attack (see Chapter 4).
- **Local conditions:** In an explosive attack, the load a specific building element must withstand varies with both the distance from and magnitude of the explosive device (see Chapter 3). If an aggressor were to strike at a particularly vulnerable time, such as when a loading dock is unattended, the effects of the explosive device could be increased as a result of the lack of standoff.
- **Aging:** If the asset has lost some of its structural capacity through age, corrosion, and lack of maintenance, the effects of an explosive device on the structural and non-structural building systems may be greater.

1.5.4 Quantifying the Potential Losses

Consequences are divided into the following four categories of impacts:

- **Human Impact (public health and safety):** Effects on human life and physical wellbeing (e.g., fatalities, injuries).
- **Economic Impact:** Direct and indirect effects on the economy with respect to the building and its functions (e.g., cost to rebuild asset, cost to respond to and recover from the attack, downstream costs resulting from the disruption of operations or service, long-term costs due to environmental damage).

- **Public Confidence (psychological):** Effect on public morale and trust in the government and critical infrastructure. This encompasses those changes in perceptions emerging after a significant incident that affect the public's sense of safety and wellbeing.
- **Government Functionality (governance):** Effect on the local government's ability to maintain order, deliver minimum essential public services, ensure public health and safety, and carry out security-related missions.

Consequences may be initially limited to the building and site, but may affect offsite operations for other building owners. For example, the effects of a fire at a telecommunications building could disrupt services for an entire area if redundancy is not provided to the facility and/or if the facility is not resilient to this type of threat. Alternatively, an offsite event affecting a critical lifeline, such as natural gas pipeline, may result in negative consequences for the building as well. The effectiveness of a resilient infrastructure or enterprise depends on its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.

The consequences rating should include the degree of debilitating impact that would be caused by the incapacity or destruction of the building's assets (occupants, critical functions, and infrastructure). The scale below (Table 1-7) uses the same type of numerical values used for rating threats and vulnerabilities to represent various levels of severity of potential losses or consequences of an attack or hazard event. The scope of potential fatalities and injuries and the degree of debilitating impact that would be caused by damage to the building's assets is described for each level.

To consider the consequences of an attack in the assessment of risk, grave consequences such as fatalities and injuries must be rated on the same scale with potential building damages and other property losses. Comparing and evaluating different types of consequences requires value judgments that are always highly subjective. Different stakeholders and decision makers will have different perspectives and value standards. While the losses associated with human assets will almost always be the primary criterion for assigning the consequences rating, as in the examples below (see Tables 1-8a and 1-8b), other types of potential losses may raise or lower that rating.

Table 1-7: Consequences Rating Scale

Consequences Rating		
Very High	10	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 for a long period of time. The consequences would have an exceptionally grave effect on public health and safety, the economy, and governance. The building owner has neither taken steps to maintain continuity of operations nor taken action to ensure that key functions will not be significantly affected by an event.
High	8–9	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 a long period of time. The consequences would have a grave effect on public health and safety, the economy, and governance. The building owner has taken little or no action to maintain continuity of operations or to ensure that key functions will not be significantly affected by an event.
Medium High	7	Loss or damage of the building's assets would have serious consequences, such as serious injuries or impairment of core processes and functions for a long period of time. The consequences would have a serious effect on public health and safety, the economy, and governance. The building owner has taken minor steps to maintain continuity of operations and/or has taken minor action to ensure that key functions will not be significantly affected by an event.
Medium	5–6	Loss or damage of the building's assets would have moderate to serious consequences, such as injuries or impairment of core functions and processes for a considerable period of time. The consequences would have a moderate to serious effect on public health and safety, the economy, and governance. The building owner has taken some steps to maintain continuity of operations and/or has taken some action to ensure that key functions will not be significantly affected by an event.
Medium Low	4	Loss or damage of the building's assets would have moderate consequences, such as minor injuries or minor impairment of core functions and processes for a considerable period of time. The consequences would have a moderate effect on public health and safety, the economy, and governance. The building owner has taken moderate steps to maintain continuity of operations and/or has taken moderate action to ensure that key functions will not be significantly affected by an event.
Low	2–3	Loss or damage of the building's assets would have minor consequences, such as slight effects on core functions and processes for a short period of time, if at all. The consequences would have a minor effect on public health and safety, the economy, and governance. The building owner has taken reasonable steps to maintain continuity of operations and/or has taken reasonable action to ensure that key functions will not be significantly affected by an event.
Very Low	1	Loss or damage of the building's assets would have negligible consequences and the effect on public health and safety, the economy and governance would be negligible. The building owner has taken sufficient steps to maintain continuity of operations and/or has taken adequate action to ensure that key functions will not be significantly affected by an event.

Examples of potential assets for a typical building with assigned value are presented in Tables 1-8a and 1-8b. Please note that ratings are presented for example only; each building should be rated to reflect its unique situation.

Table 1-8a: Nominal Example of Consequences Rating for an Urban Multistory Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	5	5	5	5	5
Engineering	8	8	8	8	8
Warehousing	3	3	3	3	3
Data Center	8	8	8	8	8
Food Service	2	2	2	2	2
Security	7	7	7	7	7
Housekeeping	2	2	2	2	2
Day Care	10	10	10	10	10

Table 1-8b: Nominal Example of Consequences Rating for an Urban Multistory Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	4	4	4	4	4
Architectural	5	5	5	5	5
Structural Systems	8	8	8	8	8
Envelope Systems	7	7	7	7	7
Utility Systems	7	7	7	7	7
Mechanical Systems	7	7	7	7	7
Plumbing and Gas Systems	5	5	5	5	5
Electrical Systems	7	7	7	7	7
Fire Alarm Systems	9	9	9	9	9
IT/Communications Systems	8	8	8	8	8

1.6 Vulnerability Assessment

The third step in the assessment process is preparation of a vulnerability assessment of building assets. Vulnerability refers to the probability that damage, casualties, and business disruption may occur as a result of a successful attack of a specific type in specific circumstances. Vulnerabilities are the characteristics of an asset, system, location, process, or operation that render it susceptible to destruction, incapacitation, or exploitation by mechanical failures, natural hazards, terrorist attacks, or other malicious acts. Vulnerability is measured by assessing features that would enhance or diminish building performance during a terrorist attack or a hazard event. For this manual, vulnerability is defined as any weakness that can be exploited by an aggressor to make an asset susceptible to hazard damage. A vulnerability assessment is an in-depth analysis of the building functions, systems, and site characteristics to identify building weaknesses and lack of redundancy that can be exploited during a terrorist attack. Such assessments are crucial for determining not only the magnitude of consequences, but also the protective measures or corrective actions that can be designed or implemented to reduce them.

Many vulnerability assessment methodologies are in use today for a variety of threats and hazards. Some are available commercially, while others have been designed or adapted to meet the specific security needs for a particular facility or associated systems and processes. The vulnerability assessment used here is based on that of FEMA 452.

1.6.1 Organize Resources to Prepare for the Assessment

Vulnerability assessments can be conducted at many different levels of detail and can focus on an individual facility, several interdependent facilities or associated elements, a certain category of facilities, or an entire sector. Organizing resources in preparation for the vulnerability assessment involves: 1) selecting the assessment team, and 2) determining the level of assessment.

Selecting the assessment team may be the most critical task in the threat assessment process. The most effective teams are composed of senior individuals with a breadth and depth of experience and understanding of other disciplines and system interdependencies.

The level of assessment for a given asset depends on a number of factors, such as building type, location, type of construction, number of occupants, and available economic resources. The assessment team and building owner determine the asset value and level of assessment.

1.6.2 Evaluate the Site and Building

The purpose of the vulnerability assessment process is to identify all the physical and organizational vulnerabilities of an asset that increase the exposure of that asset to risks from a specific threat or hazard. Vulnerability assessments are designed to provide an in-depth analysis of the characteristics of the facility or associated elements to identify weaknesses and lack of redundancy, as well as to determine protective or corrective actions that can be designed or implemented to reduce the vulnerabilities.

The purpose of the vulnerability assessment process is to identify all the physical and organizational vulnerabilities of an asset to risks.

An evaluation of site and building vulnerabilities involves meeting with building owners and operation personnel; reviewing background information, such as construction documents and prior threats to the facility; conducting site and building tours; and reviewing emergency and operational procedures.

1.6.3 Prepare the Vulnerability Portfolio

The vulnerability portfolio is a set of items required to carry out the vulnerability assessment that should include the building vulnerability assessment checklist, pre-assessment screening matrix, risk assessment matrices, and risk assessment database. FEMA 452 lists and explains thoroughly all the items required for a vulnerability assessment.

The most crucial step in preparing the vulnerability portfolio is to answer the vulnerability questions in the Building Vulnerability Assessment Checklist (Appendix F). This checklist provides a comprehensive view of the building and critical lifelines that affect vulnerability and, ultimately, the overall risk and the resiliency of each asset. Fire is the main threat that affects a building and is handled well by modern building codes and standards; therefore, fire is not the focus of this assessment checklist. The questions on building fire allow the assessor(s) to evaluate whether that threat is being adequately addressed through regular inspections and maintenance.

The most crucial step in preparing the vulnerability portfolio is to answer the vulnerability questions in the Building Vulnerability Assessment Checklist.

1.6.4 Determining Vulnerability Rating

This task involves determining a vulnerability rating that reflects the weaknesses of functions, systems, and sites in regard to a particular threat/hazard. Weakness includes the lack of redundancies for building systems that must remain operational after an event.

Table 1-9 provides a scale for selecting a vulnerability rating. Similar to the rating for threats and consequences, the vulnerability scale is a combination of a 7-level nominal scale and a 10-point numerical scale (10 being the greatest level of vulnerability). The key elements of this scale are the weaknesses of the site and building to the selected threats and the ease or difficulty aggressors may face when attempting to generate damage. Also, the loss of operations in case of an event and the lack of redundancies are considered. Tables 1-10a and 1-10b provide a nominal example applying vulnerability ratings to an urban multistory building.

Table 1-9: Vulnerability Rating Scale

Vulnerability Rating		
Very High	10	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/resilience and the entire building would only be functional again a very long period of time after an event.
High	8–9	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/resilience and most parts of the building would only be functional again a long period of time after an event.
Medium High	7	An important weakness has been identified that makes the asset very susceptible to an aggressor or hazard. The building has inadequate redundancies/physical protection/resilience and most critical functions would only be operational again a long period of time after an event.
Medium	5–6	A weakness has been identified that makes the asset fairly susceptible to an aggressor or hazard. The building has insufficient redundancies/physical protection/resilience and most parts of the building would only be functional again a considerable period of time after an event.
Medium Low	4	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/resilience and most critical functions would only be operational again a considerable period of time after an event.
Low	2–3	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/resilience and the building would be operational within a short period of time after an event.
Very Low	1	No weaknesses exist. The building has incorporated excellent redundancies/physical protection/resilience and the building would be operational immediately after an event.

Table 1-10a: Nominal Example of Vulnerability Rating for a Specific Multistory Building (Building Function)

Function	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Administration	7	7	9	9	9
Engineering	4	4	5	6	6
Warehousing	4	8	9	9	9
Data Center	5	4	3	4	4
Food Service	1	4	5	9	9
Security	5	5	10	9	9
Housekeeping	1	3	3	3	3
Day Care	3	9	9	9	9

Table 1-10b: Nominal Example of Vulnerability Rating for a Specific Multistory Building (Building Infrastructure)

Infrastructure	Cyber Attack	Vehicle Bomb	Suicide Bomber	Chemical (Sarin)	Biological (Ricin)
Site	1	7	6	4	4
Architectural	1	9	7	2	2
Structural Systems	1	10	7	2	1
Envelope Systems	1	9	7	2	1
Utility Systems	2	6	2	2	1
Mechanical Systems	1	8	5	9	9
Plumbing and Gas Systems	1	6	3	6	2
Electrical Systems	7	8	6	2	1
Fire Alarm Systems	1	6	8	2	1
IT/Communications Systems	8	6	8	2	1

1.7 Risk Assessment

The risk assessment integrates the likelihood, or probability, of the attack (threat) occurring with the probability that a successful attack will produce consequences of a certain magnitude, given the vulnerabilities of the target. It should provide a relative risk profile for each type of threat or hazard. These risk profiles facilitate prioritization and a more efficient allocation of resources to implement protective measures.

This manual uses the FEMA 452 methodology, in which the approach is to assemble the results of the threat assessment, consequences assessment, and vulnerability assessment, and to determine a numeric value of risk for each asset and threat/hazard pair in accordance with the following formula:

Risk = Threat Rating x Consequences Rating x Vulnerability Rating

The risk assessment process involves the following tasks:

- Preparation of risk assessment matrices.
- Determination of risk ratings.
- Prioritization of observations in the building vulnerability assessment checklists.

The risk assessment integrates the likelihood, or probability, of the attack (threat) occurring with the probability that a successful attack will produce consequences of a certain magnitude, given the vulnerabilities of the target.

These tasks are described in detail in FEMA 452.

To improve accuracy of the above risk equation, the assessors are advised to include interrelations between threats, consequences, and vulnerabilities during the assessment process. In FEMA 455, as well as BIPS 04 (IRVS), such interrelations are accounted for within the tool algorithm itself.

1.7.1 Preparing Risk Assessment Matrices

FEMA 452 provides a series of matrices for use in estimating potential losses. The inputs for these matrices are based on the analysis performed in the threat, consequences, and vulnerability assessments. These risk assessment matrices can provide both a quantitative score and color code (see Table 1-11) to objectively and visually determine the functions and systems that have been determined to be at risk. In the risk assessment matrices, the threats are listed across the top, and the functions and infrastructure are listed down the side to create threat-pairs. A hypothetical example of a site pre-assessment matrix is shown in Table 1-12.

Table 1-11: Total Risk Scale Color Code

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

Table 1-12: Site Functional Pre-Assessment Screening Matrix

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

1.7.2 Determination of Risk Ratings

In the risk estimation matrices, three components of risk are considered for each function or system against each threat previously identified. Total risk is quantified by multiplying the values assigned to each of the three components.

$$\text{Risk} = \text{Threat Rating} \times \text{Consequences Rating} \times \text{Vulnerability Rating}$$

The total risk for each function or system against each threat is assigned a color code in accordance with Table 1-11. Nominal examples of both the functional and infrastructure matrices are shown in Tables 1-12. The results of the risk assessment should be used to help prioritize which mitigation measures should be adopted, given limited resources, to achieve a desired level of protection (see Section 3.1.4).

1.7.3 Prioritizing Observations in the Building Vulnerability Assessment Checklist

The building vulnerability assessment checklist addresses building core infrastructure. This checklist is a key tool in the preparation of the vulnerability assessment. Vulnerabilities are prioritized, based on the greatest vulnerabilities that can be exploited by an aggressor and largest risks in terms of loss, to determine the most effective mitigation measures. In this final task, assessors rank their observations and proposed remedial actions.

1.8 Risk Management

Traditionally, the building regulatory system has addressed natural disaster mitigation (hurricane, tornado, flood, earthquake, windstorm, and snow storm) through prescriptive building codes supported by well-established and accepted reference standards, regulations, inspections, and assessment techniques. Some manmade risks (e.g., hazmat storage) and specific societal goals (energy conservation and life safety) have been similarly addressed. However, the building regulatory system has not yet fully addressed the risks from manmade hazards or terrorist threats.

Risk management seeks to reduce various risks by manipulating the three risk components. The management of threats is usually the province of authorities at a higher level, such as governments, especially within military, intelligence, and law enforcement agencies. The management of risk at the level of individual buildings must necessarily focus on minimizing consequences by reducing potential vulnerabilities of assets or by

increasing preparedness and response capabilities. This manual focuses on the reduction of physical and organizational vulnerabilities of buildings and systems.

The protective measures reduce the vulnerabilities in different ways and with different degrees of effectiveness. The most ideal protective measures are ones that reduce the vulnerabilities in the most cost-effective manner. For example, glazing protection can be achieved with blast curtains or a fragment retention film (FRF), and the most appropriate measure is selected in accordance with the desired level of protection. Decisionmakers determine the desired level of protection based on circumstances associated with the building's physical and operational characteristics, as well as social and economic mandates and constraints of ownership.

Protective measures reduce the vulnerabilities in different ways and with different degrees of effectiveness. The most ideal protective measures are ones that reduce the vulnerabilities in the most cost-effective manner.

Members of the assessment team including engineers, architects, landscape architects, and other technical experts should be involved in this process to ensure that the results of the risk assessment are met with sound protective measures that will increase the capability of the building to resist potential terrorist attacks. If given the opportunity, the design professional should provide the building owner with a menu of options of possible protective measures to reduce risk. For example, a building owner may only want protective measures against a single threat or hazard (i.e., vehicle bomb) and not others. In other cases, the owner may choose to implement the protective measures that are the least costly, or are eligible for Federal grant monies, or protect only human life and not infrastructure, or are implementable in a timely fashion, among other factors. In this case, the building owner is making risk management decisions and accepting a certain amount of residual risk.

The design professional can prepare a risk matrix to help the building owner select the most appropriate protective measures.

The design professional can prepare a risk matrix to help the building owner select the most appropriate protective measures. The risk matrix ties the protective measures—selected to reduce the vulnerabilities identified using the Building Vulnerability Assessment Checklist—to the risk scores in the matrix. There is no set method for selecting protective measures; however, the following list provides some options for accomplishing this goal:

- Protective measures that reduce the risk with the highest scores should have priority. Therefore, the top 10 projects to implement are the 10 that will reduce risk the most.

- Protective measures that reduce the most overall risk for one or more design basis threats should be selected. For example, if the matrix includes 15 high-risk scores relating to vehicular bombs, but only one high-risk score for armed attacks, focus on protective measures that will reduce vulnerabilities for a vehicular bomb attack.
- Protective measures that fit the building owner's overall planning and capital improvement process, as well as budget and time constraints should have priority.

Note that the implementation of a certain type of protective measure may reduce the building's vulnerability and the aggregate risk only for a specific set of threats and targets, but may not reduce the overall risk. This is because each set of protective measures may increase the vulnerability of other assets, by shifting the focus of the potential aggressor to a less protected asset.

Design professionals need to understand the threats and hazards that the building design should address. Just as seismic design requires an understanding of geology, soil structure, and the maximum credible earthquake accelerations possible at a given location, the building designer needs to comprehend the maximum credible bomb size, vehicle size, and gun or other weapon size (the threats upon which to base design) to provide an appropriate level of protection. The level of threat and the desired level of protection are equally important to the design. For most cases across the United States, the threats and risks for a specific building will be low. For buildings exposed to higher risk, higher standards and performance may be required. The DOD, DOS, VA, GSA, and DHS (ISC) all have established processes to identify threats upon which to base design for their facilities.

The typical building design and construction process is sequential, progressing from identifying building use and design goals through actual construction. This process is illustrated in Figure 1-5.

Figure 1-5: Typical building design and construction process

In every design and renovation project, the owner/decision maker ultimately has three choices when addressing the risk posed by terrorism:

1. Do nothing and accept the risk.

2. Perform a risk assessment and manage the risk by installing reasonable protective measures.
3. Harden the building against all threats to reduce the risk to a minimum acceptable risk.

Figure 1-6 represents three choices. Since 9/11, terrorism has become a dominant concern in building design. Life, safety, and security protective measures should be design goals from the beginning.

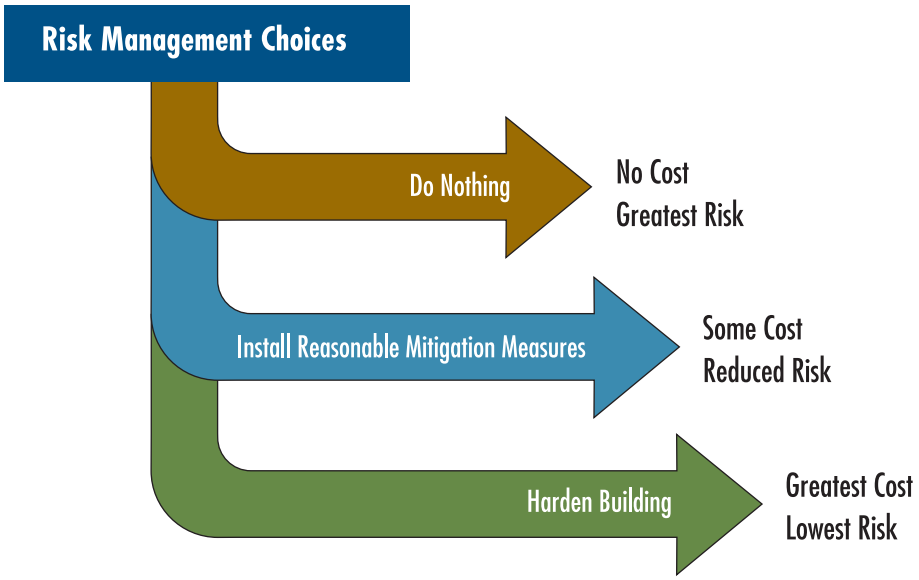


Figure 1-6:
Risk management choices

Building owners should use the results of the risk assessment to integrate protective measures into the existing planning and design process. Most building owners or organizations have a five-year plan (or similar) that shows how capital improvement monies will be spent to construct new facilities or renovate existing ones. The design professional should work with the implementers of the five-year plan to identify opportunities for integrating protective measures into projects scheduled as part of the five-year plan. By doing so, the project costs for the protective measures can be greatly reduced. For example, if a building has a deficient roof deck attachment (roofs are subjected to downward and upward overpressure from explosive loads that could cause collapse) and the roof covering is scheduled to be replaced in three years, the deck attachment could be addressed in three years as part of the reroofing project.

1.8.1 Benefit-Cost Analysis

Benefit-cost analysis (BCA), as the name implies, involves comparing the costs of a given protection solution to its perceived benefits. The BCA is usually performed in relation to a particular situation at a particular time. In relation to the scope of this manual, a BCA is typically done as

a continuation of the risk assessment process and during the design of protective measures (or mitigation options). The BCA is necessary to ensure that the designed protective measure offers the greatest mitigation of risk for any given expenditure.

In many cases, the cost is the initial cost of installation, although life-cycle cost (LCC) or life-cycle analysis may be necessary in some situations. The BCA is used in risk management decision as explained below:

- When the benefits of all protection measures are similar, then the best solution is the least costly solution.
- When the costs of all protection measures are similar, then the best solution is the one that provides the most benefits (which may include benefits beyond protection). For example, if solution A is a more aesthetical solution than B, and both solutions have the same cost and offer the same protection measures, then solution A is the better solution.
- When costs and benefits vary, then a more in depth benefit-cost comparison should be performed. In some situations, a comprehensive life-cycle analysis is needed.

1.8.2 Life-Cycle Costs

The LCC represents the combined sum of all relevant costs associated with owning and operating a constructed facility over a specified period of time, usually the estimated life span of a building. The LCC method is used to compare alternative designs or solutions that provide different levels of protection on the basis of their LCCs to determine which is the least costly over a specified period. The more extensive and, therefore, costlier protective measures will reduce the potential losses resulting from successful attacks over the life span of an asset. Conversely, unprotected buildings with low-cost protective measures will have a greater chance of incurring the potentially significant losses over the life span of a building. In other words, LCC helps the decision maker to determine whether the higher initial cost of a constructed facility or system is economically justified by lower future costs, such as losses resulting from hazard events or terrorist attacks, when compared to an alternative with a lower initial cost but higher future costs.

1.8.3 Estimating Costs

Both the benefit-cost and life-cycle analyses calculate the costs of a particular protective design solution and weigh them against the intended benefits, usually expressed as losses avoided. However, the application

of these methods for evaluating the cost effectiveness of protective measures is challenging because of the following three factors.

The probability of occurrence or frequency of an attack is unknown. Although estimating how often natural hazard events will occur (i.e., a structure located in the 100-year floodplain is considered to have a 1-percent chance of being flooded in any given year) is possible, quantifying the likelihood of a terrorist attack is very difficult. Quantitative methods to estimate these probabilities are being developed, but have not yet been refined to the point where they can be used to determine incident probability for a specific building. The assessment team may use a qualitative approach based on threat and vulnerability considerations to estimate the relative likelihood of an attack or accident rather than the precise frequency. Such an approach is necessarily subjective, but can be combined with quantitative estimates of cost effectiveness (the cost of an action compared to the value of the lives and property it saves in a worst-case scenario) to help illustrate the overall risk reduction achieved by a particular mitigation action.

The deterrence rate may not be known. The deterrence or preventive value of a measure cannot be calculated if the number of incidents it averts is not known. Deterrence in the case of terrorism may also have a secondary impact in that, after a potential target is hardened, a terrorist may turn to a less protected facility, changing the likelihood of an attack for both targets.

The lifespan of the action may be difficult to quantify. The lifespans of various protective measures are frequently different. Some are designed for single use, while others remain effective over the life span of a building. Because future benefits, (i.e., losses avoided), are generally calculated by estimating the number of times the protective measure will perform successfully over the course of its useful life, comparing them is difficult. For example, blast-resistant window film may have been fully effective in preventing injuries from flying glass, but it may still need replacement after one incident, while some other measures, such as a building setback, cannot ever be rendered ineffective.

To improve cost estimation, a general spectrum of protective measures ranging from the least protective and least costly to the most protective and most costly, are provided in Figures 1-7 and 1-8. These protective measures are arranged by layers of defense: the second layer pertains mostly to the site and the third layer generally refers to the building itself. The figures provide examples of protective measures for each layer and indicate a potential correlation between the level of protection and the cost of the measure.

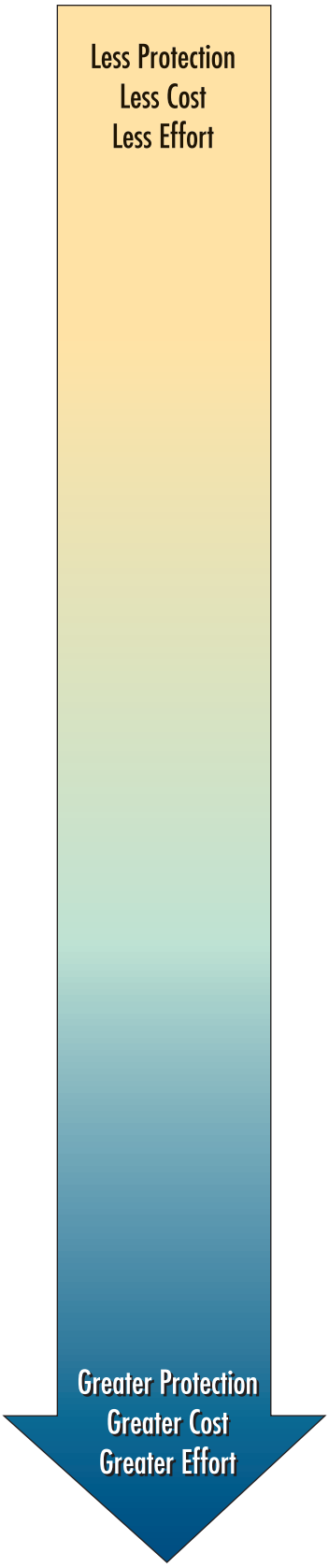
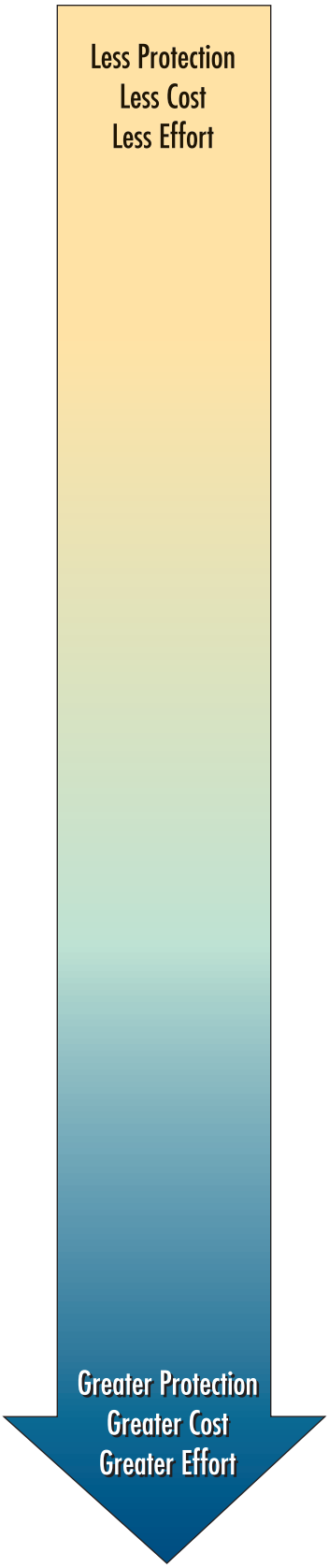


Figure 1-7: Protective measures for the second layer of defense

- 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.
- Use a geographic information system (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 standoff.
- Locate and consolidate high-risk land uses in the interior of the site.
- Select and design barriers based on threat levels.
- Maintain as much standoff 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).

Figure 1-7 : Protective measures for the second layer of defense (cont.)

- Establish law enforcement or security force presence.
- Install quick connects for portable utility backup systems.
- Install security lighting.
- Install closed-circuit television (CCTV) 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 standoff for vehicle bombs.
- Position buildings to permit occupants and security personnel to monitor the site.
- Site the building at an appropriate distance from 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 standoff, push the line farther outward by restricting or eliminating parking along the curb, eliminating loading zones, or closing streets.
- 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.



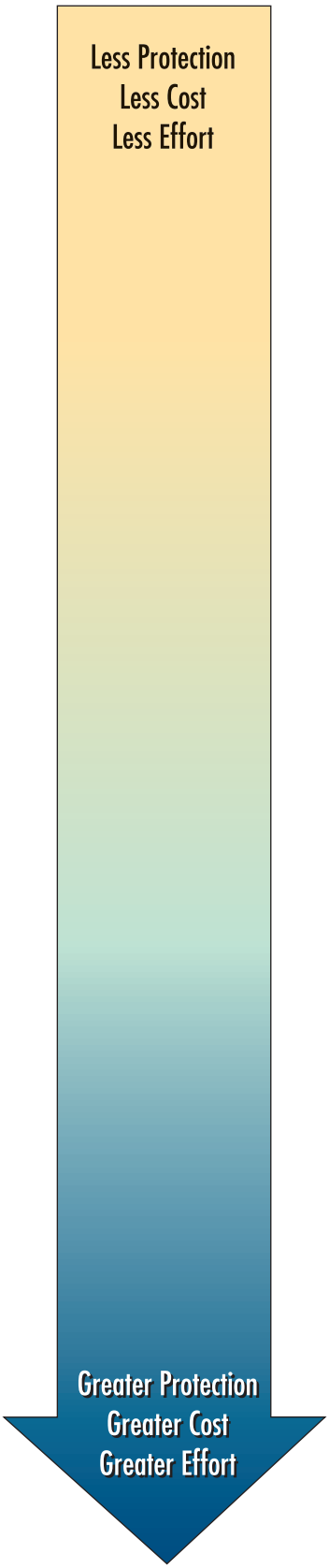
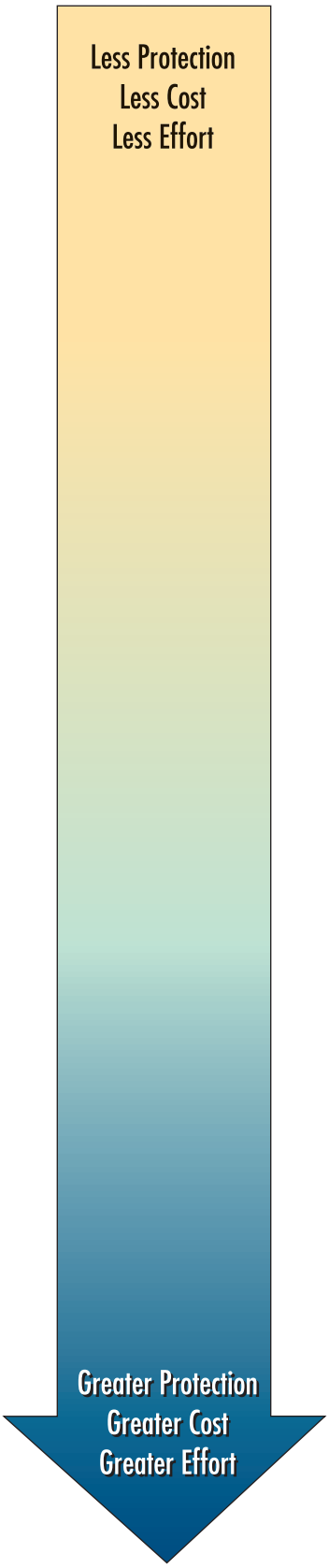


Figure 1-8: Protective measures for the third layer of defense

- Install active vehicle crash barriers. Ensure that exterior doors into inhabited areas open outward. Ensure emergency exit doors only facilitate exiting.
- Secure roof access hatches from the interior. Prevent public access to building roofs.
- Restrict access to building operation systems.
- Conduct periodic training of heating, ventilation, and air-conditioning (HVAC) operations and maintenance staff.
- Evaluate HVAC control options.
- Install empty conduits for future security control equipment during initial construction or major renovation.
- Do not mount plumbing, electrical fixtures, or utility lines on the inside of exterior walls.
- Establish emergency plans, policies, and procedures.
- Establish written plans for evacuation and sheltering in place.
- Illuminate building access points.
- Restrict access to building information.
- Secure HVAC intakes and mechanical rooms.
- Limit the number of doors used for normal entry/egress.
- Lock all utility access openings.
- Provide emergency power for emergency lighting in restrooms, egress routes, and any meeting room without windows.
- Install an internal public address system.
- Stagger interior doors and offset interior and exterior doors.
- Eliminate hiding places.
- Install a second and separate telephone service.
- Install radio telemetry distributed antennas throughout the facility.
- Use a badge identification system for building access.
- Install a CCTV surveillance system.
- Install an electronic security alarm system.
- Install rapid response and isolation features into HVAC systems.

Figure 1-8: Protective measures for the third layer of defense (cont.)

- Use interior barriers to differentiate levels of security.
- Locate utility systems away from likely areas of potential attack.
- Install call buttons at key public contact areas.
- Install emergency and normal electric equipment at different locations.
- Avoid exposed structural elements.
- Reinforce foyer walks.
- Use architectural features to deny contact with exposed primary vertical load members.
- Isolate lobbies, mailrooms, loading docks, and storage areas.
- Locate stairwells remotely. Do not discharge stairs into lobbies, parking, or loading areas.
- Elevate HVAC fresh-air intakes.
- Create "shelter-in-place" rooms or areas.
- Separate HVAC zones. Eliminate leaks and increase building air tightness.
- Install blast-resistant doors or steel doors with steel frames.
- Physically separate unsecured areas from the main building.
- Install HVAC exhausting and purging systems.
- Connect interior non-load-bearing walls to structure with non-rigid connections.
- Use structural design techniques to resist progressive collapse.
- Treat exterior shear walls as primary structures.
- Orient glazing perpendicular to the primary façade facing uncontrolled vehicle approaches.
- Use reinforced concrete wall systems in lieu of masonry or curtain walls.
- Ensure active fire system is protected from single-point failure in case of blast event.
- Install a backup control center.
- Avoid eaves and overhangs or harden to withstand blast effects.
- Establish ground floor elevation four feet above grade.
- Avoid re-entrant corners as the building exterior.



1.9 Protective Measures

United States building codes and standards set minimum requirements, primarily for health and life safety, for earthquake, winds, floods, and fire hazards. Building owners and developers, as a rule, are not required to address the risks from natural hazards beyond compliance with the building codes and other standards or to adopt blast and CBR-protective measures when designing a new building or rehabilitating existing ones. However, resurgent terrorist attacks and ever more frequent natural and manmade hazard incidents, make it prudent to design the Nation's building inventories to be resilient to all hazards and threats, i.e., to be able to anticipate, absorb, adapt to, and rapidly recover from any disruptive event.

In 2007, the U.S. Congress passed the Energy Independence and Security Act (EISA) of 2007 (Public Law 110-140), which defines high performance as "the integration and optimization on a life cycle basis of all major high performance attributes, including energy conservation, environment, safety, security, durability, accessibility, cost-benefit, productivity, sustainability, functionality and operational considerations." The positive public attention received by this important law provides public and private sectors with opportunities to introduce high-performance standards that promote the integration, compilation, and harmonization of building considerations to ensure acceptable and appropriate levels of performance-based requirements for buildings to withstand all hazards, including the impact of explosive blast and CBR attacks. The primary reason for having a comprehensive approach to all-hazards integrated design is to prevent partial or total collapse of a building and improve its capability to operate in the aftermath of any hazardous event. DHS is currently working toward these goals and created the High Performance and Integrated Design Resilience Program. The program's overall goal is to better prepare buildings and infrastructure to recover from manmade and natural disaster events by analyzing and compiling a range of high-performance requirements, including energy conservation, safety, security, environmental footprint, sustainability, durability, continuity of operations, and rapid recovery to provide for an improved comprehensive solution to our Nation's building stock (see Figure 1-9).

High Performance= "the integration and optimization on a life cycle basis of all major high performance attributes, including energy conservation, environment, safety, security, durability, accessibility, cost-benefit, productivity, sustainability, functionality and operational considerations."

The program is supported by three primary paradigms:

1. It is possible to provide a built environment that has the highest level of performance and resiliency in a comprehensive and cost-effective manner.
2. All facets of the process from design to operation must be integrated.
3. Through high performance and integrated design, infrastructure can achieve resilience from a disruptive event.

Figure 1-9:
High-performance buildings

1.10 Integrated Design System Interactions

To assist the reader in evaluating the interactions between protective design methods, Table 1-14 summarizes the interactions between protective measures discussed in this manual and common protective measures for earthquakes, floods, high winds, and fire, covered in other publications of the Risk Management Series. In addition, the table also includes provisions for blast and CBR resistance.

The vertical columns in Table 1-14 include the six primary threats, or hazards, and each horizontal row shows how the site characteristic, building characteristic, or protective measure interacts with the respective threat/hazard indicating positive reinforcement (synergistic benefit),

negative conflict (detrimental effects), or neutral interaction. The comments in Reasons for Evaluations column are not absolute restrictions or recommendations, but rather are intended to provoke thought and further design integration. Reinforcement between hazard protection measures may be gained, and undesirable conditions and conflict can be resolved by coordinated design starting at the inception of the design process. The table provides succinct information to help the reader develop a list of reinforcements and conflicts for the particular combination of threats and hazards that may be faced. This list may be used to structure initial discussion on the impact of multihazard design on building performance and cost that, in turn, can guide an integrated design strategy for protection.

High-Performance and Integrated Design Resilience Program

This project, BIPS 04, on the cutting edge of building design, is expected to have a great impact on how buildings are designed and constructed in the United States. The identification and definition of high-performance requirements will enable designers, developers, and owners to produce buildings that significantly exceed the minimum requirements of current codes and standards. High-performance buildings will not only be much safer during catastrophic events but will use much less energy, with the potential to improve the health, safety, comfort, and productivity of their occupants. One major objective is to develop an Owner Performance Requirements tool to allow building owners to select a series of performance-level parameters to accommodate regional risks (natural and manmade) as well as to provide enhanced building performance for a range of attributes for security, natural hazards resistance, energy efficiency, environmental sustainability, durability, cost, and life-cycle of a particular asset. The tool is intended to become an ASTM International (ASTM) standard.

The result of this project will provide DHS S&T IDD with the capacity to review, understand, and promote the adoption of advanced high-performance building envelope systems and components that will provide for enhanced infrastructure protection (against natural and manmade hazards) beyond current codes and standards. The project will facilitate the adoption of blast protection as it builds upon a model charged with the integration, compilation, and harmonization of a series of high-performing attributes included in the EISA 2007. For DHS, it is essential to have high performance metrics in place to comply with this public law.

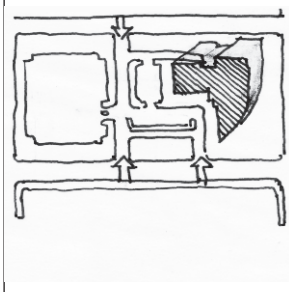
The DHS High-Performance and Integrated Design Resilience Program is based on the assumption that buildings can achieve resilience through a combination of good initial design and construction for new facilities, effective retrofit for existing facilities, and appropriate operational programs to ensure that mitigation plans are in place and the building's systems are operated effectively. The model adopted by DHS pursues the integration of all the attributes included in EISA 2007, which are many times in conflict or regulated by different agencies or organizations. For this program, the concept of resilience conveys the ability to maintain critical operations and functions in the face of crisis, to respond and manage a crisis or disruption as it unfolds, and to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruptive event.

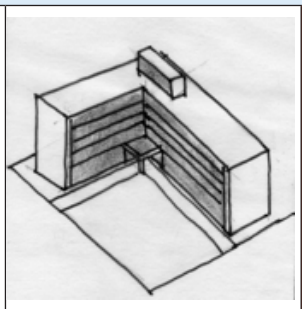
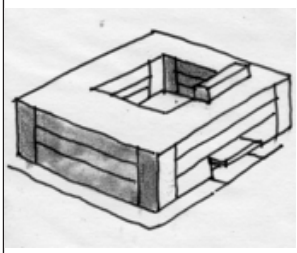
The symbols used in Table 1-14 are provided below in Table 1-13:

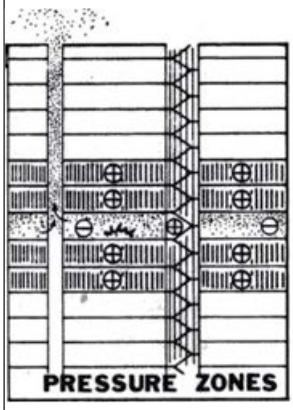
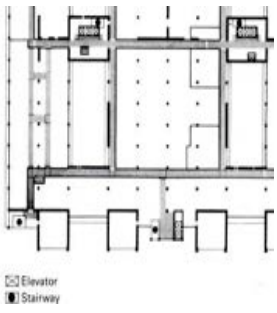
Table 1-13: Multihazard Integrated Design System Interactions

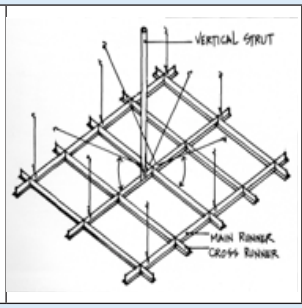
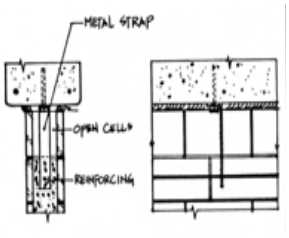
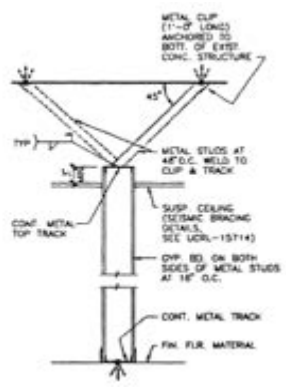
+	green	Desirable condition or method for designated component/system
-	red	Undesirable condition for designated component/system
0	yellow	Little or no significance for designated component/system
+/-	white	Significance may vary, see Reasons for Evaluations column

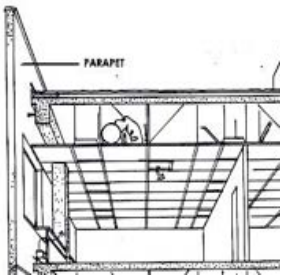
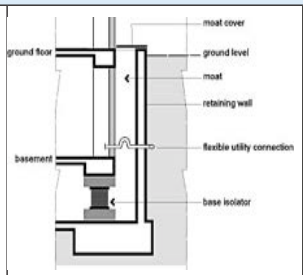
Table 1-14: Multihazard Design System Interactions

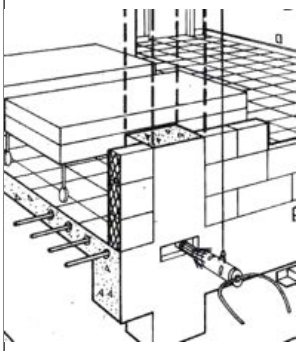
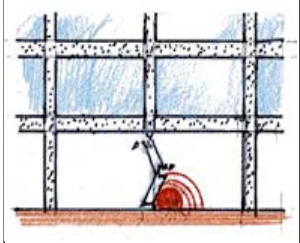
Building System Protection Methods: Reinforcements and Conflicts										
			The Hazards							
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	Earthquake	Flood	Wind	Fire	CBR	Blast	Reasons For Evaluations
1	SITE									
1A	Site–specific all–hazard analysis, including possibility of tsunami or hurricane–induced flooding		+	+	+	+	+	+	Beneficial for all hazards.
1B	Two or more means of access to the site		+	+	+	+	+	+	Beneficial for all hazards.
1C	Site modification to provide elevated building on engineered fill		–	+	0	0	0	+	Highly beneficial for flood. Needs very careful site engineering for earthquake. Not significant for wind, fire, or CBR hazards. Soft soil can absorb blast energy, thus reducing effect of bomb blast pressures on building envelopes.

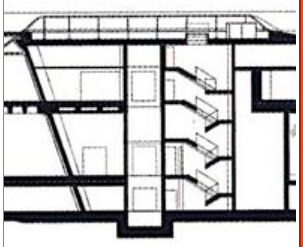
Building System Protection Methods: Reinforcements and Conflicts										
			The Hazards							
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	Earthquake	Flood	Wind	Fire	CBR	Blast	Reasons For Evaluations
1D	Building placed in a depression or low terrain area		0	–	0	–	–	–	Not significant for earthquake or wind. Possibly vulnerable to flooding. Reflection of blast pressures may increase building damage. Depression can trap vapor and inhibit natural decontamination. Might inhibit emergency access.
2	ARCHITECTURAL									
2A	Configuration									
2A–1	Re–entrant corner plan forms		–	0	–	0	–	–	May cause stress concentrations and torsion in earthquakes and develop localized high–wind pressures. May cause unwanted blast reflections on structure. Air intakes should not be placed near reentrant corner.
2A–2	Enclosed courtyard plan forms		–	0	0	0	+/–	+/–	May cause stress concentrations and torsion in earthquakes. Undesirable for CBR hazard and blast, but effects may vary depending on whether attack is internal or external and the relative size of the courtyard.
2A–3	Large atrium with expanse of structural glazing for roofs and walls		–	0	–	–	–	–	Needs special consideration for earthquake, wind, fire, CBR hazard, and blast. Only an issue for floods if floor level is below grade.

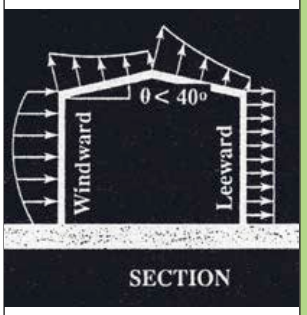
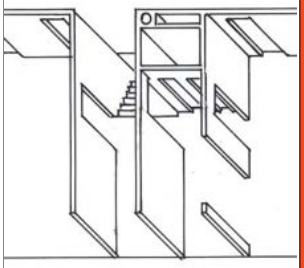
Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
2A–4	Very irregular three–dimensional building forms		–	–	–	–	–	–	May create indirect load paths, stress concentrations, and torsion in earthquakes, and possible confusing evacuation paths for firefighting. Complicates flood resistance by means other than site fill. May develop localized high wind pressures. CBR agents may have unpredictable behavior, and indirect load paths are vulnerable to blast.
2A–5	Large roof overhangs		–	0	–	0	–	–	Possibly vulnerable to vertical earthquake forces and high–wind forces. CBR–agent behavior may be unpredictable. Vulnerable to uplift blast pressure.
2A–6	Stairwells designed for pressurization		+	0	0	+	+	+	Not significant for flood or wind. Can be beneficial after an earthquake, internal blast, or CBR release, especially if pressurization keeps smoke, dust, or agent out of the evacuation route. Beneficial for fire and CBR hazard.
2B	Planning and Function									
2B–1	Exit routes, including stairs, are adequately sized, well marked, and clear of untraced nonstructural elements or contents that might fall and block exit ways		+	+	+	+	+	+	Not significant for flood or wind. Can be beneficial after an earthquake, internal blast, or CBR release, especially if pressurization keeps smoke, dust, or agent out of the evacuation route. Beneficial for fire and CBR hazard.

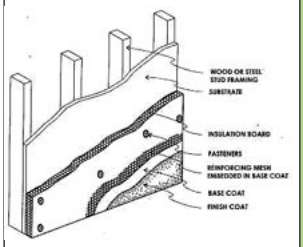
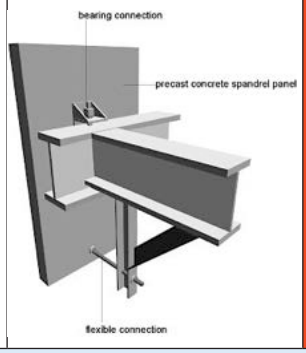
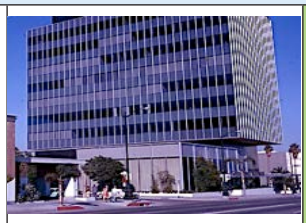
Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
2C	Ceilings								
2C–1	Stairwells designed for pressurization		+	0	0	+	0	–	Reduced damage from earthquakes. If part of fire protection system, increases possibility of retaining integrity. Needs to be designed for required blast pressures.
2D	Partitions								
2D–1	Unreinforced masonry (URM) or hollow clay tile, used as partitions or infill for structural framing		–	+	–	+	–	–	URM has high vulnerability to earthquake, wind, and blast. Desirable against fire and flood if not subject to damage from other hazards. Vulnerable to CBR hazard because it is permeable to CBR agents and subject to infiltration. Acceptable for flood and fire.
2D–2	Use of non–rigid (ductile) connections for attachment of interior non–load–bearing walls to structures in severe seismic zones, including extra–high and extra–heavy gypsum board walls		+	0	0	–	–	+	Gaps provided for this may threaten fire resistance integrity, and special detailing is necessary. Not significant for flood and wind. Can spread CBR agents quicker. Can be beneficial for blast assuming adequate ductility is provided.
2D–3	Gypsum wall board partitions		+	–	0	+	–	+	Gypsum partitions that terminate at ceiling in earthquake zones should be braced to structure. Susceptible to flood damage. Good performance in fire if properly specified resistance is used; not significant for wind. Gaps can be detrimental during CBR events. Beneficial in blast if properly braced.

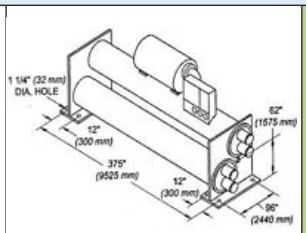
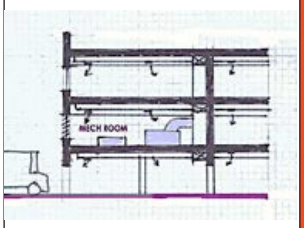
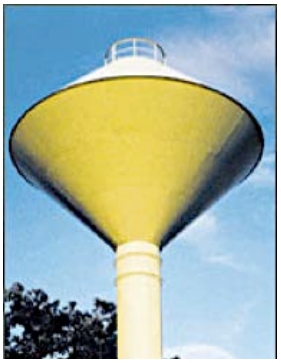
Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
2E	Other Elements								
2E–1	Tile roofs		–	0	–	–	0	–	Undesirable in quakes and blast unless properly attached. On light structures, disproportionate heavy roof load may cause collapse. Good fire protection, but may also collapse fire-weakened structure. Undesirable in high-wind regions.
2E-2	Parapets		+	0	+	+	0	–	Properly engineered, acceptable for quakes, but unbraced URM is very dangerous in quake and wind. May assist in reducing fire spread. Not significant in flood and CBR. If strong, will increase reflected blast pressure. If weak may fragment and act as missiles.
3	STRUCTURAL SYSTEM								
3A	Use of base isolation and/or energy dissipating dampers		+	–	0	0	0	–	Beneficial for earthquake. Base isolation in basement vulnerable to damage in flood. Not significant for wind, fire, and CBR hazard. Can be detrimental during blast.
3B	Wood frame structure, used for small hospitals and ancillary and service buildings		+	–	–	+	–	–	Light weight good for earthquake if good connections and shear walls. Not significant in fire if correctly fireproofed. Materials vulnerable to damage in floods and winds (unless properly designed for wind loads). Light weight detrimental during blast (less ductility than light steel frame). Subject to CBR permeability.

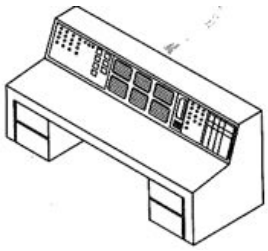
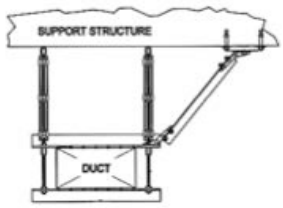
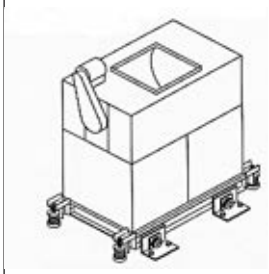
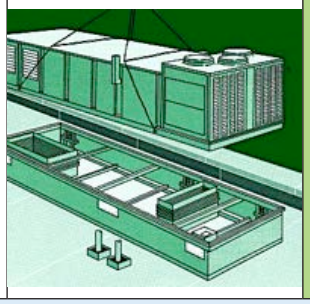
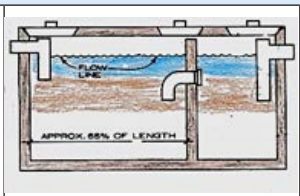
Building System Protection Methods: Reinforcements and Conflicts											
			The Hazards								
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	Earthquake	Flood	Wind	Fire	CBR	Blast	Reasons For Evaluations
3C	Heavy structure with concrete floors: reinforced concrete moment frame or frame and some reinforced concrete shear walls or reinforced masonry walls		+	+	+	+	+		Weight increases earthquake forces but not a design problem, requires special non-ductile detailing for large building frames. Generally beneficial for all other hazards. Heavy mass may slow or prevent spread of CBR agents and performs well against blast.
3D	Reinforced concrete or reinforced CMU structural walls with concrete floors and roof deck		+	+	+	+	+		Very beneficial for wind and good performance for earthquake, flood, and fire when correctly designed and constructed. Heavy mass may slow or prevent spread of CBR agents and good performance against blast.
3E	Steel structural frame		+	+/–	+	+	0		Lighter than concrete, needs properly detailed moment frame, steel braces, or shear walls in earthquake and wind. Good performance in flood with proper detailing and good for elevated structure. Not significant for CBR because steel frame does not affect infiltration through envelope. Good performance for blast if well detailed.
3F	Pre-stressed or post-tensioned structure		0	+	0	0	0	–	Not significant for earthquake, wind, fire, and CBR hazard. Limitation of cracking may be beneficial in flood. Care needed in blast to avoid spreading loss of tension capacity.
3G	Structure designed to resist progressive collapse		+	0	+	+	0		Beneficial for earthquake, wind, and fire by increasing redundancy such that any local structural failure is less likely to spread globally. Essential for blast. Not significant for flood and CBR.

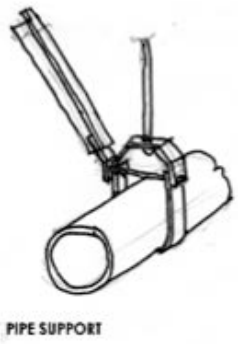
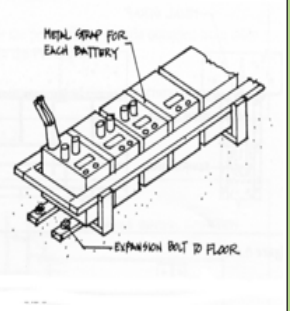
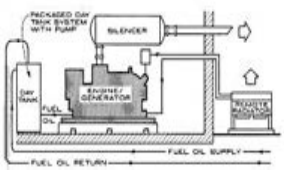
Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
3H	Unreinforced masonry load-bearing walls		–	–	–	–	0	–	Very poor performance in earthquakes and high winds. Not permitted in California since 1933. Undesirable for all hazards, except CBR hazard, because of possibility of collapse.
3I	Well-designed steel or concrete frame structure with open first floor		0	+	0	0	0	–	Very beneficial for flood. Not significant for earthquake, wind,, and fire. Not significant for CBR hazard. Detrimental for blast if bomb explosive placed directly under building or next to a structural support.
3J	Soft/weak first story architectural/ structural configuration		–	–	–	–	0	–	Very poor earthquake performance and a primary cause of collapse. Generally undesirable for flood, wind, fire, and blast. Elevated first floor is very beneficial for flood only if well designed and constructed.
3K	Non-standard or variable floor heights		–	0	0	0	0	–	May introduce vertical stiffness irregularities leading to local stress concentrations in earthquakes. Many blast practices are based on standard floor heights.
3L	Discontinuities in vertical structure system		–	0	–	–	0	–	May introduce vertical stiffness irregularities leading to local stress concentrations in earthquakes. Many blast practices are based on standard floor heights.

Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
3M	Large seismic separation joints in structure		+	0	0	–	–	+	Improves earthquake response. Possible path for toxic gases or CBR agents to migrate to other floors and spread. Cause of deaths in Las Vegas MGM Grand fire.. Structural separations beneficial in blast event, limiting progressive collapse.
3N	Design structural system and building envelope for uplift from wind forces, and extreme cantilevers for seismic		+	0	+	0	0	+	Necessary for wind and unusual vertical earthquake forces. Not significant for flood, CBR hazard, or fire. Beneficial for blast.
3O	Reinforced concrete or reinforced CMU around exit ways and exit stairs		–	0	+	+	0	+	May create torsional response and/or stress concentrations in earthquakes in frame structures, unless isolated. Properly designed, will preserve evacuation routes in event of fire, and will assist in limiting high-wind and blast effects.
4	BUILDING ENVELOPE								
4A	Exterior Wall Cladding								
4A-1	Brick veneer on exterior walls		–	–	–	0	0	–	In earthquakes, winds, and floods, material may detach and cause costly damage and injury. Careful detailing and quality control necessary for good performance. Can detach and act as missiles during blast event.

Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
4A-2	Lightweight insulated cladding		+	0	0	0	–	–	Light weight reduces earthquake response. Not significant for floods, winds, or fire. Leaks can spread CBR agents. Light weight vulnerable in blast event unless carefully designed to hold cladding to frame.
4A-3	Exterior insulation and finishing system (EIFS)-insulated cladding		+	0	–	0	0	–	Light weight reduces structural response. Needs very careful engineering and application to prevent leakage and detachment in winds. Not significant in floods or fire. Light weight vulnerable in blast event unless carefully designed to hold cladding to frame.
4A-4	Precast concrete panels		–	0	+	0	+	+	In high earthquake hazard zones, requires special detailing, including ductile connections to structure. Good performance for wind if well attached. If well designed and detailed to be leak proof, can slow CBR agents. Beneficial in blast events if strong and flexible connections designed for blast are able to hold panels to frame.
4B	Glazing									
4B-1	Metal/glass curtain wall		+	0	0	–	–	–	Light weight reduces earthquake forces. If properly detailed and installed, performance is good for earthquake and wind. Fire can spread upward behind curtain wall if not properly fireproofed. Can be designed for increased resistance to blast.
4B-2	Impact-resistant glazing, and applied anti-shatter or anti-glare film	Glass (basis weakest to strongest) With film Annealed (with shards) Heat Strengthened (with glass above, acts more like laminated) Impact Resistant Tempered (pellets) Laminated (large pieces) Polycarbonate (bullet resistant)	+	0	+	–	–	+	Good performance against wind-borne debris. May be beneficial for earthquake. Not significant for flood. Can cause problems during fire suppression operations, limiting smoke ventilation and access. Can be undesirable for CBR hazard. Beneficial for blast protection.

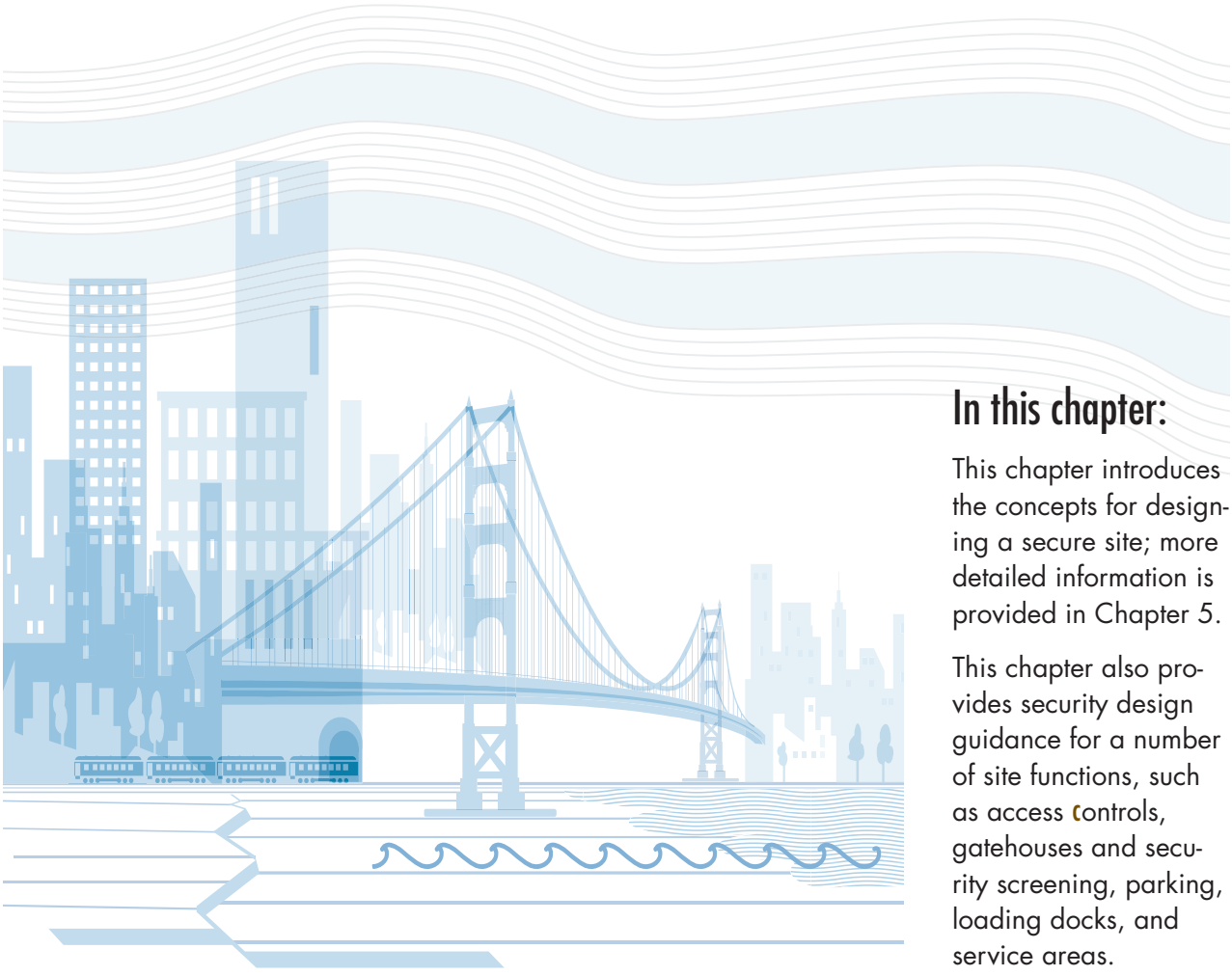
Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
5	UTILITIES								
5A	System components well supported and braced where necessary	 Chiller support	+	+	+	0	0	+	Essential for earthquake and wind (especially for exterior-mounted components). Beneficial for flood and wind. Not significant for fire or CBR. Essential for blast, and need to be well designed.
5B	System components located above flood level		–	+	0	0	0	–	Very beneficial for flood. If on upper floors, may be subject to greater forces in earthquake. Not significant for wind or fire or CBR. If heavy, can have undesirable effects for progressive collapse.
5C	Underground fuel tanks		–	–	–	0	0	0	Need careful design for earthquake. Susceptible to flooding. Not significant for other hazards.
5D	Above ground fuel tanks		–	0	–	0	0	–	Need careful support design for earthquake. Not significant for flood, fire, or CBR hazard. Can be vulnerable to wind or blast.
5E	Elevated water tanks		–	0	–	0	0	–	Vulnerable to earthquake, wind, and blast. Acceptable for flood if well designed, but possible soil erosion around tank supports may result in damage to whole tank. Not significant for fire and CBR hazard.

Building System Protection Methods: Reinforcements and Conflicts										
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	The Hazards						Reasons For Evaluations
			Earthquake	Flood	Wind	Fire	CBR	Blast	
5F	Location of single or multiple building facilities control centers		–	–	–	–	–	–	Control center locations can be vulnerable to all natural hazards. If not hardened can be vulnerable to fire, CBR hazard, and blast.
6	MECHANICAL								
6A	System components well supported and braced where necessary		+	+	+	+	0	+	Essential for earthquake and wind (especially exterior-mounted components). Beneficial for flood and CBR hazard. Blast protection might require different design than earthquake protection.
6B	Vibration-isolated equipment designed for seismic and wind forces: snubbers prevent equipment from falling off isolators		+	0	+	0	0	+	Very beneficial for earthquake. Not significant for flood, CBR, or fire. If designed to resist uplift, acceptable for wind. Beneficial for blast, but frequency requirements might differ from those for earthquake.
6C	Very securely attached roof-top equipment		+	0	+	0	0	+	Very beneficial for wind and earthquake (with seismic-designed isolators where necessary). Not significant for floods and fire. Beneficial for heavier than air CBR agents, but not for lighter CBR agents. Special filtering. Beneficial for blast.
7	PLUMBING AND GAS PIPING								
7A	Underground sewer system and septic tanks		–	–	0	0	0	0	Need careful design, particularly at joints, for seismic and flood.

Building System Protection Methods: Reinforcements and Conflicts										
			The Hazards							
System ID	Site and Building Characteristics	Examples of Site and Building Characteristics	Earthquake	Flood	Wind	Fire	CBR	Blast	Reasons For Evaluations
7B	System components well supported and braced where necessary		+	0	+	+	0	+	Essential for earthquake and wind (especially for exterior-mounted systems). Beneficial for fire and blast, but different design might be necessary for blast.
8	ELECTRICAL AND COMMUNICATIONS EQUIPMENT									
8A	Well supported and braced where necessary		+	0	+	+	0	+	Essential for earthquake and wind (especially for exterior-mounted systems). Beneficial for fire and blast, but different design might be necessary for blast.
8B	Additional emergency power to supply essential services during and/or after natural or manmade event , separated from main/utility power supply, and equipment securely braced		+	+	+	+	+	+	Essential for earthquake, wind, fire, and flood. Provides redundancy of capacity for CBR hazard and redundancy locations for blast.
8C	Emergency power equipment located in basement (below grade)		0	–	0	–	0	0	May be susceptible to flooding. During fire, may be affected by fire-fighting water. Not significant for earthquake, wind, CBR hazard, and blast.

2

Site Design for Security



In this chapter:

This chapter introduces the concepts for designing a secure site; more detailed information is provided in Chapter 5.

This chapter also provides security design guidance for a number of site functions, such as access controls, gatehouses and security screening, parking, loading docks, and service areas.

2.1 Introduction

Site design plays a major role in reducing the risks of a terrorist attack on a building. Perimeter barriers and protective design measures between the site perimeter and the building can greatly reduce the possibility and effectiveness of an attack, as well as the need for other costly measures to improve the resilience of the building itself. The location and orientation of a building may additionally reduce the risks of a CBR attack and, depending on the size of the site, also facilitate provision of staging areas for CBR evacuation. This chapter introduces the concepts for designing a secure site; more detailed information is provided in Chapter 5.

Site design plays a major role in reducing the risks of a terrorist attack on a building.

This chapter also provides security design guidance for a number of site functions, such as access controls, gatehouses and security screening, parking, loading docks, and service areas. Examples of well-designed barrier systems, together with examples of approaches to avoid, are provided.

Site design involves integrating general planning tasks, such as building placement, parking, and site infrastructure planning, with security needs. Finally, site security design measures, whether for a newly developed or an existing site, are conceived and implemented within a highly developed system of land use planning that aims to order and regulate the use of land in an efficient and ethical way. The following section discusses some of the implications of this planning context.

2.1.1 Site Security Design and the Planning Context

Planning regulation is typically the province of local governments within a context determined by Federal or State authorities. These regulations cover such issues as land and subdivision development, permitting, and zoning, as well as deed restrictions and easements. Economic policies determine the scale and scope of development based on land market values, insurance costs, tax incentives, and impact fees, together with the prevailing status of capital investment and predictions as to future costs and benefits.

Some controls may either increase or decrease security. For example, a deed restriction limiting the use of an adjacent parcel to open space or recreation may present a security advantage in terms of setback and standoff (the distance from the building face to nearest point that an explosive device can approach from any side, assuming that all security measures are in place), but such spaces may also make hostile

surveillance and attack preparations difficult to detect. Creating an overlay zone (sub-zoning to address area-specific considerations) based on security requirements could firmly establish antiterrorism as a key design consideration, but it could also cause the "branding" of an area as high risk, thus jeopardizing the success of any development nearby. Careful economic and social investigation is necessary to ensure a positive security benefit.

Site security design must consider many different aspects, from the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of activities on adjacent properties, to their implications for the protection of the people, property, and operations on the site under consideration. Conflicts sometimes arise between security-oriented site design and conventional site design, particularly with regard to the openness of the site and buildings to the public, often an objective of conventional design.

Site security design must consider many different aspects, from the characteristics of the surrounding area, including construction type, occupancies, and the nature and intensity of activities on adjacent properties, to their implications for the protection of the people, property, and operations on the site under consideration.

Another aspect of the design construction context is represented by the building codes and other regulations such as Americans with Disabilities Act (ADA) Accessibility Guidelines, Uniform Federal Accessibility Standards, and National Fire Protection Codes, to name a few.

2.1.2 Multihazard Issues: The Fire Protection Dilemma

The perennial threat of fire, which may be accidental, deliberate, or a consequence of an attack with explosives, is usually at odds with design measures for site security. Security measures for protecting a site always include physical barriers that keep vehicles and frequently the passers-by as far away from a building as possible (see Section 2.3.3 for approach speed control strategies). Fire protection, on the other hand, requires quick and unobstructed access of firefighting vehicles, personnel, and equipment to the site and the threatened building, which may be in direct conflict with the goals of site security design.

The resolution of this conflict requires early consultation among the stakeholders—building owners, designers, and local authorities. The building owner and designer may be required to accept a lesser level of protection against attack on the grounds if the probability of an attack is lower than the probability of a fire. The fire marshal may also have to accept an approach to the building that takes a few minutes longer and

is perhaps more difficult (in terms of access roads that provide fire apparatus and other emergency response vehicles access to the facility or building). Innovation in design may also provide a solution. For example, a dedicated "express" lane to the building with operable barriers that can be opened remotely by the fire department may be justified and feasible, as may some variation of a limited, monitored use of such an express lane.

2.2 Characteristics of Sites That Affect Building Vulnerability

Nearly all aspects of risk—from intentional (terrorist) attack or accidental exposure of a building to explosive blast or CBR agents—are influenced by the characteristics of the site on which the building is situated. This is one of the reasons why most new construction of commercial and institutional facilities is preceded by a very careful and complex process of site selection that is conducted by specialized multidisciplinary teams. The criteria used to evaluate the site vary from engineering aspects, such as soil characteristics or hydrology, to issues of safety and security and from marketing aspects, such as demography, regional traffic patterns, and financial and legal issues, to planning, environmental, or historic preservation requirements. Before selecting a site, owners and developers of commercial facilities must also assess the site for its visibility in the community, i.e., the level of public awareness of the site location, its accessibility, proximity to facilities that may be important or necessary for site use, and many others aspects.

Nearly all aspects of risk are influenced by the characteristics of the site on which the building is situated.

This manual recognizes the importance of the site selection process from both the business and security perspectives. However, because the focus of this manual is the protection of buildings, it must necessarily concentrate on the implications of a given site for building security. The following are some of the building site characteristics that may affect vulnerability of the building to blast and CBR attacks:

- Building footprint relative to total land available
- Existing or proposed location relative to the site perimeter and adjacent land uses, and the available distance between the defended perimeter and improved areas offsite
- Overall size and number of buildings to be placed on the site
- Massing and placement of buildings that may impact views, sight lines, and screening
- Access via foot, road, rail, water, and air

- Presence of natural physical barriers, such as water features, dense vegetation, and terrain, that could provide access control or shielding, or suitability of the site for the incorporation of such features
- Topographic and climatic characteristics that could affect the performance of chemical or other windborne agents and other weapons
- Ability to limit the number of access and egress points, such as visitor entries, staff entries, and loading docks
- Internal vehicular circulation (e.g., driveways, surface parking areas) and pedestrian circulation (e.g., sidewalks, tunnels, bridges)
- Location of uses and operations within the building, such as high-risk areas that require access control and higher levels of security, and their interface with site requirements

This section reviews the most important of these characteristics from the perspective of security protection.

2.2.1 Location and Size

In most cases, the size of the site is commensurate with its location within a metropolitan area. In the context of this manual, building sites can be described generally as the following based on location and size:

- **Urban Sites:** These lots have relatively small areas not covered with a building. Depending on the size and location of these open areas, urban sites are distinguished as: (i) building lots with zero setbacks, where the site perimeter is at the building face; (ii) building lots with private yards between the perimeter and the building face; and (iii) building lots with plazas, large open spaces that can be either private or public.
- **Open Sites:** Large, open sites with a vehicular approach from the perimeter can contain either a single building or a number of buildings. The latter are known as campus type, and include colleges, medical centers, or industrial parks.

Urban sites are usually smaller, and because of the higher cost of land, especially in central business districts (CBDs), the lot coverage is very high, at times even approaching full coverage, i.e., the building footprint is the same size as the lot. Smaller building sites usually have high floor area ratios as well, i.e., the size of the building area is frequently several times larger than the site area (size of the lot).

Building sites can be described generally as the following:

Urban Sites: These lots have relatively small areas not covered with a building.

Open Sites: Large, open sites with a vehicular approach from the perimeter can contain either a single building or a number of buildings.

Sites in suburban and newly developed areas on the periphery of cities are much larger, and usually have low lot-coverage ratios, which means that the building can be placed further away from streets and other public areas.

Vulnerability to attack with explosives is most closely related to the standoff, the distance between the building and the closest place to which an explosive device can be delivered. The study of the blast effects, which may come from an IED, VBIED, or other device, and their relationship to standoff distance reveals that the energy released from a high-energy detonation decreases rapidly, as the blast front expands spherically from the detonation. Therefore, the larger the standoff distance from the detonation to the structure the lower the intensity of the blast loading. The optimum standoff distance is a function of the type and size of the explosive device as well as the constraints imposed by site conditions.

Figure 2-1 plots peak reflected pressure versus range and reflected impulse versus range, and highlights the benefit of increased standoff distance for three different magnitudes of explosive threat. For both of these charts, the shock wave is considered to be perpendicular to the reflecting surface and, therefore, produces the maximum coefficient of reflection (Cr), as indicated in Figure 2-1. For example, increasing the standoff distance from 20 feet (6 meters) to 40 feet (12 meters) reduces the peak reflected pressure by a factor of four for a charge weight of 10 pounds (4.5 kilograms) and a factor of nearly seven for a charge weight of 1,000 pounds (454 kilograms). However, the corresponding reduction in reflected impulse associated with the same increase in standoff distance is a factor of two for a charge weight of 10 pounds (4.5 kilograms) and a factor of nearly two and a half for a charge weight of 1,000 pounds (454 kilograms).

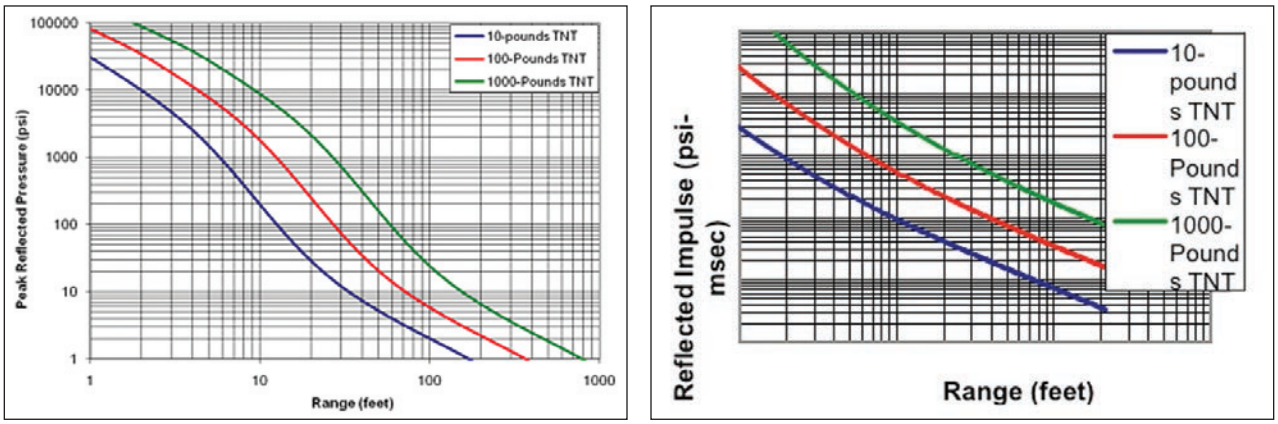


Figure 2-1: Peak reflected pressure and reflected impulse as a function of standoff distance (See Chapter 3, Section 3.1.1, on the nature of explosive blasts).

As suggested by Figure 2-1, the critical location of the weapon is a function of the site, building layout, and the level of security measures in place. For blasts from VBIEDs, the critical locations are considered to be 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 outside the building, or at the entry control point where inspection takes place. For internal weapons, location is dictated by the areas of the building that are publicly accessible (e.g., lobbies, loading docks, corridors, auditoriums, cafeterias, commercial retail).

Similarly to blast threats, vulnerability to CBR attacks is affected by location and size of the building site. Unrestricted access to the site and to the building provides plenty of opportunities for surreptitious release of toxic agents. More information is provided in Section 2.4.7 and in Chapter 4.

Similarly to blast threats, vulnerability to CBR attacks is affected by location and size of the building site.

2.2.2 Topography

The topography of the site is a very important security issue because, depending on the placement of the building on the site, it determines the opportunities for internal surveillance of site perimeters and screening of internal areas from external observation. Building form, placement, and landscaping may help to define the line of sight, which facilitates effective control of potential hostile surveillance. Denying aggressors a line of sight, either from onsite or offsite, increases the ability to protect sensitive functions and operations from aggressors.

Depending on the circumstances, the topography may be either beneficial or detrimental with respect to surveillance. Elevated sites may enhance surveillance of the surrounding area from inside the facility, but may also allow observation of onsite areas by adversaries. Buildings placed immediately adjacent to higher surrounding terrain may be overly exposed to intrusive surveillance.

High-risk facilities frequently require additional protection immediately adjacent to the structure in the form of a clear zone, free of all topographic obstructions or even landscaping that might provide hiding places (Figure 2-2). The clear zone facilitates monitoring of the immediate vicinity and visual detection of attackers or intruders.

The topography of the site is a very important security issue because it determines the opportunities for internal surveillance of site perimeters and screening of internal areas from external observation.

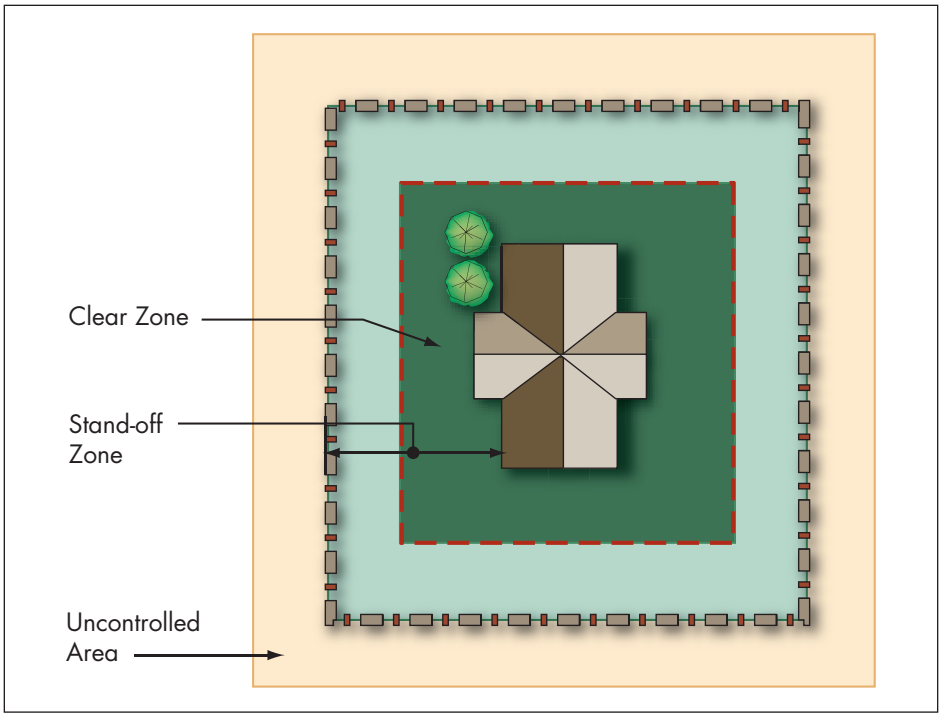


Figure 2-2: Clear zone with unobstructed views

SOURCE: U.S. AIR FORCE INSTALLATION ENTRY CONTROL FACILITIES DESIGN GUIDE

2.2.3 Building Orientation

Orientation, or the physical positioning of a building on the site, can be a major determinant of security. For the purpose of this manual, the term "orientation" refers to three distinct characteristics: a building's spatial relationship to the site, its orientation relative to the sun and prevailing winds, and its vertical or horizontal aspect relative to the ground. A structure's orientation relative to its surroundings defines its relationship to that area. In both aesthetic and functional terms, a building can "open up" to the area or "turn its back"; it can be inviting to those outside, or it can "hunker down" defensively.

By optimizing the positioning of the building relative to the sun, climate control and lighting requirements can be met while reducing power consumption. Similarly, the use of light shelves, skylights, clerestories, and atria can help meet illumination requirements while reducing energy usage. Light pipes supplying natural light from the roof or a hardened wall can reduce the size and number of windows, reducing energy usage and reducing the cost of hardening the building envelope.

Some of these energy conservation techniques have important security implications and must be examined carefully for their vulnerability to blast loading and exposure to CBR agents. For example, although natural ventilation is an effective and time-tested technique for efficiently

cooling buildings, the use of unfiltered outside air is a major vulnerability with respect to attacks with aerosolized CBR agents and accidental releases of hazardous materials, while the operable windows may be more vulnerable to blast damage than the fixed ones.

A structure's orientation in relation to the prevailing winds onsite is an especially significant characteristic of a site considering the possibility of a CBR attack or hazardous material release. Wind may be beneficial in mitigating the effects of windborne hazards in that it reduces the concentration of agents in the air as distance from the source increases, spreading the plume laterally and upwind. The annual wind rose for the area is a good indicator of the probable distribution of wind speed and direction for a given period (see Figure 2-3).

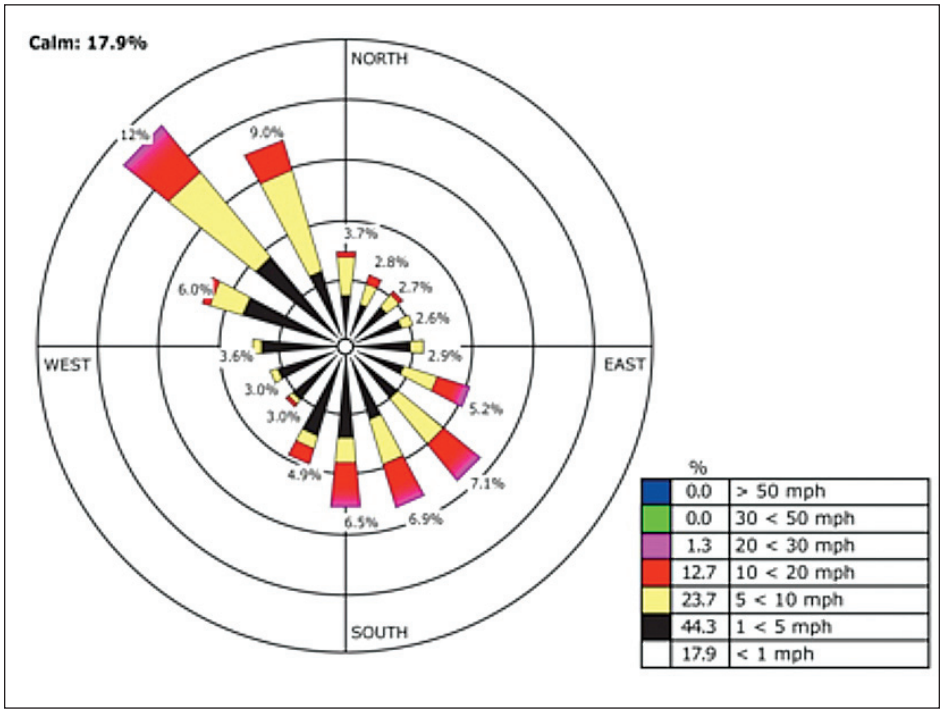


Figure 2-3:
Typical wind rose showing probability of wind speed and direction over a period of time for a specific city

SOURCE: NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION

2.2.4 Clustered or Dispersed Building Groups

A site may accommodate a single building or a group of buildings, depending on its size and other site characteristics, as well as building occupancy requirements. Groups of buildings may be clustered tightly in one area or dispersed across the site. The concentration of buildings, people, and operations in one place creates a target-rich environment, and the mere proximity of any one building to any other may increase the risk of collateral losses. In addition, the potential exists for the establishment of more single-point vulnerabilities in a clustered design than would exist in a more dispersed formation.

On the other hand, grouping high-risk activities, concentrations of personnel, and critical functions into a cluster can help maximize standoff from the perimeter and create a more effective defensible space. This may also reduce the number of access and surveillance points and minimize the size of the perimeter needed to protect the facilities.

By contrast, the dispersal of buildings, people, and operations across the site reduces the risk that an attack on any one part of the site will impact the other parts. However, this may have a functional or social isolating effect, reduce the effectiveness of onsite surveillance, increase the complexity of security systems and emergency response, and create a less defensible space (Figure 2-4).

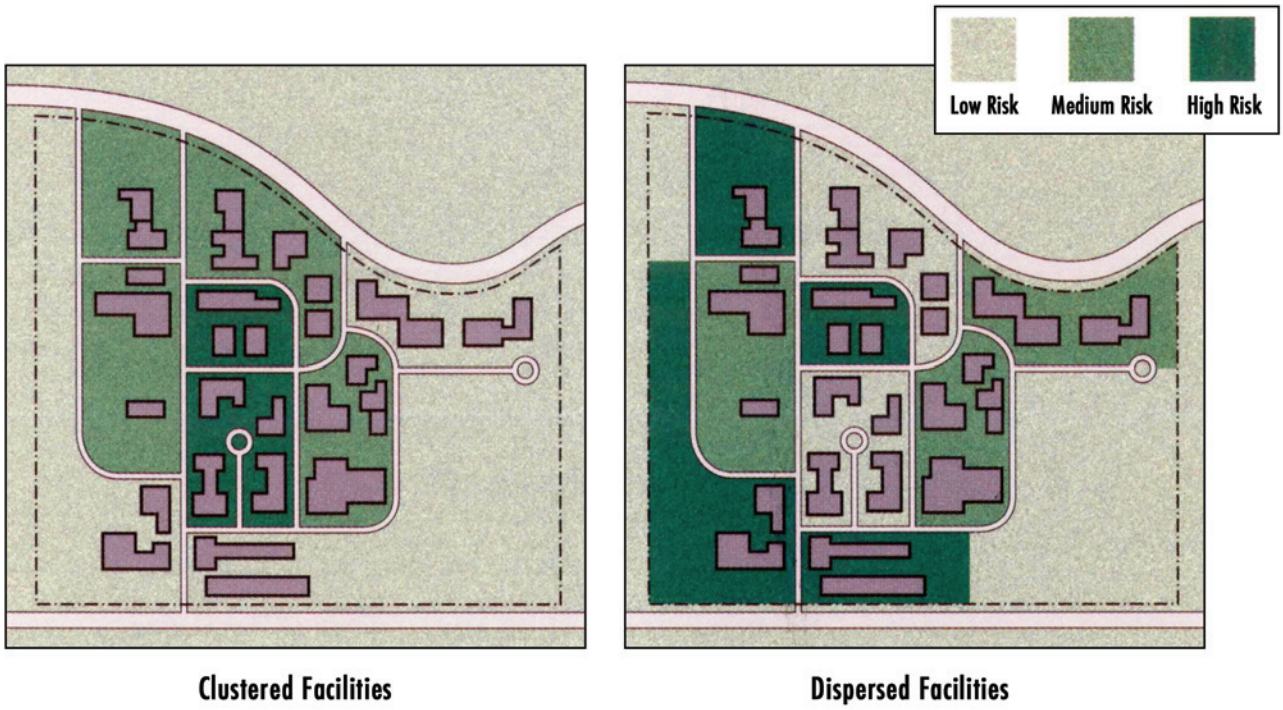


Figure 2-4: Clustered facilities (left) and dispersed facilities (right)

SOURCE: U.S. AIR FORCE INSTALLATION FORCE PROTECTION GUIDE

2.2.5 Vegetation

Vegetation onsite can open or block views, not only for security purposes but also to provide shade and enhance the appearance of the site. However, vegetation at the base of buildings and structures may exacerbate certain vulnerabilities by obscuring views from inside, providing hiding places for people and explosive devices, and facilitating surreptitious approach by potential attackers (see Figure 2-5).

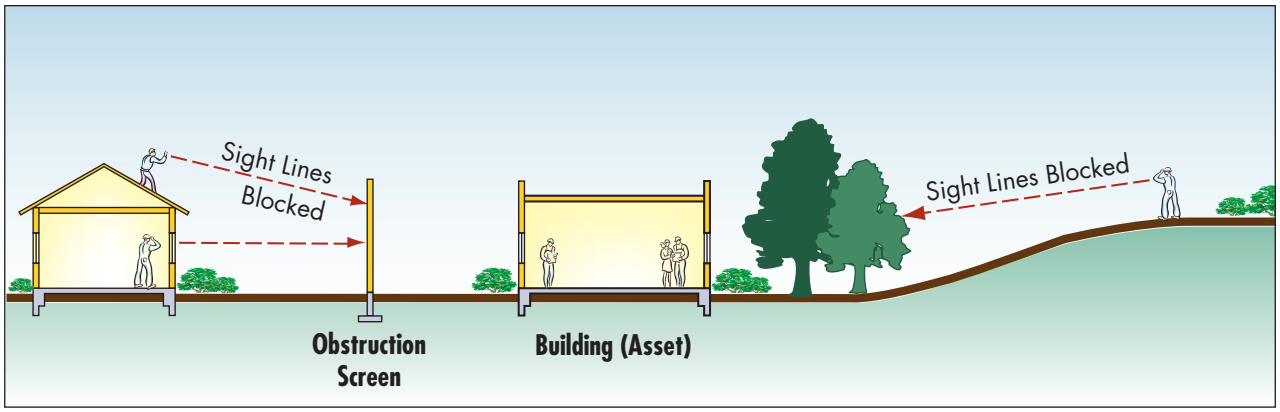


Figure 2-5: Trees and screens blocking sight lines into the site

SOURCE: U.S. AIR FORCE INSTALLATION FORCE PROTECTION GUIDE

2.3 General Site Security Design Strategies

The fundamental objective of site planning is to place buildings, parking areas, and other necessary structures to provide a setting that is functionally effective as well as aesthetically pleasing. The need for security adds another dimension to the range of issues that must be considered.

The design of protective measures for reducing site-related building vulnerabilities is based on a number of strategies that also represent the core principles of an effective security policy. They comprise the principles of a layered defense approach to security, standoff, access control, and secure perimeter.

2.3.1 Layers of Defense

The basic approach to site security design promoted in this manual is the concept of layers of defense. These are multiple consecutive layers of protective measures deployed in concentric circles around an asset that needs to be protected. They start from the outer perimeter and move inward to the area of the building with the greatest need for protection. The layers are mutually independent and designed to reduce the effectiveness of an attack by attrition, i.e., each layer is designed to delay and disable the attack as much as possible. To mount a successful attack, terrorists must penetrate and overcome each security layer without losses in momentum or capacity. This cumulative protection strategy is also known as protection-in-depth

The basic approach to site security design promoted in this manual is the concept of **Layers of Defense.**

and has been one of the basic CPTED strategies for protecting assets behind multiple barriers. Three main layers of defense emphasized in this manual are:

First or Outer Layer that consists of natural or manmade barriers usually at a property line or sidewalk/curb line.

Second or Middle Layer that usually extends from the perimeter of the site to the exterior face of a building. Similar to the first layer, protective measures consist of natural or manmade barriers along with a site design strategy of keeping terrorists away from the inhabited building.

First Layer of Defense: Consists of barriers usually at a property line or sidewalk/curb line.

Second Layer of Defense: Extends from the perimeter of the site to the exterior face of a building.

Third Layer of Defense: Usually inside the building and separates unsecured from secured areas.

Third or Inner Layer that is usually the facade and/or inside the building and separates unsecured from secured areas. The key concept of the third layer is building "hardening," or strengthening.

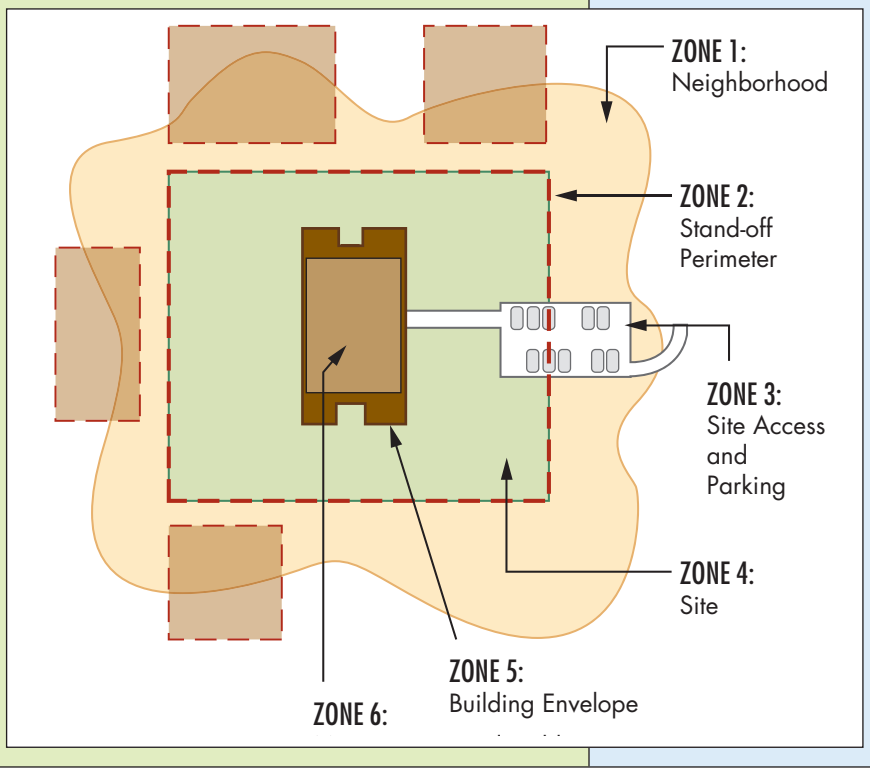
GSA has a similar approach to site security using the concept of six zones of security. The site security zones follow from the outside (Zone 1) to the inside of the building (Zone 6). Each zone offers opportunities to increase site security and enhance site appearance and function (GSA 2007). Table 2-1 compares FEMA's three layers of defense to the GSA concept of six zones of security for a building site, in which the sixth "zone" is management and operations.

Crime Prevention Through Environmental Design (CPTED)

CPTED is a methodology for crime prevention based on studies showing how physical design contributes to victimization by criminals. The methodology was originally applied to improve security in public housing, but now embraces wider aspects of criminality and terrorism. CPTED defines three basic strategies for security design: natural access control, natural surveillance, and territorial reinforcement. For more details about CPTED, refer to www.cpted.net.

Table 2-1: GSA Zones of Security and FEMA Layers of Defense

GSA Zones of Security	FEMA Layers of Defense
1. Neighborhood 2. Standoff Perimeter 3. Site Access and Parking 4. Site 5. Building Envelope 6. Management and Building Operations	1. First or Outer Layer 2. Second or Middle Layer 3. Third or Inner Layer



Most of the protective measures associated with the different layers of defense are relevant for high- to medium-risk buildings; precise measures are designed in response to the calculated blast threat and the desired protection level. These security elements can be implemented in conjunction with CPTED procedures.

2.3.1.1 Layers of Defense for Single Building Open Sites

On an open site, the defended perimeter may or may not be on the property line. Typically, the perimeter barrier designates the standoff distance around the building, beyond which is the area that building owners and occupants do not control.

Figure 2-6 shows a whole site as an exclusive protected area; the perimeter barrier is located on the property line and the onsite parking is within the second layer of defense. Crash-rated barriers are used where the site is vulnerable to invasive vehicles. The rear of the site is impassable to vehicles, so the barrier is limited to a fence to deter intruders.

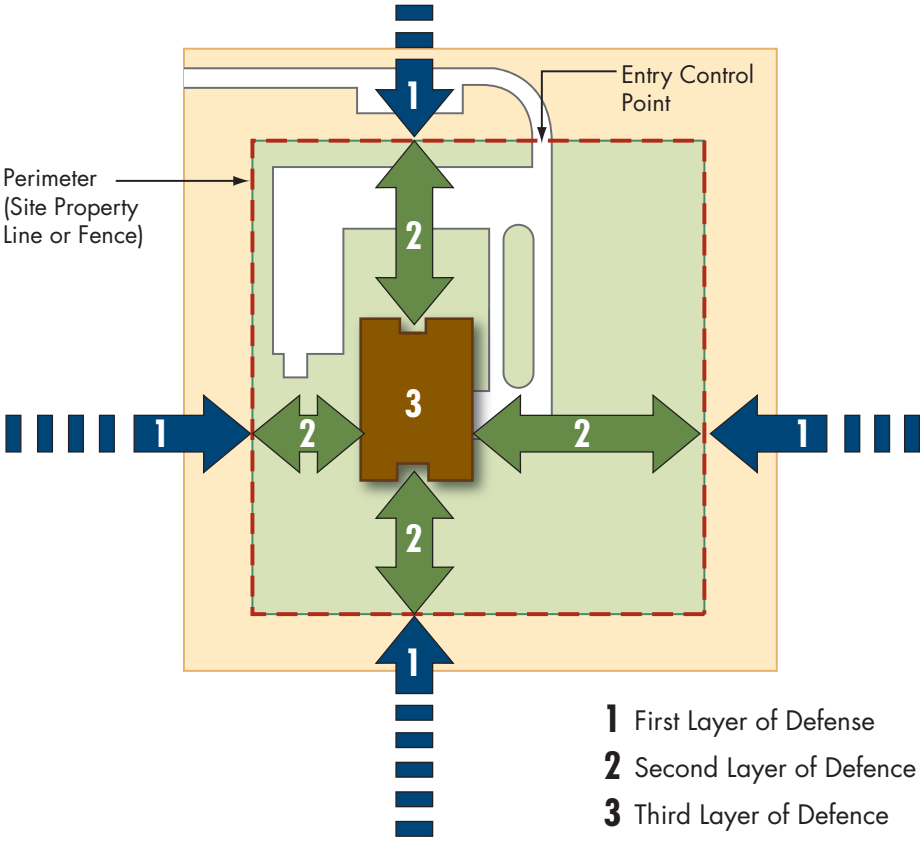


Figure 2-6:
Protective barrier located on the property line to provide required standoff, with onsite parking within the protected area

SOURCE: FEMA 430

An alternative solution is to place the protective barrier inside the property line, thus reducing the barrier's length and cost. The onsite parking is outside the access-controlled area, and a minimum standoff distance is provided (Figure 2-7)

An alternative solution is to place the protective barrier inside the property line, thus reducing the barrier's length and cost.

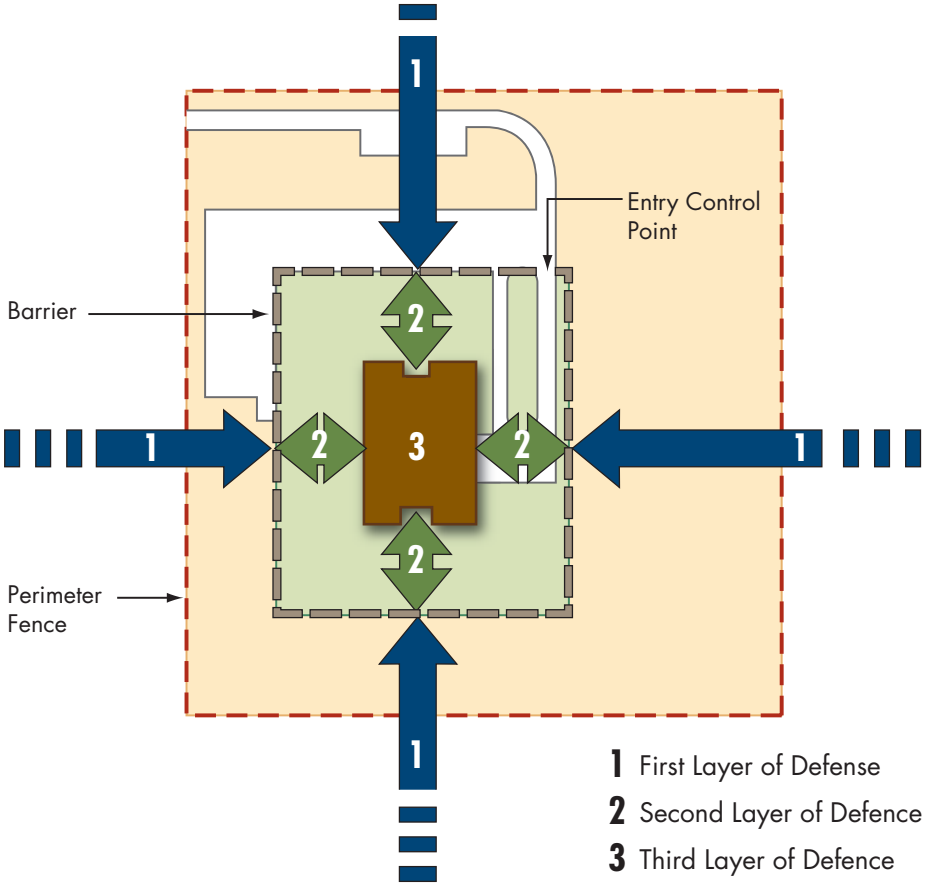


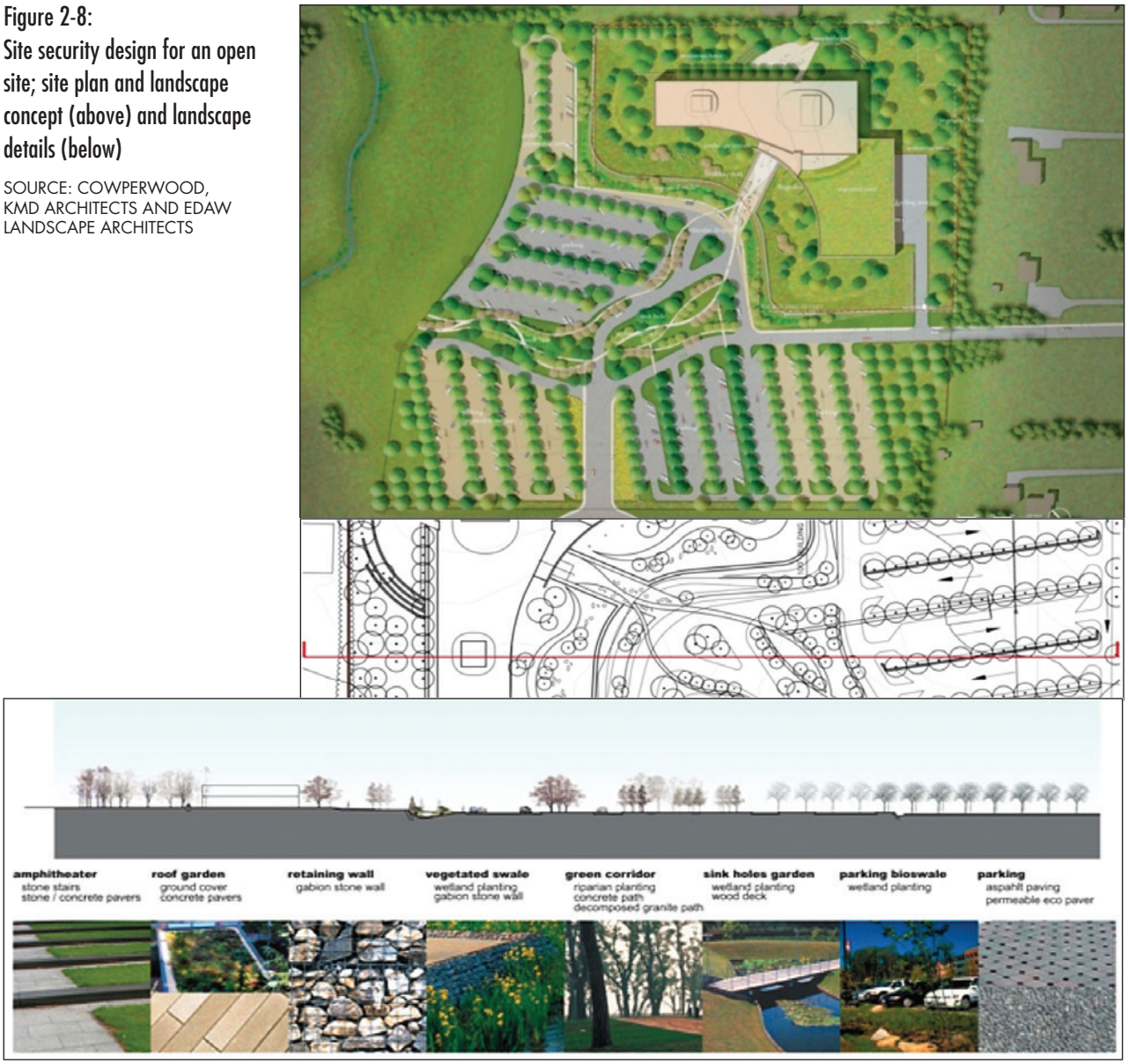
Figure 2-7:
Protective barrier located within the site, providing minimum standoff

SOURCE: FEMA 430

Figure 2-8 illustrates an example of a site security design for an open site. Note the indirect approaches to the building and the variety of landscape details.

Figure 2-8:
Site security design for an open site; site plan and landscape concept (above) and landscape details (below)

SOURCE: COWPERWOOD, KMD ARCHITECTS AND EDAW LANDSCAPE ARCHITECTS



2.3.1.2 Layers of Defense for Campus Sites

Layers of defense for a campus site may take several forms, depending on the threat level for the site as a whole as well as for individual buildings. The campus site in Figure 2-9 shows a typical first line of defense at the transition between the first and second layers of defense; additionally, inside the fully protected perimeter, areas of the site (e.g., buildings, public spaces, parking lots) also assume the role of first, second, and third lines of defense for one or more higher risk buildings.

Layers of defense for a campus site may take several forms, depending on the threat level for the site as a whole as well as for individual buildings.

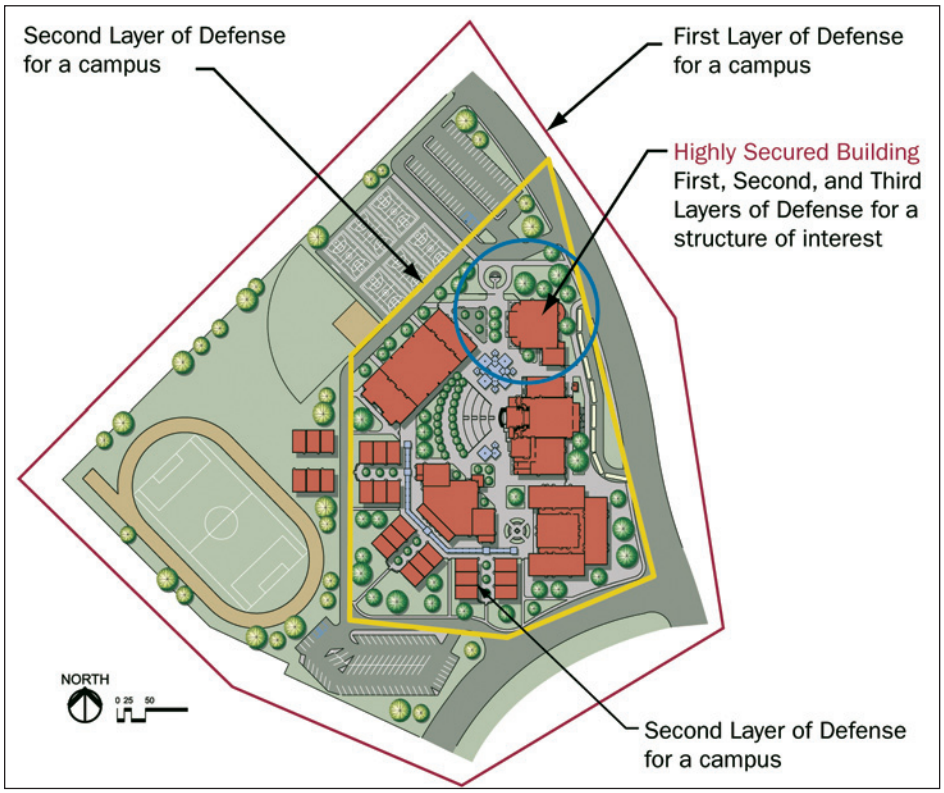


Figure 2-9:
Layers of defense for a campus site

SOURCE: WLC ARCHITECTS, INC.

In this example, the campus may have open access, but individual buildings have varying protection, from minimal access control to the full three layers of defense around a high-risk building. In this latter case, the rest of the campus with first and second layers of defense becomes the first layer of defense for the high-risk building. Protection for campus sites may reflect other variations:

- The campus site may have limited access control, as in a university that provides information and parking permits at entry points and a degree of security against normal criminal activity. Specific high-risk buildings on a campus, such as laboratories, may also have the full three layers of defense.
- The whole campus may be a high-risk site, for example, a military installation, a critical industrial facility, or a sensitive government laboratory. This campus site would have full perimeter barriers and access control, as well as second and third layers of defense measures within the perimeter.

2.3.1.3 Layers of Defense for Urban Sites

Urban sites, particularly the CBDs, comprise mostly commercial and institutional facilities. Building sites in the CBD are restricted in size because of the high cost of land and limited availability of buildable space, which has significant implications for site security design.

Although the layers of defense for a CBD site are compressed, the general principles still apply.

Although the layers of defense for a CBD site are compressed, the general principles still apply. The layers may be narrow and some may overlap for different protected spaces (as with campus sites explained above). As shown below in Figure 2-11, a zero-setback site may not have a second layer of defense. Building yards and plazas, or even the sidewalk, may provide the only setback (which is analogous to standoff distance); however, every foot of setback is of value.

Three generic building lot types are found in the CBD of any large city:

- **Buildings on lots with zero setbacks or adjacent to alleys:** The front face of the building is on the property line. Another face of the building may be on an alley
- **Building lots with yards:** The building is set back a small distance from the property line, and the space between is usually landscaped.
- **Building lots with plazas:** The building is sited within a private or public open space that is publicly accessible.

All CBD sites have a common set of urban elements, including sidewalks, streets, and streetscape (e.g., benches, planters, signs, trash receptacles). Planning, design, and placement of security elements in the CBD should not be detrimental to the critical urban design components that contribute to the success of vibrant, livable cities.

Zero-Setback Building Lots. Because of the high cost of urban real estate, most CBD buildings are on the property line. In such cases, the first layer of defense is outside the building owner's control and is usually a public sidewalk. The sidewalk may take on aspects of the second layer of defense if the building owner is granted permission to place vehicle barriers at the curb on municipal property. The third layer of defense then starts at the building face, i.e., the property line (Figure 2-10).

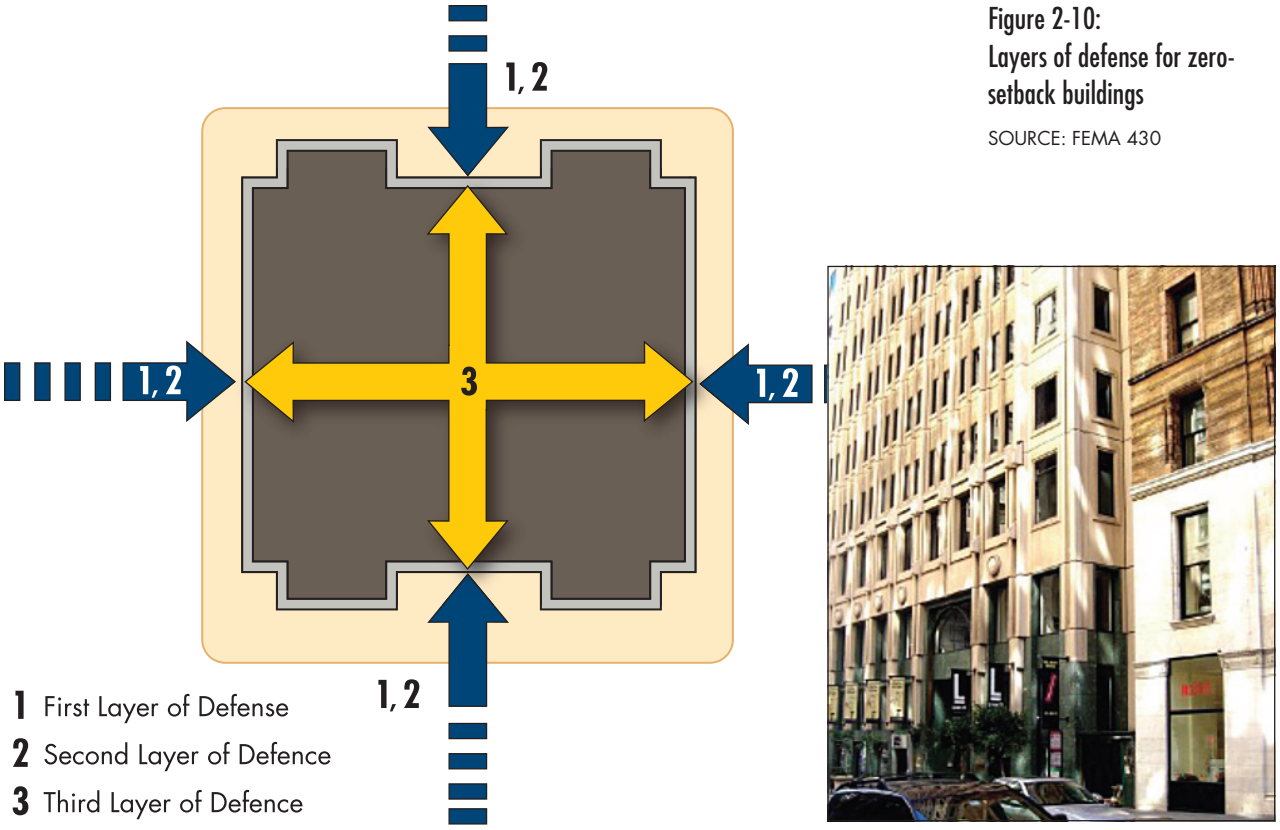


Figure 2-10:
Layers of defense for zero-setback buildings

SOURCE: FEMA 430

Where the public sidewalk is very narrow, or the building's face is on a narrow alley used for delivery vehicles, only a limited number of strategies can be employed, and increased risks may have to be accepted. Possible security strategies include the following:

- Extend the perimeter barrier across the public domain of the sidewalk, and eliminate a parking lane to gain standoff as a permanent measure.
- Prohibit street parking or close lanes as a temporary measure during times of increased threat.
- Provide adequate standoff and restrict vehicular access in urban locations of very high risk by closing streets and controlling and inspecting vehicles, as exemplified by the London "Ring of Steel" (Wall Street Journal 2006).
- When street closure is not feasible, the default solutions include hardening the building structure, glazing, and openings; providing increased surveillance to identify suspicious vehicles on adjacent streets; adding security with effective screening at public entrances and service areas; or accepting the risk. CPTED strategies may be appropriate to protect against conventional criminal acts.

- When the threat to an individual building in the CBD is relatively low, the building is well constructed, and the possibility of a head-on high-velocity vehicle attack is minimal, acceptance of risk may be the most reasonable course of action.
- For high-threat sites, a perimeter barrier at the edge of the sidewalk (allowing space for car doors to open) may reduce the risk of potential attack.

Zero-setback building lots adjacent to an alley are most at risk. The typical alley roadway is about 20 feet (6 meters) wide, with a sidewalk as narrow as 6 feet (1.8 meters) or less. Sometimes alleys do not have a discernible sidewalk, or a sidewalk is on one side only (Figure 2-11).

Figure 2-11: Typical alley (left) and alley with single sidewalk (right)

Permanent closure of alleys and typical urban streets is often not feasible because of service entry needs. In this instance, street closure that also allows service access may be achieved using active barriers, such as retractable bollards or other devices, together with security personnel and well-planned screening and inspection facilities.

Building Yards. Some buildings have a yard between the building face and the sidewalk. The yard is within the property line and typically consists of a grassy or planted area adjacent to the building. Yards are usually

included in governmental or institutional buildings, for which coverage of the entire site may not be as economically critical as it is in private development. Yards are typically narrow, on the order of 10 to 20 feet (3 to 6 meters), and provide some standoff distance beyond the sidewalk.

Although compressed, the three layers of defense can be identified in the building with a narrow yard shown in Figure 2-12. The curb lane and the sidewalk form the first layer of defense. The sidewalk serves as the common space for pedestrian movement, activity, and interaction. The building yard is the second layer of defense. In the yard, security components should complement the building architecture and landscaping, because they will be easily visible from the sidewalk, and should be located near the outer edge of the yard. An engineered planter or plinth wall can provide a good security barrier for this layer (Figure 2-13, left). The third layer of defense is the face and interior of the building.

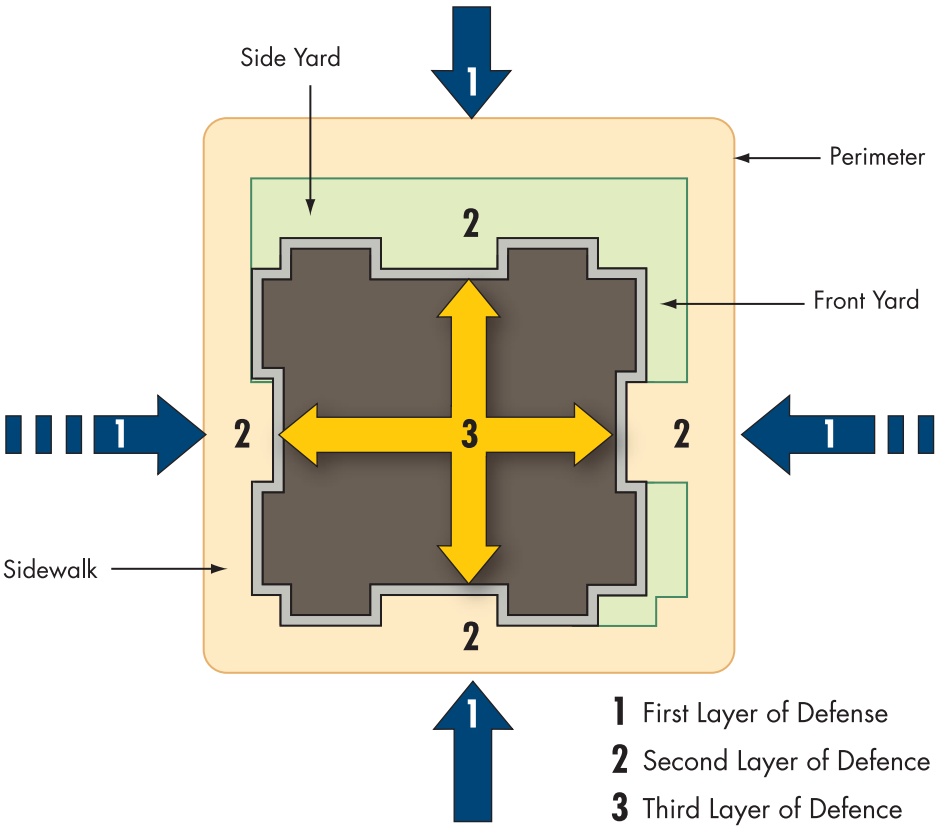


Figure 2-12:
Layers of defense for a building with yards

SOURCE: FEMA 430

Some major public buildings may have wide yards in the form of landscaped forecourts that offer reasonable standoff distance. Sometimes small yards (within the property line) are matched with a wide sidewalk provided by the city. The one shown at the right in Figure 2-13 is about 40 feet (12 meters) wide, which is an effective standoff distance.

Figure 2-13: Narrow yard with a raised planter (left); narrow yard and low planter with a wide sidewalk (right)

SOURCE: FEMA 430

Plazas. When extensive CBD development with very large buildings began after World War II and the straight tower with no setbacks became fashionable, new ordinances permitted developers to build taller buildings, with greater floor area, if a public plaza was incorporated (Figure 2-14) in the site design.

Figure 2-14
Major office building on a public plaza

SOURCE: FEMA 430

A plaza is an extended building yard, located outside the access-controlled area of the building, which provides an open public space. Plaza layers of defense are similar in arrangement to those of a yard. The additional space provided by a plaza allows a more effective second layer of defense to be achieved in an urban setting and often creates an acceptable standoff distance from one or more faces of the building, depending on the plaza-to-building relationship. Figure 2-15 shows the layers of defense with a plaza.

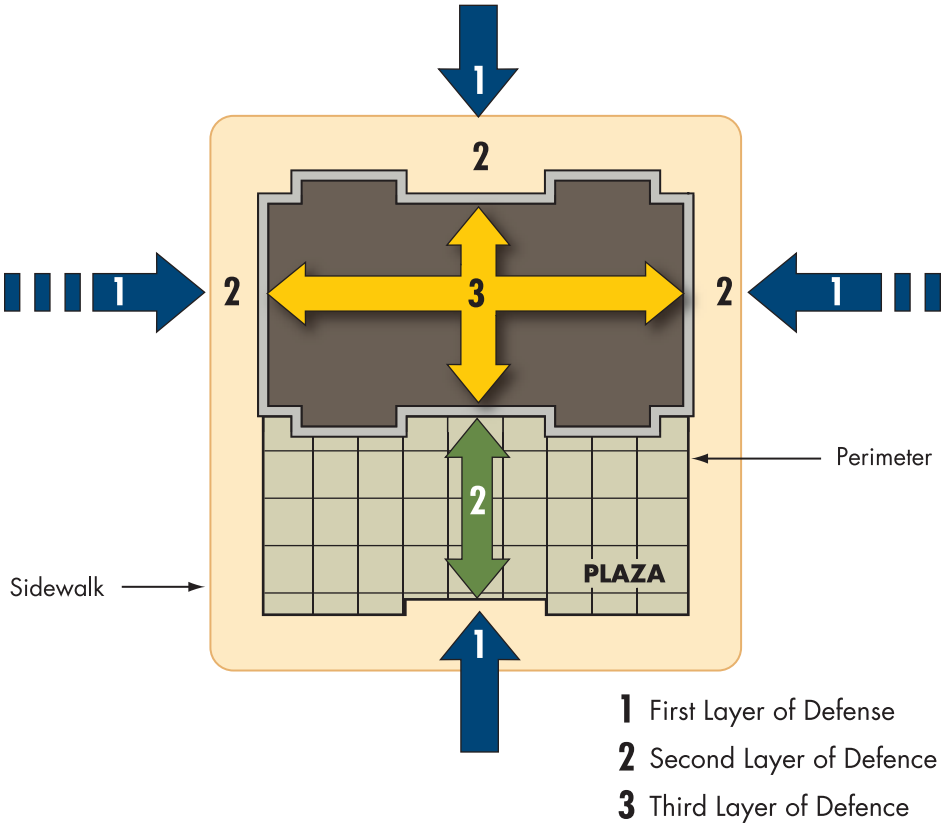


Figure 2-15:
Layers of defense for a plaza

SOURCE: FEMA 430

The plaza also provides an opportunity to install barriers within the second line of defense, which is the plaza itself. Designers are now experimenting with the use of interesting forms intended to enhance the aesthetics of the plaza while improving security (Figure 2-16).

In Figure 2-16, an existing plaza was retrofitted with barriers that are sculptured objects to make the plaza almost impenetrable by a vehicle. Combined with landscape features, such as plants, pools, and seating, these barriers make the plaza a much more interesting place than it was prior to the security retrofit.

Figure 2-16:
Sculptured forms, streetscape elements, and custom-designed bollards used as barriers at the San Francisco Federal Building

SOURCE: DELLA VALLE + BERNHEIMER ARCHITECTS/ RICHARD BARNES

2.3.2 Standoff Distance

For the protection of assets against outside explosions, especially those associated with VBIED, the most cost-effective solution for mitigating blast effects is to ensure the explosion occurs as far away from the building as possible. This distance, from the building face to nearest point that an explosive device can approach from any side, assuming that all security measures are in place, is referred to as the standoff distance or simply standoff (Figure 2-17).

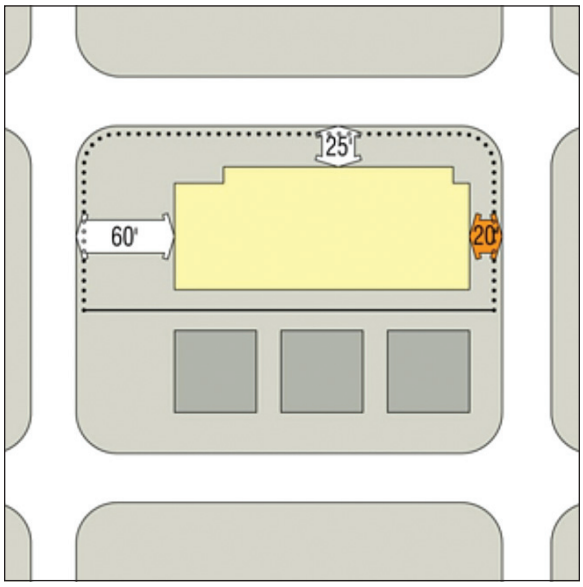


Figure 2-17: Standoff distance

SOURCE: DAVID SCHAFER ARCHITECT

For estimating purposes, the standoff distance is measured from the center of gravity of the charge located in the vehicle or other container to the face of the building under consideration.

2.3.2.1 Determining Standoff Distances

Determination of the minimum standoff is specific for each building or other asset and is based on the following:

- A prediction of the explosive weight of the weapon (expected blast load provided by the threat assessment).

- The required level of protection, which may be specified in the case of a Federal or other government building, using the ISC Security Design Criteria scale, UFC, or VA criteria. For a privately owned building, it is a determination of the acceptable risk made during the risk assessment process.
- An evaluation of the type of building construction, whether existing or proposed, including the building structure and the nature of the building envelope.

The DOD prescribes minimum standoff distances based on the required level of protection and expected blast load. Where minimum standoff distances are met, conventional construction techniques can be used with some modifications. In cases where the minimum standoff cannot be achieved, the building must be hardened to achieve the required level of protection. (See UFC 4-010-02, *UFC DOD Minimum Standoff Distances for Buildings* [DOD 2007b], and UFC 4-010-01, *UFC DOD Minimum Antiterrorism Standards for Buildings* [DOD 2007a].)

VA criteria limit unscreened vehicles from traveling or parking within 50 feet (15 meters) of their mission critical facilities; screened vehicles may travel/park as close as 5 feet (1.5 meters) to the facility. For VA life-safety protected facilities, vehicles are permitted to travel or park up to 5 feet (1.5 meters) from the facility.

The ISC Security Design Criteria, which apply to new Federal courthouses, Government offices, and major modernization projects, also recommend standoff distances based on the level of protection for the facility, but do not prescribe a minimum distance. These recommended distances apply for vehicles that are parked on adjacent properties and for vehicles that are parked on the building site. The ISC Security Design Criteria permit different levels so that each unique building can be designed to the level of protection that is appropriate for its unique circumstances as discussed further in Chapter 3, Section 3.1.4. (See *ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, Part 1 and Part II: Tables, Design Tactics and Additional Risk Guidelines* [DHS 2004a], and *ISC Security Standards for Leased Spaces* [DHS 2005].)

2.3.2.2 Constraints and Opportunities Provided by the Site

Because most open sites provide considerable open space for standoff, conventional construction, with minor modification, may provide an acceptable level of protection against blast. A satisfactory standoff, however, may be completely unachievable on a typical urban site, because the building face may be only 10 to 20 feet (3 to 6 meters) from the curb,

which is not an acceptable minimum distance from a potential blast. In such cases, alternative responses include protective measures, such as perimeter barriers, structural hardening, building envelope enhancement, operational procedures such as increased surveillance, or acceptance of some higher degree of risk.

At small standoff distances, even a few feet make a large difference in the blast loading. As noted above, increasing the standoff distance from 20 feet (6 meters) to 40 feet (12 meters) reduces the peak reflected pressure by a factor of four for a charge weight of 10 pounds (4.5 kilograms) and a factor of nearly seven for a charge weight of 1,000 pounds (454 kilograms). The relationship between standoff distance and component cost is illustrated in Figure 2-18.

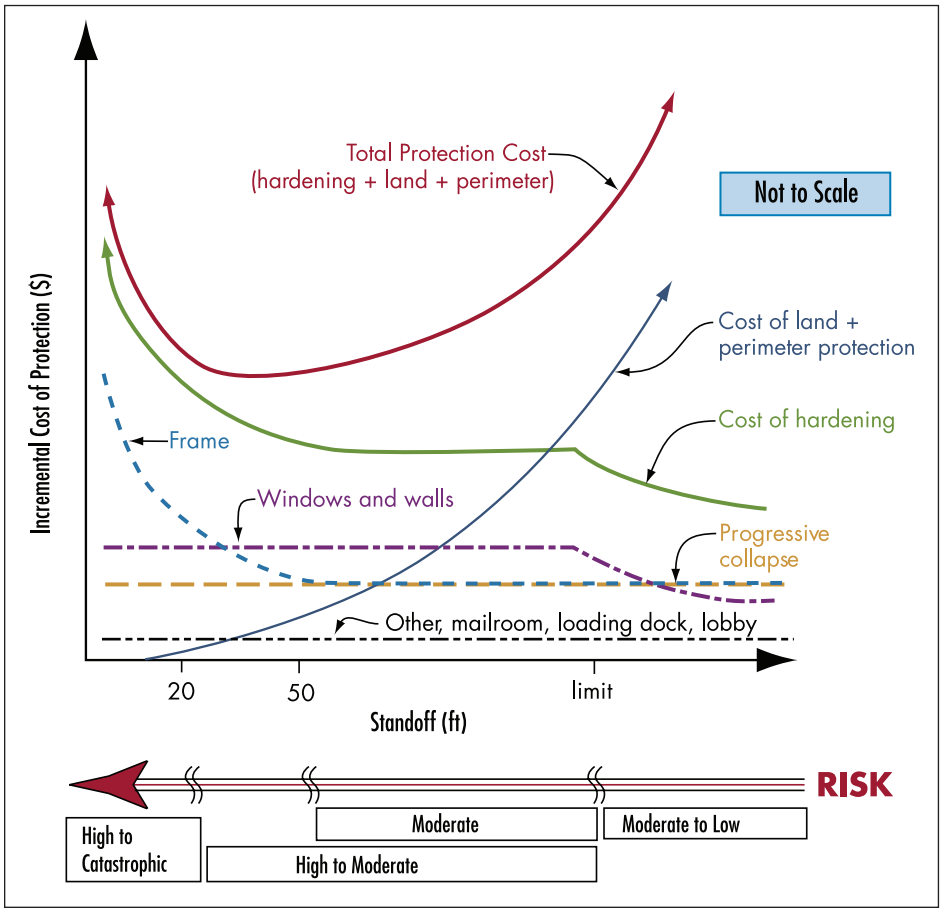


Figure 2-18:
Impact of standoff distance on component costs

SOURCE: JOSEPH L. SMITH, PSP AND LARRY M. BRYANT, APPLIED RESEARCH ASSOCIATES , INC.

For a more complete discussion of levels of protection, blast loading, standoff distance, and effects of blast see Chapter 3, Sections 3.1.2 and 3.1.4. See Section 2.3.1 for more detailed discussion of protective design for urban sites.

2.3.3 Access Control

Access control is one of the key considerations when determining an effective placement for a building[2]. Designers should determine whether the building to be protected requires an exclusive or nonexclusive access zone (see Figure 2-19). An exclusive zone is defined as the area surrounding a single building or building complex that is in the exclusive control of the owners or occupants: anyone entering an exclusive zone must have a legitimate reason. A nonexclusive zone may be either a public right-of-way, such as plazas, sidewalks, and streets surrounding a downtown building, or an area related to several buildings, such as a courtyard in an industrial park with open access. The access-controlled zone may range from a complete physical perimeter barrier (full control), to relatively minimal anti-vehicle protection with full pedestrian access, or simple electronic monitoring of the perimeter.

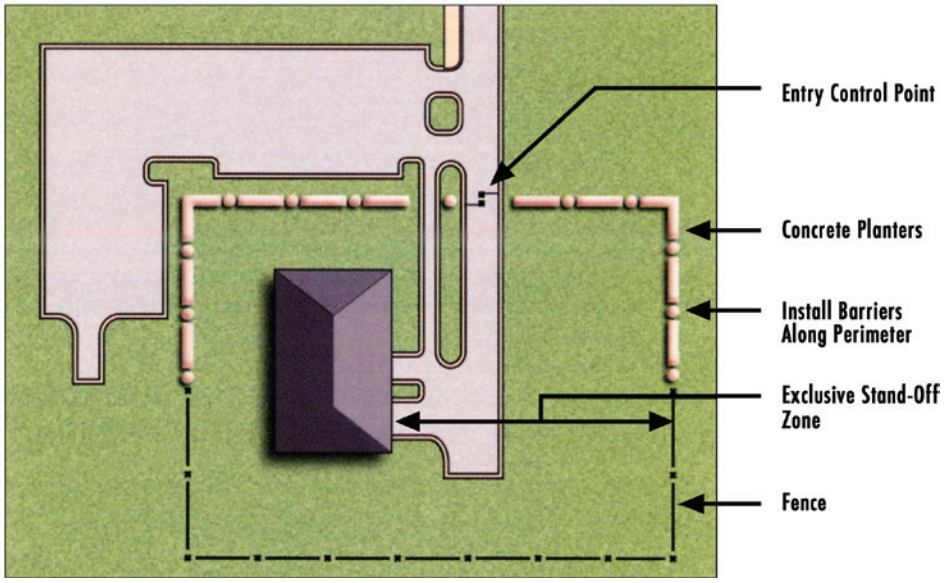


Figure 2-19:
Exclusive zone within the site property

SOURCE: U.S. AIR FORCE INSTALLATION FORCE PROTECTION GUIDE

Some projects may require control of pedestrians and bicycles. In these cases, provision of a walkway and a turnstile for pedestrians (complying with the ADA Accessibility Guidelines) should be considered.

2.3.3.1 Vehicle Approach Speed Control

The threat of vehicular attack can be reduced significantly by controlling vehicular speed and removing the opportunity for direct collision with the building. If a vehicle is forced to slow down and impact a barrier at a shallow angle, the impact forces are reduced, and the barrier can be designed to lower impact requirements.

2 See Chapter 5 for a complete discussion of access control, specifically Section 5.5.2.

The speed of vehicles can be reduced by designing entry roads to sites and buildings that do not provide direct or straight-line access, making it impossible for a vehicle to gather speed as it approaches. Indirect approaches to a building, together with appropriate landscaping and earth forms, can also increase the attractiveness of the access road. Controlling the view of the building by landscaping can enhance the aesthetic experience.

Figure 2-20 shows a portion of an analysis of threat vehicle approach speed, which is used to determine the alignment and curvature of access roads to a large facility. The objective is to force the vehicle to impact the barrier at reduced speed and at a shallow angle. This method of analyzing vehicle approaches and speeds also can be used for enhancing the overall urban design of a site and its environs, as well as increasing pedestrian safety.

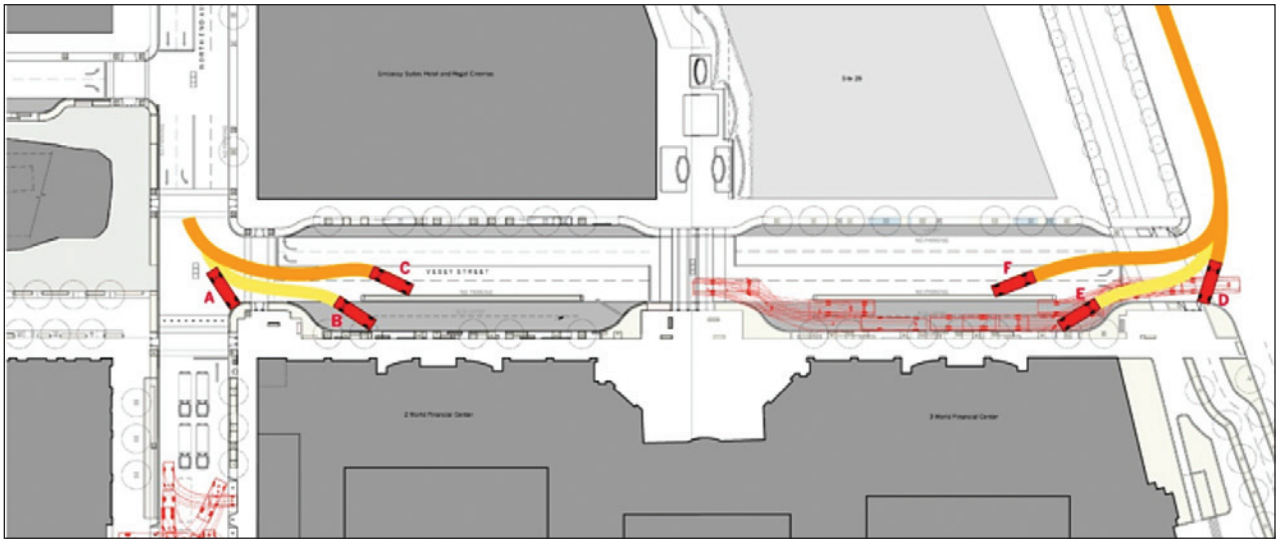


Figure 2-20: Portion of threat vehicle approach speed analysis

SOURCE: ROGERS MARVEL ARCHITECTS LLC

The following represent some familiar devices and design methods for reducing vehicle speed:

- Traffic circles
- Curved roadways
- Chicanes (obstacle placement used to create a curved path on a straight roadway)
- Speed bumps and speed tables
- Raised crosswalks
- Pavement treatments
- Use of berms, high curbs, and trees to prevent vehicles departing the roadway

Speed control of vehicles approaching gatehouses is also a concern. Some of the devices and design methods listed above can be used when approaching gates. In addition, bollards around the gatehouse can be used to narrow the approach. Truck entrances will require wider lanes that can be handled by either active or removable bollards to limit the opening when trucks are not entering.

2.3.3.2 Entry Control and Vehicular Access

The objective of the access point is to prevent unauthorized access, while at the same time controlling the rate of entry for vehicles and pedestrians. An access point is a designated area for authorized building users, such as employees, visitors, and service providers. Access points along the defended perimeter are commonly shared between the first and second layers of defense, providing observation of approach, controlled entry, and queuing areas. Structures such as control booths and equipment such as active barriers, communications, and VASS (or closed-circuit television [CCTV][3] are layered throughout the entry sequence to provide secured access points. Although the access itself is from a public roadway, these site features are typically within the site property line and form part of the first defense layer.

The objective of the access point is to prevent unauthorized access, while at the same time controlling the rate of entry for vehicles and pedestrians.

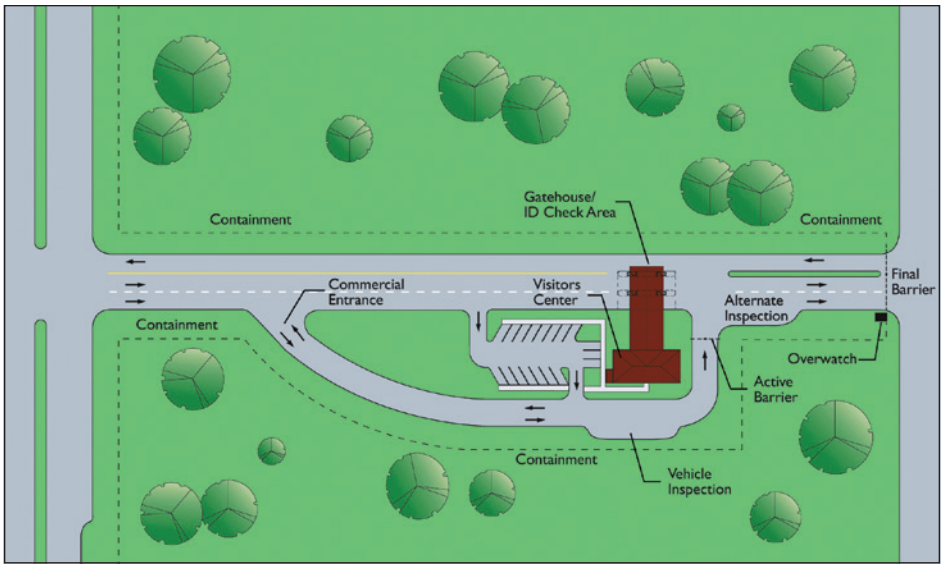


Figure 2-21:
Typical entry control point layout

SOURCE: U.S. AIR FORCE INSTALLATION ENTRY CONTROL FACILITIES DESIGN GUIDE

3 See Chapter 5, because security video serves two distinct purposes, assessment and surveillance, the term used here is video assessment and surveillance system (VASS). Historically, the term for a security video system was CCTV, a closed analog video system.

The location of access control points and inspection areas should be at a sufficient standoff distance that the detonation of a bomb on an uninspected vehicle does not impact the closest building and cause lethal damage. Figure 2-21 shows a typical layout of a high-security vehicle entry point and an access-controlled zone within a protected perimeter.

Whenever possible, commercial, service, and delivery vehicles should have a designated entry point to the site, preferably away from high-risk buildings. Active perimeter entrances should be designated so that security personnel can maintain full control without creating unnecessary delays. This can be accomplished by the provision of a sufficient number of entry points to accommodate the peak flow of pedestrians and vehicular traffic, as well as adequate lighting for rapid and efficient inspection.

The number of access points into a site should be minimized because they are a potential source of weakness in the controlled perimeter, and are costly to construct and operate. However, at least two access control points should be provided in case one is shut down by maintenance, bomb squad activity, or other activities.

2.3.3.3 Gatehouses and Security Screening

Gatehouses and screening require manned access control. Design of the entry control point must accomplish many security-related functions to accommodate traffic, control the approach and direction of vehicles, accommodate queuing, and support the inspection staff. The placement of the control point itself, with the associated lanes and gates as well as the guardhouse and/or visitor center, must balance all these requirements.

Guidance for the design of gatehouses includes the following:

- Gatehouses should be hardened as determined by the expected blast load and should provide protection from the elements.
- If identification (ID) checking is also required between the traffic lanes, some measure of protection against hostile activity should be provided for the security guard.
- Gatehouses, lobbies, and guard posts should be provided with clear views of approaching traffic, both pedestrian and vehicular.
- Queuing space for pedestrian visitors should be provided in a screening pavilion beyond the building entry, which should be at a distance from the main facility.

- Active vehicle crash barriers are necessary to deny entry and to give entry control personnel adequate time to respond to unauthorized activities. The response time is defined as the time required for complete activation of the active vehicle barrier once a threat (vehicle circumventing access control) is detected. The response time includes the time for security personnel to react to a threat and initiate the activation of the barrier system, and the time for the selected barrier to fully deploy and close the roadway.

Active vehicle crash barriers are necessary to deny entry and to give entry control personnel adequate time to respond to unauthorized activities.

Figure 2-22 shows a detailed basic layout for a vehicle entry control point with a gatehouse at one side. This arrangement is suitable for low throughput situations, but for high throughput, the gatehouse should be on the driver's side of vehicles entering the site (between the entrance and exit lanes) so that the security guard need not walk around the vehicle.

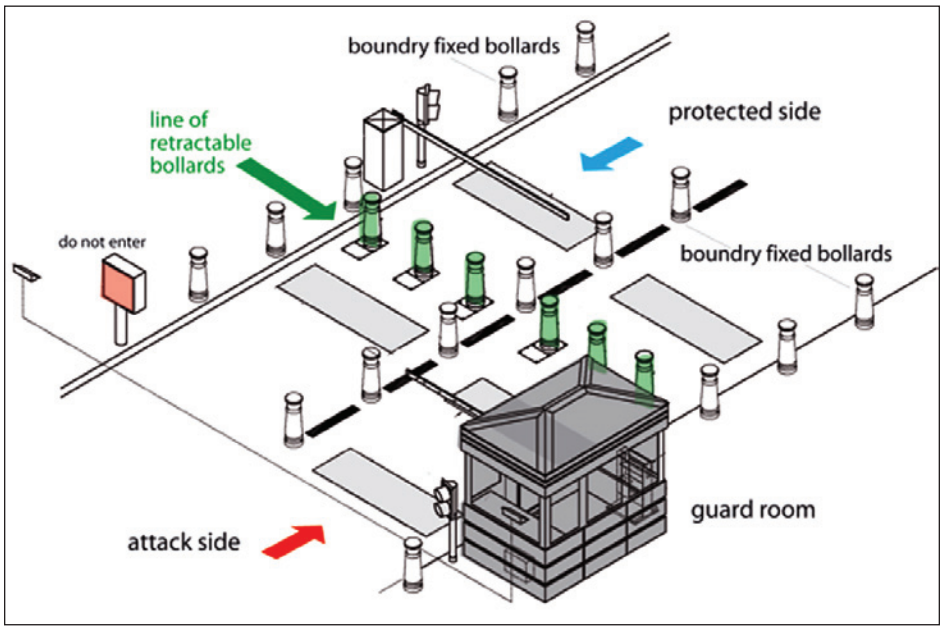


Figure 2-22:
Features of a typical vehicular entry control post, with gatehouse at side

SOURCE: DELTA SCIENTIFIC CORP.

While Figure 2-22 shows a typical metal prefabricated gatehouse, gatehouses designed to harmonize with the building architecture are more attractive. Figure 2-23 shows a simple but well-detailed concrete structure (left) that matches the contemporary concrete building design, and a more decorative small building (right) with fine iron gates to reflect the architecture of the buildings protected.

Figure 2-23: Gatehouses that match the architecture

SOURCE: FEMA 430

When considering access roads and inspection lanes, designers should have in mind the following:

- Approaches to the site should be designed to accommodate peak traffic demand without impeding traffic flow on the surrounding roadways.
- Pullover lanes at site entry gates should be provided for an initial vehicle check prior to allowing access to a site.
- Holding or containment areas for screening vehicles should be established outside the secured perimeter that establishes the standoff distance. The proper placement of these areas is critical to their effectiveness, the functionality of the site, and the overall appearance of the project.
- Inspection areas should be large enough to accommodate a minimum of one vehicle and a pullout lane. They should also be covered and be capable of accommodating the inspection of the undercarriage and overhead inspection equipment.
- Parking of vehicles too close to the building should be avoided even after screening.
- Available inspection technologies (e.g., above-vehicle and under-vehicle surveillance systems, ion scanning, x-ray equipment) should be investigated when sizing and designing the inspection areas.

A separate, sheltered structure for pedestrian visitors may be a good solution when lobby space is limited. This also facilitates screening of small packages outside the main building footprint.

For high-security buildings, a final denial barrier after initial screening is necessary to stop unauthorized vehicles from entering the site. Most individuals who attempt to enter without authorization are lost, confused, or inattentive, but some may intend to "run the gate." A properly designed final denial barrier will take into account both groups, safely stopping the individuals who have made an honest mistake, but providing a properly designed barrier to stop those with hostile intentions.

Placement of the final denial barrier is based on the activation time of an explosive device and the response time needed for a given scenario. For example, to stop a high-performance vehicle that accelerates from a stop at the ID check, given an 8-second response time, an active barrier should be placed approximately 330 feet (100 meters) from the access control point (Figure 2-24).

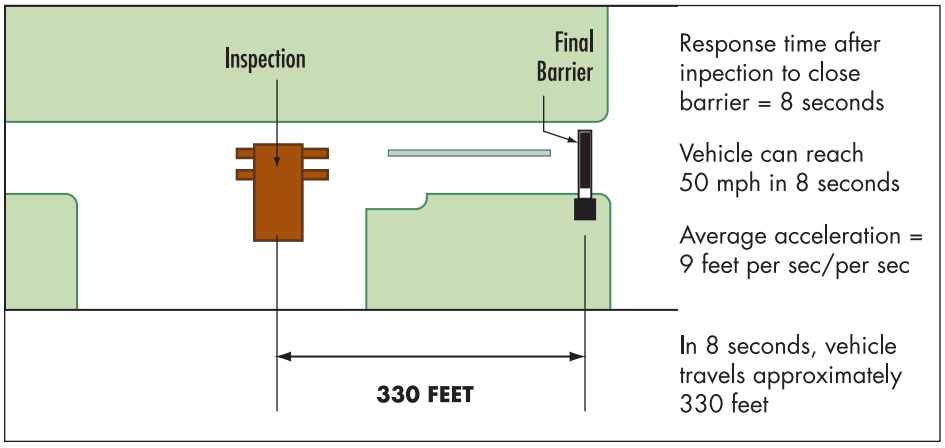


Figure 2-24: The final barrier

SOURCE: FEMA 430

2.3.3.4 Sally Ports

In very high-risk situations, a double row of barriers is used, creating a sally port. Before 9/11, sally ports were used almost exclusively in correctional institutions and military installations. They consist of an enclosure with two electrically operated barriers; only one barrier is allowed to open at any one time. The first barrier opens only after authorized entry is determined and closed after the vehicle enters; the second barrier is opened after the inspection is completed and closed after the vehicle exits. This ensures that a following vehicle cannot "tailgate" the lead vehicle and obtain entry without screening. Figure 2-25 shows a sally port used for vehicular entry.

Figure 2-25: Sally port installation with two active barriers

NOTE: NOGO BARRIERS AT THE SIDES. SEE TABLE 2-4, ID P3 FOR DESCRIPTION.

2.3.4 Perimeter Security

A perimeter security system comprises two main elements: the perimeter barrier that prevents unauthorized vehicles and pedestrians from entering the site, and access control points at which vehicles and pedestrians can be screened and, if necessary, inspected before they pass through the barrier.

After 9/11 many cities experienced a proliferation of barriers, street closures, and other security measures around high-risk Federal and private buildings. In some cases, these measures have been considered successful from a security, architectural, urban planning, and cultural preservation standpoint. In many cases, however, the installation of security barriers has been acknowledged as detrimental to the function, quality, and utility of the public realm. Restricting vehicle access can cause significant traffic congestion and can create unnecessary obstacles on streets and sidewalks that minimize the efficiency of pedestrian and vehicle circulation systems and hinder the access of first responders in emergencies.

The following goals are suggested for perimeter security planning:

- To provide perimeter security in a manner that does not impede the city's commerce and vitality, nor excessively restrict or impede use of sidewalks and pedestrian and vehicular mobility, nor affect the health of existing trees.
- To provide security in the context of streetscape enhancement and public realm beautification, rather than as a separate or redundant system of components whose only purpose is security.
- To produce a coherent strategy for deploying specific families of streetscape and security elements in which priority is given to achieving aesthetic continuity along streets, rather than solutions selected solely by the needs of a particular building under the jurisdiction of one public agency.

Perimeter security protection is accomplished by design strategies that use a variety of methods to protect the site. The architecture and the landscaping of the site entry elements are the first part (and may be the only part) of the project that is visible to the general public. As such, they introduce the identity of the site, its architectural style and quality, and impart a sense of welcome or rebuff.

Perimeter security protection is accomplished by design strategies that use a variety of methods to protect the site.

To achieve a welcoming atmosphere when incorporating security barrier systems, the following should be considered:

- Sidewalks should be open and accessible to pedestrians to the greatest extent possible, and security elements should not interfere with circulation, particularly in crowded locations.
- Barrier layout at sidewalks should be such that a constant clear path of 8 feet (2.4 meters) or 50 percent of the sidewalk, whichever is greater, is maintained.
- All necessary security elements should be installed to minimize obstruction of the clear path. They should be placed in an available amenity strip adjacent to most curbs, which is typically designated for street furniture and trees and not part of the existing clear path.
- Any security (or other) object placed at the curb should be at least 2 feet (0.6 meter) from the curb line to allow for door opening and to facilitate passenger vehicle pickup and dropoff where permitted along the curb. Ideally, passenger dropoff points should be located in pullover or stopping points where the setback is greatest.

- Design and selection of barriers should be based directly on the threat assessed for the project, as well as available countermeasures and their ability to mitigate risk; excessive barriers should be avoided.
- Block after block of the same element, no matter how attractive, does not create good design. When a continuous line of bollards approaches 100 feet (30 meters), it should be interspersed with other streetscape elements, such as hardened benches, planters, or trees.

Opportunities to add a palette of elements, such as varied bollard types, engineered sculptured forms, hardened street furniture, low walls, and judicious landscaping can all assist in creating a functional yet attractive barrier that will enhance the setting. Solutions that integrate a number of appropriate perimeter barriers into the overall site design will be more successful.

2.3.4.1 Barrier Performance Criteria

The security design criteria required for a barrier are largely determined by key information obtained in the following steps in the risk assessment process.

1. A threat analysis based on the expected blast loads provides the following:
   - Vehicle size, weight, speed
   - Bomb size (weapon yield in pounds of trinitrotoluene [TNT] equivalent) and worst-case standoff distance
2. The vulnerability analysis provides:
   - Building envelope and structural information that contributes to the determination of the appropriate standoff distance, and that enable possible tradeoff between alternative building characteristics and standoff distances to be evaluated and budgeted.
   - Information on available standoff distances.
   - Information on the possible reduction of vehicle speed through the existing or modified characteristics of approach roads using various traffic calming techniques.
   - Limitations imposed by underground utilities.
   - Information on the types of soil, which affect barrier standards.
3. The risk assessment provides:
   - Information to assist the property owner in determining the acceptable risk and the desired level of protection.

In an urban setting, engineered bollards are the most common type of barriers used because of their high-performance rating. In open sites, where more space is available, a large variety of barriers and obstacles are used. Barrier systems must be properly designed, constructed, and maintained regularly to ensure their correct operation. This particularly applies to active barriers with movable elements.

In urban sites, the greenfield bollard foundation, as shown in Figure 2-26, may only be suitable for a limited portion of a building site perimeter that does not require site-specific modifications as a result of sub-grade interference with utilities, vaults, and other urban infrastructure. The bollards should be placed as close to the roadway as possible, which may require obtaining permission if the installation is within public space (e.g., a sidewalk owned by the local municipality). In some cities, such as New York City and Washington, DC, individual approvals must be obtained from various utility companies prior to the construction of bollards. Additionally, utility companies may require evidence that gravity and impact loads do not harm performance of the utilities. The foundation details must also provide utility companies with proper access to their infrastructure.

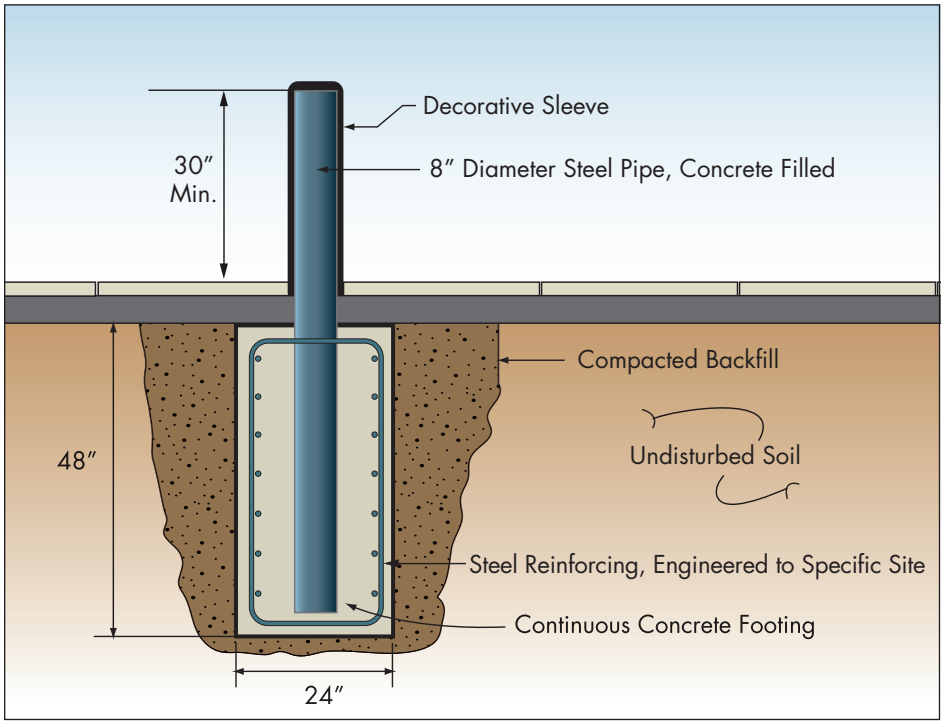


Figure 2-26:
Section through typical greenfield bollard

SOURCE: DOS

Local government planning legislation designates permitted uses of land based on prescriptive zoning. An example of prescriptive zoning, which may seriously impact barrier development, is that of revocable consent.

Several methods can be used to evaluate the expected performance of anti-ram barriers. Two primary methods are developing and evaluating analytical models and performing crash tests of sample barriers in controlled conditions.

2.3.4.2 Analytical Models

Analytical methods used to evaluate performance vary in accuracy. Three main methods are used.

Equivalent force methods are the simplest and typically use the ultimate force of the barrier materials, such as ultimate bending capacity of the pipe bollard, to design the foundation. This method does not take into account the amount of energy that is dissipated when the attack vehicle crushes upon impact with the barrier; thus, it typically produces large foundations that may exceed the size of foundations that are validated through impact testing.

Analytical methods used to evaluate performance vary in accuracy. Three main methods are used: equivalent force; energy methods; and the advanced non-linear finite method.

Energy methods are generally less conservative than equivalent force methods, and much more rigorous. These methods account for the energy dissipation of elastic and plastic deformation of the bollard system. The kinetic energy of the moving vehicle is transferred into the bollard and its foundation, and the full energy of the impact is dissipated through deformation of the bollard system. However, the result is also conservative because it does not take into account the crushing of the impact vehicle itself.

The **advanced non-linear finite method** is the only analysis that can reasonably calculate the strength and performance of an anti-ram barrier while accounting for site-specific subgrade conditions. Use of this approach to model structural configurations of interest allows for detailed representation of the structural system and subgrade conditions through failure. Models can include details such as utility penetrations, varying depths of foundations, varying soil compositions, reinforcing configurations, and other site-specific conditions. Modeling both the impacting vehicle and the barrier accurately accounts for energy dissipation from plastic deformation of impact and crushing. Variations in impact conditions, impact speed, and angle of approach can be easily addressed. Although the application of finite element methods to impact analyses is an established practice, the finite element models and software must be validated against actual impact tests to validate their accuracy. The cost associated with use of finite element models is greater than the use of simplified tools, but the results are more accurate and allow site-specific conditions to be addressed.

2.3.4.3 Barrier Crash Testing

The designer must be familiar with the relative performance of various methods of perimeter protection so that appropriate choices can be made given the particular site conditions. This manual is primarily concerned with protecting buildings from explosive loads; therefore, effectiveness of barriers in stopping vehicle entry is a critical performance parameter.

DOS developed the crash test standard in common use. To obtain DOS certification, the vehicle barrier must be tested by an independent crash test facility to meet DOS standards. The test specifies perpendicular barrier impact by a 15,000-pound (6804-kilogram) diesel truck.

Initially, the DOS standard provided for three levels of intrusion:

- **Level 3:** Allows intrusion of the vehicle 36 inches (0.91 meters) into the barrier.
- **Level 2:** Allows intrusion of the vehicle 20 feet (6.1 meters) into the barrier.
- **Level 1:** Allows intrusion of the vehicle 50 feet (15.2 meters) into the barrier.

In 2003, the standard was revised, and levels 1 and 2 were deleted. The foremost reason for the change was that limited setback distances precluded the use of any devices at DOS facilities or compounds that did not meet the highest test level—those allowing no more than 36 inches (0.91 meters) penetration distance. The standard currently provides certification for three classes of protection.

Certification Class	Speed (mph)	Speed (km/h)
K12	50 mph	80 km/h
K8	40 mph	65 km/h
K4	30 mph	48 km/h

To become certified with a DOS K rating, the 15,000-pound (6,804-kilogram) truck must achieve one of the K-rating speeds, and the bed of the truck must not penetrate the barrier by more than 36 inches. The test vehicle is a medium-duty truck, such as those that any driver with a commercial license and a credit card can buy or rent. Note that the amount of intrusion is measured to the front of the cargo bed of the truck, where explosives would typically be located, as shown in Figure 2-27.

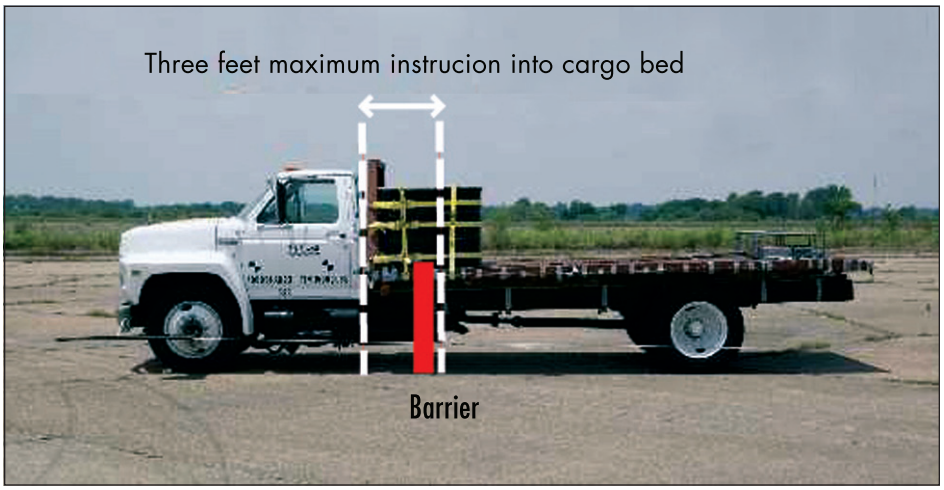


Figure 2-27:
Barrier test intrusion limits
SOURCE: FEMA 430

Beginning February 1, 2009, DOS decided to evaluate new antiram barriers tested under ASTM F2656-07 *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers* for selection and approval for use at DOS facilities. The only barriers considered are those with an ASTM F2656-07 rating of M30 P1, M40 P1, and M50 P1. The chosen impact point must be agreed to by DOS.

ASTM F 2656-07 provides a range of vehicle impact conditions, designations, and penetration performance levels that allow an agency or owner to select passive perimeter barriers and active entry point barriers appropriate for use at facilities exposed to VBIED threats.

Table 2-2 provides information for four different vehicle types: small passenger car (C), pickup truck (P), medium-duty truck (M), and heavy goods vehicle (H). Nominal minimum test velocities vary from 30 miles per hour (mph) to 60 mph for each vehicle type. Condition designations are provided for each vehicle type and appropriate nominal speed. As an example, the condition designations for the M cited in the DOS considerations above are M30, M40, and M50, with the number indicating the nominal speed.

Table 2-2: Impact Condition Designations

Test Vehicle/ Minimum Mass lb (kg)	Nominal Min.Test Vehicle Velocity mph (km/h)	Kinetic Energy ft-kips (KJ)	Condition Designation
Small Passenger Car (C) 2,430 (1,100)	40 (65)	131 (179)	C-40
	50 (80)	205 (271)	C-50
	60 (100)	295 (424)	C-60
Pickup Truck (P) 5,070 (2,300)	40 (65)	273 (375)	PU- 40
	50 (80)	426 (528)	PU-50
	60 (100)	613 (887)	PU-60
Medium-Duty Truck (M) 15,000 (6,810)	30 (50)	451 (656)	M-30
	40 (65)	802 (1,110)	M-40
	50 (80)	1,250 (1,680)	M-50
Heavy Goods Vehicle (H) plus 15,000 (6,810)	30 (50)	11,950 (2,850)	H-30
	40 (65)	3,470 (4,810)	H-40
	50 (80)	5, 430 (7,820)	H-50

SOURCE: ADAPTED FROM ASTM F 2656-07, TABLE 1

Notes: lb = pound, kg = kilogram, mph = miles per hour, km/h = kilometers per hour, ft-kips = foot-kilopounds, KJ = kilojoules

Table 2-3 provides impact penetration ratings. Note that P1, the penetration acceptable to DOS, is shaded.

Table 2-3: Impact Penetration Ratings

Designation	Dynamic Penetration Rating
P1	less or equal to 3.3 feet (1 meters)
P2	3.31 to 23.0 feet (1.01 to 7 meters)
P3	23.1 to 98.4 feet (7.01 to 30 meters)
P4	98 feet or greater (30 meters)

SOURCE: ASTM F 2656-07, TABLE 2

Together the impact condition ratings M30, M40, and M50 and the impact penetration rating P1 are equivalent to the previously designated K4, K8, and K12 standard cited in FEMA 430, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks* (2007), Section 4.2.2, for a 15,000-pound (6,804-kilogram) vehicle. Other impact conditions and impact penetration ratings may be applicable to other building owners and site conditions.

2.3.4.4 Barrier System Design Examples

There are two basic categories of barriers: passive (fixed) and active (operable).

Passive barriers are fixed in place, do not allow for vehicle entry, and are used to provide perimeter protection away from vehicle access points. Passive barriers include:

- Fixed bollards
- Engineered planters
- Heavy objects and trees
- Walls and ha-ha barriers
- Water obstacles
- Jersey barriers
- Fences

Active barriers are used at vehicular access control points within a perimeter barrier system or at the entry to specific buildings within a site, such as a parking structure or a parking garage within an occupied building to provide a barrier for vehicle screening or inspection; they can be operated to allow vehicle passage. Active barriers include:

- Retractable bollards
- Rising wedge systems
- Rotating wedge systems
- Drop arms crash beams
- Crash gates
- Surface-mounted wedges and plates

The following two tables summarize installation and design implications for the typical range of barrier types. Table 2-4 covers passive barriers and Table 2-5 covers active barriers.

Table 2-4: Passive Barriers

ID	Barrier Type	Descriptions, Installation, and Design Implications
P1	Fixed Bollards	A bollard is a vehicle barrier consisting of a cylinder usually made of steel and filled with concrete placed on end in a deep concrete footing in the ground to prevent vehicles from passing, but allowing the entrance of pedestrians and bicycles. Bollards can be specified with ornamental steel trim attached directly to the bollard or with selected cast sleeves of aluminum, iron, or bronze that slip over the crash tube.  *Custom bollard covers* SOURCE: DELTA SCIENTIFIC INC.  *A long line of bollards can appear as a wall.* **Installation:** The need for bollards to penetrate several feet into the ground may cause problems with underground utilities whose location may not be known with certainty (see figure below). If underground utilities make the installation of conventional bollard foundations too difficult, bollards with a wide shallow base and a system of beams below the pavement to provide resistance against overturning (see figure below) are a possible solution.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P1	Fixed Bollards (cont.)	

Installation of fixed bollard line (left)

SOURCE: SECUREUSA, INC.

Bollards on shallow beam system (right)

SOURCE: RSA PROTECTIVE TECHNOLOGIES

Design Implications:

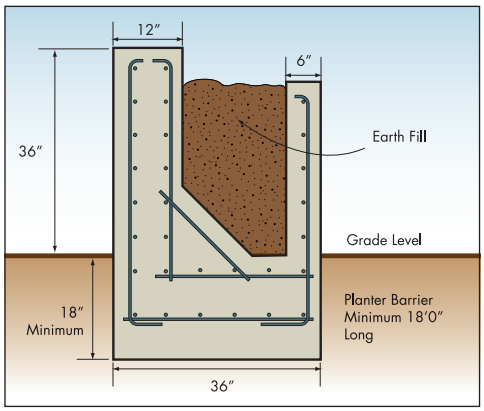
Bollards are by their nature an intrusion into the streetscape. A bollard system must be very thoughtfully designed, limited in extent, and well integrated into the perimeter security design and the streetscape to minimize visual impacts.

To reduce the visual impact, bollard height should typically not be more than 30 inches. However, this height may be ineffective for some vehicular threats; for example, some States allow the maximum height of a bumper to be 31 inches (0.8 meter) above grade. Site-specific conditions, such as road surface grade and curb height, may help improve the effectiveness of a bollard for impact, while making the bollard appear less obtrusive.

A bollard reduces the effective sidewalk width by the width of the curb to bollard (typically 24 inches [0.6 meter]) plus the width of the bollard. In high-pedestrian and narrow-sidewalk areas of a CBD, the reduction in effective sidewalk width can be problematic.

Other bollard system guidelines include the following:

- Bollard spacing should be between 36 and 48 inches (0.9 and 1.2 meters), depending on the kind of traffic expected and the needs of pedestrians and the handicapped.
- Where a long line of bollards is unavoidable, the bollards can be interspersed with trees and oversize bollards that can act as seats. In a few years, the trees will dominate the streetscape, and the barriers will be unobtrusive.
- Bollards should be kept clear of ADA access ramps and the corner quadrants at streets.
- Bollards should be arranged in a linear fashion in which the center of the bollards is parallel to the centerline of existing streets.
- Bollards may be custom designed for an individual project to harmonize with the materials and form of the building; but to provide adequate protection, they must be tested by an independent laboratory.
- Closely spaced bollards can also make the navigation to curb cuts particularly challenging for wheelchairs.
- In no case should bollards exceed a height of 38 inches (1 meter), inclusive of any decorative sleeve.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P1	Fixed Bollards (cont.)	 *A long line of bollards with trees interspersed (left). Custom bollards used in conjunction with a sloping wall barrier (right).*  *Corner installation of custom concrete bollards that match the building architecture*
P2	Engineered Planters	Well-designed planters can form an effective vehicle barrier. Planters located on the surface rely on friction to stop or delay a vehicle and will be pushed aside by any heavy or fast-moving vehicles; displaced planters may become dangerous projectiles. Engineered planters need considerable reinforcing and below-grade depth to be effective and become fixed elements in the landscape design. The planter shown provides a DOS K12 rating. 

Typical engineering detail of reinforced planter with DOS K12 performance
 
Planter with concealed crash-rated bollards
SOURCE: WAUSAU TILE |

ID	Barrier Type	Descriptions, Installation, and Design Implications
P2	Engineered Planters (cont.)	**Installation:** Some guidelines for planter system installation include the following: • Rectangular planters should be no more than 2 feet (0.6 meter) wide and 6 feet (1.8 meters) long, and circular planters should be no more than 3 feet (0.9 meter) in diameter. • A maximum distance of 4 feet (1.2 meters), depending on the kind of traffic anticipated, should be maintained between planters and other permanent streetscape elements. • Planters should not be used in high pedestrian traffic areas. • Planters should be oriented in a direction parallel to the curb or primary flow of pedestrian traffic. In no case should a planter or line of planters be placed perpendicular to the curb. • Landscaping within planters should be kept below 2.5 feet (0.8 meter) in height, except when special use requirements call for increased foliage. Depending on the threat, consideration should be given to ensuring that a 6-inch-high (15-centimeter-high) package could not be concealed in the foliage. **Design Implications:** Planters can have a major impact on pedestrian movement, reducing the effective sidewalk width. However, well-designed and placed planters can have multiple functions and be civic amenities.  *These planters are formed by the top of retaining walls (left). Alternating bollards and planted retaining walls as a barrier (right).*
P3	Heavy Objects and Trees	Heavy objects that can resist vehicular passage include sculptural objects, massive boulders, earthen berms or concrete forms with unassailable slopes, and dense planting and trees. Many heavy objects can be used in a similar way to bollards to prevent vehicles from passing, while allowing the passage of pedestrians and bicycles. To ensure that such barriers can effectively reduce the identified vulnerability, engineering design and/or evaluation is necessary.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P3	Heavy Objects and Trees (cont.)	

Groups of mature palm trees as protection from vehicular intrusion

SOURCE: PHOENIX POLICE DEPARTMENT, ARIZONA CENTER, ROUSE DEVELOPMENT CO.

Decorative obelisk at the approach to a Civic Plaza

SOURCE: PHOENIX, ARIZONA, POLICE DEPT., TODD WHITE

Boulders and custom bollards as barriers

SOURCE: EDAW DESIGN

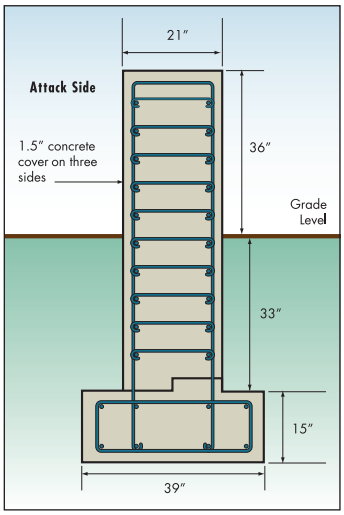
Installation:

Objects used as barriers need varying degrees of embedment and reinforcement, depending on their weight, footprint, and height/width ratio.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P3	Heavy Objects and Trees (cont.)	**Design Implications:** The use of natural features, such as rocks, or manmade objects, such as sculpture, provide opportunities for creating barriers that enhance the visual environment, effectively delineate pathways, clarify public and private space, and provide protection in an unobtrusive manner. Specially designed objects that also serve a practical and aesthetic purpose can be used as effective barriers. For example, existing dense thickets of mature trees can be incorporated into a perimeter system.  Landscape barriers on a courthouse plaza built on a parking garage roof. The design refers to the State's cultural and natural history: earth mound and logs. The earth mounds are almost impossible to drive over but if any vehicle surmounts it the mound will collapse into the void. The huge logs also limit the possibility of direct access but also provide pedestrian seating and lead them towards the main entry.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P3	Heavy Objects and Trees (cont.)	 SOURCE: COURTESY OF MARTHA SCHWARTZ, INC.  Originally designed for the Wall Street area of New York City, the NOGO barrier is visually attractive, useful to lean on, socialize around, or act as a lunch table. The NOGO is part barrier and part art object. While more expensive than bollards the barriers provide a lasting benefit to the street scene.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P4	Wall and Ha-ha's	The hardened (or engineered) wall group includes retaining walls and freestanding walls. These may be constructed of reinforced or mass concrete, concrete masonry, brick, and natural stone, or other materials typically reinforced with steel.



Typical reinforcing for a low-wall barrier

SOURCE: DOS

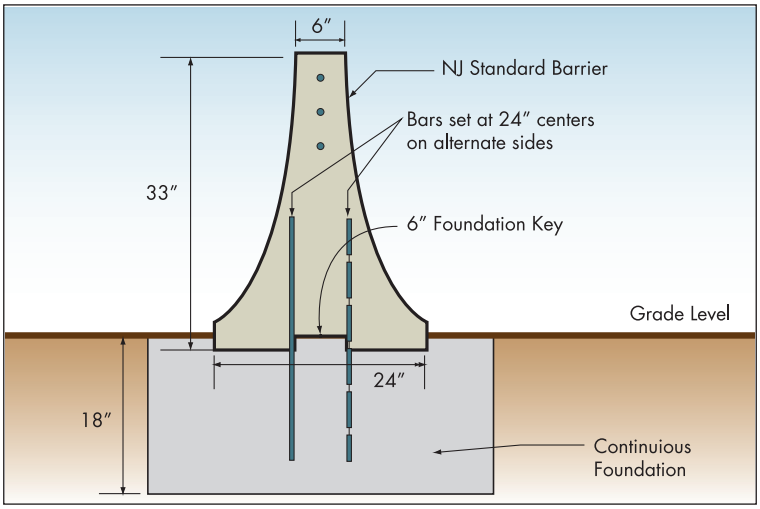
The ha-ha originated for aesthetic purposes in 17th-century England to prevent cattle from wandering up to a country mansion. The same strategy has been used in security barriers.

Ha-ha principle (left). Ha-ha and bollards (right). SOURCE: FEMA 430

Spaced engineered walls (left). Retaining walls on sloping site (right).

SOURCE: PHOENIX, ARIZONA, POLICE DEPT., TODD WHITE (LEFT)

ID	Barrier Type	Descriptions, Installation, and Design Implications
P4	Wall and Ha-ha's (cont.)	**Installation:** Although the mass alone of heavy masonry walls installed in a ha-ha design may provide an effective barrier, typical concrete walls require heavy reinforcing. **Design Implications:** Unless carefully placed and designed, barrier walls can be intrusive elements. A ha-ha is an effective way of providing a nonintrusive barrier. Walls and ha-ha's should be carefully studied in configuration, dimension, and materials in relation to the types of vehicles expected to be encountered. Spaced walls allow for pedestrian penetration. Retaining walls, if sufficiently high, can create an effective barrier and also be aesthetically pleasing.
P5	Water Obstacles	Water, in the form of the moat, around a medieval castle is one of the oldest methods of site security design. A modern example is of their use is around selected water "palaces" in Iraq. Artificial or natural lakes, ponds, rivers, and fountains can also be effective and beautiful choices for barriers. The configuration of a channel can be designed as an effective "tank trap," or the walls of the pool or mass of the fountain can be engineered to stop a vehicle. Water barriers can be designed in a variety of formations, flat and smooth or enhanced with movement by falls or fountains. Water features generally require ongoing maintenance with filters, pumps, and cleaning.   This proposed un-built design for the re-design of the Washington Monument grounds uses water to create a barrier. SOURCE: MICHAEL VAN VALKENBURGH AND ASSOCIATES

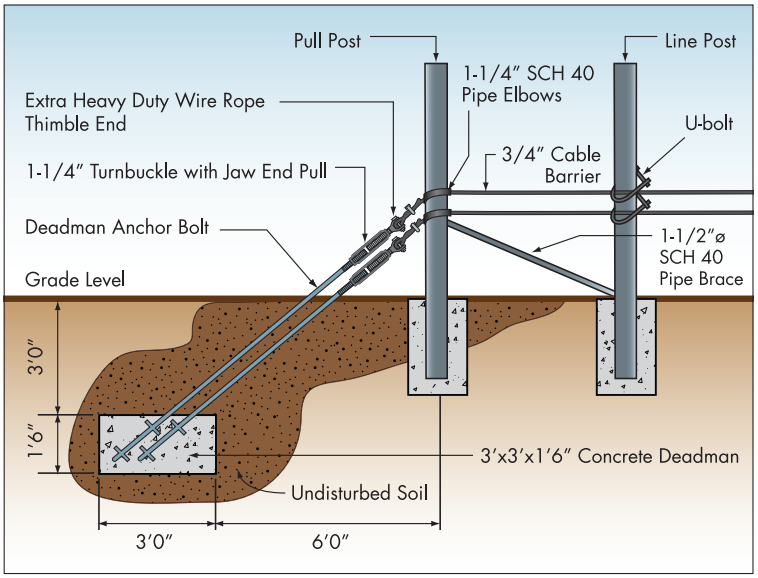
ID	Barrier Type	Descriptions, Installation, and Design Implications
P5	Water Obstacles (cont.)	 This steep flight of steps and water feature act as barriers. SOURCE: PETER WALKER AND PARTNERS
P6	Jersey Barrier	A Jersey barrier is a standardized precast concrete element originally developed in the 1940s and 1950s by New Jersey, California, and other States as a highway median barrier to prevent vehicle crossovers into oncoming traffic. The barrier came into wide use after 9/11 as an anti-ram and traffic control barrier against terrorist attack. Jersey barriers were originally thought to provide protection through their mass—a 12-foot (four-meter) barrier weighs approximately 5,700 pounds (2,586 kilograms)—but, when placed on the ground surface, they are ineffective against vehicular attack. To be effective, they need to be embedded and include vertical anchorage of steel reinforcing through the barrier into the pavement. The jersey barriers are not easily adaptable. They come in standard lengths of 12.5 and 20 feet (3.8 and 6 meters), making their use inflexible, and they must be carefully installed or they may create undesirable spaces where they overlap, narrowing sidewalks to non-navigable widths.  Embedded Jersey barrier as permanent installation SOURCE: *DOD HANDBOOK: SELECTION AND APPLICATION OF VEHICLE BARRIERS*,MIL-HDBK-1013/14,1999

ID	Barrier Type	Descriptions, Installation, and Design Implications
P6	Jersey Barrier (cont.)	**Installation:** When installed on a sidewalk, a Jersey barrier reduces the effective sidewalk width by 3.5 feet (1.1 meters), plus whatever distance it is placed from the curb. Some installations can be dangerous in the event of an emergency evacuation, particularly when several barriers are connected without breaks, because there is no easy way for pedestrians to move past them. **Design Implications:** Because they are relatively inexpensive and readily available, Jersey barriers have become ubiquitous in the protection of public buildings and monuments in Washington, New York, and elsewhere. However, their often awkward placement may degrade the beauty of the urban scene and disrupt access and movement for those on affected streets and sidewalks. Their most effective use is on a temporary basis.  Example of temporary applications of Jersey barriers that are inadequate for vehicle ram protection and severely impede pedestrian movement. SOURCE: FEMA 430
P7	Fences	Fences are a traditional choice for security barriers, primarily intended to discourage or delay intruders or serve as a barrier against standoff weapons (e.g., rocket-propelled grenades) or hand-thrown weapons (e.g., grenades, fire-bombs). Familiar fence types include: • Chain-link • Monumental fences (metal) • Anti-climb (CPTED) fence • Wire (barbed, barbed tape or concertina, triple-standard concertina, tangle-foot) These fence types are primarily intended to delay intrusion. They provide very little protection against vehicles, but they can act as a psychological deterrent when an aggressor is deciding which building to attack. Fencing can also incorporate various types of sensing devices that relay warning of an intruder to security personnel. Fences can be constructed as engineered anti-ram systems. An effective solution is to use cable restraints to stop the vehicle: these can be placed at bumper height within the fence and hidden in plantings.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P7	Fences (cont.)	

Crash-rated fence

SOURCE: AMERISTAR FENCE PRODUCTS INC.



Layout of cable fencing, used in conjunction with planting

SOURCE: *DOD HANDBOOK: SELECTION AND APPLICATION OF VEHICLE BARRIERS*, MIL-HDBK-1013/14, 1999

Installation:

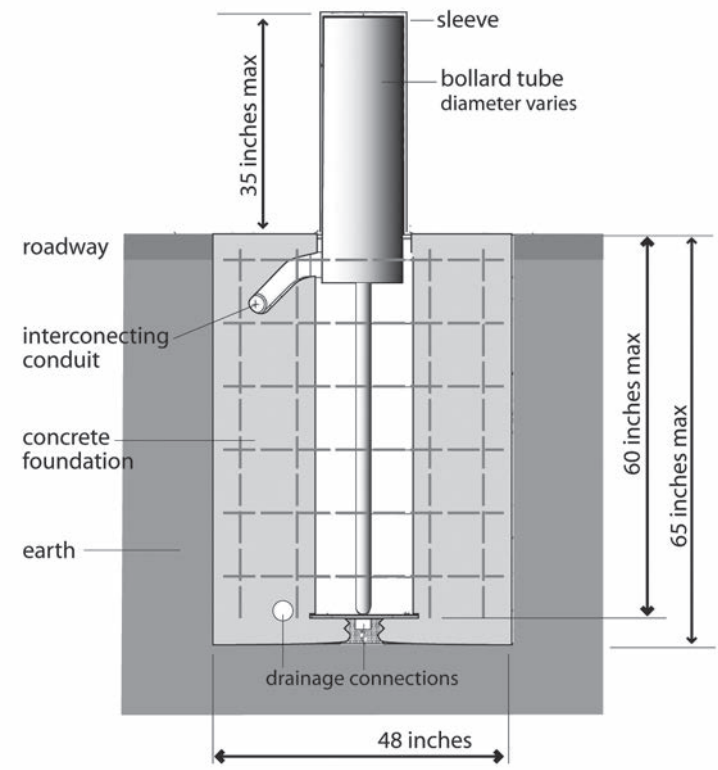
Cable system fences allow considerable deflection and partial penetration of the site before resistance occurs. The amount of deflection is based upon the distance between the concrete "dead men," typically about 200 feet. As a result, the installation requirements for fences and gates that incorporate a cable system differ slightly from other types of walls and fences.

ID	Barrier Type	Descriptions, Installation, and Design Implications
P7	Fences (cont.)	**Design Implications:** Fences for the protection of property have a long history and have also often been elements of great beauty. Modern fences are governed more by function and cost, but variations of historic fence design have been used as barriers for important historic building. The appearance of less attractive fencing can be improved by plantings.
P8	Reinforced Street Furniture and Fixtures	Common streetscape elements can be reinforced to serve as anti-ram barriers. These elements can be hardened so that they function both as amenities and components of perimeter security. This approach to protection has been limited because of the lack of tested and certified products. Security device manufacturers have found sufficient demand to justify development and testing of active and passive bollards and moving wedge-type devices, and have responded to design demands by providing decorative covers for bollards. An improvised example of hardened street furniture uses crash-rated bollards concealed between two benches (top figure). Some major building projects have been able to justify the expense of developing custom-designed engineered furniture (bottom figures), but bollards need to be supplemented with other reinforced streetscape components, such as lamp standards, bus shelters, and kiosks. Such components require testing to ensure acceptable performance. Their use also enhances the streetscape.  *Outdoor seating reinforced with hidden bollards* SOURCE: SECURE U.S.A, INC.

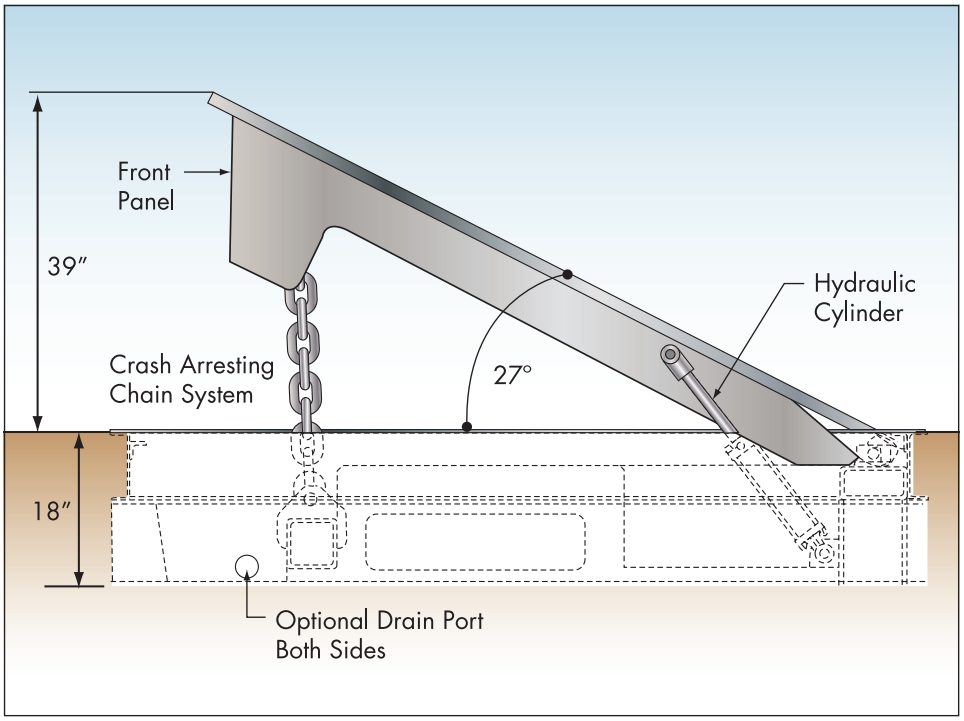
ID	Barrier Type	Descriptions, Installation, and Design Implications
P8	Reinforced Street Furniture and Fixtures (cont.)	 *Custom designed street furniture barriers*

Table 2-5: Active Barriers

ID	Barrier Type	Descriptions, Installation, and Design Implications
A1	Retractable Bollards	A retractable bollard system consists of one or more rising bollards operating independently or in groups of two or more units. The retractable bollard is a below-ground assembly consisting of a foundation structure and a heavy cylindrical bollard that can be raised or lowered by a buried hydraulic or pneumatic power unit, controlled remotely by a range of access control devices. Typical retractable bollards are 12 to 13 inches (30 to 33 centimeters) in diameter, up to 35 inches (0.9 meter) high, and are usually mounted 3 feet (0.9 meter) apart, depending on typical traffic. Retractable bollards are used in high-traffic entry and exit lanes where vehicle screening is necessary, at site entrances, and at entries such as parking garages and building services. Unlike rising or rotating wedge systems, the entry is freely accessible to pedestrians when the bollards are raised. Normal bollard operating time is field adjustable and ranges from 3.0 to 10.0 seconds. Emergency operating systems can raise bollards to the guard position from fully down in 1.5 seconds. **Installation:** Retractable bollards are expensive because they need broad and deep excavation for the bollards and operating mechanisms. Also, as with all active barriers, they require regular maintenance to ensure continued operation. **Design Implications:** Retractable bollards are relatively unobtrusive barriers that need only to be raised when screening is necessary. A retractable bollard system is generally accompanied by fixed bollards at the sides, and a secure control booth is necessary for security personnel.

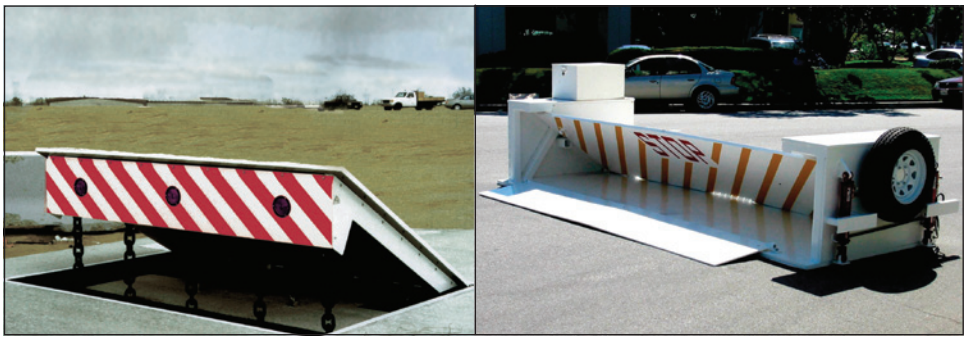
ID	Barrier Type	Descriptions, Installation, and Design Implications
A1	Retractable Bollards (cont.)	 *Retractable bollard installation, section* SOURCE: DELTA SCIENTIFIC CORP.  *Typical retractable bollard systems at a service entry; note fixed bollards at sides*

ID	Barrier Type	Descriptions, Installation, and Design Implications
A2	Rising Wedge System	Wedge systems, sometimes called rotating plate barriers, consist of a metal plate installed in a roadway that can be raised or lowered by an attendant usually located in a booth next to the metal plate, thus regulating vehicle access to the street in which it is installed. These barriers can be crash rated and can effectively stop vehicles. Wedge barriers can be surface mounted or mounted in a shallow excavation about 18 in deep. Shallow foundation systems are available to a DOS M50 P1 rating or DOS K12 rating. Raised heights are from about 21 to 38 inches (0.5 to 1 meter), and a standard width is 10 feet (3 meters).



Rising wedge barrier

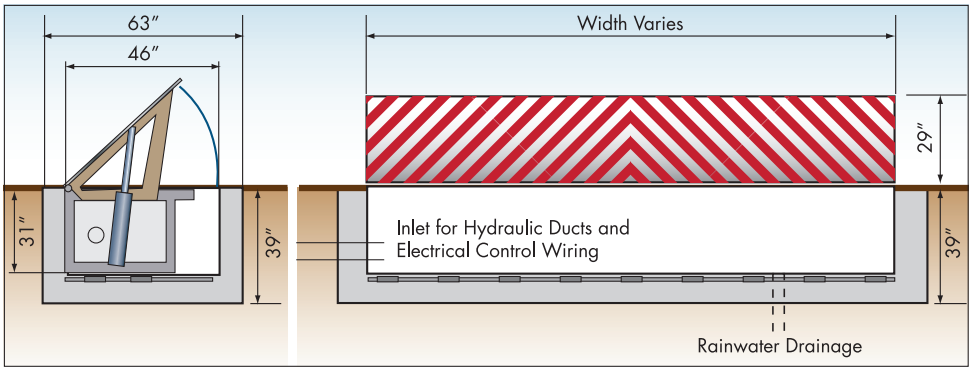
SOURCE: DELTA SCIENTIFIC CORP.



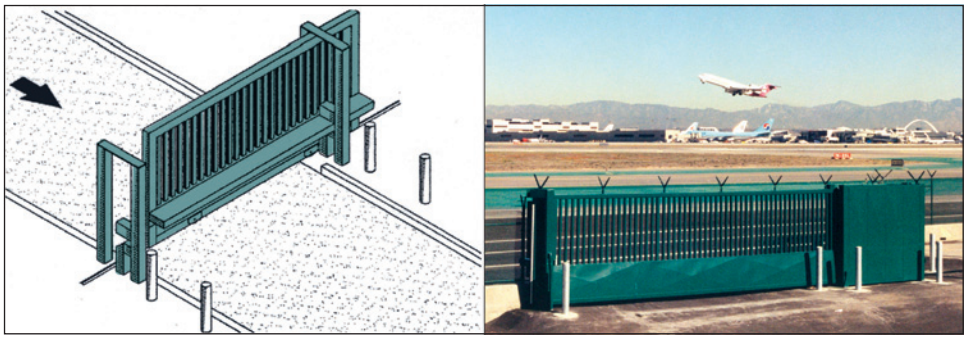
Rising wedge barrier

Mobile wedge barrier

SOURCE: DELTA SCIENTIFIC CORP.

ID	Barrier Type	Descriptions, Installation, and Design Implications
A2	Rising Wedge System (cont.)	**Installation:** Wedge barriers can be surface mounted or mounted in a shallow excavation, about 18 inches deep. In the latter installation, the barricade plate is flush with the road surface when retracted. The power unit can be configured to operate one or more barricades and can be operated by a range of optional remote control inputs. In surface-mounted installations, all components are mounted above grade; no cutting or excavation is required on good concrete surfaces. Mobile wedge barriers that can be moved into position by a medium-sized pickup truck in 15 minutes are also available. These can form an effective element of a planned temporary barrier system to respond to a heightened threat. **Design Implications:** Rising wedge barriers are one of the earliest active barrier systems to be developed. They are somewhat utilitarian in appearance when compared to retractable bollards or rotating wedge systems. These barriers effectively restrict vehicular access but care must be taken to ensure that limitations for the passage of bicycles, cars, and emergency vehicles are maintained. Like all active barriers, these barriers must be a tended at all times.
A3	Rotating Wedge Systems	Rotating wedge systems are similar in action to the rising wedge barrier discussed in A2 but have a curved front face, providing a better appearance, and are embedded to a greater depth. The height of the obstacle is between 24 and 28 inches (0.6 and 0.7 meter) and a standard width is 10 feet (3 meters). The obstacle is operated hydraulically by heavy duty rams. Operating time is about 3 seconds per movement.  *Typical rotating wedge barrier dimensions and installation requirements* SOURCE: DELTA SCIENTIFIC CORP.  *Rotating wedge*

ID	Barrier Type	Descriptions, Installation, and Design Implications
A3	Rotating Wedge Systems (cont.)	**Installation:** The pit to receive the system is approximately 5 feet (1.5 meters) wide, 40 inches (1 meter) deep, and about 6 inches (15 centimeters) wider than the width of the obstacle. The hydraulic mechanism can be located up to 50 feet (15 meters) away from the barrier. **Design Implications** Appearance depends on the layout and design of any accompanying fixed barriers and control booths, the design of operating buttresses, and the color and pattern of the barrier.
A4	Drop-Arm Crash Beams	Drop-arm crash beams are a greatly strengthened version of barriers familiar at parking garage entries and the like. A crash barrier assembly consists of a steel crash beam, support, and pivot assembly; cast-in-place concrete buttress; and locking and anchoring mechanisms. In addition, crash-rated beams incorporate a high-strength steel cable, which is attached to both buttresses when the arm is in a down position. Clear opening range is from 10 to 24 feet (3 to 7 meters). The arm is raised and lowered using a hydraulic or pneumatic system, or manually with a counter-balanced arm. While their performance is typically less effective than other active systems, drop-arm barriers can be obtained with a certified DOS M50 P1 or DOS K12 performance rating.  *Drop-arm crash beam*

ID	Barrier Type	Descriptions, Installation, and Design Implications
A5	Crash Gates	Some crash-rated gates operate without contact with the ground, while others use a rack-and-pinion drive across a V-groove. Swing versions are also available. The clear opening range is from 12 to 30 feet (4 to 9 meters). Typical heights are 7 to 9 feet (2 to 3 meters). Crash ratings up to DOS M50 P1 or DOS K12 rating can be obtained.  *Typical crash gate installation* SOURCE: DELTA SCIENTIFIC CORP.
A6	Surface-Mounted Rotating Plates	Surface-mounted wedges and plates are modular bolt-down barrier systems in which all components are mounted above grade, and no cutting or excavation is needed on most concrete surfaces. The moving plate or wedge is raised and lowered by a hydraulic, pneumatic, or electromechanical drive. A typical unit incorporates a single buttress with a ramp width of 10 feet (3 meters) and a raised height of 21 to 28 inches (0.5 to 0.7 meter). Dual buttress systems have a width of about 18 feet (5.5 meters). These systems can be installed quickly and removed easily. Some systems incorporate a drop arm and traffic lights for additional safety. Typical cycle time is 3 to 4 seconds with a 1.5-second emergency cycle. High-performance systems are capable of a DOS K4 or M30 P1 rating.  *Single buttress* *Dual buttress* SOURCE: SECURE U.S.A, INC.

2.4 Site Security Design Guidelines

2.4.1 Parking

Parking must be designed to accommodate both pedestrians and vehicles safely and efficiently in keeping with the overall security design strategy. Five characteristic methods are used to provide parking spaces for staff, visitors, residents, and others:

- Surface parking lots
- Free-standing parking structures
- Public on-street parking lanes
- Parking underground and underneath buildings

Parking on open sites is typically accommodated by surface parking lots and/or parking structures. Parking within buildings or in underground parking structures is common in the CBD. On-street parking lanes may occur on any site but are particularly characteristic of urban areas.

2.4.1.1 Surface Parking Lots

All parking in an open site should be located outside the standoff zone for high-risk buildings. Access control may be necessary at the entry to parking in nonexclusive zones for regulation and fee collection. If the site has a perimeter barrier, authorization to enter the site and any necessary inspection can take place at entry control points.

All parking in an open site should be located outside the standoff zone for high-risk buildings.

Warning signs should be easy to understand and placed along the physical barriers and at each entry.

Warning signs should be easy to understand and placed along the physical barriers and at each entry. An important design goal is to develop an efficient layout of parking spaces and provide an internal circulation that has clear paths for pedestrians and vehicles. Parking restrictions can help to keep potential threats away from a building. Operational measures may also be necessary to inspect or screen vehicles entering parking areas.

The following considerations may help designers to implement sound parking measures for high-risk buildings:

- Only inspected vehicles should be allowed to approach or park within the standoff zones.

- Parking areas should be at an appropriate setback (standoff) from to the protected building. Structural hardening may be required if the setback is insufficient. In new buildings, adjusting the location of the building on the site may be possible to provide adequate setback from adjacent properties.
- Where possible, unexpected visitor or general public parking should be outside the standoff zone.
- Locate vehicle parking away from high-risk buildings to minimize collateral blast effects from potential VBIEDs.
- Locate general parking in areas that present the fewest security risks to personnel.
- Where possible, parking lots should have one-way circulation to facilitate monitoring for potential aggressors.
- Possible fragmentation of the axles and engine block as a result of an explosion requires that parking be oriented so that the front or rear of the vehicle is not pointed toward a nearby building or guardhouse.
- Parking should be within view of occupied buildings. Plantings around parking structures and parking lots should permit observation of pedestrians, while at the same time reducing the visual impact of automobiles.
- Uninspected vehicles should not be allowed to park within the exclusive zone or in the second layer of defense.
- Where parking within the building is required, restrictions should apply.
- Whenever possible, parking beneath or within a building should be avoided.
- Parking between individual buildings, especially when the buildings are relatively close together, should be restricted because of the danger of reflected blast pressures.
- Emergency communication systems (e.g., intercom, telephones, call boxes) should be mounted at readily identified, well-lighted, CCTV-monitored locations to permit direct contact with security personnel.
- Parking lots should be equipped with CCTV cameras connected to the security system and adequate lighting to ensure lot activity is visible to security personnel and recorded.

2.4.1.2 Free-Standing Parking Structures

Free-standing parking structures refer to standalone, aboveground parking garages. The garage could be adjacent or nearby to the building. Considerations for free standing parking structures include the following:

- Parking should be restricted to flat surfaces.
- Dead-end parking areas and any possible places for concealment should be avoided.
- Pedestrian access and pathways should be separate from vehicle circulation.
- Parking structures should provide sufficient visibility for surveillance into, out of, and across the garage.
- Parking structures open to the public should be designed with consideration of standoff from other buildings and screening to protect critical operations and sensitive areas that might be observed from within the parking structure, which can be used as a point of access or staging for use of weapons or explosives.

2.4.1.3 Public Street Parking

Public street parking is often located within a desired standoff zone. Evaluation of this option must consider the role of the street within the local infrastructure, whether the municipality must be reimbursed for loss of metered parking income, and whether an additional lane provides significant improvement of the standoff distance.

If street parking lanes are unacceptable because of the high risk, access to the vulnerable streets and parking may have to be prohibited to create an adequate standoff zone. This approach has been adopted in the New York City Financial District. Street closure has serious implications for everyday function and accessibility, and should only be undertaken if no other solution, such as building hardening, is feasible.

Considerations for public street parking include the following:

- In densely populated areas, parking in curb lanes may be restricted to company-owned vehicles or key employee vehicles.
- Appropriate setback from parking on adjacent properties is recommended, and if insufficient, structural hardening may be required.
- Pickup and dropoff areas should have appropriate barriers at the edge of the curb to enforce standoff distances for unscreened vehicles.
- Circulation plans should ensure that effective access is available for first responders and emergency vehicles.

2.4.1.4 Parking Underground and Beneath Buildings

The risk of collateral damage to buildings adjacent to underground parking must be evaluated to determine the level of inspection and access control required at the garage entry. Typically, this would be limited to fee taking and cursory inspection, but for high-risk buildings or in cases of heightened security careful inspection may be necessary on a temporary basis.

The protection of primary vertical load-carrying members of the building by barriers that can keep an explosive as far away as possible makes a big difference. Simple structures around accessible portions of columns may be sufficient to prevent a column failure. Typical entry control to protect underground parking beneath high-risk buildings is shown in Figure 2-28. Note the provision for queuing and the gatehouse design in harmony with the building architecture.

The risk of collateral damage to buildings adjacent to underground parking must be evaluated to determine the level of inspection and access control required at the garage entry.

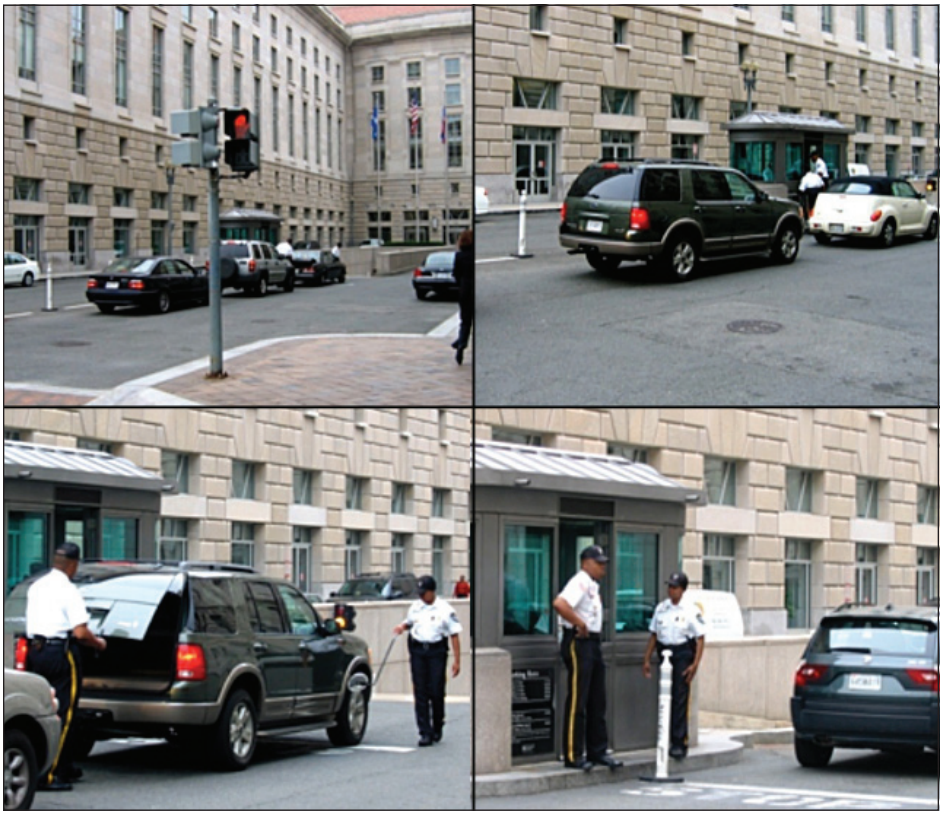


Figure 2-28: Entry control to underground garage

Where parking beneath a building must be provided, access to the parking area should be controlled and spaces should be well lighted, free of places for concealment, and free of dead-end parking spaces. The following use restrictions may need to be applied:

- Public parking allowed, but only with ID check
- Parking for company vehicles and employees of the building only
- Parking for selected company employees, or only those at higher risk

In addition to previously mentioned design considerations for parking structures, underground parking and parking beneath buildings require the following additional considerations:

- Pedestrian paths should be designed to concentrate activity to the extent possible. For example, directing all pedestrians through one portal rather than allowing them to disperse to numerous access points improves their ability to see and be seen by other users. Limiting vehicular entry/exits to a minimum number of locations is also beneficial.
- Access to crawl spaces, utility tunnels, and other means of under building access should be controlled to limit opportunities for aggressors to place explosives underneath buildings.
- Screening or inspection at parking structures should be located outside, at adequate standoff distances, to control impact from explosions. Adequate space should be provided for queuing and inspection, so as not to slow traffic in and out of the garage (Figure 2-29).

Figure 2-29:
Queuing and inspection outside an entry to parking beneath a building

2.4.2 Loading Docks and Service Areas

Loading docks and service areas are commonly kept as unobtrusive as possible, but special entry controls may be required (i.e., a screening area or gated entry way). Significant structural damage to the walls and ceiling of the loading dock may be tolerable as long as the areas adjacent to the loading dock do not experience severe structural damage or collapse. Adequate structural design (robust and redundant load paths) can limit damage to the loading dock area and allow explosive forces to vent to the building exterior.

Design guidelines for loading docks and service access include the following:

- Provide an inspection area for screening, either offsite or a significant distance away from the loading dock, before permitting entrance to the loading dock.
- Locate loading docks and shipping and receiving areas away from utility rooms, utility mains, and service entrances, including electrical, telephone/data, fire detection/alarm systems, fire-suppression water mains, cooling and heating mains, and others.
- Avoid the placement of driveways within or under buildings.
- Consider whether areas below the loading dock are occupied or contain critical utilities in determining whether to design the loading dock for blast resistance.
- Provide signage to clearly mark separate entrances for deliveries.

2.4.3 Physical Security Lighting

Security lighting should be provided throughout the site, with special emphasis on building and perimeter illumination. Lighting may provide both a real and psychological deterrent for continuous or periodic observation by an aggressor. Lighting is relatively inexpensive to maintain and may decrease the need for security personnel by reducing opportunities for surreptitious approach by potential attackers.

Lighting is particularly desirable for sensitive areas of a site, such as pier and dock areas, secured buildings, storage areas, and vulnerable control points in communications, power, and water distribution systems. It facilitates detection of unauthorized personnel and makes the job of an attacker more difficult. Lighting must be compatible with CCTV systems, as the cameras may need high intensity, low intensity, or infrared light for proper operation.

At entry control points, a minimum surface lighting average of 4 horizontal foot-candles will help ensure adequate lighting for pedestrians, islands, and guards in approach and exit zones. However, this level is inadequate in control zones where IDs will be checked. The guardhouse and check positions should have a minimum of 10 foot-candles, with 20 foot-candles preferred. Thus, lighting intensity should increase as the control point is approached.

At entry control points, a minimum surface lighting average of 4 horizontal foot-candles will help ensure adequate lighting for pedestrians, islands, and guards in approach and exit zones.

Where practical, high-mast lighting is recommended, because it gives a broader, more natural light distribution, requires fewer poles and is more aesthetically pleasing than standard lighting. Lighting of the entry control point should give drivers a clear view of the gatehouse and, for security personnel, a clear view of vehicles in the area.

The type of site lighting system used depends on the overall requirements of the site and the building. Four types of lighting are used for security lighting systems.

- **Continuous lighting** is the most common security lighting system. It consists of a series of fixed lights arranged to flood a given area continuously during darkness with overlapping cones of light. Two primary methods of using continuous lighting are glare projection and controlled lighting:
  - The glare projection security lighting method lights a controlled area with high-intensity lighting. It is a strong deterrent to a potential intruder because it makes him or her very visible, while making it difficult to see inside the secure area. Guards are protected by being kept in comparative darkness, but are able to observe intruders at a considerable distance. This method should not be used when the glare of lights directed across the surrounding territory could annoy or interfere with adjacent operations.
  - Controlled lighting is best when the lighted area outside the perimeter is limited, such as along highways. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit a particular need. This method of lighting may illuminate or silhouette security personnel.
- **Standby lighting** has a layout similar to continuous lighting; however, the lights are not continuously lit, but are either automatically or manually turned on when suspicious activity is detected or suspected by security personnel or alarm systems.

- **Movable lighting** consists of manually operated, movable searchlights that may be lit during hours of darkness or as needed. The system normally is used to supplement continuous or standby lighting. Movable lighting is also used to assist in vehicle inspection in temporary and permanent vehicle inspection areas.
- **Emergency lighting** is a backup power system of lighting that may duplicate any or all of the above systems. Its use is limited to times of power failure or other emergencies that render the normal system inoperative. It depends on an alternative power source, such as installed or portable generators or batteries. Emergency backup power for security lighting should be considered.

Site lighting can be separated into zones to concentrate light where it is most needed. Prioritization will allow for the most efficient use of lighting, while keeping within a reasonable budget. Figure 2-30 shows some typical zones; the numbers on the figure refer to the descriptions below.

1. Exterior surface of building, including walls, doors, windows, rooftop terraces, and balconies.
2. Outdoor areas directly associated with entryways to building, including walkways, steps, ramps, terraces, and loading docks.
3. Intermediate outdoor areas, including driveways and parking; walkways and paved terraces; small gardens and large, remote landscaped areas; recreational facilities; and utility, service, and storage areas.
4. Areas immediately inside the perimeter, including inside faces of walls and required clearances, pedestrian entryways, vehicular entryways, and security check points.
5. Areas outside the perimeter that may be considered defensible space, including public sidewalks and streets, waterways, and adjacent nonpublic properties.

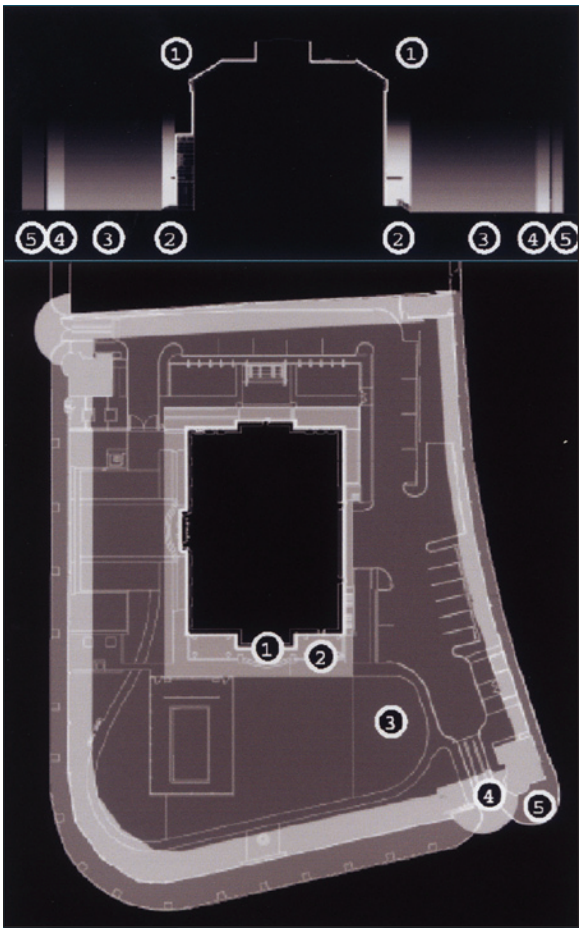


Figure 2-30: Site lighting zones

SOURCE: DOS

Operational costs, such as LCCs for energy and maintenance, should be considered when designing an appropriate lighting situation, because of their effect on project sustainability.

In addition, site lighting can be helpful as a response to different levels of alert, by designing it to be increased in times of high security alert. Provision of additional light is a common CPTED technique to discourage unwanted activities on sites and within buildings and to enhance desirable activities.

2.4.4 Signage

Signs for vehicular and pedestrian circulation are an important element of security. Signs can clarify entries and routes for pedestrians, staff, visitors, deliveries, and service, each with differing functional objectives and security requirements. Signage can be designed to keep intruders out of restricted areas, but inadequate signage can create confusion and defeat its primary purpose. Confusion over site circulation, parking, and entrance locations can contribute to the reduction of site security. Unless required, signs should not identify sensitive areas. Signs should be provided offsite and at entrances.

A comprehensive signage plan should include the following:

- Signs for each entry control point
- Signs that explain current entry procedures for drivers and pedestrians
- Traffic regulatory and directional signs that control traffic flow and direct vehicles to specific appropriate points
- Street addresses or building numbers instead of detailed descriptive information inside the site
- Minimization of the number of signs identifying high-risk buildings; however, a significant number of warning signs to ensure that possible intruders are aware of entry into restricted areas
- Minimization of signs identifying critical utility complexes (e.g., power plants, water treatment plants); clearly worded signs to minimize accidental entry by unauthorized persons into critical asset areas
- Both (or more) languages in areas where two or more languages are commonly spoken
- Posting at intervals of no more than 100 feet (30 meters) and not on fences equipped with intrusion-detection equipment
- Posting at all entrances to limited, controlled, and exclusive areas
- Posting of variable message signs that give information on special events and visitors far inside site perimeters and not readily observable from outside the perimeter

2.4.5 In-ground Site Utilities

In-ground infrastructure includes any system that can be used by persons to gain access to the building, such as subway tunnels, stations, utility corridors, large sewer or water tunnels, and large pipes.

Failure of part of the in-ground infrastructure may affect the structural integrity of the building. When the infrastructure and the building are in close proximity or rigidly linked, the failure of one system may initiate the failure of others. The parts of the structure closest to the in-ground infrastructure are the most vulnerable. They should be hardened so that any local failure would not initiate progressive collapse in the rest of the building. Aside from hardening, other measures available are increased setback and rigorous access control.

2.4.5.1 Utility System Protective Measures

Utility systems can suffer significant damage when subjected to the shock of an explosion. Some utilities may be critical for evacuation of people from the building. Destruction of these utilities could cause additional damage disproportionate to the damage resulting from an explosion. To minimize the possibility of such hazards, the following measures should be employed:

- Wherever possible, utilities should be underground, concealed, and protected.
- Redundant utility systems should be placed along separated paths or rights-of-way to support site security, life safety, and rescue functions.
- If redundant sources are not available, quick connects for portable utility backup systems, such as emergency generators should be provided.
- The vulnerability of all utility services, including all utility lines, storm sewers, gas transmission lines, electricity transmission lines, and other utilities that may cross the site perimeter, should be assessed.
- Water treatment plants and storage tanks should be protected from waterborne contaminants by securing access points, such as manholes. Maintain routine water testing to help detect waterborne contaminants.
- Petroleum, oil, and lubricant storage tanks and operations buildings should be located down slope at least 100 feet (30 meters) from all other buildings, with fuel tanks at an elevation lower than operational buildings or utility plants.

Utility systems can suffer significant damage when subjected to the shock of an explosion.

- The main fuel storage should be away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals).
- Multiple communications networks, instead of centralized networks, should be used to strengthen the communications system's ability to withstand the effects of a terrorist attack. Careful consideration should be made in locating, concealing, and protecting key network resources such as network control centers.
- Trash receptacles should be as far away from the building as possible, subject to convenience of use, as they are easy locations for the deposit of explosives.
- Low-impact development practices should be considered to enhance security, such as retaining stormwater onsite in a pond to create standoff, instead of sending it into the sewer system.
- GSA recommends that critical utilities and services be located at least 50 feet (15 meters) from loading docks, front entrances, and parking areas. (See GSA Public Building Standard 2010 P100 for further recommendations on the location of critical components.)
- Where redundant utilities are required in accordance with other requirements or criteria, they should not be collocated or placed in the same chases (a trench or shaft to run power, water, data, and other services to the building). This minimizes the possibility that both sets of utilities will be adversely affected by a single event.
- Where emergency backup systems are required, they should be located away from the system components for which they provide backup.

2.4.5.2 Protective Measures for Utility Penetrations

All utility penetrations of a site's perimeter barrier, including penetrations in fences, walls, or other perimeter structures, should be sealed or secured to eliminate openings large enough to pass intruders. Typical penetrations could be for storm sewers, water, electricity, or other site utility services. Specific requirements of various openings are discussed below:

- All utility penetrations of the site's perimeter should be screened, sealed, or secured to prevent their use as access points for unauthorized entry into the site. When access is required for maintenance of utilities, all penetrations should be secured with screening, grating, latticework, or other similar devices so that openings do not allow intruder access. Intrusion detection sensors and visual surveillance systems should be used if warranted by the sensitivity of assets requiring protection.

- Drainage ditches, culverts, vents, ducts, and other openings with a cross-sectional area greater than approximately 96 square inches (0.1 square meter) and with a smallest dimension greater than 6 inches (15 centimeters) should be protected by securely fastened welded bar grilles. As an alternative, drainage structures may be constructed of multiple pipes, with each pipe having a diameter of 10 inches (25 centimeters) or less. Multiple pipes of this diameter may also be placed and secured in the inflow end of a drainage culvert to prevent intrusion into the area. Any addition of grills or pipes to culverts or other drainage structures should be coordinated with the engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.
- Manhole covers 10 inches (25 centimeters) or more in diameter should be secured to prevent unauthorized opening. Covers may be secured with corrosion resistant locks and hasps, or bolted to their frames. Keyed bolts (which make removal by unauthorized personnel more difficult) are also available. When very high security is required, manhole covers that resist shattering after being artificially "frozen" by an aggressor should be considered.

2.4.6 Landscaping

Selection of appropriate plant materials for security is an important task. Security plantings often suffer from harsh environmental conditions, such as limited watering, undersized planting areas and beds, compacted soils, and runoff of chemicals from roads and sidewalks. These conditions are not conducive to healthy plants.

Following are some considerations for security planting:

- When a living landscape is installed with a security function, it needs to be well maintained to support its continued health and effectiveness.
- Planting can be effectively used to soften and enhance the sometimes stark appearance of barrier walls, planters, and other security elements (Figure 2-31).
- Existing plant materials onsite may be retained or new plantings established in accordance with the condition of the materials, the design intent for the project, and the extent of construction.
- Planting can be used as a perimeter barrier in the form of thorny hedges and dense hedgerows though security specialists usually prefer permanent structural solutions.
- Conflicts may occur between planting areas and underground utilities. Underground conditions should be accurately identified before landscape design is begun.

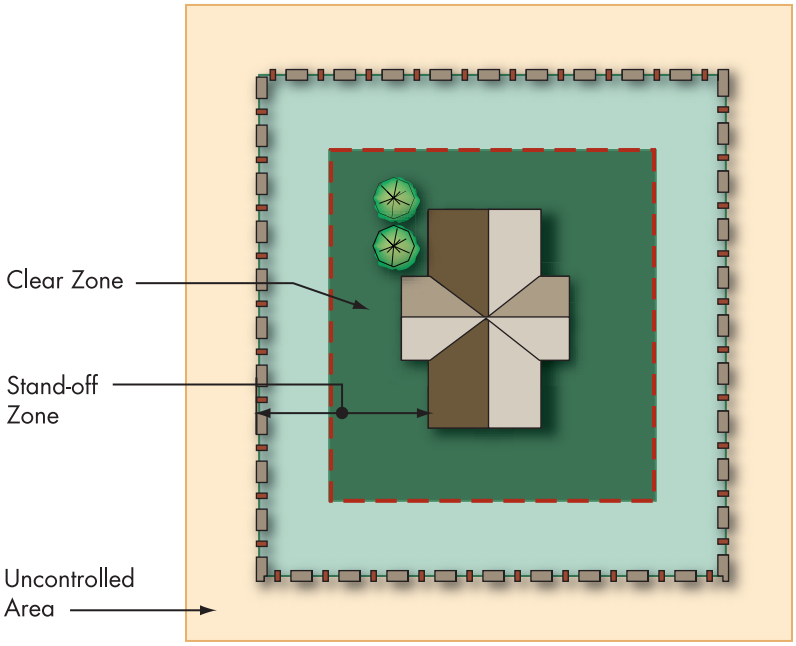
Figure 2-31:
Use of planting to soften and enhance the appearance of walls and other security elements at the Seattle Courthouse

SOURCE: PETER WALKER AND PARTNERS

For some high-risk facilities, providing additional protection immediately adjacent to the structure by creating a clear zone that is free of all visual obstructions or landscaping that might hide packages (Figure 2-32) may be necessary. Here, very low or high planting may be permissible, so long as one is not able to hide in it a package 6 or more inches (15 or more centimeters) thick.

Figure 2-32:
Clear zone with unobstructed views

SOURCE: U.S. AIR FORCE INSTALLATION ENTRY CONTROL FACILITIES DESIGN GUIDE



The clear zone facilitates monitoring of the immediate vicinity and visual detection of intruders. Walkways and other circulation features within a clear zone should be located so that buildings do not block views of pedestrians and vehicles. If clear zones are implemented, implementing additional anti-surveillance and security measures may be necessary.

The clear zone facilitates monitoring of the immediate vicinity and visual detection of intruders.

2.4.7 Chemical, Biological, and Radiological Site Considerations

Standoff is a principal site and layout consideration for CBR attacks, as it is for blasts. The standoff provided by a secure perimeter may be an effective measure for reducing vulnerability to a ground level release of hazmat. However, its effectiveness is greatly affected by wind direction and speed, air intake location, and location of the hazmat.

2.4.7.1 Prevailing Wind Direction

The site should provide the largest available standoff distance on the side of the prevailing wind. All intakes should be elevated, even those serving basement mechanical rooms. Locating intakes on the side of the building opposite the prevailing wind increases the effective standoff distance of the intake, further diluting the plume, whose source is the direction of the prevailing wind. hazmat from a ground-level source are more likely to be drawn into a building's mechanical ventilation system if intakes are at or below grade. As illustrated by the Granville, SC, train accident, described in Chapter 4, Section 4.3.4, gases that are heavier than air flow downhill when released in calm, stable conditions.

The site should provide the largest available standoff distance on the side of the prevailing wind.

2.4.7.2 Known Potential Sources

The likelihood of a hazmat incident increases if a building site is near a chemical plant/storage facility, rail line, major highway, or shipping waterway on which hazmat are routinely shipped, especially if the prevailing winds come from the direction of these potential sources. The distance to the potential sources also affects the probability of a hazardous incident affecting the building. Information on potential sources can be obtained from the LEPC which can also assist in determining the distance that can be considered safe from the potential sources. Iconic buildings or monuments and Federal facilities can also be considered among the potential sources in that they have in increased threat of a terrorist attack. The peripheral/downwind hazard of such an attack should be among the site considerations. Entry and exit points should also be considered in relation to the vulnerability of the site to CBR attack.

2.4.7.3 Visitor Screening

For access-controlled buildings that have entry screening, the vulnerability to an internal CBR release or bomb detonation can be reduced by placing the screening and visitor processing operations in a separate building at the secure perimeter. This building houses the magnetometer, x-ray, and other screening equipment, as well as badging and security personnel. Placing these operations outside the main building envelope eliminates the possibility of an internal attack occurring during or prior to the security screening. Visitors cannot enter until they have been checked to ensure they possess no toxic materials, explosive devices, or weapons.

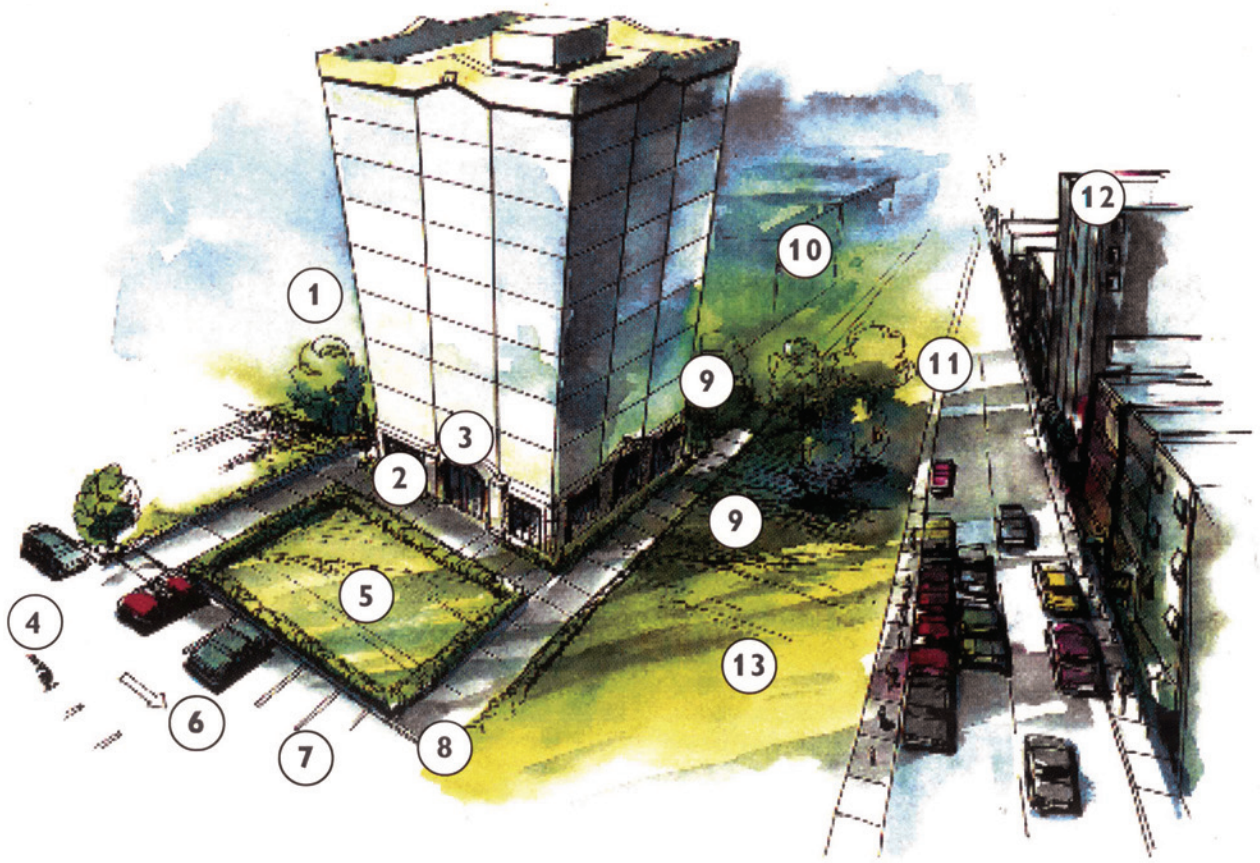
2.4.7.4 Site Exits

Evacuation, the most common response to a hazmat emergency, can be impeded if exit points from the secure perimeter are limited. Though a building will have multiple exits to facilitate rapid evacuation, secure perimeters often have only one. The secure perimeter should have a minimum of two exits through which rapid evacuation from the site is possible in the event of a hazmat release.

2.5 Summary of Site Protection Measures

A general spectrum of site mitigation measures ranging from ones that offer the least protection, at the least cost and least effort, to ones that offer the greatest protection, at the greatest cost, and greatest effort, is presented below. This is a nominal ranking of mitigation measures. In practice, the effectiveness and cost of individual mitigation measures may be different for specific applications.

Figure 2-33 is a graphic summary of site mitigation measures to protect building occupants.



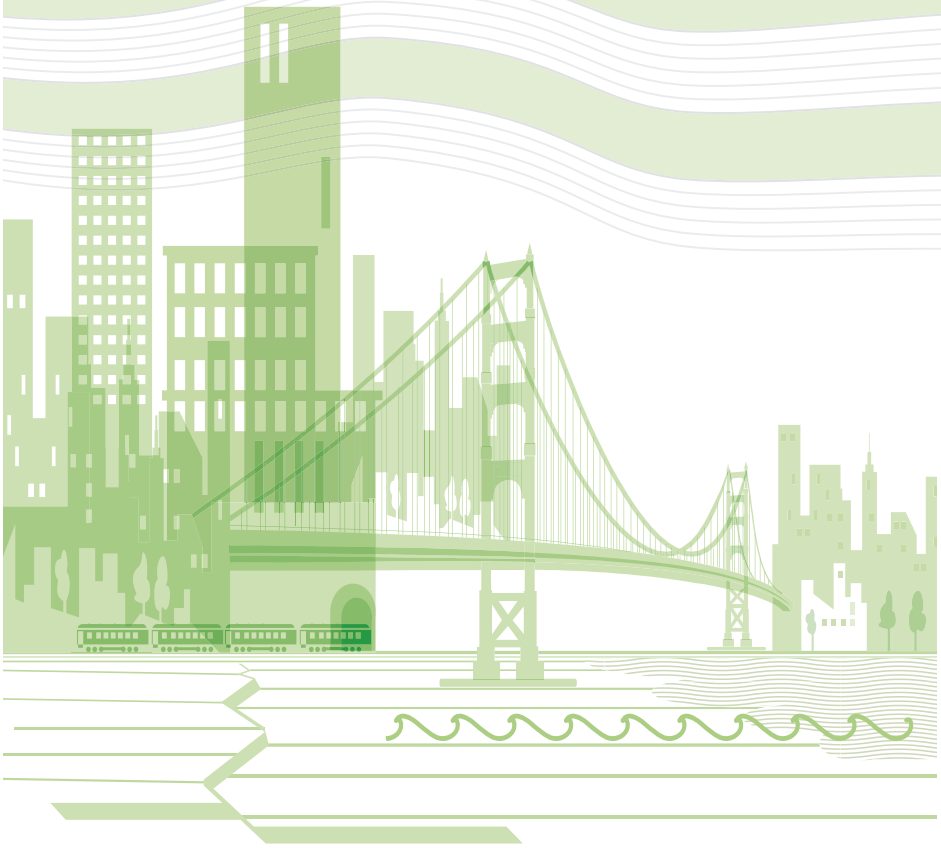
1. Locate assets stored on site, but outside the building within view of occupied rooms in the facility.	8. Minimize vehicle access points.
2. Eliminate parking beneath buildings.	9. Eliminate potential hiding places near the building; provide an unobstructed view around building.
3. Minimize exterior signage or other indications of asset locations.	10. Site building within view of other occupied buildings on the site.
4. Locate trash receptacles as far from the building as possible.	11. Maximize distance from the building to the site boundary.
5. Eliminate lines of approach perpendicular to the building.	12. Locate building away from natural or manmade vantage points.
6. Locate parking to obtain stand-off distance from the building.	13. Secure access to power/heat plants, gas mains, water supplies, and electrical service.
7. Illuminate building exteriors or sites where exposed assets are located.	

Figure 2-33: Site mitigation measures

SOURCE: U.S. AIR FORCE, *INSTALLATION FORCE PROTECTION GUIDE*

3

Protection of Buildings From Explosive Blast



In this chapter:

This chapter discusses the nature of explosive blasts, their effects on buildings and occupants, and the concept of levels of protection. Specific vulnerabilities and protective design and construction measures are reviewed for each category of building elements and systems. Chapter 2 discusses blast design concerns and protective measures for areas surrounding buildings.

3.1 Introduction

Historically, explosive blast attacks have been a favorite tactic of terrorists and will likely continue to be into the future for a variety of reasons. Ingredients for IED and homemade bombs can be easily obtained on the open market, as can the techniques for making bombs. Also, attacks with explosives are easy and quick to execute. VBIEDs bring large quantities of explosives to the doorstep of the target undetected. Finally, terrorists and criminals often attempt to use the dramatic impact of explosions, in terms of the sheer destruction they cause, to generate media coverage in hopes of transmitting their political message to the public.

Terrorists and criminals often attempt to use the dramatic impact of explosions, in terms of the sheer destruction they cause, to generate media coverage in hopes of transmitting their political message to the public.

The DOD, GSA, DOS, and DHS have considerable experience with blast effects and blast mitigation. In the past decade, a number of architects, engineers, security, and building designers have developed the understanding and expertise to conduct blast analyses. Also, new construction methods and materials have been developed that can mitigate many of the explosive risks.

This chapter discusses the nature of explosive blasts, their effects on buildings and occupants, and the concept of levels of protection. Specific vulnerabilities and protective design and construction measures are reviewed for each category of building elements and systems. Chapter 2 discusses blast design concerns and protective measures for areas surrounding buildings.

3.1.1 The Nature of Explosive Blasts

When a high order explosion is initiated, a very rapid chemical reaction occurs. As the reaction progresses, the solid or liquid explosive materials convert to very hot, dense, high-pressure gas. These products of explosion initially expand at very high velocities in an attempt to reach equilibrium with the surrounding air, causing a shock wave. A shock wave consists of highly compressed air, traveling radially outward from the source at supersonic speeds. Approximately one-third of the chemical energy available in most high explosives is released in the detonation process. The remaining two-thirds are released more slowly as the detonation products mix with air and burn. This afterburning process has little effect on the initial blast wave, because it occurs much more slowly than the original detonation. However, later stages of the blast wave can be affected by the afterburning (increasing the strength), particularly for explosions in confined spaces.

As the shock wave expands, the energy is distributed over an increasing volume and the corresponding peak pressures decrease. The blast pressures decay not only as a function of the distance but also over time (i.e., exponentially) and the duration of the pressure pulse is typically measured in thousandths of a second, or milliseconds. An explosion can be visualized as a "bubble" of highly compressed air that expands until it reaches equilibrium with the surrounding air. Alternatively, the pressure wave that is produced by an explosion may be visualized as concentric rings of diminishing intensity, similar to the circular ripples that are created when an object is dropped into a pool of water.

Explosive detonations create an incident blast wave, characterized by an almost instantaneous rise from atmospheric pressure to a peak overpressure.

Explosive detonations create an incident blast wave, characterized by an almost instantaneous rise from atmospheric pressure to a peak overpressure. As the shock front expands, the pressure decays to ambient pressure; however, because the rapidly expanding pressure wave pushes air away from the source of the detonation, a suction soon follows, and this is characterized by a low-intensity negative pressure phase that is usually longer in duration than the positive phase as shown in Figure 3-1. Although the negative phase is a physical phenomenon that may be observed in unobstructed detonations, the negative phase is frequently obscured as a result of reflections off buildings or other massive objects, and may therefore not be reliably observed in most blast-resistant design situations.

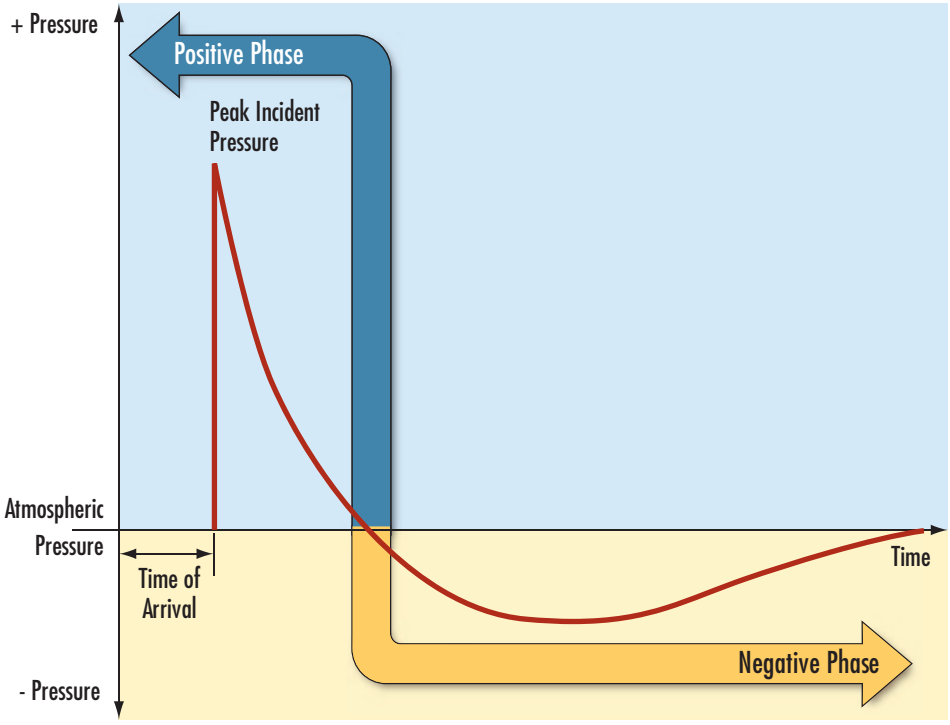


Figure 3-1:
Blast wave diagram and terminology

- **Shock Wave:** Supersonic propagation of pressure pulse
- **Positive Phase:** The initial outward movement of shock wave pressures from the source of the detonation, characterized by a nearly instantaneous rise in peak pressure followed by an exponential decay
- **Negative Phase:** The subsequent underpressure that trails the outward moving shock wave, creating a partial vacuum as air particles are moved with the shock front
- **Incident Pressure:** Shock wave overpressure that propagates unobstructed away from the detonation
- **Reflected Pressure:** Overpressures that are stagnated by obstructions in the path of the shock wave and are amplified in magnitude
- **Dynamic Pressure:** The drag forces applied to objects by the flow of air particles following the shock wave

When a structure or other massive objects obstruct the propagation of the incident pressure wave, the air particles are stagnated and the pressure is amplified. The magnitude of the resulting reflected pressure pulse that is applied to the obstructing surface is, therefore, greater than the incident pressure at the same distance from the explosion. The magnitude of the reflected pressure varies with the angle of incidence of the shock wave. When the surface of the obstructing object is perpendicular to the direction of the shock wave propagation, the obstructing object will experience the maximum reflected pressure. When the reflecting surface is parallel to the propagation of the blast wave, the waves are not obstructed and there will be no amplification of the incident pressure pulse. Consequently, the intensity of the pressure wave is amplified on the surface of an obstructing object, and the magnitude of the amplification depends on the angle of incidence and the magnitude of the peak incident pressure wave. Higher intensity pressure pulses are amplified to a greater extent than lower intensity pressure pulses, and the amplification factor is, therefore, a function of the net explosive weight and distance from the detonation.

Figure 3-2 shows typical reflected pressure coefficients versus the angle of incidence for four different peak incident pressures. The reflected pressure coefficient (coefficient of reflection, Cr) equals the ratio of the peak reflected pressure (Pr) to the peak incident pressure (Pi): (Cr = Pr / Pi). Reflected pressures for explosive detonations can be almost 13 times greater than peak incident pressures, and, for all angles of incidence, the reflected pressure coefficients are significantly greater for the higher intensity pressures than they are for the lower intensity pressures. For example, at a distance of 50 feet (15 meters) the detonation of

500 pounds (227 kilograms) of TNT equivalent will produce an incident peak pressure of 25 pounds per square inch (psi), and a reflecting surface perpendicular to the propagation of the shock wave at this location will cause the peak pressure to be amplified to 80 psi. If the standoff distance were reduced to 10 feet (3 meters), the incident peak pressure is 707 psi and the reflected pressure is 5,732 psi. The corresponding amplification factors are 3.2 for the lower intensity peak pressure and 8.1 for the higher intensity peak pressure.

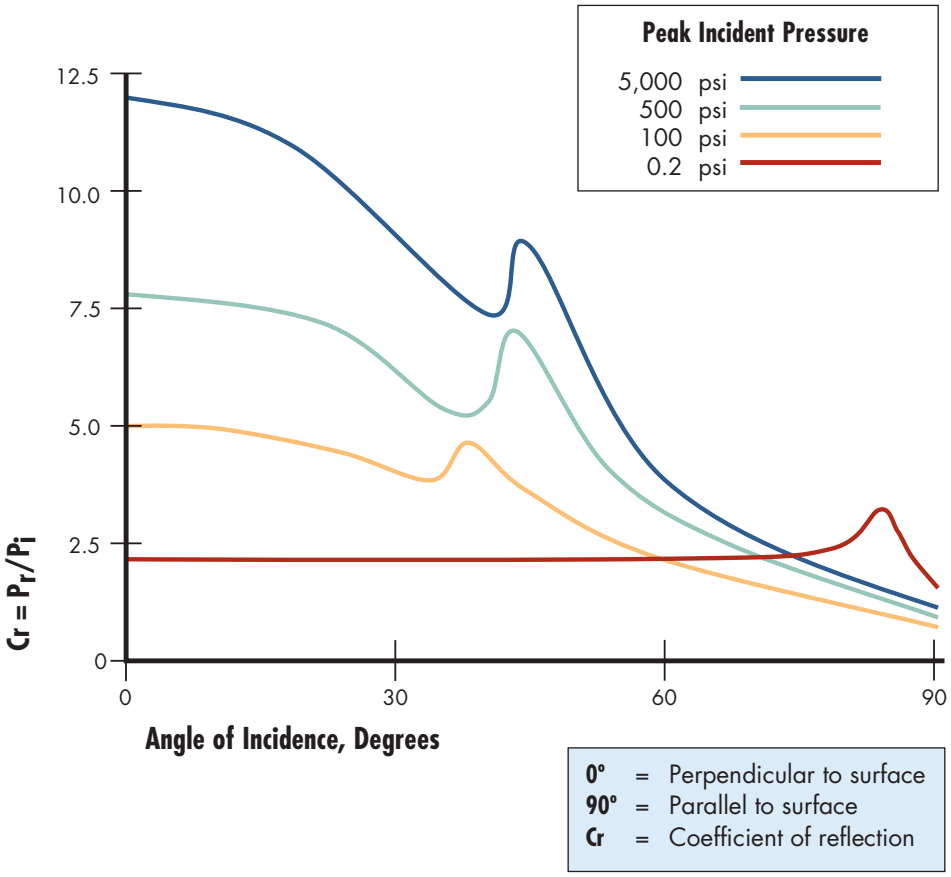


Figure 3-2:
Peak incident pressure

Similarly, a detonation on a hard surface, such as the ground, produces a reflection off the hard surface and the shock wave that would have radiated spherically is forced to radiate hemispherically. Focusing of all the blast waves away from the reflecting surface increases the intensity of the pressure pulse. As a simple example, a rigid surface directly beneath a detonation generates a pressure pulse that is effectively equivalent to the explosion of double the weight of the explosive. As the height of burst (center of explosive mass above the ground) is increased from zero (contact with the ground), the effectiveness of the ground reflectivity (and the corresponding reflection factor) is reduced.

Explosive detonations at very short standoff distances from an obstruction may produce large intensity blast loads over relatively small surface areas, but these high-intensity loads diminish rapidly with distance from the origin of the detonation. Conversely, explosive detonations at greater standoff distances from an obstruction produce less variation of the intensity over the surface of the obstruction. Close in detonations, therefore, produce locally intense blast loading (tending to punch through the obstruction), and large standoff detonations generally produce a more uniform intensity of blast loading (like wind against the upper floors of a building).

The amplification of shock waves that are caused by reflections off an obstruction may be diminished in the vicinity of an edge or opening of the obstruction due to clearing effects. The magnitude of the blast pressure is reduced from the reflected intensity to the incident intensity when the stagnated air is able to move around an edge or through an opening. The time at which this decay occurs is a function of the blast wave speed and the clearing distance to the edge or opening. Because amplifications are caused by the stagnation of the incident pressures, any free edge will allow the blast pressures to flow around the obstruction and, thereby, relieve the effect of the stagnation. The effectiveness of this relief wave is a function of the duration of the pressure pulse, the speed of the pressure wave, and the distance from a free edge.

Impulse is calculated as the area under a plot of blast pressure versus time (sometimes called a pressure time history plot), and it characterizes the duration of the dynamic loading. Incident impulse corresponds to the area under the incident pressure time-history curve, and reflected impulse corresponds to the area under the reflected pressure time-history curve. Whereas the magnitude of the shock wave's peak pressure is analogous to the punch, the magnitude of the shock wave's impulse may be thought of as the push. Therefore, the magnitude of the peak pressure alone is inadequate to describe the intensity of the blast loading. Instead of decaying exponentially with time as shock waves do, the decay may be approximated as linear. The duration of the linearly decaying positive phase pressure pulse may be calculated as twice the impulse divided by the magnitude of the peak pressure, as shown on Figure 3-3.

Impulse is calculated as the area under a plot of blast pressure versus time and it characterizes the duration of the dynamic loading.

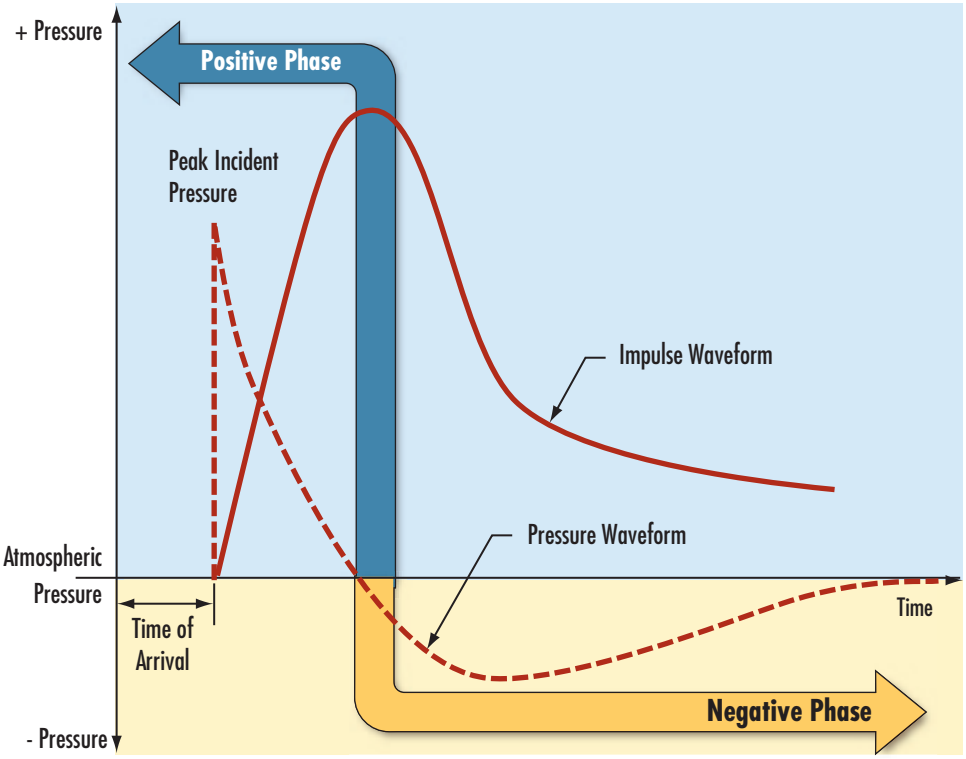


Figure 3-3:
Relationship between pressure pulse and impulse

The magnitude and distribution of blast loads on a structure are functions of several factors:

- Explosive properties (type of material, energy output, and quantity of explosive)
- Location of the detonation relative to the structure (standoff distance)
- Amplification of the pressure pulse through its interaction with the ground or structure (reflections)

The blast loading that may be applied to the surface of a structure is a function of the reflected pressure and reflected impulse. Blast loads vary in time and space over the exposed surface of the building, depending on the location of the detonation in relation to the building. Therefore, a set of different loading scenarios may be required in order to determine the worst-case effect.

3.1.2 The Effects of Explosive Blast on Buildings

Compared to other hazards (e.g., earthquakes, winds, floods), an explosive attack has the following distinguishing features:

- The intensity of the pressures acting on a targeted building can be several orders of magnitude greater than the intensities associated

with other hazards. Often, the peak incident pressure on a structure may be in excess of 100 psi. Most construction materials will sustain major damage or failure at these peak pressure levels.

- Explosive pressures decay with distance from the source, and the most severe effects are typically localized in proximity to the point of detonation. As a result, the damages on the side of a building facing a detonation may be significantly more severe than on the opposite side. However, in an urban setting, reflections off surrounding buildings can affect these damage patterns.
- The duration of the blast event is significantly shorter and measured in milliseconds, compared with the duration of earthquakes and wind gusts, which are measured in seconds or sustained wind or flood situations, which may be measured in hours. Although the structure's inertial resistance may mitigate its response to blast loading (the loading has passed before the structure begins to move), the structure's mass tends to resonate with the earthquake or wind loading frequencies (loading gets the structure moving and the frequency of that movement can be destructive).

The extent and severity of damage and injuries that result from an explosive detonation may vary widely depending on specific details of construction and materials. Although many of the specific details are not known, the overall level of damage and injuries that may be expected in response to an explosive event can be calculated. These evaluations are based on the size of the explosion, distance from the event, and assumptions about the construction of the building.

Building systems may often be evaluated independently because of the nature of the loading and their response (Figure 3-4). In particular, engineers often evaluate the primary structural frame (consisting of columns, girders, shear walls, and other components that contribute to global stability), secondary floor systems (consisting of slabs and filler beams that contribute to the localized gravity load carrying capacity of the floor plate), and the exterior façade (consisting of curtain walls, windows, masonry walls, and other components that form the exterior envelope). Each of these building systems has inherent capacity to resist extreme loading, deform without failure, and redistribute forces. The evaluation of building damage recognizes these different systems capacities and loading characteristics.

The extent and severity of damage and injuries that result from an explosive detonation may vary widely depending on specific details of construction and materials.

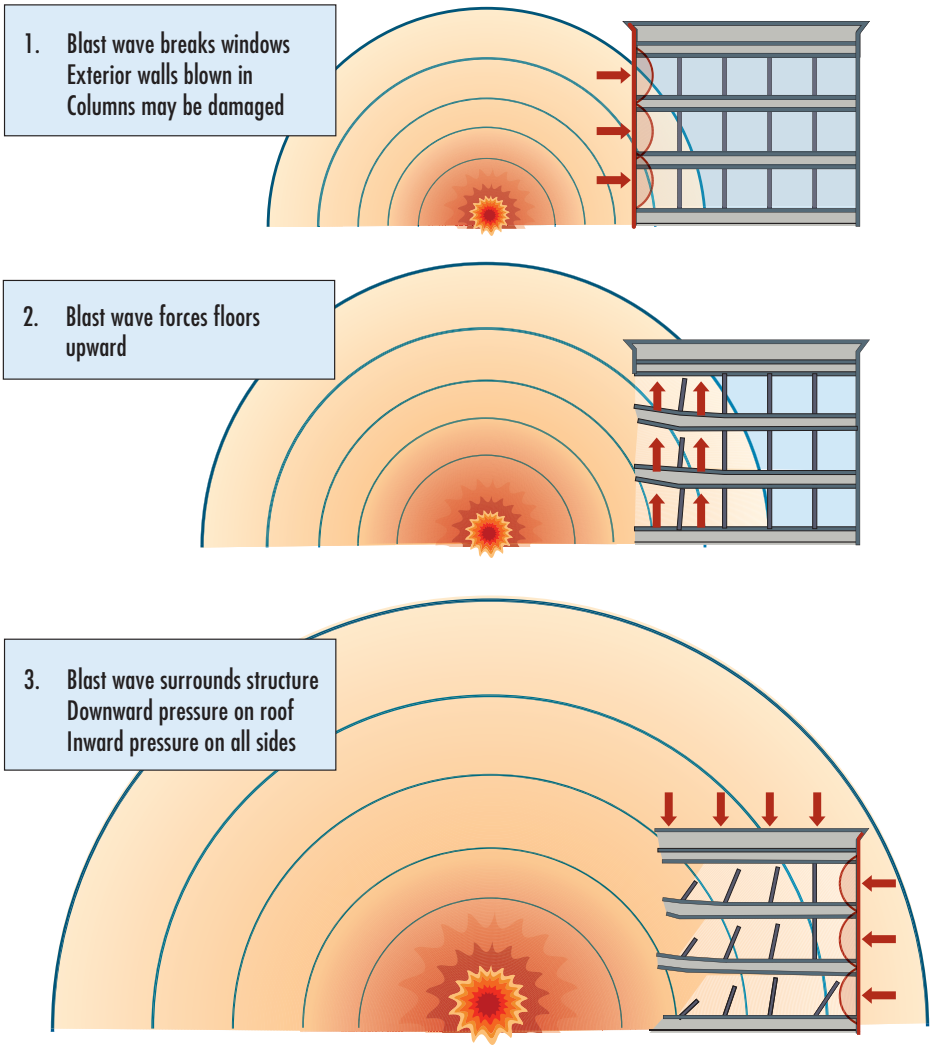


Figure 3-4:
Schematic showing sequence of building damage

SOURCE: NAVAL FACILITIES ENGINEERING SERVICE CENTER, USER'S GUIDE ON PROTECTION AGAINST TERRORIST VEHICLE BOMBS, MAY 1998

The primary structural frame (primary structure) is the most robust building system component and has the greatest inherent resistance to extreme loading. First floor columns and girders are typically designed to resist the cumulative effects of gravity and wind load, and the taller the building, the greater the robustness of these members. Because blast loading diminishes with distance from the detonation, the upper floors of buildings are subjected to lower blast forces from an explosive detonated at grade than the lower floors. Correspondingly, the upper-floor framing members resist smaller cumulative gravity loads than the lower-floor framing members, and as a result, the lower floors are most likely to resist the largest blast loads by virtue of the gravity load demands at this location.

The primary structural frame (primary structure) is the most robust building system component and has the greatest inherent resistance to extreme loading.

Structural members are likely to develop flexural deformations in response to the explosives that are

detonated at larger standoff distances. Unlike a VBIED, a hand-carried explosive may be placed directly adjacent to or directly above a primary framing member. Despite the relatively small weight of a hand-carried bomb, the close proximity of the detonation may cause a breach, brisance (projected fragments of building materials), or shear failure of the structure. In demolition terms, this is called a "cutting charge" designed to cut the column or beam to induce failure. Because every structural member has its limiting capacity, the stability of the building depends more on the structural redundancy and its ability to redistribute the gravity loads by means of alternate load paths.

Primary Structure: General gravity and lateral load resisting system, consisting of columns, girders, beams, shear walls, etc.; most vulnerable to near-contact detonations.

Secondary Structure: Local floor beams and slabs; most vulnerable to uplift infill pressures.

Exterior Façade: Building envelope most exposed to initial blast loading; most fragile and lightweight building materials.

Some structural systems are less forgiving than others. In particular, columns that are discontinuous from the roof to the foundation rely on girders or trusses to transfer loads over irregularities in the structural framing. Structural systems that transfer loads from the upper floors with smaller column spacing to lower floors with larger column spacing tend to be vulnerable to extreme loading because they concentrate loads to fewer members at the base of the building. These systems have less inherent ability to redistribute loads or find alternate load paths. This is especially significant for the potential of progressive collapse, as discussed later.

The design of the secondary structure, such as floor slabs and filler beams, depends on the span and the occupancy at a given floor location. The design of these members does not depend of the number of stories in the building; therefore, no inherent robustness of the secondary structure is associated with the size of the building. Furthermore, floor slab systems project large tributary areas to uplift blast loads, which may only be mitigated by the resistance of the exterior façade and the line-of-sight geometry from the threat vehicle to the underside of the slab. Although uplift damage to the lower floor slabs may occur in response to the exterior blast loads, localized breach and uplift may occur at any floor that is exposed to an explosive blast from a hand-carried satchel bomb.

The exterior façade is both the largest building component exposed to the exterior air blast loading and the most fragile. Glass and unreinforced and ungrouted masonry block, which are common façade construction materials, are inherently brittle and are likely to shatter under explosive loading, producing hazardous debris. The lower-floor façade is most vulnerable to the exterior vehicle threat because of its proximity to the

greatest intensity peak pressure and impulse. The design of the upper stories of high-rise construction may very well be governed by wind. To the extent the hardened façade resists the effects of an external detonation, the interior structure is isolated from the full intensity of infill pressures, which is the pressure that enters the building when the exterior façade fails. The greater the capacity of the exterior façade to resist pressures, the less potential there is for uplift pressures to be applied to the underside of the floor system. Extensive investigations have been performed to catalog the likely performance of a variety of building enclosure materials, and analytical tools are available to extend this database to different façade geometry, material properties, and loading scenarios.[4]

3.1.3 Injuries

Injuries resulting from exposure to explosive detonation may occur for several reasons. Primary injury is associated with the direct impact of the air blast overpressure. In addition to the shock wave, consideration should be given to the dynamic pressures that are associated with the detonation. Primary injuries are generally categorized by their severity: eardrum damage, lung damage, and lethal lung damage. Although the potential for serious injury is associated with both peak pressure and duration, the threshold of lung lethality is an incident pressure of approximately 100 psi for 3 milliseconds or an incident pressure of approximately 25 psi for 20 milliseconds. Table 3-1 summarizes the thresholds based on peak dynamic pressure as provided in DOD UFC 3-340-02, S*tructures to Resist the Effects of Accidental Explosions* (2008b). The likelihood of survival increases with the weight of the individual, so lower pressures than those shown for adults may cause lung damage or lethality in children.

Table 3-1: Primary Injury Thresholds

Critical Effect	Likelihood of Effect	Peak Pressure (psi)
Eardrum Rupture	Threshold	5
	50%	15
Lung Damage	Threshold	30
	50%	80
Lethality	Threshold	100
	50%	130
	Near 100%	200

4 Information can be found using DHS S&T's Owner Performance Requirements Tool at www.oprtool.org/demo and the Advanced and High Performance Materials Database at www.advmat.org.

Secondary injuries are caused by debris impact. Debris is most often associated with failed façade, finishes, and furnishings; however, debris may also be associated with damaged structural elements. Tertiary injuries may occur when individuals are thrown off their feet and onto the ground or into other hard objects. These injuries are typically head injuries suffered upon impact. Tertiary injury may be associated with the air overpressure or the base motions caused by in-structure shock.

Hence, the severity and type of injury patterns that result from explosive events may be related to the level of damage in the occupied space. The air-blast pressures that enter through broken windows can cause eardrum damage and lung collapse. As the air-blast damages the building components in its path, airborne debris may cause impact injuries. Airborne glass fragments typically cause penetration or laceration-type injuries. Larger fragments, such as the impact of a sheet of disengaged laminated glass, may cause non-penetrating, or blunt trauma, injuries. Additionally, the air-blast pressures and floor motions can cause occupants to be bodily thrown against objects or to fall.

Lacerations due to high-velocity flying glass fragments have been responsible for a significant portion of the injuries received in explosion incidents. In the bombing in Oklahoma City, for instance, 40 percent of the survivors in the Murrah Federal Building cited glass (and window blinds) as contributing to their injuries; among those injured within nearby buildings, laceration estimates ranged from 25 to 30 percent.

Figure 3-5 depicts the thresholds of different types of injury associated with damage to wall fragments and/or glazing. This generic range-to-effects chart shows the interaction between the weight of the explosive threat and its distance to an occupied building for common façade and structural components. 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-specific that the generic charts provide little more than general guidance in the absence of more reliable site-specific information and should never be used for design purposes. Based on the information provided in the chart, the onset of significant glass debris hazards is associated with standoff distances on the order of hundreds of feet from a blast, while the onset of column failure is associated with standoff distances on the order of tens of feet.

Lacerations due to high-velocity flying glass fragments have been responsible for a significant portion of the injuries received in explosion incidents.

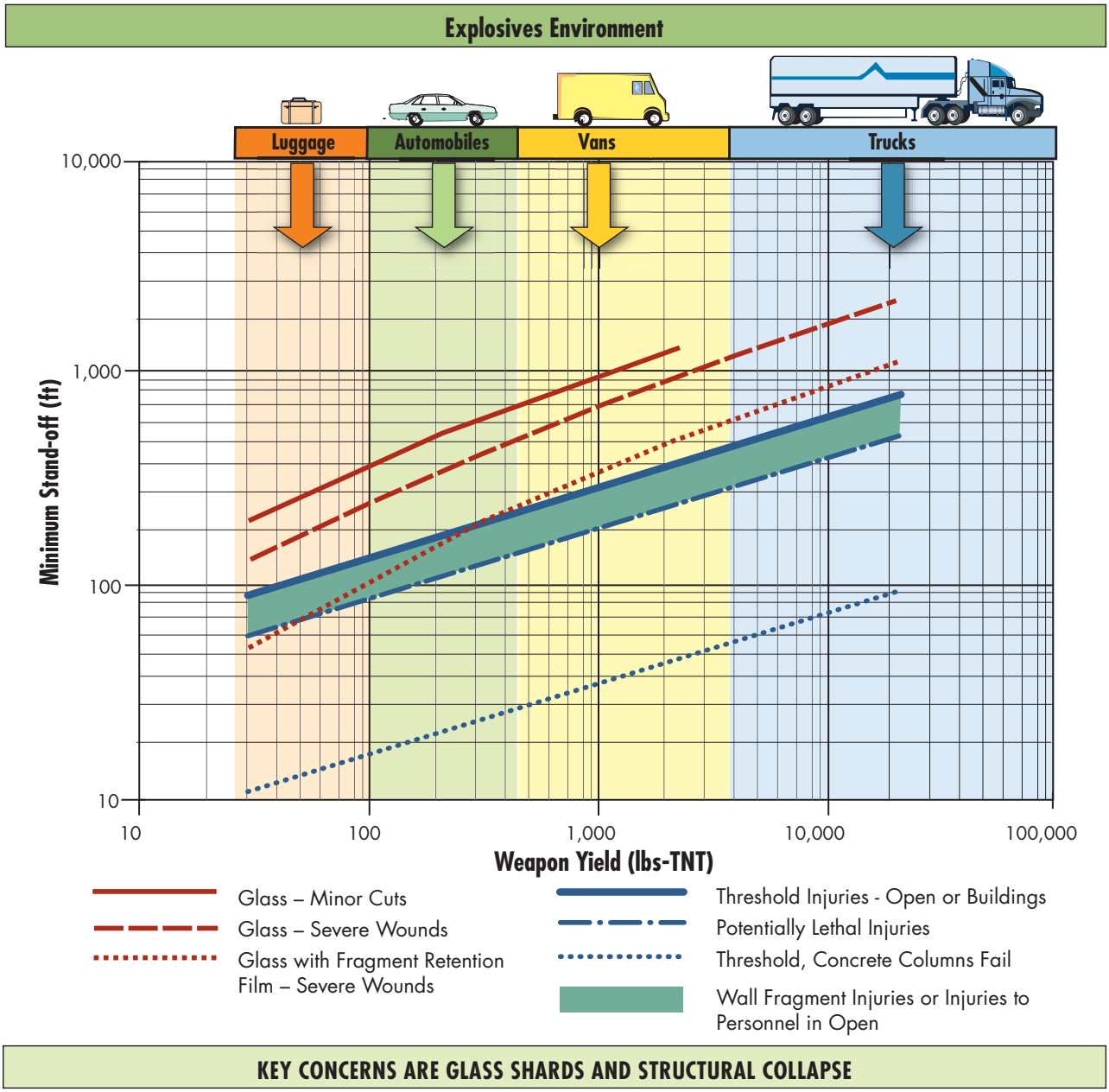


Figure 3-5: Generic range-to-effects chart. SOURCE: DEFENSE THREAT REDUCTION AGENCY

3.1.4 Levels of Protection

The effects of an explosion are related to both the size of the blast and the level of protection that is provided by the design in response to the blast loads. Levels of protection, often described in qualitative terms, such as low, medium, and high, are generally associated with different extents of damage and potential injury. Table 3-2 provides definitions for the levels of protection from the UFC 4-010-01, *DOD Minimum Antiterrorism Standards for Buildings* (2007a).

Table 3-2: DOD Minimum Antiterrorism Standards for Buildings

Level of Protection	Potential Building Damage / Performance[2]	Potential Door and Glazing Hazards[3]	Potential Injury
Below AT standards[1]	Severe damage. Progressive collapse likely. Space in and around damaged area will be unusable.	Doors and windows will fail catastrophically and result in lethal hazards. (High hazard rating)	Majority of personnel in collapse region suffer fatalities. Potential fatalities in areas outside of collapsed area likely.
Very Low	Heavy damage - Onset of structural collapse, but progressive collapse is unlikely. Space in and around damaged area will be unusable.	Glazing will fracture, come out of the frame, and is likely to be propelled into the building, with the potential to cause serious injuries. (Low hazard rating) Doors may be propelled into rooms, presenting serious hazards.	Majority of personnel in damaged area suffer serious injuries with a potential for fatalities. Personnel in areas outside damaged area will experience minor to moderate injuries.
Low	Moderate damage – Building damage will not be economically repairable. Progressive collapse will not occur. Space in and around damaged area will be unusable.	Glazing will fracture, potentially come out of the frame, but at a reduced velocity, does not present a significant injury hazard. (Very low hazard rating) Doors may fail, but they will rebound out of their frames, presenting minimal hazards.	Majority of personnel in damaged area suffer minor to moderate injuries with the potential for a few serious injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience a minor to moderate injuries.
Medium	Minor damage – Building damage will be economically repairable. Space in and around damaged area can be used and will be fully functional after cleanup and repairs.	Glazing will fracture, remain in the frame and results in a minimal hazard consisting of glass dust and slivers. (Minimal hazard rating) Doors will stay in frames, but will not be reusable.	Personnel in damaged area may suffer minor to moderate injuries, but fatalities are unlikely. Personnel in areas outside damaged areas will potentially experience superficial injuries.
High	Minimal damage. No permanent deformations. Facility will be immediately operable.	Glazing will not break. (No hazard rating) Doors will be reusable.	Only superficial injuries are likely.

1. This is not a level of protection, and should never be a design goal. It only defines a realm of more severe structural response, and may provide useful information in some cases.
2. For damage / performance descriptions for primary, secondary, and nonstructural members, refer to UFC 4-020-02, *DOD Security Engineering Facilities Design Manual* (2007b).
3. Glazing hazard levels are from ASTM F 1642.

The UFC DOD antiterrorism force protection standard establishes a mandatory standoff distance to achieve a given level of protection, with the explicit statement that DOD recognizes and accepts that a modest percentage of the occupants will be injured or killed if an event occurs. The UFC distinguishes between a conventional construction standoff distance, at which no structural hardening is required, and a minimum standoff distance for which the building structure must be hardened. Although increased structural hardening could reduce the effect of detonations at shorter distances, the specified minimum standoff distance is reserved to accommodate future upgrades that could be necessitated by emerging threats.

The ISC criteria of 2004, Security Design Criteria for New Federal Office Buildings and Major Modernization Projects, also use a minimum standoff distance, typically 20 to 50 feet, but do not explicitly address how many casualties are likely to occur or are acceptable (DHS 2004a). The ISC level of protection criteria is based on acceptable building damage.

Unfortunately, both standards, unintentionally, conflict with local jurisdictional zoning, planning, and land use. Very few communities, particularly urban and semi-urban, can afford or want to have a government facility that requires extensive land in a high value area and creates a potential for collateral damage to adjacent public infrastructure, private-sector structures, and businesses.

To address these concerns, as well as to incorporate the advances in risk analysis and construction materials and methods, the ISC issued new physical criteria, Physical Security Criteria for Federal Facilities, in April 2010. The new ICS criteria establishes a risk-based process that is coupled with the facility security level (FSL), from 1 (minimum) to 5 (very high). Larger buildings or those with high-risk tenants have higher FSL ratings. The ISC establishes compliance criteria for six areas:

- Site includes the site perimeter, site access, exterior areas and assets, and parking.
- Structure includes structural hardening, façade, windows, and building systems.

Levels of Protection

Quantitatively, the levels of protection for structural elements are defined in terms of deformation, ductility, or edge rotation. The ductility ratio ($\mu = Du/Dy$) is the ratio of the ultimate deflection Du at a given load level to the deflection at the yield stage Dy, where Dy varies with the structural properties (e.g., geometry, material properties, reinforcement ratio). The DOD quantified the different levels of response associated with the different levels of protection based on measurements from blast testing and the results of blast response analyses. The magnitudes of deformation, ductility, and edge rotation that are associated with the different levels of protection vary for different types of construction. Similarly, the performance of a glass façade is related to the extent of hazardous debris that may result from the applied blast loading. These characteristics of glass response are also based on the observations of blast testing and the results of blast response analyses.

- Facility entrances include employee and visitor pedestrian entrances and exits, loading docks, and other openings in the building envelope.
- Interior includes space planning and security of specific interior spaces.
- Security systems include intrusion-detection, access-control, and CCTV camera systems.
- Security operations and administration include planning, guard-force operations, management, decisionmaking, and mail handling and receiving.

Performance-Based Design (PBD)

PBD is uniquely suited to addressing building security. It relates postulated threats, system vulnerabilities, and perceived consequences in a quantifiable fashion. The emergence of powerful modern computing capabilities and efficient analysis techniques makes PBD a useful design technique. The design steps in a PBD approach can be summarized as follows:

1. Estimate/postulate threat (design basis threat selected by owners / decision makers / assessment team).
2. Analyze the response of the structure of interest to the postulated threat. Generally speaking, such an analysis is high resolution analysis, which can predict nonlinear behavior as well as failure of components, if applicable.
3. Estimate the costs of the structural failures (consequences) as computed in #2.
4. Evaluate the costs of #3. If the costs are adequate, then the design is adequate. If the costs are too high, then improve the design in #2, and re-compute the costs.
5. Continue the iterations of #1 through #4 until a reasonable balance between postulated threat (#1), design (#2), and consequences (#3) costs is obtained. Changes in the design basis threat will require concurrence by owners/decision makers.

Note that the costs in PBD are not necessarily direct monetary costs. They include casualties, human injuries, down-time of operations, etc. The PBD paradigm can even be generalized to be a very powerful benefit-cost, LCC, or life-cycle analysis tool. The procedures are similar to the above steps, with slightly more computational demands. Moreover, PBD can also be used in a multihazard environment, where additional hazards are included in the above-mentioned steps. In all, PBD provides a versatile design method that can ensure adequate performance and acceptable consequences at reasonable costs.

The new ISC criteria do not prescribe a minimum building standoff distance. A combination of façade and structure hardening, emergency occupant plans, operational security, and other protective elements are

used to reduce the risk to an acceptable level. The standard recognizes that complete protection from all the possible attack modes and weapons is not possible, and that the objective of explosive blast protection is to prevent progressive collapse and minimize mass casualties.

Note that not all building components may be designed to the same level of protection against the same intensity of blast loading.

Note that not all building components may be designed to the same level of protection against the same intensity of blast loading. Because of the nature of the structural materials and section properties, the primary structural frame may be reasonably designed to resist the effects of an explosive load at a given standoff distances while preventing collapse and minimizing structural damage.

At lower elevations, in close proximity to the blast loading, the secondary structure will require very thick and highly reinforced slab and beam members to provide the same level of protection for this magnitude of explosive threat. However, the glass façade is likely to be overwhelmed by the high intensity blast loads. Because structural collapse is more catastrophic than flying glass debris, dual criteria are often established that require the façade to be designed to provide a specified level of protection in response to a much lower intensity blast loading than the primary structure. This is acknowledged in the ISC *Physical Security Criteria for Federal Facilities* (DHS 2010), which require the structure to be designed to resist a specified explosive threat detonated at the protected perimeter, but permit a specified percentage of the façade to produce high hazard debris in response to the same blast loading intensity.

Range-to-effects charts (Figure 3-5) may be used to determine the standoff distances at which a given size bomb will produce a specified effect. These types of charts are not very accurate; however, they can be used to obtain an approximation of the blast response of a building component or window at different levels of protection. They can also be used to consolidate all building response information to assess needed actions if the design threat changes (size of explosive). When accuracy is needed, a building-specific range-to-effects chart should be prepared to determine the necessary standoff distance for a given amount of explosives, typically expressed in terms of TNT equivalence.

3.1.5 Collateral Damage

The effects of an explosion may not be limited to the targeted structure that is in closest proximity to the detonation. Large explosive events affect structures at great distances from the detonation. Depending on the type of construction and the distance from the intended target, both the structure and façade or only the façade may be damaged.

Furthermore, dense urban streetscapes do not permit the blast energy from an explosion to radiate even hemispherically away from the detonation. The channeling of blast waves through "urban canyons" may concentrate the blast loading and create a complex pattern of focus and shadow zones. Therefore, the blast loading that may result from distant detonations may be amplified or attenuated by the height and density of surrounding structures and the width of streets. Although computationally intensive, these effects may be calculated using computational fluid dynamics software. Reasonable approximations may be made using simpler analytical tools to account for surrounding structures. Figure 3-6 depicts the propagation of a blast wave through a dense urban landscape in which tall buildings focus and channel the air blast; this results in significant enhancement of blast pressure, as pressure waves reflect off of adjacent buildings, or shielding of blast loads, as some buildings are shadowed from the blast. As a result, collateral damage may be extensive over large areas, injurious, and cause significant property damage.

Figure 3-6:
Snapshot of shock wave propagating through urban landscape

As an example, 10 structures collapsed, 21 structures sustained structural damage, and 253 buildings sustained minor damage from the 1995 explosion at the Alfred Murrah Federal Building in Oklahoma City. Glass was damaged for nearly ¾ mile from the detonation (Figure 3-7).

Blast Load Effects in Urban Canyons

Since 2008, the DHS S&T IDD and Program Executive Office Counter Improvised Explosive Devices have been working together to enable first responders, building designers, building owners, and the industry to protect U.S. building stock and infrastructure. The Blast Load Effects in Urban Canyons project is directed at reducing substantial damage to buildings located in large urban centers as a result of IED attacks. In this project's first phase, the streetscapes of the New York City Financial District were modeled to include rigid representations of all the buildings and the geometry of all the streets and alleys.

The Blast Load Effects in Urban Canyons project focuses on the development of:

- An Urban Blast Tool, which allows the design and first responder communities to estimate the intensity of blast effects to buildings. The analysis, calculations, and modeling have been captured in a database to be used for the fast-running tool. The tool uses the results stored in the database to interpolate expected blast effects for a user-entered location.
- A Design Guidance Report, which includes an analysis of different building structural systems (steel-moment frame, concrete-moment frame, and flat-plate construction) to determine their sensitivity to progressive collapse following the removal of key first-floor structural elements.
- A study of structural response, emergency evacuation, rescue, and recovery systems. These systems include egress stairway enclosures, stair pressurization systems, fire doors, fire/smoke detection systems, sprinkler pipe systems, emergency communication/fire alarm systems, emergency lighting, emergency generators, emergency elevators, air ducts, and conduit chases.

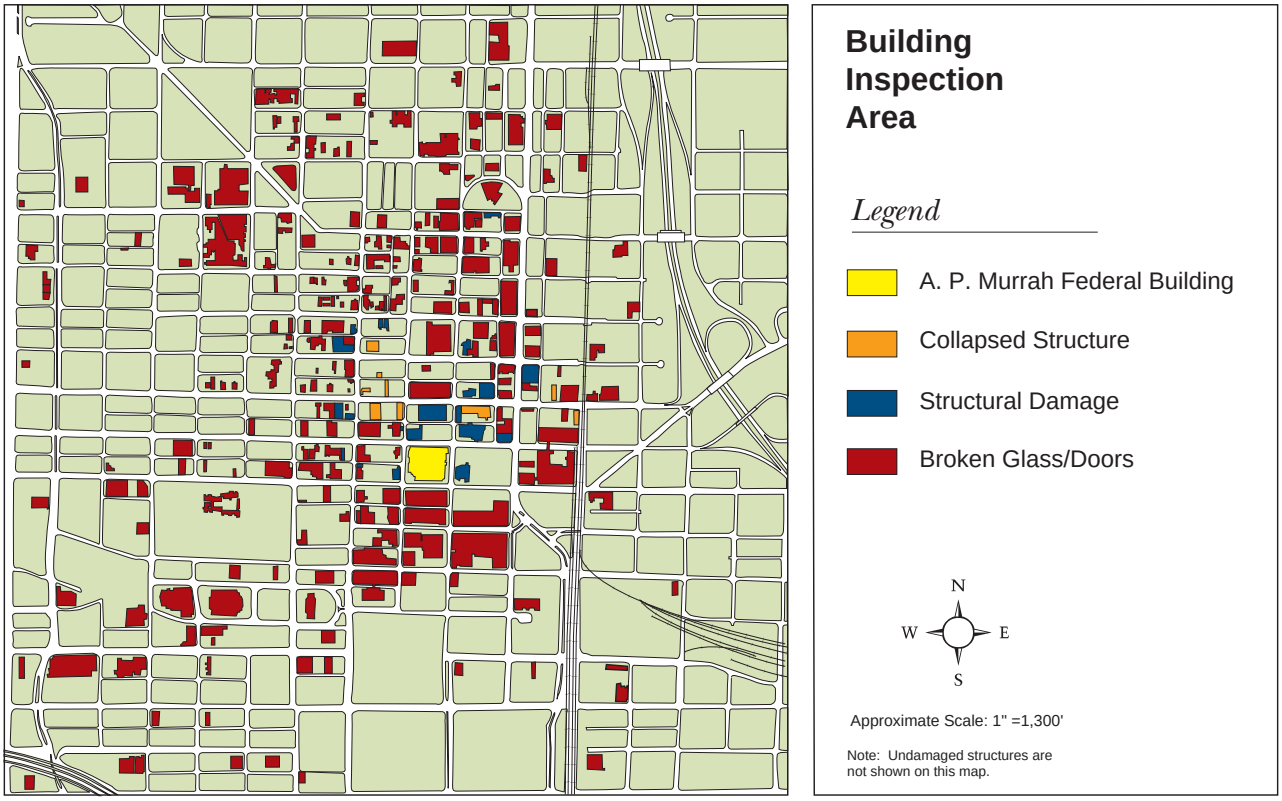


Figure 3-7: Extent of collateral damage following the explosion at the Alfred Murrah Federal Building. SOURCE: FEMA 277

3.2 Architecture

When a desired level of protection cannot be achieved solely through site design measures, presented in Chapter 2, designers should consider additional protective measures at the level of building design. Although the design of a structural system is of pre-eminent importance for building resilience, many aspects of architectural design significantly affect the vulnerability of buildings to blast impact. Architectural considerations that affect a building's resilience include building configuration, interior layout and space planning and design, the building envelope, glazing materials, and environmental and utility systems. Architectural design also affects post-incident performance of the building insofar as the optimal placement of evacuation routes, emergency exits, and other critical functions can facilitate emergency evacuation, rescue, and recovery efforts.

Appropriate architectural design of these systems can contribute a great deal to the reduction of risks, especially because the necessary protective measures often add very little to the overall cost, if implemented early in the design process.

Security specialists and protection engineers should take part in the design process and work with the architects as soon as the design process begins. Additionally, architects must interface with specialized design consultants, local planning commissions, and other regulatory bodies and are responsible for integration and coordination of all aspects of a project throughout its implementation.

3.2.1 Building Size and Configuration

The characteristics of buildings that affect their performance under blast loads comprise the overall building size and its geometric configuration. The aspects of building geometry that have particular importance for the protection from blast include the building height, the presence of reentrant corners, circular and concave forms, and the overall irregularity of the building form.

Low-rise buildings (Figure 3-8) have a large footprint relative to their floor area, which makes collapse of an entire building from a single blast very unlikely. People, assets, systems, and operations are spread across wide areas in low-rise buildings, which generally tends to reduce the damage and effects from a single incident. Low-rise buildings offer opportunities to use interior courtyards or atria to bring light and a natural setting to the building, without adding vulnerable openings to the exterior. Because access can be more easily controlled, courtyards and atria typically require less hardening compared to the building perimeter.

Figure 3-8:
Low-rise buildings

However, low-rise structures may be vulnerable to additional loading as the blast wave sweeps over the roof. This is especially true for an explosion generated by a large VBIED at the greater standoff distance that applies large blast loads to the roof of the low-rise structure. Unless the roof is concrete deck or concrete slab construction, it will likely be subjected to blast loads that far exceed conventional design loads and may cause failure. Retrofit hardening of an existing structure to increase the roof's resistance to blast loading usually requires extensive renovation of the entire building structure and can be difficult to achieve. For a new building, however, the necessary protective measures are not difficult to analyze and design.

Retrofit of Buildings and Infrastructure in Large Urban Areas

This new DHS project focuses on identifying innovative curtain wall systems and connections that will resist the impact of different ranges of explosive loads during terrorist events. This project aims to expand the understanding of existing materials and curtain wall systems that are suitable for blast resistance as well as cost effective for a series of attributes, such as energy efficiency, moisture penetration, and air leakage. In addition, the project seeks to identify cost-effective, innovative systems that can be widely used by manufacturers, architects, engineers, and construction contractors. The benefit-cost assessment can profoundly affect the owner's decisions to make optional improvements to the building's performance that are well above minimum requirements set by codes and standards. For this project, six curtain wall systems and four novel connection concepts will be identified addressing explosive blast and other major design attributes. For the proof-of-concept, coordination will be well established with organizations, such as DOS, University of California-San Diego, Energetic Materials Research and Testing Center, and manufacturers, such as U.S.G (Fortocrete™) and Lafarge (Ductal®). Curtain wall systems and connections will be analyzed using advanced physics-based finite element models; field testing will be conducted. Based on the results of the analysis, promising curtain wall test specimens and/or connections will be selected for testing.

Mid-rise buildings' (Figure 3-9) vulnerability depends on their size and complexity of configuration. If large, they are less likely to suffer complete collapse from a single blast. They may contain mixed uses and interior parking, which can add to the vulnerability of the structure.

Figure 3-9:
Mid-rise buildings

High-rise and very tall buildings (Figure 3-10) must resist very high gravitational and lateral loads, although the choice of framing system, specific structural details, and building configuration will determine the overall performance. The lower floors, which are in closest proximity to a potential VBIED attack, are inherently robust and more likely to be resistant to blast loading than those in smaller buildings. However, tall buildings are likely to be located in dense urban environments that tend to trap the blast energy within the canyon-like streets, thereby increasing the danger from waves that reflect off neighboring structures. Tall buildings are likely to contain loading docks in narrow alleys that can introduce significant additional vulnerabilities (see Chapter 2). High-rise and very high-rise buildings generally require less explosive blast hardening in the upper floors compared to the lower stories, because blast intensity diminishes with distance. For example, a typical sixth floor will be over 70 feet (21 meters) from the ground, which is a significant standoff. However, egress planning for emergencies is more critical and tends to be more complex in this type of building.

deef-ə-

Reentrant corners are defined as internal or inside corners in the building envelope, usually at angles 90 degrees and greater.

Reentrant corners are defined as internal or inside corners in the building envelope, usually at angles 90 degrees and greater, as shown in Figure 3-11. As with buildings that are U- or L-shaped in plan, or that have similar configurations, the reentrant corners tend to trap and reflect shock waves thereby increasing explosive blast effects. Thus the geometry of a building may significantly affect the performance of the structure under blast loads.

Figure 3-10:
High-rise (left) and very high-rise, 60 stories (right)

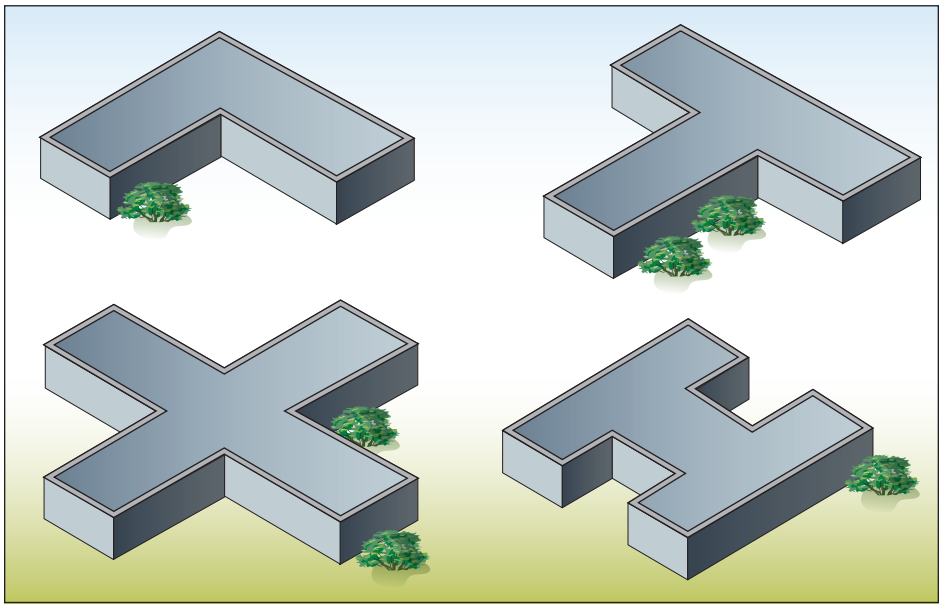


Figure 3-11:
Reentrant corner building forms

Figure 3-12 illustrates the concentration of blast loads for building configurations that have either U-shaped floor plans or large overhangs. Instead of simply amplifying the blast load and then propagating away from a building façade, blast waves that are reflected within reentrant surfaces are trapped, and the load is intensified. The right figure shows a vertical reentrant corner, or overhang. The arrows indicate the direction of reflected blast waves in each situation.

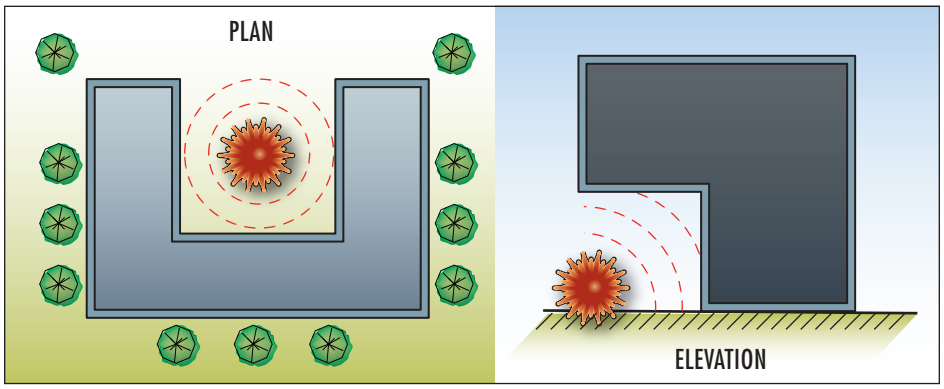


Figure 3-12:
Blast waves related to building configuration

SOURCE: FEMA 427

Irregular shape (Figure 3-13) is another aspect of building geometry that affects a building's response to blast loads. Most buildings, mainly for economic reasons, are simple rectangular forms, or combinations of simple forms. However, some buildings, for reasons of image or iconic significance, are very complex, or irregular in their geometry. Such buildings require detailed analyses of their vulnerability to blast and possible mitigation methods.

In general, convex shapes perform better under blast loading. Buildings that are circular in plan, for example, act to reduce the air-blast pressures because the angle of incidence of the shock wave or wind increases more rapidly than in a rectangular building. Wind design following American Society of Civil Engineers (ASCE) Standard 7-05 indicates a range of 29- to 65-percent reduction in the force coefficient for loading on a circular structure compared to a flat façade (Figure 3-14). Concave plan forms tend to amplify the blast effect in a similar manner to the U-shaped buildings.

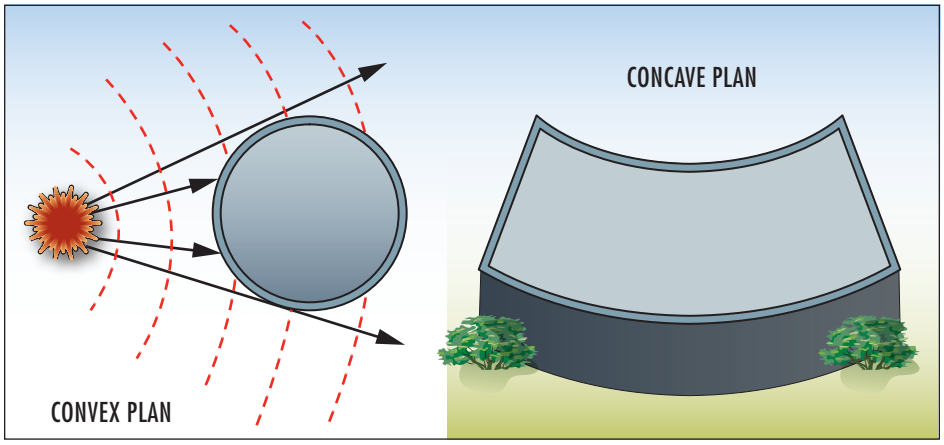


Figure 3-13:
Convex (circular) plan form (left) and concave plan form (right)

SOURCE: FEMA 427

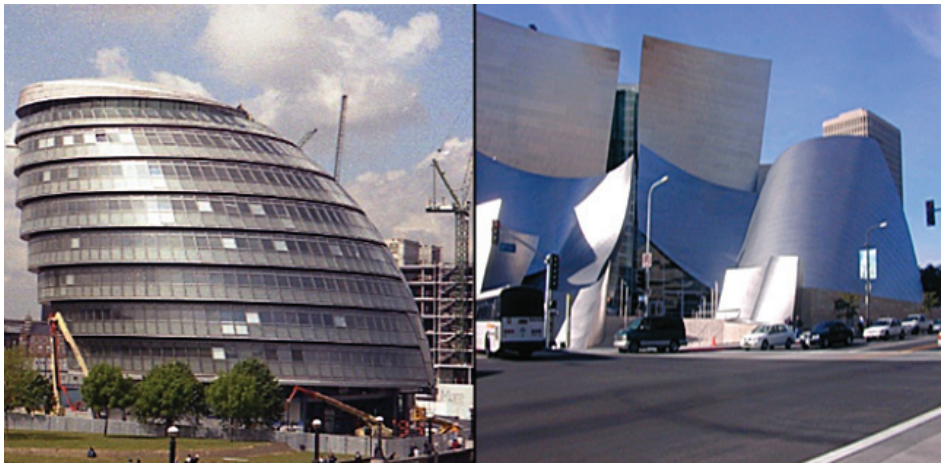


Figure 3-14:
Highly irregular shaped buildings:

Civic building (left) and Performance Center (right)

3.2.2 Layout Design

General building layout is traditionally determined by a combination of functional, aesthetic, economic, and other criteria. The addition of security criteria helps organize the space and building functions to reduce their vulnerability to external blast. For example, entry lobbies and areas that contain retail facilities or bars and restaurants must necessarily be open and, therefore, largely unsecured. Other areas like loading docks, mailrooms, or parking garages may not be as open, but are still vulnerable because of the lack of access controls.

Layout and space design must take into consideration the placement of secured and unsecured areas within a building, either by separating them with buffer zones, like corridors, mechanical rooms/floors, and storage areas on the secure side of the public areas, or by hardening the separation between them. To reduce the building vulnerability further, designers may place unoccupied or limited occupancy spaces on the perimeter of the building, especially in the absence of sufficient standoff or hardening. Even when hardening is added, placing unoccupied or limited occupancy space on the building perimeter adds additional protection to the occupied space further into the building interior. Figure 3-15 illustrates an improved layout based on these concepts.

Layout and space design must take into consideration the placement of secured and unsecured areas within a building, either by separating them with buffer zones, like corridors, mechanical rooms/floors, and storage areas on the secure side of the public areas, or by hardening the separation between them.

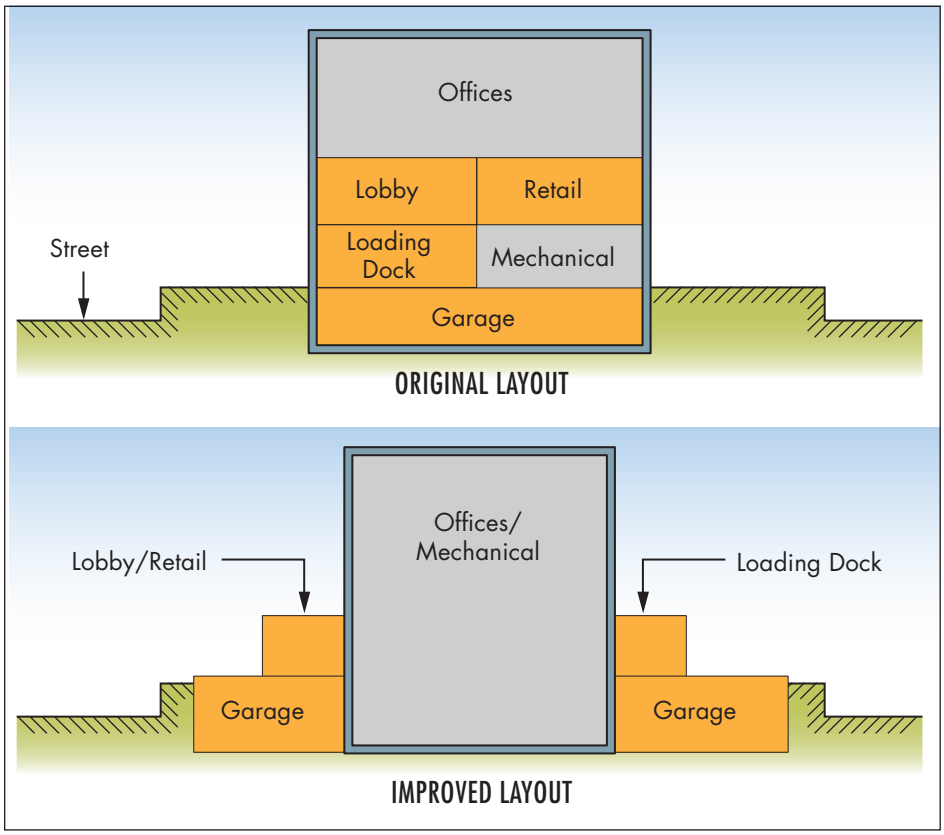


Figure 3-15:
Improved layout for adjacent unsecured and secured spaces

SOURCE: FEMA 427

The concept of separating secure and unsecured space is relevant to other building systems, especially those needed for life safety and continuity of operations. In these cases separation distance is more important than buffer zones, although hardening may be applicable for certain systems, such as stairwells, sprinklers, elevators, utility rooms, plumbing risers, and utility chases. Keeping these systems away from the vulnerable areas and separating the system components is advisable, so that a single incident cannot simultaneously make inoperative both the primary and backup systems, such elevator banks and stairways.

GSA recommends a minimum 50-foot (15-meter) separation between primary and backup systems. For example, elevators and stairways should not exit directly into a loading dock or lobby, or near other vulnerable, high-risk spaces. Where three or more backup power generators are planned, consider installing them in two separate locations. Similarly, the electric utility switchgear, the automatic transfer switch, and the backup switchgear should be in separate locations with sufficient separation distance. The same approach should be followed for the placement of IT (data and voice) systems. The convenience of putting all cabling in a single vertical riser leads to single-point vulnerability; therefore, the primary and backup cabling should be split among multiple risers.

3.2.3 General Design Considerations

The following general design considerations generally reduce the building's vulnerability:

- Buildings should be oriented horizontally rather than vertically to reduce the building's profile and exposure and to facilitate the clearance of a blast wave.
- The ground floor elevation of a building should be at 4 feet (1.2 meters) above grade to mitigate vehicle ramming, where appropriate for the general building design. The substantial nature of basement/foundation walls may withstand the impact and keep the vehicle outside the building footprint.
- Low-rise buildings should not have overhangs. When needed, overhangs should be carefully designed for blast loading, because they can be points of high local pressure and suction.
- Low-rise buildings should use earth berms or similar structures to reduce blast wave effects. This approach deflects the shock wave above the building (where the berm is about as tall as the building walls) and also reduces the possibility of fragmentation within the building. However, blast waves reform after they sweep over the berm, which requires the berms to be located close to the protected building or in contact with the building envelope, as in earth-sheltered design. Earth-sheltered design has significant energy conservation and fragmentation benefits.
- Major glazing should be perpendicular to the primary façade, facing the direction of a potential VBIED attack, to reduce exposure to blast and projectiles and to reduce the number of windows requiring hardening (Figure 3-16).
- Low-rise buildings should have pitched roofs (and pitched window sills) to increase the likelihood of deflecting thrown explosives, thus increasing the standoff from a potential explosive device and reducing damage.
- Key assets should be located as far into the interior of a building as possible and as far away as possible from areas of high visitor activity.
- Key assets should be located in spaces that are occupied 24 hours per day and where they are visible to more than one person.
- Unsecured areas should be physically separated from the main building or building core to the extent possible.
- Where it is not possible to place vulnerable areas outside the main building, they should be placed along the building exterior, and the building layout should create buffer zones.

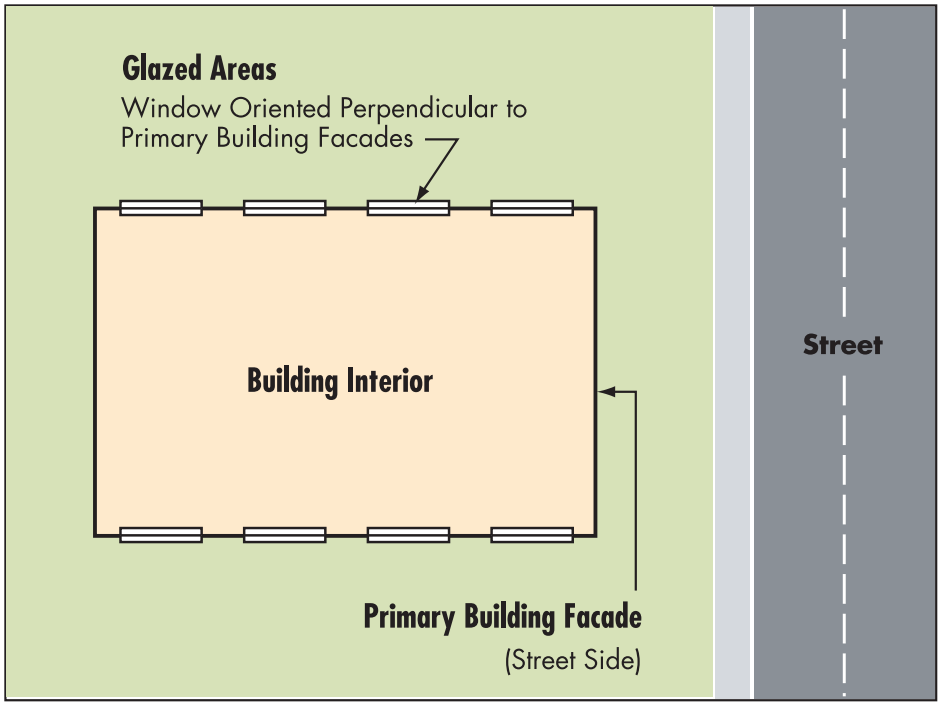


Figure 3-16:
Main glazed areas oriented perpendicular to approach street

SOURCE: U.S. AIR FORCE INSTALLATION FORCE PROTECTION GUIDE

- Vulnerable areas (where suspect material may enter a building), such as lobbies, loading docks, mailrooms, and parking garages should be isolated from the rest of the building and protected by using reinforced floors, ceilings, and full height walls, and hardened doors. No building systems or utilities, other than those directly supporting the function within, should be placed on either side of the walls for these areas. Both interior and exterior doors to these areas should remain closed when not in use.
- Secured occupied or critical areas should not be placed above or below unsecured areas, like garages, without a buffer zone or security-hardened protection.
- Doors in interior hallways should be staggered (instead of placed directly across from each other) to limit the effects of a blast inside the structure. This approach is also recommended in lobby foyers, but may be possible only in smaller buildings.
- Vulnerable/public interior spaces should be vented to the outside of the structure—for interior explosive forces and gases—but should be protected from blast pressures applied to the outside. Blow-out panels and window system designs that resist blast forces from the outside, but that readily fail and vent if exposed to blast pressure on the inside, will reduce internal pressures and lessen damage to the remainder of the building.

Lobbies should accommodate spaces for security personnel and inspection stations. Second generation x-ray equipment is larger than first generation equipment; designers should plan inspection spaces accordingly. GSA requires the lobby of a Federal building to be designed to separate secure and unsecured areas. Interior wall area and exposed structural columns should be minimized in unsecured lobby areas to reduce hardening costs.

Lobbies should accommodate spaces for security personnel and inspection stations.

Lobbies with retail and other mixed uses, which have been encouraged in public buildings by the Public Buildings Cooperative Use Act of 1976, should be open and inviting. Although important to the public nature of the buildings, the presence of retail and other mixed uses may present a risk to buildings and their occupants and should be carefully considered on a project-specific basis during project design. In buildings that are potentially at risk of terrorist attacks, retail and mixed uses may be accommodated by providing separate entryways, controlled access, and hardening of shared partitions.

Figure 3-17 shows some suggested arrangements of lobby, main occupied space, and retail spaces.

Lobbies with retail and other mixed uses should be open and inviting.

Mixed occupancies require special design considerations, especially when high-risk tenants are housed with low-risk tenants. Terrorists may identify targets based on their symbolism, visibility, ideology, political views, potential for publicity, or, simply, the consequences of their loss. For example, a post office processing mail should not be located in the same building as a childcare center.

Security personnel should be located so that they cannot be seen from uncontrolled public areas such as streets, plazas, or pedestrian walkways (other than in the lobby). Whenever possible, spaces for security personnel should face courtyards, internal sites, or controlled areas. Where this is not possible, suitable obscuring glazing or window treatments should be provided, including impact-resistant glass, blast curtains, or other interior protection systems.

Public toilets and service areas or access to vertical circulation systems should not be located in unsecured areas, including the queuing area before visitor screening at the public entrance.

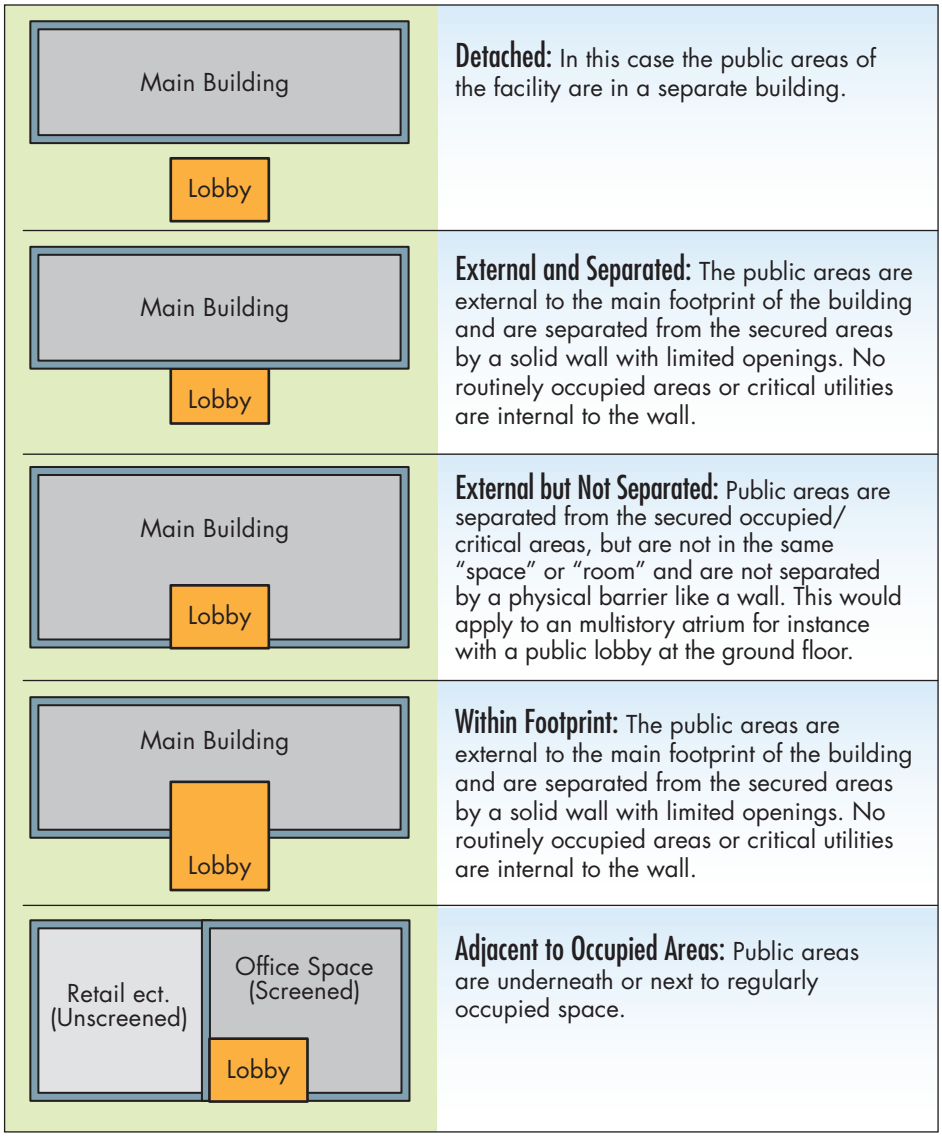


Figure 3-17:
Lobby, main building, and retail location alternatives

SOURCE: FEMA 455

Safe havens and safe rooms represent the innermost layer of protection within a physical security system. Safe havens are not expected to withstand a determined paramilitary attack using explosives or heavy weapons. The safe haven should be designed to delay an attack in order to allow first responders to arrive. Safe rooms provide more generic protection from natural hazards, explosive blast, and toxic agents. For additional information on safe havens and safe rooms, see FEMA 453, *Safe Rooms and Shelters – Protecting People Against Terrorist Attacks* (2006).

3.3 Structural Systems And Components

The most important role of the structural system is to prevent building collapse. Because the main objective of a terrorist attack with explosives is to cause the building to collapse—and thereby inflict heavy casualties among the occupants—collapse prevention and strengthening of a building's structural system must be the designer's primary concern. This is especially important as the majority of fatalities in terrorist attacks directed against buildings result from building collapse, as evidenced by the Oklahoma City bombing in 1995, where 87 percent of victims were killed in the collapsed portion of the Murrah Federal Building, or the WTC attack in 2001 (9/11), where over 2,600 people died in the progressive collapse of both towers.

When considering mitigation measures for explosive blast threats, the primary strategy is to keep explosive devices as far away from the building as possible (maximize standoff distance). This is usually the easiest and least costly way to achieve a desired level of protection. In cases where sufficient standoff distance is not available to protect the building, the building's structural systems may require hardening, as well as appropriate design to prevent progressive collapse. The following sections highlight the key elements that designers must consider when evaluating protective measures for a building's structural system.

The design team must determine which measures are appropriate and cost effective based on the acceptable level of protection and the available resources. The discussions presented herein cover basic principles of design; additional technical information for implementation can be found in the referenced documents. All designs must comply with all applicable Federal, State, and local codes.

3.3.1 Blast-Related Vulnerabilities

The study of effects of numerous bomb attacks against buildings during the past two decades has deepened the knowledge and understanding of the structural system's response to explosive blast. It points to a number of characteristics of structural systems, materials, and designs that contribute to poor building performance under blast loading. This section discusses the nature of these blast vulnerabilities.

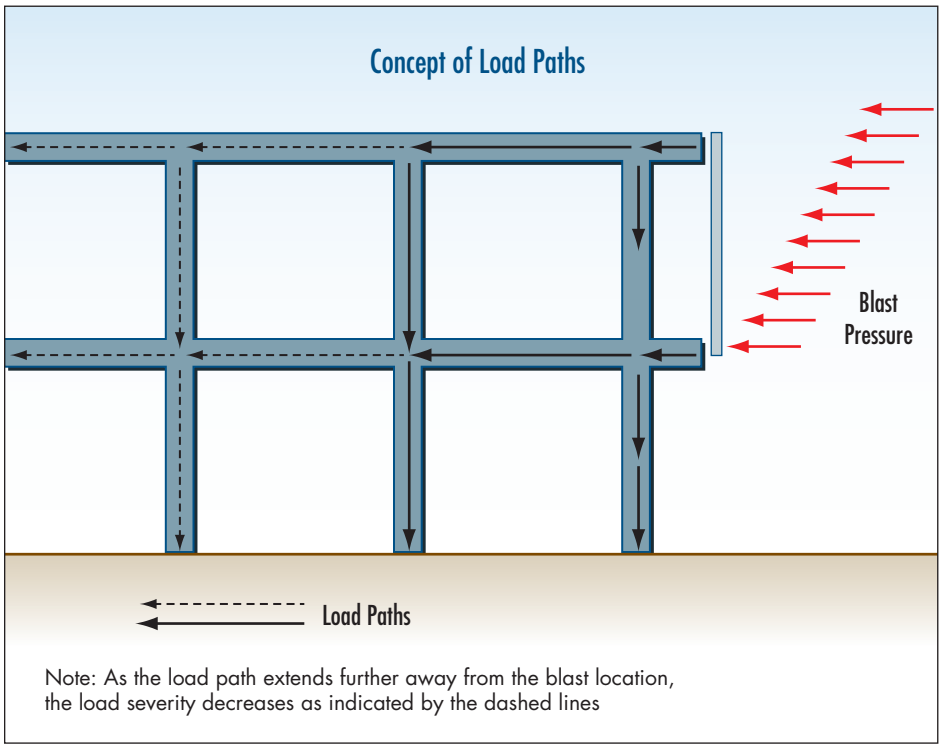
3.3.1.1 Lack of Redundancy and Indirect Load Paths

Structural systems that provide a continuous load path for all vertical and lateral loads acting on a building are highly desirable. A continuous load path ties all structural components together with connections

that should be capable of developing the full capacity of the members (all applied loads must eventually be transferred to the foundations and the vertical load path must be continuous from the uppermost structural component to the foundation). To provide comprehensive protection, the capacity of each component should be balanced with the capacity of all other components and the connection details that tie them together.

The calculated blast loads (from the design threat) should be applied to the exterior wall and roof surfaces to determine the design forces for the structural elements. The continuous load path carries the loads acting on a building's exterior façade and roof through the floor diaphragms to the gravity and lateral load-resisting systems (Figure 3-18).

Figure 3-18:
Concept of continuous load paths in buildings



Redundancy, also known as alternative load path, is another method of mitigating progressive collapse in the event of an explosive blast. Conceptually, it is based on designing several redundant load paths within the structural system so that when a particular load path fails, the other elements can continue to carry the load and prevent a structural failure. Figure 3-19 shows a structure (steel or concrete) with ductile moment connections. Such a structure has numerous load paths through the ductile moment connections. If one column in the structure fails, the loads will redistribute along the remaining (redundant) load paths and the structure will remain stable. Members and connections must be specifically designed to support the redistributed loads.

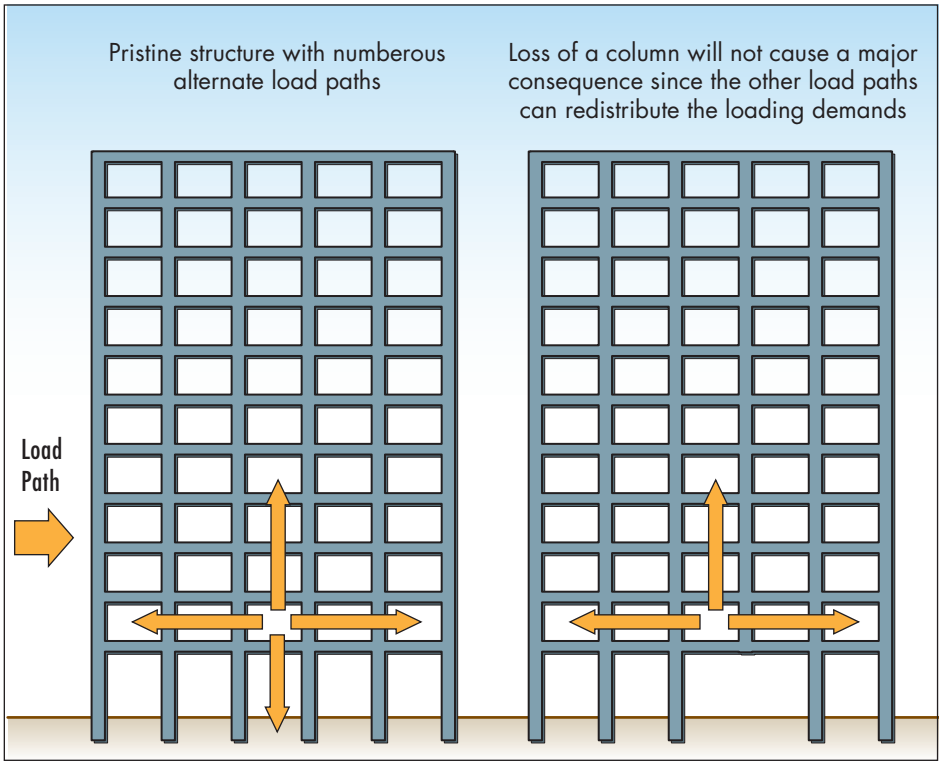


Figure 3-19: Redundancy in moment frame construction

Successful redundancy requires sufficient vertical supports to permit load transfer. Figure 3-20 shows a design with no redundancy; removal of any first floor column will initiate collapse.

Figure 3-21 shows the effect of connection types on building redundancy (top), a typical shear connection (left), and a fully rigid moment connection (right), as shown in the GSA's Progressive Collapse Guidelines (2003).

Redundancy provides multiple locations for yielding to occur, which increases the probability that damage will be constrained.

Increased redundancy is not easy to implement as a retrofit for existing buildings, because it often involves adding structural columns to reduce beam and girder spans. It can sometimes be more economical for new construction, but reducing column spacing may have undesirable functional effects. However, provision of adequate redundancy is the most effective means of limiting progressive collapse.

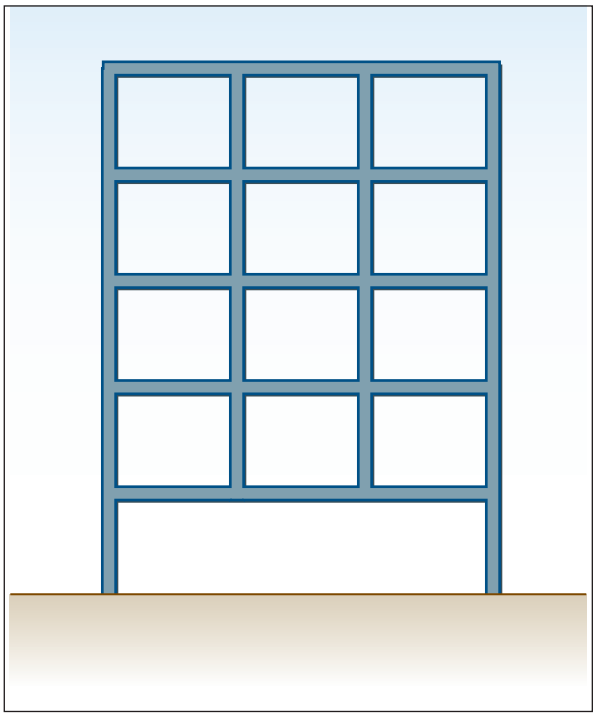


Figure 3-20: Structure with no redundancy

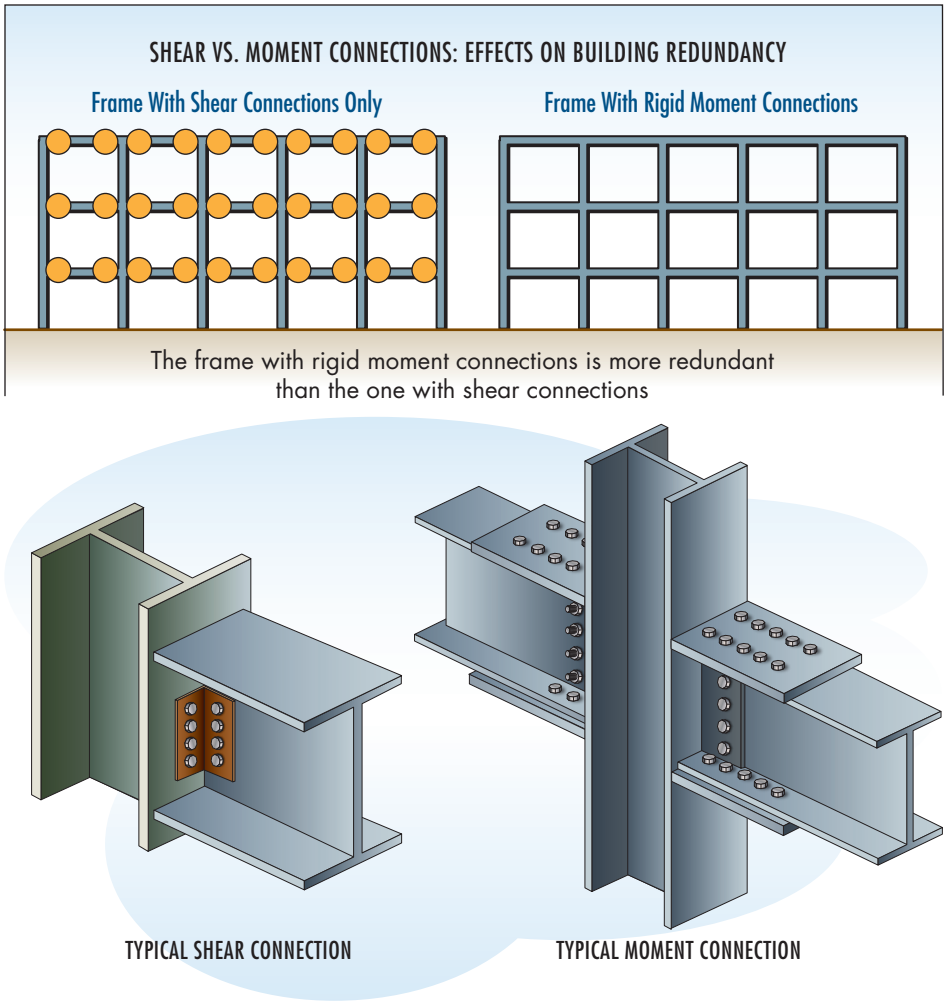


Figure 3-21:
Shear (left) versus moment (right) connections, effect on structural redundancy (top)

3.3.1.2 Lack of Ductility

Structural members and their connections may have to maintain their strength while experiencing large deformations in response to blast loading. Ductility refers to the characteristic of materials, such as steel, that can deform and continue to carry the load until the deformation reaches its limit. At the point of deformation, the material absorbs energy and defers absolute failure of the material. The material bends, but does not break, and so continues to resist forces and support loads, although with diminished effectiveness. Materials that are the opposite of ductile, such as unreinforced concrete, are called brittle. Figure 3-22 illustrates ductile behavior in a steel beam that deforms (deflects) with increasing load but continues to provide significant support until it finally breaks.

ductility (dəf-ə-)
Ductility refers to the characteristic of materials, such as steel, that can deform and continue to carry the load until the deformation reaches its limit.

The Khobar Towers complex in Saudi Arabia is one example of effective redundancy. The complex was attacked using a VBIED with an explosive equivalent of 20,000 pounds of TNT in 1996. The explosive device was delivered by a truck close to Building 131, an 8-story building that was built using precast concrete units. This structural system offered much higher redundancy than found in typical precast construction or conventional flat plate concrete systems, largely because the design followed a British code that incorporated requirements to prevent progressive collapse. The damage to the building was limited to the front façade, and the structural integrity was not compromised, mainly because the precast panels were adequately tied together.

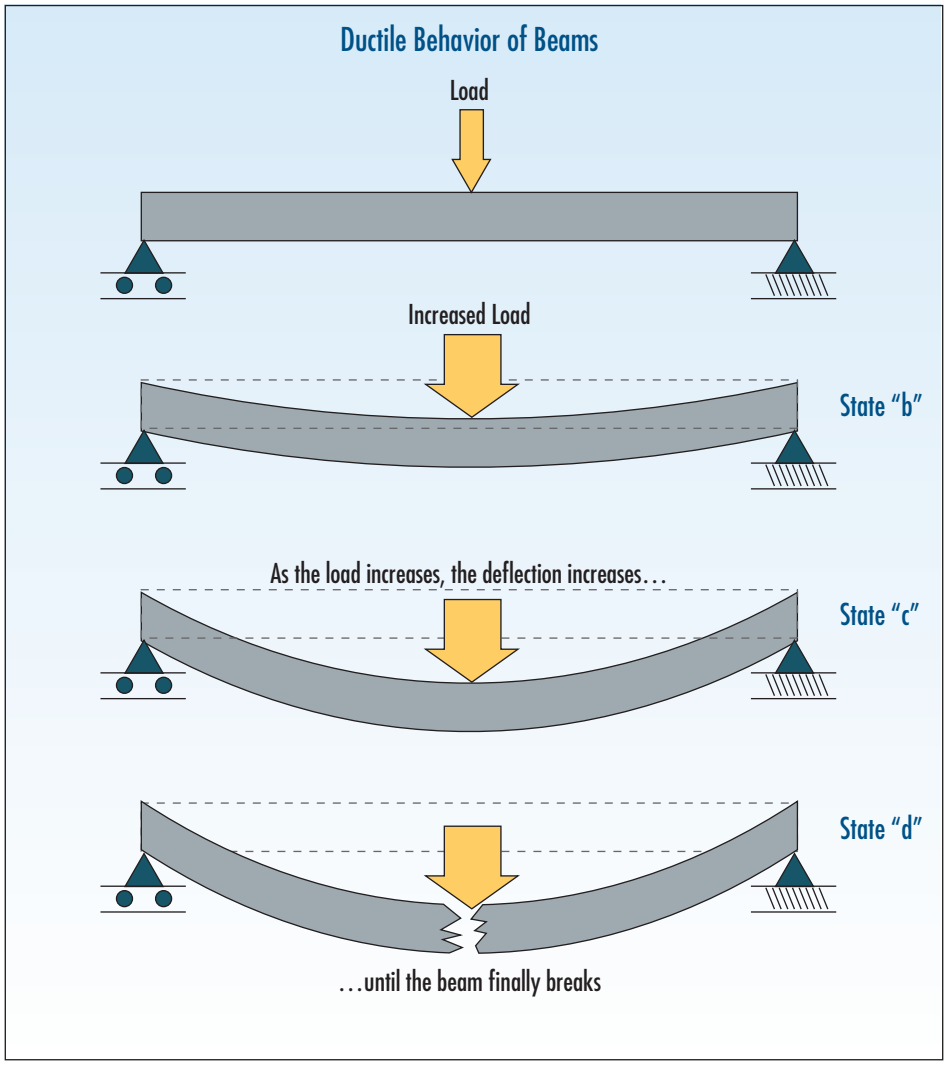


Figure 3-22:
Ductile behavior of a steel beam

URM and concrete are inherently brittle. Concrete members and connections can be detailed to achieve ductility by the use of specially designed steel reinforcing that involves increased density of steel reinforcement (compared to what is required to carry loads) and carefully controlled placement, as shown in Figure 3-23.

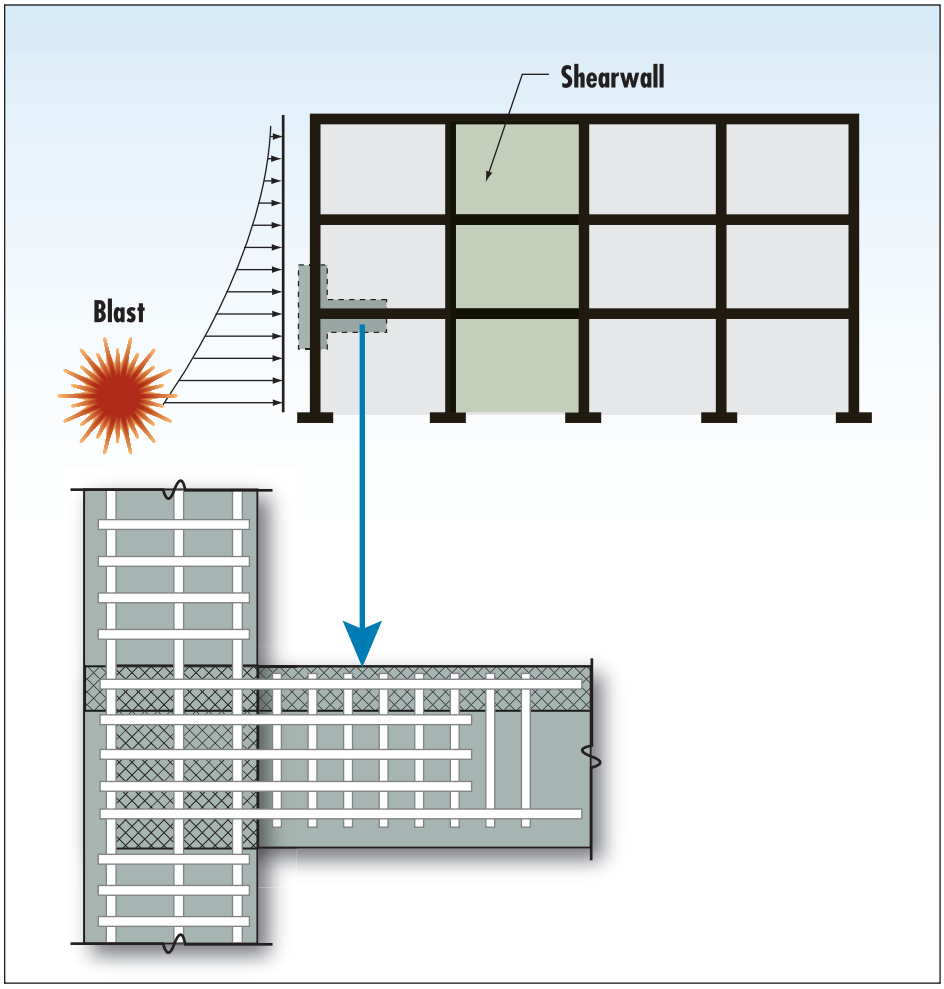


Figure 3-23:
Ductile detailing of connection in reinforced concrete structure; note the dense reinforcing in the vicinity of the connection

3.3.1.3 Load Reversals and Uplift

Floor slabs expose large tributary areas to uplift blast loads— for explosives detonated close to the building—that vary according to the resistance of the exterior façade and the height of the floor above the ground. To the extent that the exterior envelope resists the effects of an external detonation, the interior structure is isolated from the full intensity of infill pressure, which is the pressure that enters the building when the exterior façade fails. However, any floor may be subject to uplift loads from the interior detonation of a hand-carried satchel explosive.

Uplift forces and load reversals from explosives are typically applied contrary to the conventional design loads. Consequently, details should be incorporated that account for these contrary patterns on conventionally designed floor-slab connections (Figure 3-24). Although some construction materials are better suited to accommodate these loads, cast-in-place reinforced concrete, steel moment frames, reinforced masonry, and panelized construction can each be detailed to provide continuous load paths.

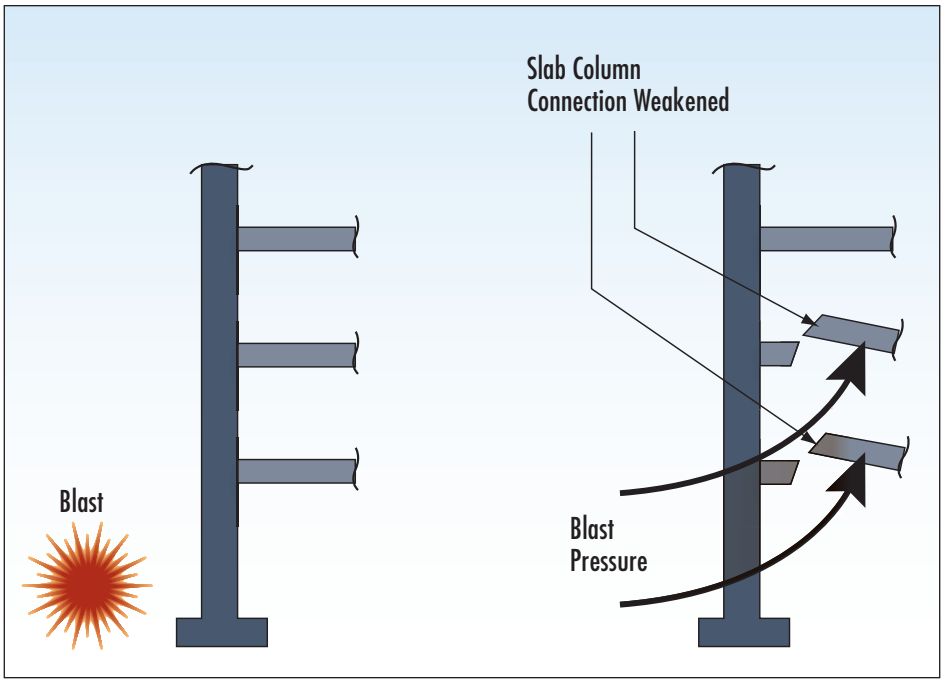


Figure 3-24:
Effects of uplift and load reversal

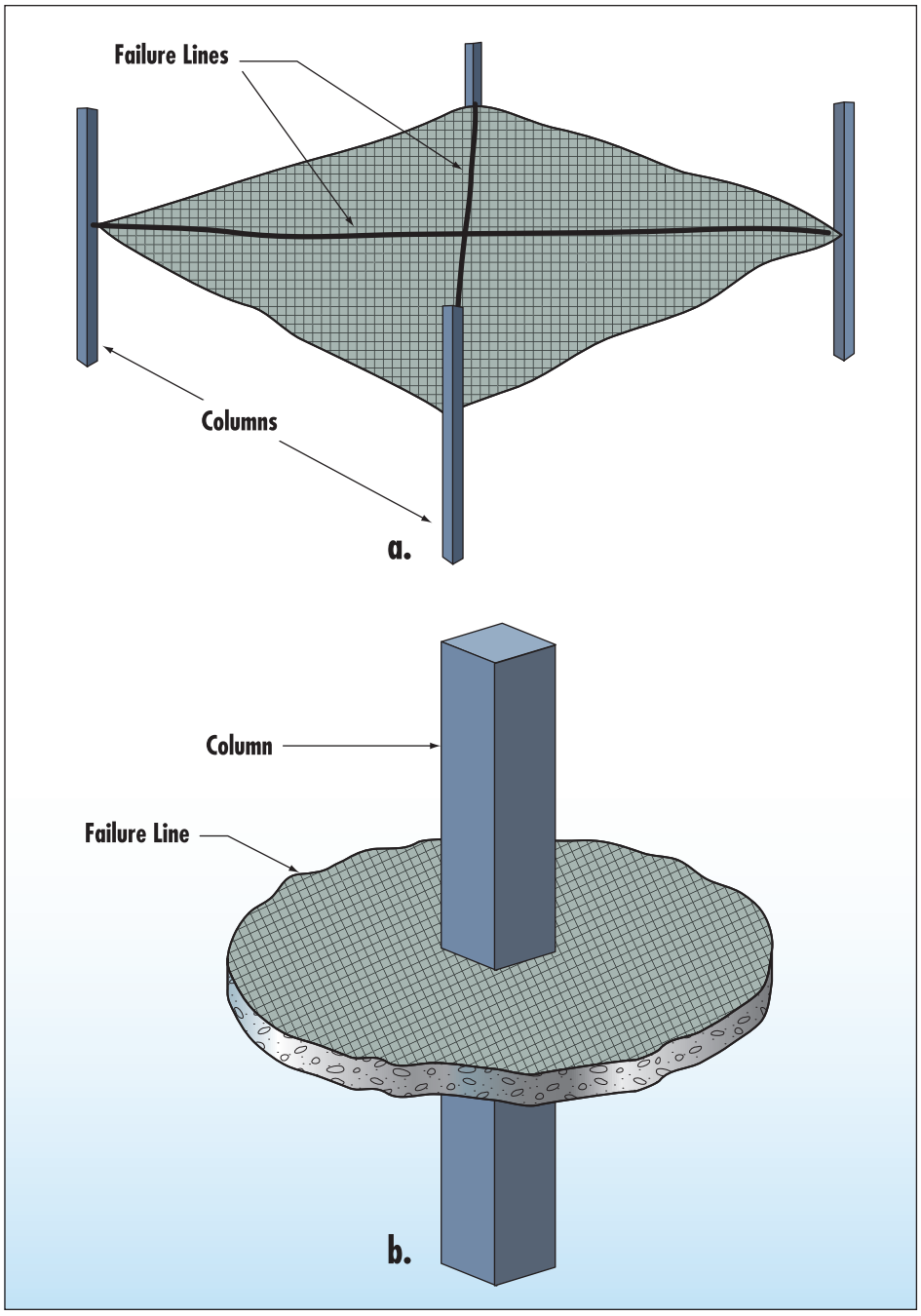
SOURCE: FEMA 453

Floor slabs are typically designed to resist downward gravitational loading and have limited capacity to resist uplift pressures or the upward deformations experienced during load reversals that may cause a flexural or punching shear failure (Figure 3-25). Therefore, floor slabs that could be subjected to uplift pressures, which may overcome the gravity loads and produce reversals in curvature, require additional reinforcement and robust connection to columns and beams. If the top portion of the slab does not contain tension reinforcement, an exterior application of glass fiber or carbon fiber reinforcing mats may be bonded to the top surface of the slab to strengthen the floors for upward loading at critical locations. This will reduce the likelihood of slab collapse from blast infill uplift pressures. An alternative approach is to notch grooves in the top of concrete slabs and epoxy carbon fiber rods into the grooves; although it is much more invasive, this approach may offer a greater load capacity.

Floor slabs are typically designed to resist downward gravitational loading and have limited capacity to resist uplift pressures or the upward deformations experienced during load reversals that may cause a flexural or punching shear failure.

Figure 3-25:
Flat slab failure mechanisms

SOURCE: FEMA 453



3.3.1.4 Transfer Girders

Transfer girders are typically long-span beams that interrupt the load path by supporting a discontinuous column above (Figure 3-26). Transfer girders may be used to span high volume areas such as a main lobbies, loading docks, or auditoria, often at the ground level of office buildings. For example, a two-story arcade around the outside of the building may have columns spaced at a greater distance than the columns above. Figure 3-27 illustrates a longer span required for clearance at a loading dock than for the office spaces above.

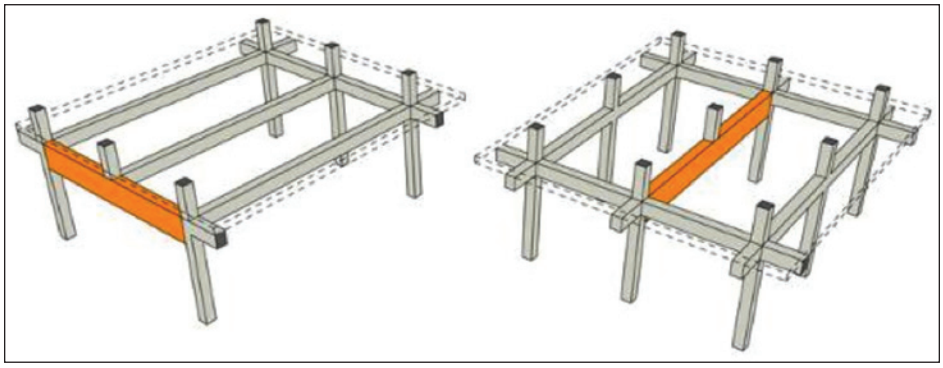


Figure 3-26:
Types of transfer girders: exterior girder supporting one column interrupting the load path (left); interior girder supporting one column interrupting the load path (right)

SOURCE: DAVID SHAFER

Figure 3-27:
Exterior transfer girder used to provide entry at loading dock

SOURCE: FEMA 455

Transfer girders that support several upper story floors require more attention (in terms of design and protection) than the girders that support only one floor. The failure of a transfer girder or a column supporting it could potentially initiate progressive collapse. Transfer girders and non-ductile, non-redundant construction may produce structural systems that are not resilient to localized damage. The columns that support transfer

girders and the transfer girders themselves may be critical to the stability of a large area of floor space.

The following represent some mitigation measures for transfer girders:

- Provide redundant load paths (additional bracing, for example).
- Design the girder, its connections, and its supports to accommodate the imposed loads.
- Increase setback distances, where possible, to reduce explosive loads.
- Conceal transfer girders and their supports, where possible, so that they are not obvious to a potential attacker.

3.3.1.5 Debris Impact

Debris impact may be minimal in response to a low- or moderate-intensity threat; however, façade materials may be locally overwhelmed, in response to a low-intensity short-standoff detonation, or generally overwhelmed, in response to a large-intensity long-standoff detonation. Airborne glass fragments typically cause penetration or laceration-type injuries. Larger fragments may cause non-penetrating, or blunt trauma, injuries. Finally, the air-blast pressures can cause occupants to be bodily thrown against objects or to fall. Lacerations due to high-velocity flying glass fragments have been responsible for a significant portion of the injuries received in explosion incidents. Although these injuries are serious, the building structure remains intact preventing the possibility of more injuries and fatalities.

3.3.2 Progressive Collapse and General Stability

The term "progressive collapse" is used to describe the spread of an initial load failure in a manner analogous to a chain reaction that leads to partial or total collapse of a building. The underlying characteristic of progressive collapse is that the final state of failure is disproportionately greater than the failure that initiated the collapse. General stability refers to the ability of the entire structure to resist collapse.

The term "progressive collapse" is used to describe the spread of an initial load failure in a manner analogous to a chain reaction that leads to partial or total collapse of a building.

The concept of progressive collapse can be illustrated by the collapse of WTC 7 as a result of the terrorist attacks on WTC 1 and 2 on 9/11 (see Figure 3-28). The structure was a 47-story office building located immediately to the north of the main WTC complex. The structure consisted of a steel frame to resist gravity loads and a perimeter moment frame and interior braced core to resist

lateral loads. Investigations suggest the impact of debris as a result of the collapse of WTC 1 caused structural damage and ignited fires on several floors. The fires on the floors spread uncontrollably because the automatic sprinkler system did not extinguish them and the firefighters lacked sufficient water supply. As the fire progressed, some of the structural steel began to heat, resulting in the loss of strength and stiffness. Buckling of critical interior columns initiated a cascade of local floor failures. As loads were redistributed, the entire building above the buckled region moved downward as a single unit in a progressive collapse. WTC 7 collapsed approximately 7 hours after fires started (U.S. Department of Commerce 2008).

The initiation and propagation of progressive collapse are diagrammed in Figure 3-29.

Figure 3-28: WTC 7 collapse

SOURCE: © 2001, ROBERTO RABANNE (FEMA 403)

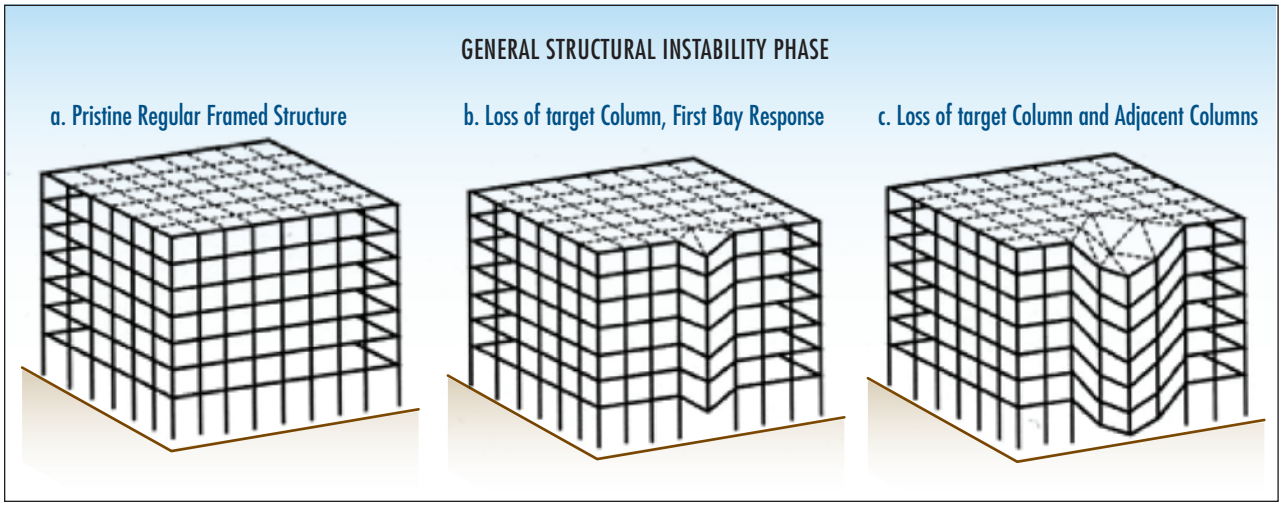


Figure 3-29: Initial phase of progressive collapse

The interrelationship between progression of collapse, component behavior, and general (overall) stable behavior is shown in figure 3-30. Note that to evaluate the potential for progressive collapse, the designer must account for both local component and general, or overall, stability behaviors of the building.

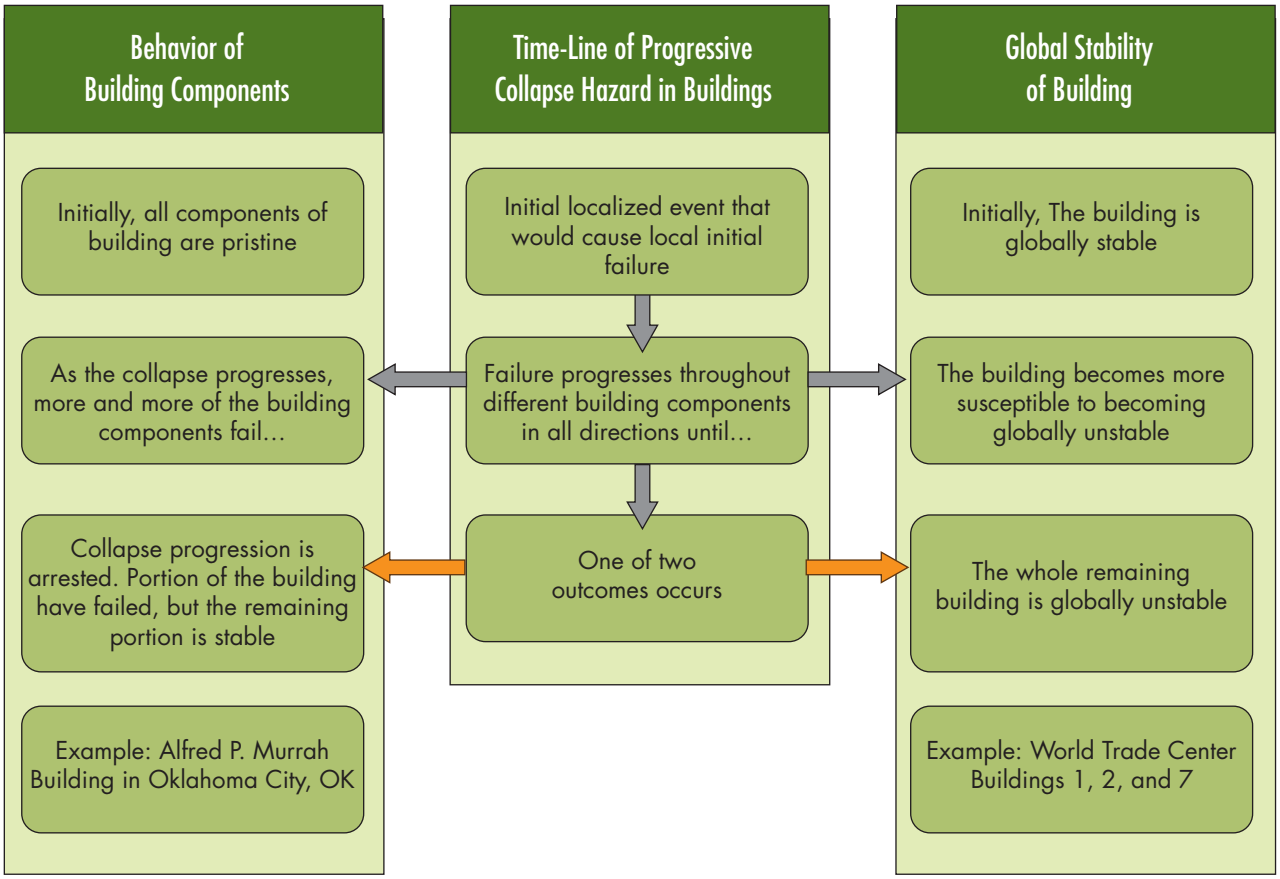


Figure 3-30: Local and general behaviors of a structure during progressive collapse

Table 3-3 summarizes structural system characteristics and their relationships to progressive collapse.

Table 3-3: Structural System Characteristics and Collapse Interactions

Structural System Considerations	Progressive Collapse Interaction
Weight	The controlling force during a progressive collapse event is gravity loads. Thus, the distribution of weight of the building can determine the extent of progressive collapse. The normal distribution of gravity-related stresses and strains should be considered in progressive collapse analysis and testing.
Load Path	Ensuring a continuous and adequate load path is a necessary mitigation technique to limit initiation and progression of collapse.
Redundancy	Adequate structural redundancy is a necessary mitigation technique to limit initiation and progression of collapse.
Tying/Bridging	Tying/bridging structural elements is a simple and inexpensive method for mitigating progressive collapse effects in certain conditions.
Ductility	Provision of ductile structural components (such as connections or beams) increases the structural capacity to resist the uncertainties of progressive collapse events.
Building Height	Progressive collapse tends to increase in severity with building height.
Transfer Girders	Presence of transfer girders tends to initiate or increase the extent of collapse progression.
Bearing Walls	Non-reinforced bearing masonry wall structures are susceptible to progressive collapse. Reinforced concrete or concrete masonry unit (CMU) bearing walls should be designed to provide direct load paths and redundancy.
Lateral Building Resistance	Lateral building structural systems (steel bracing, concrete shear walls, moment frames, etc.) assist in the provision of general structural stability. Such systems should be carefully designed to remain effective during and after progressive collapse events.
Columns	In structural frame systems, columns provide the major load path for gravity loads. Columns should be designed to enable an adequate number of columns to remain effective after an event to prevent progressive collapse.
Hardening/ Local Resistance	Hardening of structural components is another mitigation measure against direct blast pressures (which are local in nature). However, hardening a local component, like a column, may change the general structural characteristics, which may affect the overall structural stability.
Load Reversal/ Uplift	Any blast-related load reversal or uplift can affect the progression of collapse. Primary members and their connections should resist upward pressure.

The development of a standardized approach to reduce the risk of progressive collapse has been difficult because structures in many recent events have behaved differently, from the initial failure to the way in which the collapse spread and to the final results of the collapse. The irregular behavior of structures in progressive collapse distinguishes it from other well-defined structural engineering concerns such as gravity, wind, seismic, or vibration loads.

Two approaches are most frequently used to provide resistance to progressive collapse, namely the ***indirect method*** and the ***direct method***. The indirect method is a prescriptive approach of providing a minimum level of connectivity between various structural components with little additional structural analysis required by the designer. In place of calculations demonstrating the effects of abnormal loads on buildings, the designer may use the implicit approach, designing the building to incorporate measures that increase the overall robustness of the structure.

Two approaches are used to provide resistance to progressive collapse, namely the indirect method and the direct method.

The direct method, on the other hand, relies heavily on structural analysis. The designer explicitly considers the ability of the structure to resist the effects of an abnormal load event. Analysis of a building's resistance to progressive collapse can be performed using various methods, ranging from a linear elastic static analysis to sophisticated non-linear dynamic finite element analysis. The physics involved in the spread of a localized failure in a structure can be complex.

Both DOD and GSA take a threat-independent approach to protection against progressive collapse. The goal of a threat-independent approach is to control and stop the continuing spread of damage after localized damage or localized collapse has occurred, regardless of how that damage occurred. The GSA P100, Facilities Standards for the Public Buildings Service (2005), states that columns should be able to span two stories unbraced to resist progressive collapse. For parking garages of two or more levels, GSA requires the design to carry the load for three stories unbraced by floor connections.

GSA and DOD require that the structural response of a building be analyzed to verify its performance following the removal of a key structural element (e.g., vertical load carrying column, section of bearing wall, beam). When effective alternate load paths are available to redistribute the loads originally supported by the removed structural element, the building has a low potential for progressive collapse.

The 1995 VBIED attack on the Murrah Federal Building in Oklahoma City provided an important lesson with regard to progressive collapse and structural stability. The explosion destroyed a first floor column, approximately 16 feet (5 meters) from the detonation, which supported a 40 foot(12-meter) long transfer girder on the front of the building. Failure of the transfer girder, in turn, caused the failure of two adjacent columns triggering progressive collapse and the destruction of most of the front of the building.

The attack on the Murrah Federal Building in Oklahoma City provided an important lesson with regard to progressive collapse and structural stability.

Even with these column losses, the two ends and the back of the building remained almost intact, precluding a total building collapse that would have resulted in additional loss of life and injuries. The building experienced only partial collapse because the structural system was designed with two massive shear walls—at the two far ends of the building—to provide its general stability (in addition to ensuring resistance to lateral wind forces). The survival of these shear walls permitted a good portion of the building to survive (Figure 3-31).

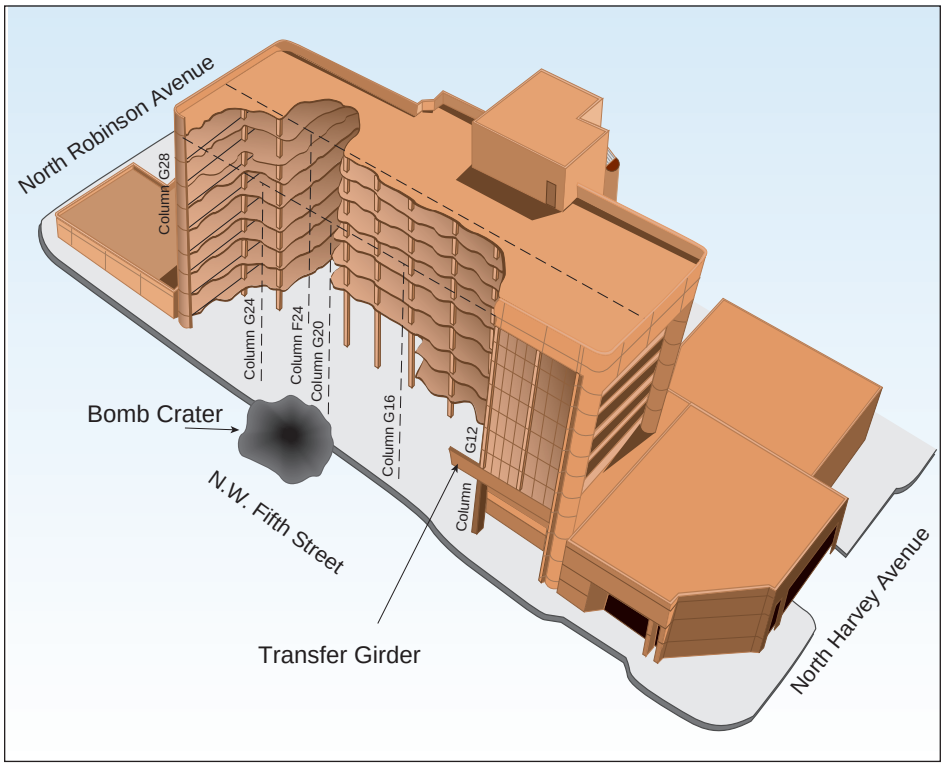


Figure 3-31:
Murrah Building, Oklahoma City: After the attack, a portion of the front of the building suffered progressive collapse; however, the bulk of the building survived because of the massive shear walls at each end.

SOURCE: FEMA 277

An important means of resisting progressive collapse and providing for general stability is to design all structural elements to be securely connected or tied together. Different guidelines prescribe different details and design requirements to accomplish this objective and provide details for bridging/linking of the structural elements. The DOD UFC 4-023-03, *Design of Buildings to Resist Progressive Collapse* (2010), covers this topic in detail. As a retrofit measure to improve performance, tying connections is relatively simple and inexpensive for small buildings subject to low threat levels when the structural members and their connections are easily accessible. For large buildings, with a large number of connections and often limited accessibility, retrofit is difficult.

Stabilization of Buildings

DHS S&T is conducting research and developing tools to assess the stabilization of damaged structures. When a building is damaged by an explosive device, it can become vulnerable to progressive collapse; failure can occur with little or no warning. Police, fire, and emergency medical technicians (i.e., first responders) are the first groups to arrive at the disaster scene. They need immediate critical information about the damage to make informed decisions about how to stabilize the building to minimize additional loss of life. This project is being executed by various research institutions and universities. The goal is to create cutting edge sensing and monitoring, general risk assessment, secondary and brittle failure assessment, and stabilization tools.

The project comprises four major areas:

- Monitoring, sensing, and modeling directed at capturing the state-of-the-art and knowledge gaps in monitoring and sensing technologies and modes of failure caused by explosive blast
- Development of a building information modeling standard for first responders to store major building information related to hot points, secondary collapses, and debris accumulation and direction
- Preparation of post-disaster risk assessment and decisionmaking tools and guidelines to facilitate the risk assessment and decision making process for first responders
- Building stabilization technologies and testing directed at identifying innovative stabilization techniques and materials for different building types after an explosive blast event

3.3.3 Materials and Systems

Reinforced concrete and steel are the two materials often used in construction of the supporting structure of buildings. Reinforced concrete is also used in the form of frames and walls, which, in conjunction with glazing, may provide the exterior envelope and nonstructural elements of a building (Figure 3-32).

Figure 3-32:
Reinforced concrete building exteriors: exterior concrete structural walls provide exterior envelope (left); reinforced concrete frame structure with nonstructural elements form the envelope (right)

Steel is used in the form of frames; the nonstructural elements and the exterior envelope are constructed with other materials. Steel is used in three basic frame systems.

1. Moment-resistant frames, in which lateral resistance is provided by specially detailed beam/column connections (Figure 3-33).

Figure 3-33:
Moment-resistant steel frame structure

Figure 3-34: Exposed steel braced frame

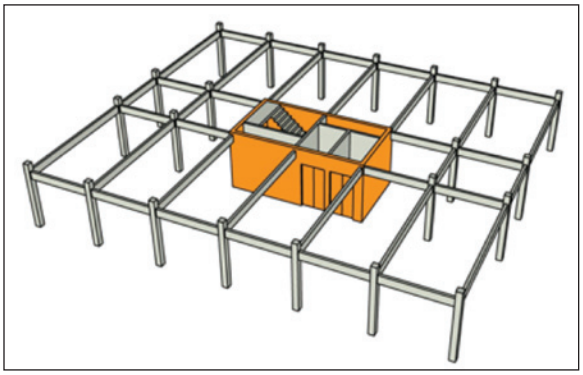


Figure 3-35:
Steel frame with core system; the strong central core resists seismic and wind forces
SOURCE: DAVID SHAFER

2. Braced frames, in which diagonal steel bracing members provide lateral resistance; braces may be concealed within the exterior envelope or exposed (Figure 3-34).
3. Simple steel frames, in which lateral bracing is provided by a structural core that contains elevators, vertical ducts, and staircases and is constructed with steel or reinforced concrete. Steel frame connections carry no lateral loads and are simply detailed (Figure 3-35).

3.3.3.1 Reinforced Concrete Construction

Cast-in-place ductile reinforced concrete is frequently used for blast resistant construction. It has significant mass, which improves its response to explosions and members can be readily proportioned and reinforced for ductile behavior. Reinforced concrete construction provides continuity between the members. Historically, reinforced concrete has been used for military bunkers, and the military has performed extensive research and testing of its performance.

Non-ductile concrete design may perform badly in response to blasts, as was witnessed by the collapse of the Alfred P. Murrah Building in Oklahoma City. This is why ductility is of utmost importance in structural design for blast resilience.

Blast-resilient design incorporating ductile reinforced concrete should exhibit the following attributes:

- Walls should span from floor to floor rather than from column to column.
- Splices should be staggered away from high-stress areas.
- Reinforcing bars should be spaced no more than one wall thickness apart, and no less than one-half the wall thickness apart.
- Special ductile seismic-type detailing should be used at connections.
- Development lengths should be used to develop the ultimate flexural capacity of the section.

- Ties should be closely spaced along the entire length of beams, spirally reinforced columns, and connections with a minimum bend angle of 135 degrees with spacing not exceeding d/2 (where d represents the distance from compression face to tension reinforcement).
- Design for preventing progressive collapse should consider a scenario in which an exterior wall measuring vertically one floor height and laterally one bay width is lost.

Ductile design allows the reinforced concrete members to sustain large deformations and reversals of loads. Additionally, concrete structural elements are typically more massive than their steel frame counterparts. The high inertial resistance as well as the continuity of cast-in-place construction assists in sustaining the high intensity and short duration effects of close-in explosions.

3.3.3.2 Poured-in-place Concrete Frames and Walls

Poured-in place reinforced concrete walls and frames are erected on the site. Concrete is poured into the formwork, generally wood or metal, from mobile equipment, the concrete is allowed to set, and the forms are removed. The formwork can provide a finished surface to the concrete or additional finish materials such as paint stucco, tile, or stone can be applied to a concrete surface created by simpler formwork. Concrete frames and walls are often used in the same overall structure.

Blast-resistant design incorporating poured-in-place reinforced concrete should exhibit the following attributes:

- Both faces should have symmetrical reinforcement.
- Walls should span from floor to floor rather than from column to column.
- Steel reinforcing splices should be staggered away from high-stress areas.
- The size and spacing of reinforcing bars should correspond to the demands of the design basis threat.
- Special seismic-type ductile detailing should be used at connections.
- Development lengths should be used to develop the ultimate flexural capacity of the section.
- Ties should be closely spaced along the entire length of beams, spirally reinforced columns, and connections with a minimum bend angle of 135 degrees with spacing not exceeding d/2.

Performance criteria for poured-in-place concrete exterior walls are developed to satisfy the structural integrity requirements of the building under specified blast conditions. These structural elements are designed to resist the blast loads but are not limited to specific levels of peak pressure or impulse. The corresponding level of damage and deformation that these shear wall elements may be permitted to sustain are considerably lower than the level of damage and deformation permitted for façade components.

The exterior walls are subject to direct reflected pressures from an explosive blast located directly across from the secured perimeter line. The objective of design, at a minimum, is to enable these members to fail in a ductile mode, such as flexure, rather than a brittle mode, such as shear. The walls also need to be able to resist the loads transmitted by blast resistant windows and doors and special reinforcing and anchors must be provided around their frames.

3.3.3.3 Precast and Prestressed Concrete Frame Systems

Precast and prestressed concrete frame systems are typically used in urban residential construction.

Panelized precast concrete systems can be detailed to permit significant deformations in response to blast loading, as demonstrated by the performance of Khobar Towers military housing, Dhahran, Saudi Arabia, during a large VBIED attack in 1996. The prefabricated concrete structure with bolted connections was designed to British standards for blast-resistant structures (Figure 3-36).

Performance criteria for poured-in-place concrete exterior walls are developed to satisfy the structural integrity requirements of the building under specified blast conditions.

Figure 3-36:
Khobar Towers, Dhahran, Saudi Arabia, 1996

Unlike the Khobar Towers design, precast panels are typically supported at the ends unless they span over multiple floors and the panels are not bolted together. The connection details for the precast panels should be designed with sufficient strength and ductility to resist both the direct blast loads in bearing (compression) and the subsequent rebound effects in tension.

Precast Wall Panels

All design should be carefully analyzed according to a calculated blast load. The minimum thickness of a precast wall panel should be 5 inches with two-way reinforcing bars sized and spaced accordingly. Because precast panels are poured flat, two-way reinforcement is needed for handling during shipping and installation to prevent cracking and other damage. Alternatively, precast sandwich wall panels may be designed with a minimum wythe thickness of 3 inches, and reinforced according to demand appropriate for fascia wythes, structural wythes, and both wythes of structurally composite sandwich wall panels. Connections into the structure should provide a straight line of load transmittal, using as few connecting pieces as possible. The connection design should reduce the loads transmitted into the connections, accommodate the flexure of the panels based on demand, and enable the connections to resist uplift and rebound effects. With well-designed ductile connections, the designer can take advantage of the normally improved materials and quality control found in precast as compared to cast-in-place concrete.

Pre-tensioned and post-tensioned construction concrete and seated connection systems may provide little resistance to upward forces, load reversals, or abnormal loading patterns. However, design of the cable profile may improve capacity for these abnormal loads and reinforcing bars may be added to the design to improve blast-resilient performance.

3.3.3.4 Reinforced Concrete Masonry Units

Reinforced CMUs are commonly used for the load-bearing walls of buildings. Fully grouted and reinforced (CMU) façades can provide effective protection against blast loads. Solid grouted 8-inch (20-centimeter) CMU walls with No. 5 vertical reinforcement at 48 inches (1.2 meters) on center and W1.7 (9 gage) horizontal joint reinforcement 16 inches (41 centimeters) on center demonstrated good ductility and blast resistance under full-scale blast load tests at the Air Force Research Laboratory in 2008. Therefore, fully grouted 8-inch (20-centimeter) block walls with vertically-centered reinforcing bars placed in each cell (or every other cell) and with horizontal reinforcement at each layer will provide considerable resistance to blast loading. Even greater blast resilience is achieved using fully-grouted 12-inch (30-centimeter) block walls with two layers of reinforcement. However, the walls must be detailed to transfer the reaction forces to the floor slabs. Although load-bearing masonry walls are typically continuous between floors in modern construction, detailing is problematic for the connection at the top of an infill wall inside the structural framework of the building.

Masonry is considered a very brittle material that may generate highly hazardous flying debris in the event of an explosion and is generally discouraged for new construction.

Brick or stone veneer does not appreciably increase the strength of the CMU wall, but the added mass increases its inertial resistance. A consideration in double wythe walls (brick or stone wall exterior/air gap/CMU wall interior) is ensuring both wythes are tied together to act as a single unit during blast events. Alternatively, filling the air gap with insulation, such as vermiculite, can provide some interaction. When the wythes act as one unit, their individual resistance to blast loading is cumulative.

Brick load-bearing walls resist blast mostly through mass; thus, thicker solid walls (on the order of 18 inches [46 centimeters]) can perform well at pressure levels less than 10 psi. Brick walls with dynamic structural response are analyzed using a kinematic model with bearing providing resistance at the hinge points.

Masonry is considered a very brittle material that may generate highly hazardous flying debris in the event of an explosion and is generally discouraged for new construction.

3.3.3.5 Unreinforced Masonry

URM walls have been prohibited for new construction where protection against explosive threats is required, because URM provides very limited protection against explosive blast. When subjected to overload from air blast, brittle URM walls will fail and the debris will be propelled into the interior of the structure, possibly causing severe injuries or death.

URM bearing walls may be encountered in older buildings, particularly historic structures, where cast iron columns were used in the building interior and URM bearing walls on the exterior. Toward the end of the 19th century, the complete steel frame was introduced, and URM was commonly used as infill in these early steel framed structures. For important buildings, rough brick infill was often installed as backing for finished masonry, such that monumental buildings constructed as late as the 1940s continued to have the appearance of masonry structures because the steel frame was not visible (Figure 3-37).

Figure 3-37:
Mills Building, San Francisco, 1891, steel frame with URM infill

SOURCE: FEMA 454

A common method of upgrading URM structural walls is an application of shotcrete (also known as gunite), a liquid concrete mix sprayed onto the wall over welded wire fabric that creates a reinforced concrete/masonry wall. This method provides tensile capacity to the existing wall and limits the amount of debris that might be propelled into the protected space.

URM and unreinforced CMU walls may also be retrofitted with a sprayed-on polymer coating (similar to truck-bed liner) to improve their air blast resistance. This innovative retrofit technique takes advantage of the toughness and resiliency of modern polymer materials to effectively deform and dissipate the blast energy while containing the shattered wall fragments.

In lieu of the polymer, an aramid (geotextile) debris catching system may be attached to the structure by means of plates bolted through the floor and ceiling slabs (Figure 3-38). Similar to the polymer retrofit, the aramid layer does not strengthen the wall; instead, it restrains the debris that would otherwise be hurled into the occupied spaces.

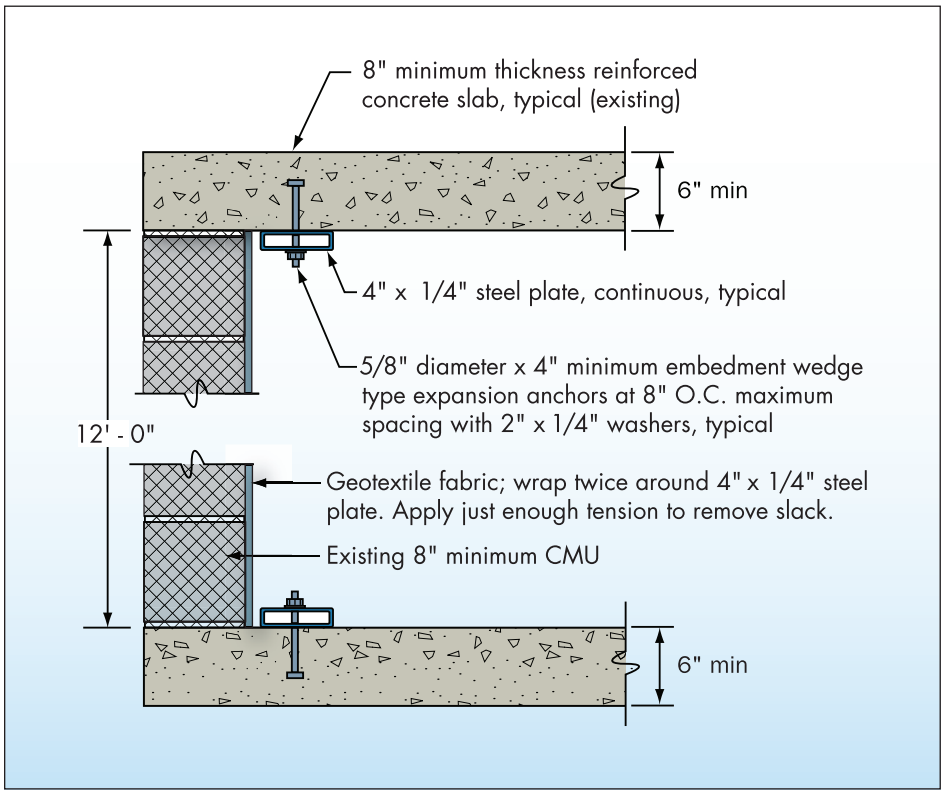


Figure 3-38: Geotextile debris-catching system

SOURCE: FEMA 453

Load bearing URM walls generally require additional strengthening to prevent the initiation of a catastrophic progressive collapse. Therefore, the fragment protection provided by a spray on elasto-polymer, a fabric spall shield, or a metal panel may have to be supplemented with structural supports, generally steel tube columns, capable of resisting lateral loads and transferring of axial forces. A typical example uses stiffened panels of steel plates to catch the debris and welded tube columns spaced approximately 3 feet (0.9 meter) on center to supplement the gravity load carrying capacity of the bearing walls. The steel tubes are connected

to the existing floor and ceiling slabs by means of base anchor bolt connectors, and similar vertical steel sections may also be installed up against existing walls to reduce the floor spans and provide additional load transfer from the floor diaphragms.

3.3.3.6 Steel Frame Systems

Steel frame systems are used for the construction of a variety of building types but are typically used in high-rise buildings. Steel is an inherently ductile material capable of sustaining large deformations. Steel structural systems should be detailed to take advantage of this inherent ductility, and connections should be designed to provide continuity between members.

Steel frame systems are used for the construction of a variety of building types but are typically used in high-rise buildings.

The typically efficient and economical thin-flanged sections used in conventional steel frame construction make it vulnerable to localized damage. Complex stress combinations and concentrations may occur and cause localized distress and prevent the section from providing its ultimate strength. Concrete encased flanged sections may be used to protect the thin-flanged sections and supplement the inertial resistance, with the additional advantage of providing effective fireproofing. Concrete encasement should extend a minimum of 4 inches (10 centimeters) beyond the width and depth of the steel flanges.

Steelwork is generally better suited to resist the relatively low-intensity, but long-duration, effects of explosions at a long-distance standoff. Steel structures may experience significant rebound because of their flexibility and must be designed to support significant reversals of loading.

Floors are typically constructed of concrete applied over metal decking. Metal deck construction provides a spall shield to the underside of the slabs, which gives additional protection to a near-contact satchel explosive placed on a floor. However, an internal explosive blast load will also load the ceiling slabs from beneath and the beams should contain an ample number of studs, far exceeding the requirements for conventional gravity design, to transfer the slab reactions to the steel supports. When the slabs are adequately connected to the steel framing members, these beams will be subjected to abnormal reversals of curvature that will subject the mid-span bottom flanges to transient compressive stress and may induce a localized buckling. Because blast loads are transient, the dominant gravity loads eventually restore the mid-span bottom flange to tension; however, unless the flange is adequately braced, the transient buckling will produce localized damage.

Concrete encasement of steel beams also provides torsional resistance to the cross-section and minimizes the need for intermediate bracing. When the depth of the composite section is minimized by embedding the steel section into the thickness of the floor slab, the slab reinforcement should either be welded to the webs or run through holes drilled into the webs to maintain continuity. All welding of reinforcing steel should be in accordance with seismic detailing to prevent brittle failures.

Steel columns require full-moment splices. To take full advantage of the steel capacity and dissipate the greatest amount of energy through ductile inelastic deformation, the beam-to-column connections should be capable of developing the plastic flexural capacity of the members. Connection details, similar to those used in seismic regions, will be required to develop the corresponding flexural and shear capacity (Figure 3-39).

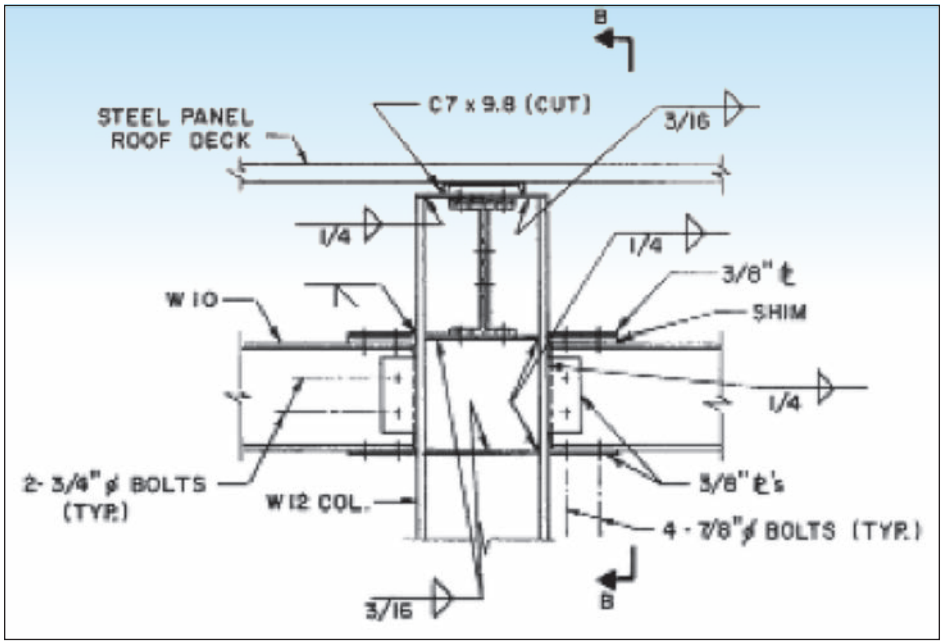
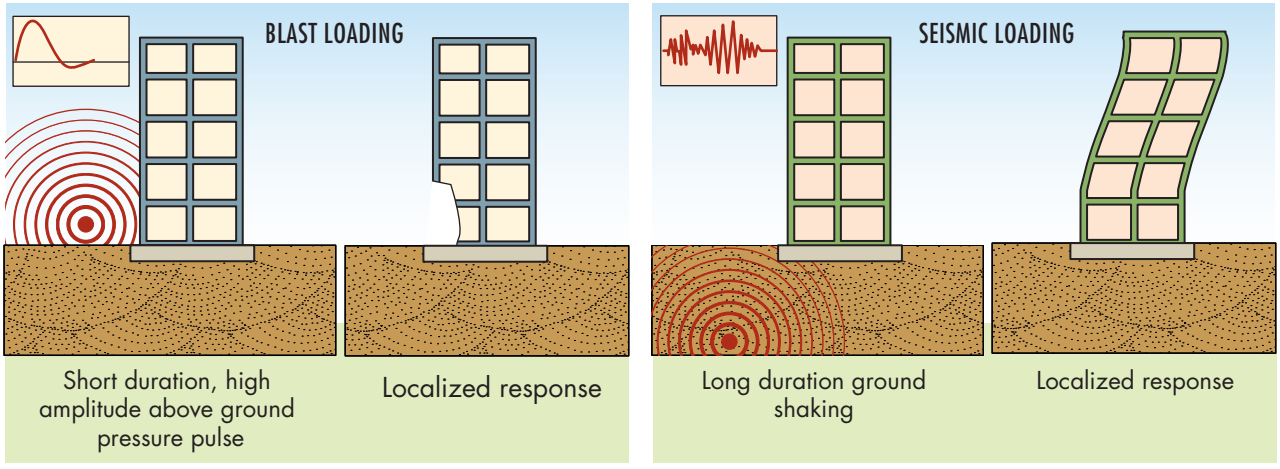


Figure 3-39:
Typical steel frame detail at column: comparisons of blast and seismic loading (top) and the structural response (bottom)

SOURCE: FEMA 453



Seismic versus Blast Protection

The nature of blast loading is quite different from the loading created by earthquake ground motion. Blast loading is of very high intensity, very localized, and lasts only milliseconds. Earthquake loading is of lesser intensity, distributed throughout the entire structure, and lasts from a number of seconds to over a minute, in some instances.

Many features of seismic design for high seismic zones, such as the emphasis on ductility in member and connection design and providing redundancy, are equally desirable in blast design. The high level of reinforcement at ductile connections designed to withstand seismic forces is particularly applicable to blast-resilient design.

Other features of seismic and blast design are less compatible. For example, hardening of columns at lower levels of buildings to resist blast pressures can result in considerable vertical irregularities that may have negative effects on the seismic behavior of the structure. These potentially conflicting demands must be considered when designing buildings for both blast and seismic resistance.

3.3.4 Structural Retrofit

Structural hardening, or the provision of localized improved resistance, is intended to enable specific structural components to meet the calculated blast loads. For example, if a particular column or set of columns in the structural system is vulnerable to the design basis threat, the retrofit for the column would be designed to resist that particular threat (Figure 3-40).

This method of providing localized improved resistance is particularly useful for retrofitting existing structures, where renovating the entire structure may be cost prohibitive or unnecessary. Although analyzing the threat and vulnerability and designing a hardening retrofit are relatively simple, the space limitations of the current layout or conditions make the implementation of the retrofit difficult and costly.

The benefits of localized resistance were observed after the 1993 bombing of the WTC, when a 1,500-pound (680-kilogram) van bomb exploded in the parking garage under Tower 1. The bomb destroyed one floor at the concourse level and six floors of the underground garage, leaving columns without any lateral support over a height of

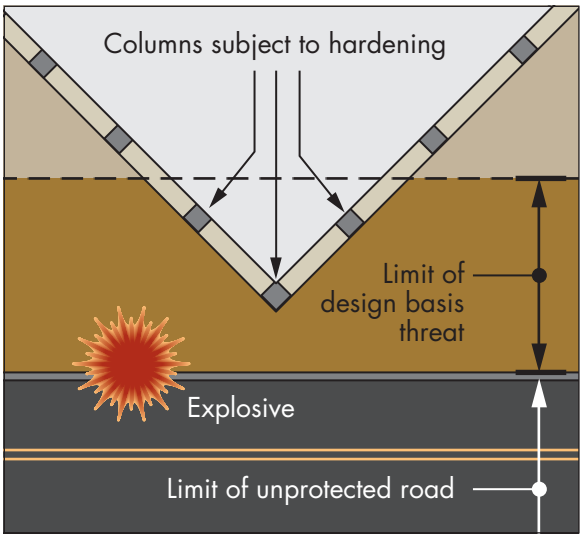


Figure 3-40:
General concept of hardening (provision of improved local resistance)

three stories. Fortunately, these columns did not buckle. The unusually large tower columns were designed to resist large vertical load demands and were able to resist the lateral blast loading. Thus the built-in local resistance of the Tower 1 structure helped to avert the loss of those columns and possible progressive collapse. The concept is shown in Figure 3-41.

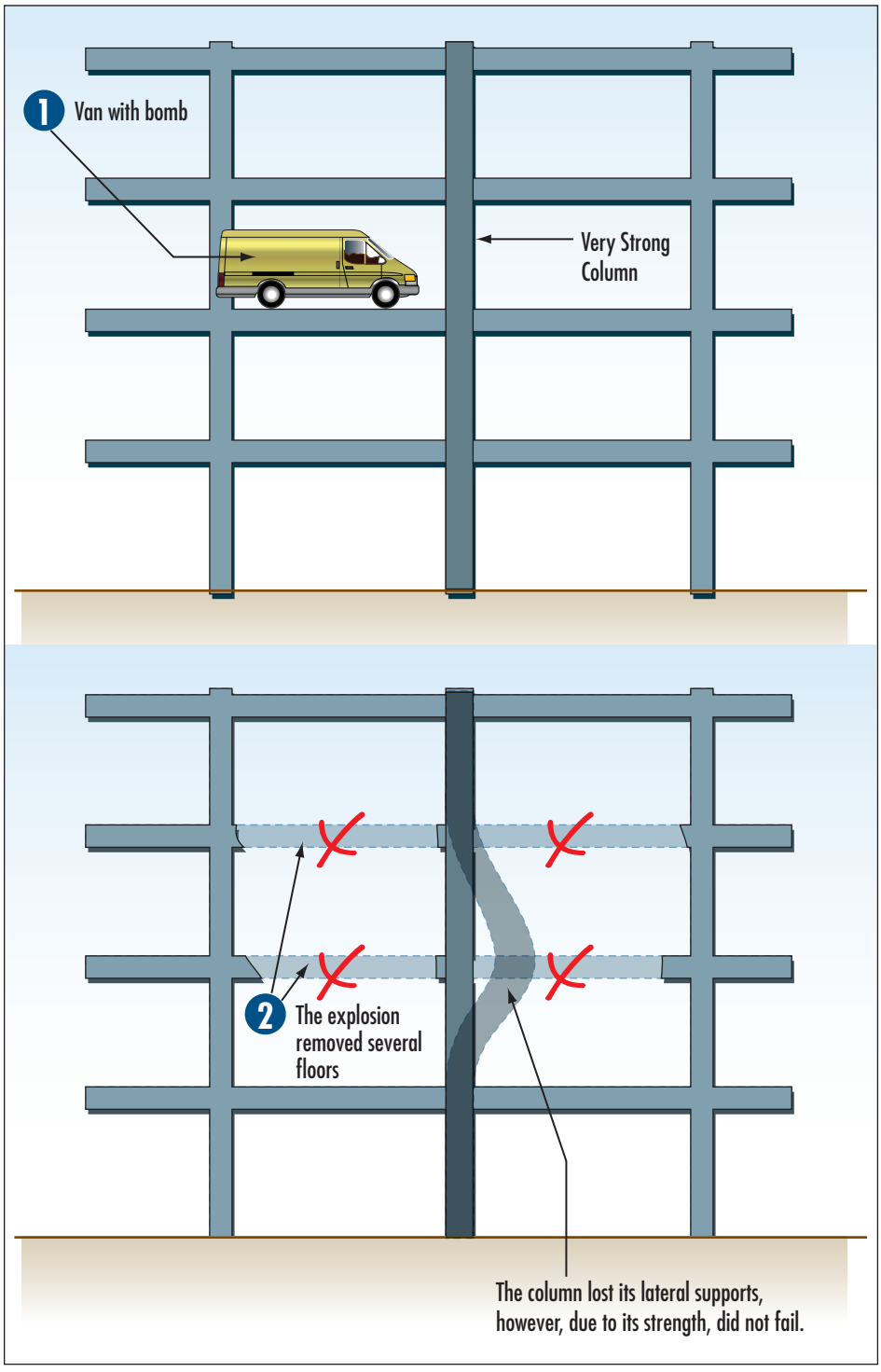


Figure 3-41:
Strong column benefits during WTC 1 bombing 1993

The vulnerability to blast loading of columns such as those in the Tower 1, which were accessible to anyone, depends also upon the tributary area and number of floors that the column supports. The slenderness (diameter in relation to the height) of the column is also significant; steel columns tend to be slender, and reinforced concrete columns tend to be massive (Figure 3-42).

Figure 3-42:
Exposed perimeter column (left), exposed columns supporting end of building (right)

Air-blast loads on columns are limited by clear-time effects in which the blast wave quickly clears the free edges and reduces the peak reflected pressure on the column. Round columns are more effective than rectangular or square columns in clearing the blast wave and reducing the reflected pressure. However, explosions in close proximity to columns may produce large inelastic flexural deformations that could initiate induced instabilities, where the drift (deviation from the vertical caused by lateral forces) on a column carrying a large downward load becomes too great and the column fails.

Nonstructural elements spaced around columns (particularly slender steel members), in the form of decorative casings, may be designed to increase the minimum standoff distance. The GSA recommends a thickness of 6 inches (15 centimeters) for casings. However, this local standoff from the casing alone may not be sufficient. Additional resistance may be provided to reinforced concrete structures by means of a steel jacket or a carbon fiber wrap that effectively confines the concrete core, thereby increasing the confined strength and shear capacity of the column and holding the rubble together to enable it to continue carrying the axial loads.

The capacity of steel-flanged columns may be increased with reinforced concrete encasements that add mass to the steel section and protect the relatively thin flange sections. The retrofit should be designed to resist the design explosive threat at the available standoff distance.

3.4 Building Envelope

The building envelope comprises the elements that separate the interior of a building from the outdoor environment. The building envelope is a critical set of building components because it separates the occupants, contents, and functions inside the building from the effects of explosive blast outside the building. This section focuses on the most important building envelope elements: the exterior façade, composed of glazed and opaque systems and roof structures.

Benefits of Envelope (or Façade) Retrofits

Perhaps the best example of façade retrofit benefits is the performance of the Pentagon window retrofits, in which the historic windows were replaced with steel frame replicas containing laminated glass and were anchored to steel H-Frames at floor and ceiling slabs. The masonry walls were backed by debris mitigating materials that inhibited the trajectory of debris. Although these protective upgrades were designed and detailed to resist specified blast load intensities, they performed admirably well in response to the aircraft impact on 9/11. The zone of aircraft impact straddled the retrofitted façade and un-retrofitted façade, which allowed for a direct comparison. The protected façade significantly reduced the extent of debris and enabled occupants to walk away from their workstations uninjured. The serendipitous benefit of the blast-resistant façade in response to the aircraft impact further demonstrates the benefits of ductile design and the use of debris-mitigating materials.

3.4.1 Vulnerabilities

In an explosion near a building, the building envelope receives the blast loading and transfers it to the supporting structural frame. The load is transferred to the supporting members only insofar as the façade system is able to resist such a load. For a wide range of design blast loads, lighter systems may be preferable for reducing adverse blast effects, if they are designed to be ductile, redundant, and balanced. By accepting some permanent damage to the exterior envelope, lighter, more cost-effective, systems can be designed that absorb energy through deformation and transmit lower forces into the connections and supporting structure, thus reducing the potential for more serious structural failures. Heavy façades may offer greater resistance to blast loading, and can transfer

significantly larger loads into the supporting structure behind the envelope, but they may be more prone to brittle failure if not properly detailed. An overly stiff or strong façade may actually be detrimental to the overall structural system response. In general, building envelope resistance to blast loads should be designed in balance with the supporting frame or structure.

The damage to exterior walls, windows, and other components that are expected to fail under a very large blast load generates flying debris that increases the risk of injuries and fatalities, both inside and outside the building. Additionally, the damage to the building envelope components and other nonstructural systems may significantly deter evacuation, rescue, and recovery efforts. To reduce the casualties from hazards associated with flying fragments, and to facilitate effective emergency response, the concepts of balanced design, ductile response, and redundancy should be considered in the design of the building envelope system.

3.4.2 General Façade Design Principles

The hardening of the building envelope should be balanced so that the columns, walls, and windows have approximately equal responses in terms of damage and injury or casualty in case of a terrorist attack using explosives.

Because attempting to design the entire façade to resist the actual pressures resulting from an explosive blast may be impractical, a more reasonable performance objective for a blast-resistant façade is to minimize the amount of glass and other fragments projected into the building interior. Performance criteria for structural walls that form the exterior façade should satisfy the structural integrity requirements of the building and be designed to resist blast loads but not be limited to a specific levels of peak pressure or impulse (that the member can withstand). The corresponding level of damage and deformation that these shear wall elements may be permitted to sustain is considerably lower than the level of damage and deformation permitted for the nonstructural façade components.

In principle, the main building structure may be expected to resist significant blast loads at a calculated standoff distance with only minimal structural damage. However, a façade, like a glass curtain wall, cannot provide equivalent protection. A compromise criterion typically accepted for protective glazing is that peak pressures and impulses of selected blast loads should not turn more than 10 percent of the glazed fenestration into high hazard debris that may be propelled into the occupied space.

Glass-Fragment Hazard Potential

Façade-system component design should be balanced to develop the capacity of the glazing material selected. A variety of government produced and sponsored computer software programs have been developed to calculate the glass-fragment hazard potential for different sizes and glass makeups in response to blast loading. Examples of these analytical methods include Window Lite Analysis Code (WINLAC), Window Glazing Analysis Response and Design (WINGARD), and Window Fragment Hazard Level Analysis (HAZL) or commercial software coupled with test data and recognized dynamic structural analysis techniques. The intent of the software is to show that the glazing can protect the occupants under the specific threat to produce a performance level selected from the GSA criteria shown in Table 3-4, which was based on U.K. research.

Table 3-4: GSA Glazing Hazard Criteria (Applied Research Associates, Inc. 2010)

Performance Condition	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 restrained 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 floor no further than 3.3 ft. from window.
3b	High	Low	Glazing cracks. Fragments enter space and land on floor no further than 10 ft. from window.
4	Medium	Medium	Glazing cracks. Fragments enter space and land on floor and impact a virtical witness panel at a distance of no more than 10 ft. from the window at a height no greater than 2 ft. above the floor.
5	Low	High	Glazing cracks and window system fails catastrophically. Fragments enter space impact a vertical witness panel at a distance of no more then 10 ft. from thee window at a height greater than 2 ft. above the floor.

Nonstructural façade components should be designed with connections adequate to transfer the collected loads to the structural system and should be detailed to absorb significant amounts of energy by means of controlled deformation. The duration of the extreme loading significantly influences the criteria governing the design of the façade systems, and significant inelastic deformations may be permitted.

Commonly used single-degree-of-freedom (SDOF) analyses produce conservative, dynamic design solutions for a wide variety of façade configurations. For the most basic glazed façades, which consist of punched windows or storefront that is broken up into symmetrical patterns of

glazing with aluminum or steel mullions, the designs developed using SDOF approaches will provide reasonably cost-effective window systems that meet specified performance requirements.

SDOF methodologies are less effective for the analysis of glazed façades with non-symmetrical configurations or large area curtain walls. Additional degrees of freedom and a more advanced mechanical representation of the system are required to effectively evaluate the performance of all the components in response to blast loading. Finite element analysis of the integrated glazed façade system overcomes all of the shortcomings of the sequential SDOF approach. However, these models are significantly more time consuming to develop and more computationally intensive to analyze. A greater amount of engineering expertise is required to model the system accurately and interpret the results. Nevertheless, the accurate representation of the system and the resulting savings in material justify the more advanced analytical methods.

Specific recommendations for design of building envelope components are discussed in Sections 3.4.3, 3.4.4, and 3.4.8.

High Performance-Based Design of the Building Envelope

Performance-based design is the process used to achieve performance levels for specific attributes based on quantifiable benchmark metrics that can be verified. The EISA defines a high-performance building as one that "integrates and optimizes on a life-cycle basis all major high-performance attributes, including energy conservation, environment, safety, security, durability, accessibility, cost-benefit, productivity, sustainability, functionality, and operational considerations." The complementary relationships between attributes provides an opportunity to incorporate blast, ballistic, and CBR protection technologies with the new and innovative building envelope technologies being developed to address the aggressive agenda laid down by the EISA.

To achieve the goals of the EISA and meet the mission of DHS IDD to improve the security of critical infrastructure, the High Performance Based Design of the Building Envelope project employs two unique approaches: 1) implementing a multi-attribute analysis of performance that includes evaluating interactions between the attributes of building design that characterize building function; and 2) automating the analysis with an online decisionmaking tool. The tool identifies performance levels and models them in a way that allows the owner's goals for a prospective project to be succinctly identified and evaluated.

The multi-attribute model and the information that populates it was created by a team of technical experts assembled by the National Institute of Building Sciences for their knowledge of multivariable modeling, performance-based design, and decision analysis encompassing risk and resilience. The expert development approach was used to formulate the most relevant characterizations of performance, progressing from current practice (Baseline) to three increasingly higher levels of performance (Improved Performance P+, Enhanced Performance P++, and High Performance HP). Capturing both code-mandated levels of performance (Baseline) and the full range of performance options available in one concise format is an important outcome of this project.

3.4.3 Structural Load-Bearing Exterior Wall Systems

Exterior load-bearing walls may also form the exterior envelope. Separate glazed systems are necessary to provide the glazed portions of the envelope; windows may be inserted in the wall or walls may alternate with curtain wall façade portions.

See Section 3.3 for blast-resistant design information.

Ballistic-Resistant Design

Ballistic-resistant design involves the use of materials that minimize the effectiveness of the weapon. To provide the required level of resistance, the walls must be constructed using the appropriate thickness of ballistic-resistant material, such as reinforced concrete, masonry, mild steel plate, or composite materials. The required thickness of these materials depends on the level of ballistic resistance required. Resistance to a high-level ballistic threat, such as a high-powered rifle, may be achieved using 6.5 inches (16.5 centimeters) of reinforced concrete, 8 inches (20 centimeters) of grouted CMU or brick, a 1-inch (2.5-centimeters) mild steel plate, or a 0.75-inch (1.9-centimeters) armor steel plate. A 0.5-inch-thick (1.3-centimeter) layer of bullet-resistant fiberglass may provide resistance up to a medium-level ballistic threat.

Bullet-resistant doors are required for a high level of protection; however, hollow steel or steel clad doors with pressed steel frames may be used with an appropriately concealed entryway. Ballistic-resistant window assemblies contain multiple layers of laminated glass or polycarbonate materials and steel frames. Because these assemblies tend to be both heavy and expensive, the number and size should be minimized. Roof structures should contain similar materials as the ballistic-resistant wall assemblies.

3.4.4 Window Systems

There are three basic types of glazing arrangements or fenestrations: punched windows, spandrel glazing, and curtain wall or storefront systems.

3.4.4.1 Punched Windows

Punched, or punched-in, windows consist of conventional windows set in an opaque structural or nonstructural wall or closely set conventional windows creating a continuous ribbon appearance (Figure 3-43). Generally, when subjected to blast loading, punched windows deflect in two directions, while ribbon windows deflect in one direction. Two-way systems resist blast loading more efficiently than one-way systems. Thus, assuming similar design conditions (cost, height of floors, and spacing of columns) punched windows tend to perform better during blast events than ribbon-type windows.

Figure 3-43:
Punched windows (left), ribbon windows (right)

In order for the mechanical bite (how far the glazing is imbedded into the frame) and attachment to be effective, the mullion deformations over the length of the pane should be limited. Wall deflections around certain members, i.e., windows and grilles, should be controlled to prevent premature failure of these members. Additional reinforcement in the wall and improved connections between the member and the wall are generally required. Torsional flexing of nonstructural walls during blast and seismic incidents may require "axles" to be added to window framing to accommodate this flexing (Figure 3-44).

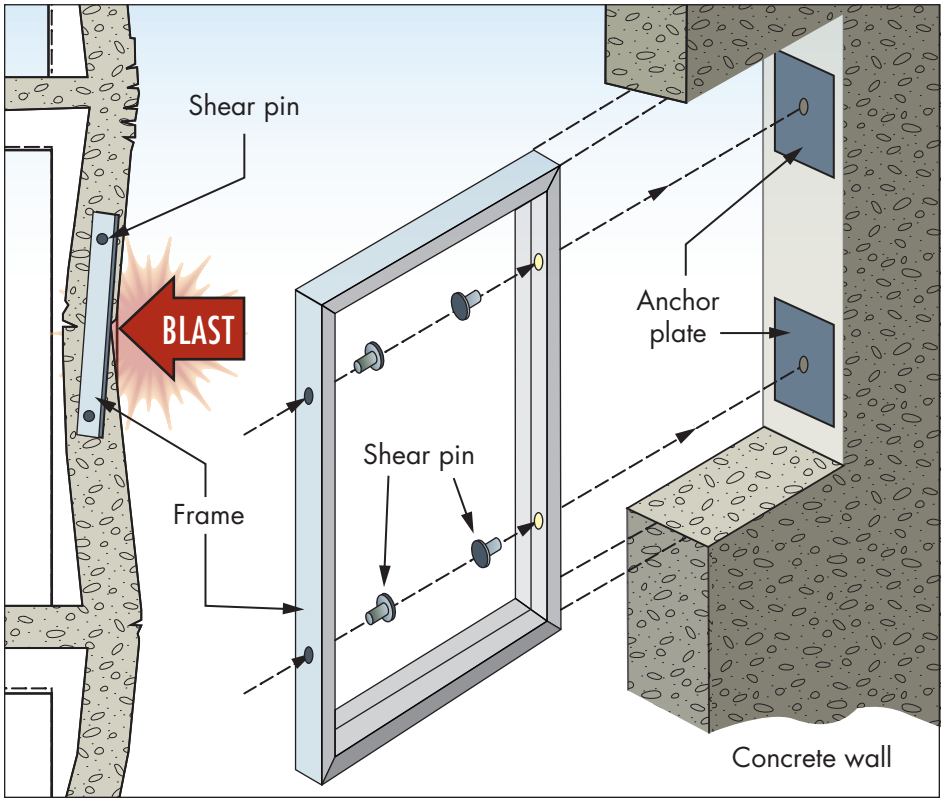


Figure 3-44:
Window framing for ductile walls

SOURCE: BASED ON EDWARD J. CONRATH, *STRUCTURAL DESIGN FOR PHYSICAL SECURITY – STATE OF THE PRACTICE*, AMERICAN SOCIETY OF CIVIL ENGINEERS, RESTON, VA, ISBN: 0-7844-0457-7] 1999

Unfortunately, the maximum extent of deformation that the frame or mullion may sustain prior to dislodging the glass is poorly defined. A conservative limit of 2 degrees from vertical is often assumed for typical protective glazing systems; however, advanced analytics may justify a significantly greater frame or mullion deformation limit. Furthermore, the performance criteria for the frames and mullions should permit greater inelastic deformation when resisting the loads equivalent to the ultimate capacity of the glass than when resisting the design level blast loads. Frames and mullions should, therefore, be able to accept the reaction forces from the edges of the glazed elements and remain intact and attached to the building.

A similar approach to design should be used for the supporting wall response. Having blast-resisting windows makes no sense if they are stronger than the wall into which they are anchored; the wall strength should be equal to or greater than the maximum strength of the window and anchorage system. This becomes particularly important in the design of ballistic-resistant and forced-entry mitigating windows, which may consist of one or more inches of glass and polycarbonate. In some applications, even the use of tempered glass can become problematic because of its strength. The anchorage system can also be problematic whenever FRF, with or without attachment, is installed. A case in point is the bombing of the U.S. Embassies in Kenya and Tanzania in 1998. FRF was installed, but the frames were not anchored to the structure, which resulted in the glass, film, and frame wall being blown into the building, causing most of the casualties. Figure 3-45 shows the generic attributes of a complete protective window system.

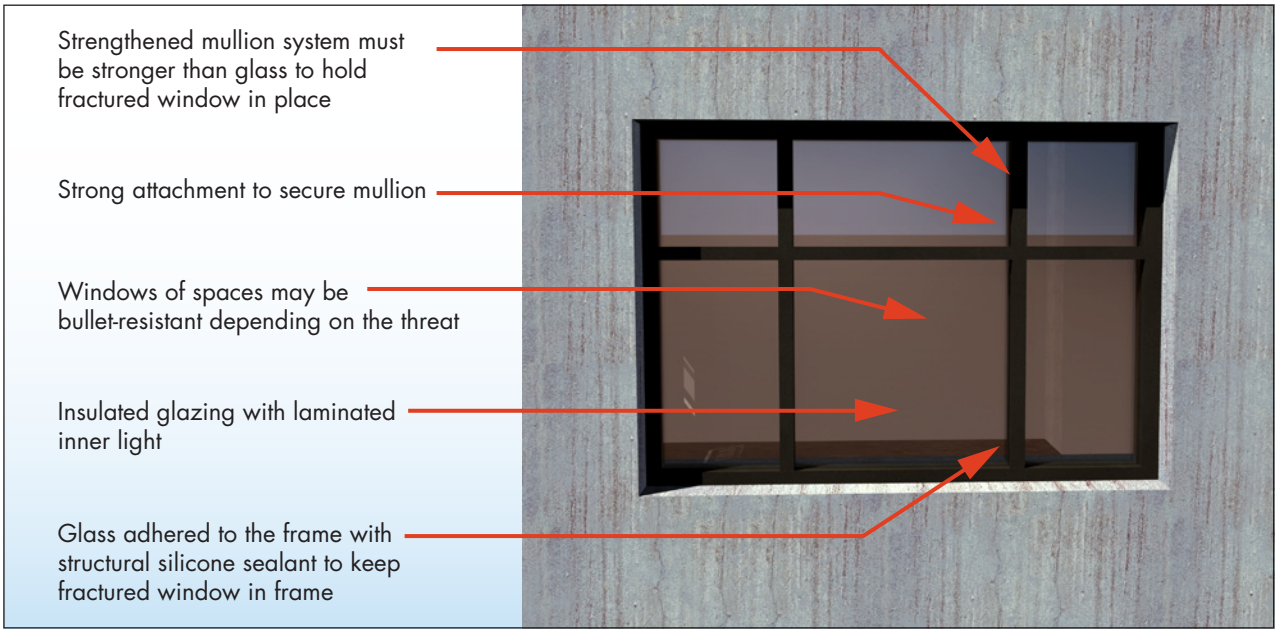


Figure 3-45: Protective glazing and framing design

SOURCE: FEMA 453, FIGURE 2-13, 2006

3.4.4.2 Spandrel Glazing

Spandrel glazing, consisting of continuous glazing, is typically inserted above a continuous structural or nonstructural spandrel.[5] This is a common glazing pattern for commercial and institutional buildings, as shown in Figures 3-46 and 3-47.

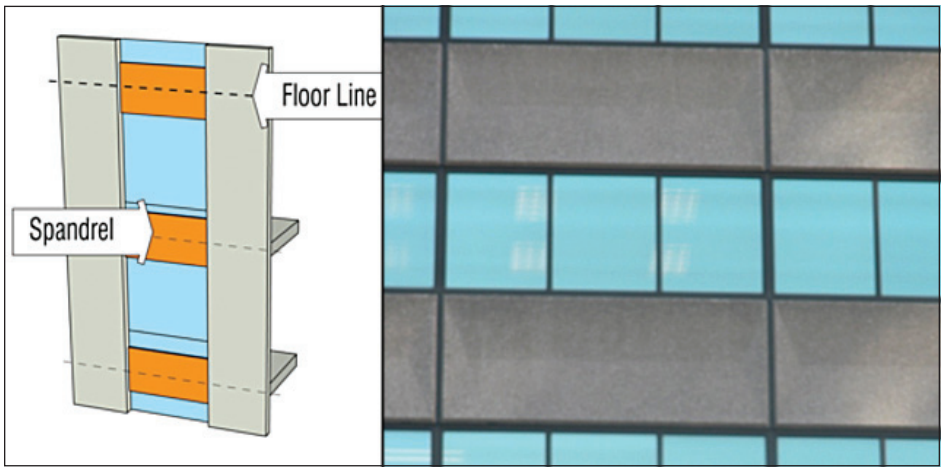


Figure 3-46:
Spandrel (left), continuous precast spandrel (right)
SOURCE: DAVID SHAFER

Nonstructural spandrels are common in curtain wall systems and use precast concrete or metal panels. Blast resistance of the glazing and spandrel must be balanced. Although unusual, structural spandrels may be integrated in a poured-in-place concrete structural system. Spandrels must provide good support for glazing framing, which must be securely attached at the head and sill.

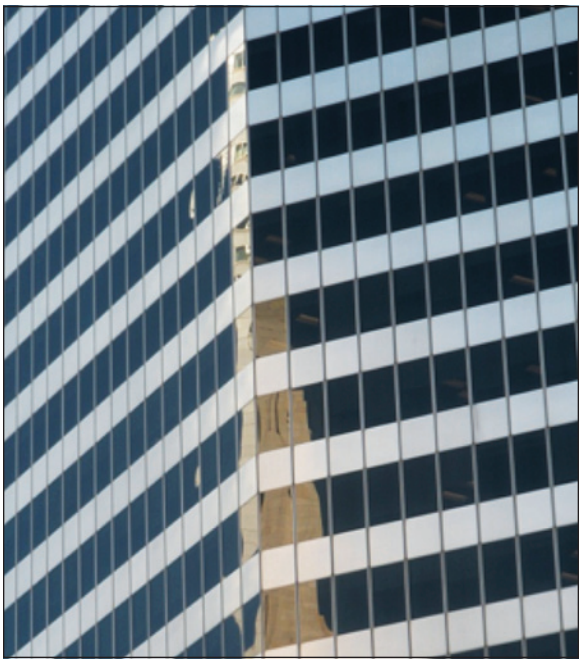


Figure 3-47:
Continuous metal spandrel panels set in metal and glass curtain wall
SOURCE: FEMA 455

3.4.4.3 Conventional Curtain Walls

A curtain wall is a nonbearing exterior enclosure that is supported by a building's structural steel or concrete frame (Figures 3-48 and 3-49).

Although lightweight and composed of relatively slender extruded aluminum members, an appropriately designed curtain wall is surprisingly resilient to explosive loading. In addition to hardening the individual members that comprise the curtain wall system, the attachments to the floor slabs or spandrel beams require special attention. These connections must be adjustable to

5 A spandrel is a horizontal piece of material that separates a row of windows.

compensate for the fabrication tolerances and accommodate the differential inter-story drifts and thermal deformations, and yet they must also be designed to transfer gravity loads, wind loads, and blast loads.

Figure 3-48:
Conventional curtain walls: expressed frame (left); framing concealed behind glazing (right)
SOURCE: FEMA 455

Curtain walls are of two basic types: stick-type wall systems and panelized systems. Though its assembly is labor intensive, the stick-type system consists of pre-assembled panel units that are attached to the field-assembled mullions that typically span from floor to floor. This system saves freight and shipping costs at the expense of field labor and erection time. The panelized system is essentially composed of large wall units that are pre-assembled and shipped in one or more story-high sections. These panels are shop-assembled and quickly erected but are more difficult to ship and handle. Most panelized systems are custom fabricated for large buildings (Figure 3-49).

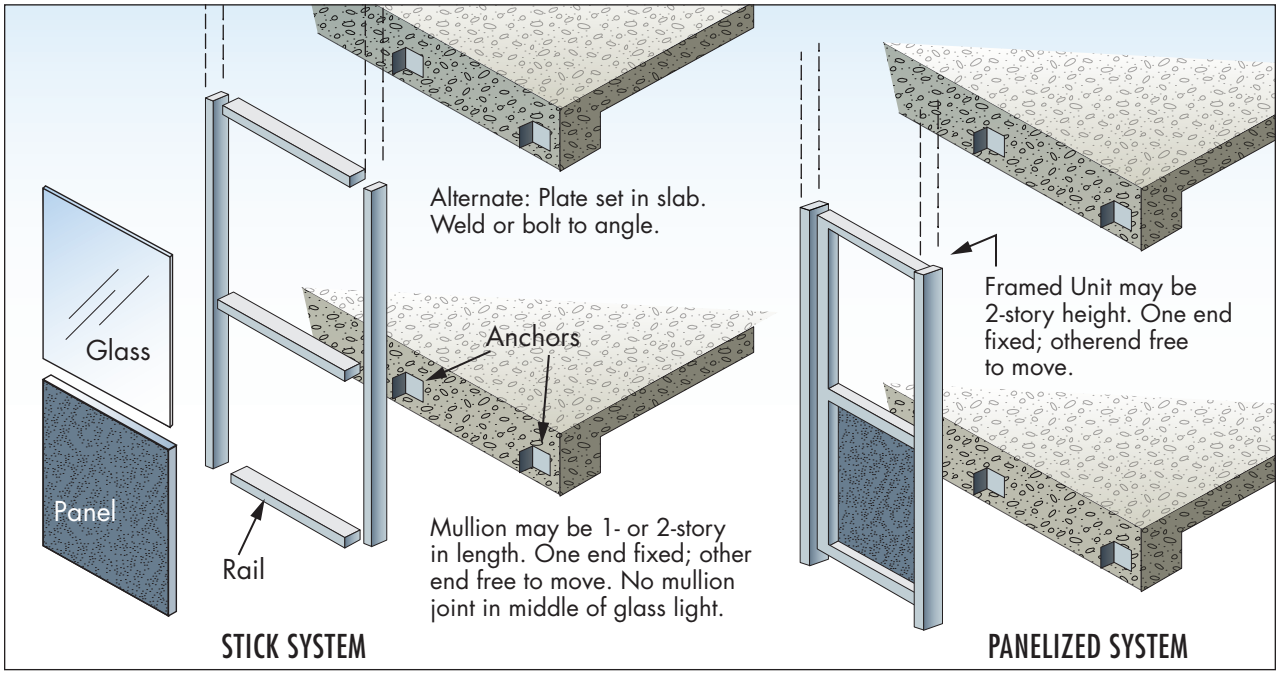


Figure 3-49: Stick curtain wall system (left); panelized curtain wall system (right)

The response of curtain wall systems to explosive loading is highly dynamic, highly inelastic, and highly interactive. By controlling flexibility and resulting deformations, curtain walls can be designed to dissipate considerable amounts of blast energy.

The design of blast-resistant curtain wall glass is similar to the design of blast-resistant windows. Glass fragment hazard software that was developed for GSA, DOS, or DOD may be used to select the required glass type, determine the fixed support reaction forces, and develop the force-displacement resistance functions of the glass.

The response of curtain wall systems to explosive loading is highly dynamic, highly inelastic, and highly interactive.

Because the intention of protective design is to limit the amount of debris, blast-resistant glass should contain either a laminated inner light or a mechanically attached protective film. The fragments remain adhered to these membranes, and their attachment to the mullions provides increased resistance to blast loading. Fundamental to the behavior of the curtain wall is the ability of the laminated or filmed glass to remain attached to the mullions.

Equally important to the selection of the blast resistant glass and framing members is the design of the attachments. For the glazing to fail according to design, it must be held in place long enough to develop the proper stresses that cause failure. Short of that, the glass will dislodge from the housing intact and cause serious damage or injury.

Curtain wall systems can now be modeled using advanced finite element methods that provide significantly more information about the performance of the curtain wall than do typical current non-blast-related methods used for wind and seismic hazards, including more detailed information about the curtain wall movement and connection forces.

3.4.4.4 Point- and Cable-Supported Curtain Walls

A point supported cable wall consists of individual panes of glass that are typically point supported at the corners where they attach to tensioned cables that either span vertically, from slab to slab, horizontally, from column to column, or both, as shown in Figure 3-50. Cable wall façade systems rely on the tension in the cable to develop the resistance to lateral loads. These cables must be appropriately sized and spaced to limit the displacements in response to wind loads and to develop the required lateral resistance in response to the tributary blast loads. The cable attachments to the building structure (slabs and columns) must be capable of developing large axial forces as they undergo significant inelastic deformation.

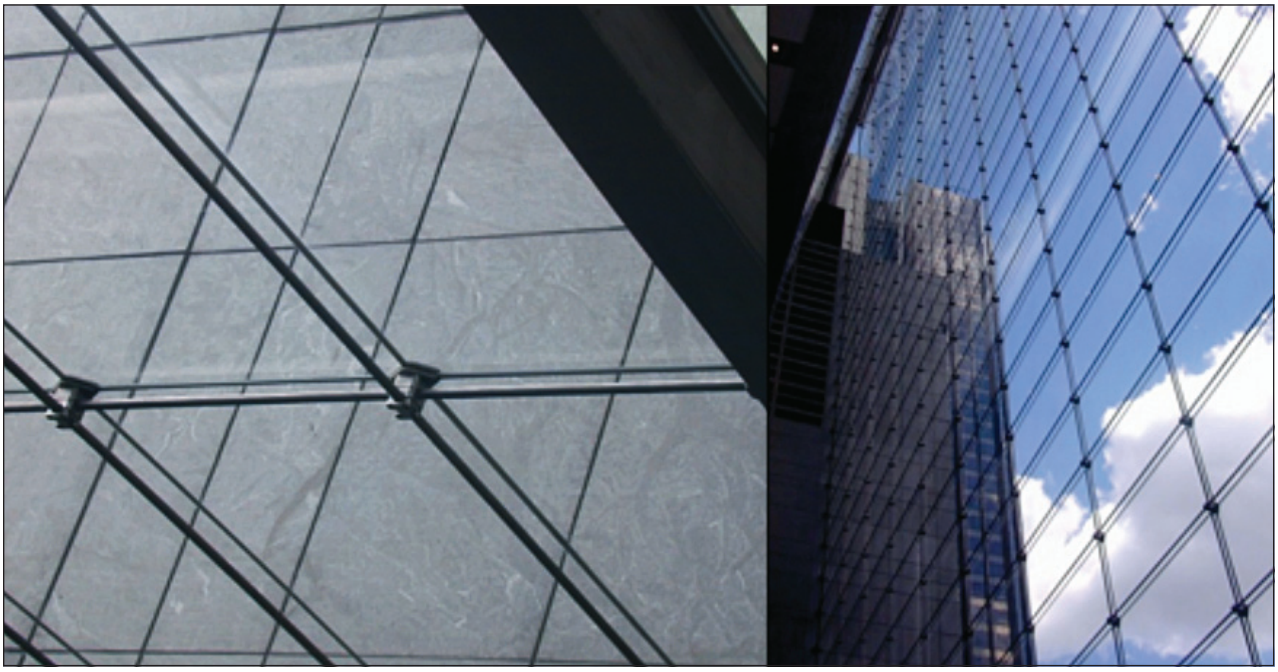


Figure 3-50: Point- and cable-supported curtain wall

The most vulnerable component of the cable wall system in response to blast loading is the point-supported glass. These panes of glass are typically attached to the cables at the four corners and sometimes at intermediate mid-section locations. Although laminated to hold the fragments together, the concentration of blast load intensity at the point supports requires very thick panes of glass to prevent fracture; once the glass cracks, the limp laminate may not remain attached to the mechanical attachment.

The most vulnerable component of the cable wall system in response to blast loading is the point-supported glass.

Although the blast resistance of cable wall hardware and glass are not well characterized by simplified analytical methods, secondary cable catch systems may be installed directly behind the glass panes and designed to intercept the glass debris, should a pane come disengaged from its support. Other specialty systems include composite materials that are interwoven with the glass laminates at the corners and gripped within the mechanical attachments; however, these systems are proprietary and must be developed on a case-by-case basis.

3.4.5 Glazing Materials

Six basic types of glazing are commonly used in the design of protective window glazing systems: annealed glass, wire-reinforced glass, heat-strengthened glass, fully thermally tempered glass, and polycarbonate. Other materials exist but are not commonly used in typical commercial window systems. Of the four common types, annealed glass and heat strengthened glass are the most frequently used materials. Any of these types of glazing can be laminated to add protection against explosive loads.

Annealed Glass, also known as float, plate, or sheet glass, is the most common glass type used in commercial construction. Annealed glass is of relatively low strength and fractures into razor sharp, dagger-shaped fragments at an incident pressure of about 0.2 psi.

Wire-reinforced Glass is a common glazing material, primarily used as a fire-resistant barrier. It consists of annealed glass with an embedded layer of wire mesh. Wire-reinforced glass has the fracture and low-strength characteristics of annealed glass. Under loading and blast pressures, although the wire may bind some fragments, it ejects a considerable amount of sharp glass and metal fragments. The glass has about one-half the strength of plain annealed glass without wire reinforcement. Wire-reinforced glass is not recommended for blast-resistant windows.

Heat-Strengthened Glass, also called double-strength glass, is intermediate in respect to strength between annealed and fully tempered glass materials. It breaks at about twice the pressure of annealed glass, hence the name double strength. Heat-strengthened glass has a reduced breakage potential for thermal and bending stresses; however, its failure characteristics are similar to that of annealed glass.

Fully Thermally Tempered Glass (TTG), also known as toughened glass, is typically four to five times stronger than annealed glass. However, abrasions on the face of TTG reduce the glass strength. The fracture characteristics of TTG are superior to those of annealed glass, producing small pellet-shaped fragments. Although TTG exhibits a relatively safe failure mode for conventional usage, failure under blast loading still presents a significant hazard of

Annealed Glass, also known as float, plate, or sheet glass, is the most common glass type used in commercial construction.

Wire-reinforced Glass is a common glazing material, primarily used as a fire-resistant barrier.

Heat-Strengthened Glass is also called double-strength glass.

Fully Thermally Tempered Glass (TTG), also known as toughened glass, is typically four to five times stronger than annealed glass.

Laminated Glass is glass composed of multiple glass layers with pliable interlayer materials.

bodily injury. Results from blast tests reveal that, upon fracture, TTG fragments may be propelled in cohesive clumps that only fragment upon impact into smaller rock salt-type fragments. Even if TTG breaks up initially into small fragments, the blast overpressure can propel the fragments at a velocity high enough to constitute a severe hazard, albeit with much less laceration and penetration capability than annealed glass.

Laminated Glass is composed of multiple glass layers with pliable interlayer materials (usually made from polyvinyl butyral [PVB]). The interlayer acts as the glue that bonds the multiple layers of glass into a single pane of a given thickness, greatly increasing its tensile strength. The interlayer provides a membrane response after the glass layers crack under loading. Annealed, heat-strengthened, TTG, or polycarbonate glazing can be mixed and matched between layers of laminated glass in order to design the most effective pane for a given application. When fractured, fragments of laminated glass tend to adhere to the PVB interlayer rather than falling free.

Laminated glass offers significant advantages over monolithic glass. It is stronger and, when failure occurs, the interlayer material may retain most of the glass fragments. Where insulated glazing units are used, a laminated inner pane of glass provides a debris barrier for the damaged outer pane of glass (which may or may not be laminated).

Laminated glass is the preferred glazing material for new construction. It is also effective for retrofit and improves the thermal performance of the façade as well. Tests have shown that laminated glass performs well under blast loads when mounted in properly designed window frames; it can be engineered to offer the highest levels of protection from glass fragments.

Laminated glass is the preferred glazing material for new construction.

Laminated glass must be correctly installed to provide long life. Regardless of the degree of protection required of the window, laminated glass must be installed with adequate sealant to prevent water from coming in contact with the edges of the glass.

Polycarbonates are very strong and suitable for blast-load-resistant window design. With 250 times the impact strength of glass, monolithic polycarbonate is available in thicknesses up to 0.5 inch (1.3 centimeters), and can be fused or laminated to obtain any thickness needed. Polycarbonate is expensive and subject to environmental degradation (especially from exposure to aromatic hydrocarbons) and abrasion. To ensure good optical quality (no yellowing or scratching), annealed glass is usually laminated to the outer surfaces of polycarbonates.

Local building codes should be consulted if polycarbonate glazing is under consideration. Several fire safety issues are associated with its use (thermoplastic polycarbonate is rated as a class CC-1 material and will often test with a smoke density rating over 500). Because of its strength, local fire codes may require a percentage of polycarbonate glazing to pop out to enable emergency egress.

3.4.6 Retrofits for Glazing

Film, also known as FRF, or anti-shatter film, shatter-resistant window film, or security film, is the most economical retrofit measure to strengthen the exterior glazed elements of the façade. Applied to the interior face of glass, FRF holds the fragments of broken glass together in one sheet, thus reducing the hazard of flying glass fragments. This retrofit measure adds tensile strength to the glazing, making the glass/film combination less brittle, especially at lower blast pressures.

Film, also known as FRF, or anti-shatter film, shatter-resistant window film, or security film, is the most economical retrofit measure to strengthen the exterior glazed elements of the façade.

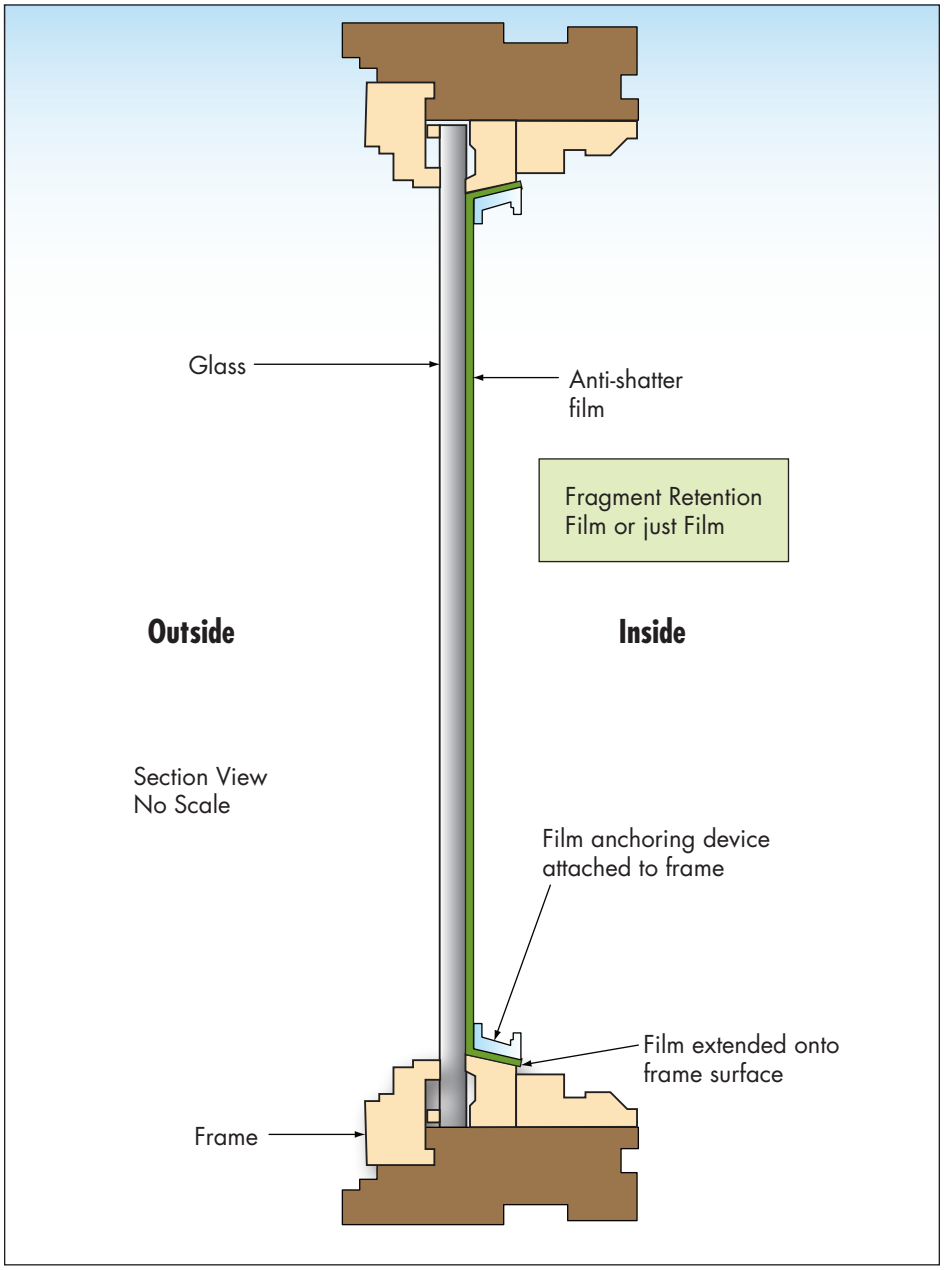
Although a film may be effective in keeping glass fragments together, it may not be particularly effective in retaining the glass in the frame. FRF is most effective when it is used with a blast-tested anchorage system. Mechanical attachment systems and wet glazing techniques are used to tie the FRF to the frame and further reduce the likelihood of the glass separating from the frame. The mechanical attachment method can be less aesthetically pleasing when compared to wet glazing because additional framework is necessary and is more expensive than the wet-glazed installation. Figure 3-51 shows a mechanical attachment system to keep the glass, film, and frame together. In wet-glazed installation, the technique uses a high-strength liquid sealant, such as structural silicone, to attach the glazing system to the frame.

Fragment Retention Film

Testing has shown that a 7-mil-thick film (mil = one thousandth of an inch), or specially manufactured 4-mil-thick film, is the minimum thickness that is required to provide hazard mitigation from a blast (NIBS 2010b). Therefore, a 4-mil-thick FRF should be used only if it has demonstrated, through blast testing, that it is capable of providing the desired hazard level response. The application of security film should, at a minimum, cover the clear area of the window. The clear area is defined as the portion of the glass unobstructed by the frame. This minimum application, termed daylight installation, is commonly used for retrofitting windows.

Figure 3-51:
Mechanically attached FRF

SOURCE: FEMA 453



Unless the window frames, framing systems, and their anchorages are capable of transferring the blast loads to the surrounding walls, the effectiveness of the attached films will be limited. Similarly, the walls should be able to withstand the blast loads that are directly applied to them and accept the blast loads that are transferred by the window system. Insufficient strength in the walls may limit the effectiveness of the glazing upgrades.

Rigid Catch Systems increase the effectiveness of film and laminated window upgrades. FRF and laminated glazing are designed to hold the glass fragments together as the window is damaged; however, unless the window frames and attachments are upgraded as well to withstand the same loads as the glazing, this retrofit will not prevent the entire sheet from flying free of the window frame. The rigid catch bars intercept the filmed or laminated glass and disrupt its flight; however, they tend to break the dislodged glazing into smaller projectiles. Catch bars are only effective if they are at the center of mass of the glass panel as shown in Figure 3-52. Where the window has multiple panes, a single rigid catch bar may only be effective for catching one or two of the panes.

Unless the window frames, framing systems, and their anchorages are capable of transferring the blast loads to the surrounding walls, the effectiveness of the attached films will be limited.

Rigid catch systems are subject to huge forces upon impact and require considerable anchorage into a very substantial structure to prevent failure. Where either the attachments or the supporting structure are incapable of restraining the forces, the catch system will be dislodged and become part of the debris.

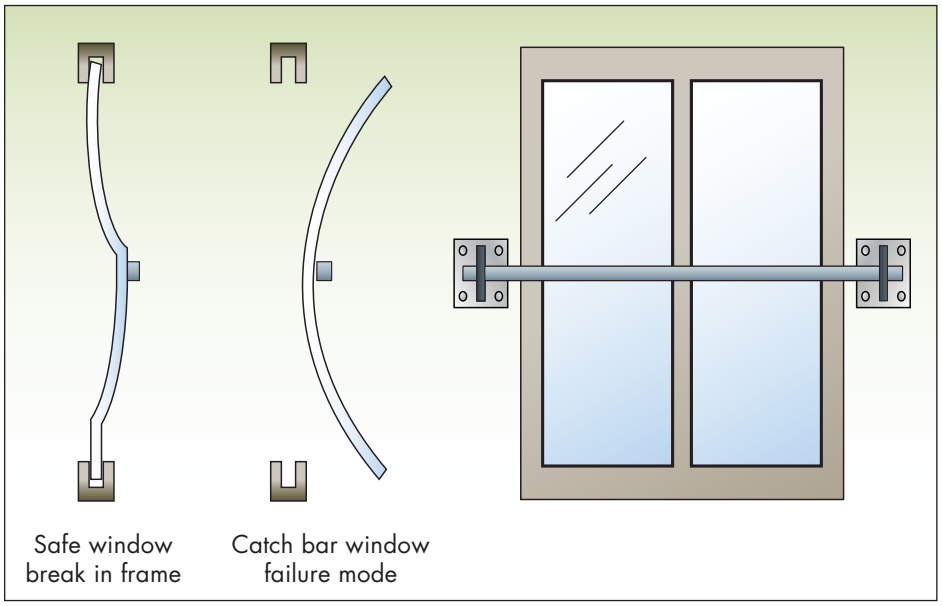


Figure 3-52:
Concept of a rigid catch bar system

SOURCE: FEMA 453

Cable Catch Systems are used extensively to absorb significant amounts of energy upon impact, and their flexibility makes them easily adaptable to many situations. Cable systems have long been recognized as an effective means of stopping massive objects moving at high velocity. The diameter of the cable, the spacing of the strands, and the means of attachment are

all critical in designing an effective catch system. An analytical simulation or a physical test is required to confirm the adequacy of the cable catch system to restrain the debris resulting from an explosive event.

High-performance energy-absorbing cable catch systems retain glass and frame fragments and limit the force transmitted to the supporting structure. Typical commercially available retrofit products consist of a series of 0.25-inch-diameter (0.64-centimeter-diameter) stainless steel cables connected with a shock-absorbing device to an aluminum box section, which is attached to the jambs, the underside of the header, and topside of the sill, as in Figure 3-53.

Figure 3-53:
Example of cable catch system

Large window systems use a network of vertical or horizontal and vertical cables of larger diameter. As with rigid catch systems, the center of mass of each pane of glass should be taken into account. The energy absorbing characteristics of these catch systems allow them to be attached to relatively weakly constructed walls without the need for additional costly structural reinforcement.

The main components of any blast curtain system are the curtain itself, the attachment mechanism affixing the curtain to the window frame, and either a trough or other retaining mechanism at the base of the window to hold the excess curtain material.

Blast Curtains are affixed to the interior frame of a window opening and essentially catch the glass fragments produced by a blast wave. The debris is then deposited on the floor at the base of the window. The use of these curtains does not eliminate the possibility of glass fragments penetrating the interior of the occupied space, but instead limits the travel distance of the airborne debris. The hazard level to occupants is significantly reduced, but a person sitting directly adjacent to a window outfitted with a blast curtain may still be injured by shards of glass. The curtain will billow out about 3 feet (0.9 meter) during a blast event.

The main components of any blast curtain system are the curtain itself, the attachment mechanism affixing the curtain to the window frame, and either a trough or other retaining mechanism at the base of the window to hold the excess curtain material. The curtain fabric, material properties, method of attachment, and manner in which they operate all vary, thereby providing many options within the overall classification of blast curtains.

Although blast curtains are intended to remain in a closed position at all times, they may be pulled away from the window to allow for cleaning and blind or shade operation. However, the curtains can be rendered ineffective if installed in a way that allows easy access and opportunity for occupants to interfere in their operation.

The curtains may either be anchored at the top and bottom of the window frame or anchored at the top only and outfitted with a weighted hem. The curtains should be extra long, exceeding the height of the window, with the surplus either wound around a dynamic tension retainer or stored in reservoir housing, as shown in Figure 3-54. When an explosion occurs, the curtain feeds out of the receptacle to absorb the force of the flying glass fragments.

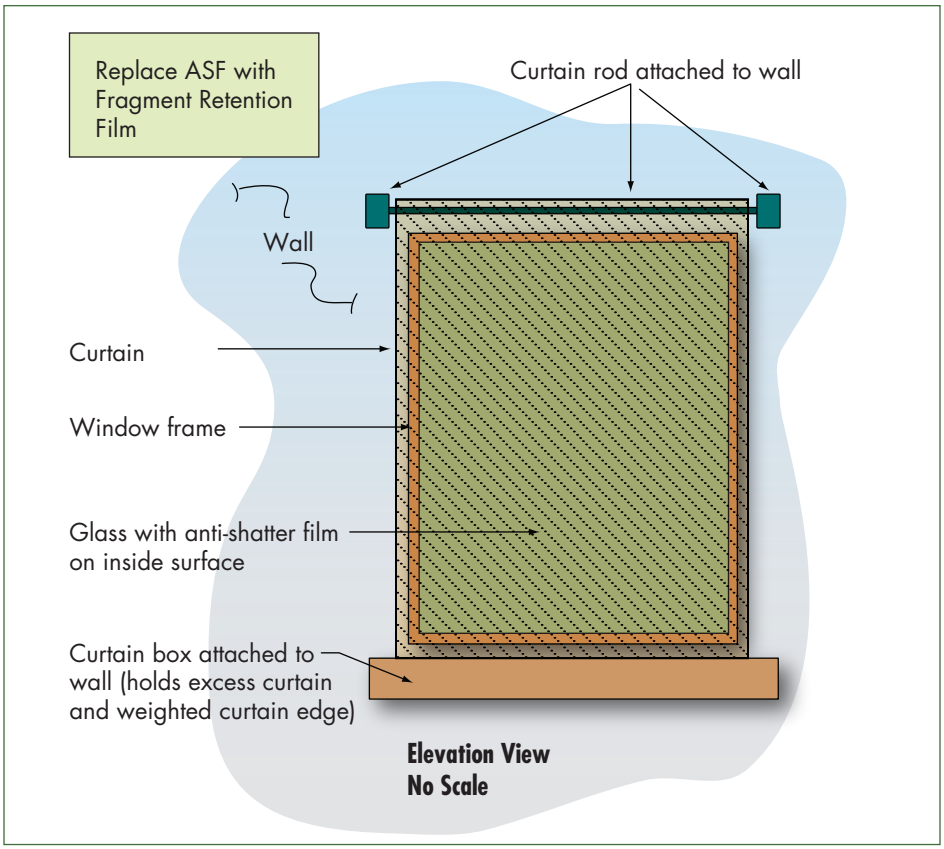


Figure 3-54:
Blast curtain system
SOURCE: FEMA 453

3.4.7 General Guidelines for Glazing Application

The following provide some general guidelines for the design of windows and glazing against extreme pressure incidents:

- Wire-reinforced glass should be avoided.
- The number and size of windows in a façade should be minimized, especially on lower floors where blast pressures are higher during an external explosion. Blast-resistant windows are more expensive, thus using fewer windows will reduce project costs.
- The window-to-wall ratio (square footage) should be minimized, where feasible, and subject to local building code minimum requirements.
- Interior courtyards or atria, as opposed to glazing on the exterior building envelope, should be considered because they require less hardening of windows and walls for explosions outside the building footprint.
- Narrow recessed windows with sloped sills are less vulnerable than conventional window designs (Figure 3-55).

- Laminated glass is preferable to conventional glazing.
- FRF should be used to add tensile strength and reduce fragmentation for weaker glazing in retrofit applications, but not in new construction, because its cost over the 25-year window life cycle is greater than the cost of installing equivalent laminated glass.
- Blast curtains should be used to prevent glass fragments from flying into occupied spaces. They are an excellent choice for blast protection in historic preservation projects in which the windows cannot be upgraded.
- The existing anchorage should meet design requirements or be upgraded on all window retrofits.
- Steel window frames are preferred for hardened windows with the frames securely fastened or cement grouted to the surrounding structure.
- Light shelves, although a great daylighting feature, require careful investigation under extreme loading conditions. The shelves may increase reflected pressures and, similar to an overhang, restrict clearing of the blast wave. The likelihood of these pressures requires significant detailing of the light shelf design to resist failure, fragmentation, and resultant breaching.
- Skylights and light pipes are recommended in lieu of light shelves. Balanced design of glass strength, frame strength, and connection detailing of the glass to frame and the frame to roof or wall also applies. Roof-mounted skylights and light pipes will receive less blast pressure than walls, but they may have to withstand greater dynamic movement as the blast wave passes.
- Stationary, non-operable windows are preferred for security and blast resistance; however, certain windows may need to be operable for emergency egress. Key-operated locks provide a greater level of protection than windows with simple latches.

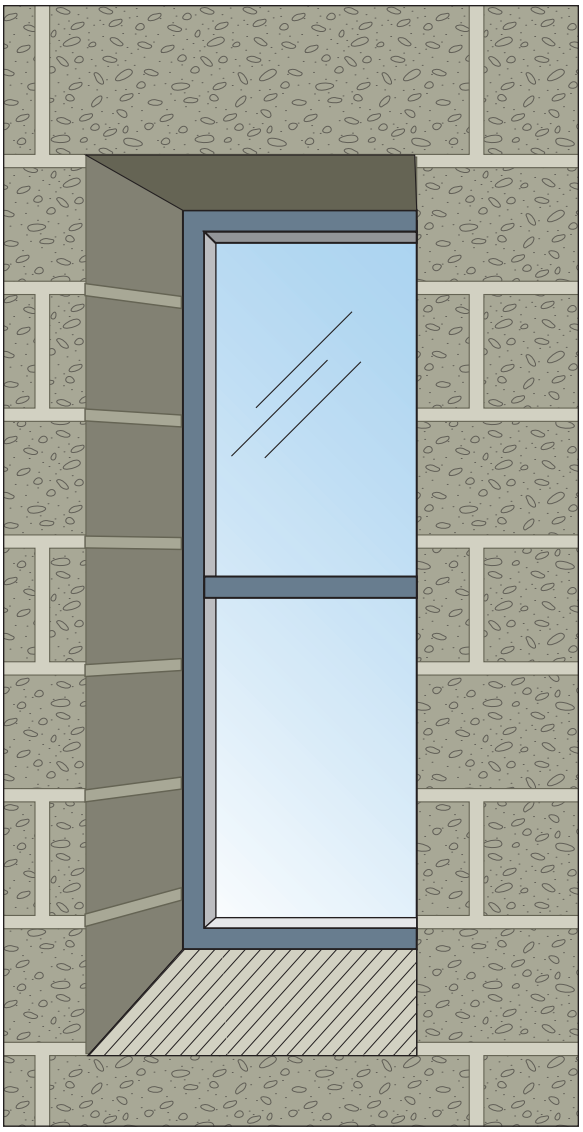


Figure 3-55: Narrow window with sloping sill

Other general security considerations for the design of glazing and windows include the following:

- Windows should not be placed adjacent to doors, because, if they are broken, the doors can be unlocked.
- Window openings should be protected with guards, such as grills, screens, or meshwork, firmly affixed to the structure.
- The operable section of a sliding window should be on the inside of the fixed section and should be secured with a broomstick, metal rod, or similar device placed at the bottom of the track.

3.4.8 Roof Systems

Although small amounts of explosives are not likely to produce significant blast loads on the roof system, a low-rise structure may be vulnerable to blast loadings created by a heavy explosive detonation at a large standoff distance that may sweep over the roof top of the building. Such blast pressures are likely to far exceed the conventional design loads.

Flat roof systems are exposed to incident blast pressures that diffuse over the top of the building, causing complex patterns of shadowing and focusing on the surface. Subsequent negative phase effects may subject pre-weakened roof systems to low intensity, long duration suction pressures, and lightweight roof systems may be susceptible to uplift effects. Secondary loads also include upward pressure on the roof structure from inside, as a result of breaching of the building envelope. The upward internal pressures may last longer if venting or rapid clearing is prevented. Considering the downward and upward loading separately is conservative.

Retrofit of an existing roof for increased hardening requires extensive renovation of the roof and its supports. A sacrificial roof is one possibility, but that requires a structural analysis for the additional weight of the roof and the measures taken to protect the existing roof and the interior. Additional considerations include the following:

- Lightweight ethylene tetrafluoroethylene (ETFE) systems should be given priority instead of long-span glass skylights. ETFE material does not resist blast loading; however, unlike glazed skylights that will propel hazardous debris when overloaded, the ETFE can be designed to tear away from the structural supports and fall, harmlessly to the floor below. Furthermore, the lightweight ETFE materials require less structure to support the gravity, wind, snow, rain and seismic loads.

- Access to roofs from adjacent buildings, fire escapes, access ladders on exterior walls, and terrain features should be prevented using fencing, anti-climb devices with padlocks, and other barriers.
- Where the roof is part of the building emergency action plan for evacuation, a procedure to gain roof access during emergencies should balance security with life safety. Refer to Section 3.5 for additional egress considerations.

3.5 Egress Systems

3.5.1 Stairs and Stairways

Figure 3-56 shows a typical egress stairwell. To improve survivability in the case of an explosive blast, egress capacity and security stairway designers should consider the following for new construction:

- Egress stairways should be designed in accordance with performance-based criteria.
- Stairways required for emergency egress should be located as far away as possible from security-sensitive or critical areas and, wherever possible, should not discharge into lobbies, parking, or loading areas.
- Egress routes should not be clustered in a single shaft. Separate egress routes as far as possible from each other, so that a single incident may not affect all routes. Building codes normally call for maximum travel distance to get to an exit. Consider the use of two to four egress stairwells for building occupants.
- Egress systems should include standard signage and guidance, so that during evacuations the systems become intuitive and obvious to all building occupants, including visitors. Unexpected deviations in the stairwells, such as floors with transfer hallways (Figure 3-56), should be appropriately marked.
- Considering past high-rise building evacuation experiences, access for first responders should be easy and efficient (Table 3-5 and Table 3-6). Increasing the width of the egress stairway so that first responders carrying equipment are easily able to pass evacuees or others going in the opposite direction is one approach. Alternatively, two or more stairways could be provided for first responders only. Computer modeling indicates that adding another 44-inch-wide (1.1-meter-wide) stairway improves ascent and descent times more than increasing two 44-inch-wide (1.1-meter-wide) stairways to 66-inch-wide (1.7-meter-wide) configurations.

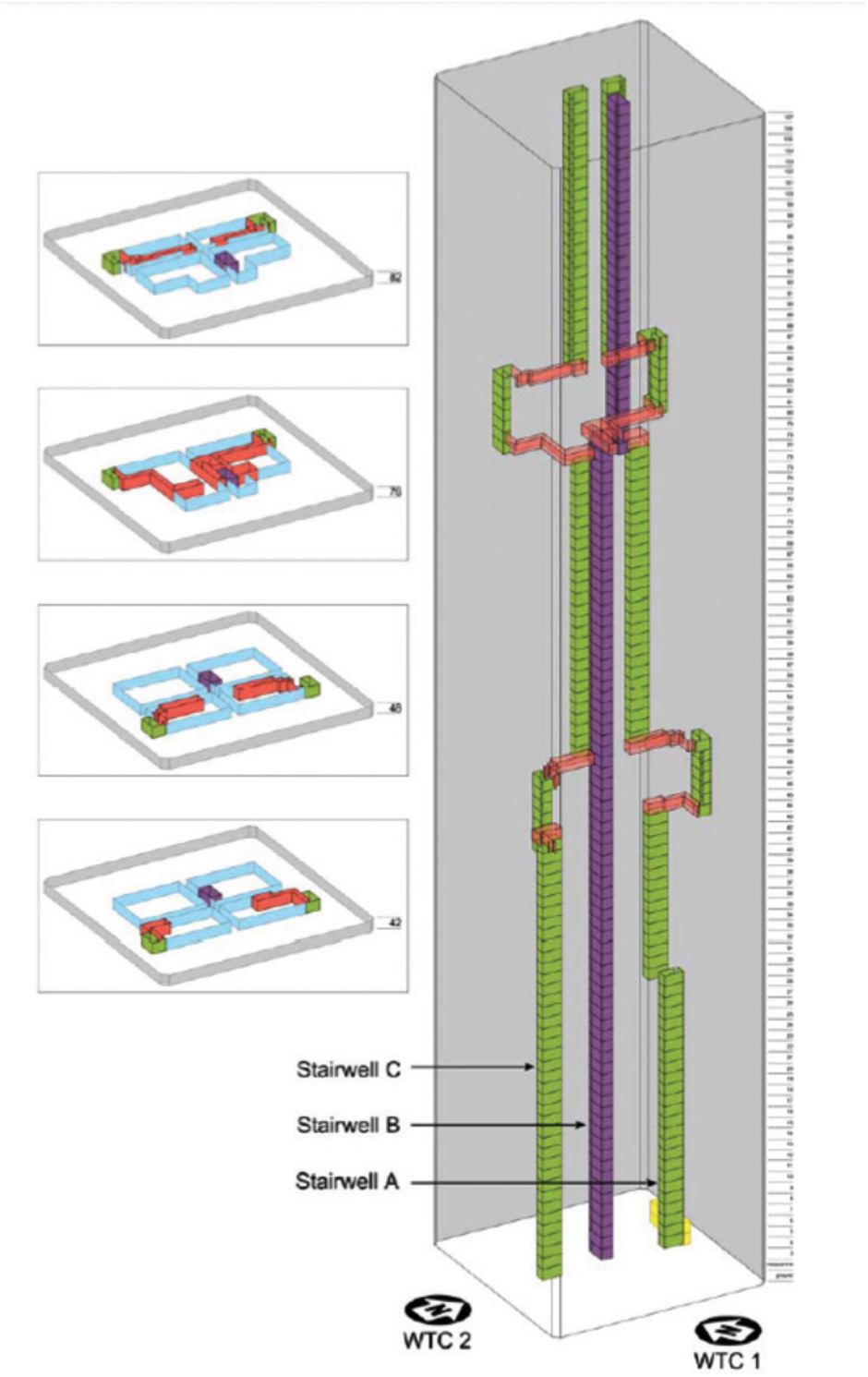


Figure 3-56:
Egress stairwells and transfer hallways in WTC Towers

SOURCE: NIST 2005

Table 3-5: Egress Stair Width Standards (NFPA 101 and NFPA 5000)

Occupant Loading Assigned to Stairs	Stair Width (inches)
< 50	36
≥50 to < 2,000	44
≥ 2,000	56

Table 3-6: Transit Time Between Floors (FEMA 453 and NIST NCSTAR 1-7)

Personnel	Travel Direction	Average Time (seconds)
Building Occupants	Down	48 *
Responders (no equipment)	Up	84 **
Responders (with equipment)	Up	120 **

* One minute/floor for downward transit is not an unreasonable design estimate considering all potential mobility-impairment situations

** Times shown for upward transit increase for greater than 60 floors

- Scissor stairwells in which two stairwells are side-by-side facing opposite downward directions should be avoided, as this provides little separation distance causing congestion between evacuees and first responders, unless one stairwell is designated for first responders only (Figure 3-57).
- Stairway pressurization keeps smoke out of the egress route using a series of fans, ductwork, and fire/smoke dampers. Pressurization is normally required by code in buildings more than 75 feet (23 meters) in height or 30 feet (9 meter) below grade, assuming exit discharge is at grade level. In addition to the stairways, transfer hallways between egress stairwells and paths to safe rooms (where people await fire rescue) should be pressurized for smoke management. Smoke control or management fans draw air into the building; therefore, smoke management air intakes should be kept away

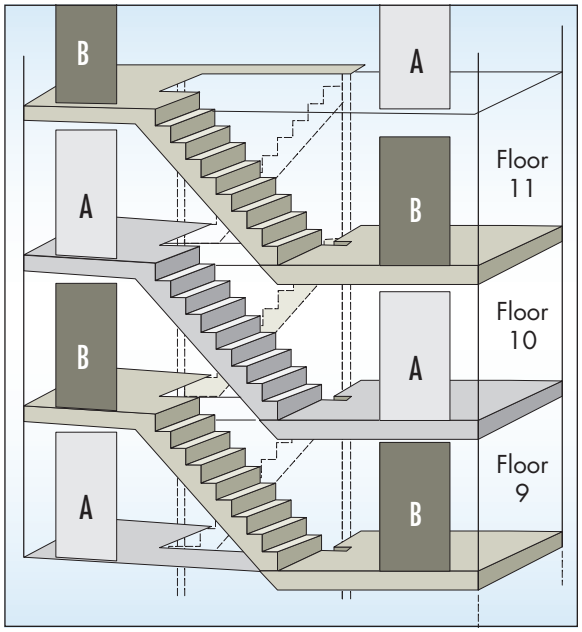


Figure 3-57: Scissor stairs

from exhaust vents and should be higher in the building, similar to other air intakes.

- Stairwell vestibules should be pressurized for the same reason stairwells are pressurized. With pressurization of vestibules and stairwells, the multiple stairway door openings during mass evacuations will reduce the potential for smoke intrusion.

Final Report on the Collapses of the World Trade Center Towers

Findings from the NIST report of the WTC Towers (WTC 1 and 2) after the 9/11 attack (U.S. Department of Commerce 2005a):

- It took an average of 6 minutes before people started leaving the WTC after the aircraft hit.
- One thousand people took the time to shut down their computers.
- Evacuation took 1 minute per floor, twice as long as emergency codes and models predicted for evacuation; about 25 percent of this time was needed to get to the stairways.
- Only 45 percent of WTC workers knew the building had three stairways; probably, fewer knew the stairways were not continuous from roof to ground floor and that transfer hallways were used to move between stairways.
- Only 50 percent of WTC workers knew that the doors to the roof were locked, thus escape from the roof by helicopter was unlikely.
- About 6 percent of the WTC survivors reported a mobility challenge (pre-existing injuries, medications, medical treatments, wheelchairs, pregnancy, or old age) that slowed their evacuation speed and impeded the evacuation of others.
- Public announcements, with instructions to return to their work locations, within WTC 2 were cited by many as a constraint to their evacuation. Other constraints included the following:

Constraints to Evacuation	WTC 1	WTC 2
– Stairways were too crowded	73%	69%
– Firefighter/police in stairway	63%	27%
– Injured/disabled in stairway	52%	33%
– Lack of direction/information	24%	29%
– Locked doors	16%	7%
– Poor lighting	11%	4%
– Bad/missing signage	5%	5%

- The most commonly mentioned forms of aid were assistance from coworkers and emergency responders and the photoluminescent markings in stairways.

Standards development and code writing organizations, such as the International Code Council (ICC), continually review data on constraints to evacuation.

- Emergency lighting fixtures and exit signs should be battery-powered because they have greater survivability than electric-powered systems during extreme events.
- Low-mounted egress lighting at eye level and above should be used because it remains visible when the egress path fills with smoke or other obscurants.
- Stairwell enclosures, if not part of the main building structure, should be hardened using reinforced concrete or CMU.
- Non-slip phosphorescent treads or photo-luminescent surfaces should be used along egress routes.
- Double doors should be used at exits to transfer hallways and final exits from the building for mass evacuation.
- Glass should not be used along primary egress routes or stairwells.
- All security locking arrangements on doors used for egress must comply with the National Fire Protection Association (NFPA) *NFPA 101: Life Safety Code* (2012). For example, the final exit doors from the building should only allow exiting and do not need an external handle.
- Roof access should controlled using a method such as a lockbox for fire wardens in case the roof is needed for egress.

3.5.2 Elevators

Conventional elevators are not designed to prevent smoke penetration into the elevator shaft, and elevator equipment is not thoroughly fire rated. Thus, elevators are normally not to be used for building egress during a fire. Currently, firefighters, at their discretion, may decide to manually operate an elevator for rescue or firefighting. One or more first responder elevators designed for rescue and firefighting would need hardened enclosures to withstand fire, blast, or other identified threat/hazard (Kuligowski 2003). The following should be considered in the design of elevators for blast resistance:

- Elevators should be separated from internal parking, loading docks, and lobbies, similar to egress stairways. A freight elevator may be placed close to the loading dock for convenience, depending upon the distance from the main passenger elevators.
- The elevator smoke management systems and elevator operation during a fire may affect pressurized areas, specifically the entrance lobby, if it is under negative pressure compared to the rest of the building.

Standards for Elevator System Design for Emergencies

The following list compares standards from GSA, NFPA, and NIST regarding elevator system design during emergencies.

- GSA mandates the following for elevator, fire alarm, lighting, and security systems:
  - These systems shall not be connected to the building automation system.
  - These systems need independent control panels and networks.
  - The building automation system monitors the status of these systems solely to prompt emergency operating modes.
- GSA also requires the connection of one elevator in each elevator bank to emergency generator backup power; this is in addition to the connection for any first responder elevator.
  - Where multiple elevators are in a common bank, a common emergency feeder from the elevator automatic transfer switch can allow each elevator to be operated individually during an emergency.
  - The elevator supplier can set up elevator programming for a controlled return to the terminal or recall floor for each elevator and then limit the number of elevators in that bank that can be run on backup power.
- *NFPA-72: National Fire Alarm and Signaling Code* (NFPA 2010) requires a coordination of building system emergency operations. Upon detection of a fire in a sprinkler-protected elevator machine room containing elevator control equipment, the main line power supply needs to be automatically disconnected prior to the application of water.
- The mass notification system should be heard and understandable in each elevator cab and in the elevator lobbies on each floor.
- NIST recommends video cameras be installed in every egress elevator lobby (similar to egress stairways) with the images displayed in the fire command center; image analysis software can minimize the fire department burden for monitoring these images.
- Video camera information and mass notification capability support shuttle operation of occupant evacuation elevators to move personnel as quickly as possible from the incident floor and two floors above and below.
  - For example, shuttle operation could commence above the 50th floor, while egress stairwells are used for the 50th floor and below.
  - After the elevators finish evacuating the upper floors, then mobility-impaired people can be shuttled from the lower floors.

- Elevator shaft/hoistway doors on each floor should be designed to keep out smoke.
- Elevator machine rooms should be served by separate, dedicated air-handling units, similar to mailrooms and entrance lobbies.

3.6 Mechanical, Electrical, and Plumbing Systems

Mechanical, electrical, and plumbing (MEP) equipment and essential utilities provide control of the building's thermal environment, power, communications and lighting services, all piped services, waste disposal, fire suppression, and smoke management. Elevators (in addition to stairways) are the main support for circulation of people and materials. Heavy equipment includes boilers, chillers, fans and cooling towers, transformers, and switching gear. Lighter, but potentially injurious, components include piping, ductwork, light fixtures, and suspended ceilings that can become flying debris in the event of an explosion, tornado, or hurricane.

When designing MEP systems for blast mitigation, the following should be considered:

- Each utility should have two or more service entrances, sufficiently separated so that one incident does not disable all service to the building.
- A minimum 50-foot (15-meter) separation should be provided between utility service entrances, primary and backup equipment for the same building system, and primary and backup distribution for system cabling and piping, and between critical system components and high-risk areas. This separation is to prevent an explosive event in one location from disrupting the operations of all important service systems.
- Fixtures, equipment, and piping should not be mounted on the inside of exterior walls, but on a separate wall at least 6 inches (15 centimeters) from the exterior wall face.
- Equipment, fixtures, conduits, and piping should not be suspended from the ceiling, unless supported and braced in accordance with seismic design requirements that also take into account additional blast loads.
- Vibration isolators should be installed on rotating equipment and flexible piping connections.

System design standards address limiting damage to this critical infrastructure (MEP), but additional considerations for upgraded goals include locating components in less vulnerable areas, limiting access to these systems, applying protective measures (security and hardening), and providing a reasonable amount of redundancy.

- Fire requirements (fire stopping), air infiltration and leakage requirements (sealing and smoke stopping), and sound transmission requirements (sound proofing) should be observed wherever system components penetrate a roof, ceiling, wall, or floor.
- Emergency backup electric power should be provided for all systems that must be operational at all times.
- In addition to separation, rooms for primary and backup systems should be hardened to improve their resilience.
- Sufficient storage capacity for fuel, oil, water, and other materials should be provided to allow the building to operate as long as required.

3.6.1 Heating, Ventilating, and Air-Conditioning Systems

Heating, ventilation, and air-conditioning (HVAC) systems are indispensable for continued operation of a building after a hazard event. For more details on designing these systems for blast resistance, see Chapter 4.

3.6.2 Electrical Systems

The major service functions of the electrical system are to maintain power to essential building services, especially those required for life safety and evacuation; to provide lighting and power for surveillance equipment; and to provide power for emergency communications. The operability of electrical systems is an important element for continuing service functions, deterring attacks, and operating life safety systems after an incident.

Electrical system designers should consider the following recommendations to mitigate potential terrorist attacks and to improve building performance under other threats and hazards:

- Two separate electric utility service feeds should be provided to all critical buildings. As a minimum, this can be provided by looped distribution from a single utility substation, or preferably separate substations to increase reliability.
- Transformers should, where possible, be located inside the building, in locations isolated from high-risk areas.
- Emergency and normal electric equipment should not be placed in the same electrical vault.
- Fuel tanks should be installed near the generator and underground whenever possible.

- Diesel fuel is the fuel of choice, as it is non-explosive compared to gasoline or natural gas.
- Protection, especially where the fuel tanks are above ground, should be the same as for the emergency generator, including the separation of the generator from the fuel tanks, so that a single event does not disable both assets. Fire-rated, hardened enclosures for fuel tanks and generators should be considered.
- Fuel tanks should be separated from high-risk areas of the building; fuel filling stations should be locked and monitored by the security VASS system.
- Fuel tanks should be sized to store an amount of fuel that will allow reasonable onsite capacity between fuel deliveries, but in no case less than 24 hours of capacity between deliveries at maximum load. GSA calls for a minimum of 48 hours of system operation between deliveries.
- Fuel deliveries should be from two or three suppliers over a wide geographic area, so that one extreme event does not affect all fuel suppliers simultaneously.
- Where fuel tanks are located far from the generator, such as in a high-rise building, systems that use jockey pumps activated by pressure drop alone to maintain pressure in the fuel piping system should be avoided. The jockey pumps require additional control measures, such as a confirmation signal that the generator is running as the reason for the pressure drop or use of the level sensors in the generator day tank to indicate refilling is required. The additional sensor should also link to a pressure drop alarm, such that this alarm activates when the other sensor is not activated, indicating a pressure drop from a leak.

- Emergency generators located inside buildings require adequate ventilation, such as large louvers, for cooling. Similar to windows, the larger the louver the higher the cost to harden against explosive blast. Where accessible from the ground, louvers should be secured to prevent forced entry.
  - A remote radiator system or a one-pass cooling heat exchanger using utility water can be used to reduce the need for large louvers.
- When an installed generator cannot be justified, provision should be made for renting a generator (trailer- or skid-mounted), housed in a soundproof and weatherproof enclosure, after an event.

3.6.3 Plumbing Systems

Plumbing systems include water distribution, water storage, sanitation systems, stormwater drainage, water heaters and softeners, and onsite treatment, as well as distribution of natural gas, laboratory gases, and medical gases. To protect against terrorist attacks and other threats and hazards, plumbing designers should evaluate at all potential scenarios: a broken water pipe can cause a flood, or a broken gas pipe can cause an explosion. To reduce the risk of these events, emergency shut-off valves and one-way check valves should be installed.

Floors in mechanical rooms where water is used should be sloped to prevent standing water near electrical equipment where personnel work.

Plumbing designers should consider the following recommendations to mitigate the effects of potential terrorist attacks, but also to improve building performance under other threats and hazards:

- The placement of plumbing on the roof surface should be avoided.
- Backflow prevention equipment should be installed at the water utility service entrance and where the potable water system supplies processing equipment.
  - Redundancy of the fire-suppression system may be increased by connecting it to the potable water system, with backflow prevention that allows flow from potable to fire suppression system only.
  - Electric-operated valves should be used to open these connections when needed.
- Water usage throughout the building should be reviewed for all possible scenarios. A sufficient water supply for all services or operations should be maintained at all times.
  - Event scenarios should evaluate potential damage and its effects. Automatic emergency shut-off valves triggered by excessive flow rates should be installed at the bottom of vertical risers.
  - Where leaks or damage can occur, drains should be installed.
- Natural gas usage throughout the building should be reviewed to enable the gas supply to be maintained throughout the period it is used.
  - Automatic emergency shut-off valves triggered by excessive flow rates should be installed at the bottom of vertical risers.

- Where leaks or damage can occur vents should be installed to prevent the gas concentration from reaching its lower explosive limit.
- Current building codes require that natural gas utility piping exit the ground prior to entering a building, which allows venting of underground leaks to the atmosphere and protects the building from leakage that can cause explosion.

4

Protection of Buildings Against Chemical, Biological, and Radiological Attacks

In this chapter:

Most buildings and building systems are not designed or equipped to protect the occupants from exposure to toxic agents, and in many cases may even exacerbate their effects by spreading toxic agents throughout the building. Of particular concern are building HVAC systems because they can become an entry point and distribution system for airborne hazardous contaminants.

The number of terrorist attacks has increased over the past two decades and with it the interest in the vulnerabilities of our public buildings to all kinds of threats, including the threats of attack with CBR weapons. Most buildings and building systems are not designed or equipped to protect the occupants from exposure to toxic agents, and in many cases may even exacerbate their effects by spreading toxic agents throughout the building. Of particular concern are building HVAC systems because they can become an entry point and distribution system for airborne hazardous contaminants.

In cases of toxic releases that originate outdoors, unprotected buildings are typically not able to offer much protection to occupants, because they have no useful separation between the outdoor and indoor environments. Toxic hazards produced by a release inside a building may have even more severe consequences for building occupants. A limited exchange of air between indoors and outdoors may produce much higher concentrations of toxins and longer periods of contamination inside the unprotected building. Airborne hazardous contaminants can be gases, vapors, or aerosols (small solid and liquid particles). Most biological and radiological agents are aerosols, whereas most chemical warfare agents are gaseous.

The number of terrorist attacks has increased over the past two decades and with it the interest in the vulnerabilities of our public buildings to all kinds of threats, including the threats of attack with CBR weapons.

This chapter is based on guidance from the CDC's NIOSH and the DOD and presents protective measures and actions to safeguard the occupants of public and commercial buildings from CBR attacks.

4.1 Risk of Chemical, Biological, or Radiological Attacks

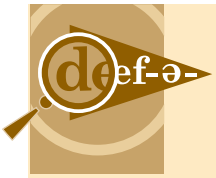
In contrast to attacks with explosives, CBR attacks are usually surreptitious. No audible or visible signs may be given that a toxic agent has been released, and the hazard may become apparent only when people begin to exhibit the symptoms of poisoning or infection. In an attack involving toxic chemicals, these symptoms may be immediate. In an attack involving the airborne release of biological or radiological agents, the symptoms are likely to be delayed for days or even weeks.

Hundreds of different toxic materials and infectious agents could be employed in a terrorist or criminal CBR attack.

Hundreds of different toxic materials and infectious agents could be employed in a terrorist or criminal CBR attack. Among these are chemical warfare agents, industrial chemicals, biological

agents, radioactive materials, toxins, irritants, and incapacitants, some of which are described further below. The threat each agent presents is determined mainly by its toxicity and persistence.[6]

- **Chemical warfare agents** are toxic substances developed or selected for use in warfare to kill or incapacitate people. These agents typically produce immediate physiological effects. The most toxic among the chemical agents are the nerve agents, such as sarin. A listing of chemical warfare agents and their characteristics can be found in the U.S. Army Field Manual FM 3-11.9, *Potential Military Chemical/Biological Agents and Compounds* (DOD 2005).
- **Toxic industrial chemicals** (TIC) are manufactured for industrial purposes. TICs are generally less toxic and less persistent than chemical warfare agents, and many are commonly stored or transported in bulk quantities. Among the several TICs used as chemical warfare agents in World War I are chlorine, phosgene, hydrogen cyanide, arsine, cyanogen chloride, and chloropicrin. Ammonia is a TIC that is widely manufactured, used, and transported; however, the toxicity of ammonia is low relative to the others, and it was never considered for use in warfare. Hydrogen cyanide, phosgene, cyanogen chloride, and arsine are four non-persistent TICs currently listed as chemical warfare agents. Chlorine was the first toxic chemical to be used on a wide scale in combat. The toxicity of some TICs is greater than others.
- **Chemical agents** vary widely in persistence. Some are gases at standard conditions, and some are liquids that evaporate at a very slow rate. Among the chemical warfare agents, vapor pressures at standard conditions range from extremely low (0.0007 millimeters of mercury [mm Hg] for the nerve agent VX) to extremely high (13,600 mm Hg) for the gas arsine. The most persistent of the chemical agents, however, are not as persistent as the radiological agents and some of the biological agents, which can remain hazardous for decades.



Chemical warfare agents are toxic substances developed or selected for use in warfare to kill or incapacitate people.

Toxic industrial chemicals are manufactured for industrial purposes.

Chemical agents vary widely in persistence. Some are gases at standard conditions, and some are liquids that evaporate at a very slow rate.

Biological agents include bacteria, viruses, fungi, and other microorganisms employed with the intent of causing illness or death.

Biological toxins are substances produced by bacteria or animals or from plants

Radiological agents are materials that emit alpha, beta, or gamma radiation.

6 For a list of specific agents, visit the NIOSH Emergency Response Safety and Health Database at www.cdc.gov/NIOSH/ershdb/AgentListCategory.html.

- **Biological agents** include bacteria, viruses, fungi, and other microorganisms employed with the intent of causing illness or death. Typically found in nature, biological agents can be altered to increase their ability to cause disease, by altering their resistance or their ability to be spread through the air and water. Production of biological agents does not require any material, equipment, or expertise that would not be found in a small pharmaceutical plant, university laboratory, or brewery. Production can be switched from industrial or research to warfare purposes in a matter of days. The potential for dual-use production facilities of very small size makes identification of countries or organizations producing biological agents extremely difficult. Biological agents can be very difficult to detect; they often do not produce immediate symptoms, and illness caused by them may not develop for several hours to several days after exposure. Disseminated as fine particles or droplets in the 1- to 5-micron (μm) size range, biological agents can remain airborne for very long periods. In still air, 1-μm particles settle at a rate of less than 1 foot per hour. Biological agents are the most toxic substances known. Because these are living organisms with rapid reproduction capabilities, all that is required to cause infections and death is a small quantity, often only 10 to 1,000 organisms.
- **Biological toxins** are substances produced by bacteria (e.g., botulinum) or animals (e.g., venoms) or from plants (e.g., ricin), and, although they do not multiply or grow once released, they are extremely toxic.
- **Radiological agents** are materials that emit alpha, beta, or gamma radiation. Radioactive materials can cause radiation sickness when released into the atmosphere as fine particles in three general scenarios. The first scenario is the detonation of a "dirty bomb" consisting of a conventional explosive combined with radioactive powder or pellets. The second scenario is an attack on a nuclear facility, and the third scenario is the detonation of a nuclear weapon. Each of these scenarios could produce radioactive aerosols that remain suspended in air and become re-suspended after deposition to produce a respiratory hazard. Radiological agents are among the most persistent agents. Decontamination is limited to removing, encapsulating, or collecting the agent. There is no natural decontamination other than radioactive decay, which can take years to millennia.

In defining defense against CBR agents, the magnitude of toxicity is related to the amount of agent that must be concealed, transported, or released to carry out an attack. The less toxic an agent is, the more of it is required, and therefore the more difficult it is to employ in a covert attack. For example, an attack with the non-persistent agent chlorine, much less toxic than nerve agents, requires very large quantities that

cannot be concealed or released without obvious warning signs. Toxicity also determines the level of protection required from various protective systems, such as air filters.

Whether an agent is persistent or non-persistent, outdoor releases result in transient concentrations. Under most conditions, airborne concentrations diminish rapidly in the open air, particularly with non-persistent agents. Agents disperse rapidly with the wind, particularly on sunny days when the ground is warmer than the air above it, producing convective flow.

Indoor concentrations persist longer because of limited air exchange with the outdoors and sorption or deposition on the interior surfaces. With limited air exchange between the indoors and the outdoors, contaminants are retained in the building and are not subjected to the environmental effects that, in many cases, cause them to become less hazardous.

In outdoor releases, the source of the hazard is most likely to be at or near ground level. Under stable atmospheric conditions, which normally occur at night, dusk, and dawn, and on overcast days, gases or aerosols released at ground level tend to remain at ground level. On sunny days, when the ground is hotter than the air above it, plumes tend to spread upward and be diluted as they rise.

Even in stable conditions, plumes originating at ground level can be diverted upward as they travel over buildings. In general, a plume will take the shortest path past a building. If the width of a building is more than twice its height, the shortest path will be over the building and the plume will travel upward to openings on upper floors.

4.2 Chemical, Biological, or Radiological Attack/Hazard Scenarios

There are many scenarios for CBR attacks; however, for the purpose of assessing a building's vulnerability to such attacks, four general scenarios that cover the range of delivery methods for an airborne agent attack on a building are discussed in this section. Each of these four scenarios may result from either an accidental or a deliberate (with a malicious intent) release.

- **Indoor Release:** The covert or overt release of agent from a device/container transported into the building; including, for example, dissemination of agent from a letter or mail-delivered device or the release from a device concealed in delivered supplies or equipment.

- **Covert Outdoor Release, Remote:** A toxic plume generated without any audible or visible indication from a point outside the secure environment of a facility.
- **Covert Outdoor Release, Proximate:** The surreptitious placement of an agent-dissemination device in or near an outside air intake or other penetration in the building shell at which there are inward pressures generated by fans, wind, or buoyancy.
- **Overt Outdoor Release:** The release of a toxic agent with some form of perceptible warning, for example, the explosive release of a TIC from a transport vehicle or storage tank or the release of a radiological agent from a dirty bomb.

Where air intakes are elevated or located on the roof of a building, the aspect ratio of the building (height ÷ width) determines whether the plume from a ground-level release near the building will flow upward and reach the intakes. A slender building, one having an aspect ratio much greater than 1, will force a ground-source plume to pass around, rather than over, the building. This rule of thumb does not apply when the source is far from the building, in which case the dilution that occurs over the large distance has a greater effect in mitigating the hazard.

4.3 Vulnerabilities of Buildings to Chemical, Biological and Radiological Attacks

Buildings contain a variety of openings that allow air to circulate. These openings are both intentional, for example, windows, doors, vents, and fresh air intakes, and unintentional, such as, cracks, joints, seams, and pores. In general, the protection a building provides against an outdoor CBR release is determined by these openings: their locations, the forces that drive the exchange of air through them, and the presence of air filters on intentional openings.

In normal operating mode, a building does little to protect occupants from airborne hazards that exist outside the building, because outdoor air continuously circulates through these openings. The concentration of airborne contaminants entering the building may be reduced, but the dosage (concentration integrated over time) will not be reduced unless the building is equipped with a high-efficiency air purification system. In the short term, a building can provide significant dosage protection; particularly, when a CBR event is transient and not continuous (reducing concentration) and occupants are evacuated when the threat has passed (reducing exposure time).

A building provides significant protection against outdoor hazards only when the outdoor air is filtered or the flow is temporarily interrupted. Interrupting the flow of fresh air, i.e., halting both mechanical and natural ventilation, is the principle applied in the protective action known as sheltering in place or unventilated sheltering.

In a mechanically ventilated building, the outdoor air enters predominantly through the fresh air intakes. However, a substantial volume of air, defined as uncontrolled air flow, enters through doorways, cracks, seams, joints, and pores in the building. Even elevators in operation, acting like pistons, draw air into the building.

Once airborne contamination enters a building, the ventilation system distributes it efficiently throughout the enclosed space. In each ventilation zone, air can be drawn through return ducts/plenums and distributed through supply ducts at high rates of flow. Air can also be driven by buoyancy pressures via stairwells or elevator shafts, particularly in winter when inside and outside temperature differences are large. At ground level, the buoyancy flow is inward in winter and outward in summer; therefore, a ground level release near the building is more likely to be drawn into a building during the winter.

Once airborne contamination enters a building, the ventilation system distributes it efficiently throughout the enclosed space.

For outdoor releases, the permeability of the building envelope is of paramount importance in determining CBR vulnerability. When the building is mechanically ventilated, as commercial buildings are, a tighter envelope (less air leakage through unintentional openings) is beneficial in reducing vulnerability to CBR attacks. A tight building envelope provides additional benefits, such as the following:

- Reducing energy consumption
- Reducing uncontrolled airflows, which have negative effects on heating and cooling and humidity control
- Facilitating pressurization
- Reducing the potential for mold/mildew that results from moisture infiltration

As much as the impermeability of a building envelope is important in reducing the vulnerability to outdoor releases, it is ineffective in reducing the vulnerability to indoor releases. For these types of attacks the most important issue in determining CBR vulnerability is access. When a building has unrestricted public access, toxic quantities of CBR agents can be hand delivered into the building or be introduced directly into the building's ventilation system.

The vulnerabilities of buildings are best illustrated by the review of four actual incidents that represent four attack types. These examples are presented to show the variety of ways in which an agent can be introduced into a building.

4.3.1 Example of an Indoor Release

At 9:45 a.m. on October 15, 2001, a staff member in the sixth-floor office of the Hart Senate Office Building in Washington, DC, cut open a taped envelope containing a powdery substance. Upon noticing a burst of dust, she placed the letter on the floor and notified the U.S. Capitol Police, who arrived within 5 minutes, followed minutes later by the Hazardous Device Unit. The officers tested the powder using commercial rapid tests, which indicated it to be anthrax spores (*B. anthracis*). This finding was later confirmed with definitive laboratory analysis.

Transport into the building: The quantity of anthrax, estimated at 1 to 2 grams, entered the building in a sealed envelope with normal mail delivery. The incident occurred before irradiation of mail was instituted in response to the threat of anthrax-bearing envelopes.

Transport within the building: Anthrax spores became airborne when the envelope was opened. With long settling times, characteristic of 1-μm particles, the spores migrated widely within the wing of the building, borne by mechanical air flows, possibly uncontrolled airflows induced by buoyancy and wind pressures, and possibly transported by people immediately after the release. In addition to the office in which the envelope was opened, positive samples of anthrax were found on the air-conditioning filter on the ninth floor, the stairwell leading from the eighth to the ninth floor, and in the freight elevator.

Warning signs to the victims: Visual observation of the powder in the envelope provided the initial indication of a hazard. At this time, or soon thereafter, people in the office had likely been exposed to the airborne spores.

Action taken when the hazard was noticed: At about 10:30 a.m., 45 minutes after the release, the ventilation system was shut down, and medical personnel began collecting nasal swabs from people in the immediate office and an adjacent office, as well as from the first responders. The person who opened the envelope removed and changed her clothing and was decontaminated with soap and water. Occupants of the building were evacuated. The southwest wing of the building was closed the morning of October 16; a decision was made to close the entire office building that evening. A total of 6,000 nasal swabs were taken and analyzed for anthrax. Twenty-eight people on two floors of the building, including five

Capitol Police officers, tested positive for exposure. All were successfully treated with antibiotics. A total of about 400 people who worked in or visited the building that day were also treated with a 60-day course of antibiotics as a precaution.

Anthrax is among the most persistent of toxic materials.

Duration of the hazard: Anthrax is among the most persistent of toxic materials. A portion of the airborne spores was likely removed from the building through natural air exchange, but most of the spores were likely retained in the building. In December 2001, the building was decontaminated, a very costly iterative process involving air and surface sampling and the use of chlorine dioxide gas, to render it safe. The Hart Senate Office Building was reopened for normal operations 3 months after the anthrax was released from the envelope.

4.3.2 Example of a Covert Outdoor Release, Remote

On June 27, 1994, members of the Aum Shinrikyo religious sect parked a delivery truck about 100 yards from an apartment building in Matsumoto, Japan. Concealed in the truck were a container of the nerve agent sarin and a battery-powered vaporizer. At about 10:44 p.m., when a light wind shifted toward the building targeted in the attack, men wearing respirators dispensed an estimated 100 grams to 1 kilogram of sarin from the truck's cargo area, generating a plume that traveled into and over the nearby buildings. The attack killed seven people and sickened about 220.

Transport into the building: This plume attack occurred in relatively stable nighttime conditions with light and variable winds (1 to 2 mph). The temperature was about 69 degrees, and windows of the buildings were open for natural ventilation. The point from which the agent was released was close to the targeted building, but variable wind direction caused the plume to spread laterally to the adjacent building, the Matsumoto Rex Heights Condominium, causing three deaths in each of the two closest buildings. One death occurred 3 to 4 blocks beyond the targeted building, on an outdoor balcony. The target, Kaichi Heights Condominium, and the other affected buildings were low-rise buildings, so the plume from the ground-level release flowed over them rather than around them, reaching open windows and causing casualties on the upper (second, third, and fourth) floors of each.

Transport within the building: With the natural ventilation of the buildings, transport within the building was predominantly by natural flows of wind and buoyancy.

Warning signs to the victims: The victims knew a hazard existed only by observing the agent's effects on people around them. Although pure sarin has no warning properties, the impure sarin used in the attack apparently presented an unusual odor. The odor, however, was not associated with a known hazard and, therefore, did not induce the victims to flee the building before they became incapacitated.

Action taken once the hazard was noticed: An emergency call was made about 30 minutes after the release began. About 2 hours after the release, police using loudspeakers instructed residents to evacuate. These actions were delayed because most victims were in their apartments, and it was not readily apparent to unaffected observers that a toxic chemical had been released.

Duration of the hazard: Sarin is considered non-persistent because it has a higher vapor pressure than most other chemical warfare agents. Although the plume was generated for only a few minutes, the agent remained at toxic levels in the buildings long enough to affect emergency responders who arrived 30 minutes after the release. Initial responders, not recognizing the hazard, did not use respiratory protection.

4.3.3 Example of a Covert Outdoor Release, Proximate

On the night of December 7, 1998, an assailant approached a two-story home in Beaver, PA, carrying a 100-pound cylinder of chlorine gas. While four members of a family slept in the home, he placed the cylinder next to the basement wall, inserted a hose through a basement vent, and opened the valve of the cylinder to release chlorine into the house. The family awoke and escaped with minor injuries.

Transport into the building: The gas was forced into the home through a ground-level penetration, a vent left open so that an electrical cord for outdoor Christmas lights could be passed through it.

Transport within the building: Although chlorine gas is heavier than air, the gas reached the upper level of the home through ducts of the forced air heating system and/or buoyancy flows resulting from the indoor-outdoor temperature difference on the cold December night.

Warning signs to the victims: The family's 13-year-old son, sleeping upstairs, awoke at 2 a.m. with throat irritation and awakened his mother. The smell of chlorine caused the family to evacuate the house. With chlorine, the odor threshold is about 0.06 parts per million (ppm); and the level at which immediate throat irritation occurs is about 15 ppm. At 50 ppm, prolonged exposure to chlorine can be fatal.

Action taken once the hazard was noticed: The family evacuated with only minor health effects.

Duration of the hazard: The chlorine was purged from the house by aeration and the use of fans the following day.

4.3.4 Example of an Overt Outdoor Release

In the early morning hours of January 6, 2005, a freight train with five chemical tank cars was diverted onto a spur line by an improperly positioned switch and crashed at 45 mph into a parked train near Main Street of the small mill town of Graniteville, SC. A tank car carrying chlorine ruptured, releasing 90 tons of the gas across the northern part of the town. The chlorine killed nine people and sent about 550 to hospitals (Dunning and Oswalt 2007).

Transport into the building: The gas plume traveled with a light wind northeasterly through the town, infiltrating buildings. Because chlorine is heavier than air and nighttime conditions were stable, it also descended southwesterly toward lower elevations and pooled in low-lying areas. The gas, reportedly, poured down storm drains like water and within minutes engulfed three buildings of the mill. Some workers in the nearest building climbed to the roof to get out of the visible cloud of gas and were later rescued. Two died after sheltering in a break room in one of the mill buildings as they waited for four hours for trained and equipped rescuers. Six of the nine who died were exposed to chlorine while indoors.

Warning signs to the victims: About 500 workers on the night shift at a textile mill near the tracks heard the accident. Five of the people who died were among mill workers who sheltered in place initially then fled the building about 10 minutes after the accident when the gas smell became too strong.

Action taken when the hazard was noticed: Local fire and law enforcement personnel arrived at the accident scene minutes after the crash, but initial responders were not equipped for the hazmat operation. A decontamination center was set up about 3 miles away about an hour after the crash. About 2½ hours after the accident, the emergency alert system was activated, telling residents to evacuate. Four hours after the accident, the Reverse 911 System was used to send a shelter-in-place message to 3,600 homes. Twelve hours after the accident, all residents within 1-mile radius of the crash site, about 5,400 people, were told to evacuate.

Duration of the hazard: A second chlorine car continued to leak for approximately 3 days, until repair crews could fabricate a patch to cover the hole.

All chlorine was removed from the tank cars by the seventh day after the accident, and Graniteville residents returned to their homes in phases between days 8 and 13.

4.3.5 Assessing the Vulnerability of a Building to Chemical, Biological, or Radiological Attack

Assessing a building's vulnerability to a CBR attack is the process of estimating the likelihood that a CBR attack will produce casualties, disrupt operations, or deny the use of the building. In each of the four general release scenarios, or attack types, the building's vulnerability is given a rating of low, medium, or high. These ratings reflect the ease with which a CBR attack may cause casualties and disrupt operations and normal use of the building. Vulnerability to CBR threats is determined primarily by the following:

- The local environment
- The architectural, mechanical system, and control system configurations of the building
- Physical security measures in place
- Plans and procedures in place for defense against CBR attacks

The essence of CBR vulnerability assessment is to identify building pathways on which pressures act to produce air exchange. For an outdoor release, the pathways of concern are those through the building envelope. For an indoor release, the pathways of concern are those from room to room, floor to floor, or zone to zone. Of greatest concern are pathways subject to continuous inward pressure – ones accessible and unsecured, unfiltered, concentrated, or high in airflow volume (serving a large space).

Vulnerability assessment requires a basic understanding of the following:

- How toxic agents can be delivered and transported into a building
- How toxic agents will be transported by air within the building
- Available defensive measures against CBR attack
- Building HVAC and air-filtration systems
- Physical security systems

Vulnerability ratings are not necessarily constant for a given building. A building assessed to have a low vulnerability rating could have a higher actual vulnerability if physical security measures are not rigorously

applied, mechanical systems and air filtration systems are not maintained, or procedures for response to an attack are not planned and executed efficiently.

Vulnerability for each type of attack is rated as low, medium, or high. Suggested benchmarks for these ratings are described below.

Indoor Release

- **Low vulnerability** rating applies to a building with access controlled by guards, entry screening with X-ray and magnetometer, isolated visitor area for entry inspections, mail screening, and supplies and equipment from trusted sources.
- **Medium vulnerability** rating applies to a building with limited physical security in the form of indoor surveillance cameras, or security guard present in the lobby/entrance, but no routine restrictions on access and no screening. Access is controlled by proximity cards, swipe cards, key pads, or other electronic devices; and the lobby has no isolation.
- **High vulnerability** rating applies to a public access building without access control or mail screening.

Covert Outdoor Release, Proximate

- **Low vulnerability** rating applies to a building with intakes that are roof-mounted on a low-rise building or at least midway up the building on a high-rise building (no ground-level intakes).
- **Medium vulnerability** rating applies to a building with first- and second-story wall-mounted intakes, intakes at grade or wall-mounted below the second story and protected by security fencing, or no intakes for a building that is not mechanically ventilated.
- **High vulnerability** rating applies to a building with intakes at or below grade or on a first-story wall with unrestricted access in areas of high pedestrian or vehicle traffic (most vulnerable), intakes at or below grade or first-story wall-mounted in a public area subject to surveillance only, or direct connection to a public access tunnel or other penetration subject to buoyancy or wind pressures.

Covert Outdoor Release, Remote

- **Low vulnerability** rating applies to a pressurized building protected by both high-efficiency particulate air (HEPA) and high-efficiency gas adsorber (HEGA) filtration; this type of filtration comprises Level 7 per FEMA 459, Incremental Protection for Existing Commercial Buildings from Terrorist Attack (2008b).

- **Medium vulnerability** rating applies to a building with recirculation filter units having absorbers and minimum-efficiency reporting value (MERV) of 14 or higher particulate filtration (FEMA 459 Levels 4, 5, or 6).
- **High vulnerability** rating applies to buildings without enhanced filtration (FEMA 459 Levels 1, 2, or 3). For filtration of makeup air, buildings that have filter ratings up to MERV 13 have low single-pass removal efficiency for aerosols of 1-μm diameter or greater.

Overt Outdoor Release

- **Low vulnerability** rating applies to a building with all the components of sheltering in place applied, including training and exercises for sheltering.
- **Medium vulnerability** rating applies to a building without sheltering in place, but with escape hood respirators for all occupants and visitors, and without external surveillance.
- **High vulnerability** rating applies to a building without all the components of sheltering in place, without special filtration, and without escape hood respirators.

4.4 Strategies for Reducing Chemical, Biological, and Radiological Vulnerability

There are four basic strategies for protecting a building and its occupants from CBR attack. These four are illustrated in Figure 4-1.

- **Physical security.** This strategy involves measures that limit or prevent access to a building or deter potential attackers. This includes the application of physical barriers, surveillance, and access-control procedures as preventive measures.
- **Air purification.** This strategy involves high-efficiency filtration, neutralization, or disinfection of the air in or entering the building. It typically involves mechanical filtration of aerosols and adsorption of chemical vapors/gases, but it may also involve the use of ultraviolet light or other non-mechanical air purification, mainly for biological agents.
- **Unventilated sheltering.** This strategy, commonly referred to as sheltering in place, involves temporarily reducing the air-exchange rate of the building or safe room, before contaminated air reaches it, and increasing the air-exchange rate after the hazardous condition passes.
- **Individual protection.** This strategy involves building occupants' use of individual protection equipment, primarily respirators capable of filtering aerosols, vapors, and gases at very high efficiency.

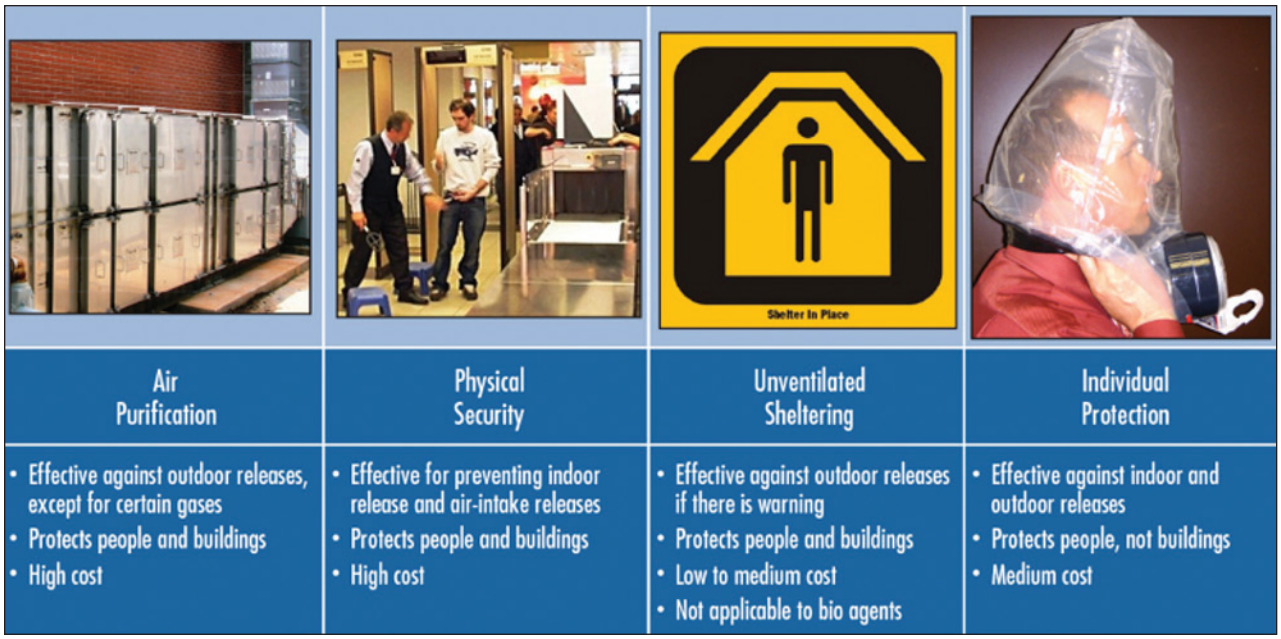


Figure 4-1: Four strategies of CBR protection for buildings

Each of these strategies has limitations; that is, none is comprehensive in its effectiveness. For this reason, achieving complete protection requires a combination of strategies and involves several protective measures—architectural, mechanical, electrical, and operational—to reduce the vulnerability of a building and its occupants to airborne hazards. These measures vary in cost as well as effectiveness.

Each strategy involves a combination of two or more protective measures. For example, unventilated sheltering in an office building is most effective when combined with the use of a single-switch HVAC system control, to quickly deactivate all fans in the building, and a public address system, to move people into a protective posture rapidly. Employed against a potential terrorist attack, sheltering also requires external surveillance, a detection system, or a community warning system. On the other hand, the full effectiveness of air purification can be achieved only when the building or the spaces selected for protection are pressurized. Pressurization is most economically achieved by tightening the building envelope with sealing measures during construction.

The effectiveness of a strategy can be stated in terms of protecting the people in the building and/or protecting the building, i.e., preventing the building from becoming contaminated with a persistent agent.

The effectiveness of a strategy can be stated in terms of protecting the people in the building and/or protecting the building, i.e., preventing the building from becoming contaminated with a persistent agent. The strategy of escape respirators does not, of course, prevent the building from becoming contaminated. Both unventilated sheltering and the use of respirators require a means of detecting a hazard. Limitations on the capability to detect CBR agents thus constrain the effectiveness of any strategy. No rapid detection capability for biological agents exists; therefore, continuous air purification is the only practical means of protection against a covert release of biological agents.

4.4.1 Physical Security Strategy – Architectural Measures

Physical security measures are considered preventive measures for defense against CBR attack. They serve to deter potential attackers, to prevent a container of toxic agent from being transported into the building, and to prevent the release of an agent from a point inside the building or through a penetration in the building envelope from a point near the building.

Several architectural measures can be applied to reduce the vulnerability of a building to a release of a toxic agent.

4.4.1.1 Securing Fresh Air Intakes

Elevating the fresh air intakes is a relatively simple means of reducing a building's CBR vulnerability (Figure 4-2). Securing air intakes can be expensive, particularly in the retrofit of an existing building; it is most easily applied in new construction. These protective measures provide the following benefits:

- Where the roof access is controlled or barred altogether, elevating intakes provides passive security against malicious acts, making it more difficult for a container of hazmat to be inserted directly into the building's HVAC system.
- Elevating intakes makes it less likely that hazmat released at ground level near the building will reach high enough concentrations at the intakes, because dilution increases with the distance from the source. In stable conditions, contaminants released near the ground will likely remain close to the ground unless the airflow over the building lifts them upward. Contaminants heavier than air will also tend to remain close to the ground under calm conditions.

The effectiveness of a strategy can be stated in terms of protecting the people in the building and/or protecting the building.

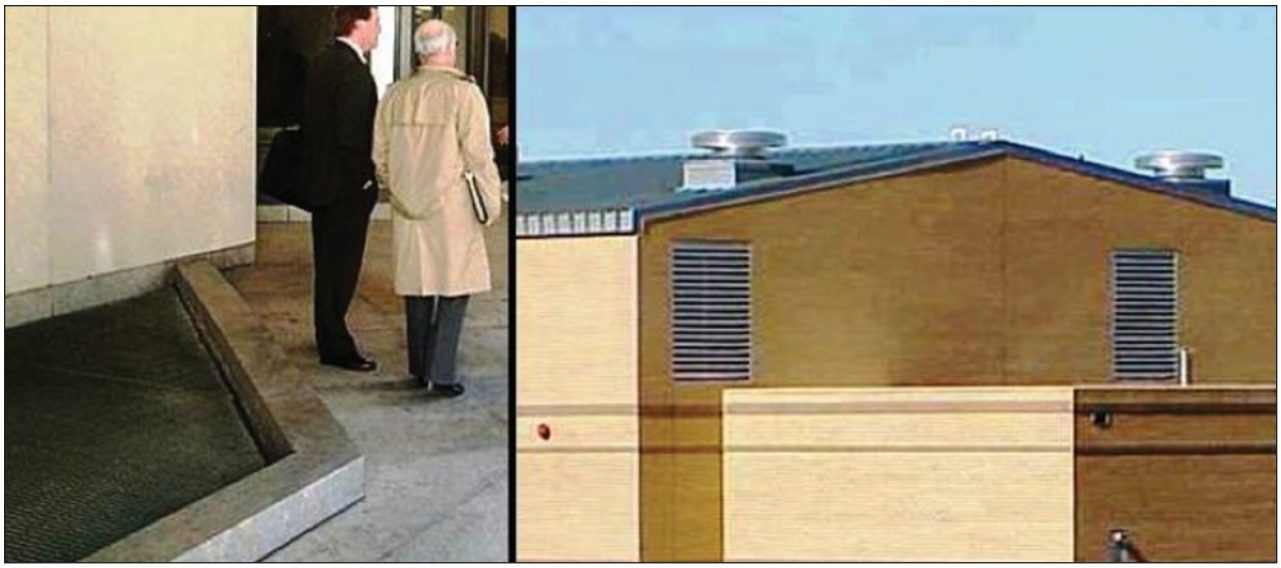


Figure 4-2: A vulnerable, ground-level intake (left); an intake elevated to the second story (right)

Elevating intakes is effective within practical limits. A plume or cloud of hazmat can reach the intakes, particularly if the source is large and distant. For low-rise buildings, a plume originating at ground level near the building is likely to travel over the building rather than around it.

Intakes should be placed at the highest practical level on the building. GSA recommends 50 feet (15 meters) above ground (4th floor or higher). Elevating the intakes has a secondary benefit of reducing the probability that vehicle exhaust fumes will be drawn into the building. GSA-recommended separation distances from other fresh air intakes or exhausts range from 10 to 25 feet (3 to 8 meters). This separation is to prevent short-circuiting (exhaust from one intake entering another) between systems.

For protection against malicious acts, intakes should be covered by screens so that objects cannot be tossed inside from the ground level. Such screens should be sloped to allow thrown objects to roll or slide off the screen, away from the intake.

Many existing buildings have air intakes that are located at or below ground level (Figure 4-3). Wall-mounted and below-grade intakes close to the building can be elevated by constructing a plenum or external shaft over the intake protected with sloping screens. Some protection can be achieved with physical security measures, such as placing fencing, surveillance cameras, and motion detectors around the intakes to facilitate monitoring by security personnel. These measures can help prevent or detect malicious acts but are less effective than elevating the intakes.

Figure 4-3:
An intake accessible from ground level

4.4.1.2 Isolating Zones

Large buildings typically have multiple HVAC zones, with each zone served by its own air-handling unit and duct system. In practice, these zones are not completely separated, particularly if they are on the same floor. Air flows between zones through hallways, atria, and doorways that are normally left open.

Isolating the separate HVAC zones minimizes the potential spread of an airborne hazard released internally by reducing the volume of space and therefore the number of people exposed. Zone separation also provides limited benefit against an external release, as it increases internal resistance to air movement produced by wind and buoyancy, thus reducing the rate of infiltration. In essence, isolating zones divides the building into separate environments, limiting the effects of a single release to an isolated portion of the building. Isolation of zones requires full-height walls with doors between adjacent zones kept closed.

For buildings that have access control, three entry zones are of concern for possible deliberate internal releases of hazmat. These entry zones are: (1) the lobby and cloakroom, where people await entry into the secure area of the building; (2) the mailroom, where mail is received for distribution; and (3) the loading dock, or the area where supplies or equipment are received and held temporarily awaiting distribution.

Where people, mail, or supplies/equipment enter the building before being screened, the ventilation system of the entry area or lobby area where they await screening should be isolated from the rest of the building. This separation is to prevent the movement of airborne hazards into the protected areas of the building in case of an indoor release in the entry zones. To achieve this isolation, the following measures should be employed:

- A separate air-handling unit should be provided for the entry area.
- Exhaust fan(s) should be used to create a slight negative pressure differential in the entry area relative to the rest of the building.
- The entry area should be surrounded with full-height walls. Walls should fully extend and be sealed to the undersides of the roof, the floor above, or hard ceilings (such as gypsum wallboard ceilings). All visible cracks, junctures between walls and ceiling, roof, or floor above, and all wall and roof penetrations should be sealed too.
- All exterior doors should have an airlock or a vestibule to maintain the pressure differential as people enter and exit. When entries are infrequent, an airlock is not essential, particularly for mailrooms or supplies receipt areas, but the doors should be of the low-leakage type.

Isolated entry zones can be incorporated in both new and retrofit designs. These measures can also reduce the potential disruptive effects of hoax letters purported to contain hazmat. Isolating storage areas where hazmat are kept or processed within a building is addressed by building fire codes. The approach for isolation of storage areas is similar to that applied for entry areas.

4.4.1.3 Installing Vestibules, Airlocks, or Revolving Doors

Vestibules, airlocks, and revolving doors provide a means of reducing uncontrolled airflow at main entrances as people enter and exit a building. These physical barriers serve two functions—to prevent the exchange of indoor and outdoor air through an open boundary door and to retain building pressure when a boundary door is opened. They are most beneficial in multistory buildings at times of great indoor-outdoor temperature differences, i.e., in winter and summer. Particularly in tall buildings, buoyancy driven airflows can be very large. Buoyancy flows are upward in the heating season and downward in the cooling season, as Figure 4-4 illustrates. Thus in the heating season, a building is more vulnerable to a ground-level outdoor release than in the cooling season. Vestibules and airlocks are effective only when a single set of doors is open at any given time.

Vestibules, airlocks, and revolving doors provide a means of reducing uncontrolled airflow at main entrances as people enter and exit a building.

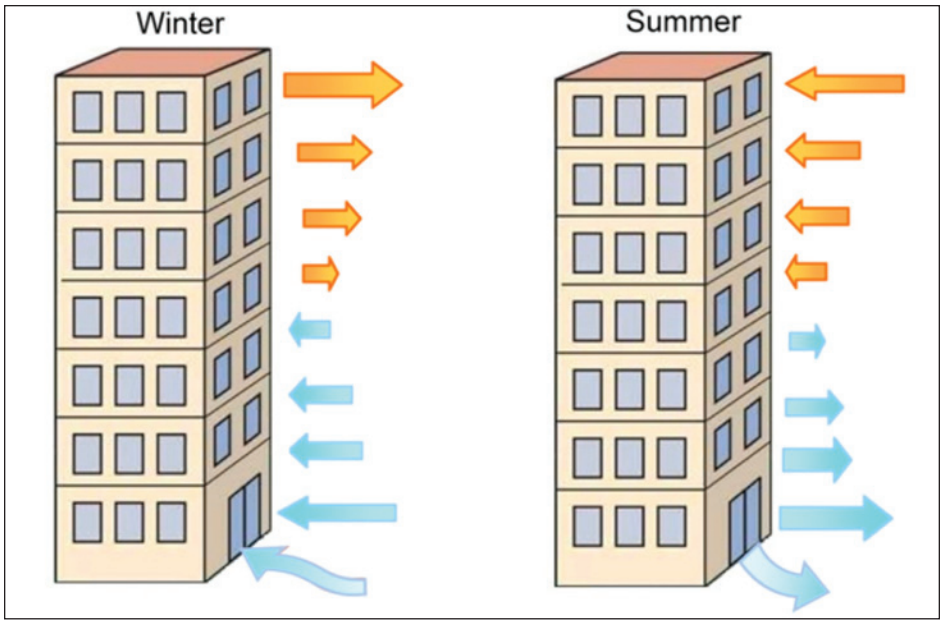


Figure 4-4:
Buoyancy pressures on a building in heating and cooling seasons

4.4.1.4 Securing Mechanical Rooms

Maintaining physical security on mechanical rooms is a simple measure to prevent the direct introduction of hazmat into the system of ducts that distributes air to the building. It requires locking and controlling the access to all mechanical rooms containing HVAC equipment, both with interior doors and exterior doors. Access to the exterior air intakes (roof-mounted or otherwise) must also be controlled, as they are frequently not located in the mechanical rooms.

4.4.1.5 Entry Inspections

Among the physical security measures for preventing CBR attack, only the entry inspection requires the capability to detect toxic agents. Because of technical challenges in detecting and reliably identifying agents in a container, entry inspection is most practical for chemical agents and least practical for biological agents. However, entry inspections to prevent containers of toxic agents from being brought into a building are only practical when access to the building is controlled by security guards.

Among the physical security measures for preventing CBR attack, only the entry inspection requires the capability to detect toxic agents.

Entry inspections have varying degrees of effectiveness for both deterrence and detection. No practical technology is available for rapid, non-intrusive detection or identification of toxic agents in containers. Methods currently applied base exclusion on the type of container or on detecting quantities of specific chemicals on exposed surfaces.

For biological agents, screening is unlikely to be effective. Significant quantities can be easily concealed in common personal items that would go unnoticed in even a thorough visual search. There are no non-intrusive detection devices for such substances, which can be disseminated throughout a building by simply opening an envelope indoors.

4.4.1.6 Video Surveillance

The principles of deterrence and detection are also applied in the use of video surveillance equipment. For detection to be effective in preventing or mitigating the effects of a release, images from the cameras must be monitored continuously in real time. For deterrence, the surveillance must be overt rather than covert. Generally, surveillance cameras should be placed in common areas that are not within the normal view of security personnel. Indoors, these areas include hallways, cloakrooms, and, obscure parts of the lobby. Outdoor areas include views of unsecured air intakes and areas where vehicles or pedestrians may approach the building undetected (presumably with the intention of releasing a toxic agent).

4.4.2 Air Purification Strategy – Mechanical and Architectural Measures

4.4.2.1 High-Efficiency Air Purification with Pressurization

Among the various approaches for protecting buildings from CBR attack, high-efficiency air purification provides the highest level of protection against outdoor releases. Air purification on a continuous basis is the only protective measure that provides a high level of protection against a covert, remote outdoor release. All other approaches rely on detecting an airborne hazard in real time.

Among the various approaches for protecting buildings from CBR attack, high-efficiency air purification provides the highest level of protection against outdoor releases.

For high-efficiency air purification to be effective, the following must be used:

- Low-leakage mounting frames for mechanical filters
- Pressurization of the protected spaces

All air filters are not equal and they vary widely in removal efficiency and tightness of seal against bypass in their retainers. Air purification involves the removal, neutralization, or disinfection of toxic aerosols, gases, or vapors from an air stream. For biological agents, protection can be achieved through disinfection of air with ultraviolet germicidal irradiation (UVGI) or plasma systems (see Section 4.4.2.5). Filtering the full

spectrum of CBR toxic agents requires three different filtration processes; most commonly, these are mechanical filtration for aerosols, physical adsorption for chemical agents of low vapor pressure, and chemisorption (chemical adsorption) for chemical agents of high vapor pressure.

Conventional CBR filtration systems apply these three processes with a HEGA filter containing impregnated carbon and a HEPA filter in series. Generally applied as a continuously operating system, this filtration is the highest level of protection. It can be applied to the whole building (excluding some spaces requiring high ventilation rates, such as garages or boiler rooms), or to selected spaces, i.e., safe rooms.

4.4.2.2 High-Efficiency Gas Adsorbers

A filter bed containing activated, impregnated carbon granules is the standard medium for high-efficiency filtration of toxic chemical vapors and gases. Activated carbon removes molecules from an air stream by adsorption, trapping molecules in the pores of the carbon. This process works best against large molecules, that is, chemicals of low vapor pressure. Because of extensive micro-porosity and a wide range of pore sizes, activated carbon is a highly effective sorbent for removing a broad range of chemical vapors.

A rule of thumb is that a chemical agent is filtered by physical adsorption when its vapor pressure is below 10 mm Hg. Examples of chemical warfare agents filtered by physical adsorption are sarin, mustard, and VX (nerve agent). Filtering chemicals of higher vapor pressure requires chemisorption, a more complex process. Chlorine, hydrogen cyanide, and phosgene are three gases that are filtered by chemisorption.

A filter bed containing activated, impregnated carbon granules is the standard medium for high-efficiency filtration of toxic chemical vapors and gases.

The service life of a HEGA filter containing impregnated carbon varies with the environment in which it is used. Hot, humid environments produce a shorter chemisorption life than cool, dry environments. The level of air pollution affects the service life as well, but for standard adsorbers, the expected service life in most environments is 3 to 4 years.

Generally, filter units available commercially are not designed to standards that ensure a high level of protection against highly toxic CBR materials. Some may provide very little protection, particularly if the manufacturer is not experienced in designing and building ultra-high-efficiency filter units. Minimum requirements that ensure a high level

of protection against highly toxic CBR materials are listed below. The vendor should provide certifications that the following requirements are met.

- The filter unit must have a HEPA filter and a HEGA filter in series.
- The adsorber must contain ASZM-TEDA (activated carbon, impregnated with copper, silver, zinc, molybdenum, and triethlyenediamine) or the equivalent. Carbon mesh size should be between 20x50 and 8x16.
- The adsorber must have an efficiency of at least 99.999 percent for physically adsorbed chemical agents and 99.9 percent for chemisorbed agents.
- The adsorber must have a total capacity of 300,000 milligram-minute per cubic meter for physically adsorbed chemical agents.
- The bypass at the seals between the adsorber and its housing must not exceed 0.1 percent.
- For installation of the filter unit outside the protected space, the fan must be upstream of the filters (blow-through configuration). For installation inside the protected space, with a duct from the wall to the filter unit, the fan must be downstream of the filters (draw-through configuration).
- When a flexible duct is used outside the shelter to convey air from the filter unit to the safe room, it must be made of a material resistant to the permeation of toxic chemicals.
- Where chemical manufacturing and storage facilities in the community present a special risk for release of toxic materials, special sorbents or sorbent layers may be required. In some cases, the chemicals produced/stored may not be filterable with a broad-spectrum impregnated carbon. For example, protection against ammonia from a nearby ammonia plant requires a special adsorber.

Three configurations of HEGA—radial-flow, V-bed, and pleated—can provide the capability for continuous operation. These three adsorber types and filter units that contain them are shown in Figure 4-5.

Figure 4-5: Three types of adsorbers and filter units for CBR protection of buildings

Sizing the filter unit correctly for the protected space is important. An undersized filter unit, one that provides inadequate flow for pressurization, substantially lowers the protection factors. Filter unit(s) must be sized to provide makeup air at a flow rate sufficient to produce a pressure of at least 0.1 inches of water gauge (inH2O) in the shelter for protected zones of one or two stories. Taller buildings require an internal pressure higher than 0.1 inH2O to overcome the buoyancy pressures that occur during extreme weather conditions (i.e., large temperature differences between the inside and outside of the building).

The airflow rate needed to achieve this pressure in a safe room varies with the size and construction of the safe room. Generally, commercial filter units available for home or office safe rooms are under rated with regard to the quantity of air needed for pressurization. For safe rooms of frame construction and standard ceiling height, most can be pressurized to 0.1 inH2O with airflow in the range of 0.5 to 1 cubic feet per minute (cfm) per square foot. Section 4.4.3 provides additional guidance in estimating the size of the filter unit for a safe room based on square footage.

The recommended procedure for ensuring that pressurization can be achieved, after all permanent sealing measures have been completed, is to perform a blower door test per ASTM E779-03, *Standard Test Method for Determining Air Leakage by Fan Pressurization*, with temporary sealing measures in place. Figure 4-6 shows a blower door test being conducted in the entrance hallway of a residential building to measure the air leakage characteristics of the building and to identify leakage pathways to be sealed.

Figure 4-6:
Blower door testing

4.4.2.3 High-Efficiency Particulate Air Filters

For protection against CBR agents, a HEPA filter is always employed in series with, and upstream of, a carbon adsorber. The HEPA filter can also be employed without the carbon filter, if the approach to CBR protection is to apply continuous, high-efficiency filtration with building

For protection against CBR agents, a HEPA filter is always employed in series with, and upstream of, a carbon adsorber.

pressurization for the biological aerosol threat (which is not detectable in real time) and sheltering in place for the chemical and radiological threats (which are detectable in real time).

The level of protection provided by an air filtration system is determined by the single-pass removal efficiency when the protected space is pressurized to a level that prevents infiltration caused by wind and buoyancy pressures.

Theoretically, the fraction of 1 μm mass-median-diameter (MMD) particles penetrating HEPA media at rated flow is about 10^{-17}. In practice, this very low penetration value is limited by the capability to seal the filter medium to the frame and the frame to the filter retainers so that no bypass occurs. Unlike carbon adsorbers, HEPA filters gain efficiency as they load with particles removed from the air. In loading, their resistance to air flow also increases.

The limiting factor in high-efficiency air purification is often the leakage, or peripheral bypass at the mounting frames of the filters. Filter mounting systems for high-efficiency filters are designed expressly to allow very little bypass. Typically HEPA and HEGA filters used for protection against toxic agents are subjected to in-place leak testing when they are installed. For HEGA filters, the leak testing involves the use of a gas that is only temporarily retained in the carbon bed. The testing is performed with a liquid aerosol in the size range of 0.3 to 0.6 μm MMD to demonstrate a leakage less than 0.03 percent for HEPA filters and 0.01 percent for HEGA filters.

4.4.2.4 Medium-Efficiency Mechanical Filtration

Approaches to filtration for a lower, or intermediate, level of protection involve the use of filters of efficiency less than HEPA and HEGA filters and the use of recirculation filtering. Recirculation filtering involves drawing air from the same space to which it is discharged. Also described as internal filtering or multiple-pass filtering, this type of filtering does not require the very high removal efficiency a single-pass filter unit used for pressurization does, and its costs are substantially lower.

The protection recirculation filtering provides varies with a number of factors, including the tightness of the building or safe room in which it operates, the efficiency and flow rate (i.e., clean air delivery rate) of the filter unit, and the volume of the room or building the filter unit serves. The level of protection that can be achieved by recirculation filtering

compared to pressurization can be illustrated in terms of a protection factor, the ratio of external dosage (concentration integrated over time) to internal dosage. External filtration systems with HEPA and HEGA filters can yield protection factors greater than 100,000. Recirculation filtering yields protection factors that are variable and likely to be about 100 or lower.

Recirculation filter units can be installed much more easily in a building, in many cases without any modifications to the building or substantial installation costs. One advantage of recirculation filtering is the purging of contaminants from a building following an indoor release. Commercially available indoor air-quality units are recirculation filters that typically contain adsorbers and HEPA filters. These are available in a variety of configurations, including ceiling-mounted, duct-mounted, and free-standing floor or table-top units. These types of filter units have been applied for enhanced sheltering in place to provide intermediate levels of protection against chemical warfare agents to buildings under the Chemical Stockpile Emergency Preparedness Program.[7]

Unlike the filter units for pressurized systems, there is no standard for the application of recirculation filter units in protective shelters, either in filtration capacity, clean air delivery rate, or flow rate per square foot of shelter area. Also, commercial recirculation filter units do not employ impregnated carbon to provide substantial capacity for toxic chemicals of high vapor pressure.

A second approach that achieves intermediate levels of protection against biological and radiological agents is to use standard HVAC particulate filters that have efficiency ratings higher than the filters typically used but not as high as HEPA.

Particulate air filters are commonly rated based on their collection efficiency, pressure drop (airflow resistance), and particulate holding capacity. Two filter-rating systems of the American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE) are Standard 52.1-1992 and Standard 52.2-1999.[8] ASHRAE Standard 52.1 is based on measurements of arrestance, dust spot efficiency, and dust holding capacity. ASHRAE Standard 52.2 is based on measurements of particle size efficiency. Standard 52.2 is a newer standard and is more descriptive in that it quantifies filtration efficiency in different particle size ranges and is more applicable in determining a filter's effectiveness to capture a spe-

7 More information about this program is available on FEMA's Web site at www.fema.gov/about/divisions/thd_csepp.shtm.

8 Both standards are available for purchase at www.ashrae.org

cific agent. Standard 52.2 reports the particle size efficiency as a MERV rating between 1 and 20, with the higher rating indicating a more efficient filter. Figure 4-7 shows the minimum particle size efficiency for three size ranges for each of the MERV numbers.

Particulate Filtration Level	ASHRAE 52.2				Typical Applications
		Particle Size Range			
	MERV	3 to 10 µm	1 to 3 µm	0.3 to 1 µm	
HVAC Filters 	1	< 20%	-	-	Residential, light, pollen, dust mites
	2	< 20%	-	-	
	3	< 20%	-	-	
	4	< 20%	-	-	
	5	20 - 35%	-	-	Industrial, dust, molds, spores
	6	35 - 50%	-	-	
	7	50 - 70%	-	-	
	8	> 70%	-	-	
	9	> 85%	< 50%	-	Industrial, Legionella, dust
	10	> 85%	50 - 65%	-	
	11	> 85%	65 - 80%	-	
	12	> 90%	> 80%	-	
	13	> 90%	> 90%	< 75%	Hospitals, Smoke removal, bacteria
Medium Efficiency Filters 	14	> 90%	> 90%	75 - 85%	Hospitals, Smoke removal, bacteria
	15	> 90%	> 90%	85 - 95%	
	16	> 95%	> 95%	> 95%	
HEPA and ULPA Filters 	17	-	*	≥ 99.97%	Clean rooms, Surgery, biodefense, viruses
	18	-	*	≥ 99.99%	
	19	-	*	≥ 99.999%	
	20	-	*	≥ 99.9999%	

* Efficiency against 1–3 microns is much higher than efficiency against 0.3 micron size.

Figure 4-7: Efficiencies relative to particle size range and MERV rating

SOURCE: AMERICAN SOCIETY OF HEATING, REFRIGERATING, AND AIR- CONDITIONING ENGINEERS (ASHRAE) STANDARD 52.2: METHOD OF TESTING GENERAL VENTILATION AIR-CLEANING DEVICES FOR REMOVAL EFFICIENCY BY PARTICLE SIZE, ATLANTA, GA., 1999

Protection against toxic aerosols, primarily biological agents, can be improved without requiring the use of relatively expensive HEPA filtration systems. Upgrading HVAC filters to MERV 14, 15, or 16 with improved filter seals can provide substantial gains in protection against aerosols in the 1- to 5-μm MMD range when the outdoor air fraction of the air-handling units is adjusted to achieve building pressurization. These filters have deeper pleats or mini-pleat configurations to achieve a higher figure of merit (ratio of efficiency to pressure drop) than standard HVAC filters.

Protection against toxic aerosols, primarily biological agents, can be improved without requiring the use of relatively expensive HEPA filtration systems.

A filter bank such as the one shown in Figure 4-8 can be modified to achieve a greater level of protection against aerosols by upgrading the filters to a higher MERV rating and may require modifications to existing retainers. The cost of these filters is higher, but because the filter media have greater surface area, their reduced operating costs are likely to offset the higher cost of the filters. Pathways for bypass include filter frames and retainers, as well as access doors on air-handling units, as illustrated in Figure 4-9.

Figure 4-8:
A bank of pleated MERV 8 pre-filters in front of MERV 14 cartridge filters in an office building air-handling unit

Figure 4-9:
Pathways for air to bypass filters in an air-handling unit

4.4.2.5 Use of Other Types of Air Purification Systems for Aerosols

Other technologies for filtration of aerosols or disinfection of air have been employed in building HVAC systems but typically not for protection against CBR agents. Among these are UVGI, electrostatically enhanced fiber, electrostatic precipitation, and reactive fibers. These have been employed at medium to high efficiencies but, generally, below the efficiency necessary for protection from biological agent aerosols.

As is the case with conventional filtration for HVAC systems, cost is the driver in selecting a filtration or purification system. One issue with regard to CBR protective applications is whether these alternatives can achieve high efficiencies at lower operating, maintenance, and initial costs than mechanical filtration, including configurations such as mini-pleats.

Ultraviolet Germicidal Irradiation (UVGI) involves the use of C-band ultraviolet (UV) light (wavelength at or near 253 nanometers) to inactivate microorganisms by breaking down organic molecular bonds, producing cellular or genetic damage to the microorganisms. This wavelength may be generated by continuous or pulsed electrical discharge through low-pressure mercury vapor enclosed in a glass tube. UV lamps have been used to inactivate microorganisms for many years, and studies on their use for disinfection of air date back to the 1930s. A rapid increase in the development of this technology came in the 1960s, with work directed at the control of tuberculosis.

Studies have shown the effectiveness of UV light against biological agents to be dependent on the intensity and duration of exposure. These studies show that microorganism susceptibility varies substantially and is dependent mainly on the presence and thickness of a cell wall.

UVGI devices for use in HVAC systems are of two types: those that irradiate filter media to kill microorganisms captured on the filter, and those that irradiate the air flowing through a duct or plenum. The latter has a greater cost benefit because it produces little or no pressure drop; however, higher UV intensities are required to achieve the necessary exposure duration and intensity as airborne microorganisms pass by at typical duct velocities.

UVGI devices for use in HVAC systems are of two types: those that irradiate filter media to kill microorganisms captured on the filter, and those that irradiate the air flowing through a duct or plenum.

Experience shows that dust collecting on bulbs and reflective interior surfaces reduces the UV-light intensity, necessitating the addition of a mechanical filter and, consequently, causing a higher pressure drop. Because both types require mechanical filtration, LCCs of both may be higher than the costs of mechanical systems of similar efficiency. UVGI is effective only for biological aerosols and has no significant effect on other toxic aerosols, which must be filtered with conventional particulate filters. Not all UVGI systems are adequate for protection against biological agents (particularly larger microbes, such as spores, which are more resistant to UVGI).

Electrostatically Enhanced Filtration uses mechanical filters with their efficiency increased by electrostatic interactions in the filtration medium. These include powered (active) and non-powered (passive) technologies. The electrostatic charge may be applied at the time of manufacture, be generated by the flow of dry air through the media, or be generated by a continuous external power source. Electrostatically enhanced filters provide the advantage of a high initial efficiency, especially for fine particles (less than 1 μm MMD) at low pressure drop, generally, about one-half to one-third the pressure drop of a mechanical filter with the same collection efficiency. These filters, therefore, provide a means of economically retrofitting existing air-handling units to achieve higher efficiencies. Filters with an external electric field can achieve substantial performance gains without an increased pressure drop, and they have been shown to have a germicidal effect. The lower operating costs offset higher initial and maintenance costs. The lower pressure drop and high

collection efficiency indicates the LCCs may be about 20 percent lower than a mechanical filter of similar efficiency. Overall, electrically enhanced filters outperform conventional mechanical filters in collection efficiency as well as maintenance requirements; however, studies have shown an inability of passive electrostatic filters to maintain efficiency for significant periods of time.

Electrostatic Precipitators (ESPs) use electrical forces to attract airborne particles to collection plates parallel to the air stream. A high voltage applied to discharge electrodes in the air stream breaks down nearby gas molecules to create a flow of ions to the collection plates. The ions interact with particles in the air, causing them to become charged. The charged particles migrate to the grounded collection plates, where they are retained. ESPs differ from electrically enhanced fibers described above but have been applied in combination with electrically enhanced fibers for increased efficiency. For HVAC system applications, precipitators are referred to as electronic air cleaners. As high-voltage devices, ESPs produce ozone, which is toxic and has deleterious effects on materials in buildings. Some pre-filtration may be required to trap large particles that can cause shorting and excessive arcing, to prevent higher levels of ozone. The cells of electronic air cleaners must be regularly cleaned, usually at a frequency of 1 to 3 months, to maintain efficiency. ESPs are sensitive to particle size, gas velocity, and particle resistivity.

Reactive Fibers/Membranes neutralize or deactivate contaminants trapped on the filter medium. This type of filter incorporates biocidal materials into traditional filter media or membranes to reduce or eliminate residual hazards associated with microorganisms trapped in the media. For biological aerosols, the reactive fibers/membranes provide the advantage of disinfecting the filter medium, preventing growth and migration through the medium over time. The costs are comparable to that of the basic filter medium. Treatments may lose reactivity quickly with dust loading and with reaction with moisture in the air.

The following criteria should be considered in selecting an air purification system, whether it is mechanical filtration or one of these alternative technologies for CBR protection.

- **High efficiency:** The system must provide an efficiency of removal, neutralization, or disinfection of 99.99 percent or greater if used to purify makeup air for pressurization of protected spaces. For recirculation filtering, which yields a lower level of protection, a lower efficiency of about 99 percent is acceptable.

- **Full-spectrum capability:** An air purification system for aerosols should provide the capability for radiological agents and toxic chemical aerosols as well as biological agents. A system for chemical agents should provide the capability for chemicals of both high and low vapor pressure.
- **Certification:** The system should have undergone testing by a government laboratory or a recognized commercial laboratory and be certified for high-efficiency performance.
- **Economy:** The system should provide economical operation throughout its life cycle. Operating costs, maintenance costs (including replacement of filter elements, bulbs, and/or consumables), and initial costs, including installation, should be considered.
- **Reliability:** Data should be available to show that the system can function properly over its intended service life under all expected ambient conditions.
- **Environmental effects:** The air purification system should not adversely affect the environment of the building through excessive noise, heating of makeup air, or generation of ozone, other irritants, or toxic reaction products.

4.4.3 Pressurization

Many buildings are pressurized, but few are pressurized with purified air (i.e., air filtered at high efficiency) as is necessary for a high level of protection against an outdoor release of CBR agents. Pressurization combined with CBR filtration ensures that when the protective system is operating, all outdoor air enters the building through the high-efficiency filters. The infiltration air exchange that normally occurs as a result of the pressures of wind, buoyancy, and normal HVAC fans must be reduced to zero. This is achieved primarily by introducing filtered air at a rate sufficient to produce an overpressure in the building and create an outward flow, exfiltration, through cracks, joints, seams, pores, and other openings in the building envelope.

Pressurization with CBR filtration is usually the element of high-level CBR protection that is a primary cost driver, because it typically necessitates a higher flow rate of outdoor makeup air than is necessary for health and comfort. This increases the heating and cooling equipment costs and operating costs. Because of the cost of pressurization, it is most cost effectively applied by reducing the leakage rate of the selected building envelope or selecting a smaller envelope to be protected. The latter is the basis for pressurizing selected safe rooms rather than whole buildings.

At least part of the building is always excluded from the pressurized area. Excluded areas have or require high rates of air exchange with the outdoors, such as mechanical rooms containing boilers or generators, garages, and receiving areas. Mechanical rooms that contain air-handling units must be included in the protective envelope. Building tightness is beneficial for both pressurized and unventilated shelters, as well as for energy efficiency in normal operation. For existing buildings, reducing the air leakage rate involves sealing penetrations, as is typically done in weatherization.

The size/capacity of filter units needed for pressurization is determined by the air-leakage characteristics and size of the building. The leakage rate of an office building typically varies from about 0.1 cfm per square foot to 2 cfm per square foot at a pressure of 0.2 inH2O, depending on the type of construction. The cost of installing a high-efficiency CBR filtration system varies directly with the leakage rate. Installation of a CBR system in an average building may cost $30 to $100 per square foot of protected floor space.

Three approaches are used for estimating the leakage rate of a selected envelope to determine the filter unit capacity needed for pressurization:

- Parametric estimates based on square footage from blower-door test data previously collected by the U.S. Army Corps of Engineers. See Table 4-1 below.
- Blower-door testing of the specific, selected envelope with temporary sealing measures applied (tape and plastic) to approximate the permanent sealing measures and dampers to be installed later.
- Use of component leakage tables from ASHRAE (1992a).

Table 4-1: Leakage Per Square Foot for 0.1 inH20 (Estimated Makeup Airflow Rate Per Square Foot [Floor Area] to Achieve an Overpressure of 0.1 inH20)

Construction Type	Leakage (cfm per square foot of floor area)
Very Tight: 26-inch-thick concrete walls and roof with no windows	0.04
Tight: 12-inch-thick concrete or block walls and roof with tight windows and multiple, sealed penetrations	0.2
Typical: 12-inch-thick concrete or block walls with gypsum wall board ceilings or composition roof and multiple, sealed penetrations	0.5
Loose: Wood-frame construction without special sealing measures	1.0

Operating costs of CBR filter units are typically high because of the relatively high pressure drop across the filters. This pressure drop ranges from approximately 1 to 4 inH2O for HEGA filters and 1 to 2 inH2O for HEPA filters. Pressure drops of HEPA filters can be reduced substantially by increasing filter surface area with increased pleat counts and greater filter depth.

Applying external filtration to a building requires modifications to the building's HVAC system and electrical system and, usually, requires minor architectural changes to reduce air leakage from the selected protective envelope. Additional mechanical space for the filter units is also required. These filter units can be mounted on rooftops, at ground level in security fenced areas, and in indoor mechanical spaces.

4.4.4 Heating, Ventilation, and Air Conditioning System Configurations to Accommodate Air Purification

If resources are not available to employ air purification and pressurization to achieve the highest efficiency (at the highest cost) in new construction or retrofit, HVAC systems can be configured or selected for adaptability to strategies of air purification, unventilated sheltering in place, and physical security.

For the air-purification strategy, air-water HVAC systems provide the most effective means of applying high-efficiency or medium-efficiency filtration. With such systems, the most efficient and effective approach is to supply and temper fresh air only through central air-handling units with no return air. High-efficiency filtration is applied to these central ventilation units. Occupant-controlled heating and cooling is supplied by fan coil units that do not supply outdoor air.

The use of unit ventilators is undesirable for CBR protection strategies of air purification and unventilated sheltering. Unit ventilators introduce fresh air into each room and, therefore, require high-efficiency filtration and/or low leakage automatic dampers at each unit. However, filters of high efficiency and low peripheral bypass are not typically available for such units. These units also increase the number of dampers in the system that must be closed for unventilated sheltering or pressurization, and often the dampers of such units do not seal well and are not easily or well maintained. The vulnerability of unit ventilators commonly used in schools is similar to that of open windows.

If resources are not available to employ air purification and pressurization to achieve the highest efficiency in new construction or retrofit, HVAC systems can be configured or selected for adaptability to strategies of air purification, unventilated sheltering in place, and physical security.

Limitations of Sheltering in Place

Sheltering in place against a toxic terrorist attack provides substantial protection against agents released outdoors by interrupting the flow of fresh air, but it has limitations. The following limitations should be considered:

- To be effective against a toxic release, sheltering in place must be implemented without delay—as rapidly as 1 minute if the release is close to the building.
- In an actual release, i.e. a toxic cloud engulfs a building, sheltering is most effective if the hazard is of short duration. Because the hazard duration is not predictable at the outset, emergency communication with authorities is essential while sheltering so that other options, such as evacuation and/or use of escape respirators, can be evaluated once information on the hazard and its likely duration becomes available.
- If designated/prepared safe rooms are employed, carbon dioxide concentrations can rise to unhealthy levels if the safe room is very tightly sealed, the occupant density is high, and the stay is long.
- Implementing sheltering in place requires rapid building-wide notification and coordinated actions (turning off all building fans and securing doors and windows). As such, it requires planning and assigning responsibilities beforehand, particularly the responsibility of an Emergency Action Coordinator.
- The use of safe rooms is not essential to effective sheltering. Safe rooms, particularly those with no exterior walls, increase the level of protection by imposing greater resistance to the flow of airborne toxic materials that infiltrate the building shell.

4.4.5 Sheltering in Place

Sheltering in place, or unventilated sheltering, has become widely used for protecting people against airborne hazards of short duration. This protective measure was originally developed for protection against fallout from a nuclear accident or attack. For many years, it has been applied or planned for application against the accidental release of toxic materials in chemical manufacturing, storage, and transport. Most recently, it has been planned and implemented for protection against a terrorist or criminal attack involving toxic agents.

Sheltering in place is a widely employed protective measure, in part because it is easily and inexpensively applied. It can be employed in most buildings, both commercial and residential, and at varying levels of protection, cost, and preparation. In its rudimentary form, it can be implemented with a list of simple instructions. Such instructions for sheltering in a dwelling consist of closing all windows, doors, and vents; turning off all fans and combustion heaters; and turning on the radio or TV for emergency instructions. More extensive preparations for sheltering in place are described in detail in FEMA 453, *Design Guidance for Shelters and Safe Rooms* (2006).

Sheltering in place can be precautionary or in response to an actual release. Precautionary sheltering may involve a longer period, because authorities may judge the threat to a building to be possible but not actual. For example, the plume of toxic gas emanating from a derailed tanker car may pose a threat to a community only when the wind shifts or corrective actions fail.

The level of protection provided by sheltering in place varies with the tightness of the building or rooms used for sheltering.

Aside from precautionary use, sheltering in place is most effective against transient hazards. When an actual hazard is likely to exist for several hours, sheltering may not be the best option, because the protection it provides diminishes with time. An example of conditions in which sheltering would not be appropriate is the nearby release of a bulk quantity of toxic chemical in calm and stable atmospheric conditions. Sheltering is often the best course of action initially, while the incident is unfolding and until the facts are known. Sheltering protection decreases with time, but normally the full details of the release and potential corrective or rescue measures are determined early on, when sheltering is most effective. Evacuation during this period is likely to increase risk and uncertainty.

The level of protection provided by sheltering in place varies with the tightness of the building or rooms used for sheltering. Using a sealed, interior room within a closed building provides greater protection than simply a closed building alone. The basis for use of designated safe rooms for sheltering in place is that a closed interior room has greater resistance to infiltration air flows driven by wind and buoyancy. However, use of designated safe rooms is not essential. In many cases, large office buildings do not have sufficient space in interior rooms for sheltering all building occupants.

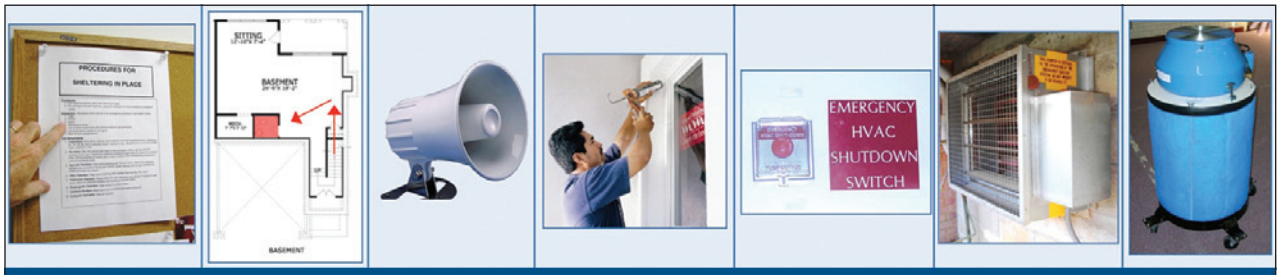
For maximum protection, sheltering in place requires two distinct actions relative to the building's indoor-outdoor air exchange rate. The first is to reduce the air exchange rate before the hazardous plume arrives. The second is to increase the air exchange rate as soon as the hazardous plume has passed. The latter is done by opening all windows and doors and restarting all fans to ventilate the building, actions that comprise the purging phase of sheltering.

To be effective, particularly against a deliberate CBR attack that may offer little warning time, sheltering in place must be implemented rapidly; preferably the transition will be completed before the leading edge of the plume or cloud reaches the building. Consequently, having the ability to turn off all building fans quickly is important. In large buildings, controls or switches for deactivating these fans are often in diverse locations that may not be rapidly accessible.

4.4.5.1 Enhancements for Sheltering in Place

Sheltering in place has several levels (Figure 4-10) that include enhancements for three purposes: (1) to yield a tighter enclosure for sheltering; (2) to make the transition to the sheltering mode more rapid, particularly for large buildings; and (3) to introduce recirculation filtering for higher levels of protection. The main components of the various levels are as follows:

- Written instructions for expedient sheltering in place
- Written plans and assigned responsibilities for:
  - Shutting down building fans and combustion sources
  - Making building-wide announcements to begin sheltering in place
  - Securing doors and windows
  - Accounting for all employees and visitors
- Permanent sealing measures (i.e., weatherization techniques)
- Rapid notification system for large buildings, i.e., a building-wide public address system
- Switch or building automation system control for rapidly turning off fans in large buildings
- Equipment for rapid, temporary sealing of the building or safe room, such as motorized dampers, manual dampers, or tape and plastic
- Selected safe rooms to which the above measures are applied
- Recirculation filter units with both carbon adsorbers and HEPA filters



1. Developing written plans and assigning responsibilities for doors, switches, emergency announcements, training, and employee accountability.
2. Selecting and designating safe rooms.
3. Developing a rapid notification system, e.g., public address system
4. Applying permanent sealing measures (weatherization techniques) to safe rooms and/or the building.
5. Developing single-command/switch control of building fans for rapidly turning off multiple fans
6. Preparing for rapid, temporary sealing of the building and safe rooms, e.g., motorized dampers, tape and plastic
7. Installing recirculation filter units with carbon adsorbers and HEPA filters.

Figure 4-10: Seven levels of measures for sheltering in place

Other components of sheltering in place are:

- Radio, television, or telephone for emergency information
- Access to drinking water, toilets, and first aid kit while sheltering
- Signage to provide condensed instructions at designated safe rooms
- Periodic training and exercises (similar to fire drills)
- Outdoor surveillance and security for large buildings and/or a community-wide warning system

Additional detailed guidance for applying these enhancements to safe rooms is presented in FEMA 453. Examples of the implementation of these measures are available in a 1999 U.S. Army Corps of Engineers report, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, and a July 2008 report prepared on behalf of the U.S. Army Chemical Materials Agency, *Collective Protection Shelters of the Chemical Stockpile Emergency Preparedness Program: Technical Record and Lessons Learned* (DOD 2008a).

Installing single-switch control or using the building automation system to turn off all fans affecting air exchange is an important capability. This capability can be enhanced by installing automatic dampers on fresh air intakes and exhaust fans not already equipped with back-draft dampers. These dampers should be rapid acting and have positive sealing, but must not be so rapid as to cause duct collapse while fans continue to turn by inertia. Turning off all fans reduces the air exchange, but the wind and buoyancy pressures that act on a building cannot be turned off. Though a building is tightly sealed, a small exchange of indoor and outdoor air is still likely.

In practice, the uncertainty about when to begin the purging phase, after the hazardous cloud has passed, makes implementation in a timely manner unlikely. The decision to emerge from a shelter would have to be made by emergency responders, and making the all clear announcement affecting a large area could take much more time than required for maximum protection. The effect of delayed purging can be minimized by the use of escape respirators in combination with unventilated sheltering. Wearing the respirators while exiting the building after the outdoor hazard has passed adds a measure of safety.

An additional enhancement for purging is to provide controls for smoke-purge fans that will allow the building, or selected floors, to be purged rapidly by introducing outdoor air at high flow rates. This capability can also be employed after an indoor release, as long as the result is not the spreading of contamination to adjacent open space and buildings.

Although sheltering in place is for protection against an external release, sheltering in place on one or more floors of a multistory building is possible—but more complex—after an internal release has occurred on a single floor. For sheltering in place under such conditions, stairwells must be isolated by closed fire doors, elevators must not be used, and clear evacuation routes must remain open for use when evacuation is required. Escape respirators may be needed when the only evacuation routes are through contaminated areas.

Another consideration for sheltering in place is that occupants cannot be forced to participate. Developing a plan, that includes awareness training on sheltering in place and the events that might make sheltering preferable to evacuation, is important to ensure cooperation of likely participants. Training programs and information announcements during an event should be tailored to help occupants make informed decisions.

4.4.5.2 Safe Room for Sheltering in Place

For protection against airborne hazards, a safe room is a space selected in preparation for sheltering in place. As described in FEMA 453, a safe room can be ventilated with purified air (pressurized) or it can be unventilated. In an unventilated safe room, occupants are protected by retaining clean air inside the room (i.e., closing doors before the contaminated air reaches the interior of the building) and minimizing the exchange of air between the inside and outside.

A tightly sealed unventilated safe room provides a high level of protection; however, unventilated tightly sealed safe rooms cannot be occupied for long periods without the risk of exposure to high carbon dioxide levels. This constraint does not apply to ventilated safe rooms, which can be designed to provide filtered, conditioned fresh air at any desired rate.

The protection a safe room provides can be increased substantially by adding high-efficiency air filtration in one of two ways: (1) removing contaminants from the air as it enters the safe room (pressurization), or (2) removing contaminants as air is circulated within the room (recirculation). The two ways of incorporating filtration, or not incorporating it at all, yield three general configurations or classes of safe rooms, designated Classes 1, 2, and 3.

Table 4-2 defines these three classes and summarizes their capabilities and limitations. A common element of all three is a tight enclosure. The three classes differ in whether/how air filtration is applied, resulting in differences in cost, level of protection, and duration of protection.

- **Class 1:** In a Class 1 safe room, air is drawn from outside the room, filtered, and discharged inside the room at a rate sufficient to produce an internal pressure. The safe room is thus ventilated with filtered air, eliminating the constraints related to carbon dioxide accumulation. The internal pressure produced with filtered air prevents infiltration of outside air through leakage paths.
- **Class 2:** This class includes air filtration, but with little or no internal pressure. Without positive pressure, the safe room does not prevent the infiltration of contaminated air. A Class 2 safe room may be ventilated or unventilated. In an unventilated Class 2 safe room, air is drawn from inside the safe room, filtered, and discharged inside it. In a ventilated Class 2 safe room, air is drawn from outside but at a flow rate too small to create a measurable pressure differential.
- **Class 3:** This class, the most widely used, has no air filtering capability and is unventilated. It is a basic safe room that derives protection only by retained clean air within a tightly sealed enclosure. Use of the Class 3 safe room is commonly referred to as sheltering in place.

Class 1: Air is drawn from outside the room, filtered, and discharged inside the room at a rate sufficient to produce an internal pressure.

Class 2: Includes air filtration, but with little or no internal pressure. It may be ventilated or unventilated.

Class 3: Has no air filtering capability and is unventilated.

Table 4-2: Comparison of the Three General Classes of Toxic Agent Safe Rooms

Class	Protection	Cost	Advantages and Limitations
1. Ventilated and pressurized with filtered air	high	high	Protection has no time limits, but against some toxic chemicals of high vapor pressure, it provides no protection.
2. Filtration with little or no pressurization	medium	medium	Protective against all gases but protection diminishes with duration of exposure (and against non-filterable gases).
3. Unventilated, no filtration	low	low	Protective against all agents, but protection diminishes with time of exposure. Carbon dioxide buildup may limit time in the shelter.

The Class 1 safe room provides the highest level of protection for most chemicals but the lowest level of protection for those toxic gases that are not filterable. It is also the most expensive option. Its disadvantage is that it does not protect against a limited number of toxic gases that cannot be filtered by conventional gas filters/adsorbers.

Although the Class 2 safe room employs air filters, it does not prevent the infiltration of outdoor air driven by natural forces of wind and buoyancy. Therefore, it provides a lower level of protection than a Class 1. When exposed to an unfilterable gas, the unventilated Class 2 safe room retains a level of protection provided by the sealed enclosure. The unventilated Class 2 safe room would thus not have a complete loss of protection, as could occur with the gas penetrating the filter of a Class 1 or Class 2 ventilated safe room.

The Class 3 safe room, with no air filtration, is the simplest and lowest in cost. It can be prepared with permanent sealing measures or with the quick application of expedient sealing techniques such as applying duct tape over the gap at the bottom of the door or over the bathroom exhaust fan grille. The disadvantage is that there is no intentional ventilation; therefore, this class of safe room cannot conform to ventilation requirements of other types of emergency shelters.

4.4.5.3 Criteria for Selecting Safe Rooms for Sheltering in Place

Although the protective envelope can be defined as the whole building, a room within the building, i.e., a safe room, can provide a higher level of protection, particularly when it is tighter than the building as a whole and/or the location of the room (e.g., not on exterior walls) is less subject to wind or buoyancy forces that induce infiltration.

Any type of room can be used as a safe room when it meets the criteria listed below. In office buildings, safe rooms can be established in conference rooms, offices, stairwells, and other large common areas. In residential buildings, safe rooms can be established in bedrooms, basements, and bathrooms. Safe rooms have the following criteria:

- **Accessibility:** The safe room must be rapidly accessible to all building occupants and visitors who are to be sheltered. It should be located so that it can be reached with minimum outdoor exposure. Although no specific requirements are established for the time to reach a safe room, reaching the safe room from the most distant point in the building should take no more than 2 minutes. For maximum accessibility, the ideal safe room is one in which one spends a substantial portion of time during a normal day. The safe room should be accessible to persons with mobility, cognitive, or other disabilities.

- **Size:** The size criterion for the toxic agent safe room is the same as that of tornado shelters. Per FEMA 361, *Design and Construction Guidance for Community Safe Rooms* (2008a), the room should provide 5 square foot per standing adult, 6 square foot per seated adult, and 10 square foot per wheelchair user for occupancy of up to 2 hours.
- **Tightness:** With doors closed, the safe room must have a low rate of air exchange with the outdoors or the adjacent indoor spaces. Rooms with few or no windows are preferable if the windows are of a type and condition that do not seal tightly (e.g., older sliders). The room must not have lay-in ceilings (suspended tile ceilings) unless there is a hard ceiling above. The room should have a minimum number of doors, and the doors should not have louvers unless they can be sealed quickly. The door undercut must be small enough to allow sealing with a door-sweep weather strip or, in emergencies, with duct tape.
- **HVAC System:** The safe room must be isolated or capable of being isolated quickly from the HVAC system of the building. When the selected room is served by supply and return ducts, preparations or modifications must include a means of temporarily closing the ducts to the safe room, as depicted in Figure 4-11. In the simplest form, this involves placing duct tape or contact paper over the supply, return, and exhaust grilles and turning off fans and air-handling units. More elaborate preparations may involve hinged covers. Where a window-type or through-the-wall air conditioner is in the selected room, plastic sheeting and tape, or a hinged cover, must be available to place over the inside of the window and/or air conditioner, which must be turned off when sheltering in the safe room.
- **Ventilation:** For Class 1 safe rooms, 15 cfm per person is the desired ventilation rate; however, the minimum ventilation rate is 5 cfm per person, when that is adequate for pressurization. Class 3 and unventilated Class 2 safe rooms are suitable only for short duration use, not only because the low ventilation rate when occupied can cause carbon dioxide levels to rise, but also because protection diminishes as the time of exposure to the hazard increases.
- **Location:** For unventilated safe rooms (Class 3 and some Class 2), there are three considerations for location within a building. First, relative to the prevailing wind, the safe room should be on the leeward side of a building. Second, the safe room should be on the side opposite the location of toxic materials storage or processing plant in the community. Third, an interior room is preferable to a room with exterior walls, when it meets the criteria for size, tightness, and accessibility. For a low-rise building, a room on the higher floors offers no substantial advantage, and a location should not be selected

based on height above ground level when it increases the time required to reach the shelter in an emergency.

- **Water and a toilet:** Drinking water and a toilet(s) should be available to occupants of a safe room. This may involve the use of canned/bottled water and portable toilets. A toilet fixture allowance is presented in FEMA 361.
- **Communications:** For sheltering situations initiated by local authorities, the safe room must contain a radio with which to receive emergency instructions for the termination of sheltering. A telephone or cell phone can be used to receive emergency instructions and to communicate with emergency management agencies. Electrical power and lighting are also required.

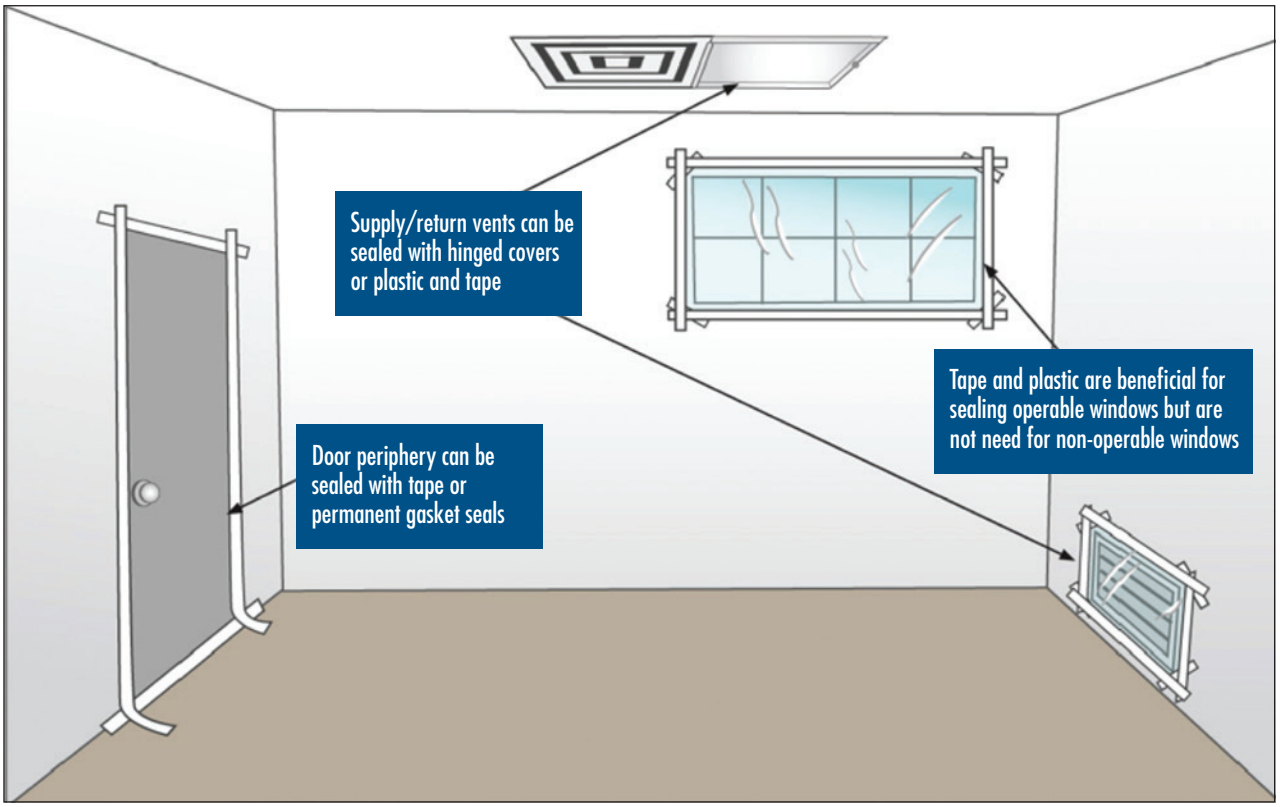


Figure 4-11: Areas to be sealed temporarily in a safe room during an emergency

4.4.5.4 Recirculation Filter Units

For the unventilated Class 2 safe room, the improvement in protection over the Class 3 safe room is determined by the flow rate and the efficiency of the particulate filter for aerosols and the efficiency of the adsorber for gases and vapors. These filter units, commonly referred to as indoor air purifiers, indoor air cleaners, or indoor air quality units, recirculate air within the safe room, and may reflect one of four configurations:

- Free-standing table top unit
- Free-standing floor unit (Figure 4-12)
- Ceiling-mounted unit
- Duct-mounted unit (with ducts completely inside the safe room)

Figure 4-12:
A portable, floor recirculation filter unit with an adsorber and HEPA filter

The protection provided by an unventilated safe room with a recirculation filter unit is determined by the clean air delivery rate of the filter unit and the tightness of the enclosure. The clean air delivery rate is a product of the filter removal efficiency (expressed as a decimal fraction) and the actual flow rate of the filter unit. When a high-efficiency filter unit is used, the clean air delivery rate approaches the actual flow rate of the unit. When the filter has a single-pass efficiency of 50 percent, for example, the clean air delivery rate is half the actual flow rate. For a given unit, the clean air delivery rate is likely to be higher for aerosols than for gases and vapors because efficiencies of adsorbers are typically lower than the efficiencies of particulate filters in these units.

Many models of these indoor air purifiers are available commercially, but not all of them have performance suitable for use in protecting against toxic aerosols, gases, and vapors. The following criteria can be used to select recirculating filter units for use in safe rooms:

- The filter unit must have both an adsorber containing activated carbon and a particulate filter.
- The adsorber must have at least 1 pound (0.5 kilogram) of activated carbon for each 20 cfm of flow rate; for example, a 200-cfm unit requires at least 10 lbs (4.5 kilograms) of carbon adsorbent.
- The particulate filter must have an efficiency of at least 99 percent against 1mμ MMD particles.
- The unit(s) must provide a total clean air delivery rate of at least 1 cfm per square foot of floor area.
- The adsorber must have the capability for chemisorption (i.e., for removal of gases that are not removed by physical adsorption).

For the unventilated safe room, floor/table model filter units and ceiling-mounted models should be placed in the center of the room to maximize air mixing. Airflow into and out of the filter units should not be obstructed. Duct-mounted models must conform to the requirements stated above for air-handling units. Ducts cannot be outside the envelope formed by the walls, ceiling, and floor of the safe room. The adsorbers of these commercial units are generally lacking in capability for filtering a broad range of high vapor pressure agents, such as some of the common industrial chemicals like ammonia.

The filter unit can be used routinely for indoor air quality; if so, a spare set of filters should be kept on hand for use in a toxic materials emergency, along with instructions for changing the filters so that the change can be made rapidly.

4.4.5.5 Single-Switch Control

Single-switch control provides the capability to activate the sheltering in place rapidly in buildings that have multiple fans to be deactivated and multiple dampers to be closed. Control switches may also include panels with status lights for air-handling units, exhaust fans, unit ventilators, dampers, and doors. Typically, the main component of each control panel is a pushbutton switch controlling fan interlock relays for de-energizing all fans that induce air exchange between the protected spaces and the outdoors. The shutdown switch, the red button, also closes motorized or pneumatic dampers.

The control panel may also be designed with features to accommodate the purge/aeration phase of unventilated sheltering. One switch is used to initiate sheltering, interrupting normal mechanical ventilation by closing outside air dampers and turning off air-handling units that induce air exchange. A second switch initiates the purge phase by turning on all fans and opening dampers once the outdoor hazard had dissipated. Figure 4-13 shows a control panel for unventilated sheltering in a large office building. The panel contains a single (red) switch to control all fans and dampers and an array of status lights for the fans and dampers.

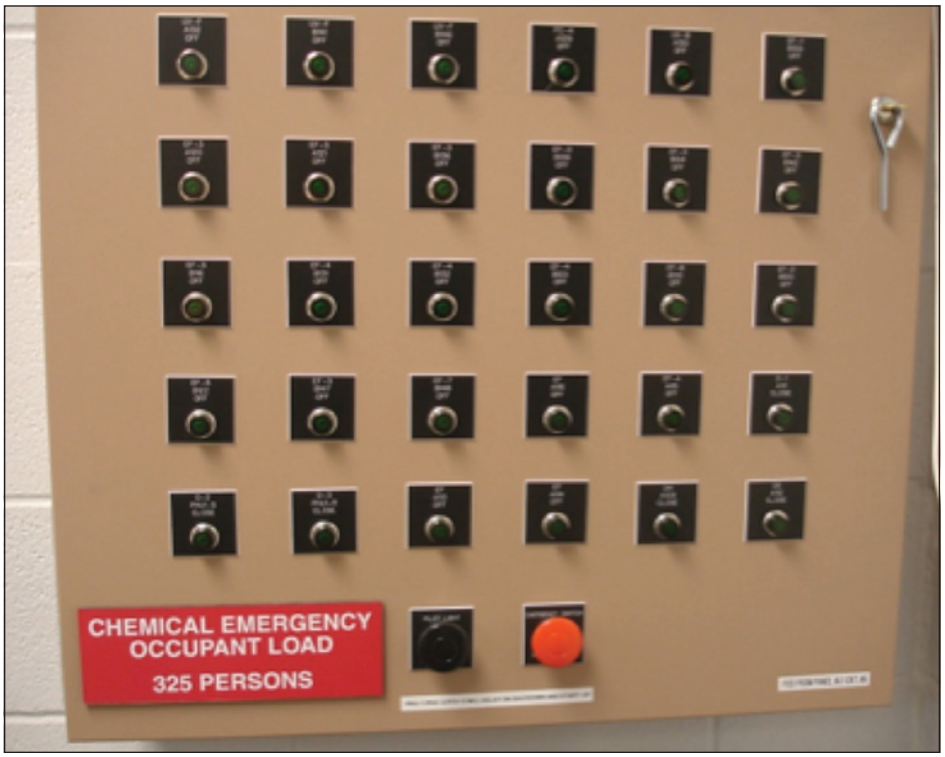


Figure 4-13:
Control panel for a building with automatic dampers and interrupts

4.4.6 Individual Protection Strategy: Respirators for Building Occupants

For protection against a terrorist CBR attack, escape respirators provide a capability that shelter in place protection does not—a high level of protection for an indoor release of an agent or for an outdoor release of an agent that infiltrates the building. Respirators also provide the capability to maximize protection when the source of the hazard—indoors or outdoors—is unknown. These protective devices are designated as escape respirators because they are designed to provide a high level of protection during the time needed to evacuate a building or contaminated area during or after an attack.

4.4.6.1 Types of Respirators

Several models of escape respirators are available that meet the criteria defined in the Federal standard for chemical, biological, radiological, and nuclear (CBRN) air-purifying escape respirators (APERs).[9] A second standard for escape hoods does not employ air filters: the standard for CBRN self-contained escape respirator. The self-contained respirator employs a compressed oxygen cylinder, rather than an air filter, to provide eye and respiratory protection for limited periods.

Both types, air-purifying and the self-contained respirators, are hooded devices. Four of the six respirators shown in Figure 4-14 are APERs that have been tested and approved by NIOSH. Many other escape respirators are on the market; however, escape respirators for CBRN protection should be purchased from the list of NIOSH-certified respirators. NIOSH-certified respirators meet the following criteria:

- Are hooded devices with sealing at the neck to provide the most reliable seal for facial hair, glasses, and/or different face sizes
- Store compactly and are easily carried or stored for ready access
- Allow rapid donning (less than 30 seconds)
- Require minimum training
- Fit most of the adult population with a single size
- Protect against a large number of toxic chemicals and aerosols
- Have a shelf life of 5 years
- Have low breathing resistance
- Provide a wide field of vision
- Require no routine maintenance

Both air-purifying and the self-contained types protect against chemical warfare agents, aerosols (including biological and radiological agents), and TICs. The APERs employ filters with impregnated carbon designed to remove a broad range of toxic chemicals. The air-purifying respirators cannot protect against all TICs. An important consideration in planning for use of APERs is that their filters are not effective against certain chemicals of high vapor pressure. For example, they may provide no protection against carbon monoxide, which is produced in fires, unless specifically certified with carbon monoxide capability.

The air-purifying escape respirators employ filters with impregnated carbon designed to remove a broad range of toxic chemicals.

9 Further information on the standard for escape respirators and hoods is available at www.cdc.gov/niosh/npptl/standardsdev/cbrn/escape/.

Figure 4-14:
Six escape hood respirators designed and tested for use in CBR emergencies

The self-contained breathing apparatus does not have limitations relative to TIC protection; however, it does have wearing time limits that vary with the work rate of the wearer. For example, it can protect a person sitting down for an hour, but a person walking rapidly up stairs for only a matter of minutes.

The escape respirators employ either an oral-nasal cup or a mouthpiece. If a mouthpiece is employed, a method of preventing nasal breathing, i.e., a nose clip, is provided. The NIOSH-certified escape respirators do not include voicemitters for improved voice transmission while wearing the mask. The NIOSH-certified respirators are marked to show the duration rating (15, 30, 45, or 60 minutes) and state that they are intended for escape use only under the CDC's *Statement of Standard for CBRN Air-Purifying Escape Respirators*, dated September 30, 2003.

Other escape respirators (see Figure 4-14) that have been certified by government testing to other standards and can also be considered for use include the following:

- The M52 Joint Service Chemical Environment Survivability Mask, a military version of escape respirator with a 10-year shelf life.
- The Victim Rescue Unit – Plus (VRU+), manufactured by Essex PB&R Corporation,[10] a self-contained escape respirator designed for escape from a burning aircraft but also tested for CBR protection.

10 Additional information on the VRU+ escape respirator is available at www.smokehoods.com/products/vru_main.aspx.

All escape respirators described above are designed to minimize the logistics burden of training, sizing, maintenance, and inventory control associated with providing respirators for building occupants.

With regard to training, Occupational Safety and Health Administration regulations require that users of NIOSH-certified respirators have annual training on how to wear them. At a minimum, this should consist of providing an instruction manual addressing donning procedures, use and care of the respirator, useful life, cautions, and limitations. Some manufacturers of escape respirators provide training aid systems, including a training respirator that simulates the performance of the approved respirator.

No routine maintenance is required over the useful life of these respirators, which is defined as the length of time a unit can remain deployed in the "ready to use" stowed condition. A packaged respirator should be replaced if the seal of the package is broken. Escape respirators are designed to fit adults with a single, universal size. They are not sized for children.

Inventory control records should be maintained to document expiration dates and lead times for replacing respirators as they reach the end of their useful life.

4.4.6.2 Usage of Escape Respirators

There are two approaches to issuing escape respirators. One is to place them in caches in offices and/or common areas so that they are readily accessible in an emergency. The second is to issue them to each individual who works or resides in the building, allowing them to keep the respirator at their workstation or to carry it.

There are two approaches to issuing escape respirators.

When escape respirators are issued to a building population, procedures, plans, and responsibilities must be defined very clearly to ensure occupants know when to put on the respirators, how to disseminate alerts, and when to take the respirators off.

The respirator plan should list situations in which the mask would not provide protection, based on the types of chemicals stored or used regularly in the building or in proximity to it. Carbon monoxide and formaldehyde are examples of gases that may not be filtered by an APER. If protection for a specific chemical is uncertain, the manufacturer of the respirator should be consulted. The plan should also list the characteristic warning properties of chemicals used/stored in or near the building for which the mask is not effective. Material safety data sheets (MSDSs) for hazmat stored in the building should be on file.

The respirator plan should also address the psychological and physiological stresses that wearing a respirator can cause. Wearing a respirator may cause panic that could lead to respiratory problems for some people.

4.5 Detection of Chemical, Biological, and Radiological Agents

The ability to detect an airborne hazard rapidly is critical to the protective strategies of unventilated sheltering and using escape respirators. It is also critical for determining whether or not to evacuate. Some CBR hazards can be identified using of automatic detectors or sensory detection.

To protect buildings and their occupants from CBR attack, automatic detectors must provide immediate or real-time response, i.e., the detector must respond accurately within approximately 15 seconds. Automatic detectors with real-time capability are available for chemical agents and radioactive materials. However, no devices exist that can accurately detect the presence of biological agents in the air in real time.

To protect buildings and their occupants from CBR attack, automatic detectors must provide immediate or real-time response.

Manual, delayed-detection devices, such as the military M256 detector kit and commercial detector tubes for TICs, can be used for chemical detection, and are intended primarily for determining when to reduce the level of protection, i.e., to remove the respirator or to test effectiveness of decontamination efforts. These devices are not useful for initiating protective actions.

Sensory detection—by smell, sight, taste, or irritation of the eyes, throat, or skin—is practical only for chemical agents. It is not applicable to radiological or biological agents, as shown in Table 4-3.

Table 4-3: Sensory Detection of Chemical, Biological, and Radiological Agents

	Is sensory detection practical?	Is automatic, rapid detection practical?
Chemical warfare agents	yes for most	yes
Toxic industrial chemicals	yes for most	yes for some
Radiological agents	no	yes
Biological agents	no	no

4.5.1 Automatic Detection

Automatic detectors are most beneficial when they can accurately detect hazards that are not perceptible by the human senses. An example of this capability is the detector for carbon monoxide, a toxic gas that is odorless and colorless. About 500 unintentional, non-fire carbon monoxide deaths occur annually in the United States. Carbon monoxide detectors provide accurate, real-time detection for this specific gas and are effective for alerting people to a hazard that would otherwise go undetected.

Detectors that have similar reliability and accuracy exist for a limited spectrum of toxic chemical agents, and apply technologies such as ion mobility spectrometry, surface acoustic wave, or gas chromatography/mass spectrometry. The sources of such detectors and their characteristics, capabilities, and limitations are described in the DHS G*uide for the Selection of Chemical Detection Equipment for Emergency First Responders* (2007b).

Such devices are generally high in cost and are not completely free of false alarms. The larger the number of chemicals a device is designed to detect, the greater is the potential for spurious responses. The effective response time of automatic detectors installed on buildings or facilities varies with the quantity and density of the detectors or sampling points in or around the building.

Detectors for biological agents have been developed to provide rapid response, with relatively low accuracy, and delayed response with greater accuracy. Devices that yield greater accuracy, generally, require trained operators and have processing times measured in minutes. A second guide, DHS *Guide for the Selection of Biological Agent Detection Equipment for Emergency First Responders* (2007a), provides a technical description of devices for detecting biological agents.

A wide variety of detectors that provide immediate, accurate responses to radiation have been developed for the nuclear industry and are commercially available.

4.5.2 Sensory Detection of Chemicals

Most TICs have warning properties. Such warning properties make chemicals perceptible; that is, the vapors or gases can be sensed by smell, sight, taste, or irritation of the eyes, throat, or skin before incapacitation or serious effects occur. The distinction between perceptible and imperceptible agents is not an exact one. The concentrations at which a person can detect an odor vary from person to person, and these thresholds also vary relative to the concentration that can produce immediate, injurious effects.

The first practical application of warning properties occurred in World War I when soldiers were taught to identify by smell such agents as mustard, phosgene, and chlorine. This detection method proved effective for determining when to put on and take off the gas mask and was also applied in World War II.

This military application illustrates that for warning properties to be effective, people must be trained to recognize them. Chemicals that elicit immediate pain, for example strongly irritating the eyes, do not require training.

Of the three examples of TICs shown in Table 4-4, two chemicals, ammonia and chlorine, are irritating to the eyes and mucous membranes at concentrations below lethal concentrations. With all three, the odor thresholds are substantially below the concentrations that produce casualties.

Table 4-4: Examples of TICs Detectable by the Senses

Chlorine	
0.06 ppm	Detectable odor threshold.
3 ppm	Irritation of the eyes and mucous membranes.
15 ppm	Immediate irritation of the throat.
50 ppm	Dangerous health hazard even for short periods. Prolonged exposure is fatal.
1,000 ppm	Potentially fatal after a short exposure.
Hydrogen Cyanide	
2 to 5 ppm	Detectable odor threshold.
18 to 36 ppm	Slight symptoms after several hours.
45 to 54 ppm	Tolerated for 0.5-1 hour without immediate or delayed effects.
110 to 135 ppm	Dangerous to life or fatal after 0.5-1 hour.
270 ppm	Immediately fatal.
Ammonia	
0.6 to 53 ppm	Detectable odor threshold.
25 to 50 ppm	Irritation of eyes and mucous membranes, which can be tolerated for several hours.
100 to 150 ppm	Immediate irritation of the throat, which may be tolerated for an hour.
400 to 700 ppm	Immediate, severe irritation of the respiratory system and eyes occurs.
>5,000 ppm	This level may cause rapid death by suffocation or fluid in the lungs.

Biological agents and radioactive aerosols have no perceptible warning properties, but visible and audible cues can indicate their release in a CBR attack.

4.5.3 Visible and Audible Cues

The release of toxic agents can produce visible and audible cues for initiating protective actions. The most obvious are those associated with explosive dissemination of agent. People can also be alerted to some airborne hazards by observing symptoms or effects on others (Table 4-5). Unlike biological and radiological agents, chemical agents produce immediate effects in most cases. Other warning signs of a hazard may involve seeing and hearing something out of the ordinary, such as the hiss of a rapid release from a pressurized cylinder.

Table 4-5: Indications and Warning Signs of Airborne Hazards

Sensory indications
• Strange or pungent odor in the building
• Irritation of the eyes or throat experienced by people in the building
• Smoke or a unusual fog in the building
• Unusual noises, such as the release of gas under pressure or an explosion in or near the building
Symptoms
• People reporting nausea, collapse, choking, or irritation of the eyes or throat
• Observing these symptoms in other people in the building
Evidence indicating malicious acts
• A spill of unknown material in or near the building
• Finding a spray device in or near the building (pressurized cylinder, batteries with pump and nozzle, container of liquid, gas, or powder)
• Finding a suspicious parcel left unattended in the building
• Receiving a letter or parcel with markings indicating hazmat
• Receiving a threat
Information of a hazardous release
• Notification from authorities that there is an outdoor hazard, such as an accident involving a storage site, tanker truck, or rail car
• Notification that there is an internal spill of cleaning material, or a release of hazmat stored indoors

4.6 Emergency Action Plans, Procedures, And Training

Every building should maintain a current emergency action plan addressing all threats, including a hazmat release, bomb threat, fire, severe weather, and other emergencies. The Occupational Safety and Health Act enacted by Congress in 1970 requires a basic emergency action plan, under its implementing regulations at 29 CFR 1910.38, to prepare and plan for emergency situations before they occur. Employers should ensure people are trained in the actions to take, and should exercise the systems and procedures to verify they work properly. The plan should cover all systems needed for life safety; HVAC systems may require more emphasis because of the greater complexity of system operating procedures relating to a hazmat release or CBR attack.

The ability to respond rapidly with appropriate protective action is of critical importance in an emergency involving an airborne hazard. Experience shows that toxic plumes can move and spread rapidly, and that building occupants cannot simply wait for emergency responders to arrive. As they do in fire emergencies, people naturally take action, such as evacuating the building, for self-protection. However, in toxic agent emergencies, evacuation is not always the best course of action.

The ability to respond rapidly with appropriate protective action is of critical importance in an emergency involving an airborne hazard.

To identify the vulnerabilities and a building's protective capability, all systems should be inspected by a certified emergency manager and an individual with knowledge on CBR threats. These inspections should be completed at least on an annual basis. Based upon information gathered in the building survey (see Section 4.4.5 below), determine whether and when it is practical to employ sheltering in place, escape respirators, evacuation, and/or purging in an emergency. Purging is most effective when the building has smoke purge fans. Respirator protection requires that CBR escape respirators, as described in Section 4.4.6, be issued to the people who work or reside in the building and are readily accessible in the case of an airborne release.

4.6.1 Emergency Action Plan for Airborne Hazards

A vulnerability assessment, as described in Section 4.3.5, provides the basis for determining the best strategies to reduce CBR vulnerability. Each strategy or combination of strategies should be documented in an emergency action plan that describes the specific procedures, training, and

responsibilities necessary to integrate the equipment and procedures into a protective system that is effective and efficient.

In addition to a vulnerability assessment, a building survey should be conducted to determine the scope and limitations of each strategy. For example, if the strategy of sheltering in place is applied, the survey should identify spaces or safe rooms that are quickly accessible and that provide space adequate for all building occupants.

The survey should determine whether hazardous chemicals present a threat specific to the building, and should answer the following questions:

- What hazardous chemicals, if any, are stored in or near the building, and where are they stored?
- What hazardous chemicals are routinely used in the building or transported near the building?
- Are MSDSs maintained for these chemicals, and are they easily accessible to building occupants and emergency responders?
- What ventilation systems (such as hoods or glove boxes) are in place to contain or isolate a release of these stored chemicals?
- Has the LEPC been consulted about hazardous chemicals that are stored, processed, or frequently transported near the building? Have the approximate distances and directions of the chemicals from the building, and their warning properties, been documented?

4.6.2 Emergency Action Decisionmaking

Effective emergency procedures must include the appointment of an emergency action coordinator (EAC), who has the responsibility for preparations, training, and decisionmaking relative to protective actions. The EAC is responsible for deciding whether to evacuate, shelter in place, use escape respirators, or turn off/on fans in the building. The EAC also contacts first responders when an event occurs. An EAC should be designated for each duty cycle or shift, and must be immediately accessible by phone, radio, pager, or direct communication at all times.

Effective emergency procedures must include the appointment of an emergency action coordinator, who has the responsibility for preparations, training, and decisionmaking relative to protective actions.

The criteria for decisionmaking—for determining whether a hazard actually exists and the best course or action for protection—should be defined beforehand and be listed in the emergency action plan. The following discussion provides an example of a decisionmaking process following a hazardous condition occurrence in a building.

Decisionmaking Example

Once an airborne hazard has been identified in the building, the most important step in deciding the best protective action is to determine whether the source of the hazard is inside or outside the building. This determination may not always be made quickly, in which case action should be taken based on the most likely location, while the actual location continues to be investigated.

Once an airborne hazard has been identified in the building, the most important step in deciding the best protective action is to determine whether the source of the hazard is inside or outside the building.

Where the source is clearly inside, such as a spill of cleaning solution or an accident causing the release of hazardous chemical stored in the building:

- Air-handling units should be shut down until the type of hazard its extent can be determined.
- All affected floor(s) should be evacuated.
- Where people may be exposed to the hazard along evacuation routes, respirators should be used based on indications of the type of hazmat (masks may not provide protection for certain types of chemicals).
- When the hazmat has a warning property (indicators such as detection alarms, visible emissions, odor, or smell), the specific area should be purged with smoke fans, if available.
- The affected area should be isolated by closing doors and fire doors.
- The fire department or hazmat unit should be called for assistance.

Where the source is inside and contained or localized, such as a package containing a toxic material:

- All air-handling units that serve the affected floor should be shut down.
- The affected area should be isolated by closing doors and fire doors.
- The fire department or hazmat unit should be called for assistance.
- The affected floor(s) should be evacuated via routes away from the affected area.
- Where people may be exposed to the hazard along evacuation routes, protective masks or respirators should be used.

Where the source is clearly outside, such as an airborne release of a chemical agent in a plaza just outside the building:

- Sheltering procedures should be initiated and local emergency responders consulted about the likely duration of the event (how long until the release is contained or the cloud passes the building).
- When the hazmat has begun to enter the building, respirators should be used.

Where the source location cannot be quickly determined, such as a chemical release several blocks away from the building that is dispersed by wind to the location of the building:

- When an odor or other warning is apparent, respirators should be used, before determining if the air is clean outside the building. If so, the building should be evacuated.
- When symptoms of a hazard are observed by occupants, but no odor or other sensory indications are apparent, the building should be evacuated.
- Other possible indicators of source should be checked:
  - In a multistory building, when signs/symptoms are not apparent on adjacent floors, an internal release on one floor is likely.
  - When visible signs are observed outside the building, such as people fleeing or otherwise reacting to an airborne hazard, an external release is likely.

4.6.3 Emergency Instructions

Emergency instructions should be prepared beforehand for each possible protective action and included in the emergency action plan. This will increase the probability that actions will be taken as rapidly as possible and that instructions will be clearly understood by everyone, including those who have not had training (e.g., visitors). The messages in the emergency instructions should be worded to be effective without causing panic. An example of a warning over the intercom: "Attention, a strange odor has been reported on parts of the third floor. If you are on the third floor, proceed down the stairs and exit the building into the north parking lot."

Evacuation messages should instruct people to avoid certain areas that are known to present a hazard. Messages for sheltering in place may include instructions on turning off fans or closing windows. In buildings with unit ventilators, sheltering messages should include instructions for turning off the ventilators. In buildings with natural ventilation, messages should include instructions for closing all windows and doors.

4.6.4 Restoration of a Building after a Chemical, Biological, or Radiological Release

When CBR agents infiltrate or are released inside a building, a portion of the contaminants will be purged by the normal exchange of air between indoors and outdoors (produced by fans, wind, and buoyancy), and a portion will be retained in the building over time by the following processes:

- Chemical agents in the gas or liquid phase will be absorbed by materials of the building and will desorb slowly over time as the airborne concentration decreases.
- Biological and radiological aerosols and other solid aerosols (e.g., tear gas) will settle onto surfaces at a rate dependent on aerodynamic particle size and air movement. These may be re-aerosolized with the movement of people, air, and equipment in the building, but a significant portion is likely to be retained indefinitely unless decontamination measures are taken.
- Acid gases, such as chlorine, will react with materials in the building and may cause deleterious effects.

Furthermore, aerosols will collect in HVAC particulate filters, even though the efficiency of such filters is low for very fine particles (e.g., 1 to 5 mμ MMDs).

Unless measures are taken to purge, decontaminate, or contain agents immediately after release, the agent can be transported and deposited onto inaccessible surfaces in the building, greatly complicating the process of decontamination. Decontamination involves removing and/or neutralizing agents. Decontamination procedures range from simple removal with soap and water to more complex procedures, equipment, and decontaminants for neutralization, disinfection, cleaning, or accelerated desorption.

Except for aeration, which is effective for non-reactive chemical agents of high vapor pressure, decontamination of a building can be a long and costly process. It is an iterative procedure involving detection in concert with removal and/or neutralization. For cases in which real time detection capability exists, as with radiological agents, this process of decontaminate-detect-decontaminate-detect is relatively simple. With biological agents and toxins, each detection step involves a delay for laboratory analysis and is, therefore, the most costly and time consuming. Although some chemical agents are detectable in real time, biological agents and toxins are not.

4.6.5 Immediate Actions

Immediate actions, as defined in emergency action plans, can be taken as soon as a CBR hazard is recognized in a building to minimize the spread and retention of agent in the building and, consequently, the extent of the decontamination that will be required.

Immediate actions to minimize retention involve controlling fans, dampers, and natural ventilation, some of which have opposite effects relative to spread and retention. Identifying whether a release is indoors or outdoors is critical, but a reliable means of making this determination is unlikely without having observed the event causing the release.

When the source is unknown (inside or outside the building), the most effective immediate action is the same as sheltering in place; that is, turn off all fans and shut all windows, dampers, and doors. This reduces exfiltration induced by fans, wind, and buoyancy. It also limits the spread through the duct system, except for the uncontrolled airflows induced by wind and buoyancy.[11]

When recirculation filter units, also known as indoor air-quality units or indoor air purifiers, are operating in the building, they should remain in operation. These filter units remove aerosols through high-efficiency filters without drawing outdoor air or distributing the contaminants to other rooms within the HVAC zone.

When the contaminant is a chemical gas or vapor and the source is known to be inside the building, all building fans should remain in operation, and the outside air fraction of air-handling units should be increased where possible.

Guidance published by the Lawrence Berkeley National Laboratory states that for an indoor release of a chemical, "It is best to leave the HVAC system operating without alteration, unless a knowledgeable building operator is available to perform HVAC manipulation. Under normal operation, the HVAC system will provide some outdoor air and will exhaust some indoor air, so it will help dilute the chemical and exhaust it from the building" (Price et al. 2003).

Where there are exhaust fans in the zone of release, they should be operated at full capacity. This provides the benefit of purging the contamination without distributing it through the duct system. The effectiveness of this purging depends on knowing the location of the release and having exhaust fans that serve the space in which the release has occurred.

---

11 Uncontrolled air flow is defined as air moving across the building envelope or between zones or components of a building, where the pathways of flow, the direction of flow, and the origin of the air are unknown, unspecified, or unintended (Cummings, et al. 1996).

5

Security System Design Guidance

In this chapter:

This chapter provides design guidance for integrating various security elements to create an effective security system that safeguards a facility's assets: people, information, and property. It identifies the elements of an effective security system and presents a general step-by-step procedure for selecting security measures, consistent with assessed risks and associated mitigation and protective measures described in Chapters 2, 3, and 4. The discussion on protective measures is found in Section 5.3.

5.1 Introduction

This chapter provides design guidance for integrating various security elements to create an effective security system that safeguards a facility's assets: people, information, and property. It identifies the elements of an effective security system and presents a general step-by-step procedure for selecting security measures, consistent with assessed risks (see Chapter 1) and associated mitigation and protective measures described in Chapters 2, 3, and 4. The discussion on protective measures is found in Section 5.3. Collectively, the selected protective measures of these chapters form the security system.

In an effort to minimize overlap with previous chapters and provide the correct context with respect to security design, this chapter takes a broader view of the security system and places the security guidance from Chapters 2, 3, and 4 within a general security policy. It also delves deeper into the operational characteristics and requirements of an effective security system. Readers are encouraged to use these chapters collectively to fully understand the design guidelines presented in the manual.

5.1.1 Security System

A security system is a combination of multiple components that must work together seamlessly to provide the appropriate level of protection for a facility. The goal of a security system is to protect the facility's assets against specific threats. An effective security system promotes facility resilience by providing layered countermeasures in a manner that allows facilities to absorb, adapt to, and/or rapidly recover from a terrorist attack.

A security system is a combination of multiple components that must work together seamlessly to provide the appropriate level of protection for a facility.

Many security systems commonly deployed today focus on a single protection strategy, such as, physical barriers, electronic security, or security guards. However, an effective security system is very complex, and the lack of one element can create substantial vulnerabilities to the protective systems and the assets they protect. These vulnerabilities may not be evident to the owner or the design team, but the aggressor is trained to identify and exploit all such vulnerabilities. Therefore, the security system design must consider a thorough approach to reduce the potential for these vulnerabilities.

This chapter focuses on a high-level security system for deployment only at facilities requiring the highest level of protection. Designers of public and commercial buildings that do not require such a high level of

protection can choose the components that are most appropriate for the functions and assets they wish to protect. The following sections describe how to design a functional security system that incorporates all the key considerations and critical components.

5.2 Components of an Effective Security System

Five principal components must be considered when developing a security system (Figure 5-1): Policies, Plans, and Procedures; Security Operations and Intelligence; Physical Barriers; Electronic Security Systems and Equipment; and Cyber Security. Failure to address all components may create a weakness in the overall system that a trained aggressor can identify and exploit. A thorough planning process is recommended to integrate all five components of an effective security system, creating layers of security to eliminate weaknesses and limit vulnerabilities in accordance with the operation requirements of a protected facility. An overview of each component is provided below.

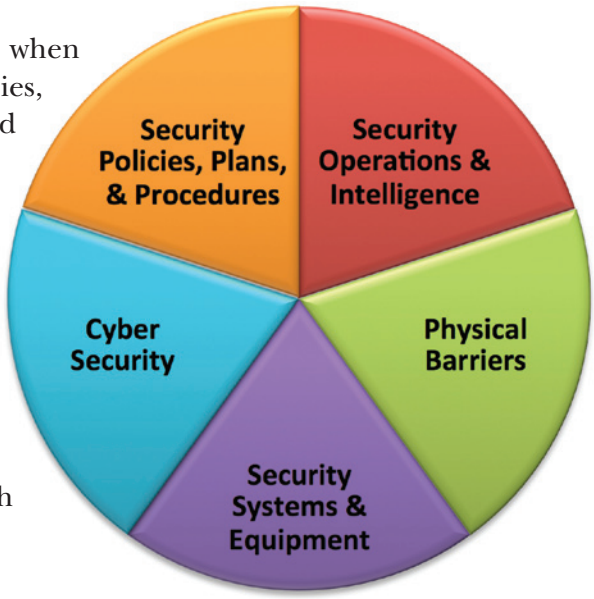


Figure 5-1: Security system essential components

5.2.1 Policies, Plans, and Procedures

Security policies, plans, and procedures are a comprehensive set of documents that establish a proactive, effective, and efficient security system (Figure 5-2). Unfortunately, security policies, plans, and procedures are often the most overlooked components of the security system that ultimately may render the whole system ineffective. Policies should be established first, to provide the strategy to develop the plans. Plans provide the structure to build the specific procedures used in the security system (Figure 5-3).

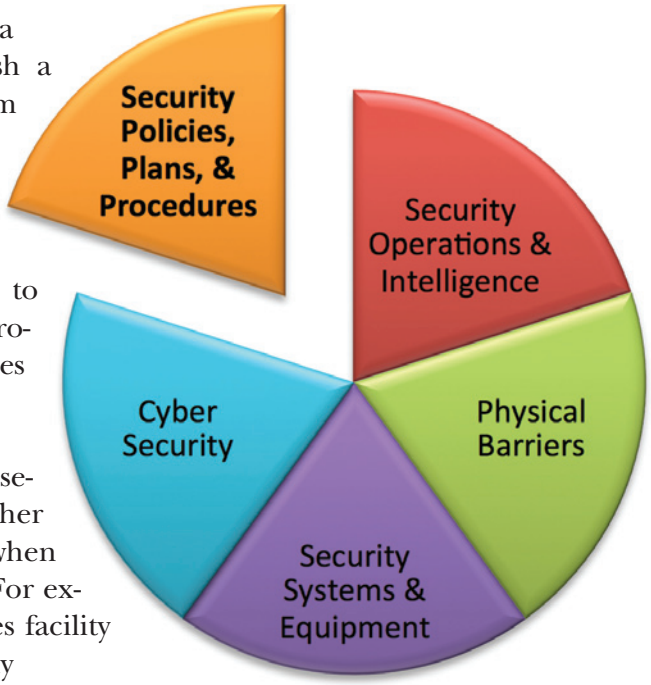


Figure 5-2: Security system essential component: Security Policies, Plans, & Procedures

Policies, plans, and procedures should include security and other facility personnel, as well as other resources (e.g., police, fire, hazmat response), when they have a role in the overall security system. For example, when a security system measure requires facility personnel to disable air handlers, or manually switch to generator power, policies, plans, and procedures must be developed to address the

responsibilities for such personnel and to ensure the security system is maintained and operates properly. The policies, plans, and procedures are an important aspect of the security system and should be reviewed annually, or as risks change.

Figure 5-3:
Security system component

Security policies establish strategic security objectives and priorities for the facility, identify the stakeholders or organizations primarily responsible for security, and set forth specific roles and responsibilities for individuals. The policies must be embraced by the entire organization from the highest level to ensure proper implementation and long-term management. Security plans include both operational and technical plans on how a system or process will operate and be managed. Plans should comprise all the other components of the security system. Plans can include general strategies for system redundancy, continuity of operations, and notification requirements.

Security policies establish strategic security objectives and priorities for the facility, identify the stakeholders or organizations primarily responsible for security, and set forth specific roles and responsibilities for individuals.

Security procedures define the established way of performing security duties. Procedures are often referred to as standard operating procedures, and commonly include established or prescribed methods to be followed routinely for the performance of designated duties (e.g., guard procedures, roving patrol procedures, evacuation operations) or in designated situations (e.g., responding to suspicious activity). Procedures may also include quick reference checklists that security personnel use to perform their duties during an event, such as checklists for bomb threats, suspicious packages, aggressor attacks, and other emergency or non-emergency situations.

Every organization develops a variety of policies, plans, and procedures that affect every person associated with the facility. These documents can include any of the following:

- **Information Security/Document Control:** High-level documents that define what information to safeguard and how to protect it from unauthorized access, use, disclosure, disruption, modification, or destruction. They should include requirements for production, classification, storage, reproduction, dissemination, transmittal, and destruction.

- **Emergency Action Plan:** Preparedness policies, plans, and procedures developed in advance to instruct staff on how to react during an incident. They include preparation instructions on what supplies to keep on hand and the type of training to conduct; how to respond to an incident, who is responsible for what, and where to go; and how to return to normal operations as quickly as possible.
- **Security Plans and Training:** Required components of a security system to ensure security personnel understand their roles and responsibilities. These plans will vary according to the importance, vulnerability, size, and other factors affecting a particular building or facility. The objective of the training program is to ensure that all personnel are able to perform routine duties and to implement emergency plans competently and efficiently.

When developing the security system plan, understanding the gaps of each security component can help in establishing procedures for security personnel to complete the security system.

Continuing training is the most effective means of obtaining and maintaining maximum proficiency of security personnel.

Continuing training is the most effective means of obtaining and maintaining maximum proficiency of security personnel. Regardless of the selection process, new personnel seldom have all of the qualifications and experience necessary to do the job. Additionally, new or revised job requirements mean that personnel must be retrained.

- **General Procedure Guidance:** Instructions that are identical for all security personnel, i.e., they apply to any guard post or patrol duty. They establish operating and performance standards, such as personal conduct and general duties.
- **Post Procedure Guidance:** The most important set of written instructions for the security personnel. Post procedures fulfill the following objectives:
  - Express the overall policies of the protected facility and asset
  - Summarize required duties in procedural form
  - Avoid the problems of word-of-mouth instructions
  - Provide the basis for site-specific training

Well-established, clear, and understandable post procedures are important for serious incidents that may call into question the integrity, competence, or capacity of the security personnel. Not every potential scenario can be described in post procedures. Innovation, flexibility, and improvisation

are important qualities that should be encouraged; however, the use of poor judgment in responding to an incident may be an indication of poor management and/or a lack of clear instructions. Most of the actions mentioned in this manual should be communicated in the security personnel post procedures. Post procedures should be available at each guard post. They are the vital link between the security system and the ability of the personnel to perform effectively in supporting that system.

Outside Resources Guidance: When dependent on outside resources to fulfill response needs, a memorandum of understanding should be initiated between the facility and outside agencies to clarify goals, responsibilities, and coordination needs. Outside response agencies should participate in drills, so they are familiar with the facility and its potential threats. This guidance is typically accomplished through mutual aid/assistance agreements.

- Additional Organizational Policies, Plans, or Procedures:
  - Security Procurement
  - Reporting or Auditing
  - Workplace Violence
  - Prohibited Items and Substances
  - Visitor Procedures
  - Key Control
  - Staff Training
  - Credentialing/Badging

5.2.2 Security Operations and Intelligence

Security operations and intelligence protective measures are essential to the success of any security system (Figure 5-4). The effectiveness of detection systems, delaying systems, response, and defense against an aggressor depends on the capabilities of security personnel. The following considerations will help to ensure the appropriate protective measures are adopted:

- **Determining the Need:** The basis for determining personnel needs is the security system design and the procedural needs. In some instances, outside response forces (police, hazmat, and fire department) may be able to respond to an incident quickly; however, many facilities may consider establishing their own contingency response teams.
- **Security Guard Duties:** Security personnel perform the following duties:

- Entrance Control. Operate and enforce a system of access control (vehicle or pedestrian), including inspection of credentials and packages.
- Roving Patrol. Patrol routes of designated areas such as, perimeters, utility areas, and public areas.
- Traffic Control. Direct traffic (vehicle or pedestrian) around vulnerable areas or verifying bills of lading and credentials; control parking.
- Security, Fire, and Utility Systems Monitoring and Response. Monitor, operate, and respond to systems alarms or protective devices.
- Response to Emergencies. In case of any emergency (such as bomb threat or bombing incident), provide response, summon assistance, administer first aid, mitigate damage by extinguishing small fires, and assist public safety personnel.

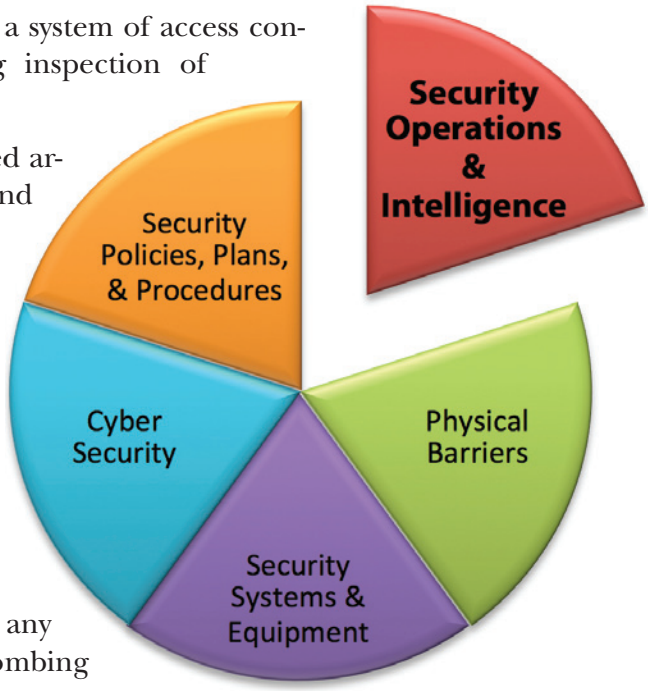


Figure 5-4: Security system essential component: Security Operations & Intelligence

- Countersurveillance. Perform countersurveillance activities to deter or thwart an aggressor's preoperational activities.

- **Intelligence and Information Sharing:** Intelligence and information sharing is relatively new to private industry. HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection, Homeland Security Presidential Directive*, establishes distinctive requirements for intelligence and information sharing (DHS 2003):

  "…the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

  - to identify, prioritize, and coordinate the protection of CIKR; and
  - to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."

For more on Information Sharing and Analysis Centers (ISACs), refer to the DHS Office of Intelligence and Analysis Web site.[12]

The security operations and intelligence component comprises the people who operate, maintain, and manage the security system. Typically, these operations are limited to security guards, but for larger facilities or those that have high threat levels the operations may include investigative and intelligence personnel. The security operations and intelligence component is responsible for developing the overall security system and performing the risk assessment.

Security personnel may include manned post, response team, training, administrative, supervisory, and management personnel. Security personnel implement, monitor, and maintain the day-to-day operations of the security system. Management personnel assist and/or oversee security-related policies, plans, and procedures.

Intelligence operational functions can range from passive activities, such as observing and reporting suspicious activity, to active intelligence operations, where aggressor activity is pursued and actively investigated. Ultimately, intelligence operations are used to better understand aggressor threats to improve protective measures. The crucial aspect of intelligence operations is sharing information on threats and trends. This can be an informal collaboration of similar organizations or a formal network such as InfraGuard.[13]

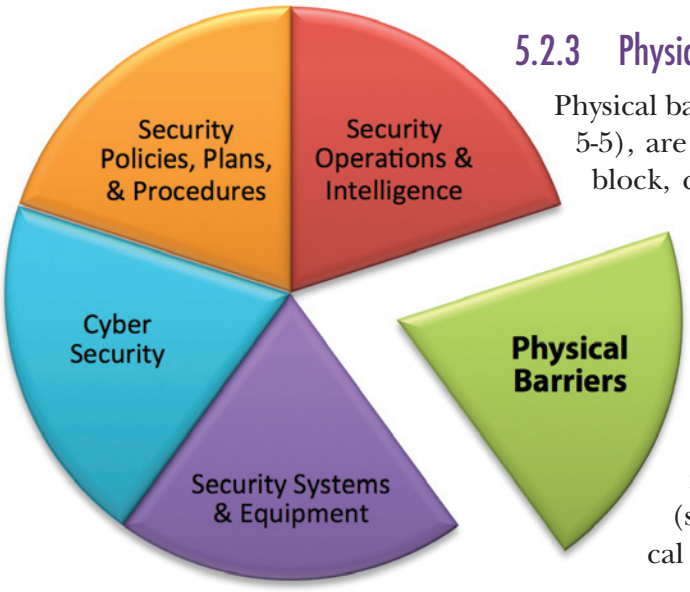


Figure 5-5: Security system essential component: Physical Barriers

5.2.3 Physical Barriers

Physical barriers, a core component of security (Figure 5-5), are manmade or natural features that control, block, contain, restrict, or direct people and vehicles with a purpose to reduce the risks from a potential terrorist attack. Physical barriers include site features such as fencing, gates, and active and passive vehicle barriers. Building physical barriers include walls, doors, windows, and other structural elements. Barriers can also provide ballistic, forced entry and blast protection to a facility (see Chapter 2 for more information on physical barriers).

12 www.dhs.gov/xabout/structure/gc_1220886590914.shtm
13 www.infraguard.net

No barrier should stand alone in a protective posture. For a barrier to be successful, it not only needs to fit the threat scenario, it also requires elements for detection and response. In most common applications, intrusion detection and video assessment systems are used to fulfill the detection elements. Guards are also used to fulfill the detection, delay, assessment, and response functions of a security system. Figure 5-6 depicts an early detection and warning system that alerts guards of potential vehicle threats, triggering precautionary measures (activation of barriers or vehicle search) to ensure the vehicle and driver are authorized to enter.

Physical barriers have been overlooked in the planning and design process in the past, and were instead, retrofitted into a facility, which frequently limited their effectiveness. Developing performance parameters and understandable methods for deployment, including placement, personnel interaction, and overall maintenance, is essential in planning physical barriers.

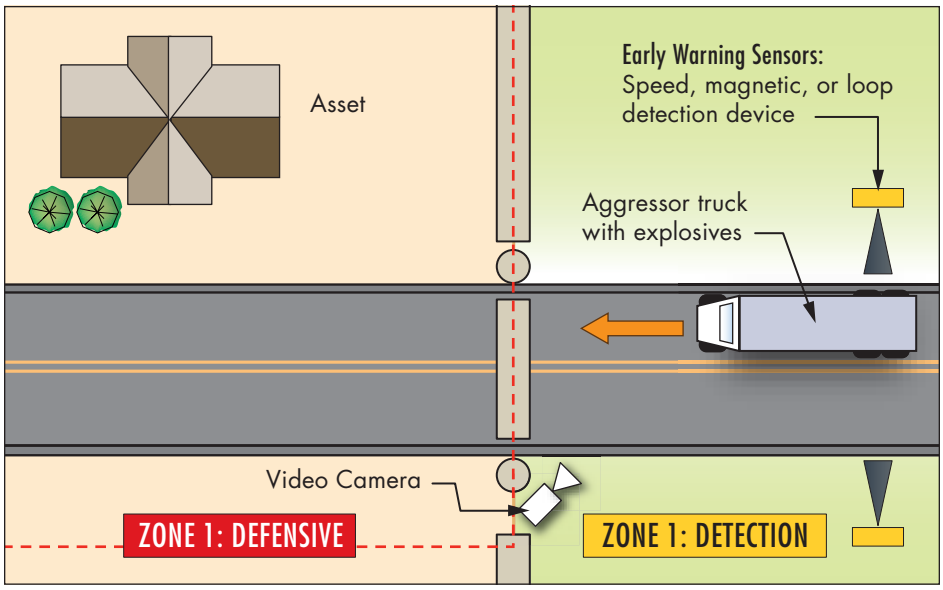


Figure 5-6:
Early warning devices

5.2.4 Security Systems and Equipment

Security systems and equipment include electronic devices, computer systems, software, wiring, and support infrastructure and equipment, such as intrusion detection, electronic entry control, video assessment and surveillance, intercommunications, and security management and monitoring functions (Figure 5-7).

Security equipment also includes screening and contraband detection devices, such as, security x-ray (e.g., explosive, weapons, backscatter), trace type detection (e.g., explosive, chemical, radiological), and magnetometers (metal detection).

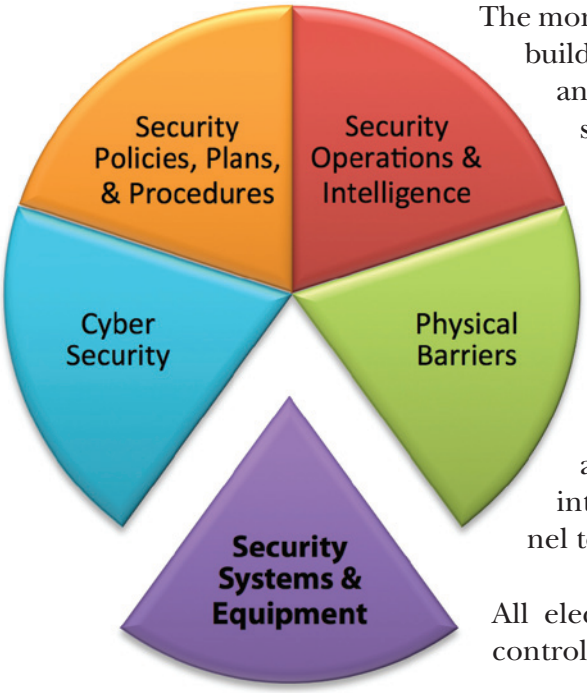


Figure 5-7: Security system essential component: Security Systems & Equipment

The monitoring element may include monitoring non-security building functions, such as power, water, communications, and heating and cooling. This monitoring element should include monitoring of systems and assets against specified threats, such as CBR and explosive sniffers

An intrusion detection system, which provides early detection of an aggressor, can be external, internal, or both. Once an alarm is activated, a signal is sent to the monitoring station. The guard assesses the alarm and takes appropriate action. The electronic entry control system can assist in delaying an aggressor and allow time for guards to respond. The intercommunication system allows the security personnel to communicate with each other or other site users.

All electronic security subsystems should be coordinated, controlled, and administered by the security management system. The security management system coordinates the use of an identification credential with the intrusion detection, electronic entry control, and VASS to grant or deny access and record the event. The security management system records all system and subsystem activity to enable re-creation of an event. The security management system can be responsible for the display of alarm and system information in the security operations center (SOC). A security management system is typically designed to accept and respond to information or inputs received from other building systems (e.g., the fire alarm system, the building automation system, elevator controls).

The SOC is the location where trained security personnel monitor the electronic security system. Alarm reporting devices and video monitors are located in the SOC. The asset's importance determines whether multiple or redundant security centers are required.

The planning and design of an electronic security system must be closely coordinated with the physical barriers, as electronic security devices must be deployed in and around the defensive layers. The intent is to have an aggressor activate an alarm point prior to penetrating or bypassing the barriers. The electronic security devices must accurately alert the guards when an aggressor attempts to penetrate the facility. The physical barrier needs to be strong enough to delay the aggressor and provide the security personnel sufficient time to assess the situation and respond. Electronic security devices (video and secondary alarm points) greatly increase the speed and accuracy of the assessment.

The planning and design of an electronic security system must be closely coordinated with the physical barriers, as electronic security devices must be deployed in and around the defensive layers.

The electronic security system is a major component of the detection zone of a facility. Detection zone types vary based on the type of a facility, equipment selected, and terrain constraints. Exceeding a zone length of 100 feet (30 meters) is not practical; zones larger than this make it difficult for guards to use VASS to pinpoint the location of an intrusion or cause of alarm. When establishing zones using multiple devices, the designer should establish coincident zones where the length and location of each individual device will be identical within a given zone. If an alarm occurs in a specific zone, the user can readily determine its approximate location by referring to a map of the perimeter. This minimizes response time by reducing the number of cameras required for assessment and simplifying the interface between alarm annunciation and video assessment systems switching.

Entry control points (vehicular and pedestrian) should be designed as independent or separate zones as they function differently during operation hours. This enables deactivation of the system in these zones, i.e., placing them in the access mode during customary working hours (assuming the entry points are manned), without having to deactivate adjacent areas.

Physical barriers and electronic security measures are used in conjunction as shown on the aggressor sequence diagram (Figure 5-14). When an aggressor attempts to breach a facility barrier, by climbing the fence, for example, an intrusion detection device mounted on the fence detects a disturbance and sends an alarm signal to the SOC. A security guard cannot be sure what caused the alarm, an aggressor or perhaps an animal rubbing against the fence. However, by using the video system or a different intrusion detection device that responds to different stimuli (such as heat, noise, motion, or pressure), guards can accurately determine the cause and respond accordingly. The next layer of physical barriers and electronic security devices would then provide sufficient delay to prevent the aggressor from gaining access to the building.

Electronic security systems can also be used in counterterrorism measures. Devices can be placed to look beyond the perimeter of the property to identify or detect abnormal or suspicious activity. These can include video analytics or intelligent video or detection/screening devices to detect an aggressor or potential attack in advance. These devices alert the security personnel to potential aggressors so that they can take appropriate action.

Figure 5-8 shows how the defense and detection zones are established using a combination of physical barriers and electronic security measures to provide an effective security system for the facility.

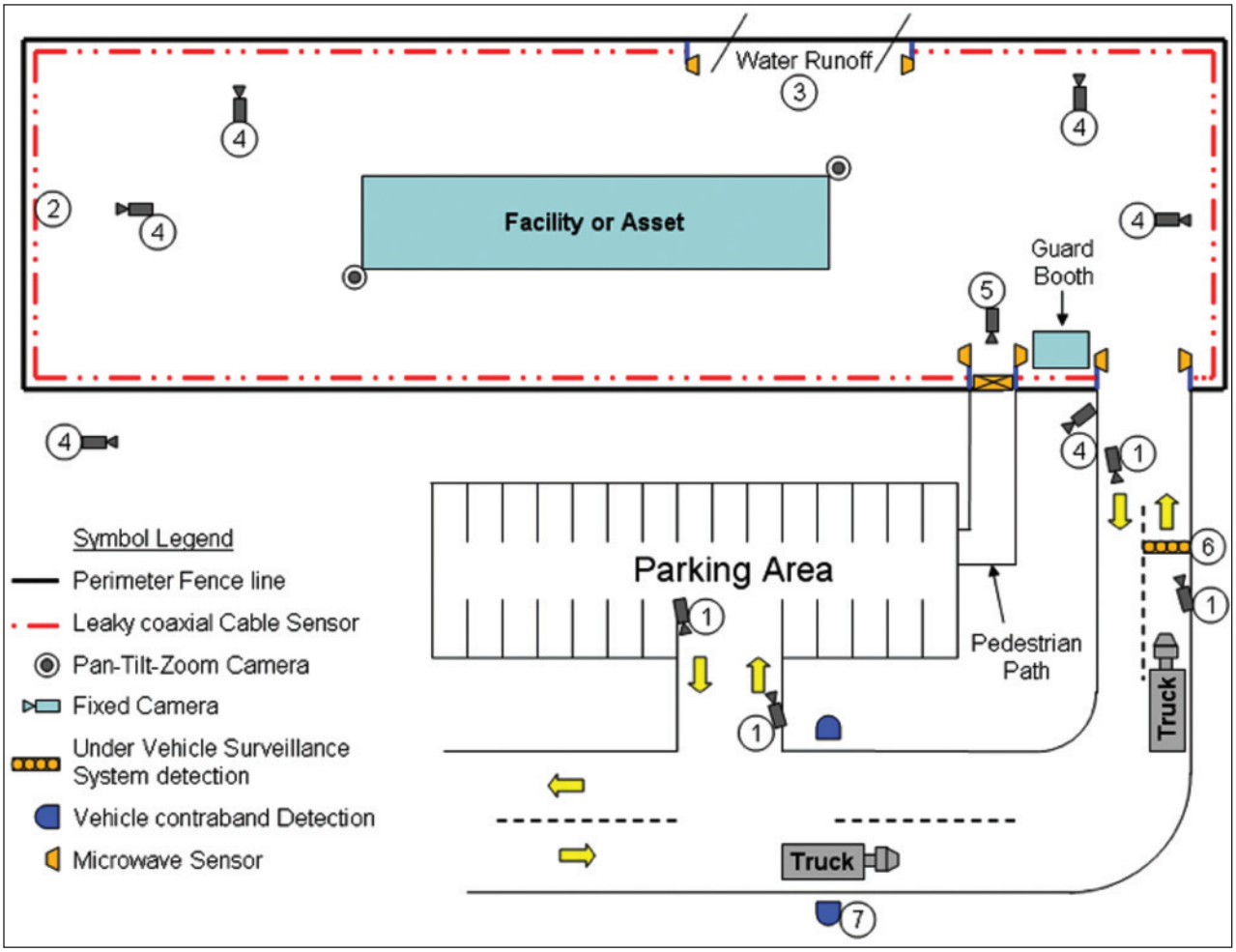


Figure 5-8: Exterior intrusion detection

KEY NOTES TO EXTERIOR INTRUSION DETECTION DIAGRAM:

1. Camera equipped with video analytics for high-speed vehicle detection.
2. Leaky coaxial cable[14] detection sensor to detect and pinpoint intrusion around the perimeter.
3. Microwave sensors where leaky coaxial cable is not appropriate.
4. Camera equipped with video analytics to capture aggressor preoperational activities (interior or exterior of perimeter).
5. Camera to provide forensic-level video of all pedestrians entering perimeter.
6. Under vehicle surveillance system to detect anomalies (e.g., abnormal mechanics on underside because an explosive device is installed) in passing vehicles.
7. Vehicle contraband detection sensor.

14 Leaky coaxial cable is a detection device that responds to dielectric or conductive materials.

5.2.5 Cyber Security

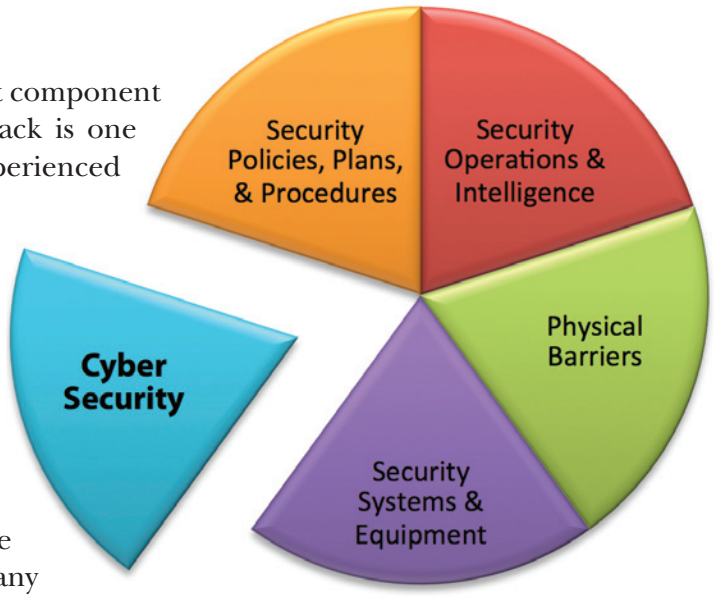


Figure 5-9: Security system essential component: Cyber Security

Cyber security has emerged as an important component of security systems (Figure 5-9). Cyber attack is one of the most active threats today and is experienced by many organizations every day. Banking institutions and much of the country's private and public critical infrastructure are primary targets. A recent report, *In the Crossfire: Critical Infrastructure in the Age of Cyber War,* found that the oil and gas sectors experience more distributed denial-of-service and extortion attacks than any other infrastructure sector (Baker et al. 2009). Although a cyber attack affecting the built environment seems improbable, many of today's facility systems (power, heating and cooling, water, telecom), even electronic security systems, are accessible from cyber space, making those systems vulnerable. Anyone from around the world with a computer and Internet connection can hack into a given system to disrupt or destroy it.

The most probable attack on an asset could involve cyber security tactics. Potential scenarios include hacking into and disrupting electrical grids, financial systems, and security systems. Cyber security in this chapter will be limited to the protection of individual assets within the built environment.

Cyber threats to the built environment are often associated with Supervisory Control and Data Acquisition (SCADA) systems, also known as Utility Monitoring and Control Systems. SCADA provides monitoring and control of utilities. For many facilities, SCADA systems perform monitoring and control of utilities over the Internet, and therein lies their most serious vulnerability. Utilities operated over the Internet are vulnerable to attacks by anyone with access to a computer and Internet connection.

Information that can be gained by accessing a SCADA system includes graphic maps and utility system details that could enable an aggressor to identify vulnerabilities and determine attack tactics. Other scenarios include an aggressor partially or completely taking control of the SCADA system to eliminate or diminish protective processes to improve the impact of a primary attack against a facility or asset.

The best measures for mitigating SCADA system vulnerabilities are the elimination of Internet access to the SCADA system and the use of the SCADA system only for monitoring functions with manual control. Many electronic security systems today are connected to the Internet via hardline or wireless connections to local area networks, and with vulnerabilities similar to SCADA systems, they have become targets for cyber attacks. Similar approaches should be taken to protect these systems' information or control from falling in the wrong hands.

Another cyber-related vulnerability relating to the built environment is associated with asset information that can be found on Web portals. Many organizations provide details of their facility and other assets on their Web sites. This information can be used against the asset, and should be removed from Web pages accessible from the Internet.

The best method of protecting against cyber threats is to limit access to the asset altogether.

The best method of protecting against cyber threats is to limit access to the asset altogether; however, some assets must be connected to cyber space (accessible via the Internet) to function. In these cases, information systems must be more secure than closed systems (those systems that are not connected to cyber space).

All organizations, whether connected to the Internet or not, should use good information security practices to safeguard their systems and data from a potential aggressor. NIST is a good source for information on cyber threats and measures to protect against them. The NIST Web site[15] provides guidance and access to publications and computer security information resources on the following IT security concerns:

- General IT Security
- Audit and Accountability
- Authentication
- Awareness and Training
- Certification and Accreditation
- Communications
- Continuity Planning
- Incident Response

15 www.nist.gov/itl/computer_security.cfm

5.3 Core Functional Considerations

Design and implementation of a security system that properly integrates the five core components introduced in Section 5.2 is a complex task that requires extensive expertise. The design team must use an effective strategy that incorporates threat-specific protective measures in a layered approach so that the asset can absorb, adapt to, and/or rapidly recover from an attack. The core considerations, shown in Figure 5-10, include the following:

- Protective Measures
- Application of Security in Layers
- Security Resiliency

Figure 5-10: Core functional considerations

Including the core functional considerations alone cannot ensure an effective security system. The security designer must use a strategy of integrating and balancing the use of the core components by following the core functional considerations. The security designer should select components to mitigate specific threats that, as a collective system, will provide benefits in terms of protective measures, security in layers, and security system resilience. Designing a system that strikes a balance between the core considerations will ensure an effective security system is maintained at all times for continued protection and operation of an asset during and after an attack (see Section 5.3.1).

5.3.1 Protective Measures

An effective security system consists of two main tactics: antiterrorism measures and counterterrorism measures as described in Table 5-1 below. These tactics reflect four important security principles: deter a potential attack, detect an aggressor, provide defensive measures to protect the assets, and interdict to defeat the aggressor.

An effective security system consists of two main tactics: antiterrorism measures and counterterrorism measures.

Table 5-1: Antiterrorism and Counterterrorism Definitions

Antiterrorism Measures	Counterterrorism Measures
Antiterrorism measures are usually passive or defensive (hardening, systems redundancy, and continuity of operations) tactics that are meant to reduce the vulnerabilities, including the effects of a terrorist act on people, facilities, and other assets.	Counterterrorism measures are active (prevention, deterrence, response and anticipatory) tactics taken to respond to terrorist acts that include the gathering of information and threat analysis.
• Establish standoff • Harden facility and systems • Cluster facility and systems • Establish defensive systems • Employ systems redundancy • Ensure continuity of operations	• Conduct countersurveillance • Conduct countersurveillance interviews (overt field interviews of potential aggressors conducting surveillance of the site) • Collect intelligence • Establish detection and assessment systems • Delay the aggressor • Perform crisis management

In recent years, a concerted effort has been made to include more organizations and operations in counterterrorism efforts. This effort stemmed from HSPD-7 (DHS 2003) and subsequent planning documents and guidelines, including the NIPP (DHS 2009b). The NIPP establishes partnerships between the government and private sectors to develop extensive coordination efforts, including information sharing. Examples of partnerships that report suspicious activity to counterterrorism centers are InfraGard (sponsored by the FBI), sector-specific ISACs[16] (sponsored by the DHS), and First Observer[17] (sponsored by the private sector). These partnerships allow security practitioners at the facility level to share threat information, including specific threats to their sector. These countersurveillance programs increase the raw data available to counterterrorism centers, which enables them to tailor investigation efforts and disseminate information regarding potential threats and tactics. In turn, this information enables facility-level security practitioners to adjust from a static responsive posture to a proactive posture and employ the appropriate counterterrorism and antiterrorism measures.

16 www.isaccouncil.org

17 www.firstobserver.com

5.3.2 Application of Security Measures in Layers

The concept of applying multiple security measures in consecutive layers starting as far away from the asset as possible (typically to the site perimeter or further with permission), often referred to as concentric layers of security, is the basic risk mitigation approach to all security systems. Planning for security in layers is based on the security industry concept of the "Four Ds" (deter, detect, defend, and defeat). Deterrence is a byproduct of planning for the other three, because you cannot design deterrence. Three basic types of security measures can be used singly or combined in each consecutive layer:

1. Defensive measures
2. Detection measures
3. Delaying measures

5.3.2.1 Defensive Measures

The objective of layers of defense is to create a consecutive number of security layers each more difficult to penetrate (Figure 5-11). This provides additional time for detection, assessment, and response, and allows building occupants to move into defensive positions or designated safe haven areas. Establishing defensive layers is a key component in the development of protective measures, particularly as the asset value and risks values increase.

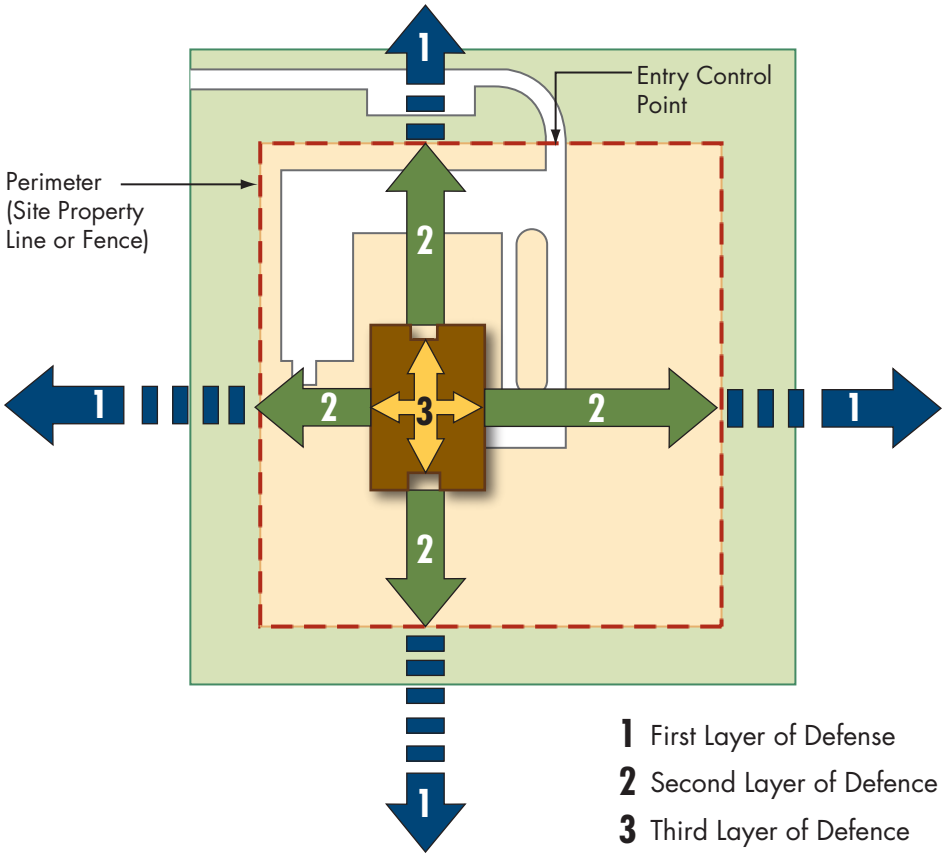
The objective of layers of defense is to create a consecutive number of security layers each more difficult to penetrate.

Layers of defense can be considered as demarcation points for different security strategies. Establishing the layers of defense early in the design process assists in determining mitigation options for assets that require protection. Refer to Chapter 2 on site security planning for details on defensive layer identification, prioritization, and characterization and its applicability to the entire building design.

More than three layers of defense may be warranted in some cases based on the results of the risk analysis. For example, when a threat of an insider sabotaging a computer center exists, additional protection layers would be warranted, because of the ability of the insider (employee of the business, institution, or agency) to bypass the typical layers of security outside the building.

Defensive layers may be placed beyond the facility's property line, such as at key infrastructure points (offsite wells or water supplies, power substations, communications) to provide suitable protection. Defensive concepts and applications are further defined in Chapters 3 and 4.

Figure 5-11:
Zones of defensive layers
SOURCE: FEMA 430



5.3.2.2 Detection Measures

Detection measures are used in different layers to identify inappropriate activities and alert security personnel in time to assess the situation. Detection measures are used in a layered approach to provide multiple detection capabilities. Detecting and assessing aggressor activity early in the pre-attack (planning) stage or early in the attack stage is important. Detection layers should begin as far away from the asset as possible (typically to the site perimeter or further with permission). Additional detection layers may be warranted at or between defensive layers depending on the risks. The more detection layers included in the protective system, the better the opportunity to detect the aggressor.

5.3.2.3 Delaying Measures

Delay is a beneficial byproduct of the defensive layers, but important enough to require special planning consideration. Delay begins once an aggressor is detected and delaying measures successfully impede the attack. Delaying measures should provide sufficient time for the security personnel to assess the situation and respond in accordance with the facility's security policy. Delay is not possible without detection, because security personnel must be aware of the intrusion to implement delaying measures.

5.3.2.4 Other Security Measures

Detection measures are used in different layers to identify inappropriate activities and alert security personnel in time to assess the situation.

Other security measures used in layers that are noteworthy and beneficial to the development of any security system are 1) access control layers and 2) assessment and surveillance layers.

Access Control Layers are commonly combined with defensive layers. They may also exist, without the defensive layers, primarily on building interiors. These access control layers provide separation between common areas and higher security areas or assets, such as data centers, utility areas, control rooms, and other high-security functions. Access controls can be in the form of the conventional lock and key, electronic access control systems (card readers), or guard forces performing an access control function at an entry portal. Normally, guards provide the access control function at various layers of defense. Access controls, similar to defensive layers, provide a delay function to the security system.

Assessment and Surveillance Layers commonly involve imaging systems, such as conventional video cameras, but can be enhanced with infrared or thermal optics. Many of today's systems use video analytics as a method to add layers of detection.

5.3.3 Security System Resilience

The NIAC introduces the concept of resilience as the ability to absorb, adapt to, and/or rapidly recover from a potentially disruptive event and developed the following requirements for resilient practices of security systems.

Absorptive capacity is the ability of the system to endure a disruption without significant deviation from normal operations. For example, fireproofing foam increases the capacity of a building system to absorb the shock of a fire.

Adaptive capacity is the ability of the system to adapt to disruption of normal operating conditions. For example, the extra transformers that the U.S. electric power companies keep on store and share increases the ability of the grid to adapt quickly to regional power losses.

Recoverability is the ability of the system to recover quickly—and at low cost—from potentially disruptive events.

Resilience is characterized by three key features:

Robustness is the ability to maintain critical operations and functions in the face of crisis. This feature can be reflected in physical building and infrastructure design (office buildings, power generation and distribution structures, bridges, dams, levees), or in system redundancy and substitution (transportation, power grid, communications networks).

Resourcefulness is the ability to skillfully prepare for, respond to, and manage a crisis or disruption as it unfolds. This feature includes identifying courses of action, business continuity planning, training, prioritizing actions to control and mitigate damage, and effectively communicating decisions.

Rapid recovery is the ability to return to and/or reconstitute normal operations as quickly and efficiently as possible after a disruption. Components include carefully drafted contingency plans, competent emergency operations, and the means to get the right people and resources to the right place.

Resilience is characterized by three key features: Robustness, Resourcefulness, and Rapid Recovery.

Depending on the threat and overall risk assessment, two characteristics of a security system should be considered with respect to resilience: redundancy and continuity. For instance, if a primary security control center is lost, the redundant (or alternate) control center can be used to maintain the monitoring and control of the security system for continued protection of the asset. In the same respect, when the overall asset is lost or severely damaged, including the security control center, a measure to have a remote security control center away from the damaged area will provide core services to ensure the continuity of command and control operations.

5.3.3.1 Security Resilience Cycle

The resilience of the security system requires an ongoing effort to ensure it is maintained and adjusted as circumstances change (see Figure 5-12). When one element of the resilience cycle is missing, vulnerabilities will occur in the overall security system. This break in the cycle will limit the effectiveness of the security system, enabling an aggressor to exploit it. Several key components in the resilience cycle are described below.

Figure 5-12:
Security system resilience cycle

Detect measures may expose an aggressor's movement or his weapons and tools via intrusion detection sensors and screening equipment. Detection measures may also include access control elements that assess the validity of identification credentials. These control elements may provide a programmed response (admission or denial), or they may relay information to security personnel for assessment. CBR and explosive detection systems must be used to detect, measure, and validate the potential for attack. The goal is to detect the aggressor activity in the pre-attack stage or early in the attack stage. Layers of detection are recommended to add redundancy to the system. Detection devices should be placed as far away from the asset as possible (typically to the site perimeter or further with permission), including outside the first layer of defense where practical. In large protection system schemes (metropolitan areas, seaports, airports, and other major infrastructure), detection systems are deployed several miles out to provide the earliest warning possible. Many of these detection systems provide valuable data about potential threats, such as when airplanes or naval ships are on course or off course.

Assess the validity of a threat identified through detection measures. Once a threat is assessed as legitimate, security personnel initiate an appropriate response.

Respond by alerting the guards, police, or emergency personnel who are trained and equipped to prevent the attack. Response may also include a reaction to the threat, such as sheltering in place or taking other preparatory measures, or a reaction to reduce the severity of consequences.

Delay, as a component of the resilience cycle, requires early detection of the attack. Examples of delay measures include fencing, distance, vehicle barriers, ditches, and culverts.

Defend using measures to protect an asset from aggression by preventing the aggressor's movement toward the asset or by shielding the asset from weapons and explosives. The objectives of defensive measures include the following:

- Delay aggressors from gaining access by forced entry. These measures include barriers along with a guard force for response.
- Prevent an aggressor's movement toward an asset. These measures provide barriers that deter movement and obscure lines of sight.
- Protect the asset from the effects of tools, weapons, and explosives.
- Incorporate an access control function when entry through the defensive layer must be provided.

Defensive measures may be active or passive. Active defensive measures are manually or automatically activated in response to acts of aggression, while passive defensive measures do not depend on detection or a response. They include such measures as blast-resistant building components, blast walls, and envelope protection against CBR attacks. Guards may also be considered a defensive measure.

Deny the aggressor access to the target or asset. Denial measures may include the use of response teams and other defensive measures.

Defeat of the aggressor's intentions is the primary objective of protective systems. Defensive and detection systems must be designed to accommodate (or at least not interfere with) response activities.

Evaluate the security system to determine the effects of an attack after it has taken place. Develop a priority list of corrective actions required to recover and fully restore the security system.

Recover once the security system is returned to operational stability following an attack or other disruption. Initial recovery may only be partial, to maintain basic functions, rather than a full restoration of the security system. Recovery may include hasty provisions that quickly repair the protective system or asset so that it can operate until more substantial repairs are made. Examples of hasty provisions include jersey barriers, portable lighting, and alternative power connections.

Reevaluate and improve the security system against new threats. This evaluation often includes an after action review by key personnel to identify what went wrong and what went right, and the development of a list of corrective actions.

Restore full functionality of the security system or asset following an attack. This normally involves replacing hasty fixes with permanent repairs. For instance, after an attack a security system may include the placement of jersey barriers to temporarily provide protection to an asset. As time progresses and resources are acquired, a permanent wall barrier may be provided to improve protection.

Test the operation of a security system against all defined threats. Testing can be performed through various methods, including the following exercises: drills, tabletop, functional unit, and full scale. Testing should occur regularly based on the threat profile. For general guidance, quick reaction drills should be performed frequently (several times a month, for varying threat scenarios), and a full-scale exercise should be performed annually. Full-scale exercises should include multiple drills (e.g., response to suspected explosive device, partial or full-scale evacuation, activation of the continuity plan).

Deter is an element commonly mentioned in security arena; however, it is not illustrated in the resilience concept, because deterrence is a byproduct of an effective security system. Deterrence is not a definable design objective, because it depends on aggressors' sophistication and determination, the asset's attractiveness, and the aggressors' objectives.

5.4 Security system design

Security practitioners and building owners have found that a multidisciplinary design approach is the most effective way to incorporate security measures. The multidisciplinary approach in developing the security system combines various architectural and engineering disciplines with expertise in security, blast resistance, and CBR protection to better define the threat and develop and apply protection strategies that complement each other to design an effective the security system.

Figure 5-13 illustrates the multidisciplinary approach and highlights each discipline's security system responsibilities. The team leader, who oversees the multidisciplinary endeavor, must understand the risks to the asset, coordinate each discipline's countermeasures, and ensure the goals of the security system are accomplished. Planning and design charettes are recommended for the multidisciplinary team to ensure all components are considered in the development of the security system. The multidisciplinary approach is a major element of the FEMA 452, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks* (2005), and FEMA 455, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks* (2009), risk publications and is strongly recommended for assessing and designing the security system.

Figure 5-13: Multidisciplinary approach to developing the security system

5.4.1 Design Process Components

Programming is the first stage in the design of a new facility or the major renovation of an existing facility. The architect/engineer design team begins by determining the needs and functions that a facility must meet. Blast, CBR, and security consultants are included at this stage of the project, because the earlier the security system can be integrated into the facility design the more functional and effective the system will be. Prior to the risk assessment, a security feasibility study should be performed on the potential facility locations, as the site location will greatly influence the risks faced and the potential protective measures available.

Programming is the first stage in the design of a new facility or the major renovation of an existing facility.

The multidisciplinary design team should participate in a security design charette to identify the constraints and opportunities for the security system. This design can include the asset site, vehicle and pedestrian circulation, and potential protective measures. The results of the design charette should be captured in a security-programming document to aid in the development of a proper security system for the facility.

Schematic Design lays out the major components of the facility based on the facility program. The security system planning begins at this stage so that the plan can be incorporated into the overall facility layout. Asset placement, space adjacencies, security layers, and facility circulation greatly affect the security plan. Security consultants play key roles in determining these aspects of a facility. This is also the first phase of the cost estimation process.

Design Development focuses on the details of the system and a refinement of the security system plan, the security program, the device layout plan, and cost estimates. The resulting information is used to conduct a BCA of the proposed security system.

Construction Documents include detailed drawings, construction specifications, and final cost estimates.

Construction supervision, site inspections, responses to requests for information, and security system testing should be performed by security experts.

5.4.2 Security System Design Process

A security system integrates all the protective measures and procedures required to protect the asset against certain threats. The ideal security system detects, delays, defends against, and defeats aggressors' attacks. Table 5-2 provides an overview of the programming procedure for developing a security system.

Table 5-2: Security System Development Procedure

Step #	Description
1	Selecting Protective Strategies
2	Assessing Design Opportunities and Constraints
3	Selecting Required Protective Measures
4	Integrating Protective Measures into the Security System
5	Assessing Security Systems Acceptability
6	Preparing Design Documentation
7	Verifying Security System

Step 1 – Selecting Protective Strategies: Selection of the appropriate design strategy for each type of attack is based on the level of protection associated with that type of attack. These strategies help designers to determine appropriate and necessary protective measures. This step should not be limited to the protective measures discussed in this manual. Measures should be tailored to project-specific conditions, using the selected strategies as guidelines only.

Step 2 – Assessing Design Opportunities and Constraints: Constraints listed in the planning phase included nontechnical considerations related to user requirements. For the design phase, assessment of opportunities and constraints must be related to technical design considerations. These considerations may include site-specific design elements, existing or planned protective measures, environmental factors, or project criteria not related to security. Opportunities to enhance protection, reduce requirements for protective measures, or solve a design problem may save time, design effort, or money. Constraints restrict design or create additional problems that must be compensated for by the protective design.

Step 3 – Selecting Required Protective Measures: Selection of required protective measures must be performed separately for each asset and each applicable type of attack. The attack types should be should be prioritized according to the severity of their effects against the asset. The protective measures for one attack type generally provide advantages for protecting against the less severe attack types. This approach most of the time eliminates the need for major modification of the design from one attack type to the next.

Step 4 – Integrating Protective Measures into the Security System: Selected protective measures for an individual asset represent a preliminary protective system. At this point, the emphasis changes from individual assets to the facility as a whole. To ensure uniform and effective protection of all assets against all threats, protective measures must be integrated into a system. Integrating the protective measures into a single system also avoids duplicated or unnecessary protective measures. To integrate a security system effectively, consider the following requirements:

- The preliminary security systems for all assets should be evaluated.
- The proposed protective measures should not adversely affect facility operations or adjacent facilities.
- The protective measures for one asset should be compatible with measures for other assets.
- Individual assets should be protected uniformly (if possible) to the appropriate levels of protection and threat severity levels. Under no circumstances should the protective measures interfere with the operations of the protected asset.
- The selected protective measures form the security system for the project, which is specified in sketches, layouts, and schematics depicting the security system components.

Step 5 – Assessing Security System Acceptability: The acceptability of the security system to the owners and users of the facility should be assessed before finalizing the design.

Step 6 – Preparing Design Documentation: The design documentation should contain the design criteria and any technical information, such as sketches, schematics, or reports, necessary to justify the proposed security system and support the cost estimate.

Step 7 – Verifying the Security System: Verification often requires the design team to review aggressor sequence diagrams and run through the various attack scenarios to confirm the security system meets the prescribed countermeasures.

5.4.3 Aggressor Sequence Diagram

The objective of the security system design process is to identify the most appropriate protective measures for the asset. The aggressor sequence diagram is a key tool for developing the security system in the design phase (see Figures 5-14 and 5-15). These diagrams allow the design team to understand each attack type scenario.

Aggressor sequence diagrams show the events between the time an attack is detected and the time it has ended. Detection begins upon receipt of the first alarm and ends when the threat is assessed. The delay function slows down the aggressor to allow the security system to respond to the attack.

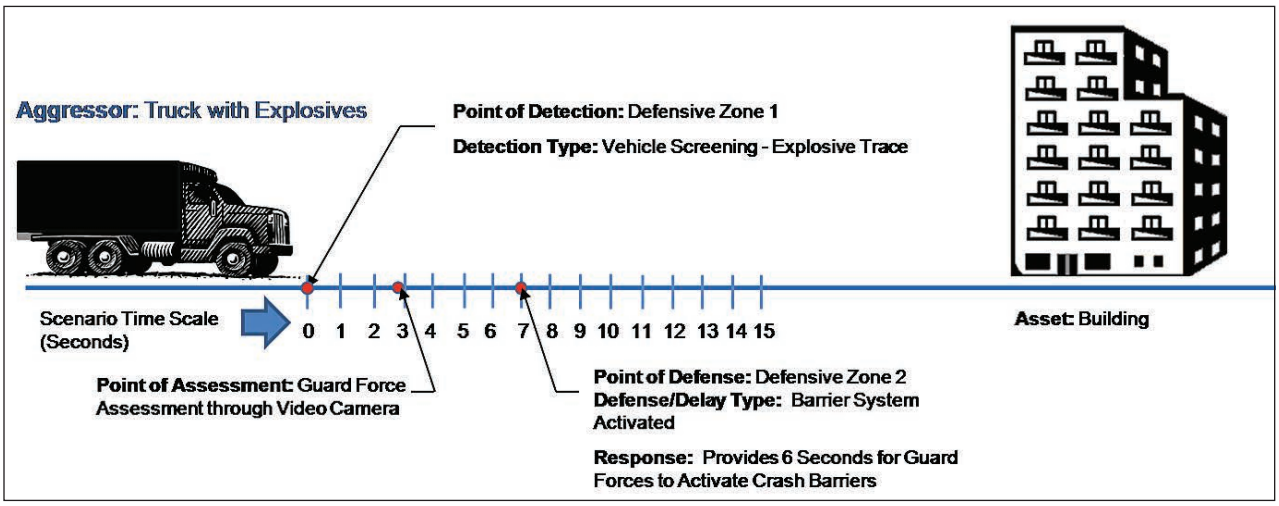


Figure 5-14: Aggressor sequence diagram of a truck with explosives

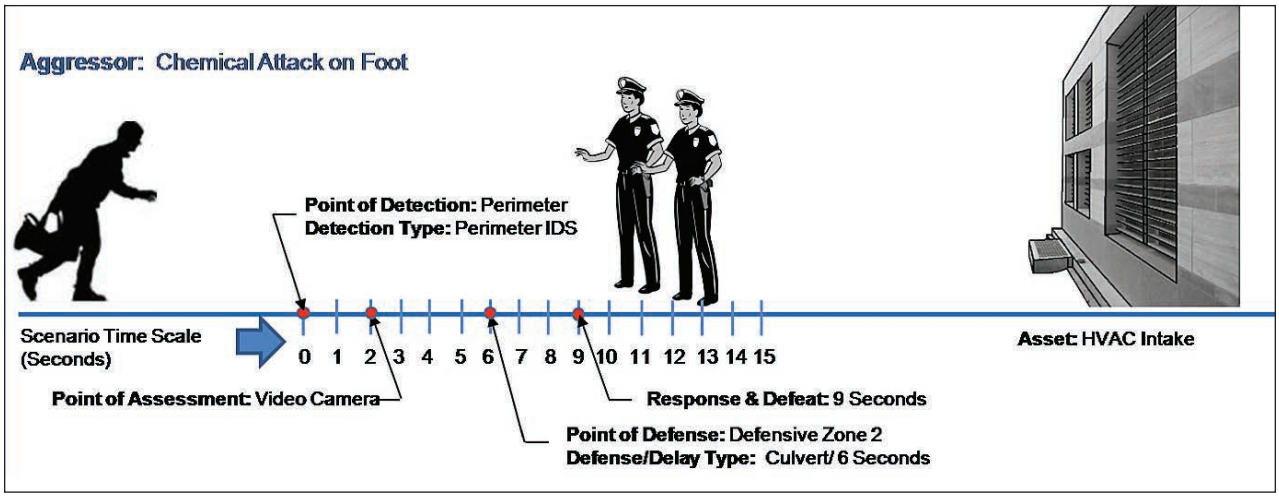


Figure 5-15: Aggressor sequence diagram of a chemical attack on foot

While these aggressor sequence diagrams are simplified, they provide examples of the attack types that the designers can use to determine effective protective measures. One potential weakness of the aggressor sequence diagram is that it illustrates only one scenario (specific location, a specific aggressor type, and a specific attack type). A well-trained aggressor will conduct preoperational surveillance of the target for a long period to understand strengths and weaknesses of various tactics against the security system. A significant validation of this strategy is the variation of aggressor tactics used in the 1993 bombing and 2001 passenger airliner attacks on the WTC. The attacks illustrate aggressors' determination, which design teams must consider.

5.4.4 Security System Evaluation and Adjustment

The security system should be evaluated and adjusted on a regular basis and as circumstances change. Changes in procedural measures may require adjustments with the security system plan where intrusion detection, electronic access controls, and video assessment systems may be used to offset the risks for procedural changes.

When evaluating the security system, the following legal matters should be considered:

- **Personal Privacy:** Privacy is a constitutionally protected right that comes into direct conflict with many antiterrorism and counterterrorism concepts. Many privacy issues can be avoided by proper signage and disclosure to inform facility users of the technologies employed as part of the security system. In any situation that creates concern over the potential violation of individual's rights, legal counsel should be obtained.
- **Premises Liability and Landlord/Tenant Responsibility:** Premises liability is the legal concept that the facility owner can be held responsible for the injury of a legitimate site user. This means that every facility owner (landlord) has a responsibility to provide a safe and secure facility for its users (tenants). Failure to do so could result in legal consequences for the facility owner. The most common legal issue a landlord faces is neglect or failure to provide a minimum level of protection in accordance with legal requirements.
- **Security Personnel:** Guards are a valuable part of the security system. However, even if armed, they are typically not sworn officers of the law and do not possess the same legal authority as that of a police officer. Facility management and the security personnel must understand the local laws governing their actions to prevent potential illegal detention, use of force, or search and seizure.

5.5 Electronic Security System Design and Equipment

An electronic security system has a degree-of-protection effectiveness that is based on its ability to detect aggressors attempting to overcome or even destroy the security system. A well-designed system minimizes the possibility of a successful attack. Sensors are designed to detect specific changes within a certain range. The probability of detection for a specific sensor is usually specified at 90 percent or greater, but this probability of detection is based on certain constraints and environmental conditions.

When a sensor malfunctions, it either does not provide an alarm when it should, or it provides a false alarm, also known as a nuisance alarm. To prevent the first malfunction, electronic security devices must be installed properly and tested in accordance with manufacturers' recommendations to identify when a sensor is not performing within its set parameters.

Nuisance alarms are a major concern for the electronic security system. Manufacturers' specifications usually do not discuss the weaknesses of devices or their vulnerability to external conditions. These can range from climatic conditions, such as wind or rain, to environmental causes, such as animals, including insects. When an alarm is annunciated in the SOC, the operator must determine the cause of the alarm (intrusion or nuisance). Timely assessment is essential, because when the operator cannot determine whether the alarm is a nuisance alarm, the security system must react as if it were an intrusion.

5.5.1 Intrusion Detection

Intrusion detection sensors are customarily used to detect an aggressor crossing the boundary of a protected area (perimeter), in clear zones between physical barriers (volumetric), or the building itself (point). Intrusion detection systems should be configured as layers of unbroken rings concentrically surrounding the building. These rings should correspond to defensive layers that constitute the delay system. The first detection layer is located at the outermost defensive layer necessary to provide the required delay. Based on the required delay time, detection layers can be on a defensive layer, in the area between two defensive layers, or on the building itself. For example, if a wall of an interior room provides sufficient delay for effective response to an attack,

Intrusion detection sensors are customarily used to detect an aggressor crossing the boundary of a protected area (perimeter), in clear zones between physical barriers (volumetric), or the building itself (point).

detection layers could be placed at a facility's perimeter or on the exterior wall. Either would detect the aggressor before penetration of the interior wall. Based on the risk, the facility could place detection devices on both the perimeter and the exterior wall to provide two layers of detection. Each added layer improves the probability of detection.

The interior detection layers and exterior detection layers are functionally uniform, but their overall effectiveness and cost may be different. Although the probability of detection is the same for both systems, exterior sensors are more likely to experience weather-related or other environmental variations that cause the system's reliability to vary. Because of environmental conditions, the exterior electronics must be designed and packaged for extremes of temperature, moisture, and wind. Consequently, exterior electronic packages are more costly than equivalent packages for interior applications.

Inclement weather (fog, snow, and rain) may also affect VASS and security lighting by reducing their capability for remote assessment of alarm alerts.

State-of-the-art exterior sensors do not detect penetration attempts above the height of a fence (typically 8 feet [2 meters]). Fence-mounted sensors are usually limited to this height because the fence fabric or poles are used to support the sensor.

An interior electronic security system may be far less costly than that of a comparable exterior electronic security system, suggesting value for the designer in selecting and deploying a well-planned, well-designed, layered system. The basic rule in overall design of an electronic security system is to design from the inside out, that is, layered from the building to the site boundary. The outer detection layers are often the most important component of the protection system because they provide the earliest detection, so the farther the detection layer is from the target the better.

5.5.1.1 Exterior Intrusion Detection Devices

Fence sensors detect attempts to penetrate a fence around a protected area. Penetration attempts (e.g., climbing, cutting, lifting) generate mechanical vibrations and stresses in fence fabric and posts that are usually different than those caused by natural phenomena like wind and rain. The basic types of sensors used to detect these vibrations and stresses are strain-sensitive cable, taut wire, fiber optics, capacitance, buried-line sensors, microwave sensors, and infrared sensors.

Fence sensors detect attempts to penetrate a fence around a protected area.

- **Strain-sensitive cable sensors** are transducers that are uniformly sensitive along their entire length. They generate an analog voltage when subject to mechanical distortions or stress resulting from fence motion. Strain-sensitive cables are sensitive to both low and high frequencies. Because the cable acts like a microphone, some manufacturers offer an option that allows the operator to listen to fence noises causing the alarm. Operators can then determine whether the noises are naturally occurring sounds from wind or rain or are from an actual intrusion attempt.
- **Taut wire sensors** combine a physically taut wire barrier with an intrusion detection sensor network. The taut wire sensor consists of a column of uniformly spaced horizontal wires up to several hundred feet in length and securely anchored at each end. Typically, the wires are spaced 4 to 8 inches (10 to 20 centimeters) apart. Each is individually tensioned and attached to a detector located in a sensor post.
- **Fiber optic cable sensors** are functionally equivalent to the strain-sensitive cable sensors. Instead of electrical signals, modulated light is transmitted down the cable and the resulting received signals are processed (automatically by software or manually) to determine whether an alarm should be initiated. Because the cable does not transmit electrical signal, fiber optic sensors, as shown in Figure 5-16, are generally less susceptible to electrical interference from lightning or other sources.

Figure 5-16:
Fiber optic sensors

COURTESY OF FIBER SENSYS CORPORATION

- **Capacitance proximity sensors** measure the electrical capacitance between the ground and an array of sensory wires. Any variations in capacitance, such as that caused by an aggressor approaching or touching one of the sensory wires, initiates an alarm. These sensors usually consist of two or three wires attached to outriggers along the top of an existing fence, wall, or roof edge.
- **Buried-line sensor systems** consist of detection probes or cable buried in the ground, typically between two fences that form an isolation zone. These devices are wired to an electronic processing unit. The processing unit generates an alarm when an aggressor passes through the detection zone (Figure 5-17). The advantages of buried-line sensors are that they are hidden, making them difficult to detect and circumvent; they follow the terrain's natural contour; and they do not physically interfere with human activities. However, they may be affected by certain environmental conditions, such as running water and ground freeze/thaw cycles.

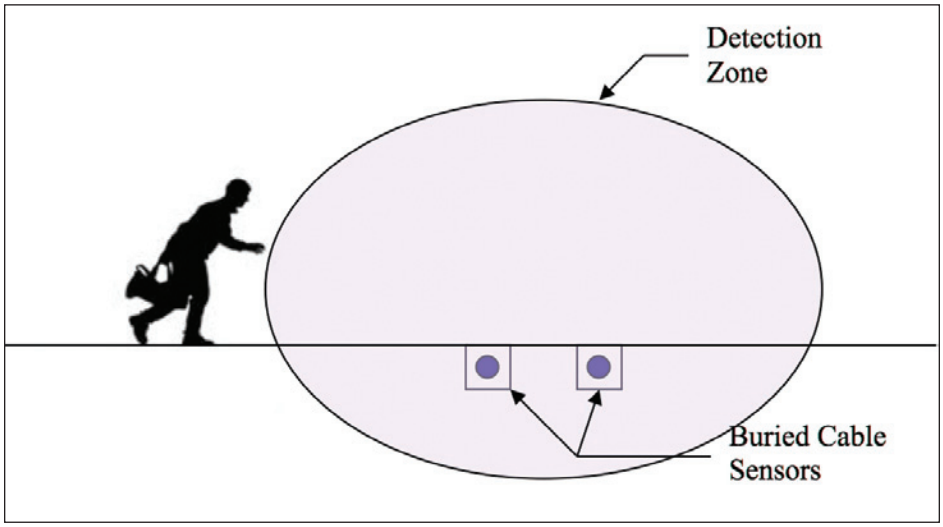


Figure 5-17: Buried-line sensor

- **Microwave sensors** can be bistatic or monostatic. Bistatic sensors use transmitting and receiving antennas located at opposite ends of the microwave link, whereas monostatic sensors use one antenna. A bistatic system uses a transmitter and a receiver, typically separated by 100 to 1,200 feet (30 to 366 meters), within direct line of sight of each other. Monostatic microwave sensors use the same antenna or virtually coincident antenna arrays for the transmitter and receiver, which are usually combined into a single package. Three dimensional microwave sensors perform volumetric types of coverage.

- **Infrared sensors** are available in both active and passive models. An active sensor generates one or more near-infrared beams that generate an alarm when interrupted. A passive sensor detects changes in thermal infrared radiation from objects located within its field of view. Active sensors consist of transmitter/receiver pairs (Figure 5-18). The transmitter contains an infrared light source, such as a gallium arsenide LED (light emitting diode) that generates an infrared beam. The light source is usually modulated to reduce the sensor's susceptibility to unwanted alarms resulting from sunlight or other infrared light sources. The receiver detects changes in the signal power of the received beam. To minimize nuisance alarms from birds or blowing debris, the alarm criteria usually require that a high percentage of the beam be blocked for a specific interval of time.

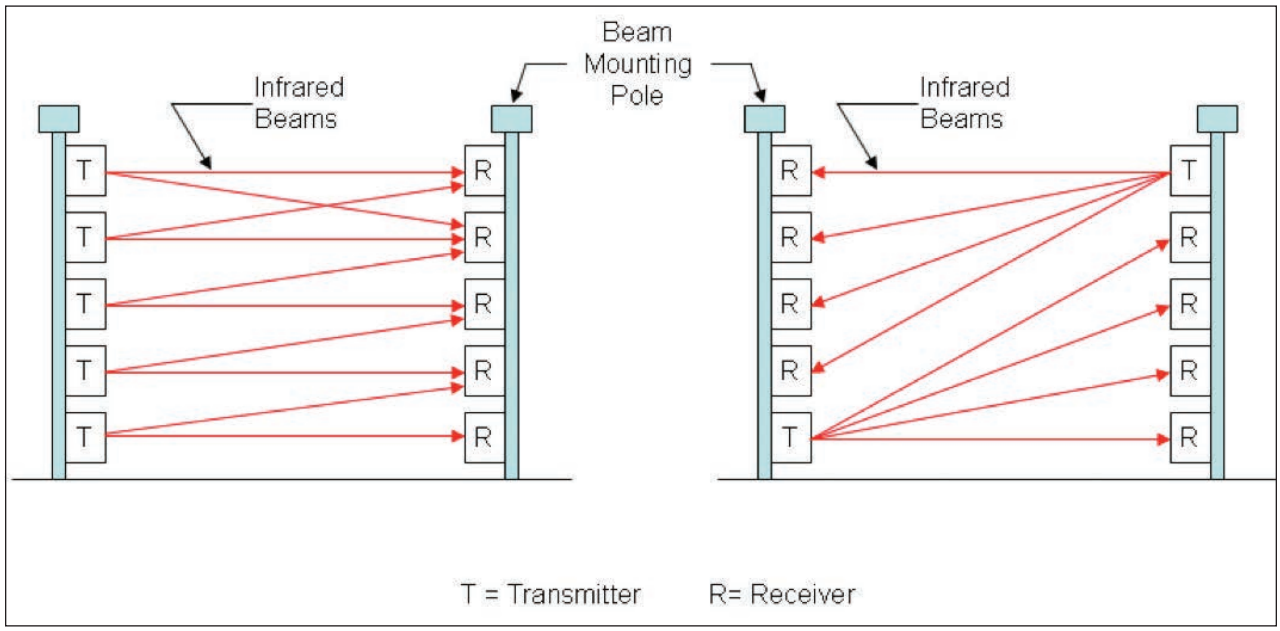


Figure 5-18: Infrared beams

SOURCE: U.S. FIELD MANUAL 3-19-30, DEPARTMENT OF THE ARMY

5.5.1.2 Interior Intrusion Detection

Interior intrusion detection typically consists of boundary-penetration sensors, volumetric motion sensors, and video analytics that are designed to detect intruders within the interior of the protected asset. Interior intrusion detection systems usually have the same probability of detection but are far less costly than comparable exterior systems because of the lack of exposure to weather-related variations and size of the detection zone.

- **Boundary-penetration** sensors are designed to detect penetration or attempted penetration through perimeter barriers. These barriers include walls, ceilings, duct openings, doors, and windows. The most common sensors are piezoelectric transducers that sense mechanical energy and convert it into electrical signals proportional in magnitude to the vibrations. Glass break sensors use microphone transducers to detect the breakage of glass. The noise from breaking glass consists of frequencies in both the audible and ultrasonic range. The sensors are designed to respond to specific frequencies only, thus minimizing false alarms. Magnetic switches are typically used to detect the opening of a door. These sensors can also be used on windows, hatches, gates, or other structural devices that can be opened to gain entry.

Interior intrusion detection typically consists of boundary-penetration sensors, volumetric motion sensors, and video analytics that are designed to detect intruders within the interior of the protected asset.

- **Volumetric motion sensors** are designed to detect motion within the interior of a protected volume, and can be active or passive. Active sensors (such as microwave) fill the volume with an energy pattern and recognize a disturbance in the pattern when anything moves within the detection zone. Unlike active sensors that generate their own energy pattern, passive sensors (such as infrared) detect energy generated by an intruder. Some sensors, known as dual technology sensors, use a combination of two different technologies, usually one active and one passive, within the same unit. Where VASS assessment or surveillance cameras are installed, video analytic sensors can be used to detect movement within the area. The most commonly used sensors are passive infrared motion sensors, which detect a change in the thermal energy pattern caused by a moving intruder and initiate an alarm when the change in energy satisfies the detector's alarm criteria. These sensors are passive devices because they do not transmit energy; they monitor the energy radiated by the surrounding environment. Microwave motion sensor is an active detection device, which is less common for interior use because microwaves easily penetrate common building materials like gypsum wallboard. When a microwave sensor is installed in a room, it commonly detects movement outside of the secure space. This creates a high rate of nuisance alarms.

Volumetric motion sensors are designed to detect motion within the interior of a protected volume, and can be active or passive.

Dual technology sensors, used to minimize the generation of alarms caused by sources other than intruders, combine two different

technologies in one unit. Ideally, this combination is achieved by combining two sensors that individually have a high probability of detection and do not respond to common sources of false alarms. Available dual technology sensors combine an active ultrasonic or microwave sensor with a passive infrared sensor. The alarms from each sensor are logically combined in an "and" configuration, such that nearly simultaneous alarms from both active and passive sensors are needed to produce a valid alarm.

- **Video analytics** or intelligent video (for intrusion detection) is a technology used to analyze video for specific data, behavior, objects, or attitude. It has a wide range of applications, including safety and security. The software processes and compares successive images with predefined alarm criteria.

  Video analytic sensors provide a new dimension to intrusion detection, and allow intrusion to be measured in many different ways. The sensors can be programmed to activate alarms, initiate recording, or any other designated action when a security camera detects activity. Video analytics can also greatly improve the efficiency of security monitoring. The following are examples uses of video analytic equipment made available by many video analytic manufacturers:

  - License plate recognition
  - Loitering recognition
  - Objects left behind
  - People counting
  - Tailgating
  - Tripwire alerts
  - Video motion alerts

Table 5-3 describes the effectiveness of different exterior sensor types in terms of the probability of detection. Table 5-4 describes the relative susceptibility of the exterior sensors to false alarms. Table 5-5 displays the relative cost comparisons of the different exterior intrusion detection systems.

Table 5-3: Estimate of Probability of Detection by Exterior Sensors

Type of Sensor	Aggressor Technique											
	Slow Walk	Walking	Running	Crawling	Rolling	Jumping	Tunneling	Trenching	Bridging	Cutting	Climbing	Lifting
Fence Mounted	N/A	N/A	N/A	N/A	N/A	VH	VL	L	VL	M/H	H	M/H
Taut Wire	N/A	N/A	N/A	N/A	N/A	VH	VL	VL	VL	H	H	H
Electric Field	VH	VH	VH	H	VH	VH	VL	L	L	N/A	N/A	N/A
Capacitance	VH	VH	VH	H	H	VH	VL	L	L	N/A	N/A	N/A
Ported Cable	H	VH	VH	VH	VH	H	M	VH	L	N/A	N/A	N/A
Seismic	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Seismic/magnetic	H	VH	H	M	M	M	L	M	L	N/A	N/A	N/A
Microwave	H	VH	H	M/H	M/H	M/H	VL	L/M	L	N/A	N/A	N/A
Infrared	VH	VH	VH	M/H	M/H	H	VL	L	VL	N/A	N/A	N/A
Video Analytics	H	VH	VH	H	H	H	VL	L/M	M	L	L	L

VL = very low, L = low, M = medium, H = high, VH = very high, N/A = not applicable

Table 5-4: Relative Susceptibility of Exterior Sensors to False Alarms

Type of Sensor	Type of Interference											
	Wind	Rain	Standing Water/ Runoff	Snow	Fog	Small Animals	Large Animals	Small Birds	Large Bird	Lighting	Overhead Power Lines	Buried Power Lines
Fence Mounted	H	M	L	L	VL	L	M	L	L	L	VL	VL
Taut Wire	VL	VL	VL	VL	VL	VL	L	VL	VL	VL	VL	VL
Electric Field	M	H	VL	M	VL	M	VH	L	M	M	L	VL
Capacitance	M	M	VL	M	VL	M	VH	L	M	M	L	VL
Ported Cable	VL	M	H	L	VL	VL	M	VL	VL	M	VL	L
Seismic	M	L	L	L	VL	L	VH	VL	VL	L	L	M
Seismic/magnetic	M	L	L	L	VL	L	VH	VL	VL	H	M	H
Microwave	L	L	M/H	L/M	L	M/H	VH	VL	M	L/M	L	VL
Infrared	L	L	L	L	M	M	VH	L	M	L	VL	VL
Video Analytics	M	L	L	L	M/H	L	VH	VL	M	L	L	VL

VL = very low, L = low, M = medium, H = high, VH = very high

Table 5-5: Exterior Intrusion Detection System Sensor Cost Comparison

Type of Sensor	Equipment	Installation	Maintenance
Fence Mounted	L	L	L
Taut Wire	H	H	M
Electric Field	H	M	M
Capacitance	M	L	M
Ported Cable	H	M	M
Seismic	M	M	L
Seismic/magnetic	H	M	L
Microwave	M	M	L
Infrared	M	L	M
Video Analytics	M	L	M

VL = very low, L = low, M = medium, H = high, VH = very high

5.5.2 Entry Control Systems

Electronic entry control systems ensure that only authorized personnel and visitors are permitted in or out of a controlled area. Electronic entry control systems are integrated into the security system layers of defense. Electronic entry control systems automatically verify that a person is authorized to enter or exit a portal. The automated system usually interfaces with locking mechanisms on doors or gates that open momentarily to permit passage. All entry control systems control passage using one or more of three authentication factors (something a person knows, something a person has, or something a person is or does). Automated entry control devices based on these techniques are grouped into three categories: coded, credential, and biometric devices.

Locations of proposed access control points should be determined based on compliance with the defensive layers and security system plan.

Electronic entry control systems ensure that only authorized personnel and visitors are permitted in or out of a controlled area.

Vehicular access control to the site and screening are covered in Chapter 2.

Vehicular access control to the building limits vehicular circulation in or around the building to trusted vehicles that have been cleared; handicapped parking and emergency apparatus must also be considered.

Pedestrian access to the building, including loading docks and any other similar portals to the building, should be protected with alarm points. Public entrances may be configured for after-hours access and/or automatic locking after hours. Signage may be necessary to direct the pedestrian traffic, and intercoms may be needed to direct visitors to the correct entry.

Access beyond the public lobby is controlled by way of visitor badging and electronic turnstiles, which need to be placed near the lobby desk to ensure that a security officer at the desk has a good view of the turnstiles, in case anyone needs assistance or attempts to circumvent them. Figure 5-19 shows, at a schematic level, lobby area security and views of various pedestrian entry types that must be considered.

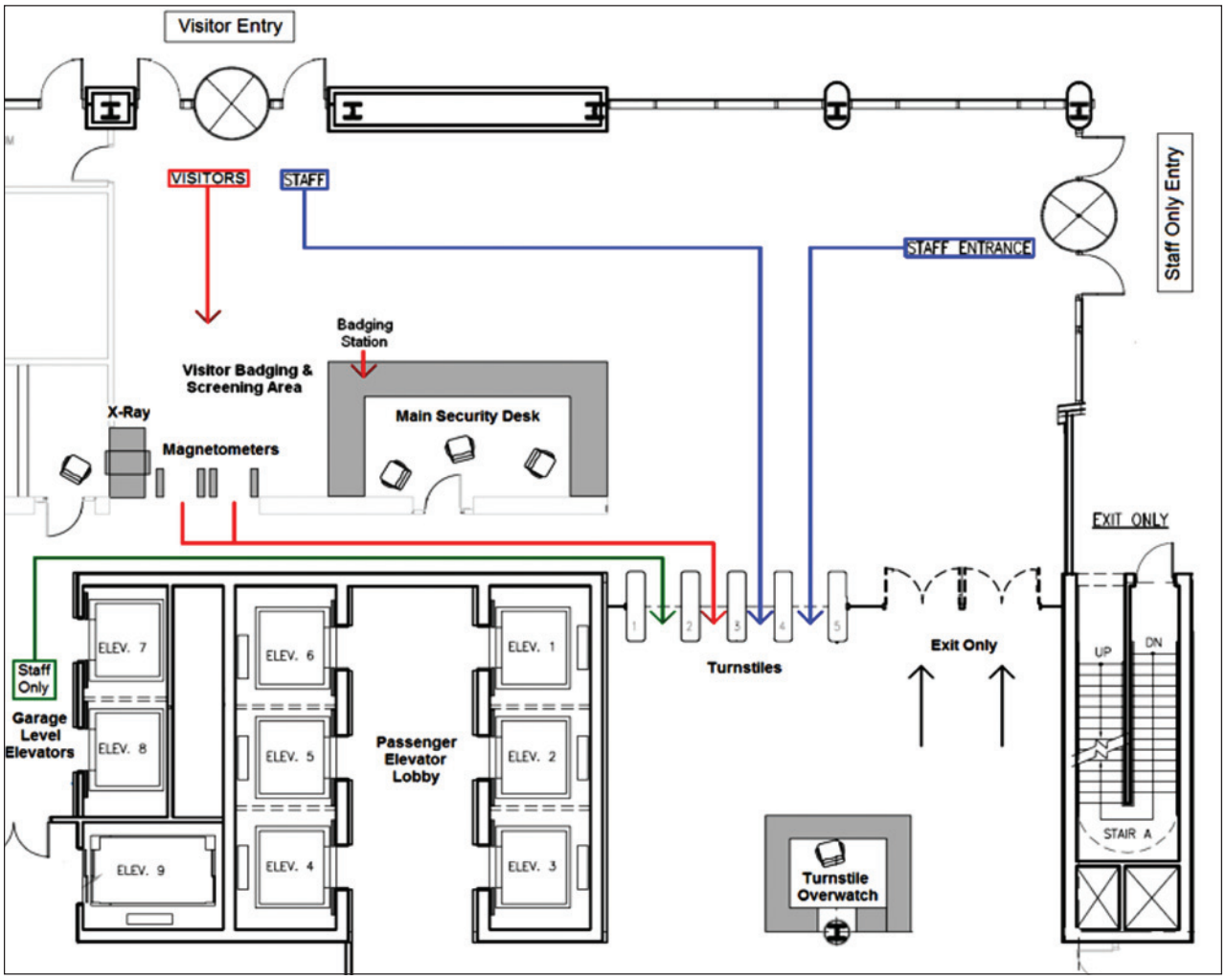


Figure 5-19: Lobby area security and pedestrian entry

Access to semipublic spaces that may include elevator lobbies and common corridors on upper floors may be permitted to screened and badged visitors, but access into staff only spaces may require escort.

Vertical access control is complicated by several factors. To start with, throughput rates must be considered for busy times, such as, the beginning of the workday (entering), lunchtime (entering and exiting), and the end of the day (exiting). Elevators are perfect conduits for tailgating, which minimizes control. Life-safety code requirements for egress add further complications. This combination of factors requires careful and purposeful design of vertical access control to meet functional requirements within the constraints of each project.

Access to high-security areas, in buildings with high-value assets, should be controlled with multi-factor authentication procedures.

Access to high-security areas, in buildings with high-value assets, should be controlled with multifactor authentication procedures. Common two-factor authentications are card plus code and card plus a biometric. Examples of high security areas where it is typical to use multifactor authentication include server rooms, datacenters, research laboratories, and classified work areas. Throughput rates are an important consideration when determining if and where to use multi-factor authentication. Electronic entry control devices are grouped into three categories: coded, credential, and biometric devices.

Coded devices operate on the principle that a person must enter a code to be admitted by an entry control device. Depending on the application, a single code can be used by all authorized persons, or each authorized person can be assigned a unique code. Group codes are useful when the group is small and controls are primarily for keeping out the general public. Individual codes are usually required for control of entry to more critical areas. Coded devices verify the authenticity of the entered code, and any person entering the correct code is authorized to enter the controlled area. Electronically coded devices include electronic and computer-controlled keypads.

- **Electronic keypad devices** consist of simple pushbutton switches. When the correct sequence of buttons is pushed, an electric signal unlocks the door for a few seconds. The common telephone keypad (12 keys) is an example of an electronic keypad.
- **Computer-controlled keypad** devices are equipped with a microprocessor in the keypad or in a separate enclosure at a different location. The microprocessor monitors the sequence in which the keys are

depressed and may provide additional functions such as personal ID and digit scrambling. When the correct code is entered and all conditions are satisfied, an electric signal unlocks the door.

Credential devices identify a person using a credential (e.g., plastic card or key) that contains a prerecorded code authorizing entry into a controlled area. Similar to coded devices, credential devices only authenticate the credential assuming the user of the credential is authorized to enter. The following cards are the most commonly used types of credentials:

- **Magnetic-stripe cards**, which many bank debit and credit card companies also use, are read by moving the card past a magnetic reader.

- **Proximity cards** are not physically inserted into a reader; the coded pattern on the card is sensed when it is brought within several inches of the reader. The card is sensed using inductive coupling via an LC circuit that includes an integrated circuitry, capacitor, and coil. The card reader produces an electromagnetic field that excites the coil and resonant current charges the capacitor, which in turn energizes and powers the integrated circuitry.

- **Smart cards** are embedded with a microprocessor, memory, communication circuitry, and a battery (Figure 5-26). The card contains edge contacts that enable a reader to communicate with the microprocessor. The smart card is a relatively new technology that the U.S. Government has standardized for use under Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors (U.S. Department of Commerce 2006), which was derived from HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors (DHS 2004b).

- **Implant chips** are slightly larger than a grain of rice, and may be implanted in a user's arm to provide access to high security areas. They are used to control access to physical structures, such as government or private sector offices or nuclear power plants, instead of swiping a smart card, an employee could swipe an arm containing the chip.

Biometric devices are based on the measurement of one or more physical or personal characteristics of an individual. Most entry control devices based on this technique rely on measurements of biological characteristics, thus they have become commonly known as biometric devices. Devices recognizing characteristics such as fingerprints, hand geometry, voiceprints, handwriting, and retinal blood vessel patterns have been used for entry control. Typically, several reference measurements are made of

the selected characteristic for the individual and stored in the device's memory or on a card. When that person attempts entry, a scan of the characteristic is compared with the reference data template. When a match is found, entry is granted. Rather than verifying an artifact, such as a code or a credential, biometric devices verify a person's physical characteristic, thus providing a form of identity verification, and are sometimes referred to as personnel identity verification devices. The most common biometric devices are discussed below:

- **Fingerprint verification devices** use one of two approaches. One is pattern recognition of the whorls, loops, and tilts of the referenced fingerprint, which is stored in a digitized representation of the image and compared with the fingerprint of the prospective entrant. The second approach is minutiae comparison, which means that the endings and branching points of ridges and valleys of the referenced fingerprint are compared with the fingerprint of the prospective entrant.
- **Retinal pattern verification** is based on the premise that the pattern of blood vessels on the retina is unique to an individual. While the eye is focused on a visual target, a low-intensity infrared light beam scans a circular area of the retina. The amount of light reflected from the eye is recorded as the beam progresses around the circular path. Reflected light is modulated by the difference in reflectivity between blood vessel pattern and adjacent tissue. This information is processed and converted to a digital template that is stored as the eye's signature. Users are allowed to wear contact lenses; however, glasses should be removed.
- **Hand geometry devices** use a variety of physical measurements of the hand, such as finger length, finger curvature, hand width, webbing between fingers, and light transmission through the skin to verify identity. Both two- and three-dimensional units are available.
- **Facial recognition devices** are much like fingerprint devices where authentication is performed by pattern recognition of the facial features. Capturing a real-time three-dimensional image of a person's facial surface, three-dimensional facial recognition uses distinctive features of the face to identify the subject. These areas are unique and do not change over time. Using depth and an axis of measurement that is not affected by lighting, three-dimensional facial recognition can be used in darkness and has the ability to recognize a subject at different view angles with the potential to recognize up to 90 degrees (a face in profile). Using the three-dimensional software, the system goes through a series of steps to verify the identity of an individual.

An image is acquired by digitally scanning an existing photograph (two-dimensional) or by using a video image to acquire a live picture of a subject (three-dimensional). Once a face is detected, the system determines the head's position, size, and pose. The system then measures the curves of the face on a submillimeter (or microwave) scale and creates a template.

Biometric devices are based on the measurement of one or more physical or personal characteristics of an individual.

Table 5-6 compares the various physical entry control devices based on level of security, throughput rate (number of successful entries), and false rejection rate.

Table 5-6: Physical Entry Control Device Comparison

Physical Entry Control Devices	Criteria		
	Level of Security	Throughput Rate	False Rejection Rate
Group Codes	L	M	L
Individual Codes	M	M	L
Electronic Keypads	M	M	L
Computer Controlled Keypads	M	M	L
Magnetic Stripe Card Reader	M	H	L
Proximity Card Reader	M	M	M
Smart Card Reader	M	M	M
Implant Chip	H	M	L
Fingerprint Scanner	H	L	L
Retinal Scanner	H	L	L
Hand Geometry Scanner	H	L	L
Facial Recognition	H	L	L

VL = very low, L = low, M = medium, H = high, VH = very high

5.5.3 Video Assessment and Surveillance System

Historically, the term for a security video system was CCTV, a closed analog video system. Very few video systems today are either closed or completely analog. Because security video serves two distinct purposes, assessment and surveillance, the term used here is video assessment and surveillance system or VASS.

The primary function of a video system is to provide a rapid and cost-effective method for determining the source of the intrusion or other detection alarms. The secondary function of a video system is to support surveillance of activities and events within and around a facility. A properly designed video system provides a cost-effective supplement to guard patrols. The cost of a video system is more easily justified for a larger facility.

Site-specific factors must be considered when selecting components that comprise a particular VASS. First, the size of the system, in terms of the number of cameras fielded, is the minimum number needed to view all electronic security system sensor detection fields. Also, some cameras may require artificial light sources. Finally, performance criteria and physical, environmental, and economic considerations must be factored into the component selection.

Figure 5-20 shows a typical VASS configuration. The security console is centrally located and monitored in the SOC. Non-monitored equipment, such as servers, time synchronization, storage devices, and data transmission media can be located in the equipment room. The VASS supports the security system. An effective VASS must be located and designed in conjunction with sensor placement for the electronic security system and the shape of the detection fields.

The primary function of a video system is to provide a rapid and cost-effective method for determining the source of the intrusion or other detection alarms.

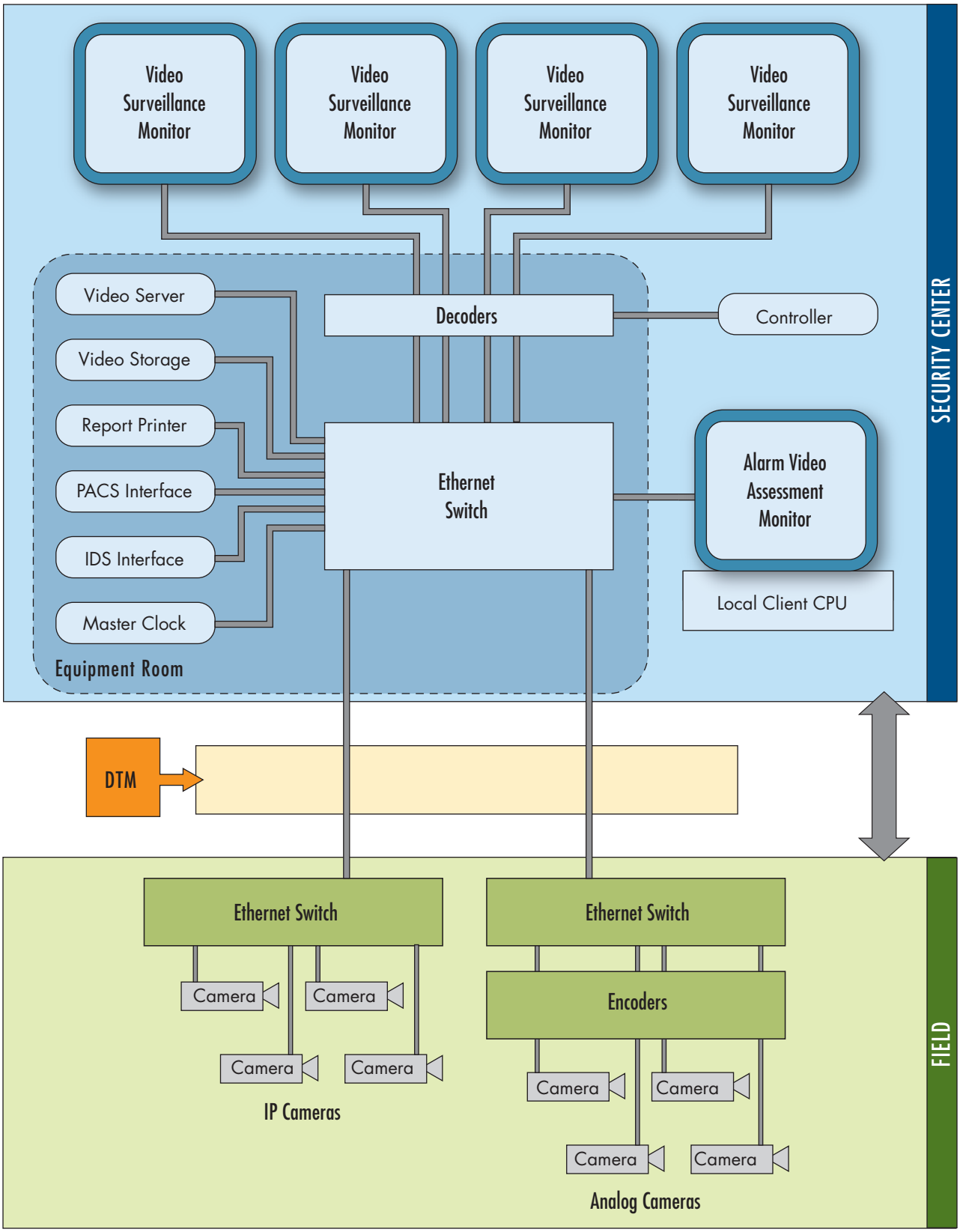


Figure 5-20: Typical digital VASS configuration. SOURCE: U.S. FIELD MANUAL 3-19-30, DEPARTMENT OF THE ARMY

5.5.3.1 Counterterrorism with Video Assessment and Surveillance System

A new effort in counterterrorism is to capture video of a potential aggressor's preoperational activities to halt the attack. Video technology is being used as a tool to capture complete scenes at specific high-risk locations where potential aggressors' preoperational activities may be spotted. Aggressors typically conduct reconnaissance activities to understand the security operations and target environment weeks or months before the actual attack. They may gather the following information in order to understand the best method of attack:

- Photos or video of the target
- Photos or video of security posts
- Photos of defensive obstacles (bollards, blast walls)
- Information based on attempts to probe gates or entry points
- Security operations and timing, by positioning themselves in the area
- Security operational response and readiness to a package left in the area

Every asset is subject to multiple means of attack. Consider the guidance provided in Chapter 1 for determining the threats. Making incomplete assumptions about threats or attack types can result in a failure to observe an aggressor's actual preoperational activity. For instance, focusing on a threat with handheld explosives directed at the lobby may detract from the preparations for the threat of a vehicle-borne explosive, which involves different preoperational activities.

5.5.3.2 Video Assessment and Surveillance System Design Considerations

Camera Location: Place cameras where they will capture an unobstructed field of view of the desired scene and where they will not be subject to vandalism, sabotage, or environmental damage. The number and type of cameras should be based on the level of detail required for the surveillance system design. For example, when facility security operators need to view the details of the face of a person entering a building as well as to see the type of car a person drives, two separate cameras may be required.

A typical site will locate video cameras to support detection in multiple locations:

- Outdoors, along site perimeter detection zones
- Outdoors, at controlled access points (sally ports)

- Outdoors, within the protected area, and to view approaches to selected assets
- Indoors, at selected assets within the protected area
- Indoors, at critical portals adjacent to assets

Place cameras where they will capture an unobstructed field of view of the desired scene and where they will not be subject to vandalism, sabotage, or environmental damage.

The placement of exterior cameras requires more attention than interior cameras because of weather and illumination extremes. The field-of-view alignment, illumination range, and balanced lighting are major design factors. Exterior design considerations include environmental housings, camera mounting heights, system types, and so forth.

Camera Type: Pan-tilt-zoom (PTZ) and fixed cameras each have distinct advantages and limitations. PTZ cameras can provide precise closeup views or wide-angle views in virtually any direction, whereas a fixed camera has a set field-of-view at all times. PTZ are best used for general surveillance of an area; fixed cameras are best used to view areas that require constant coverage.

Scene Resolution: The image detail in a camera scene is referred to as resolution. A video assessment system should provide sufficient resolution to provide the console operator with the ability to determine whether the sensor detected an intruder or is responding to a nuisance condition. For assessment purposes, three resolution requirements are generally accepted. In order of increasing resolution requirements, they are general surveillance, forensic detail, and high detail.

- General surveillance video should provide a minimum of 20 pixels per foot. This level of detail is often used for live viewing, where the detail of a recorded video is not necessary, for example, observing crowd activity without needing to recognize faces.
- Forensic-detail video should be a minimum of 40 pixels per foot. This level of detail is necessary to see, record, and recognize images such as license plates and faces. This allows the video to be referenced after an incident to determine exactly what happened and provide forensic evidence.
- High-detail video should provide a minimum of 80 pixels per foot. This level of detail is applicable in a retail or banking context in which the customer's and employee's faces, as well as the currency in their hands, can be seen.

Illumination Levels: For interior applications, where the same camera type is used in several different areas and the scene illumination in each area is constant, a manually adjustable iris is usually specified. A manual iris allows for adjustment appropriate to the illumination level at the time of installation. Where the camera must operate in an area subject to a dynamic range of illumination levels, such as outdoors or in a lobby with curtain walls, an automatically adjustable iris feature should be specified.

Cost Considerations: The cost of a VASS is usually quoted as per assessment zone. When estimating the cost for the total system, video-processor equipment and the video-transmission system must be included. Other potentially significant costs are outdoor lighting system upgrades and site preparation required to support the cameras. A VASS is expensive compared to other electronic security subsystems and should be specified with discretion.

Video Cameras: Cameras come in four main types. Understanding the distinctions makes it possible to select the right camera for the task and avoid spending more money than necessary by purchasing unneeded features. Most cameras come with fixed position or PTZ functionality.

- **Image sensors** are the heart of video camera technology. An image sensor is the component that is responsible for converting an image into an electrical signal. Two types of image sensors are most common in today's video cameras: charge coupled device (CCD) and complementary metal oxide semiconductor (CMOS). The CCD image sensor provides better low-light imaging. A CMOS imager is a pure digital sensor capable of higher resolution images than a CCD sensor. Another benefit of a CMOS sensor is that it provides a digital system from sensor to storage, whereas a CCD sensor must be digitized at some point for storage, and the encoding process creates some loss in image quality. All analog cameras use a CCD sensor, while digital (also known as Internet protocol [IP]) cameras use a mix of CCD and CMOS sensors. Image sensors of the same technology vary in quality, resulting in variations in the quality of images even with the same resolution.
- **Standard analog cameras** may be black and white or color. The most commonly used cameras are analog-based and may or may not have digital effects. Resolution ranges from 220 horizontal lines (very low) to 580 horizontal lines (very high). Light sensitivity varies between 0.005 lux (.00046 foot-candles), which is very low, to 10 lux (.929 foot-candles), which is very high. Color cameras are the most restricted by low-light conditions. To compensate for that limitation,

manufacturers have developed hybrid analog cameras. Some use infrared sensitivity to capture more light. Others combine color and black and white image capability in one unit, capturing color images during the daytime and black and white images at night or when the light level is low. Other cameras use intensifiers between the lens and the image sensor to amplify the available light tens of thousands of times. Analog cameras come in various mounting methods (indoor, outdoor, wall, ceiling, or parapet).

- **IP or digital cameras** come in black and white or color, similar to their analog counterparts, and require visible light to create an image. Resolution is typically measured in pixels and varies widely from a standard 0.3 megapixel (640x480 pixels) to 5 megapixels (2560x1920 pixels). The higher resolution of these cameras allows the use of fewer cameras to capture the same area when compared to analog cameras. The placement of video analytics at the camera is becoming more common on IP cameras, making it a powerful detection device. (Refer to Section 5.5.1.2, for a discussion of video analytics.) Many IP cameras use Power over Ethernet technology, by operating off an Ethernet switch requiring no other power source. Digital cameras have gained in popularity and have become a preferred technology.
- **Forward-looking infrared cameras** require an infrared light source to create an image. They are used where visible light is not an option.
- **Thermal cameras** require neither visible nor infrared light to produce an image, and are popular for low-light environments. Using special filters and lenses, the cameras monitor the temperature of objects in their field of view and use colors to represent temperatures. Thermal cameras are often used in long-range surveillance, such as monitoring ships in a harbor several miles away.

5.5.3.3 Video Recording and Retention

When planning to retain and use images for security purposes, the user must decide whether the objective is to verify information, prove it, or aid prosecution with it. This decision dictates the best type of video imaging for the situation. For example, when video information is used in a courtroom, admissibility may be determined by the quality of the recorded information, the way it was obtained, and proof of origin.

In comparing recording and storage systems with a mix of analog and digital video, understanding the fundamental differences in terminology is important. Analog video is measured in frames, whereas digital video is measured in images. An analog image is separated into two frames, one horizontal and one vertical.

The following are the basic types of recorders in use today:

- **Time-lapse recorders (analog)** are designed to make 2-hour videocassette recordings of up to 900 hours by allowing time to lapse between recorded images. The chosen duration dictates how much information is recorded. Instead of a full 30 frames per second[18] of video information, a time-lapse record may capture only a fraction as many frames. The strongest markets for the time-lapse machine are retail, industrial, and long-term surveillance. Time-lapse recorders are being replaced with newer digital technology.
- **Digital video recorders (DVR) or network digital recorders (NVR)** capture digital video signals, not analog (unless the analog signal is first converted to digital format and compressed). These recorders store video data on a disk, such as disk arrays, compact disk (CD), digital video disk (DVD), or other medium. Most DVRs/NVRs compress the video image, using a compression device or program known as a codec, because video data requires a large amount of storage space. Most DVRs/NVRs can be programmed to record a different number of images per second from each camera input. They should record 15 or more images per second when screening personnel at a vehicle entrance where a high-level image recording is required. However, screening pedestrians at an elevator lobby requires only two to three images per second. The DVR/NVR can also be programmed to record prior to an alarm stimulus at higher rates and for a specified duration after the alarm clears.
- **Storage array networks (SANs)** are cost effective non-proprietary means of archiving recorded video images that are becoming the standard storage configuration for large-scale video systems. SANs attach multiple remote storage devices (disk arrays) to a server in a manner that makes them appear and act as local devices. A SAN is quicker and more efficient to use than a remote storage device. Even though the storage array and the server may be physically separated, the server treats the storage array as a local onboard device. SANs are commonly deployed in a redundant array of independent disks (RAID) configuration. RAID configuration data is replicated and distributed among multiple hard disks, but to users the RAID appears as a single disk. RAID configurations range from simply replicating data to replicating data and providing fault tolerance.

18 Frame rated used by the National Television System Committee, the analog television system used in the United States.

5.5.4 Intercommunication Systems

Security communications systems facilitate rapid information gathering, decisionmaking, and response. Two types of communications systems are used in a security system: devices for the guards to communicate with each other and devices for the guards to communicate with the site users.

- **Two-way radio systems** facilitate constant communication among guard personnel and the security control center. These systems are perhaps the best method of communication for many reasons, including ease of use and broadcast functionality across multiple users or radio frequencies. Two-way radio systems can comprise an assembly of handheld radios with no master station or may be equipped with a master station at the security control center. Two-way radio systems can be integrated via communications software with other communication systems to create a consolidated communications system that can integrate radios, telephone, pagers, and intercoms into a single communications platform. Radio systems require careful planning and testing, including repeater locations to provide consistent coverage.

Security communications systems facilitate rapid information gathering, decisionmaking, and response.

- **Direct ring-down intercoms** are standard telephones that ring to a specific number when the receiver is lifted or the call button is pressed (hands-free version). These are commonly used in guard posts for direct communication with the security control center or other guard posts. The direct ring-down intercom is the best method of communicating with remote sites with limited two-way radio capability. They are commonly used for back-up communication should radio communication fail. To enhance functionality during emergencies, direct ring-down intercoms are often separate from the telephone system (not tied into the private branch exchange [PBX]).
- **Standard telephone landlines** normally run through PBX systems that are commonly switched to emergency power sources to operate when primary power is lost. Voice over Internet Protocol (VoIP) phone systems have been introduced in the last few years. VoIP systems run on converged IT networks to streamline system infrastructure and overall costs. A dual redundant ring configuration is recommended for the VoIP systems network; each network node supporting the VoIP should be powered by an uninterrupted power source.

- **Wireless phones** are becoming common communication devices for roving patrols and guard posts where mobile communication is critical. During a widespread emergency the volume of traffic can quickly overwhelm wireless phone systems causing them to fail, as happened in both New York City and Washington, DC, on 9/11. As a result of these limitations, wireless phones should not be relied upon as part of emergency communication systems.
- **Duress alarms/panic buttons** are devices used to alert security personnel of an emergency situation or that an attack is taking place. These are typically located in sensitive areas or where the level of interaction with the public is high. They are normally hardwired to the intrusion detection system. They can be wireless; however, wireless devices are not preferred, because the exact location of the incident it not known to the guard force.
- **Intercoms** are typically standalone systems that allow the guard force in the SOC to communicate with visitors or site users. Most intercoms are analog systems; however, new technologies allow them to operate by VoIP. Intercoms are often located with electronic entry control devices and have video cameras covering them.
- **Emergency call boxes** are made available to site users in case of an emergency. They have a direct connection to the security operation to alert the control center of an emergency. They are generally located in remote areas and have video cameras covering them to aid security personnel in assessing the emergency. Emergency call boxes typically are clearly marked with a light and/or siren to indicate when they are activated.
- **Mass notification systems** are becoming more commonly used to provide information in emergency and non-emergency situations to a large number of site users in a timely manner. These systems vary greatly in how the information is disseminated, ranging from integration with fire alarms, sirens, speakers or video signals, to text-messages or email.

Communications is a critical component supporting the response portion of the security system. A major vulnerability identified after 9/11 was the lack of communications redundancy and interoperability. An initiative by the Federal Communications Commission provided additional bandwidth for organizations requiring emergency communications and the provision enhanced interoperability among various emergency responders (police, hazmat, fire, etc.). Many high-risk organizations have developed improved communications interoperability with police, fire, hazmat, and other emergency response agencies in an effort to enhance their security programs. These organizations also learned that their internal systems required substantial improvements to support high-volume communications and emergency communications should their primary systems (radio or telephone) fail.

5.5.4.1 Security Operations Center and Security Management Systems

The SOC is the centralized location where trained personnel monitor and control the facility's security system. This is the location where all the electronic security subsystems are monitored and from where operations are directed in normal and emergency situations. The SOC must be protected as a facility asset, because it is the hub of communications and control during an attack.

The security management system coordinates, controls, and administers all electronic security subsystems. Many of the subsystems are capable of operating independently, but a truly integrated security system ties them all together to support and operate as one system.

The security management system coordinates the use of identification credentialing with intrusion detection, electronic entry control, and VASS to grant or deny access and record the event. It records all system and subsystem activity to enable re-creation of an event. A security management system is typically designed to accept and respond to information or input received from other building systems (e.g., fire alarm, building automation, elevator controls).

The Security Operations Center is the centralized location where trained personnel monitor and control the facility's security system.

Status information from the various intrusion detection sensors and entry control terminal devices must be collected from the field and transmitted to the alarm annunciation system in the SOC, where it is processed and annunciated and where response action is initiated. The alarm annunciation system should also interface with a VASS for assessment video of the alarm condition. Two types of alarm annunciation configurations are available. The simplest configuration, suitable for small installations, is the point-to-point configuration in which a separate transmission line is routed from the protected area to the SOC. The second, and more popular, is a digital multiplexed configuration that allows multiple protected areas to communicate with the SOC over a common data line. Figure 5-21 provides a block diagram of a typical multiplexed alarm annunciation system.

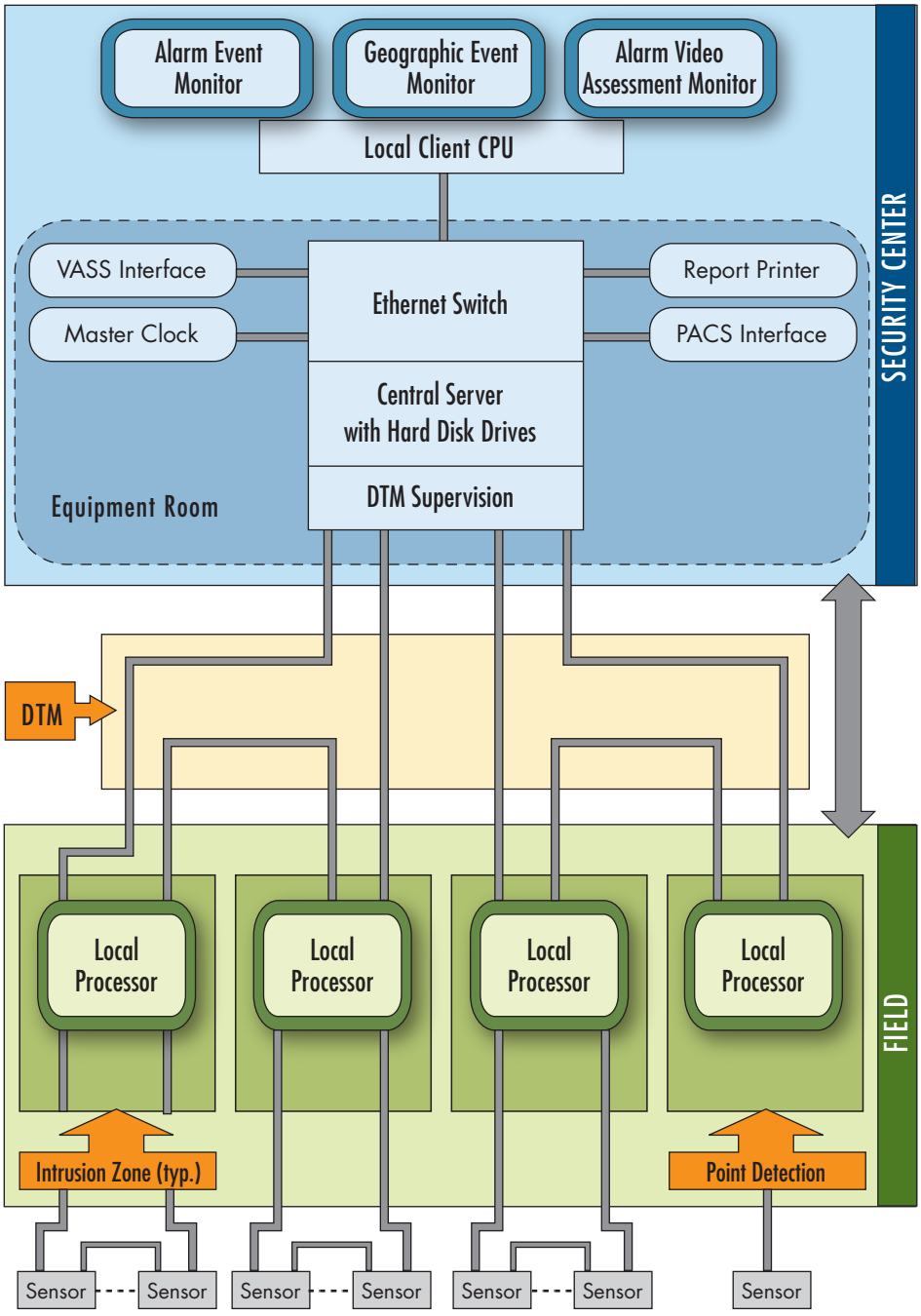


Figure 5-21: Alarm annunciation block diagram

SOURCE: U.S. FIELD MANUAL 3-19-30, DEPARTMENT OF THE ARMY

Figure 5-21 shows the central computer as the hub of the information flow. The central computer receives and displays alarm and device status information and sends operator-control commands to the electronic security system's local processors. It also interfaces with the VASS. For larger facilities, the management of the communications tasks may be delegated to a separate communication processor so that the central computer

is solely used to interpret the incoming information and update the control and display devices located at the security console (display, logging, control, and storage devices).

The central computer may consist of one or more servers and client systems for operations, supervision, and administration functions. A real-time clock is integral to the central computer to provide a time stamp for alarms and other events, and for time synchronization with the VASS and other systems. All system events must be properly time-correlated. For example, an exact time correlation for an electronic security system alarm event will be reported on the alarm monitor and the corresponding video recorded by the VASS processor. This system synchronization improves the alarm event assessment process.

The equipment installed at the SOC should consider the following two characteristics for effective security operations:

- **Data Storage:** Computer-based systems require large amounts of storage space for system software, application programs, data structures, and system event recording and retention. Therefore, a large amount of nonvolatile memory is required. The semiconductor memory provided with a central computer is designed for rapid storage and retrieval and possesses extremely fast access times. The most commonly used media for archival storage are DVD, magnetic tape, mirrored hard drives, or RAID configurations.
- **Operator Interface:** The operator interacts with the alarm annunciation system through devices that can be seen, heard, or touched and manipulated. Visual displays inform the operator of an alarm or equipment status. Audible devices alert an operator to an alarm or equipment failure. Push buttons and keyboards permit an operator to acknowledge and reset alarms, as well as change operational parameters.
  - **Visual displays** are used to inform the operator of the electronic security system status usually displayed with both text and graphic information in a variety of colors. Multiple alarms may also be displayed. Higher-priority alarms may be highlighted by blinking, using bold print or reverse video, or changing colors. To assist the operator in determining the correct response, alarm-specific instructions may be displayed adjacent to the alarm information.
  - **Audible alarm devices** are used in conjunction with the visual display to attract the operator's attention. The audible alarm may be produced by the ringing of a computer's wave file or by the generation of a steady or pulsating tone from an electronic device.

- **Logging devices** are used to log and record all alarm system activity (such as a change of access/secure status, an alarm event, an entry control transaction, or a trouble event). Logged information is important not only for security personnel investigating an event, but also for maintenance personnel checking the causes of false and nuisance alarms. Most alarm-annunciation systems are equipped with logging and alarm printers.

- **Report printers,** similar to those found in modern offices, are used by most electronic security systems to generate reports using information stored by the central computer.

Figure 5-22 is a schematic layout of a typical SOC with the associated electronic security equipment.

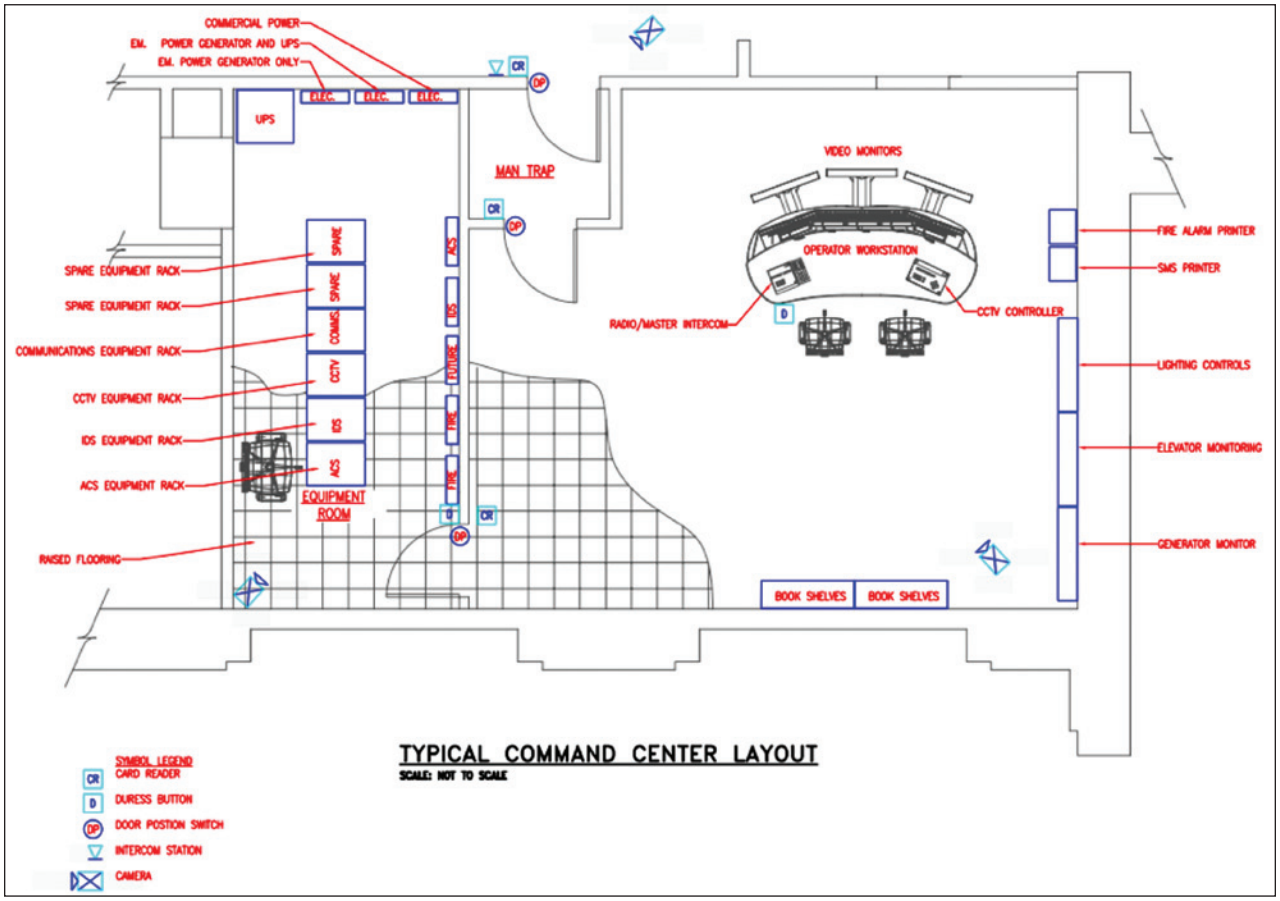


Figure 5-22: Security system control console
COURTESY OF SMITHSONIAN INSTITUTION

5.5.4.2 Data Transmission Media

A critical element in an integrated electronic security system is the data transmission from sensors, entry control devices, and video components to display and assessment equipment. A data transmission media link is a path for transmitting data between two or more components (such as a sensor and alarm reporting system, a card reader and controller, a VASS camera and monitor, or a transmitter and receiver). The data transmission media links connect remote electronic security system components to the SOC. An effective data transmission media link ensures rapid and reliable operation.

A number of different media are used in transmitting data between elements of an intrusion detection system, a physical access control system, and a VASS. These include wire lines, coaxial cable, fiber optic cable, and radio frequency (RF) transmission.

- **Wire lines** are insulated copper conductors used to transmit operating voltages or electrical signals. Wire line conductors used to transmit electrical signals are usually twisted; wire line conductors used to transmit power are usually untwisted. Wire line conductors can be grouped in jackets as multiple single conductors or in single or multiple pairs. The jacket protects the conductors inside from the environment and rigors of installation. The following are examples of wire lines:
  - **Category 5 cable (Cat 5)** is a high-signal integrity cable, comprised of four twisted pairs of 24 American wire gauge (AWG) copper conductors. Cat 5 cables are typically used for 100BASE-TX Megabit Ethernets.
  - **Category 6 cable (Cat 6)** is comprised of four twisted pairs of 24 AWG copper conductors. The signal integrity of Cat 6 is higher than that of Cat 5. Cat 6 specifications for crosstalk and system noise are more stringent. Cat 6 is used for 1000BASE-T, 1000BASE-TX, and 10BASE-T 10 Gigabit Ethernets.
- **Coaxial cable** consists of a center conductor surrounded by a shield. The shield protects against electromagnetic interference and is separated from the center by a dielectric.
- **Fiber optics** uses the wide bandwidth properties of light traveling through transparent fibers. Fiber optics is a reliable communication medium best suited for point-to-point, high-speed data transmission. Fiber optics is immune to RF electromagnetic interference and does

not produce electromagnetic radiation emission. The preferred data transmission medium for an electronic security system is fiber optic cables unless economic or technical factors justify using other types of media.

- **RF transmission,** via a RF-modulated signal, can be used as data transmission medium with the installation of radio receivers and transmitters. An RF transmission system does not require a direct physical link between the points of communication, and it is useful for communicating over barriers such as bodies of water and heavily forested terrain. A disadvantage is that the signal power received depends on many factors (including transmission power, antenna pattern, path length, physical obstructions, and climatic conditions). Also, RF transmission is susceptible to interception and jamming and its use must be coordinated to avoid interference with other existing or planned facility RF systems.

The two basic types of communication links are point-to-point and multiplex lines. A point-to-point link is characterized by a separate path for each pair of communication components. This approach is cost effective for several component pairs or when a number of scattered remote areas communicate with a single central location. The multiplex link, commonly referred to as a multidrop or multipoint link, is a path shared by a number of components. Depending on the number and location of components, this type of configuration can reduce the amount of cabling required. However, the cost reduction from reduced cabling is somewhat offset by the cost of equipment required to multiplex and demultiplex data.

The two basic types of communication links are point-to-point and multiplex lines.

A **point-to-point link** is characterized by a separate path for each pair of communication components.

A **multiplex link**, commonly referred to as a multidrop or multipoint link, is a path shared by a number of components.

Data links used to communicate the status of electronic security system devices or other sensitive information to the SOC must be protected from possible compromise. Attempts to defeat the security system may range from simple efforts to cut or short circuit the transmission line to more sophisticated undertakings, such as tapping and substituting bogus signals. Data links can be made more secure by physical protection, tamper protection, line supervision, and encryption.

A

Acronyms

ADA	Americans with Disabilities Act
APER	air-purifying escape respirator
ASCE	American Society of Civil Engineers
ASHRAE	American Society of Heating, Refrigeration, and Air Conditioning Engineers
ASTM	American Society for Testing and Materials, ASTM International
AWG	American wire gauge
BCA	benefit-cost analysis
Cat	Category (5 or 6 cable)
CBD	central business district
CBR	chemical, biological, and radiological
CBRN	chemical, biological, radiological, and nuclear
CCD	charge coupled device
CCTV	closed-circuit television
CDC	Centers for Disease Control and Prevention
cfm	cubic feet per minute

CIKR	critical infrastructure and key resources
CMOS	complementary metal oxide semiconductor
CMU	concrete masonry unit
CPTED	Crime Prevention Through Environmental Design
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOS	U.S. Department of State
DOT	U.S. Department of Transportation
DVR	digital video recorder
EAC	emergency action coordinator
ED	U.S. Department of Education
EIFS	exterior insulation and finishing system
EISA	Energy Independence and Security Act of 2007
ESP	electrostatic precipitator
ETFE	ethylene tetrafluoroethylene
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FRF	fragment retention film
GIS	geographic information system
GSA	General Services Administration
HAZL	Window Fragment Hazard Level Analysis
hazmat	hazardous material(s)
HEGA	high-efficiency gas adsorber
HEPA	high-efficiency particulate air
HHS	U.S. Department of Health and Human Services
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSPD	Homeland Security Presidential Directive
HVAC	heating, ventilation, and air conditioning
ICC	International Code Council

ID	identification
IDD	Infrastructure Protection and Disaster Management Division
IED	improvised explosive device
inH2O	inches of water gauge
IP	Internet protocol
IRVS	integrated rapid visual screening
ISAC	Information Sharing and Analysis Center
ISC	Interagency Security Committee
IT	information technology
LCC	life-cycle cost
LEPC	Local Emergency Planning Committee
µm	micron
MEP	mechanical, electrical, and plumbing
MERV	minimum-efficiency reporting value
MMD	mass-median-diameter
mm Hg	millimeters of mercury
mph	miles per hour
NCTC	National Counterterrorism Center
NFPA	National Fire Protection Association
NIAC	National Infrastructure Advisory Council
NIBS	National Institute of Building Sciences
NIOSH	National Institute for Occupational Safety and Health
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NVR	network digital recorder
PBD	performance-based design
PBX	private branch exchange
ppm	parts per million
psi	pounds per square inch
PVB	polyvinyl butyral

PTZ	pan-tilt-zoom
RAID	redundant array of independent disks
RF	radio frequency
SAN	storage array network
SCADA	Supervisory Control and Data Acquisition
SDOF	single-degree-of-freedom
SERC	State Emergency Response Commission
SOC	security operations center
SSA	sector-specific agency
S&T	DHS Science and Technology Directorate
TIC	toxic industrial chemical
TNT	trinitrotoluene
TTG	thermally tempered glass
UFC	Unified Facilities Criteria
URM	unreinforced masonry
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
UV	ultraviolet
UVGI	ultraviolet germicidal irradiation
VA	U.S. Department of Veterans Affairs
VASS	video assessment and surveillance system(s)
VBIED	vehicle-borne improvised explosive device
VoIP	Voice over Internet Protocol
WINGARD	Window Glazing Analysis Response and Design
WINLAC	Window Lite Analysis Code
WTC	World Trade Center

B

Glossary

This appendix contains some terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

A

Access control. Any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.

Access control point. A station at an entrance to a building or a portion of a building where identification is checked and people and hand-carried items are searched.

Access controls. Procedures and controls that limit or detect access to minimum essential infrastructure resource elements (e.g., people, technology, applications, data, facilities), thereby protecting these resources against loss of integrity, confidentiality, accountability, and/or availability.

Access control system. Also referred to as an electronic entry control systems; an electronic system that controls entry and egress from a building or area.

Access control system elements. Detection measures used to control vehicle or personnel entry into a protected area. Access control system elements include locks, electronic entry control systems, and guards.

Access group. A software configuration of an access control system that groups together access points or authorized users for easier arrangement and maintenance of the system.

Access road. Any roadway such as a maintenance, delivery, service, emergency, or other special limited use road that is necessary for the operation of a building or structure.

Accountability. The explicit assignment of responsibilities for oversight of areas of control to executives, managers, staff, owners, providers, and users of minimum essential infrastructure resource elements.

Active vehicle barrier. An impediment placed at an access control point that may be manually or automatically deployed in response to detection of a threat.

Aerosol. Fine liquid or solid particles suspended in a gas (e.g., fog, smoke).

Aggressor. Any person seeking to compromise a function or structure.

Airborne contamination. Chemical or biological agents introduced into and fouling the source of supply of breathing or conditioning air.

Airlock. A building entry configuration with which airflow from the outside can be prevented from entering a toxic-free area. An airlock uses two doors, only one of which can be opened at a time, and a blower system to maintain positive air pressures and purge contaminated air from the airlock before the second door is opened.

Air-water heating, ventilation, and air-conditioning (HVAC) systems. Combinations of air and water systems such as radiant heating supplemented with single-zone interior air supply for ventilation; hydronic systems at the periphery of a building to offset skin transmission losses only, combined with the use of an air system for space cooling and ventilation loads.

Alarm assessment. Verification and evaluation of an alarm alert through the use of closed-circuit television (CCTV) or human observation. Systems used for alarm assessment are designed to respond rapidly, automatically, and predictably to the receipt of alarms at the security center.

Alarm priority. A hierarchy of alarms by order of importance. This is often used in larger systems to give priority to alarms with greater importance.

Annunciation. A visual, audible, or other indication by a security system of a condition.

Antiterrorism. Defensive measures used to reduce the vulnerability of individuals, forces, and property to terrorist acts.

Area lighting. Lighting that illuminates a large exterior area.

Assessment. The evaluation and interpretation of measurements and other information to provide a basis for decisionmaking.

Assessment system elements. Detection measures used to assist guards in visual verification of intrusion detection system alarms and access control system functions and to assist in visual detection by guards. Assessment system elements include CCTV and protective lighting.

Asset. A resource of value requiring protection. An asset can be tangible (e.g., people, buildings, facilities, equipment, activities, operations, information) or intangible (e.g., processes, a company's information and reputation).

Asset protection. Security program designed to protect personnel, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combating terrorism, physical security, operations security, and personal protective services, and supported by intelligence, counterintelligence, and other security programs.

Asset value. The degree of debilitating impact that would be caused by the incapacity or destruction of an asset.

Attack. A hostile action resulting in the destruction, injury, or death to the civilian population, or damage or destruction to public and private property.

Audible alarm device. An alarm device that produces an audible announcement (e.g., bell, horn, siren) of an alarm condition.

B

Balanced magnetic switch. A door position switch using a reed switch held in a balanced or center position by interacting magnetic fields when not in alarm condition.

Ballistics attack. An attack in which small arms (e.g., pistols, submachine guns, shotguns, rifles) are fired from a distance and rely on the flight of the projectile to damage the target.

Barcode. A black bar printed on white paper or tape that can be easily read with an optical scanner.

Benefit cost analysis (BCA). Comparing the costs of a given protection solution to its perceived benefits.

Biological agents. Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

Biometric reader. A device that gathers and analyzes biometric features.

Biometrics. The use of physical characteristics of the human body as a unique identification method.

Blast curtains. Heavy curtains made of blast-resistant materials that could protect the occupants of a room from flying debris.

Blast-resistant glazing. Window opening glazing that is resistant to blast effects because of the interrelated function of the frame and glazing material properties frequently dependent upon tempered glass, polycarbonate, or laminated glazing.

Blast vulnerability envelope. The geographical area in which an explosive device will cause damage to assets.

Bollard. A vehicle barrier consisting of a cylinder, usually made of steel and sometimes filled with concrete, placed on end in the ground and spaced about 3 feet apart to prevent vehicles from passing, but allowing entrance of pedestrians and bicycles.

Boundary penetration sensor. An interior intrusion detection sensor that detects attempts by individuals to penetrate or enter a building.

Building hardening. Enhanced construction that reduces vulnerability to external blast and ballistic attacks.

Building separation. The distance between closest points on the exterior walls of adjacent buildings or structures.

C

Cable barrier. Cable or wire rope anchored to and suspended off the ground or attached to chain-link fence to act as a barrier to moving vehicles.

Capacitance sensor. A device that detects an intruder approaching or touching a metal object by sensing a change in capacitance between the object and the ground.

Card reader. A device that gathers or reads information when a card is presented as an identification method.

Chemical agent. A chemical substance that is intended to kill, seriously injure, or incapacitate people through physiological effects. Generally separated by severity of effect (e.g., lethal, blister, incapacitating).

Chimney effect. Air movement in a building between floors caused by differential air temperature (differences in density) between the air inside and outside the building. It occurs in vertical shafts, such as elevators, stairwells, and conduit/wiring/piping chases. Hotter air inside the building will rise and be replaced by infiltration with colder outside air through the lower portions of the building. Conversely, reversing the temperature will reverse the flow (down the chimney). Also known as stack effect.

Clear zone. An area that is clear of visual obstructions and landscape materials that could conceal a threat or perpetrator.

Closed-circuit television (CCTV). An electronic system of cameras, control equipment, recorders, and related apparatus used for surveillance or alarm assessment.

Collateral damage. Injury or damage to assets that are not the primary target of an attack.

Community. A political entity that has the authority to adopt and enforce laws and ordinances for the area under its jurisdiction. In most cases, the community is an incorporated town, city, township, village, or unincorporated area of a county; however, each State defines its own political subdivisions and forms of government.

Components and cladding. Elements of the building envelope that do not qualify as part of the main wind-force resisting system.

Confidentiality. The protection of sensitive information against unauthorized disclosure and sensitive facilities from physical, technical, or electronic penetration or exploitation.

Consequence management. Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. State and local governments exercise the primary authority to respond to the consequences of terrorism.

Contamination. The undesirable deposition of a chemical, biological, or radiological (CBR) material on the surface of structures, areas, objects, or people.

Continuity of services and operations. Controls to ensure that, when unexpected events occur, departmental/agency minimum essential infrastructure services and operations, including computer operations, continue without interruption or are promptly resumed, and that critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.

Control center. A centrally located room or facility staffed by personnel charged with the oversight of specific situations and/or equipment.

Controlled area. An area into which access is controlled or limited. The portion of a restricted area usually near or surrounding a limited or exclusion area. Correlates with exclusion zone.

Controlled lighting. Illumination of specific areas or sections.

Controlled perimeter. A physical boundary at which vehicle and personnel access is controlled at the perimeter of a site. Access control at a

controlled perimeter should demonstrate the capability to search individuals and vehicles.

Conventional construction. Building construction that is not specifically designed to resist weapons, explosives, or CBR effects. Conventional construction is designed only to resist common loadings and environmental effects such as wind, seismic, and snow loads.

Coordinate. To advance systematically an exchange of information among principals who have or may have a need to know certain information in order to carry out their roles in a response.

Counterintelligence. Information gathered and activities conducted to protect against: espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons; or international terrorist activities, excluding personnel, physical, document, and communications security programs.

Counterterrorism. Offensive measures taken to prevent, deter, and respond to terrorism.

Covert entry. Attempts to enter a facility by using false credentials or stealth.

Crash bar. A mechanical egress device located on the interior side of a door that unlocks the door when pressure is applied in the direction of egress.

Crime Prevention Through Environmental Design (CPTED). A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. CPTED usually involves the use of three principles: natural surveillance (by placing physical features, activities, and people to maximize visibility); natural access control (through the judicial placement of entrances, exits, fencing, landscaping, and lighting); and territorial reinforcement (using buildings, fences, pavement, signs, and landscaping to express ownership).

Crisis management. The measures taken to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism.

Critical assets. Those assets essential to the minimum operations of the organization, and to ensure the health and safety of the general public.

Critical infrastructure. Primary infrastructure systems (e.g., utilities, telecommunications, transportation) whose incapacity would have a debilitating impact on the organization's ability to function.

Critical infrastructure and key resources (CIKR). Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health, or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction. Key resources are publicly or privately controlled resources essential to the minimal operations of the economy and government,

D

Data transmission equipment. A path for transmitting data between two or more components (e.g., a sensor and alarm reporting system, a card reader and controller, a CCTV camera and monitor, a transmitter and receiver).

Decontamination. The reduction or removal of a CBR material from the surface of a structure, area, object, or person.

Defensive layer. Building design or exterior perimeter barriers intended to delay attempted forced entry.

Defensive measures. Protective measures that delay or prevent attack on an asset or that shield the asset from weapons, explosives, and CBR effects. Defensive measures include site work and building design.

Delay rating. A measure of the effectiveness of penetration protection of a defense layer.

Design basis threat. The threat (e.g., tactics and associated weapons, tools, explosives) against which assets within a building must be protected and upon which the security engineering design of the building is based.

Design constraint. Anything that restricts the design options for a protective system or that creates additional problems for which the design must compensate.

Design opportunity. Anything that enhances protection, reduces requirements for protective measures, or solves a design problem.

Design team. A group of individuals from various engineering and architectural disciplines responsible for the protective system design.

Detection layer. A ring of intrusion detection sensors located on or adjacent to a defensive layer or between two defensive layers.

Detection measures. Protective measures that detect intruders, weapons, or explosives; assist in assessing the validity of detection; control access to protected areas; and communicate the appropriate information to the response force. Detection measures include detection systems, assessment systems, and access control system elements.

Detection system elements. Detection measures that detect the presence of intruders, weapons, or explosives. Detection system elements include intrusion detection systems, weapons and explosives detectors, and guards.

Disaster. An occurrence of a natural catastrophe, technological accident, or human-caused event that has resulted in severe property damage, deaths, and/or multiple injuries.

Domestic terrorism. The unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.

Door position switch. A switch that changes state based on whether or not a door is closed. Typically, a switch mounted in a frame that is actuated by a magnet in a door.

Door strike, electronic. An electromechanical lock that releases a door plunger to unlock the door. Typically, an electronic door strike is mounted in place of or near a normal door strike plate.

Dose rate (radiation). A general term indicating the quantity (total or accumulated) of ionizing radiation or energy absorbed by a person or animal, per unit of time.

Dosimeter. An instrument for measuring and registering total accumulated exposure to ionizing radiation.

Dual technology sensor. A sensor that combines two different technologies in one unit.

Duress alarm devices. Also known as panic buttons, these devices are designated specifically to initiate a panic alarm.

E

Effective standoff distance. A standoff distance at which the required level of protection can be shown to be achieved through analysis or can be achieved through building hardening or other mitigating construction or retrofit.

Electromagnetic pulse. A sharp pulse of energy radiated instantaneously by a nuclear detonation that may affect or damage electronic components and equipment. An electromagnetic pulse can also be generated in lesser intensity by non-nuclear means in specific frequency ranges to perform the same disruptive function.

Electronic emanations. Electromagnetic emissions from computers, communications, electronics, wiring, and related equipment.

Electronic-emanations eavesdropping. Use of electronic-emanation surveillance equipment from outside a facility or its restricted area to monitor electronic emanations from computers, communications, and related equipment.

Electronic entry control systems. Electronic devices that automatically verify authorization for a person to enter or exit a controlled area.

Electronic security system. An integrated system that encompasses interior and exterior sensors, CCTV systems for assessment of alarm conditions, electronic entry control systems, data transmission media, and alarm reporting systems for monitoring, control, and display of various alarm and system information.

Emergency. Any natural or human-caused situation that results in or may result in substantial injury or harm to the population or substantial damage to or loss of property.

Emergency action coordinator (EAC). Appointed individual with the responsibility for preparations, training, and decisionmaking relative to protective actions.

Emergency alert system. A communications system of broadcast stations and interconnecting facilities authorized by the Federal Communications Commission. The system provides the President and other Federal, State, and local officials the means to broadcast emergency information to the public before, during, and after disasters.

Emergency environmental health services. Services required to correct or improve damaging environmental health effects on humans, including inspection for food contamination, inspection for water contamination, and vector control; providing for sewage and solid waste inspection and disposal; cleanup and disposal of hazardous materials; and sanitation inspection for emergency shelter facilities.

Emergency medical services. Services including personnel, facilities, and equipment required to ensure proper medical care for the sick and injured from the time of injury to the time of final disposition, including medical disposition within a hospital, temporary medical facility, or special care facility; release from the site; or declared dead. Further, emergency medical services specifically include those services immediately required to ensure proper medical care and specialized treatment for patients in a hospital and coordination of related hospital services.

Emergency operations center. The protected site from which State and local civil government officials coordinate, monitor, and direct emergency response activities during an emergency.

Emergency operations plan. A document that describes how people and property will be protected in disaster and disaster threat situations; details who is responsible for carrying out specific actions; identifies the personnel, equipment, facilities, supplies, and other resources available for use in the disaster; and outlines how all actions will be coordinated.

Emergency planning zones. Areas around a facility for which planning is needed to ensure prompt and effective actions are taken to protect the health and safety of the public if an accident or disaster occurs.

Emergency public information. Information that is disseminated primarily in anticipation of an emergency or at the actual time of an emergency and, in addition to providing information, frequently directs actions, instructs, and transmits direct orders.

Entity-wide security. Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.

Entry control point. A continuously or intermittently manned station at which entry to sensitive or restricted areas is controlled.

Entry control stations. Entry control stations should be provided at main perimeter entrances where security personnel are present. Entry control

stations should be located as close as practical to the perimeter entrance to permit personnel inside the station to maintain constant surveillance over the entrance and its approaches.

Equipment closet. A room where field control equipment such as data gathering panels and power supplies are typically located.

Evacuation. Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.

Evacuation, mandatory or directed. This is a warning to persons within the designated area that an imminent threat to life and property exists and individuals MU.S.T evacuate in accordance with the instructions of local officials.

Evacuation, spontaneous. Residents or citizens in the threatened areas observe an emergency event or receive unofficial word of an actual or perceived threat and, without receiving instructions to do so, elect to evacuate the area. Their movement, means, and direction of travel are unorganized and unsupervised.

Evacuation, voluntary. This is a warning to persons within a designated area that a threat to life and property exists or is likely to exist in the immediate future. Individuals issued this type of warning or order are NOT required to evacuate; however, it would be to their advantage to do so.

Evacuees. All persons removed or moving from areas threatened or struck by a disaster.

Exclusion area. A restricted area containing a security interest. Uncontrolled movement permits direct access to the item. See controlled area and limited area.

Exclusion zone. An area around an asset that has controlled entry with highly restrictive access. See controlled area.

F

Facial recognition. A biometric technology that is based on features of the human face.

Federal Response Plan. A Federal plan that establishes a process and structure for the systematic, coordinated, and effective delivery of Federal

assistance to address the consequences of any major disaster or emergency.

Fence protection. An intrusion detection technology that detects a person crossing a fence by various methods such as climbing, crawling, cutting, etc.

Fence sensor. An exterior intrusion detection sensor that detects aggressors as they attempt to climb over, cut through, or otherwise disturb a fence.

Fiber optics. A method of data transfer by passing bursts of light through a strand of glass or clear plastic.

Field of view. The visible area in a video picture.

First responder. Local police, fire, and emergency medical personnel who first arrive on the scene of an incident and take action to save lives, protect property, and meet basic human needs.

Flash flood. Follows a situation in which rainfall is so intense and severe and runoff so rapid that it precludes recording and relating it to stream stages and other information in time to forecast a flood condition.

Flood. A general and temporary condition of partial or complete inundation of normally dry land areas from overflow of inland or tidal waters, unusual or rapid accumulation or runoff of surface waters, or mudslides/mudflows caused by accumulation of water.

Forced entry. Entry to a denied area achieved through force to create an opening in fence, walls, doors, etc., or to overpower guards.

Fragment-retention film (FRF). A thin, optically clear film applied to glass to minimize the spread of glass fragments when the glass is shattered.

Frame rate. In digital video, a measurement of the rate of change in a series of pictures, often measured in frames per second.

Frangible construction. Building components that are designed to fail to vent blast pressures from an enclosure in a controlled manner and direction.

G

Glare security lighting. Illumination projected from a secure perimeter into the surrounding area, making it possible to see potential intruders at a considerable distance while making it difficult to observe activities within the secure perimeter.

Glass-break detector. An intrusion detection sensor that is designed to detect breaking glass either through vibration or acoustics.

Glazing. A material installed in a sash, ventilator, or panes (e.g., glass, plastic, thin granite installed in a curtain wall).

Grid wire sensor. An intrusion detection sensor that uses a grid of wires to cover a wall or fence. An alarm is sounded if the wires are cut.

H

Hand geometry. A biometric technology that is based on characteristics of the human hand.

Hazard. A source of potential danger or adverse condition.

Hazard mitigation. Any action taken to reduce or eliminate the long-term risk to human life and property from hazards. The term is sometimes used in a stricter sense to mean cost-effective measures to reduce the potential for damage to a facility or facilities from a disaster event.

Hazardous material (hazmat). Any substance or material that, when involved in an accident and released in sufficient quantities, poses a risk to people's health, safety, and/or property. These substances and materials include explosives, radioactive materials, flammable liquids or solids, combustible liquids or solids, poisons, oxidizers, toxins, and corrosive materials.

High-hazard areas. Geographic locations that, for planning purposes, have been determined through historical experience and vulnerability analysis to be likely to experience the effects of a specific hazard (e.g., hurricane, earthquake, hazardous materials accident), resulting in vast property damage and loss of life.

High-risk target. Any material resource or facility that, because of mission sensitivity, ease of access, isolation, and symbolic value, may be an especially attractive or accessible terrorist target.

Human-caused hazard. Human-caused hazards are technological hazards and terrorism. They are distinct from natural hazards primarily in that they originate from human activity. Within the military services, the term threat is typically used for human-caused hazard. See definitions of technological hazards and terrorism for further information.

Hurricane. A tropical cyclone, formed in the atmosphere over warm ocean areas, in which wind speeds reach 74 miles per hour or more and blow in a large spiral around a relatively calm center or "eye." Circulation is counter-clockwise in the Northern Hemisphere and clockwise in the Southern Hemisphere.

I

Impact analysis. A management level analysis that identifies the impacts of losing the entity's resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide the entity with reliable data upon which to base decisions on hazard mitigation and continuity planning.

Improvised explosive device (IED). A device placed or fabricated in an improvised manner incorporating destuctive, lethal, noxious, pyrotechnic, or incendiary chemicals and designed to destroy, incapacitate, harass, or distract. It may incorporate conventional military construction (e.g., artillery round), but is normally devised from nonmilitary components.

InfraGard. A partnership between the Federal Bureau of Investigation (FBI) and the private sector. InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

Incident Command System (ICS). A standardized organizational structure used to command, control, and coordinate the use of resources and personnel that have responded to the scene of an emergency. The concepts and principles for ICS include common terminology, modular organization, integrated communication, unified command structure, consolidated action plan, manageable span of control, designated incident facilities, and comprehensive resource management.

Insider compromise. A person authorized access to a facility (an insider) compromises assets by taking advantage of that accessibility.

Insider threat. An aggressor who is an employee of a business, institution, or agency seeking to compromise a function or the building of the employer.

Intercom door/gate station. Part of an intercom system where communication is typically initiated, usually located at a door or gate.

Intercom master station. Part of an intercom system that monitors one or more intercom door/gate stations; typically, where initial communication is received.

Intercom switcher. Part of an intercom system that controls the flow of communications between various stations.

Intercom system. An electronic system that allows simplex, half-duplex, or full-duplex audio communications.

Intergrated rapid visual screening (IRVS). Quick and simple procedure to assess the risk and resiliency of a building, mass transit station, or tunnel in an all-hazard (manmade and natural) context.

International terrorism. Violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Intrusion detection sensor. A device that initiates alarm signals by sensing the stimulus, change, or condition for which it was designed.

Intrusion detection system. The combination of components, including sensors, control units, transmission lines, and monitor units, integrated to operate in a specified manner.

Isolated fenced perimeters. Fenced perimeters with 100 feet or more of space outside the fence that is clear of obstruction, making approach obvious.

J

Jersey barrier. A protective concrete barrier initially and still used as a highway divider that now also functions as an expedient method for traffic speed control at entrance gates and to keep vehicles away from buildings.

Jurisdiction. Typically counties and cities within a State, but States may elect to define them differently in order to facilitate their assessment process.

L

Laminated glass. A flat lite of uniform thickness consisting of two monolithic glass plies bonded together with an interlayer material as defined in Specification C1172. Many different interlayer materials are used in laminated glass.

Landscaping. The use of plantings (shrubs and trees), with or without landforms and/or large boulders, to act as a perimeter barrier against defined threats.

Laser card. A card technology that uses a laser reflected off of a card for uniquely identifying the card.

Layers of protection. A traditional approach in security engineering using concentric circles extending out from an area to be protected as demarcation points for different security strategies.

Level of protection. The degree to which an asset is protected against injury or damage from an attack.

Life cycle costs (LCC). The combined sum of all relevant costs associated with owning and operating a constructed facility over a specified period of time, usually the estimated life span of a building.

Limited area. A restricted area within close proximity of a security interest. Uncontrolled movement may permit access to the item. Escorts and other internal restrictions may prevent access to the item. See controlled area and exclusion area.

Line of sight. Direct observation between two points with the naked eye or hand-held optics.

Line-of-sight sensor. A pair of devices used as an intrusion detection sensor that monitor any movement through the field between the sensors.

Line supervision. A data integrity strategy that monitors the communications link for connectivity and tampering. In intrusion detection system sensors, line supervision is often referred to as two-State, three-State, or four-State in respect to the number of conditions monitored. The frequency of sampling the link also plays a big part in the supervision of the line.

Local government. Any county, city, village, town, district, or political subdivision of any State, and Indian tribe or authorized tribal organization, or Alaska Native village or organization, including any rural community or unincorporated town or village or any other public entity.

M

Magnetic lock. An electromagnetic lock that unlocks a door when power is removed.

Magnetic stripe. A card technology that uses a magnetic stripe on the card to encode data used for unique identification of the card.

Mail-bomb delivery. Bombs or incendiary devices delivered to the target in letters or packages.

Man-trap. An access control strategy that uses a pair of interlocking doors to prevent tailgating. Only one door can be unlocked at a time.

Mass notification. Capability to provide real-time information to all building occupants or personnel in the immediate vicinity of a building during emergency situations.

Microwave motion sensor. An intrusion detection sensor that uses microwave energy to sense movement within the sensor's field of view. These sensors work similar to radar by using the Doppler effect to measure a shift in frequency.

Minimum-efficiency reporting value (MERV). commonly known as MERV rating is a measurement scale to rate the effectiveness of air filters. The MERV

rating is from 1 to 16. Higher MERV ratings correspond to a greater percentage of particles captured on each pass, with a MERV 16 filter capturing more than 95% of particles over the full range.Minimum essential infrastructure resource elements. The broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency, or organization to conduct its core mission(s).

Minimum measures. Protective measures that can be applied to all buildings regardless of the identified threat. These measures offer defense or detection opportunities for minimal cost, facilitate future upgrades, and may deter acts of aggression.

Mitigation. Those actions taken to reduce the exposure to and impact of an attack or disaster.

Motion detector. An intrusion detection sensor that changes state based on movement in the sensor's field of view.

Moving vehicle bomb. An explosive-laden car or truck driven into or near a building and detonated.

Mutual aid agreement. A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.

N

Natural hazard. Naturally-occurring events such as floods, earthquakes, tornadoes, tsunami, coastal storms, landslides, and wildfires that strike populated areas. A natural event is a hazard when it has the potential to harm people or property. The risks of natural hazards may be increased or decreased as a result of human activity; however, they are not inherently human-induced.

Natural protective barriers. Natural protective barriers are mountains and deserts, cliffs and ditches, water obstacles, or other terrain features that are difficult to traverse.

Non-exclusive zone. An area around an asset that has controlled entry, but shared or less restrictive access than an exclusive zone.

Non-persistent agent. An agent that, upon release, loses its ability to cause casualties after 10 to 15 minutes. It has a high evaporation rate, is lighter

than air, and will disperse rapidly. It is considered to be a short-term hazard; however, in small, unventilated areas, the agent will be more persistent.

Nuclear, biological, or chemical weapons. Also called weapons of mass destruction (WMD). Weapons that are characterized by their capability to produce mass casualties.

Nuclear detonation. An explosion resulting from fission and/or fusion reactions in nuclear material, such as that from a nuclear weapon.

O

Open systems architecture. A term borrowed from the IT industry to claim that systems are capable of interfacing with other systems from any vendor, which also uses open system architecture. The opposite would be a proprietary system.

Operator interface. The part of a security management system that provides that user interface to humans.

Organizational areas of control. The policies, procedures, practices, and organization structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

P

Pan-tilt-zoom (PTZ) camera. A camera that can move side to side, up and down, and zoom in or out.

Passive infrared motion sensor. A device that detects a change in the thermal energy pattern caused by a moving intruder and initiates an alarm when the change in energy satisfies the detector's alarm criteria.

Passive vehicle barrier. A vehicle barrier that is permanently deployed and does not require response to be effective.

Patch panel. A concentrated termination point that separates backbone cabling from devices cabling for easy maintenance and troubleshooting.

Performance-based design (PBD). The process used to achieve performance levels for specific attributes based on quantifiable benchmark metrics that can be verified.

Perimeter barrier. A fence, wall, vehicle barrier, landform, or line of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

Persistent agent. An agent that, upon release, retains its casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air; therefore, its vapor cloud tends to hug the ground. It is considered to be a long-term hazard. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

Physical security. The part of security concerned with measures/concepts designed to safeguard personnel; to prevent unauthorized access to equipment, installations, materiel, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Planter barrier. A passive vehicle barrier, usually constructed of concrete and filled with dirt (and flowers for aesthetics). Planters, along with bollards, are the usual street furniture used to keep vehicles away from existing buildings. Overall size and the depth of installation below grade determine the vehicle stopping capability of the individual planter.

Plume. Airborne material spreading from a particular source; the dispersal of particles, gases, vapors, and aerosols into the atmosphere.

Polycarbonate glazing. A plastic glazing material with enhanced resistance to ballistics or blast effects.

Predetonation screen. A fence that causes an anti-tank round to detonate or prevents it from arming before it reaches its target.

Preparedness. Establishing the plans, training, exercises, and resources necessary to enhance mitigation of and achieve readiness for response to, and recovery from all hazards, disasters, and emergencies, including WMD incidents.

Pressure mat. A mat that generates an alarm when pressure is applied to any part of the mat's surface, such as when someone steps on the mat. Pressure mats can be used to detect an intruder approaching a protected object, or they can be placed by doors and windows to detect entry.

Primary asset. An asset that is the ultimate target for compromise by an aggressor.

Primary gathering building. Inhabited buildings routinely occupied by 50 or more personnel. This designation applies to the entire portion of a building that meets the population density requirements for an inhabited building.

Probability of detection. A measure of an intrusion detection sensor's performance in detecting an intruder within its detection zone.

Probability of intercept. The probability that an act of aggression will be detected and that a response force will intercept the aggressor before the asset can be compromised.

Progressive collapse. A chain reaction failure of building members to an extent disproportionate to the original localized damage. Such damage may result in upper floors of a building collapsing onto lower floors.

Protective barriers. Define the physical limits of a site, activity, or area by restricting, channeling, or impeding access and forming a continuous obstacle around the object.

Protective measures. Elements of a protective system that protect an asset against a threat. Protective measures are divided into defensive and detection measures.

Protective system. An integration of all of the protective measures required to protect an asset against the range of threats applicable to the asset.

Proximity sensor. An intrusion detection sensor that changes state based on the close distance or contact of a human to the sensor. These sensors often measure the change in capacitance as a human body enters the measured field.

R

Radiation. High-energy particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay. Particles can be either charged alpha or beta particles or neutral neutron or gamma rays.

Radiation sickness. The symptoms characterizing the sickness known as radiation injury, resulting from excessive exposure of the whole body to ionizing radiation.

Radiological monitoring. The process of locating and measuring radiation by means of survey instruments that can detect and measure (as exposure rates) ionizing radiation.

Recovery. The long-term activities beyond the initial crisis period and emergency response phase of disaster operations that focus on returning all systems in the community to a normal status or to reconstitute these systems to a new condition that is less vulnerable.

Report printers. A separate, dedicated printer attached to the electronic security systems used for generating reports using information stored by the central computer.

Request-to-exit device. Passive infrared motion sensors or push buttons that are used to signal an electronic entry control system that egress is imminent or to unlock a door.

Resolution. The level to which video details can be determined in a CCTV scene.

Response. Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population.

Response force. The people who respond to an act of aggression. Depending on the nature of the threat, the response force could consist of guards, special reaction teams, military or civilian police, an explosives ordnance disposal team, or a fire department.

Response time. The length of time from the instant an attack is detected to the instant a security force arrives on site.

Restricted area. Any area with access controls that is subject to these special restrictions or controls for security reasons. See controlled area, limited area, exclusion area, and exclusion zone.

Retinal pattern. A biometric technology that is based on features of the human eye.

Radio Frequency (RF) data transmission. A communications link using RF to send or receive data.

Risk. The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it.

Rotating drum or rotating plate vehicle barrier. An active vehicle barrier used at vehicle entrances to controlled areas based on a drum or plate rotating into the path of the vehicle when signaled.

Routinely occupied. For the purposes of these standards, an established or predictable pattern of activity within a building that terrorists could recognize and exploit.

S

Sacrificial roof or wall. Roofs or walls that can be lost in a blast without damage to the primary asset.

Safe haven. Secure areas within the interior of the facility. A safe haven should be designed such that it requires more time to penetrate by aggressors than it takes for the response force to reach the protected area to rescue the occupants. It may be a haven from a physical attack or air-isolated haven from CBR contamination.

Supervisory control and data acquisition (SCADA). Utility and control systems for facilities such as computer systems that monitor and control industrial, infrastructure, or facility-based processes.

Scramble keypad. A keypad on which the numbers change pattern with each use to enhance security by preventing eavesdropping observation of the entered numbers.

Secondary asset. An asset that supports a primary asset and whose compromise would indirectly affect the operation of the primary asset.

Secondary hazard. A threat whose potential would be realized as the result of a triggering event that of itself would constitute an emergency (e.g., dam failure might be a secondary hazard associated with earthquakes).

Sector-specific agency (SSA). Sector-specific agency refers to federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors.

Secure/access mode. The state of an area monitored by an intrusion detection system in regards to how alarm conditions are reported.

Security analysis. The method of studying the nature of and the relationship between assets, threats, and vulnerabilities.

Security console. Specialized furniture, racking, and related apparatus used to house the security equipment required in a control center.

Security engineering. The process of identifying practical, risk managed short- and long-term solutions to reduce and/or mitigate dynamic manmade hazards by integrating multiple factors, including construction, equipment, manpower, and procedures.

Security engineering design process. The process through which assets requiring protection are identified, the threat to and vulnerability of those assets is determined, and a protective system is designed to protect the assets.

Security operations center (SOC). A centralized location within a building that deals with security issues, on a organizational and technical level. The SOC is where staff supervise the site using data processing technology equipped for access control monitoring, control of lighting, cameras, alarms, and vehicle barriers.

Segregation of duties. Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to minimum essential infrastructure resource elements.

Semi-isolated fenced perimeters. Fence lines where approach areas are clear of obstruction for 60 to 100 feet outside of the fence and where the general public or other personnel seldom have reason to be in the area.

Shielded wire. Wire with a conductive wrap used to mitigate electromagnetic emanations.

Situational crime prevention. A crime prevention strategy based on reducing the opportunities for crime by increasing the effort required to commit a crime, increasing the risks associated with committing the crime, and reducing the target appeal or vulnerability (whether property or person). This opportunity reduction is achieved by management and use policies such as procedures and training, as well as physical approaches such as alteration of the built environment.

Smart card. A newer card technology that allows data to be written, stored, and read on a card typically used for identification and/or access.

Specific threat. Known or postulated aggressor activity focused on targeting a particular asset.

Standoff distance. A distance maintained between a building or portion thereof and the potential location for an explosive detonation or other threat.

Standoff weapons. Weapons such as antitank weapons and mortars that are launched from a distance at a target.

Stationary vehicle bomb. An explosive-laden car or truck stopped or parked near a building.

Storm surge. A dome of sea water created by the strong winds and low barometric pressure in a hurricane that causes severe coastal flooding as the hurricane strikes land.

Strain sensitive cable. Strain sensitive cables are transducers that are uniformly sensitive along their entire length and generate an analog voltage when subjected to mechanical distortions or stress resulting from fence motion. They are typically attached to a chain-link fence about halfway between the bottom and top of the fence fabric with plastic ties.

Structural protective barriers. Manmade devices (e.g., fences, walls, floors, roofs, grills, bars, roadblocks, signs, other construction) used to restrict, channel, or impede access.

Superstructure. The supporting elements of a building above the foundation.

Supplies-bomb delivery. Bombs or incendiary devices concealed and delivered to supply or material handling points such as loading docks.

System events. Events that occur normally in the operation of a security management system. Examples include access control operations and changes of state in intrusion detection sensors.

System software. Controls that limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

T

Tactics. The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.

Tamper switch. Intrusion detection sensor that monitors an equipment enclosure for breach.

Tangle-foot wire. Barbed wire or tape suspended on short metal or wooden pickets outside a perimeter fence to create an obstacle to approach.

Taut wire sensor. An intrusion detection sensor using a column of uniformly spaced horizontal wires, securely anchored at each end and stretched taut. Each wire is attached to a sensor to indicate movement of the wire.

Technical assistance. The provisioning of direct assistance to States and local jurisdictions to improve capabilities for program development, planning, and operational performances related to responses to WMD terrorist incidents.

Technological hazards. Incidents that can arise from human activities such as manufacture, transportation, storage, and use of hazardous materials. For the sake of simplicity, technological emergencies are assumed to be accidental and their consequences are unintended.

Terrorism. The unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Thermally tempered glass (TTG). Glass that is heat-treated to have a higher tensile strength and resistance to blast pressures, although with a greater susceptibility to airborne debris.

Threat. Any indication, circumstance, or event with the potential to cause loss of, or damage to an asset.

Threat analysis. A continual process of compiling and examining all available information concerning potential threats and human-caused hazards. A common method to evaluate terrorist groups is to review the factors of existence, capability, intentions, history, and targeting.

TNT equivalent weight. The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.

Tornado. A local atmospheric storm, generally of short duration, formed by winds rotating at very high speeds, usually in a counter-clockwise direction. The vortex, up to several hundred yards wide, is visible to the observer as a whirlpool-like column of winds rotating about a hollow cavity or funnel. Winds may reach 300 miles per hour or higher.

Toxic-free area. An area within a facility in which the air supply is free of toxic chemical or biological agents.

Toxic industrial chemical (TIC). Manufactured for chemical industrial purposes. TICs are generally less toxic and less persistent than chemical warfare agents, and many are commonly stored or transported in bulk quantities.

Toxicity. A measure of the harmful effects produced by a given amount of a toxin on a living organism.

Tsunami. Sea waves produced by an undersea earthquake. Such sea waves can reach a height of 80 feet and can devastate coastal cities and low-lying coastal areas.

Twisted pair wire. Wire that uses pairs of wires twisted together to mitigate electromagnetic interference.

Two-person rule. A security strategy that requires two people to be present in or gain access to a secured area to prevent unobserved access by any individual.

U

Unobstructed space. Space around an inhabited building without obstruction large enough to conceal explosive devices 150 mm (6 inches) or greater in height.

Unshielded wire. Wire that does not have a conductive wrap.

V

Vault. A reinforced room for securing items.

Vertical rod. Typical door hardware often used with a crash bar to lock a door by inserting rods vertically from the door into the doorframe.

Vibration sensor. An intrusion detection sensor that changes state when vibration is present.

Video analytics (or intelligent video). The use of computer software in surveillance to automatically identify things of interest such as behavior, objects, or attitude, without an operator having to view the video.

Video assessment and surveillance system(s) (VASS). Digital monitoring and control systems to provide a rapid and cost-effective method for determining the source of the intrusion or other detection alarms

Video intercom system. An intercom system that also incorporates a small CCTV system for verification.

Video motion detection. Motion detection technology that looks for changes in the pixels of a video image.

Video multiplexer. A device used to connect multiple video signals to a single location for viewing and/or recording.

Visual displays. A display or monitor used to inform the operator visually of the status of the electronic security system.

Visual surveillance. The aggressor uses ocular and photographic devices (such as binoculars and cameras with telephoto lenses) to monitor facility or installation operations or to see assets.

Voice recognition. A biometric technology that is based on nuances of the human voice.

Volumetric motion sensor. An interior intrusion detection sensor that is designed to sense aggressor motion within a protected space.

Vulnerability. Any weakness that can be exploited by an aggressor or, in a nonterrorist threat environment, make an asset susceptible to hazard damage.

W

Warning. The alerting of emergency response personnel and the public to the threat of extraordinary danger and the related effects that specific hazards may cause.

Watch. Indication in a defined area that conditions are favorable for the specified type of severe weather (e.g., flash flood watch, severe thunderstorm watch, tornado watch, tropical storm watch).

Waterborne contamination. CBR agent introduced into and fouling a water supply.

Weapons-grade material. Nuclear material considered most suitable for a nuclear weapon. It usually connotes uranium enriched to above 90 percent uranium-235 or plutonium with greater than about 90 percent plutonium-239.

Weapon of mass destruction (WMD). Any device, material, or substance used in a manner, in a quantity or type, or under circumstances showing an intent to cause death or serious injury to persons, or significant damage to property. An explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Weigand protocol. A security industry standard data protocol for card readers.

Z

Zoom. The ability of a CCTV camera to close and focus or open and widen the field of view.

C

Chemical, Biolological, and Radiological Glossary

This appendix contains some CBR terms that do not actually appear in this manual. They have been included to present a comprehensive list that pertains to this series of publications.

Chemical Terms

A

Acetylcholinesterase. An enzyme that hydrolyzes the neurotransmitter acetylcholine. The action of this enzyme is inhibited by nerve agents.

Aerosol. Fine liquid or solid particles suspended in a gas (e.g., fog, smoke).

Atropine. A compound used as an antidote for nerve agents.

C

Casualty (toxic) agents. Agents that produce incapacitation, serious injury, or death, and can be used to incapacitate or kill victims. They are the blister, blood, choking, and nerve agents.

> **Blister agents.** Substances that cause blistering of the skin. Exposure is through liquid or vapor contact with any exposed tissue (eyes,

skin, lungs). Examples are distilled mustard (HD), nitrogen mustard (HN), lewisite (L), mustard/lewisite (HL), and phenodichloroarsine (PD).

Blood agents. Substances that injure a person by interfering with cell respiration (the exchange of oxygen and carbon dioxide between blood and tissues). Examples are arsine (SA), cyanogen chloride (CK), hydrogen chloride (HCl), and hydrogen cyanide (AC).

Choking/lung/pulmonary agents. Substances that cause physical injury to the lungs. Exposure is through inhalation. In extreme cases, membranes swell and lungs become filled with liquid. Death results from lack of oxygen; hence, the victim is "choked." Examples are chlorine (CL), diphosgene (DP), cyanide (KCN), nitrogen oxide (NO), perfluororisobutylene (PHIB), phosgene (CG), red phosphorous (RP), sulfur trioxide-chlorosulfonic acid (FS), Teflon and PHIB, titanium tetrachloride (FM), and zinc oxide (HC).

Nerve agents. Substances that interfere with the central nervous system. Exposure is primarily through contact with the liquid (skin and eyes) and secondarily through inhalation of the vapor. Three distinct symptoms associated with nerve agents are: pin-point pupils, an extreme headache, and severe tightness in the chest. See also G-series and V-series nerve agents.

Chemical agents. Substances that are intended for use in military operations to kill, seriously injure, or incapacitate people through their physiological effects. Excluded from consideration are riot control agents and smoke and flame materials. The agent may appear as a vapor, aerosol, or liquid; it can be either a casualty/toxic agent or an incapacitating agent.

Cutaneous. Pertaining to the skin.

D

Decontamination. The process of making any person, object, or area safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

G

G-series nerve agents. Chemical agents of moderate to high toxicity developed in the 1930s. Examples are tabun (GA), sarin (GB), soman (GD), phosphonofluoridic acid, ethyl-, 1-methylethyl ester (GE), and cyclohexyl sarin (GF).

Incapacitating agents. Agents that produce temporary physiological and/or mental effects via action on the central nervous system. Effects may persist for hours or days, but victims usually do not require medical treatment; however, such treatment speeds recovery.

> **Vomiting agents.** Agents that produce nausea and vomiting effects; can also cause coughing, sneezing, pain in the nose and throat, nasal discharge, and tears. Examples are adamsite (DM), diphenylchloroarsine (DA), and diphenylcyanoarsine (DC).
>
> **Tear (riot control) agents.** Agents that produce irritating or disabling effects that rapidly disappear within minutes after exposure ceases. Examples are bromobenzylcyanide (CA), chloroacetophenone (CN or commercially known as Mace), chloropicrin (PS), CNB (CN in benzene and carbon tetrachloride), CNC (CN in chloroform), CNS (CN and chloropicrin in chloroform, CR (dibenz-(b,f)-1,4-oxazepine, a tear gas), CS (tear gas), and Capsaicin (pepper spray).
>
> **Central nervous system depressants.** Compounds that have the predominant effect of depressing or blocking the activity of the central nervous system. The primary mental effects include the disruption of the ability to think, sedation, and elimination of motivation.
>
> **Central nervous system stimulants.** Compounds that have the predominant effect of flooding the brain with too much information. The primary mental effect is loss of concentration, causing indecisiveness and the inability to act in a sustained, purposeful manner.
>
> Examples of compounds that are both depressants and stimulants include agent 15 (suspected Iraqi BZ), BZ (3-quinulidinyle benzilate), canniboids, fentanyls, LSD (lysergic acid diethylamide), and phenothiazines.

Industrial agents. Chemicals developed or manufactured for use in industrial operations or research by industry, government, or academia. These chemicals are not primarily manufactured for the specific purpose of producing human casualties or rendering equipment, facilities, or areas dangerous for use by man. Hydrogen cyanide, cyanogen chloride, phosgene, chloropicrin, and many herbicides and pesticides are industrial chemicals that also can be chemical agents.

L

Liquid agents. Chemical agents that appear to be an oily film or droplets. The color ranges from clear to brownish amber.

N

Nonpersistent agents. Agents that, upon release, lose the ability to cause casualties after 10 to 15 minutes. They have a high evaporation rate and are lighter than air and will disperse rapidly. They are considered to be short-term hazards; however, in small unventilated areas, these agents will be more persistent.

O

Organophosphorous compound. A compound containing the elements phosphorus and carbon, whose physiological effects include inhibition of acetylcholinesterase. Many pesticides (malathione and parathion) and virtually all nerve agents are organophosphorous compounds.

P

Percutaneous agents. Agents that are able to be absorbed by the body through the skin.

Persistent agents. Agents that, upon release, retain their casualty-producing effects for an extended period of time, usually anywhere from 30 minutes to several days. A persistent agent usually has a low evaporation rate and its vapor is heavier than air. Therefore, its vapor cloud tends to hug the ground. They are considered to be long-term hazards. Although inhalation hazards are still a concern, extreme caution should be taken to avoid skin contact as well.

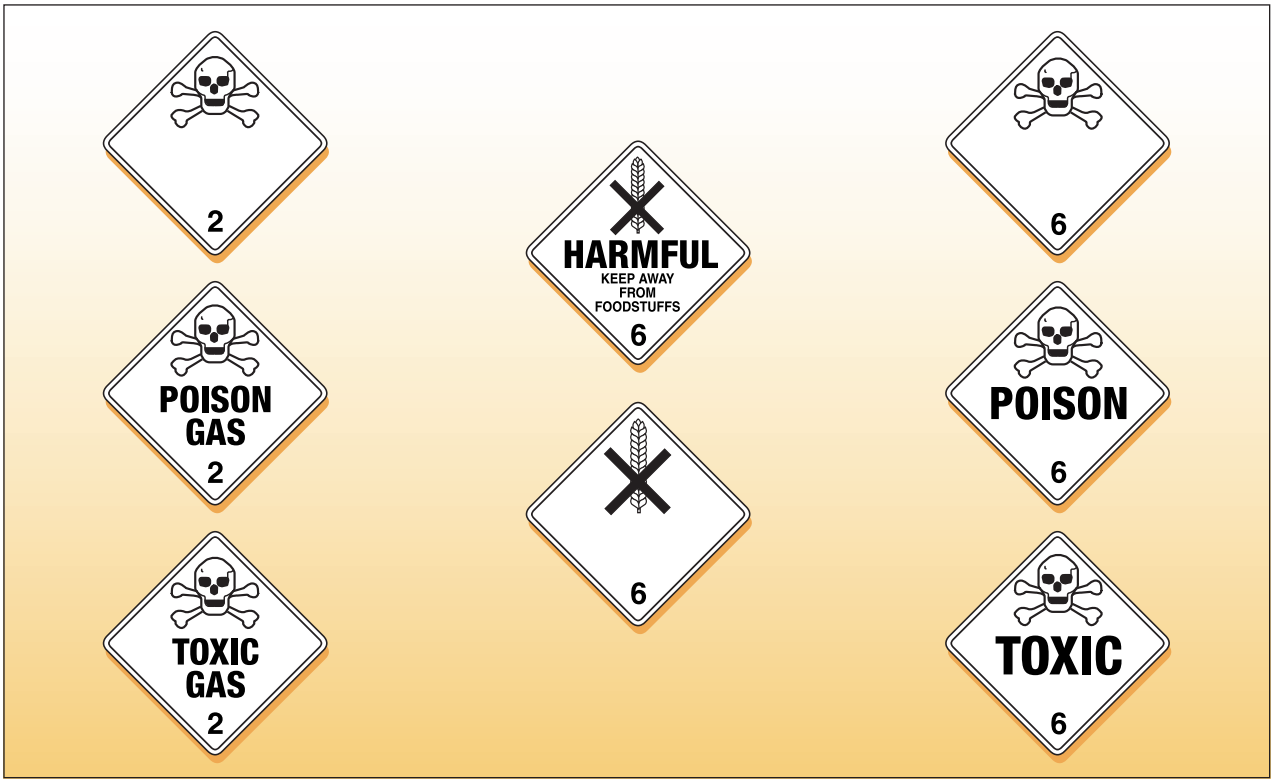
Protection. Any means by which an individual protects his or her body. Measures include masks, self-contained breathing apparatuses, clothing, structures such as buildings, and vehicles.

V

V-series nerve agents. Chemical agents of moderate to high toxicity developed in the 1950s. They are generally persistent. Examples are VE (phosphonothioic acid, ethyl-, S-[2-(diethylamino)ethyl] O-ethylester), VG (phosphorothioic acid, S-[2-(diethylamino)ethyl] O, O-diethyl ester), VM (phosphonothioic acid, methyl-, S-[2-(diethylamino) ethyl] O-ethyl ester), VS (phosphonothioic acid, ethyl, S-[2-[bis(1-methylethyl) amino] ethyl] O-ethyl ester), and VX (phosphonothioic acid, methyl-, S-[2-[bis(1-methylethyl)amino]ethyl] O-ethyl ester).

Vapor agents. A gaseous form of a chemical agent. If heavier than air, the cloud will be close to the ground. If lighter than air, the cloud will rise and disperse more quickly.

Volatility. A measure of how readily a substance will vaporize.



Placards Associated with Chemical Incidents

Biological Terms

A

Aerosol. Fine liquid or solid particles suspended in a gas (e.g., fog, smoke).

Antibiotic. A substance that inhibits the growth of or kills microorganisms.

Antisera. The liquid part of blood containing antibodies that react against disease-causing agents such as those used in biological warfare.

B

Bacteria. Single-celled organisms that multiply by cell division and that can cause disease in humans, plants, or animals.

Biochemicals. The chemicals that make up or are produced by living things.

Biological warfare. The intentional use of biological agents as weapons to kill or injure humans, animals, or plants, or to damage equipment.

Biological warfare agents. Living organisms or the materials derived from them that cause disease in or harm to humans, animals, or plants, or cause deterioration of material. Biological agents may be used as liquid droplets, aerosols, or dry powders.

Bioregulators. Biochemicals that regulate bodily functions. Bioregulators that are produced by the body are termed "endogenous." Some of these same bioregulators can be chemically synthesized.

C

Causative agents. The organism or toxin that is responsible for causing a specific disease or harmful effect.

Contagious. Capable of being transmitted from one person to another.

Culture. A population of microorganisms grown in a medium.

D

Decontamination. The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

F

Fungi. Any of a group of plants mainly characterized by the absence of chlorophyll, the green colored compound found in other plants. Fungi range from microscopic single-celled plants (such as molds and mildews) to large plants (such as mushrooms).

H

Host. An animal or plant that harbors or nourishes another organism.

I

Incapacitating agents. Agents that produce physical or psychological effects, or both, that may persist for hours or days after exposure, rendering victims incapable of performing normal physical and mental tasks.

Infectious agents. Biological agents capable of causing disease in a susceptible host.

Infectivity. (1) The ability of an organism to spread. (2) The number of organisms required to cause an infection to secondary hosts. (3) The capability of an organism to spread out from the site of infection and cause disease in the host organism.

L

Line-source delivery system. A delivery system in which the biological agent is dispersed from a moving ground or air vehicle in a line perpendicular to the direction of the prevailing wind. (See also "point-source delivery system.")

M

Microorganism. Any organism, such as bacteria, viruses, and some fungi, that can be seen only with a microscope.

Mycotoxin. A toxin produced by fungi.

N

Nebulizer. A device for producing a fine spray or aerosol.

O

Organism. Any individual living thing, whether animal or plant.

P

Parasite. Any organism that lives in or on another organism without providing benefit in return.

Pathogen. Any organism (usually living), such as bacteria, fungi, and viruses, capable of producing serious disease or death.

Pathogenic agents. Biological agents capable of causing serious disease.

Point-source delivery system. A delivery system in which the biological agent is dispersed from a stationary position. This delivery method results in coverage over a smaller area than with the line-source system. See also line-source delivery system.

R

Route of exposure (entry). The path by which a person comes into contact with an agent or organism (e.g., through breathing, digestion, skin contact).

S

Single-cell protein. Protein-rich material obtained from cultured algae, fungi, protein, and bacteria, and often used as food or animal feed.

Spore. A reproductive form some microorganisms can take to become resistant to environmental conditions, such as extreme heat or cold, while in a "resting stage."

T

Toxicity. A measure of the harmful effect produced by a given amount of a toxin on a living organism. The relative toxicity of an agent can be expressed in milligrams of toxin needed per kilogram of body weight to kill experimental animals.

Toxins. Poisonous substances produced by living organisms.

V

Vaccine. A preparation of killed or weakened microorganism products used to artificially induce immunity against a disease.

Vector. An agent, such as an insect or rat, capable of transferring a pathogen from one organism to another.

Venom. A poison produced in the glands of some animals (e.g., snakes, scorpions, bees).

Virus. An infectious microorganism that exists as a particle rather than as a complete cell. Particle sizes range from 20 to 400 nanometers (one-billionth of a meter). Viruses are not capable of reproducing outside of a host cell.

Placards Associated with Biological Incidents

Radiological Terms

A

Acute radiation syndrome. Consists of three levels of effects: hernatopoletic (blood cells, most sensitive); gastrointestinal (GI cells, very sensitive); and central nervous system (brain/muscle cells, insensitive). The initial signs and symptoms are nausea, vomiting, fatigue, and loss of appetite. Below about 200 rems, these symptoms may be the only indication of radiation exposure.

Alpha particles (α). Alpha particles have a very short range in air and a very low ability to penetrate other materials, but also have a strong ability to ionize materials. Alpha particles are unable to penetrate even the thin layer of dead cells of human skin and consequently are not an external radiation hazard. Alpha-emitting nuclides inside the body as a result of inhalation or ingestion are a considerable internal radiation hazard.

B

Beta particles (β). High-energy electrons emitted from the nucleus of an atom during radioactive decay. They normally can be stopped by the skin or a very thin sheet of metal.

C

Cesium-137 (Cs-137). A strong gamma ray source that can contaminate property, entailing extensive cleanup. It is commonly used in industrial measurement gauges and for irradiation of material. Its half-life is 30.2 years.

Cobalt-60 (Co-60). A strong gamma ray source that is extensively used as a radiotherapeutic for treating cancer, food and material irradiation, gamma radiography, and industrial measurement gauges. Its half-life is 5.27 years.

Curie (Ci). A unit of radioactive decay rate defined as 3.7 x 1010 disintegrations per second.

D

Decay. The process by which an unstable element is changed to another isotope or another element by the spontaneous emission of radiation from its nucleus. This process can be measured using radiation detectors such as Geiger counters.

Decontamination. The process of making people, objects, or areas safe by absorbing, destroying, neutralizing, making harmless, or removing the hazardous material.

Dose. A general term for the amount of radiation absorbed over a period of time.

Dosimeter. A portable instrument for measuring and registering the total accumulated dose to ionizing radiation.

G

Gamma ray (γ). A high-energy photon emitted from the nucleus of atoms; similar to an x-ray. It can penetrate deeply into body tissue and many materials. Cobalt-60 and Cesium-137 are both strong gamma-emitters. Shielding against gamma radiation requires thick layers of dense materials, such as lead. Gamma rays are potentially lethal to humans.

H

Half-life. The amount of time needed for half of the atoms of a radioactive material to decay.

Highly enriched uranium (HEU). Uranium that is enriched to above 20 percent Uranium-235 (U-235). Weapons-grade HEU is enriched to above 90 percent in U-235.

I

Ionize. To split off one or more electrons from an atom, thus leaving it with a positive electric charge. The electrons usually attach to one of the atoms or molecules, giving them a negative charge.

Iridium-192. A gamma ray emitting radioisotope used for gamma radiography. Its half-life is 73.83 days.

Isotope. Forms of the same element that have different numbers of neutrons in the nucleus. For example, deuterium (2H) and tritium (3H) are isotopes of ordinary hydrogen (H).

L

Lethal dose (50/30). The dose of radiation expected to cause death within 30 days to 50 percent of those exposed without medical treatment. The generally accepted range is from 400–500 rem received over a short period of time.

N

Nuclear reactor. A device in which a controlled, self-sustaining nuclear chain reaction can be maintained with the use of cooling to remove generated heat.

P

Plutonium-239 (Pu-239). A metallic element used for nuclear weapons. Its half-life is 24,110 years.

R

Rad. A unit of absorbed dose of radiation defined as deposition of 100 ergs of energy per gram of tissue. A rad amounts to approximately one ionization per cubic micron.

Radiation. High energy alpha or beta particles or gamma rays that are emitted by an atom as the substance undergoes radioactive decay.

Radiation sickness. Symptoms resulting from excessive exposure of the body to radiation.

Radioactive waste. Disposable, radioactive materials resulting from nuclear operations. Wastes are generally classified into two categories, high-level and low-level.

Radiological Dispersal Device (RDD). A device (weapon or equipment), other than a nuclear explosive device, designed to disseminate radioactive material in order to cause destruction, damage, or injury by means of the radiation produced by the decay of such material.

Radioluminescence. The luminescence produced by particles emitted during radioactive decay.

Roentgen Equivalent Man (REM or rem). A unit of absorbed dose that takes into account the relative effectiveness of radiation that harms human health.

S

Shielding. Materials (lead, concrete, etc.) used to block or attenuate radiation for protection of equipment, materials, or people.

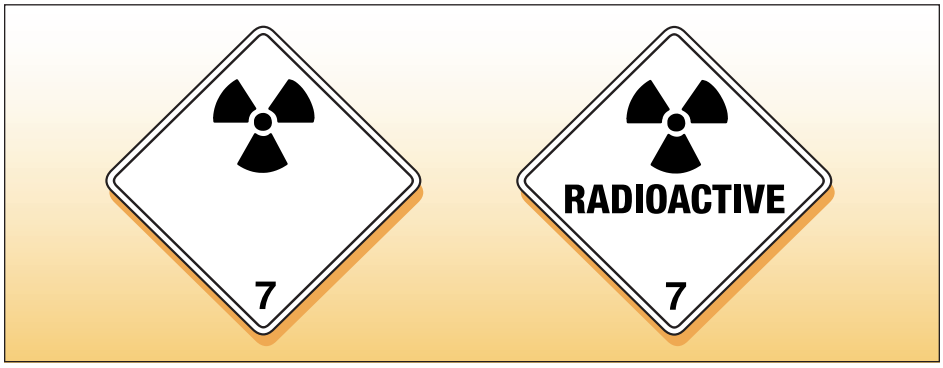
Special Nuclear Material (SNM). Plutonium and uranium enriched in the isotopes Uranium-233 or Uranium-235.

U

Uranium 235 (U-235). Naturally-occurring U-235 is found at 0.72 percent enrichment. U-235 is used as a reactor fuel or for weapons; however, weapons typically use U-235 enriched to 90 percent. Its half-life is 7.04 x 108 years.

X

X-ray. An invisible, highly penetrating electromagnetic radiation of much shorter wavelength (higher frequency) than visible light. Very similar to gamma rays.



Placards Associated with Radiological Incidents

Chemical Warfare Agent Characteristics

Sources: U.S. Department of the Army, *Potential Military Chemical/Biological Agents and Compounds*, U.S. Army Field Manual 3-9, (NAVFAC P-467, AFR 355-'7), 12 December 1990. Washington, D.C.: U.S. Government Printing Office.

Committee on Toxicology, National Research Council. 1997. *Review of Acute Human-Toxicity Estimates for Selected Chemical Warfare Agents*. Washington, D.C.: National Academy Press.

		PHYSICAL AND CHEMICAL PROPERTIES													PHYSIOLOGICAL ACTION						CWC
Agent Type	Chemical Agent; **Symbol** Chemical Structure	Molecular Weight	State @ 20°C	Odor	Vapor Density (Air = 1)	Liquid Density (g/cc)	Freezing/ Melting Point (°C)	Boiling Point (°C)	Vapor Pressure (mm^Hg)	Volatility (mg/m^3)	Heat of Vaporization (cal/g)	Decomposition Temperature (°C)	Flash Point	Stability	Median Lethal Dose (LD_{50}) (mg-min/m^3)	Median Incapacitating Dose (ID_{50})	Eye & Skin Toxicity	Rate of Action	Physiological Action	Detoxification Rate	CWC Schedule
NERVE	Tabun; **GA** $C_2H_5OPO(CN)N(CH_3)_2$	162.3	Colorless to brown liquid	Faintly fruity; none when pure	5.63	1.073 at 25°C	-5	240	0.037 @ 20°C	610 @ 25°C	79.56	150	78°C	Stable in steel at normal temperatures	15,000 by skin (vapor) or 1500 (liquid); 70 inhaled	<50 inhaled	Very high	Very Rapid	Cessation of breath -- death may follow	Slight, but definite	1.A.(2)
	Sarin; **GB** $CH_3PO(F)OCH(CH_3)_2$	140.1	Colorless liquid	Almost none when pure	4.86	1.0887 at 25°C	-56	158	2.9 @ 25°C; 2.10 @ 20°C	22,000 @ 25°C; 16,090 @ 20°C	80	150	Non-flammable	Stable when pure	10,000 by skin (vapor) or 1700 (liquid); 35 inhaled	25 inhaled	Very high	Very rapid	Cessation of breath – death may follow	cumulative	1.A.(1)
	Soman; **GD** $CH_3PO(F)OCH(CH_3)C(CH_3)_3$	182.178	Colorless liquid	Fruity; camphor when impure	6.33	1.0222 at 25°C	-42	198	0.4 @ 25°C	3,900 @ 25°C	72.4	130	High enough not to interfere w/ military use	Less stable than GA or GB	2,500 by skin (vapor) or 350 (liquid); 35 inhaled	25 inhaled	Very high	Very rapid	Cessation of breath – death may follow	Low, essentially cumulative	1.A.(1)
	(Cyclo-sarin); **GF** $CH_3PO(F)OC_6H_{11}$	180.2	Liquid	Sweet; musty; peaches; shellac	6.2	1.1327 at 20°C	-30	239	0.044 @ 20°C	438 @ 20°C	90.5	---	94°C	Relatively stable in steel	2,500 by skin (vapor) or 350 (liquid); 35 inhaled	25 inhaled	Very high	Very rapid	Cessation of breath – death may follow	Low	1.A.(1)
	VX $(C_2H_5O)(CH_3O)P(O)S(C_2H_4)N(C_2H_5(CH_3)_2]_2$	267.38	Colorless to amber liquid	None	9.2	1.0083 at 20°C	below -51	298	0.0007 @ 20°C	10.5 @ 25°C	78.2 @ 25°C	Half-life of 36 hr at 150	159°C	Relatively stable at room temperature	150 by skin (vapor) or 5 (liquid); 15 inhaled	25 by skin (vapor) or 2.5 (liquid); 10 inhaled	Very high	Very rapid	Produces casualties when inhaled or absorbed	low, essentially cumulative	1.A.(3)
	V_x ("V sub x")	211.2	Colorless liquid	None	7.29	1.062 at 20°C	---	256	0.007 @ 25°C; 0.004 @ 20°C	75 @ 25°C; 48 @ 20°C	67.2	---	---	Relatively stable	---	---	Very high	Rapid	Produces casualties when inhaled or absorbed	low, essentially cumulative	
BLISTER	Distilled Mustard; **HD** $(ClCH_2CH_2)_2S$	159.08	Colorless to pale yellow liquid	Garlic or horseradish	5.4	1.268 @ 25°C; 1.27 @ 20°C	14.45	217	0.072 @ 20°C	610 @ 20°C	94	149 – 177	105°C; ignited by large explosive charges	Stable in steel or aluminum	900 (inhaled); 5,000 by skin (vapor) or 1,400 (liquid)	500 (skin); 100 (inhaled); 25 (eyes or nose)	Eyes very susceptible; skin less so	Delayed: hours to days	Blisters; destroys tissue; injures blood cells	Very low – cumulative	1.A.(4)
	Nitrogen Mustard; **HN-1** $(ClCH_2CH_2)_2NC_2H_5$	170.08	Dark liquid	Fishy or musty	5.9	1.09 @ 20°C	-34	194	0.24 @ 25°C	1,520 @ 20°C	77	Decomposes before boiling is reached	High enough not to interfere w/ military use	Adequate	1,500 (inhaled); 20,000 (skin)	200 by eye; 9,000 by skin	Eyes susceptible to low concentration; skin less so	Delayed: 12 hours or longer	Blisters; affects respiratory tract; destroys tissue; injures blood cells	Not detoxified; cumulative	1.A.(6)
	Nitrogen Mustard; **HN-2** $(ClCH_2CH_2)_2NCH_3$	156.07	Dark liquid	Soapy (low concentrations); Fruity (high)	5.4	1.15 @ 20°C	-65 to -60	75 at 15mmHg	0.29 @ 20°C	3,580 @ 25°C	78.8	Below boiling; polymerizes with heat generation	High enough not to interfere w/ military use	Unstable	3,000 (inhaled)	<HN-1 & >HN-3; 100 by eye	Toxic to eyes; blisters skin	*Skin* – delayed 12 hrs or more; *Eyes* – faster than HD	Similar to HD; bronchopneumonia possible after 24 hours	Not detoxified; cumulative	1.A.(6)
	Nitrogen Mustard; **HN-3** $N(CH_2CH_2Cl)_3$	204.54	Dark liquid	None, if pure	7.1	1.24 @ 20°C	-37	256	0.0109 @ 25°C	121 @ 25°C	74	Below boiling point	High enough not to interfere w/ military use	Stable	1,500 (inhaled); 10,000 by skin (est.)	200 by eye; 2,500 by skin (est.)	Eyes very susceptible; skin less so	Serious effects same as HD; minor effects sooner	Similar to HN-2	Not detoxified – cumulative	1.A.(6)
	Phosgene oximedichloro-foroxime; **CX** CCl_2NOH	113.94	Colorless solid or liquid	Sharp, penetrating	3.9	--	35 to 40	53 –54 at 28mmHg	11.2 @ 25°C (solid); 13 @ 40°C (liquid)	1,800 @ 20°C	101 at 40°C	Decomposes slowly at normal temperature	---	Decomposes slowly	3,200 (inhaled)	very low	Powerful irritant to eyes and nose; liquid corrosive to skin	Immediate effects on contact	Violently irritates mucous membranes, eyes, and nose; forms wheals rapidly	---	
	Lewisite; **L** $ClCHCHAsCl_2$	207.35	Colorless to brownish	Varies; may resemble geraniums	7.1	1.89 @ 20°C	-18	190	0.394 @ 20°C	4,480 @ 20°C	58 at 0°C to 190°C	>100	None	Stable in steel and glass	1,200–1,500 (inhaled); 100,000 (skin)	<300 by eye; >1,500 to 2,000 by skin	Severe eye damage; skin less so	Rapid	Similar to HD, plus may cause systemic poisoning	Not detoxified	1.A.(5)
	Mustard-Lewisite mixture; **HL**	186.4	Dark, oily liquid	Garlic	6.5	1.66 @ 20°C	-25.4 (pure)	<190	0.248@ 20°C	2,730 @ 20°C	58 to 94	>100	High enough not to interfere w/ military use	Stable in lacquered steel	15,000 (inhaled); >10,000 (skin)	200 by eye; 1,500 to 2,000 by skin	Very high	Prompt stinging; blistering agent about 13 hours	Similar to HD, plus may cause systemic poisoning	Not detoxified	1.A.(4); 1.A.(5)
	Phenyldichlorarsine; **PD** $C_6H_5AsCl_2$	222.91	Colorless liquid	None	7.7	1.65 @ 20°C	-20	252 to 255	0.033 @ 25°C	390 @ 25°C	69	Stable to boiling point	High enough not to interfere w/ military use	Very stable	2,600 (inhaled)	16 as vomiting agent; 1,800 as blister	633 mg-min/m^3 produces eye casualty; less toxic to skin	Immediate eye effects; skin effects in 30 to 60 minutes	Irritates; causes nausea, vomiting and blisters	Probably rapid	
	Ethyldichlorarsine; **ED** $C_2H_5AsCl_2$	174.88	Colorless liquid	Fruity, but biting; irritating	6.0	1.66 @ 20°C	-65	156	2.09 @ 20°C	20,000 @ 20°C	52.5	Stable to boiling point	High enough not to interfere w/ military use	Stable in steel	3,000–5,000 (inhaled); 100,000 (skin)	5 to 10 by inhalation	Vapor harmful on long exposure; liquid blisters <L	Immediate irritation; delayed blistering	Damages respiratory tract; effects eyes; blisters; can cause systemic poisoning	Rapid	
	Methyldichlorarsine; **MD** CH_3AsCl_2	160.86	Colorless liquid	None	5.5	1.836 @ 20°C	-55	133	7.76 @ 20°C	74,900 @ 20°C	49	Stable to boiling point	High enough not to interfere w/ military use	Stable in steel	3,000 – 5,000 (est.)	25 by inhalation	Eye damage possible; blisters less than HD	Immediate irritation; delayed blistering	Irritates respiratory tract; Injures lungs and eyes; Causes systemic poisoning	Rapid	
BLOOD	Hydrogen cyanide; **AC** HCN	27.02	Colorless gas or liquid	Bitter almonds	0.990 @ 20°C	0.687 @ 20°C	-13.3	25.7	742 @ 25°C; 612 @ 20°C	1,080,000 @ 25°C	233	>65.5	0°C; ignited 50% of time when disseminated by artillery shells	Stable if pure; can burn on explosion	Varies widely with concentration	Varies with concentration	Moderate	Very rapid	Interferes with body tissues' oxygen use; accelerates rate of breathing	Rapid: 0.017 mg/kg/min	3.A.(3)
	Cyanogen chloride; **CK** CNCl	61.48	Colorless gas or liquid	Pungent, biting; Can go unnoticed	2.1	1.18 @ 20°C	-6.9	12.8	1,000 @ 25°C	2,600,000 @ 20°C	103	100	None	Tends to polymerize; may explode	11,000	7,000	Low; lacrimatory and irritating	Very rapid	Chokes, irritates, causes slow breathing rate	Rapid: 0.02 to 0.1 mg/kg/min	3.A.(2)
	Arsine; **SA** AsH_3	77.93	Colorless gas	Mild garlic	2.69	1.34 @ 20°C	-116	-62.5	11,100 @ 20°C	30,900,000 @ 20°C	53.7 @ -62.5°C	280	Below detonation temp.; mixtures w/ air may explode spontaneously	Not stable in uncoated metal containers	5,000	2,500	None	Delayed 2 hours to 11 days	Damages blood, liver, and kidneys	Low	
CHOKING	Phosgene; **CG** $COCl_2$	98.92	Colorless gas	New-mown hay; green corn	3.4	1.37 @ 20°C	-128	7.6	1.173 @ 20°C	4,300,000 @ 7.6°C	59	800	None	Stable in steel if dry	3,200	1,600	None	Immediate to 3 hr, depending on conc.	Damages and floods lungs	Not detoxified – cumulative	3.A.(1)
	Diphosgene; **DP** $ClCOOCCl_3$	197.85	Colorless gas	New-mown hay; green corn	6.8	1.65 @ 20°C	-57	127–128	4.2 @ 20°C	45,000 @ 20°C	57.4	300 to 350	None	Unstable; tends to convert to CG	3,200	1,600	Slightly lacrimatory	Immediate to 3 hr, depending on conc.	Damages and floods lungs	Not detoxified – cumulative	3.A.(1)
VOMITING	Diphenylchloroarsine; **DA** $(C_6H_5)_2AsCl$	264.5	White to brown solid	None	Forms little vapor	1.387 @ 50°C	41 to 44.5	333	0.0036 @ 45°C	48 @ 45°C	56.6	300	350	Stable if pure	15,000 (est.)	12 (>10 minutes)	Irritating; not toxic	Very rapid	Like cold symptoms, plus headache, vomiting, nausea	Moderate	
	Adamsite; **DM** $C_6H_4(AsCl)-NH)C_6H_4$	277.57	Yellow to green solid	None	Forms little vapor	1.65 (solid) @ 20°C	195	410	Negligible	Negligible	80	>boiling point	None	Stable in glass or steel	Variable; avg.: 11,000	22 (1 min.); 8 (60 min. exposure)	Irritating; relatively not toxic	Very rapid	Like cold symptoms, plus headache, vomiting, nausea	Rapid in small amounts	
	Deiphenylcyanoarsine; **DC** $(C_6H_5)_2AsCN$	255.0	White to pink solid	Bitter almond-garlic mixture	Forms little vapor	1.3338 @ 35°C	31.5 to 35	350	0.0002 @ 20°C	2.8 @ 20°C	71.1	300 (25% decomposed)	Low	Stable at normal temperatures	10,000 (est.)	30 (30 sec); 20 (5 min. exposure)	Irritating; not toxic	More rapid than DM or DA	Like cold symptoms, plus headache, vomiting, nausea	Rapid	
Incapacitating	**BZ**	337.4	White crystal	None	11.6	Bulk 0.51 solid; Crystal 1.33	167.5	320	0.03 @ 70°C	0.5 @ 70°C	62.9	begins at 170°C	246°C	Adequate	200,000 (est.)	112	---	Delayed; 1 to 4 hours depending on exposure	Fast heart beat, vomiting, dry mouth, blurred vision, stupor, increasing random activity	---	2.A.(3)
TEAR	Chloroacetophenone; **CN** $C_6H_5COCH_2Cl$	154.59	Solid	Apple blossoms	5.3	1.318 (solid) @ 20°C	54	248	0.0041 @ 20°C	34.3 @ 20°C	98	Stable to boiling point	High enough not to interfere w/ military use	Stable	7,000 to 14,000	80	Temporarily severe eye irritation; mild skin irritation	Instantaneous	Causes tearing; irritates eyes and respiratory tract	Rapid	
	Chloroacetophenone in Chloroform; **CNC**	128.17	Liquid	Chloroform	4.4	1.40 @ 20°C	0.23	variable, 60 to 247	127 @ 20°C	Indeterminate	n/a	Stable to boiling point	None	Adequate	11,000 (est.)	80	Temporarily severe eye irritation; mild skin irritation	Instantaneous	Cause tearing; irritates eyes and respiratory tract	Rapid	
	Chloroacetophenone and Chloropicrin in Chloroform; **CNS**	141.78	Liquid	Flypaper	~5	1.47 @ 20°C	2	variable, 60 to 247	78 @ 20°C	610,000 @ 20°C (includes solvent)	n/a	Stable to boiling point	None	Adequate	11,400	60	Irritating; not toxic	Instantaneous	Vomiting and choking agent as well as a tear agent	Slow because of effect of PS	
	Chloroacetophenone in Benzene and Carbon Tetrachloride; **CNB**	119.7	Liquid	Benzene	~4	1.14 @ 20°C	-7 to -30	variable 75 to 247	variable; mostly solvent vapor	Indeterminate	n/a	>247	<4.44°C	Adequate	11,000 (est.)	80	Temporarily severe eye irritation; mild skin irritation	Instantaneous	Powerfully lacrimatory	Rapid	
	Bromobenzylcyanide; **CA** $BrC_6H_4CH_2CN$	196	Yellow or solid liquid	Soured fruit	6.7	1.47 @ 25°C	25.5	Decomposes at 242	0.011 @ 20°C	115 @ 20°C	79.5 @ 20°C	60 to 242	None	Fairly stable in glass, lead, or enamel	8,000 to 11,000 (est.)	30	Irritating; not toxic	Instantaneous	Irritates eyes and respiratory passages	Rapid in low dosage	
	O-chlorobenzylmalonitrile; **CS** $ClC_6H_4CHC(CN)_2$	188.5	Colorless solid	Pepper	---	1.04 @ 20°C	93 to 95	310 to 315	0.00034 @ 20°C	0.71 @ 25°C	53.6	---	197°C	Stable	61,000	10 to 20	Highly irritating; not toxic	Instantaneous	Highly irritating; not toxic	Rapid	
	CR $(C_6H_4)_2(O)(N)CH$	195.25	Yellow powder in solution	Burning sensation	6.7	---	72	335	0.00059 @ 20°C	0.63 @ 25°C	---	---	188°C	Stable	---	0.15	Highly irritating; not toxic	Instantaneous	Irritates skin, eyes, nose, and throat	Moderate	
	Chloropicrin; **PS** Cl_3CNO_2	164.38	Liquid	Stinging; pungent	5.6	1.66	-69	112	18.3 @ 20°C	165,000 @ 20°C	---	>400	Not flammable	Adequate; unstable in light	2,000	9	Highly irritating	Instantaneous	Acts as tear, vomiting, and choking agent	Slow	3.A.(4)

Selected Biological Agent Characteristics

Agent Type	Disease/Condition *Causative Agent/ Pathogen*	Description of Agent	Transmissible Person to Person	Infectivity/ Lethality	Incubation Period	Duration of Illness	Persistence/ Stability	Vaccination/ Toxoids	Rate of Action	Symptoms	Treatment	Possible Means of Delivery
BACTERIA	Anthrax (inhalation) *Bacillus anthracis*	Rod-shaped, gram-positive, aerobic sporulating micro-organism, individual spores ~(1–1.2)x(3–5)µ	No	Moderate/ High	1–7 days	3–5 days	Spores are highly stable	Yes	Symptoms in 2–3 days; Shock and death occurs with 24–36 hrs after symptoms	Fever, malaise, fatigue, cough and mild chest discomfort, followed by severe respiratory distress with dyspnea, diaphoresis, stridor, and cyanosis	Usually not effective after symptoms are present, high dose antibiotic treatment with penicillin, ciprofloxacin, or doxycycline should be undertaken. Supportive therapy may be necessary.	Aerosol.
	Brucellosis *Brucella suis, melitensis & abortus*	All non-motile, non-sporulating, gram negative, aerobic bacterium; ~(0.5-1)x(1-2)µ	No	High/Low	Days to months	Weeks to months	Organisms are stable for several weeks in wet soil and food.	Yes	Highly variable, usually 6-60 days.	Chills, sweats, headache, fatigue, myalgias, arthralgias, and anorexia. Cough may occur. Complications include sacroiliitis, arthritis, vertebral osteomyelitis, epididymoorchitis, and rarely endocarditis.	Recommended treatment is doxycycline (200 mg/day) plus rifampin (900 mg/day) for 6 weeks.	Aerosol. Expected to mimic a natural disease.
	Cholera *Vibrio cholerae*	Short, curved, motile, gram-negative, non-sporulating rod. Strongly anaerobic, these organisms prefer alkaline and high salt environments.	Negl.	Low/Moderate-High	1-5 days	1 or more weeks	Unstable in aerosols and pure water, more so in polluted water.	Yes	Sudden onset after 1-5 day incubation period.	Initial vomiting and abdominal distension with little or no fever or abdominal pain. Followed rapidly by diarrhea, which may be either mild or profuse and watery, with fluid losses exceeding 5 to 10 liters or more per day. Without treatment, death may result from severe dehydration, hypovolemia, and shock.	Therapy consists of fluid and electrolyte replacement. Antibiotics will shorten the duration of diarrhea and thereby reduce fluid losses. Tetracycline, ampicillin, or trimethoprim-sulfamethoxazole are most commonly used.	1. Sabotage (food/water supply) 2. Aerosol
	Glanders *Burkholderia mallei*	Gram-negative bacillus primarily noted for producing disease in horses, mules, and donkeys	Negl.	/Moderate-High	10-14 days	N/A	N/A	No	N/A	Inhalational exposure produces fever, rigors, sweats, myalgia, headache, pleuritic chest pain, cervical adenopathy, splenomegaly, and generalized papular/pustular eruptions. Almost always fatal without treatment.	Few antibiotics have been evaluated *in vivo*. Sulfadiazine may be effective in some cases. Ciprofloxacin, doxycycline, and rifampin have *in vitro* efficacy. Extrapolating from melioidosis guidelines, a combination of TMP-SMX + ceftazidime ± gentamicin might be considered.	Aerosol.
	Plague (pneumonic, bubonic) *Yersinia pestis*	Rod-shaped, non-motile, non-sporulating, gram-negative, aerobic bacterium; ~(0.5-1)x(1-2)µ	High	High/Very High in untreated personnel, the mortality is 100%	2 to 6 days for bubonic and 3 to 4 days for pneumonic	1-2 days	Less important because of high transmissibility.	Yes	Two to three days	High fever, chills, headache, hemoptysis, and toxemia, progressing rapidly to dyspnea, sturdier, and cyanosis. Death results from respiratory failure, circulatory collapse, and a bleeding diathesis.	Early administration of antibiotics is very effective. Supportive therapy for pneumonic and septicemic forms is required.	May be delivered via contaminated vectors (fleas) causing bubonic type, or, more likely, via aerosol causing pneumonic type.
	Shigellosis *Shigella Dysenteriae*	Rod-shaped, gram-negative, non-motile, non-sporulating bacterium	Negl.	High/Low	1-7 days (usually 2-3)	N/A	Unstable in aerosols and pure water, more so in polluted water.	No	Symptoms usually within 2-3 days, however, known to demonstrate in as little as 12 hours or as long as 7 days.	Fever, nausea, vomiting, abdominal cramps, watery diarrhea, and occasionally, traces of blood in the feces. Symptoms range from mild to severe with some infected individuals not experiencing any symptoms.	The antibiotics commonly used for treatment are ampicillin, trimethoprim/sulfamethoxazole (also known as Bactrim* or Septra*), nalidixic acid, or ciprofloxacin. Persons with mild infections will usually recover quickly without antibiotic treatment. Antidiarrheal agents such as loperamide (Imodium*) or diphenoxylate with atropine (Lomotil*) are likely to make the illness worse and should be avoided.	Contaminated food or water
	Tularemia *Francisella tularensis*	Small, aerobic, non-sporulating, non-motile, gram-negative *cocco-bacillus* ~0.2x(0.2-0.7)µ	No	High/ Moderate if untreated	1-10 days	2 or more weeks	Not very stable	Yes	Three to five days	Ulceroglandular tularemia with local ulcer and regional lymphadenopathy, fever, chills, headache, and malaise. Typhoidal or septicemic tularemia presents with fever, headache, malaise, substernal discomfort, prostration, weight loss, and non-productive cough.	Administration of anitbiotics with early treatment is very effective. Streptomycin – 1 gm I. M. q. 12 hrs x 10 10-14 d. Gentamicin – 3-5 mg/kg/day x 10-14 d.	Aerosol.
	Typhoid *Salmonella typhi*	Rod-shaped, motile, non-sporulating gram-negative bacterium	Negl.	Moderate/ Moderate if untreated	6-21 days	Several weeks	Stable	Yes	One to three days	Sustained fever, severe headache, malaise, anorexia, a relative bradycardia, splenomegaly, nonproductive cough in the early stage of the illness, and constipation more commonly than diarrhea.	Chloramphenicol amoxicillin or TMP-SMX. Quilone derivatives and third generation cephalusporins and supportive therapy.	Sabotage of food and water supplies.
RICKETTSIAE	Q-Fever *Coxiella burneti*	Bacterium-like, gram-negative organism, pleomorphic 300-700 nm	No	High/Very low	10-20	2 days to 2 weeks	Stable	Yes	Onset may be sudden	Chills, retrobulbar headache, weakness, malaise and severe sweats.	Tetracycline or doxycycline are the treatment of choice and are given orally for 5 to 7 days.	May be a dust cloud either from a line source or a point source (downwind one-half mile or more).
	Typhus (classic) *Rickettsia prowazeki*	Non-motile, minute, coccoid or rod shaped rickettsiae, in pairs or chains, 300 nm	No	High/High	6-15 days	Weeks to months	Not very stable	No	Variable onset, often sudden. Terminates by rapid lysis after about 2 weeks of fever	Headache, chills, prostration, fever, and general pain. A macular eruption appears on the fifth to sixth day, initially on the upper trunk, followed by spread to the entire body, but usually not the face, palms, or soles.	Tetracyclines or chlormphenical orally in a loading dose of 2-3 g, followed by daily doses of 1-2 g/day in 4 divided doses until ind. becomes afelorite (usually 2 days) plus 1 day.	May be delivered via contaminated vectors (lice or fleas).
VIRUSES	Encephalitis	Lipid-enveloped virions of 50-60 nm dia., icosohedral nucleocapsid w. 2 glycoproteins										
	-Eastern/Western Equine Encephalitis (EEE, WEE)		Negl.	High/High	5-15 days	1-3 weeks	Relatively unstable	Yes		Inflammation of the mengies of the brain, headache, fever, dizziness, drowsiness or stupor, tremors or convulsions, muscular incoordination.	No specific treatment; supportive treatment is essential	Airborne spread possible.
	-Venezuelan Equine Encephalitis		Low	High/Low	1-5 days	Days to weeks	Relatively unstable	Yes	Sudden	Inflammation of the mengies of the brain, headache, fever, dizziness, drowsiness or stupor, tremors or convulsions, muscular incoordination.	No specific treatment; supportive treatment is essential	Airborne spread possible.
	Hemorrhagic Fever									Malaise, myalgias, headache, vomiting, and diarrhea may occur with any of the hemorrhagic fevers	No specific treatment; intensive supportive treatment is essential	Airborne spread possible.
	-Ebola Fever	Filovirus	Moderate	High/High	7-9 days	5-16 days	Relatively unstable	No		May also include a macular dermatologic eruption.		
	-Marburg	Filovirus	Moderate					No		May also include a macular dermatologic eruption.		
	-Yellow Fever	Flavivirus. Isosahedral nucleocapsid 37-50 nm diam., lipoprotein env. w/ short surface spikes	Negl.	High/High	3-6 days	1-2 weeks	Relatively unstable	Yes	Sudden			
	Variola Virus (Smallpox)	Asymmetric, brick-shaped, rounded corners; DNA virus	High	High/High	7-17 days	1-2 weeks	Stable	Yes	2-4 days	Malaise, fever, rigors, vomiting, headache, and backache. 2-3 days later lesions appear which quickly progress from macules to papules, and eventually to pustular vesicles. They are more abundant on the extremities and face, and develop synchronously.	No specific treatment; supportive treatment is essential	Airborne spread possible.
TOXIN	Botulinum Toxin	any of the seven distinct neurotoxins produced by the bacillus, *Clostridium botulinum*	No	NA/High	Variable (hours to days)	24-72 hours/Months if lethal	Stable	Yes	12-72 hours	Initial signs and symptoms include ptosis, generalized weakness, lassitude, and dizziness. Diminished salivation with extreme dryness of the mouth and throat may cause complaints of a sore throat. Urinary retention or ileus may also occur. Motor symptoms usually are present early in the disease; cranial nerves are affected first with blurred vision, diplopia, ptosis, and photophobia. Bulbar nerve dysfunction causes dysarthria, dysphonia, and dysphagia. This is followed by a symmetrical, descending, progressive weakness of the extremities along with weakness of the respiratory muscles. Development of respiratory failure may be abrupt.	(1) Respiratory failure—tracheostomy and ventilatory assistance, fatalities should be <5%. Intensive and prolonged nursing care may be required for recovery (which may take several weeks or even months). (2) Food-borne botulism and aerosol exposure—equine antitoxin is probably helpful, sometimes even after onset of signs of intoxication. Administration of antitoxin is reasonable if disease has not progressed to a stable state. Use requires pretesting for sensitivity to horse serum (and desensitization for those allergic). Disadvantages include rapid clearance by immune elimination, as well as a theoretical risk of serum sickness.	1. Sabotage (food/water supply) 2. Aerosol
	Ricin	Glycoprotein toxin (66,000 daltons) from the seed of the castor plant	No	NA/High	Hours	Days	Stable	Not effective	6-72 hours	Rapid onset of nausea, vomiting, abdominal cramps and severe diarrhea with vascular collapse; death has occurred on the third day or later. Following inhalation, one might expect nonspecific symptoms of weakness, fever, cough, and hypothermia followed by hypotension and cardiovascular collapse.	Management is supportive and should include maintenance of intravascular volume. Standard management for poison ingestion should be employed if intoxication is by the oral route.	Aerosol
	Staphylococcal enterotoxin B	One of several exotoxins produced by *Staphylococcus aureus*	No	NA/Low	Days to weeks	Days to weeks	Stable	Not effective	30 min-6 hours	Fever, chills, headache, myalgia, and nonproductive cough. In more severe cases, dyspnea and retrosternal chest pain may also be present. In many patients nausea, vomiting, and diarrhea will also occur.	Treatment is limited to supportive care. No specific antitoxin for human use is available.	1. Sabotage (food/water supply) 2. Aerosol
	Trichothecene (T-2) Mycotoxins	A diverse group of more than 40 compounds produced by fungi.	No	NA/High	Hours	Hours	Stable	Not effective	Sudden	Victims are reported to have suffered painful skin lesions, lightheadedness, dyspnea, and a rapid onset of hemorrhage, incapacitation and death. Survivors developed a radiation-like sickness including fever, nausea, vomiting, diarrhea, leukopenia, bleeding, and sepsis.	General supportive measures are used to alleviate acute T-2 toxicoses. Prompt (within 5-60 min of exposure) soap and water wash significantly reduces the development of the localized destructive, cutaneous effects of the toxin. After oral exposure management should include standard therapy for poison ingestion.	1. Sabotage 2. Aerosol

D

References

American Society of Civil Engineer (ASCE) and Structural Engineering Institute (SEI), 2006, *Minimum Design Loads for Buildings and Other Structures,* ASCE/SEI 7-05, http://www.asce.org/Product.aspx?id=2147485519.

American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE), 1992a, *Evaluation of the Techniques for the Measurement of Air Leakage of Building Components*, ASHRAE Research Project 438-RP, submitted by Dr. Donald G. Colliver, P.E., Dr. William E. Murphy, P.E., Wei Sun, Agricultural Engineering Department, University of Kentucky, Lexington, KY 40546-0276, December 30, 1992, http://rp.ashrae.biz/page/RP438.pdf.

ASHRAE, 1992b, *Gravimetric and Dust Spot Procedures for Testing Air Cleaning Devices Used in General Ventilation for Removing Particulate Matter,* Standard 52.1-92.

ASHRAE, 1999, Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size, Standard 52.2-99.

ASTM International (ASTM), 2007, ASTM F2656-07, *Standard Test Method for Vehicle Crash Testing of Perimeter Barriers*, http://www.astm.org/Standards/F2656.htm.

ASTM, 2003, ASTM E779-03, *Standard Test Method for Determining Air Leakage by Fan Pressurization*, http://www.astm.org/DATABASE.CART/HISTORICAL/E779-03.htm.

Baker, Stewart; Shaun Waterman; and George Ivanov, 2009, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, McAfee, Santa Clara, CA.

Centers for Disease Control (CDC) National Institute for Occupational Safety and Health (NIOSH), 2003, *Statement of Standard for CBRN Air-Purifying Escape Respirator and Self-Contained Escape Respirators*, September 30, 2003, http://www.cdc.gov/niosh/npptl/standardsdev/cbrn/escape/.

Cummings, J.B., C.R. Withers, N. Moyer, P. Fairey, B. McKendry, 1996, "Uncontrolled Air Flow in Non-Residential Buildings," prepared for Florida Energy Office, Department of Community Affairs, FSEC-CR-878-96, March 29, 1996.

Dunning, A. E. and Jennifer L. Oswalt, 2007, "Train Wreck and Chlorine Spill in Graniteville, South Carolina: Transportation Effects and Lessons in Small-Town Capacity for No-Notice Evacuation," *Transportation Research Record: Journal of the Transportation Research Board*, No. 2009, Transportation Research Board of the National Academies, Washington, D.C., 2007, pp. 130–135., http://www.dot.gov/disaster_recovery/resources/TrainWreckChlorineSpillGranitevilleSC.pdf.

Federal Emergency Management Agency (FEMA), 2005, *Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks*, FEMA 452, http://www.fema.gov/plan/prevent/rms/rmsp452.shtm.

FEMA, 2006, *Safe Rooms and Shelters – Protecting People Against Terrorist Attacks*, FEMA 453, http://www.fema.gov/plan/prevent/rms/rmsp453.shtm.

FEMA, 2007, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks*, FEMA 430, http://www.fema.gov/library/viewRecord.do?id=3135.

FEMA, 2008a, *Design and Construction Guidance for Community Safe Rooms*, FEMA 361, http://www.fema.gov/plan/prevent/saferoom/fema361.shtm.

FEMA, 2008b, *Incremental Protection for Existing Commercial Buildings from Terrorist Attack*, FEMA 459, http://www.fema.gov/library/viewRecord.do?id=3270.

FEMA, 2009, *Handbook for Rapid Visual Screening of Buildings to Evaluate Terrorism Risks*, FEMA 455, http://www.fema.gov/library/viewRecord.do?id=1567.

General Services Administration (GSA), 2003, *Progressive Collapse Guidelines, prepared by the Building Security Technology Program Team*, http://www.gsa.gov/portal/content/103205.

GSA, 2005, *Facilities Standards for the Public Buildings Service* (P100), http://www.gsa.gov/portal/content/104821.

GSA, 2007, *The Site Security Design Guide*, June 2007, http://www.gsa.gov/portal/content/280533.

GSA 2010, *Facilities Standards for the Public Buildings Service* (P100), http://www.gsa.gov/portal/category/27243.

Kuligowski, E., 2003, E*levators for Occupant Evacuation and Fire Department Access*, Proceedings of the CIB-CTBUH International Conference on Tall Buildings, May 8–10, 2003, Malaysia, http://www.fire.nist.gov/bfrlpubs/fire03/PDF/f03046.pdf.

National Fire Protection Association (NFPA), 2010, N*FPA 72: National Fire Alarm and Signaling Code*, http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=72.

NFPA, 2012, *NFPA 101: Life Safety Code*, http://www.nfpa.org/aboutthecodes/AboutTheCodes.asp?DocNum=101.

NFPA, 2012, *NFPA 5000: Building Construction and Safety Code*, http://www.nfpa.org/AboutTheCodes/AboutTheCodes.asp?DocNum=5000.

National Institute of Building Sciences (NIBS) Whole Building Design Guide Program, 2010a, *Glazing Hazard Mitigation*, prepared by Joseph L. Smith, PSP and Nancy A. Renfroe, PSP, Applied Research Associates, Inc., Last updated: July 23, 2010, http://www.wbdg.org/resources/glazingmitigation.php.

NIBS Whole Building Design Guide Program, 2010b, *Retrofitting Existing Buildings to Resist Explosive Threats*, prepared by Daniel Watch and Deepa Tolat, Perkins + Will, Last updated: July, 23, 2010, http://www.wbdg.org/resources/retro_rstexplo.php.

Price, Phillip N, Michael D. Sohn, Ashok J. Gadgil, William W. Delp, David M. Lorenzetti, Elizabeth U. Finlayson, Tracy L. Thatcher, Richard G. Sextro, Elisabeth A. Derby, and Sondra A. Jarvis, 2003, *Protecting Buildings from a Biological or Chemical Attack: Actions to take before or during a release.* LBNL/PUB-51959, January 10, 2003, http://securebuildings.lbl.gov/images/BldgAdvice.pdf.

U.S. Army Corps of Engineers, 1999, *Design of Collective Protection Shelters to Resist Chemical, Biological, and Radiological (CBR) Agents*, ETL 1110-3-498, Washington, DC.

U.S. Department of Commerce, 2005a, National Institute of Standards and Technology (NIST), *Final Report of the National Construction Safety Team on the Collapses of the World Trade Center Towers*, Federal Building and Fire Safety Investigation of the World Trade Center Disaster, NIST NCSTAR 1, December 2005, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909017.

U.S. Department of Commerce, 2005b, NIST, *Occupant Behavior, Egress, and Emergency Communications, Federal Building and Fire Safety Investigation of the World Trade Center Disaster*, NIST NCSTAR 1-7, September 2005, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=101046.

U.S. Department of Commerce, 2006, NIST, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, Federal Information Processing Standard Publication 201 (FIPS 201), http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

U.S. Department of Commerce, 2008, NIST, *Final Report on the Collapse of the World Trade Center Building 7, Federal Building and Fire Safety Investigation of the World Trade Center Disaster*, NIST NCSTAR 1A, November 2008, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=861610.

U.S. Department of Defense (DOD), 2003, *Interim Technical Guidance (ITG) Entry Control Facilities*, ITG 03-03, prepared by U.S. Army Corps of Engineers Naval Facilities Engineering Command, Atlantic Division, Norfolk, VA.

DOD, 2005, *Potential Military Chemical/Biological Agents and Compounds*, U.S. Army Field Manual FM 3-11.9, http://www.fas.org/irp/doddir/army/fm3-11-9.pdf.

DOD, 2007a, *UFC DOD Minimum Antiterrorism Standards for Buildings UFC 4-010-01*, http://www.wbdg.org/ccb/DOD/UFC/ufc_4_010_01.pdf.

DOD, 2007b, UFC DOD Minimum Standoff Distances for Buildings, UFC 4-010-02, www.wbdg.org/ccb/DOD/UFC/ufc_4_010_02.pdf.

DOD, 2008a, *Collective Protection Shelters of the Chemical Stockpile Emergency Preparedness Program: Technical Record and Lessons Learned*, prepared by the Chemical, Biological, Radiological & Nuclear Defense Information Analysis Center on behalf of the U.S. Army Chemical Materials Agency,

Aberdeen Proving Ground, MD, http://www.csepp.net/~bill/PIX/OverpressurePix/CSEPP_CPFinalReport(2ndEd)_Sep2008.pdf.

DOD, 2008b, *Structures to Resist the Effects of Accidental Explosions*, UFC 3-340-02, http://www.wbdg.org/ccb/DOD/UFC/ufc_3_340_02.pdf.

DOD, 2010, *Design of Buildings to Resist Progressive Collapse*, UFC 4-023-03, http://www.wbdg.org/ccb/DOD/UFC/ufc_4_023_03.pdf.

U.S. Department of Homeland Security (DHS), 2003, *Critical Infrastructure Identification, Prioritization, and Protection*, HSPD-7, http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.

DHS, 2004a, Interagency Security Committee (ISC) *Security Design Criteria for New Federal Office Buildings and Major Modernization Projects.*

DHS, 2004b, *Policy for a Common Identification Standard for Federal Employees and Contractors*, HSPD-12, http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

DHS, 2005, ISC *Security Standards for Leased Spaces.*

DHS, 2007a, *Guide for the Selection of Biological Agent Detection Equipment for Emergency First Responders*, DHS 101-06, March 2007, https://www.rkb.us/contentdetail.cfm?content_id=97649.

DHS, 2007b, *Guide for the Selection of Chemical Detection Equipment for Emergency First Responders*, Third Edition, DHS 100-06, January 2007, https://www.rkb.us/contentdetail.cfm?content_id=97670.

DHS, 2009a, *Critical Infrastructure Resilience Final Report and Recommendations*, prepared by the National Infrastructure Advisory Council, September 2009. http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf.

DHS, 2009b, *National Infrastructure Protection Plan*, http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

DHS, 2010, ISC *Physical Security Criteria for Federal Facilities.*

Wall Street Journal, 2006, "Ring of Steel for New York?" January 25, 2006.

Associations

American Lifelines Alliance
http://www.americanlifelinesalliance.org

Applied Technology Council
http://www.atcouncil.org

Battelle Memorial Institute, National Security Program
http://www.battelle.org/natsecurity/default.stm

Center for Strategic and International Studies (CSIS)
http://www.csis.org

Centers for Disease Control and Prevention (CDC)/National Institute for Occupational Safety and Health (NIOSH)
http://www.cdc.gov/niosh

Central Intelligence Agency (CIA)
http://www.cia.gov

Council on Tall Buildings and Urban Habitat (CTBUH)
http://www.ctbuh.org

Federal Aviation Administration (FAA)
http://www.faa.gov

Healthy Buildings International, Inc.
http://www.healthybuildings.com

Institute of Transportation Engineers
http://www.ite.org

Interagency Security Committee (ISC)
http://www.dhs.gov/files/committees/gc_1194539370126.shtm

International CPTED [Crime Prevention Through Environmental Design] Association (ICA)
http://www.cpted.net/

Lawrence Berkeley National Laboratory (LBNL)
http://securebuildings.lbl.gov

National Academy of Sciences
http://www.nasonline.org/

Federal Facilities Council (FFC) Standing Committee on Physical Security and Hazard Mitigation
http://sites.nationalacademies.org/DEPS/FFC/DEPS_047556

National Research Council
http://www.nationalacademies.org/nrc/index.html

National Defense Industrial Association (NDIA)
http://www.ndia.org

Public Entity Risk Institute
http://www.riskinstitute.org

Security Design Coalition
http://www.designingforsecurity.org

Security Industry Association (SIA)
http://www.siaonline.org/

Technical Support Working Group
(Departments of Defense and State)
http://www.tswg.gov

U.S. Air Force Electronic System Center (ESC),
Hanscom Air Force Base
http://www.hanscom.af.mil/units/esc/index.asp

U.S. Army Soldiers and Biological Chemical Command (SBCCOM)
http://www.globalsecurity.org/military/agency/army/sbccom.htm

U.S. Department of Justice
http://www.justice.gov/

Federal Bureau of Investigation: Terrorism in the United States reports
http://www.fbi.gov/stats-services/publications

National Institute of Justice (NIJ)
http://nij.gov/

Office of Domestic Preparedness (ODP)
http://www.ojp.usdoj.gov/

U.S. Marshals Service (U.S.MS)
http://www.usmarshals.gov/

The Infrastructure Security Partnership (TISP)
http://www.tisp.org
Founding Organizations

American Council of Engineering Companies (ACEC)
http://www.acec.org

The American Institute of Architects (AIA)
http://www.aia.org/

American Society of Civil Engineers (ASCE)
http://www.asce.org

Architectural Engineering Institute (AEI)
http://content.aeinstitute.org/inside/intro.html

Civil Engineering Research Foundation (CERF) of ASCE
http://www.cerf.org

Structural Engineering Institute (SEI) of ASCE
http://www.seinstitute.org

Associated General Contractors of America
http://www.agc.org

Construction Industry Institute
http://construction-institute.org

Federal Emergency Management Agency (FEMA)
http://www.fema.gov

Human Caused Hazards
http://www.fema.gov/hazard/index.shtm

Mitigation Planning
http://www.fema.gov/plan/mitplanning/index.shtm

Federal Facilities Council – See National Academy of Sciences

National Institute of Standards and Technology (NIST), Building and Fire Research Laboratory
http://www.nist.gov/building-and-fire-research-portal.cfm

Naval Facilities Engineering Command
http://www.navfac.navy.mil

Society of American Military Engineers (SAME)
http://www.same.org

U.S. Army Corps of Engineers
http://www.usace.army.mil

Selected Member Organizations

Air-Conditioning and Refrigeration Institute, Inc.
http://www.ari.org

Air Conditioning Contractors of America
http://www.acca.org

Airport Consultants Council
http://www.acconline.org

Alliance for Fire & Smoke Containment & Control
http://www.afscconline.org

American Association of State Highway and Transportation Officials (AASHTO)
http://www.transportation.org

American Institute of Chemical Engineers, Center for Chemical Process Safety
http://www.aiche.org/ccps

American Planning Association
http://www.planning.org

American Public Works Association
http://www.apwa.net

American Railway Engineering & Maintenance of Way Association
http://www.arema.org

American Society for Industrial Security International (ASIS)
http://www.asisonline.org

American Society of Heating, Refrigerating, and
Air-Conditioning Engineers (ASHRAE)
http://www.ashrae.org

American Society of Interior Designers
http://www.asid.org

American Society of Landscape Architects (ASLA)
http://www.asla.org

American Society of Mechanical Engineers (ASME)
http://www.asme.org

American Underground Construction Association (AUA)
http://www.auca.org

American Water Resources Association (AWRA)
http://www.awra.org

Associated Locksmiths of America
http://www.aloa.org

Association of Metropolitan Water Agencies
http://www.amwa.net

Association of State Dam Safety Officials
http://www.damsafety.org

Building Futures Council
http://www.thebfc.org/Home_Page.html

Building Owners and Managers Association International (BOMA), Emergency Resource Center
http://www.boma.org/

California Department of Health Services, Division of Drinking Water & Environmental Management
http://www.dhs.cahwnet.gov/ps/ddwem

Construction Industry Roundtable
http://www.cirt.org

Construction Innovation Forum
http://www.cif.org

Construction Specifications Institute
http://www.csinet.org

Construction Users Roundtable
http://www.curt.org

Defense Threat Reduction Agency (DTRA)
http://www.dtra.mil

Design-Build Institute of America
http://www.dbia.org

Drexel (University) Intelligent Infrastructure & Transportation Safety Institute
http://www.di3.drexel.edu

Federal Highway Administration
http://www.fhwa.dot.gov

Florida Department of Transportation, Emergency Management Office
http://www.dot.state.fl.us/EmergencyManagement/

George Washington University, Institute for Crisis, Disaster, and Risk Management
http://www.cee.seas.gwu.edu
or
http://www.seas.gwu.edu/~icdm

Homeland Protection Institute, Ltd.
http://www.hpi-tech.org

Inland Rivers Ports and Terminals
http://www.irpt.net

Institute of Electrical and Electronics Engineers, Inc. - U.S.A
http://www.ieeeusa.org

International Association of Foundation Drilling
http://www.adsc-iafd.com

International Code Council (ICC)
http://www.intlcode.org
Consolidates services, products, and operations of BOCA (Building Officials and Code Administrators), ICBO (International Conference of Building Officials) and SBCCI (Southern Building Code Congress International) into one member service organization — the International Code Council (ICC) in January 2003.

International Facility Management Association (IFMA)
http://www.ifma.org

Market Development Alliance of the FRP Composites Industry
http://www.mdacomposites.org

Multidisciplinary Center for Earthquake Engineering Research
http://mceer.buffalo.edu

National Aeronautics and Space Administration
http://www.nasa.gov

National Capital Planning Commission (NCPC)
http://www.ncpc.gov

National Center for Manufacturing Sciences
http://www.ncms.org

National Concrete Masonry Association
http://www.ncma.org

National Conference of States on Building Codes and Standards
http://www.ncsbcs.org

National Council of Structural Engineers Associations (NCSEA)
http://www.ncsea.com/

National Crime Prevention Institute
http://louisville.edu/ncpi

National Fire Protection Association
http://www.nfpa.org

National Institute of Building Sciences (NIBS)
http://www.nibs.org and http://www.wbdg.org

National Park Service, Denver Service Center
http://www.nps.gov/dsc

National Precast Concrete Association
http://www.precast.org

New York City Office of Emergency Management
http://www.nyc.gov/html/oem/html/home/home.shtml

Ohio State University
http://www.osu.edu/homelandsecurity

Pentagon Renovation Program
http://renovation.pentagon.mil

Portland Cement Association (PCA)
http://www.cement.org/

Protective Glazing Council
http://www.protectiveglazing.org

Protective Technology Center at Penn State University
http://www.ptc.psu.edu

SAVE International
http://www.value-eng.org

Society of Fire Protection Engineers
http://www.sfpe.org

Southern Building Code Congress, International
http://www.sbcci.org

Sustainable Buildings Industry Council
http://www.sbicouncil.org

Transportation Research Board/Marine Board
http://www.trb.org

Transportation Security Administration
http://www.tsa.gov

U.S. Air Force Civil Engineer Support Agency
http://www.afcesa.af.mil

U.S. Coast Guard
http://www.uscg.mil

U.S. Department of Energy
http://www.energy.gov

Sandia National Laboratories (SNL)
http://www.sandia.gov

U.S. Department of Health and Human Services
http://www.hhs.gov

U.S. Department of Veterans Affairs (VA)
http://www.va.gov/

U.S. Environmental Protection Agency (EPA), Chemical Emergency Preparedness and Prevention Office (CEPPO)– Counter-terrorism
http://www.epa.gov/ceppo/

U.S. General Services Administration (GSA)
http://www.gsa.gov

U.S. Green Building Council
http://www.usgbc.org

U.S. Marine Corps Headquarters
http://www.marines.mil/unit/hqmc/Pages/default.aspx

U.S. Society on Dams
http://www.ussdams.org

University of Missouri, Department of Civil & Environmental Engineering, National Center for Explosion Resistant Design
http://ncerd.missouri.edu/

Virginia Polytechnic Institute and State University
http://www.vt.edu/

Water and Wastewater Equipment Manufacturers Association
http://www.wwema.org
The Partnership for Critical Infrastructure (PCIS)
http://www.pcis.org
Note: Involved mainly with information systems and not building real property.

Government

Department of Energy (DOE)
http://www.energy.gov

Department of Homeland Security
www.dhs.gov/

National Infrastructure Protection Center (NIPC)
http://www.nipc.gov
Private Sector

Anser Institute for Homeland Security (ANSER)
http://www.homelandsecurity.org

CERT® Coordination Center (CERT/CC)
http://www.cert.org

Electronic Warfare Associates (EWA)
http://www.ewa.com

The Institute for Internal Auditors (IIA)
http://www.theiia.org

National Cyber Security Alliance (Alliance)
http://www.staysafeonline.org/

North American Electric Reliability Council (NERC)
http://www.nerc.com

SANS Institute (SANS - SysAdmin, Audit, Network, Security)
http://www.sans.org

The Financial Services Roundtable Technology Group (BITS)
http://www.bits.org

The U.S. Chamber of Commerce, Center for Corporate Citizenship (CCC)
http://www.uschamber.com/chambers/ccc

Selected States and Local Organizations

Association of Metropolitan Water Agencies
http://www.amwa.net

The Council of State Governments (CSG)
http://www.csg.org

International Association of Emergency Managers (IAEM)
http://www.iaem.com

National Association of State CIOs (NASCIO)
http://www.nascio.org

National Emergency Managers Association (NEMA)
http://www.nemaweb.org

National Governor's Association (NGA)
http://www.nga.org

The National League of Cities (NLC)
http://www.nlc.org

F

Building Vulnerability Assessment Checklist

The Building Vulnerability Assessment Checklist is based on the checklist developed by the Department of Veterans Affairs (VA) and compiles many best practices based on technologies and scientific research to consider during the design of a new building or renovation of an existing building. It allows a consistent security evaluation of designs at various levels. The checklist can be used as a screening tool for preliminary design vulnerability assessment. In addition to examining design issues that affect vulnerability, the checklist includes questions that determine if critical systems continue to function in order to enhance deterrence, detection, denial, and damage limitation, and to ensure that emergency systems function during a threat or hazard situation.

The checklist is organized into the 14 sections listed below. 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. If assessing an existing building, vulnerabilities can also be documented with

The checklist is organized into the 14 sections. 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.

photographs, if possible. The results of the 14 assessments should be integrated into a master vulnerability assessment and provide a basis for determining vulnerability ratings during the assessment process.

1. Site
2. Architectural
3. Structural Systems
4. Building Envelope
5. Utility Systems
6. Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)
7. Plumbing and Gas Systems
8. Electrical Systems
9. Fire Alarm Systems
10. Communications and Information Technology (IT) Systems
11. Equipment Operations and Maintenance
12. Security Systems
13. Security Master Plan
14 COOP Facility: Additional Concerns

Section 1	Vulnerability Question	Guidance	Observations
Site			
Antiterrorism			
1.1	What major structures surround the facility (site or building(s))? What critical infrastructure, government, military, or recreation facilities are in the local area that impact transportation, utilities, and collateral damage (attack at this facility impacting the other major structures or attack on the major structures impacting this facility)? What are the adjacent land uses immediately outside the perimeter of this facility (site or building(s))?	Critical infrastructure to consider includes: **Telecommunications infrastructure** Facilities for broadcast TV, cable TV; cellular networks; newspaper offices, production, and distribution; radio stations; satellite base stations; telephone trunking and switching stations, including critical cable routes and major rights of way **Electric power systems** Power plants, especially nuclear facilities; transmission and distribution system components; fuel distribution, delivery, and storage **Gas and oil facilities** Hazardous material facilities, oil/gas pipelines and storage facilities	

Section 1	Vulnerability Question	Guidance	Observations
Site			
Antiterrorism (cont.)			
1.1	Do future development plans change these land uses outside the facility (site or building (s)) perimeter? Although this question bridges threat and vulnerability, the threat is the man-made hazard that can occur (likelihood and impact) and the vulnerability is the proximity of the hazard to the building(s) being assessed. Thus, a chemical plant release may be a threat/hazard, but vulnerability changes if the plant is 1 mile upwind for the prevailing winds versus 10 miles away and downwind. Similarly, a terrorist attack upon an adjacent building may impact the building(s) being assessed. The Murrah Federal Building in Oklahoma City was not the only building to have severe damage caused by the explosion of the Ryder rental truck bomb.	**Banking and finance institutions** Financial institutions (banks, credit unions) and the business district; note schedule business/financial district may follow; armored car services **Transportation networks** **Airports:** carriers, flight paths, and airport layout; location of air traffic control towers, runways, passenger terminals, and parking areas **Bus Stations** **Pipelines:** oil; gas Trains/Subways: rails and lines, railheads/rail yards, interchanges, tunnels, and cargo/passenger terminals; note hazardous material transported **Traffic:** interstate highways/roads/tunnels/bridges carrying large volumes; points of congestion; note time of day and day of week. **Trucking:** hazardous materials cargo loading/unloading facilities; truck terminals, weigh stations, and rest areas **Waterways:** dams; levees; berths and ports for cruise ships, ferries, roll-on/roll-off cargo vessels, and container ships; international (foreign) flagged vessels (and cargo) **Water supply systems** Pipelines and process/treatment facilities, dams for water collection; wastewater treatment. **Government services** **Federal/state/local government offices:** post offices, law enforcement stations, fire/rescue, town/city hall, local mayor's/governor's residences, judicial offices and courts, military installations (include type-Active, Reserves, National Guard) **Emergency services** Backup facilities, communication centers, Emergency Operations Centers (EOCs), fire/emergency medical service (EMS) facilities, emergency medical centers (EMCs), law enforcement facilities	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.1		The following are not critical infrastructure, but have collateral damage potential to consider: **Agricultural facilities:** chemical distribution, storage, and application sites; crop spraying services; farms and ranches; food processing, storage, and distribution facilities **Commercial manufacturing/industrial facilities:** apartment buildings; business/corporate centers; chemical plants (especially those with Section 302 Extremely Hazardous Substances); factories; fuel production, distribution, and storage facilities; hotels and convention centers; industrial plants; raw material production, distribution, and storage facilities; research facilities and laboratories; shipping, warehousing, transfer, and logistical centers **Events and attractions:** festivals and celebrations; open-air markets; parades; rallies, demonstrations, and marches; religious services; scenic tours; theme parks **Health care system components:** family planning clinics; health department offices; hospitals; radiological material and medical waste transportation, storage, and disposal; research facilities and laboratories, walk-in clinics **Political or symbolically significant sites:** embassies, consulates, landmarks, monuments, political party and special interest groups offices, religious sites **Public/private institutions:** academic institutions, cultural centers, libraries, museums, research facilities and laboratories, schools **Recreation facilities:** auditoriums, casinos, concert halls and pavilions, parks, restaurants and clubs (frequented by potential target populations), sports arenas, stadiums, theaters, malls, and special interest group facilities; note congestion date and times for shopping centers REFERENCE: FEMA 386-7, FEMA SLG 101, DOJ NCJ181200	
1.2	Does the terrain place the building in a depression or low area?	Depressions or low areas can trap heavy vapors, inhibit natural decontamination by prevailing winds, and reduce the effectiveness of in-place sheltering. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.3	In dense, urban areas, does curb lane parking place uncontrolled parked vehicles unacceptably close to a building in public rights-of-way?	Where distance from the building to the nearest curb provides insufficient setback, restrict parking in the curb lane. For typical city streets this may require negotiating to close the curb lane. Setback is common terminology for the distance between a building and its associated roadway or parking. It is analogous to stand-off between a vehicle bomb and the building. The benefit per foot of increased stand-off between a potential vehicle bomb and a building is very high when close to a building and decreases rapidly as the distance increases. Note that the July 1, 1994 Americans with Disabilities Act Standards for Accessible Design states that required handicapped parking shall be located on the shortest accessible route of travel from adjacent parking to an accessible entrance. REFERENCE: GSA PBS-P100	
1.4	Is a perimeter fence or other types of barrier controls in place?	The intent is to channel pedestrian traffic onto a site with multiple buildings through known access control points. For a single building the intent is to have a single visitor entrance. REFERENCE: GSA PBS-P100	
1.5	What are the site access points to the site or building?	The goal is to have at least two access points - one for passenger vehicles and one for delivery trucks due to the different procedures needed for each. Having two access points also helps if one of the access points becomes unusable, then traffic can be routed through the other access point. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
1.6	Is vehicle traffic separated from pedestrian traffic on the site?	Pedestrian access should not be endangered by car traffic. Pedestrian access, especially from public transportation, should not cross vehicle traffic if possible. REFERENCE: GSA PBS-P100 AND FEMA 386-7	
1.7	Is there vehicle and pedestrian access control at the perimeter of the site?	Vehicle and pedestrian access control and inspection should occur as far from facilities as possible (preferably at the site perimeter) with the ability to regulate the flow of people and vehicles one at a time. Control on-site parking with identification checks, security personnel, and access control systems. REFERENCE: FEMA 386-7	
1.8	Is there space for inspection at the curb line or outside the protected perimeter? What is the minimum distance from the inspection location to the building?	Design features for the vehicular inspection point include: vehicle arrest devices that prevent vehicles from leaving the vehicular inspection area and prevent tailgating. If screening space cannot be provided, consider other design features such as: hardening and alternative location for vehicle search/ inspection. REFERENCE: GSA PBS-P100	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.9	Is there any potential access to the site or building through utility paths or water runoff?	Eliminate potential site access through utility tunnels, corridors, manholes, storm water runoff culverts, etc. Ensure covers to these access points are secured. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
1.10	What are the existing types of vehicle anti-ram devices for the site or building? Are these devices at the property boundary or at the building?	Passive barriers include bollards, walls, hardened fences (steel cable interlaced), trenches, ponds/basins, concrete planters, street furniture, plantings, trees, sculptures, and fountains. Active barriers include pop-up bollards, swing arm gates, and rotating plates and drums, etc. REFERENCE: GSA PBS-P100	
1.11	What is the anti-ram buffer zone stand-off distance from the building to unscreened vehicles or parking?	If the recommended distance for the postulated threat is not available, consider reducing the stand-off required through structural hardening or manufacturing additional stand-off through barriers and parking restrictions. Also consider relocation of vulnerable functions within the building or to a more hazard resistant building. More stand-off should be used for unscreened vehicles than for screened vehicles that are searched. REFERENCE: GSA PBS P-100	
1.12	Are perimeter barriers capable of stopping vehicles? Will the vehicle barriers at the perimeter and building maintain access for emergency responders, including large fire apparatus?	Anti-ram protection may be provided by adequately designed: bollards, street furniture, sculpture, landscaping, walls, and fences. The anti-ram protection must be able to stop the threat vehicle size (weight) at the speed attainable by that vehicle at impact. If the anti-ram protection cannot absorb the desired kinetic energy, consider adding speed controls (serpentines or speed bumps) to limit the speed at impact. If the resultant speed is still too great, the anti-ram protection should be improved. REFERENCE: MILITARY HANDBOOK 1013/14 AND GSA PBS P-100	
1.13	Does site circulation prevent high-speed approaches by vehicles?	The intent is to use site circulation to minimize vehicle speeds and eliminate direct approaches to structures. REFERENCE: GSA PBS-P100	
1.14	Are there offsetting vehicle entrances from the direction of a vehicle's approach to force a reduction of speed?	Single or double 90 degree turns effectively reduce vehicle approach speed. REFERENCE: GSA PBS-P100	
1.15	Is there a minimum setback distance between the building and parked vehicles?	Adjacent public parking should be directed to more distant or better-protected areas, segregated from employee parking and away from the building. Some publications use the term setback in lieu of the term stand-off. REFERENCE: GSA PBS-P100	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.16	Does adjacent surface parking onsite maintain a minimum stand-off distance?	The specific stand-off distance needed is based upon the design basis threat bomb size and the building construction. For initial screening, consider using 25 meters (82 feet) as a minimum, with more distance needed for unreinforced masonry or wooden walls. REFERENCE: GSA PBS-P100	
1.17	Do stand-alone, above ground parking garages provide adequate visibility across as well as into and out of the parking garage?	Pedestrian paths should be planned to concentrate activity to the extent possible. Limiting vehicular entry/exits to a minimum number of locations is beneficial. Stair tower and elevator lobby design shall be as open as code permits. Stair and/or elevator waiting areas should be as open to the exterior and/or the parking areas as possible and well lighted. Impact-resistant, laminated glass for stair towers and elevators is one way to provide visual openness. Potential hiding places below stairs should be closed off; nooks and crannies should be avoided, and dead-end parking areas should be eliminated. REFERENCE: GSA PBS-P100	
1.18	Are garage or service area entrances for employee-permitted vehicles protected by suitable anti-ram devices? Coordinate this protection with other anti-ram devices, such as on the perimeter or property boundary to avoid duplication of arresting capability.	Control internal building parking, underground parking garages, and access to service areas and loading docks in this manner with proper access control, or eliminate it altogether. The anti-ram device must be capable of arresting a vehicle of the designated threat size at the speed attainable at the location. REFERENCE: GSA PBS-P100	
1.19	Do site landscaping and street furniture provide hiding places?	Minimize concealment opportunities by keeping landscape plantings (hedges, shrubbery, and large plants with heavy ground cover) and street furniture (bus shelters, benches, trash receptacles, mailboxes, newspaper vending machines) away from the building to permit observation of intruders and prevent hiding of packages. If mail or express boxes are used, the size of the openings should be restricted to prohibit the insertion of packages. REFERENCE: GSA PBS-P100	
1.20	Is the site lighting adequate from a security perspective in roadway access and parking areas?	Security protection can be successfully addressed through adequate lighting. The type and design of lighting, including illumination levels, is critical. Illuminating Engineering Society of North America (IESNA) guidelines can be used. The site lighting should be coordinated with the CCTV system. REFERENCE: GSA PBS-P100	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.21	Is line-of-sight perspectives from outside the secured boundary to the building and on the property along pedestrian and vehicle routes integrated with landscaping and green space?	The goal is to prevent the observation of critical assets by persons outside the secure boundary of the site. For individual buildings in an urban environment, this could mean appropriate window treatments or no windows for portions of the building. Once on the site, the concern is to ensure observation by a general workforce aware of any pedestrians or vehicles outside normal circulation routes or attempting to approach the building unobserved. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
1.22	Do signs provide control of vehicles and people?	The signage should be simple and have the necessary level of clarity. However, signs that identify sensitive areas should generally not be provided. REFERENCE: GSA PBS-P100	
1.23	Are all existing fire hydrants on the site accessible?	Just as vehicle access points to the site must be able to transit emergency vehicles, so too must the emergency vehicles have access to the buildings and, in the case of fire trucks, the fire hydrants. Thus, security considerations must accommodate emergency response requirements. REFERENCE: GSA PBS-P100	
1.24	Is there any in-ground infrastructure in the vicinity of the building? How far in the horizontal direction? How deep in the vertical direction from grade level? Do any of these in-ground infrastructures directly support structurally any part of the building?	In-ground infrastructure can be any of the following: 1. Any structure that can be used by persons, such as subway stations, tunnels, large sewer or water tunnels or pipes. 2. Standard utility lifelines, such as water, gas, steam, sewer, storm-water, electric, communications, etc. See Question 5.22. 3. Ventilation shafts supplying either the building or the in-ground infrastructure. The zone of dynamic effects that can reach the building from an event in the infrastructure is of interest. This zone is defined by the horizontal and vertical distances between the building and the infrastructure of interest. The buried infrastructure and the building will interact through physical structural connections or the soil and water table. REFERENCES: FEMA 430, BOLLINGER 1980 BLAST VIBRATION ANALYSIS AND PRAKASH 1981 SOIL DYNAMICS	

Section 1	Vulnerability Question	Guidance	Observations
Site			
1.25	Is any of the nearby in-ground infrastructure connected to the building? How are theses physical connections made? Can the building be either sealed or isolated at the interface?	On the site, the building and in-ground infrastructure can be physically connected by passageways, subways, tunnels, connectors stairways, entrance/exit portals, ventilation shafts, and by direct utility connections from utility lifelines. These physical connections can have unwarranted security impacts from events in the in-ground infrastructure that then affect the building, such as explosive blast, CBR release, and access control that then enter the building being assessed. An event in the in-ground infrastructure can interact with the building through the soil and water table, in addition to the physical connections. The physical connections could be structurally connected, seismically isolated, or some other method to tie the in-ground infrastructure to the building. REFERENCES: FEMA 430, PRAKASH 1981 SOIL DYNAMICS, AND KRAMER 1996 GEOTECHNICAL EARTHQUAKE ENGINEERING	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.1	Does the site and architectural design incorporate strategies from a Crime Prevention Through Environmental Design (CPTED) perspective?	The focus of CPTED is on creating defensible space by employing: **1. Natural access controls:** • Design streets, sidewalks, and building entrances to clearly indicate public routes and direct people away from private/restricted areas • Discourage access to private areas with structural elements and limit access (no cut-through streets) • Loading zones should be separate from public parking **2. Natural surveillance:** • Design that maximizes visibility of people, parking areas, and building entrances: Doors and windows that look out on to streets and parking areas • Shrubbery under 2 feet in height for visibility • Lower branches of existing trees kept at least ten feet off ground • Pedestrian-friendly sidewalks and streets to control pedestrian and vehicle circulation • Adequate nighttime lighting, especially at exterior doorways	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.1		**3. Territorial reinforcement** • Design that defines property lines • Design that distinguishes private/restricted spaces from public spaces using separation, landscape plantings; pavement designs (pathway and roadway placement); gateway treatments at lobbies, corridors, and door placement; walls, barriers, signage, lighting, and "CPTED" fences • "Traffic-calming" devices for vehicle speed control **4. Target hardening** • Prohibit entry or access: window locks, dead bolts for doors, interior door hinges • Access control (building and employee/visitor parking) and intrusion detection systems • Closed circuit television cameras • Prevent crime and influence positive behavior, while enhancing the intended uses of space. In other words, design that eliminates or reduces criminal behavior and at the same time encourages people to "keep an eye out" for each other. REFERENCE: GSA PBS-P100 AND FEMA 386-7	
2.2	Is it a mixed-tenant building?	Separate high-risk tenants from low-risk tenants and from publicly accessible areas. Mixed uses may be accommodated through such means as separating entryways, controlling access, and hardening shared partitions, as well as through special security operational countermeasures. REFERENCE: GSA PBS-P100	
2.3	Are pedestrian paths planned to concentrate activity to aid in detection?	Site planning and landscape design can provide natural surveillance by concentrating pedestrian activity, limiting entrances/exits, and eliminating concealment opportunities. Also, prevent pedestrian access to parking areas other than via established entrances. REFERENCE: GSA PBS-P100.	
2.4	Are there trash receptacles and mailboxes in close proximity to the building that can be used to hide explosive devices?	The size of the trash receptacles and mailbox openings should be restricted to prohibit insertion of packages. Street furniture, such as newspaper vending machines, should be kept sufficient distance (10 meters or 33 feet) from the building, or brought inside to a secure area. REFERENCES: U.S.AF INSTALLATION FORCE PROTECTION GUIDE, DOD MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS	
2.5	Do entrances avoid significant queuing?	If queuing will occur within the building footprint, the area should be enclosed in blast-resistant construction. If queuing is expected outside the building, a rain cover should be provided. For manpower and equipment requirements collocate or combine staff and visitor entrances. REFERENCE: GSA PBS-P100	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.6	Does security screening cover all public and private areas? Are public and private activities separated? Are public toilets, service spaces, or access to stairs or elevators located in any non-secure areas, including the queuing area before screening at the public entrance?	Retail activities should be prohibited in non-secured areas. However the Public Building Cooperative Use Act of 1976 encourages retail and mixed uses to create open and inviting buildings. Consider separating entryways, controlling access, hardening shared partitions, and special security operational countermeasures. REFERENCE: GSA PBS-P100 AND FEMA 386-7	
2.7	Is access control provided through main entrance points for employees and visitors? (lobby receptionist, sign-in, staff escorts, issue of visitor badges, checking forms of personal identification, electronic access control systems)	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
2.8	Is access to private and public space or restricted area space clearly defined through the design of the space, signage, use of electronic security devices, etc.?	Finishes and signage should be designed for visual simplicity. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
2.9	Is access to elevators distinguished as to those that are designated only for employees and visitors?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
2.10	Do public and employee entrances include space for possible future installation of access control and screening equipment?	These include walk-through metal detectors and x-ray devices, identification check, electronic access card, search stations, and turnstiles. REFERENCE: GSA PBS-P100	
2.11	Do foyers have reinforced concrete walls and offset interior and exterior doors from each other?	Consider for exterior entrances to the building or to access critical areas within the building if explosive blast hazard must be mitigated. REFERENCE: U.S. ARMY TM 5-853	
2.12	Do doors and walls along the line of security screening meet requirements of UL752 "Standard for Safety: Bullet-Resisting Equipment"?	If the postulated threat in designing entrance access control includes rifles, pistols, or shotguns, then the screening area should have bullet-resistance to protect security personnel and uninvolved bystanders. Glass, if present, should also be bullet-resistant. REFERENCE: GSA PBS-P100	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.13	Do circulation routes have unobstructed views of people approaching controlled access points?	This applies to building entrances and to critical areas within the building. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE AND DOD UFC 4-010-01	
2.14	Is roof access limited to authorized personnel by means of locking mechanisms?	REFERENCE: GSA PBS-P100 AND CDC/NIOSH, PUB 2002-139	
2.15	Are critical assets (people, activities, building systems and components) located close to any main entrance, vehicle circulation, parking, maintenance area, loading dock, or interior parking? Are the critical building systems and components hardened?	Critical building components include: • Emergency generator including fuel systems, day tank, fire sprinkler, and water supply; • Normal fuel storage; • Main switchgear; • Telephone distribution and main switchgear; • Fire pumps; • Building control centers; • Uninterruptible Power Supply (UPS) systems controlling critical functions; • Main refrigeration and ventilation systems if critical to building operation; • Elevator machinery and controls; • Shafts for stairs, elevators, and utilities; • Critical distribution feeders for emergency power. Evacuation and rescue require emergency systems to remain operational during a disaster and they should be located away from attack locations. Primary and backup systems should be separated to reduce the risk of both being impacted by a single incident if collocated. Utility systems should be located at least 50 feet from loading docks, front entrances, and parking areas. One way to harden critical building systems and components is to enclose them within hardened walls, floors, and ceilings. Do not place them near high-risk areas where they can receive collateral damage. REFERENCE: GSA PBS-P100	
2.16	Are high-value or critical assets located as far into the interior of the building as possible and separated from the public areas of the building?	Critical assets, such as people and activities, are more vulnerable to hazards when on an exterior building wall or adjacent to uncontrolled public areas inside the building. REFERENCE: GSA PBS-P100	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.17	Is high visitor activity away from critical assets?	High-risk activities should also be separated from low-risk activities. Also, visitor activities should be separated from daily activities. REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
2.18	Are critical assets located in spaces that are occupied 24 hours per day? Are assets located in areas where they are visible to more than one person?	REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
2.19	Are loading docks and receiving and shipping areas separated in any direction from utility rooms, utility mains, and service entrances including electrical, telephone/ data, fire detection/alarm systems, fire suppression water mains, cooling and heating mains, etc.?	Loading docks should be designed to keep vehicles from driving into or parking under the building. If loading docks are in close proximity to critical equipment, consider hardening the equipment and service against explosive blast. Consider a 50-foot separation distance in all directions. REFERENCE: GSA PBS-P100	
2.20	Are mailrooms located away from building main entrances, areas containing critical services, utilities, distribution systems, and important assets? Is the mailroom located near the loading dock?	The mailroom should be located at the perimeter of the building with an outside wall or window designed for pressure relief. By separating the mailroom and the loading dock, the collateral damage of an incident at one has less impact upon the other. However, this may be the preferred mailroom location. Off-site screening stations or a separate delivery processing building on site may be cost-effective, particularly if several buildings may share one mailroom. A separate delivery processing building reduces risk and simplifies protection measures. REFERENCE: GSA PBS-P100	
2.21	Does the mailroom have adequate space available for equipment to examine incoming packages and for an explosive disposal container?	Screening of all deliveries to the building includes U.S. mail, commercial package delivery services, delivery of office supplies, etc. REFERENCE: GSA PBS-P100	
2.22	Are areas of refuge identified, with special consideration given to egress?	Areas of refuge can be safe havens, shelters, or protected spaces for use during specified hazards. REFERENCE: FEMA 386-7	

Section 2	Vulnerability Question	Guidance	Observations
Architecture			
2.23	Are stairwells required for emergency egress located as remotely as possible from high-risk areas where blast events might occur? Are stairways maintained with positive pressure or are there other smoke control systems?	Consider designing stairs so that they discharge into other than lobbies, parking, or loading areas. Maintaining positive pressure from a clean source of air (may require special filtering) aids in egress by keeping smoke, heat, toxic fumes, etc. out of the stairway. Pressurize exit stairways in accordance with the National Model Building Code. REFERENCE: GSA PBS-P100 AND CDC/NIOSH, PUB 2002-139	
2.24	Are enclosures for emergency egress hardened to limit the extent of debris that might otherwise impede safe passage and reduce the flow of evacuees?	Egress pathways should be hardened and discharge into safe areas. REFERENCE: FEMA 386-7	
2.25	Do interior barriers differentiate level of security within a building?	REFERENCE: U.S.AF INSTALLATION FORCE PROTECTION GUIDE	
2.26	Are emergency systems located away from high-risk areas?	The intent is to keep the emergency systems out of harm's way, such that one incident takes out all capability – both the regular systems and their backups. REFERENCE: FEMA 386-7	
2.27	Is interior glazing near high-risk areas minimized? Is interior glazing in other areas shatter resistant?	Interior glazing should be minimized where a threat exists and should be avoided in enclosures of critical functions next to high-risk areas. REFERENCE: GSA PBS-P100	
2.28	Are ceiling and lighting systems designed to remain in place during hazard events?	When an explosive blast shatters a window, the blast wave enters the interior space, putting structural and non-structural building components under loads not considered in standard building codes. It has been shown that connection criteria for these systems in high seismic activity areas resulted in much less falling debris that could injure building occupants. Mount all overhead utilities and other fixtures weighing 14 kilograms (31 pounds) or more to minimize the likelihood that they will fall and injure building occupants. Design all equipment mountings to resist forces of 0.5 times the equipment weight in any direction and 1.5 times the equipment weight in the downward direction. This standard does not preclude the need to design equipment mountings for forces required by other criteria such as seismic standards. REFERENCE: DOD MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.1	What type of construction? What type of concrete and reinforcing steel? What type of steel? What type of foundation?	The type of construction provides an indication of the robustness to abnormal loading and load reversals. A reinforced concrete moment-resisting frame provides greater ductility and redundancy than a flat-slab or flat-plate construction. The ductility of steel frame with metal deck depends on the connection details and pre-tensioned or post-tensioned construction provides little capacity for abnormal loading patterns and load reversals. The resistance of load-bearing wall structures varies to a great extent, depending on whether the walls are reinforced or un-reinforced. There are relative blast loading tables that indicate range of pressure for relative levels of damage to general construction types. There are similar tables for seismic response. For example, wood buildings of all types tend to have great capacity to withstand seismic events, but are much less resilient to explosive blast loading. Un-reinforced masonry is weak in both situations. Cast-in-place concrete has good performance in blast situations, but is not as capable during seismic events. As a rule, if the building is designed for ductile behavior, such as seismic, blast or progressive collapse, it is expected to behave better than non-ductile design. REFERENCES: FEMA 154, PHYSICAL SECURITY ASSESSMENT FOR THE DEPARTMENT OF VETERANS AFFAIRS FACILITIES, BIGGS 1964 INTRODUCTION TO STRUCTURAL DYNAMICS, AND MAYS 1995 BLAST EFFECTS OF BUILDINGS	
3.2	Do the reinforced concrete structures contain symmetric steel reinforcement (positive and negative faces) in all floor slabs, roof slabs, walls, beams, and girders that may be subjected to rebound, uplift, and suction pressures? Do the lap splices fully develop the capacity of the reinforcement? Are lap splices and other discontinuities staggered? Do the connections possess ductile details? Is special shear reinforcement, including ties and stirrups, available to allow large post-elastic behavior?	See Questions 3.13 and 3.14 for other types and concerns of concrete construction. REFERENCE: GSA PBS-P100	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.3	Are the steel frame connections moment connections? Is the column spacing minimized so that reasonably sized members will resist the design loads and increase the redundancy of the system? What are the floor-to-floor heights?	A practical upper level for column spacing is generally 30 feet. Unless there is an overriding architectural requirement, a practical limit for floor-to-floor heights is generally less than or equal to 16 feet. REFERENCE: GSA PBS-P100	
3.4	Are critical elements vulnerable to failure? Are there any interior or exterior structural/ architectural components that, if damage, result in additional failures? Are any of these structural/ architectural components vulnerable either directly or indirectly to explosive blast? What types of connection(s) exist between structural/ architectural component and the general structural system?	The priority for upgrades should be based on the relative importance of structural and non-structural elements that are essential to mitigating injury and damage. **Primary Structural Elements** provide the essential parts of the building's resistance to catastrophic blast loads and progressive collapse. These include columns, girders, roof beams, load-bearing walls, and the main lateral resistance system. **Secondary Structural Elements** consist of all other load-bearing members, such as floor beams, slabs, etc. **Primary Non-Structural Elements** consist of elements (including their attachments) that are essential for life safety systems or elements that can cause substantial injury if failure occurs, including ceilings or heavy suspended mechanical units. **Secondary Non-Structural Elements** consist of all elements not covered in primary non-structural elements, such as partitions, furniture, and light fixtures. There are two types of structural/architectural components that are of concern: 1. A separate structural component that is very dominant within the building (e.g., long span auditorium covers, water tanks, transmission towers, and antennas). Most of such massive components will exceed a fraction of the weight of floor immediately attached to them (25% or more of the weight of the neighboring two-bays). Auditoriums-within a building need special attention, especially if they include a usable floor space on top of them. 2. Structural/architectural components that are not part of the main structural system (e.g., massive awnings, massive signs or flagpoles). When these are damaged the failure mechanism can impact the structural system. An explosive blast that affects these components can cause a disproportionate failure in the building. For this reason, ductile connections are preferred to limit failure. REFERENCES: GSA PBS-P100, IBC 2006, FEMA 430, NAIR 2006 PREVENTING DISPROPORTIONATE COLLAPSE, ACI 318-05, AND AISC 2001 LOAD & RESISTANCE FACTOR DESIGN: MANUAL OF STEEL CONSTRUCTION	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.5	Will the structure suffer an unacceptable level of damage resulting from the postulated threat (blast loading or weapon impact)?	The extent of damage to the structure and exterior wall systems from the bomb threat may be related to a protection level. The following is for new buildings: **Level of Protection Below Antiterrorism Standards - Severe damage.** Frame collapse/massive destruction. Little left standing. Doors and windows fail and result in lethal hazards. Majority of personnel suffer fatalities. **Very Low Level Protection - Heavy damage.** Onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of non-structural elements. Glazing will break and is likely to be propelled into the building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. Majority of personnel suffer serious injuries. There are likely to be a limited number (10 percent to 25 percent) of fatalities. **Low Level of Protection - Moderate damage, un-repairable.** Major deformation of non-structural elements and secondary structural members and minor deformation of primary structural members, but progressive collapse is unlikely. Glazing will break, but fall within 1 meter of the wall or otherwise not present a significant fragment hazard. Doors may fail, but they will rebound out of their frames, presenting minimal hazards. Majority of personnel suffer significant injuries. There may be a few (<10 percent) fatalities. **Medium Level Protection - Minor damage, repairable.** Minor deformations of non-structural elements and secondary structural members and no permanent deformation in primary structural members. Glazing will break, but will remain in the window frame. Doors will stay in frames, but will not be reusable. Some minor injuries, but fatalities are unlikely. **High Level Protection - Minimal damage, repairable.** No permanent deformation of primary and secondary structural members or non-structural elements. Glazing will not break. Doors will be reusable. Only superficial injuries are likely. REFERENCE: DOD UFC 4-010-01	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.6	Is the structure vulnerable to progressive collapse? Is the building capable of sustaining the removal of a column for one floor above grade at the building perimeter without progressive collapse? In the event of an internal explosion in an uncontrolled public ground floor area does the design prevent progressive collapse due to the loss of one primary column? Do architectural or structural features provide a minimum 6-inch stand-off to the internal columns (primary vertical load carrying members)? Are the columns in the unscreened internal spaces designed for an un-braced length equal to two floors, or three floors where there are two levels of parking?	Design to mitigate progressive collapse is an independent analysis to determine a system's ability to resist structural collapse upon the loss of a major structural element or the system's ability to resist the loss of a major structural element. Design to mitigate progressive collapse may be based on the methods outlined in ASCE 7-98 (now 7-02). Designers may apply static and/or dynamic methods of analysis to meet this requirement and ultimate load capacities may be assumed in the analyses. Combine structural upgrades for retrofits to existing buildings, such as seismic and progressive collapse, into a single project due to the economic synergies and other cross benefits. Existing facilities may be retrofitted to withstand the design level threat or to accept the loss of a column for one floor above grade at the building perimeter without progressive collapse. Note that collapse of floors or roof must not be permitted. REFERENCE: GSA PBS-P100	
3.7	Are there adequate redundant load paths in the structure? Are there also adequate redundant load paths for structural/architectural components (described in Question 3.4)?	Special considerations should be given to materials that have inherent ductility and that are better able to respond to load reversals, such as cast-in-place reinforced concrete, reinforced masonry, and steel construction. Careful detailing is required for material such as pre-stressed concrete, pre-cast concrete, and masonry to adequately respond to the design loads. Primary vertical load carrying members should be protected where parking is inside a facility and the building superstructure is supported by the parking structure. Redundant systems are preferred. For example, several cables carrying a massive awning should be supported at different locations within the building structural system. Single girder or truss configurations are less redundant than multiple girders or trusses configurations. The structure should be capable of withstanding the loss of local components without propagating the failure. REFERENCES: GSA PBS-P100, FEMA 430, SMITH 1998 PROGRESSIVE COLLAPSE ANALYSIS AND DESIGN GUIDANCE, AND ETTOUNEY 2004 DEVELOPMENT OF A PROGRESSIVE COLLAPSE TOOL	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.8	Are there transfer girders supported by columns within unscreened public spaces or at the exterior of the building?	Transfer girders allow discontinuities in columns between roof and foundation. This design has inherent difficulty in transferring load to redundant paths upon loss of a column or the girder. Transfer beams and girders that, if lost, may cause progressive collapse are therefore highly discouraged. REFERENCE: GSA PBS-P100	
3.9	What is the grouting and reinforcement of masonry (brick and/or concrete masonry unit (CMU)) exterior walls?	Avoid un-reinforced masonry exterior walls. Reinforcement can run the range of light to heavy depending upon the stand-off distance available and postulated design threat. REFERENCES: GSA PBS-P100 RECOMMENDS FULLY GROUTED AND REINFORCED CMU CONSTRUCTION WHERE CMU IS SELECTED. DOD MINIMUM ANTITERRORISM STANDARDS FOR BUILDINGS STATES "UNREINFORCED MASONRY WALLS ARE PROHIBITED FOR THE EXTERIOR WALLS OF NEW BUILDINGS. A MINIMUM OF 0.05 PERCENT VERTICAL REINFORCEMENT WITH A MAXIMUM SPACING OF 1200 MM (48 IN) WILL BE PROVIDED. FOR EXISTING BUILDINGS, IMPLEMENT MITIGATING MEASURES TO PROVIDE AN EQUIVALENT LEVEL OF PROTECTION." [THIS IS LIGHT REINFORCEMENT AND BASED UPON THE RECOMMENDED STAND-OFF DISTANCE FOR THE SITUATION.]	
3.10	Will the loading dock design limit damage to adjacent areas and vent explosive force to the exterior of the building?	Design the floor of the loading dock for blast resistance if the area below is occupied or contains critical utilities. REFERENCE: GSA PBS-P100	
3.11	Are mailrooms, where packages are received and opened for inspection, and unscreened retail spaces designed to mitigate the effects of a blast on primary vertical or lateral bracing members?	Where mailrooms and unscreened retail spaces are located in occupied areas or adjacent to critical utilities, walls, ceilings, and floors, they should be blast- and fragment- resistant. Methods to facilitate the venting of explosive forces and gases from the interior spaces to the outside of the structure may include blow-out panels and window system designs that provide protection from blast pressure applied to the outside, but that readily fail and vent if exposed to blast pressure on the inside. REFERENCE: GSA PBS-P100	
3.12	Is the structural/architectural component components (described in Question 3.4) an integral part of the original building? Is it an added feature? Was it designed to resist any abnormal loading?	An integrated design tends to ensure adequate connection detailing. Add-on construction might need an in-depth investigation to the adequacy of the joints between older and newer construction. REFERENCE: FEMA 430	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.13	Are pre-cast concrete units used as a part of the structural system of the building? Are the pre-cast connections ductile? Can the system resist progressive collapse that might result from postulated threats?	The progressive collapse of pre-cast concrete buildings, such as the Ronan point event in the United Kingdom and Khobar Towers in Saudi Arabia, showed the importance of adequate connection detailing for that type of construction. The fact that the collapse was limited to the front load-bearing walls at Khobar Towers, while the collapse spread up- and down- the height of the building at Ronan Point show the need for considering the interrelationship between the postulated threat and the expected progression of collapse. Non-ductile connections at Ronan Point changed UK design standards resulting in ductile connections at Khobar Towers using the updated UK standards. REFERENCES: SMITH 1998 PROGRESSIVE COLLAPSE ANALYSIS AND DESIGN GUIDANCE AND ETTOUNEY 1998 INTEGRATED STUDY OF PROGRESSIVE COLLAPSE OF BUILDINGS	
3.14	Are there any pre-stressed or post-tensioned concrete components in the structural system? What type of components? Are any parts of those components vulnerable to bomb blast? How far into the building do the pre-stressed or post-tensioned tendons extend?	Pre-stressed or post-tensioned concrete construction imparts high energy in the cables, and ties long sections of the building together. A sudden loss of a cable can produce damage and loss of load carrying capability over a disproportionate large part of the structure. The end anchors should be specially protected from potential blast situations. REFERENCE: COLLINS 1990 PRE-STRESSED CONCRETE STRUCTURES	
3.15	What is the main lateral stability system, or systems, for this building? Are any of these systems vulnerable to explosive blast at any building level? For steel bracing, concrete shear wall, or any combination of either of these two systems, how far are the bracing bays/shear walls separated from each other? Has this building been evaluated for seismic redundancy?	The well-being of lateral stability systems in buildings is an essential requisite for avoiding progressive collapse. The lateral stability components such as bracing, reinforced concrete shear walls, and reinforced masonry shear walls, must be protected from adverse explosive blast conditions. The lateral stability systems are usually placed in several bays of the building. It is advisable to place these lateral bracing systems away from each other. The separation of lateral systems from each other would ensure that if one of the systems fails due to a blast event, the other systems would survive. A measure of lateral global stability will still be in effect. Placing all of the global lateral stability system close to each other might result in losing all of them during a blast event, thus exposing the building to global loss of stability. The required separation of lateral systems will depend on the postulated threat. However, it might be a good practice to place some measure of lateral resisting systems at the four corners of the building as a minimum. See Question 3.7 for additional redundancy information. REFERENCES: IBC 2006 AND ETTOUNEY 2006 GLOBAL SYSTEM CONSIDERATIONS FOR PROGRESSIVE COLLAPSE	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.16	Is the structural framing system of the inverted pyramid style? If so, what are the types of connections use at the edges of the building? Are there any special provisions taken to accommodate the inverted-pyramid geometry during blast or progressive collapse events?	In an inverted pyramid style construction, the weight and the area of floors increase for higher floors. This represents additional and non-standard demands on the structural system. Such demands increase the potential of progressive collapse of the building. The basic problem in inverted pyramid type geometry is that the geometry itself does not lend itself to standardized beam/column geometry in a conventional construction. For example, the loss of support at a lower level will result in a longer equivalent cantilever length for the higher levels. Such longer length will result in a non-standard moments on the interior connections. These non-standard moment demands will require special attention. For example, stronger moment connections, additional intermediate columns, or additional bracings might be needed. REFERENCE: FEMA 430	
3.17	How many floors (vertical) and bays (in both horizontal directions)? What is the height-to width, and height-to depth ratio of the overall building?	Slender buildings are more susceptible to progressive collapse than wider buildings. If the building is irregular, then the controlling parameter to this question is the ground floor level. REFERENCE: ETTOUNEY 2004 DEVELOPMENT OF A PROGRESSIVE COLLAPSE TOOL	
3.18	What are the structural system types of the in-ground infrastructures in the vicinity of the building? Are the construction material or construction details ductile?	Structural systems of underground infrastructures include reinforced concrete tunnels, steel tunnels, and steel or reinforced concrete frames. Some modern construction includes pre-stressed or post-tensioned constructions. Some older underground infrastructures were built using masonry, brick or limestone walls or abutments. Older masonry brick construction can be less ductile than modern reinforced concrete or steel construction. REFERENCE: WINTERKORN 1975 FOUNDATION ENGINEERING HANDBOOK	
3.19	What is the soil types encompassing the building and the in-ground infrastructures?	Soil conditions can have major effects during explosive blast. Weak soils (such as landfill or loose sand) can fail easily, but will not propagate blast effects for long distances. Strong soils (such as stiff sand or hard rock) will not fail as easily, but the blast effects will be felt at longer distances. Similarly, soils can affect CBR agent transfer whereby porous soils could allow lighter-than-air agents to rise to the surface, while dense soils could force the agents to follow the path of the utility lifeline, allowing agent to enter the building. This is why natural gas utility service entrances must come out of the ground before entering a building so that gas following the piping vents to atmosphere and does not enter the building to accumulate to explosive levels. REFERENCES: BOLLINGER 1980 BLAST VIBRATION ANALYSIS AND ETTOUNEY 1998 EARTHQUAKE DESIGN VS. BLAST DESIGN – A SHORT COMPARISON	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.20	What are the maximum and minimum water table levels within the site (relative to the ground level on each side of the building)? Would a breach in any building wall below water table cause unacceptable flooding? Are there any interior or exterior liners?	Presence of underground water can have negative and unexpected effects on underground infrastructure and nearby buildings. Attenuation of blast pressures in wet soil is much lower than that in dry soil. Also, blast pressures can reflect from the surface of the underground water table, creating an undesirable vertically propagating blast wave that will hit the building from the bottom, causing uplift of part or the whole building (an unexpected loading direction). REFERENCES: FEMA 430, WINTERKORN 1975 FOUNDATION ENGINEERING HANDBOOK, AND BROWN 1996 PRACTICAL FOUNDATION ENGINEERING	
3.21	Would failure of part of the in-ground infrastructure affect the structural system of the building? Would failure of part of the in-ground infrastructure physical connections to the building affect the structural system of the building and/or the structural system of the in-ground infrastructures? Would this failure initiate progressive collapse in the building and/or the in-ground infrastructure? Are any mitigation measures (hardening included) installed to limit these failures?	When the infrastructure and the building are in close proximity, or when they are rigidly linked, the failure of one system might initiate the failure of the other system. Similarly, a failure in the physical connection between the in-ground infrastructure and the building might cause failure in both the building and in-ground infrastructures The part of the structure closest to the in-ground infrastructure is the most vulnerable. It should be hardened so that any local failure would not initiate progressive collapse in the rest of the building. Aside from hardening, other measures available are increased ductility, increased setback, or better access control. REFERENCES: FEMA 430, SMITH 1998 PROGRESSIVE COLLAPSE ANALYSIS AND DESIGN GUIDANCE, AND ETTOUNEY 2004 DEVELOPMENT OF A PROGRESSIVE COLLAPSE TOOL	
3.22	Are there any retaining walls, moats, or any other structural constructs that lay between the in-ground infrastructure and the building? When were these constructs built? Were ductile features accommodated while designing these constructs?	There can be architectural or structural features between the building and the in-ground infrastructure that is not physically connected to either the building or the infrastructure. Such architectural or structural features can act as a conduit of stress waves between the infrastructure and the building, even if they are not directly connected to either. For example a retaining wall that functions as a noise barrier will not be directly connected to either the building or the in-ground infrastructure, yet in case of blast pressure within the soil, the presence of this wall can re-focus the blast pressure and damage the structures in the vicinity. Moats can also have similar effects. When these constructs were built can indicate if they were part of the original design or a hardening feature for one tactic that could have a negative effect for another tactic. REFERENCES: WINTERKORN 1975 FOUNDATION ENGINEERING HANDBOOK AND BOLLINGER 1980 BLAST VIBRATION ANALYSIS	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.23	How the redundancy of the structural system is achieved?	Redundancy of the structural system is needed to reduce propensity of the system to progression of collapse. Note that redundancy is needed for both vertical (gravity) loads and horizontal (such as blast, wind and seismic) loads. REFERENCES: INTERNATIONAL BUILDING CODE, (IBC) 2003, AND ETTOUNEY, M., SMILOWITZ, R., TANG, M., AND HAPIJ, A., (2006) "GLOBAL SYSTEM CONSIDERATIONS FOR PROGRESSIVE COLLAPSE WITH EXTENSIONS TO OTHER NATURAL AND MAN-MADE HAZARDS," ASCE J. OF CONSTRUCTED FACILITIES, VOL. 20, NO. 4.	
3.24	Are there any unusually special structural components with long spans in the building? How are these long span components connected to the main structural system of the building? Are these connections adequate and in good condition?	Some buildings have components that serve special functions such as auditoriums, inside cafeterias, or sport halls. Such special functions may require unusually high columns or long span beams, arches or trusses. In such a situation, special considerations for blast and progressive collapse designs must be provided. REFERENCES: INTERNATIONAL BUILDING CODE, (IBC) 2003.	
3.25	Is there any high performance / advanced materials (such as high performance concrete or steel) used in the structural system? How are such high performance materials incorporated in the design or detailing within conventional materials?	High performance concrete or steel is being increasingly used in retrofitting existing buildings or in the construction of new buildings. The presence of such materials is an indication of robust structural behavior. Attention is needed when the structural system REFERENCES: "HIGH-PERFORMANCE CEMENT-BASED CONCRETE COMPOSITES: PROCEEDINGS OF THE INDO-U.S. WORKSHOP ON HIGH-PERFORMANCE CEMENT-BASED CONCRETE COMPOSITES," CHENNAI, INDIA (2005) BY JOSEPH J. BIERNACKI, SURENDRA P. SHAH, N. LAKSHMANAN, S. GOPALAKRISHNAN	
3.26	Are there any modern structural components in the structural system?	Lately, there has been an influx of innovative modern structural systems. Such innovative system includes, but not limited to: Pre-stressed masonry columns, Steel Plate Shear walls or special devices for steel bracing. The incorporation of such innovative structural solutions improves structural performance. It also requires special considerations when designing for blast or progressive collapse. REFERENCES: "SHEAR WALL DESIGN GUIDE," AMERICAN IRON AND STEEL INSTITUTE, 1998.	
3.27	Is the building located in a dense urban setting?	Dense urban settings (urban canyons) can affect the blast pressure computations; thus affect the building response to explosive devices. Special care is needed when computing the blast response of buildings in an urban canyon setting. REFERENCES: MAYS, G.C. AND SMITH, P.D. (1995). BLAST EFFECTS OF BUILDINGS: DESIGN OF BUILDINGS TO OPTIMIZE RESISTANCE TO BLAST LOADING. LONDON.	

Section 3	Vulnerability Questions	Guidance	Observations
Structural Systems			
3.28	Is the design of the structural system conformant with the EISA?	Energy Independence and Security Act of 2007 (EISA) stipulates that building designs should accommodate a balance of resource consumption, durability, functionality, and maintainability. REFERENCES: HIGH PERFORMANCE BUILDING COUNCIL (HPBC) PROGRAM IS MANAGED BY NATIONAL INSTITUTE OF BUILDING SCIENCES. HPBC OBJECTIVE IS TO PROMOTE HIGH PERFORMANCE BUILDINGS.	
3.29	Are there considerations to improve building resiliency?	Structures with higher redundancy and hardening levels have higher resiliency. REFERENCES: BRUNEAU, M, AND REINHORN, A. "EXPLORING THE CONCEPT OF SEISMIC RESILIENCE FOR ACUTE CARE FACILITIES," EARTHQUAKE ENGINEERING RESEARCH INSTITUTE, EARTHQUAKE SPECTRA, VOL. 23, NO. 1, 2007 AND ALAMPALLI, S, AND ETTOUNEY, M., "RESILIENCY OF BRIDGES: A DECISION MAKING TOOL," BRIDGE STRUCTURES, JOURNAL, IOS PRESS.	

Section 4	Vulnerability Questions	Guidance	Observations
Building Envelope			
4.1	What is the designed or estimated protection level of the exterior walls against the postulated explosive threat?	The performance of the façade varies to a great extent on the materials. Different construction includes brick or stone with block back-up, steel stud walls, pre-cast panels, curtain wall with glass, stone, or metal panel elements. Shear walls that are essential to the lateral and vertical load bearing system and that also function as exterior walls should be considered primary structures and should resist the actual blast loads predicted from the threats specified. Where exterior walls are not designed for the full design loads, special consideration shall be given to construction types that reduce the potential for injury. REFERENCE: GSA PBS-P100	

Section 4	Vulnerability Questions	Guidance	Observations
Building Envelope			
4.2	Is there less than 40 % fenestration openings per structural bay? Is the window system design on the exterior façade balanced to mitigate the hazardous effects of flying glazing following an explosive event? - (glazing, frames, anchorage to supporting walls, etc.) Do the glazing systems with a ½-inch (3/4-inch better) bite contain an application of structural silicone? Is the glazing laminated or is it protected with an anti-shatter (fragment retention) film? If an anti-shatter film is used, is it a minimum of a 7-mil thick film, or specially manufactured 4-mil thick film?	The performance of the glass will similarly depend on the materials. Glazing may be single pane or double pane, monolithic or laminated, annealed, heat strengthened or fully tempered. The percent fenestration is a balance between protection level, cost, the architectural look of the building within its surroundings, and building codes. One goal is to keep fenestration to below 40% of the building envelope vertical surface area, but the process must balance differing requirements. A blast engineer may prefer no windows, an architect may favor window curtain walls, building codes require so much fenestration per square footage of floor area, fire codes require a prescribed window opening area if the window is a designated escape route, and the building owner has cost concerns. Ideally, an owner would want 100% of the glazed area to provide the design protection level against the postulated explosive threat (design basis threat – weapon size at the expected stand-off distance). However, economics and geometry may allow 80% to 90% due to the statistical differences in the manufacturing process for glass or the angle of incidence of the blast wave upon upper story windows (4th floor and higher). See Question 4.7 for another perspective on glazing. REFERENCE: GSA PBS-P100	
4.3	Do the walls, anchorage, and window framing fully develop the capacity of the glazing material selected? Are the walls capable of withstanding the dynamic reactions from the windows? Will the anchorage remain attached to the walls of the building during an explosive event without failure? Is the façade connected to back-up block or to the structural frame? Are non-bearing masonry walls reinforced?	Government produced and sponsored computer programs coupled with test data and recognized dynamic structural analysis techniques may be used to determine whether the glazing either survives the specified threats or the post damage performance of the glazing protects the occupants. A breakage probability no higher than 750 breaks per 1,000 may be used when calculating loads to frames and anchorage. The intent is to ensure the building envelope provides relatively equal protection against the postulated explosive threat for the walls and window systems for protection of the occupants, especially in rooms with exterior walls. See Questions 3.13 and 3.14 for other types and concerns of concrete construction. REFERENCE: GSA PBS-P100	

Section 4	Vulnerability Questions	Guidance	Observations
Building Envelope			
4.4	Does the building contain ballistic glazing? Does the ballistic glazing meet the requirements of UL 752 Bullet-Resistant Glazing? Does the building contain security-glazing? Does the security-glazing meet the requirements of ASTM F1233 or UL 972, Burglary Resistant Glazing Material? Do the window assemblies containing forced entry resistant glazing (excluding the glazing) meet the requirements of ASTM F 588?	Glass-clad polycarbonate or laminated polycarbonate are two types of acceptable glazing material. If windows are upgraded to bullet-resistant, burglar-resistant, or forced entry- resistant, then ensure that doors, ceilings, and floors, as applicable, can resist the same for the areas of concern. REFERENCE: GSA PBS-P100	
4.5	Do non-window openings, such as mechanical vents and exposed plenums, provide the same level of protection required for the exterior wall?	In-filling of blast over-pressures must be considered through non-window openings such that structural members and all mechanical system mountings and attachments should resist these interior fill pressures. These non-window openings should also be as secure as the rest of the building envelope against forced entry. REFERENCE: GSA PBS-P100	
4.6	What is the basic construction of the building envelope? Are there any seismic gaps between the envelope and the structural framing? Are interactions between out of plane forces (for example, wind or blast pressures) and in-plane forces (for example, seismic forces) accounted for in the design of the connections between the envelope and the structural system? What wind speed/wind pressure was used to design the building?	Types of envelope construction include prefabricated concrete units, aluminum frames, CMUs (concrete masonry unit), etc. Seismic gaps would permit independent lateral movement between the wall and the structure; they might not be adequate for high pressures, such as very high winds or blast situations. In fact, seismic gaps need careful detailing so as to not cause loss of wall support during dynamic blast situations that stress the flexibility of the wall system. The wind speed/wind pressure used to design a building would indicate the adequacy of the components of the building envelope during a blast event. For example, Miami-Dade County Florida hurricane code calls for design to 146 miles per hour (mph) wind speed and wind-borne debris protection (9 pound wooden 2x4 at 34 mph and 0.07 ounce steel sphere at 89 mph) indicates an improved response to explosive blast compared to standard construction. REFERENCE: IBC 2006	

Section 4	Vulnerability Questions	Guidance	Observations
Building Envelope			
4.7	What is the current condition of the window glazing? What is the current condition of the rest of the envelope: cladding, curtain walls, veneer, etc.?	Window, glazing, and building envelope design information is sometimes not well coordinated between architects and structural engineers for assessment of explosive blast response. During the interview process, a review of problems (leaks, glass falling out, loss of seal between double pane glass, window operating difficulties, etc.) and retrofits undertaken to overcome these problems can provide valuable assessment information. REFERENCE: FEMA 430	

Section 5	Vulnerability Questions	Guidance	Observations
Utility Systems			
5.1	What is the source of domestic water? (utility, municipal, wells, lake, river, storage tank) Is there a secure alternate drinking water supply?	Domestic water is critical for continued building operation. While bottled water can satisfy requirements for drinking water and minimal sanitation, domestic water meets many other needs – flushing toilets, building heating and cooling system operation, cooling of emergency generators, humidification, etc. REFERENCE: FEMA 386-7	
5.2	Are there multiple entry points for the water supply?	If the building or site has only one source of water entering at one location, the entry point should be secure. REFERENCE: GSA PBS-P100	
5.3	Is the incoming water supply in a secure location?	Ensure that only authorized personnel have access to the water supply and its components. REFERENCE: FEMA 386-7	
5.4	Does the building or site have storage capacity for domestic water? How many gallons and how long will it allow operations to continue?	Operational facilities will require reliance on adequate domestic water supply. Storage capacity can meet short-term needs and use water trucks to replenish for extended outages. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES.	
5.5	What is the source of water for the fire suppression system? (local utility company lines, storage tanks with utility company backup, lake, or river) Are there alternate water supplies for fire suppression?	The fire suppression system water may be supplied from the domestic water or it may have a separate source, separate storage, or non-potable alternate sources. For a site with multiple buildings, the concern is that the supply should be adequate to fight the worst case situation according to the fire codes. Recent major construction may change that requirement. REFERENCE: FEMA 386-7	

Section 5	Vulnerability Questions	Guidance	Observations
Utility Systems			
5.6	Is the fire suppression system adequate, code-compliant, and protected (secure location)?	Standpipes, water supply control valves, and other system components should be secure or supervised. REFERENCE: FEMA 386-7	
5.7	Do the sprinkler/standpipe interior controls (risers) have fire- and blast-resistant separation? Are the sprinkler and standpipe connections adequate and redundant? Are there fire hydrant and water supply connections near the sprinkler/standpipe connections?	The incoming fire protection water line should be encased, buried, or located 50 feet from high-risk areas. The interior mains should be looped and sectionalized. REFERENCE: GSA PBS-P100	
5.8	Are there redundant fire water pumps (e.g., one electric, one diesel)? Are the pumps located apart from each other?	Collocating fire water pumps puts them at risk for a single incident to disable the fire suppression system. REFERENCE: GSA PBS-P100 AND FEMA 386-7	
5.9	Are sewer systems accessible? Are they protected or secured?	Sanitary and storm water sewers should be protected from unauthorized access. The main concerns are backup or flooding into the building, causing a health risk, shorting out electrical equipment, and loss of building use. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.10	What fuel supplies do the building rely upon for critical operation?	Typically, natural gas, propane, or fuel oil is required for continued operation. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.11	How much fuel is stored on the site or at the building and how long can this quantity support critical operations? How is it stored? How is it secured?	Fuel storage protection is essential for continued operation. Main fuel storage should be located away from loading docks, entrances, and parking. Access should be restricted and protected (e.g., locks on caps and seals). REFERENCE: GSA PBS-P100 AND PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.12	Where is the fuel supply obtained? How is it delivered?	The supply of fuel is dependent on the reliability of the supplier. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 5	Vulnerability Questions	Guidance	Observations
Utility Systems			
5.13	Are there alternate sources of fuel? Can alternate fuels be used?	Critical functions may be served by alternate methods if normal fuel supply is interrupted. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.14	What is the normal source of electrical service for the site or building?	Utilities are the general source unless co-generation or a private energy provider is available. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.15	Is there a redundant electrical service source? Can the site or buildings be fed from more than one utility substation?	The utility may have only one source of power from a single substation. There may be only single feeders from the main substation. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.16	How may service entry points does the site or building have for electricity?	Electrical supply at one location creates a vulnerable situation unless an alternate source is available. Ensure disconnecting requirements according to NFPA 70 (National Fire Protection Association, National Electric Code) are met for multiple service entrances. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.17	Is the incoming electric service to the building secure?	Typically, the service entrance is a locked room, inaccessible to the public. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.18	What provisions for emergency power exist? What systems receive emergency power and have capacity requirements been tested? Is the emergency power collocated with the commercial electric service? Is there an exterior connection for emergency power?	Besides installed generators to supply emergency power, portable generators or rental generators available under emergency contract can be quickly connected to a building with an exterior quick disconnect already installed. Testing under actual loading and operational conditions ensures the critical systems requiring emergency power receive it with a high assurance of reliability. REFERENCE: GSA PBS-P10	
5.19	By what means does the main telephone and data communications interface the site or building?	Typically, communication ducts or other conduits are available. Overhead service is more identifiable and vulnerable REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 5	Vulnerability Questions	Guidance	Observations
Utility Systems			
5.20	Are there multiple or redundant locations for the telephone and communication service?	Secure locations of communications wiring entry to the site or building are required. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.21	Does the fire alarm system require communication with external sources? By what method is the alarm signal sent to the responding agency? (telephone, radio, etc) Is there an intermediary alarm monitoring center?	Typically, the local fire department responds to an alarm that sounds at the station or is transmitted over phone lines by an auto dialer. An intermediary control center for fire, security, and/or building system alarms may receive the initial notification at an on-site or off-site location. This center may then determine the necessary response and inform the responding agency. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
5.22	Are utility lifelines aboveground, underground, or direct buried? Are these lifelines nearby? How far (vertical and horizontal) in-ground or aboveground? How are utility lifelines service entrances attached? Do any utility lifelines allow physical access to the building? Are these attachments sealed to prevent infiltration of CBR agents and secure to prevent personnel access?	Utility lifelines (water, power, communications, etc.) can be protected by concealing, burying, or encasing. Based upon the size of the lifeline, access to the site may be possible, such as larger sewer systems. Based upon the size of the utility service entrance into the building, the utility lifelines can allow personnel or CBR agents to enter the building. Some lifelines nearby, but not connected to the building, can still pose a threat to the building (such as a natural gas pipeline). REFERENCES: GSA PBS-P100, FEMA 386-7, FEMA 430, AND O'ROURKE 1999 RESPONSE OF BURIED PIPELINES SUBJECTED TO EARTHQUAKE EFFECTS	

Section 6	Vulnerability Questions	Guidance	Observations
Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)			
6.1	Where are the air intakes and exhaust louvers for the building? (low, high, or midpoint of the building structure) Are the intakes and exhausts accessible to the public?	Air intakes should be located on the roof or as high as possible. Otherwise secure within CPTED-compliant fencing or enclosure. The fencing or enclosure should have a sloped roof to prevent throwing anything into the enclosure near the intakes. REFERENCES: GSA PBS-P100 states that air intakes should be on the fourth floor or higher and on buildings with three floors or less, they should be on the roof or as high as practical. Locating intakes high on a wall is preferred over a roof location. DOD UFC 4-010-01 states that, for all new inhabited buildings covered by this document, all air intakes should be located at least 3 meters (10 feet) above the ground. CDC/NIOSH, PUB 2002-139 states: "An extension height of 12 feet (3.7 •) will place the intake out of reach of individuals without some assistance. Also, the entrance to the intake should be covered with a sloped metal mesh to reduce the threat of objects being tossed into the intake. A minimum slope of 45° is generally adequate. Extension height should be increased where existing platforms or building features (i.e., loading docks, retaining walls) might provide access to the outdoor air intakes. LBNL PUB-51959: Exhausts are also a concern during an outdoor release, especially if exhaust fans are not in continuous operation, due to wind effects and chimney effects (air movement due to differential temperature)	
6.2	Is roof access limited to authorized personnel by means of locking mechanisms? Is access to mechanical areas similarly controlled?	Roofs are like entrances to the building and are like mechanical rooms when HVAC is installed. Adjacent structures or landscaping should not allow access to the roof. REFERENCES: GSA PBS-P100, CDC/NIOSH, PUB 2002-139, AND LBNL PUB 51959	
6.3	Are there multiple air intake locations?	Single air intakes may feed several air handling units. Indicate if the air intakes are localized or separated. Installing low-leakage dampers is one way to provide the system separation when necessary. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 6	Vulnerability Questions	Guidance	Observations
Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)			
6.4	What are the types of air filtration? Include the efficiency and number of filter modules for each of the main air handling systems. Is there any collective protection for chemical, biological, and radiological contamination designed into the building?	MERV – Minimum Efficiency Reporting Value HEPA – High Efficiency Particulate Air - Activated charcoal for gases - Ultraviolet C for biologicals Consider mix of approaches for optimum protection and cost effectiveness. REFERENCE: CDC/NIOSH, PUB 2002-139	
6.5	Is there space for larger filter assemblies on critical air handling systems?	Air handling units serving critical functions during continued operation may be retrofitted to provide enhanced protection during emergencies. However, upgraded filtration may have negative effects upon the overall air handling system operation, such as increased pressure drop. REFERENCE: CDC/NIOSH, PUB 2002-139	
6.6	Are there provisions for air monitors or sensors for chemical or biological agents?	Duct mounted sensors are found in limited cases generally in laboratory areas. Sensors generally have a limited spectrum of high reliability and are costly. Many different technologies are undergoing research to provide capability REFERENCE: CDC/NIOSH, PUB 2002-139	
6.7	By what method is air intakes and exhausts closed when not operational?	Motorized (low-leakage, fast-acting) dampers are the preferred method for closure with fail-safe to the closed position so as to support in-place sheltering. REFERENCES: CDC/NIOSH, PUB 2002-139 AND LBNL PUB 51959	
6.8	How are air-handling systems zoned? What areas and functions does each of the primary air handling systems serve?	Understanding the critical areas of the building that must continue functioning focuses security and hazard mitigation measures. Applying HVAC zones that Isolate lobbies, mailrooms, loading docks, and other entry and storage areas from the rest of the building HVAC zones and maintaining negative pressure within these areas will contain CBR releases. Identify common return systems that service more than one zone, effectively making a large single zone. Conversely, emergency egress routes should receive positive pressurization to ensure contamination does not hinder egress. Consider filtering of the pressurization air. REFERENCES: CDC/NIOSH, PUB 2002-139 AND LBNL PUB 51959	
6.9	Are there large central air handling units or are there multiple units serving separate zones?	Independent units can continue to operate if damage occurs to limited areas of the building. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 6	Vulnerability Questions	Guidance	Observations
Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)			
6.10	Are there any redundancies in the air handling system? Can critical areas be served from other units if a major system is disabled?	Redundancy reduces the security measures required compared to a non-redundant situation. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
6.11	Is the air supply to critical areas compartmentalized? Similarly, are the critical areas or the building as a whole, considered tight with little or no inleakage?	During chemical, biological, and radiological situations the intent is to either keep the contamination localized in the critical area or prevent its entry into other critical, non-critical, or public areas. Systems can be cross-connected through building openings (doorways, ceilings, partial wall)), ductwork leakage, or pressure differences in air handling system. In standard practice, there is almost always some air carried between ventilation zones by pressure imbalances, due to elevator piston action, chimney effect, and wind effects. Smoke testing of the air supply to critical areas may be necessary. REFERENCES: CDC/NIOSH, PUB 2002-139 AND LBNL PUB 51959	
6.12	Are supply, return, and exhaust air systems for critical areas secure? Are all supply and return ducts completely connected to their grilles and registers and secure? Is the return air not ducted?	The air systems to critical areas should be inaccessible to the public, especially if the ductwork runs through the public areas of the building. It is also more secure to have a ducted air handling system versus sharing hallways and plenums above drop ceilings for return air. Non-ducted systems provide greater opportunity for introducing contaminants. REFERENCES: CDC/NIOSH, PUB 2002-139 AND LBNL PUB 51959	
6.13	What is the method of temperature and humidity control? Is it localized or centralized?	Central systems can range from monitoring only to full control. Local control may be available to override central operation. Of greatest concern are systems needed before, during, and after an incident that may be unavailable due to temperature and humidity exceeding operational limits (e.g. main telephone switch room). REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
6.14	Where are the building automation control centers and cabinets located? Are they in secure areas? How is the control wiring routed?	Access to any component of the building automation and control system could compromise the functioning of the system, increasing vulnerability to a hazard or precluding their proper operation during a hazard incident. The HVAC and exhaust system controls should be in a secure area that allows rapid shutdown or other activation based upon location and type of attack. REFERENCES: FEMA 386-7, DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1 AND LBNL PUB 51959	

Section 6	Vulnerability Questions	Guidance	Observations
Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)			
6.15	Does the control of air handling systems support plans for sheltering in place or other protective approach?	The micro-meteorological effects of buildings and terrain can alter travel and duration of chemical agents and hazardous material releases. Shielding in the form of sheltering in place can protect people and property from harmful effects. To support in-place sheltering, the air handling systems require the ability for authorized personnel to rapidly turn off all systems. However, if the system is properly filtered, then keeping the system operating will provide protection as long as the air handling system does not distribute an internal release to other portions of the building. REFERENCE: CDC/NIOSH, PUB 2002-139	
6.16	Are there any smoke evacuation systems installed? Does it have purge capability?	For an internal blast, a smoke removal system may be essential, particularly in large, open spaces. The equipment should be located away from high risk areas, the system controls and wiring should be protected, and it should be connected to emergency power. This exhaust capability can be built into areas with significant risk on internal events, such as lobbies, loading docks, and mailrooms. Consider filtering of the exhaust to capture CBR contaminants. REFERENCES: GSA PBS-P100, CDC/NIOSH, PUB 2002-139, AND LBNL PUB 51959	
6.17	Where is roof-mounted equipment located on the roof? (near perimeter, at center of roof)	Roof-mounted equipment should be kept away from the building perimeter. REFERENCE: U.S. ARMY TM 5-853	
6.18	Are fire dampers installed at all fire barriers? Are all dampers functional and seal well when closed?	All dampers (fire, smoke, outdoor air, return air, bypass) must be functional for proper protection within the building during an incident. REFERENCE: CDC/NIOSH, PUB 2002-139	
6.19	Do fire walls and fire doors maintain their integrity?	The tightness of the building (both exterior, by weatherization to seal cracks around doors and windows, and internal – by zone ducting, fire walls, fire stops, and fire doors) provide energy conservation benefits and functional benefits during a CBR incident. REFERENCE: LBNL PUB 51595	
6.20	Do elevators have recall capability and elevator emergency message capability?	Although a life-safety code and fire response requirement, the control of elevators also has benefit during a CBR incident. The elevators generate a piston effect causing pressure differentials in the elevator shaft and associated floors that can force contamination to flow up or down. REFERENCE: LBNL PUB 51959	

Section 6	Vulnerability Questions	Guidance	Observations
Mechanical Systems (heating, ventilation, and air conditioning (HVAC) and CBR)			
6.21	Is access to building information restricted?	Information on building operations, schematics, procedures, plans, and specifications should be strictly controlled and available only to authorized personnel. REFERENCES: CDC/NIOSH 2002-139 AND LBNL PUB 51959	
6.22	Does the HVAC maintenance staff have the proper training, procedures, and preventive maintenance schedule to ensure CBR equipment is functional?	Functional equipment must interface with operational procedures in an emergency plan to ensure the equipment is properly operated to provide the protection desired. The HVAC system can be operated in different ways depending upon an external or internal release and where in the building an internal release occurs. Thus maintenance and security staff must have the training to properly operate the HVAC system under different circumstances, even if the procedure is to turn off all air movement equipment. REFERENCES: CDC/NIOSH, PUB 2002-139 AND LBNL PUB 51959	

Section 7	Vulnerability Questions	Guidance	Observations
Plumbing and Gas Systems			
7.1	What is the method of water distribution?	Central shaft locations for piping are more vulnerable than multiple riser locations. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
7.2	What is the method of gas distribution? (heating, cooking, medical, process)	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
7.3	Is there redundancy to the main piping distribution?	Looping of piping and use of section valves provide redundancies in the event sections of the system are damaged. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
7.4	What is the method of heating domestic water? What fuel(s) is used?	Single source of hot water with one fuel source is more vulnerable than multiple sources and multiple fuel types. Domestic hot water availability is an operational concern for many building occupancies. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 7	Vulnerability Questions	Guidance	Observations
Plumbing and Gas Systems			
7.5	Where are gas storage tanks located? (heating, cooking, medical, process) How are they piped to the distribution system? (above or below ground)	The concern is that the tanks and piping could be vulnerable to a moving vehicle or a bomb blast either directly or by collateral damage due to proximity to a higher-risk area. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
7.6	Are there reserve supplies of critical gases?	Localized gas cylinders could be available in the event of damage to the central tank system. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 8	Vulnerability Questions	Guidance	Observations
Electrical Systems			
8.1	Are there any transformers or switchgears located outside the building or accessible from the building exterior? Are they vulnerable to public access? Are they secured?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
8.2	What is the extent of the external building lighting in utility and service areas and at normal entryways used by the building occupants?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
8.3	How are the electrical rooms secured and where are they located relative to other higher risk areas, starting with the main electrical distribution room at the service entrance?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
8.4	Are critical electrical systems collocated with other building systems? Are critical electrical systems located in areas outside of secured electrical areas? Is security system wiring located separately from electrical and other service systems?	Collocation concerns include rooms, ceilings, raceways, conduits, panels, and risers. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 8	Vulnerability Questions	Guidance	Observations
Electrical Systems			
8.5	How are electrical distribution panels serving branch circuits secured or are they in secure locations?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
8.6	Does emergency backup power exist for all areas within the building or for critical areas only? How is the emergency power distributed? Is the emergency power system independent from the normal electrical service, particularly in critical areas?	There should be no single critical node that allows both the normal electrical service and the emergency backup power to be affected by a single incident. Automatic transfer switches and interconnecting switchgear are the initial concerns. Emergency and normal electrical equipment should be installed separately, at different locations, and as far apart as possible. REFERENCE: GSA PBS-P100	
8.7	How is the primary electrical system wiring distributed? Is it collocated with other major utilities? Is there redundancy of distribution to critical areas?	Central utility shafts may be subject to damage, especially if there is only one for the building. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR THE DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 9	Vulnerability Questions	Guidance	Observations
Fire Alarm Systems			
9.1	Is the building fire alarm system centralized or localized? How are alarms made known, both locally and centrally? Are critical documents and control systems located in a secure yet accessible location?	Fire alarm systems must first warn building occupants to evacuate for life safety. Then they must inform the responding agency to dispatch fire equipment and personnel. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
9.2	Where are the fire alarm panels located? Do they allow access to unauthorized personnel?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 9	Vulnerability Questions	Guidance	Observations
Fire Alarm Systems			
9.3	Is the fire alarm system standalone or integrated with other functions such as security and environmental or building management systems? What is the interface?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
9.4	Do key fire alarm system components have fire and blast-resistant separation?	This is especially necessary for the fire command center or fire alarm control center. The concern is to similarly protect critical components as described in Items 2.19, 5.7, and 10.3	
9.5	Is there redundant off-premises fire alarm reporting?	Fire alarms can ring at a fire station, at an intermediary alarm monitoring center, or autodial someone else. See Items 5.21 and 10.5.	

Section 10	Vulnerability Questions	Guidance	Observations
Communications and Information Technology (IT) Systems			
Antiterrorism			
10.1	Where is the main telephone distribution room and where is it in relation to higher-risk areas? Is the main telephone distribution room secure?	One can expect to find voice, data, signal, and alarm systems to be routed through the main telephone distribution room. REFERENCE: FEMA 386-7	
10.2	Does the telephone system have an UPS (uninterruptible power supply)? What is its type, power rating, operational duration under load, and location? (battery, on-line, filtered)	Many telephone systems are now computerized and need an UPS to ensure reliability during power fluctuations. The UPS is also needed to await any emergency power coming on line or allow orderly shutdown. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
10.3	Where are communication systems wiring closets located? (voice, data, signal, alarm) Are they collocated with other utilities? Are they in secure areas?	Concern is to have separation distance from other utilities and higher risk areas to avoid collateral damage. Security approaches on the closets include door alarms, closed circuit television, swipe cards, or other logging notifications to ensure only authorized personnel have access to these closets. REFERENCE: FEMA 386-7	

Section 10	Vulnerability Questions	Guidance	Observations
Communications and Information Technology (IT) Systems			
10.4	How is communications system wiring distributed? (secure chases and risers, accessible public areas)	The intent is to prevent tampering with the systems. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
10.5	Are there redundant communications systems available?	Critical areas should be supplied with multiple or redundant means of communications. Power outage phones can provide redundancy as they connect directly to the local commercial telephone switch off site and not through the building telephone switch in the main telephone distribution room. A base radio communication system with antenna can be installed in stairwells, and portable sets distributed to floors. REFERENCE: GSA PBS-P100 AND FEMA 386-7	
10.6	Where are the main distribution facility, data centers, routers, firewalls, and servers located and are they secure? Where are the secondary and/or intermediate distribution facilities and are they secure?	Concern is collateral damage from man-made hazards and redundancy of critical functions. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
10.7	What type and where are the Wide Area Network (WAN) connections?	Critical facilities should have two MPOPs (Minimum-Point-of-Presence) where the telephone company's outside cable terminates inside the building. It is functionally a service entrance connection that demarcates where the telephone company's property stops and the building owner's property begins. The MPOPs should not be collocated and they should connect to different telephone company central offices so that the loss of one cable or central office does not reduce capability. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
10.8	What are the type, power rating, and location of the uninterruptible power supply? (battery, on-line, filtered) Are the UPS also connected to emergency power?	Consider that UPS should be found at all computerized points from the main distribution facility to individual data closets and at critical personal computers/terminals. Critical LAN sections should also be on backup power. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	

Section 10	Vulnerability Questions	Guidance	Observations
Communications and Information Technology (IT) Systems			
10.9	What type of Local Area Network (LAN) cabling and physical topology is used? (Category (Cat) 5, Gigabit Ethernet, Ethernet, Token Ring)	The physical topology of a network is the way in which the cables and computers are connected to each other. The main types of physical topologies are: Bus (single radial where any damage on the bus affects the whole system, but especially all portions downstream) Star (several computes are connected to a hub and many hubs can be in the network–the hubs can be critical nodes, but the other hubs continue to function if one fails) Ring (a bus with a continuous connection– least used but can tolerate some damage because if the ring fails at a single point it can be rerouted much like a looped electric or water system) The configuration and the availability of surplus cable or spare capacity on individual cables can reduce vulnerability to hazard incidents. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
10.10	For installed radio/wireless systems, what are their types and where are they located? (radio frequency (RF), high frequency (HF), very high frequency (VHF), medium wave (MW))	Depending upon the function of the wireless system, it could be susceptible to accidental or intended jamming or collateral damage. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
10.11	Do the Information Technology (IT) computer systems meet requirements of confidentiality, integrity, and availability?	Ensure access to terminals and equipment for authorized personnel only and ensure system up-time to meet operational needs. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
10.12	Where is the disaster recovery/mirroring site?	A site with suitable equipment which allows continuation of operations or that mirrors (operates in parallel to) the existing operation is beneficial if equipment is lost during a natural or manmade disaster. The need is based upon the criticality of the operation and how quickly replacement equipment can be put in place and operated. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
10.13	Where is the back-up tape/file storage site and what is the type of safe environment? (safe, vault, underground) Is there redundant refrigeration in the site?	If equipment is lost, data is most likely lost too. Backups are needed to continue operations at the disaster recovery site or when equipment can be delivered and installed. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	

Section 10	Vulnerability Questions	Guidance	Observations
Communications and Information Technology (IT) Systems			
10.14	Are there any satellite communications (SATCOM) links? (location, power, UPS, emergency power, spare capacity/capability)	SATCOM links can serve as redundant communications for voice and data if configured to support required capability after a hazard incident. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
10.15	Is there a mass notification system that reaches all building occupants? (public address, pager, cell phone, computer override, etc.) Will one or more of these systems be operational under hazard conditions? (UPS, emergency power)	Depending upon building size, a mass notification system will provide warning and alert information, along with actions to take before and after an incident if there is redundancy and power. REFERENCE: DOD UFC 4-010-01	
10.16	Do control centers and their designated alternate locations have equivalent or reduced capability for voice, data, mass notification, etc.? (emergency operations, security, fire alarms, building automation) Do the alternate locations also have access to backup systems, including emergency power?	REFERENCE: GSA PBS-P100	

Section 11	Vulnerability Questions	Guidance	Observations
Equipment Operations and Maintenance			
Antiterrorism			
11.1	Are there composite drawings indicating location and capacities of major systems and are they current? (electrical, mechanical, and fire protection; and date of last update) Do updated operations and maintenance (O&•) manuals exist?	Within critical infrastructure protection at the building level, the current configuration and capacity of all critical systems must be understood to ensure they meet emergency needs. Manuals must also be current to ensure operation and maintenance keeps these systems properly functioning. The system must function during an emergency unless directly affected by the hazard incident. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 11	Vulnerability Questions	Guidance	Observations
Equipment Operations and Maintenance			
11.2	Have critical air systems been rebalanced? If so, when and how often?	Although the system may function, it periodically must be tested to ensure it is performing as designed. Balancing is also critical after initial construction to set equipment to proper performance per the design. Rebalancing may only occur during renovation. REFERENCE: CDC/NIOSH, PUB 2002-139	
11.3	Is air pressurization monitored regularly?	Some areas required positive or negative pressure to function properly. Pressurization is critical in a hazardous environment or emergency situation. Measuring pressure drop across filters is an indication when filters should be changed, but also may indicate that low pressures are developing downstream resulting in loss of expected protection. REFERENCE: CDC/NIOSH, PUB 2002-139	
11.4	Does the building have a policy or procedure for periodic re-commissioning of major Mechanical/ Electrical/Plumbing (• /E/P) systems?	Re-commissioning involves testing and balancing of systems to ascertain their capability to perform as described. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
11.5	Is there an adequate O&• program, including training of facilities management staff?	If O&• of critical systems is done with in-house personnel, management must know what needs to be done and the workforce must have the necessary training to ensure systems reliability. REFERENCE: CDC/NIOSH, PUB 2002-139	
11.6	What maintenance and service agreements exist for • /E/P systems?	When an in-house facility maintenance work force does not exist or does not have the capability to perform the work, maintenance and service contracts are the alternative to ensure critical systems will work under all conditions. The facility management staff requires the same knowledge to oversee these contracts as overseeing the work if done by in-house personnel. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
11.7	Are backup power systems periodically tested under load?	Loading should be at or above maximum connected load to ensure available capacity and automatic sensors should be tested at least once per year. Periodically (once a year as a minimum) check the duration of capacity of backup systems by running them for the expected emergency duration or estimating operational duration through fuel consumption, water consumption, or voltage loss. REFERENCE: FEMA 386-7	

Section 11	Vulnerability Questions	Guidance	Observations
Equipment Operations and Maintenance			
11.8	Is stairway and exit sign lighting operational?	The maintenance program for stairway and exit sign lighting (all egress lighting) should ensure functioning under normal and emergency power conditions. Expect building codes to be updated as emergency egress lighting is moving from upper walls and over doorways to floor level as heat and smoke drive occupants to crawl along the floor to get out of the building. Signs and lights mounted high have limited or no benefit when obscured. REFERENCE: FEMA 386-7	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
Perimeter Security			
12.1	Are black/white or color CCTV (closed circuit television) cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What are the number of fixed, wireless and pan-tilt-zoom cameras used? Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	Security technology is frequently considered to compliment or supplement security personnel forces and to provide a wider area of coverage. Typically, these physical security elements provide the first line of defense in deterring, detecting, and responding to threats and reducing vulnerabilities. They must be viewed are an integral component of the overall security program. Their design, engineering, installation, operation, and management must be able to meet daily security challenges from a cost effective and efficiency perspective. During and after an incident, the system, or its backups, should be functional per the planned design. Consider color CCTV cameras to view and record activity at the perimeter of the building, particularly at primary entrances and exits. A mix of monochrome cameras should be considered for areas that lack adequate illumination for color cameras. REFERENCE: GSA PBS P-100	
12.2	Are the cameras programmed to respond automatically to perimeter building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. Adjustment may be required after installation due to initial false alarms, usually caused by wind or small animals. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.3	What type of camera housings are used and are they environmental in design to protect against exposure to heat and cold weather elements?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.4	Are panic/duress alarm buttons or sensors used, where are they located and are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other areas high risk locations by assessment. REFERENCE: GSA PBS P-100	
12.5	Are intercom call boxes used in parking areas or along the building perimeter?	See item 12.4.	
12.6	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.7	Who monitors the CCTV system?	REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
12.8	What is the quality of video images both during the day and hours of darkness? Are infrared camera illuminators used?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.9	Are the perimeter cameras supported by an uninterruptible power supply, battery, or building emergency power?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.10	What type of exterior Intrusion Detection System (IDS) sensors are used: (electromagnetic, fiber optic, active infrared, bi-static microwave, seismic, photoelectric, ground, fence, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches)	Consider balanced magnetic contact switch sets for all exterior doors, including overhead/roll-up doors and review roof intrusion detection. Consider glass break sensors for windows up to scalable heights. REFERENCE: GSA PBS-P100	
12.11	Is a global positioning satellite system (GPS) used to monitor vehicles and asset movements?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
Interior Security			
12.12	Are black/white or color CCTV cameras used? Are they monitored and recorded 24 hours/7 days a week? By whom? Are they analog or digital by design? What are the number of fixed, wireless and pan-tilt-zoom cameras used? Who are the manufacturers of the CCTV cameras? What is the age of the CCTV cameras in use?	See Item 12.1. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.13	Are the cameras programmed to respond automatically to interior building alarm events? Do they have built-in video motion capabilities?	The efficiency of monitoring multiple screens decreases as the number of screens increases. Tying the alarm system or motion sensors to a CCTV camera and a monitoring screen improves the man-machine interface by drawing attention to a specific screen and its associated camera. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.14	What type of camera housings are used and are they designed to protect against exposure or tampering?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.15	Do the camera lenses used have the proper specifications, especially distance viewing and clarity?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.16	What is the transmission media used to transmit camera video signals: fiber, wire line, telephone wire, coaxial, wireless?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.17	Are the interior camera video images of good visual and recording quality?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.18	Are the interior cameras supported by an uninterruptible power supply source, battery, or building emergency power?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.19	What are the first costs and maintenance costs associated with the interior cameras?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.20	What type of security access control system is used? Are the devices used for physical security also used (integrated) with security computer networks (e.g. in place of or in combination with user ID and system passwords)?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.21	What type of access control transmission media is used to transmit access control system signals (same as defined for CCTV cameras)?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.22	What is the backup power supply source for the access control systems? (battery, uninterruptible power supply)	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.23	What access control system equipment is used? How old are the systems and what are the related first and maintenance service costs?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.24	Are panic/duress alarm sensors used? Where are they located? Are they hardwired or portable?	Call buttons should be provided at key public contact areas and as needed in offices of managers and directors, in garages and parking lots, and other areas high risk locations by assessment. REFERENCE: GSA PBS P-100	
12.25	Are intercom call-boxes or a building intercom system used throughout the building?	See Item 12.24.	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.26	Are magnetometers (metal detectors) and x-ray equipment used? At what locations within the building	REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
12.27	What type of interior IDS sensors are used: electromagnetic, fiber optic, active infrared-motion detector, photoelectric, glass break (vibration/shock), single, double and roll-up door magnetic contacts or switches?	Consider magnetic reed switches for interior doors and openings. REFERENCE: GSA PBS-P100	
12.28	Are mechanical, electrical, gas, power supply, radiological material storage, voice/data telecommunication system nodes, security system panels, elevator and critical system panels, and other sensitive rooms continuously locked, under electronic security, CCTV camera, and intrusion alarm systems surveillance?	REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
12.29	What types of locking hardware are used throughout the building? Are manual and electromagnetic cipher, keypad, pushbutton, panic bar, door strikes and related hardware and software used?	As a minimum, electric utility closets, mechanical rooms, and telephone closets should be secured. The mailroom should also be secured, allowing only authorized personnel into the area where mail is screened and sorted. Separate the public access area from the screening area for the postulated mailroom threats. All security locking arrangements on doors used for egress must comply with NFPA 101, Life Safety Code. REFERENCE: GSA PBS-P100	
12.30	Are any potentially hazardous chemicals, combustible or toxic materials stored on-site in non-secure and non-monitored areas?	These storage, use, and handling locations should also be kept away from other activities. The concern is that an intruder need not bring the material into the building if it is already there and accessible. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.31	What security controls are in place to handle the processing of mail and protect against potential biological, explosive, or other threatening exposures?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.32	Is there a designated security control room and console in place to monitor security, fire alarm, and other building systems? Is there a backup control center designated and equipped? Is there off-site 24-hour monitoring of intrusion detection systems?	Monitoring can be done at an off-site facility, at an on-site monitoring center during normal duty hours, or at a 24-hour on-site monitoring center. REFERENCE: GSA PBS-P100	
12.33	Is the security console and control room adequate in size and does it provide room for expansion? Does it have adequate environment controls (e.g., a/c, lighting, heating, air circulation, backup power)? Is it ergonomically designed?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.34	Is the location of the security room in a secure area with limited, controlled and restricted access controls in place?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.35	What are the means by which facility and security personnel can communicate with one another: portable radio, pager, cell phone, personal data assistants (PDA's), etc)? What problems have been experienced with these and other electronic security systems?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.36	Is there a computerized security incident reporting system used to prepare reports and track security incident trends and patterns?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.37	Does the current security force have access to use a computerized guard tour system?	This system allows for the systematic performance of guard patrols with validation indicators built in. The system notes stations/locations checked or missed, dates and times of such patrols and who conducted them on what shifts. Management reports can be produced for record keeping and manpower analysis purposes. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.38	Are vaults or safes in the building? Where are they located?	Basic structural design requires an understanding of where heavy concentrations of floor loading may occur so as to strengthen the floor and structural framing to handle this downward load. Security design also needs this information to analyze how this concentrated load affects upward and downward loadings under blast conditions and its impact upon progressive collapse. Location is important because safes can be moved by blast so that they should be located away from people and away from exterior windows. Vaults, on the other hand, require construction above the building requirements with thick masonry walls and steel reinforcement. A vault can provide protection in many instances due to its robust construction. Safes and vaults may also require security sensors and equipment, depending upon the level of protection and defensive layers needed. REFERENCE: U.S. ARMY TM 5-853	
Documents			
12.39	Have security system as-built drawings been generated and are they ready for review?	Drawings are critical to the consideration and operation of security technologies, including its overall design and engineering processes. These historical Reference documents outline system specifications and layout security devices used, as well as their application, location, and connectivity. They are a critical resource tool for troubleshooting system problems, and replacing and adding other security system hardware and software products. Such documents are an integral component to new and retrofit construction projects. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 12	Vulnerability Questions	Guidance	Observations
Security Systems			
12.40	Have security system design and drawing standards been developed?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.41	Are security equipment selection criteria defined?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.42	What contingency plans have been developed or are in place to deal with security control center redundancy and backup operations?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.43	Have security system construction specification documents been prepared and standardized?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.44	Do all security system documents include current as-built drawings?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.45	Have qualifications been determined in using security consultants, system designers/engineers, installation vendors, and contractors?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.46	Are security systems decentralized, centralized, or integrated? Do they operate over an existing IT network or are they a standalone method of operation?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.47	What security systems manuals are available?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
12.48	What maintenance or service agreements exist for security systems?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 13	Vulnerability Questions	Guidance	Observations
Security Master Plan			
Antiterrorism			
13.1	Does a written security plan exist for this site or building? When was the initial security plan written and last revised? Who is responsible for preparing and reviewing the security plan?	The development and implementation of a security master plan provides a roadmap that outlines the strategic direction and vision, operational, managerial, and technological mission, goals, and objectives of the organization's security program. REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT F RAMEWORK 1.1	
13.2	Has the security plan been communicated and disseminated to key management personnel and departments?	The security plan should be part of the building design so that the construction or renovation of the structure integrates with the security procedures to be used during daily operations. REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.3	Has the security plan been benchmarked or compared against related organizations and operational entities?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.4	Has the security plan ever been tested and evaluated from a benefit/cost and operational efficiency and effectiveness perspective?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.5	Does the security plan define mission, vision, short- and long- term security program goals and objectives?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.6	Are threats/hazards, vulnerabilities, and risks adequately defined and security countermeasures addressed and prioritized relevant to their criticality and probability of occurrence?	REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	
13.7	Has a security implementation schedule been established to address recommended security solutions?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	

Section 13	Vulnerability Questions	Guidance	Observations
Security Master Plan			
13.8	Have security operating and capital budgets been addressed, approved, and established to support the plan?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.9	What regulatory or industry guidelines/standards were followed in the preparation of the security plan?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.10	Does the security plan address existing security conditions from an administrative, operational, managerial and technical security systems perspective?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.11	Does the security plan address the protection of people, property, assets, and information?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.12	Does the security plan address the following major components: access control, surveillance, response, building hardening and protection against CBR and cyber-network attacks?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.13	Has the level of risk been identified and communicated in the security plan through the performance of a physical security assessment?	REFERENCE: PHYSICAL SECURITY ASSESSMENT FOR DEPARTMENT OF VETERANS AFFAIRS FACILITIES	
13.14	When was the last security assessment performed? Who performed the security risk assessment?	REFERENCE: DOC CIAO VULNERABILITY ASSESSMENT FRAMEWORK 1.1	

Section 13	Vulnerability Questions	Guidance	Observations
Security Master Plan			
13.15	Were the following areas of security analysis addressed in the security master plan: **Asset Analysis:** Does the security plan identify and prioritize the assets to be protected in accordance to their location, control, current value, and replacement value? **Threat Analysis**: Does the security plan address potential threats; causes of potential harm in the form of death, injury, destruction, disclosure, interruption of operations, or denial of services? (possible criminal acts (documented and review of police/security incident reports) associated with forced entry, bombs, ballistic assault, biochemical and related terrorist tactics, attacks against utility systems infrastructure and buildings) **Vulnerability Analysis:** Does the security plan address other areas associated with the site or building and its operations that can be taken advantage of to carry out a threat? (architectural design and construction of new and existing buildings, technological support systems [e.g. heating, air conditioning, power, lighting and security systems, etc.] and operational procedures, policies, and controls) **Risk Analysis:** Does the security plan address the findings from the asset, threat/hazard, and vulnerability analyses to develop, recommend, and consider implementation of appropriate security countermeasures?	This process is the input to the building design and what mitigation measures will be included in the facility project to reduce risk and increase safety of the building and people. REFERENCE: U.S.A TM 5-853, SECURITY ENGINEERING	

Section 14	Vulnerability Questions	Guidance	Observations
COOP Facility: Additional Concerns			
Antiterrorism			
14.1	Essential Functions: Have the essential functions been identified and prioritized to establish the planning parameters for the alternate operating facility?	Essential functions are those functions that enable agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial / economic base in an emergency. Record essential functions and resources requirements on the Site Information form. REFERENCE: FPC: PARA 19, B.	
14.2	Essential Functions: Have reliable processes and procedures been established to acquire resources necessary to continue essential functions and sustain operations until normal business activities can be reconstituted, which could be up to 30 days?	Review the alternate operating facility essential functions and resource requirements on the Site Information form. REFERENCE: FPC: PARA 10, A, (8).	
14.3	Communications: Does the alternate operating facility provide interoperable communications, including a means for secure communications, with all identified essential internal and external organizations, customers, and the public?	Review the alternate operating facility communication requirements on the database Site Information form. REFERENCE: FPC: PARA 10, E, (5).	
14.4	Communications: Have the internal and external communications capabilities at the alternate operating facility been validated quarterly?	The ability of an agency to execute its essential functions at its alternate operating facilities is dependent upon the identification, availability, and redundancy of critical communications and information technology systems to support connectivity between key government leadership, internal elements, other agencies, critical customers, and the public. REFERENCE: FPC: PARA 10, F.	
14.5	Communications: Does the COOP facility have wireless / cell phone capability? Have wireless and cell phone providers been reviewed and compared to ensure the best service is provided? Are services available/ compatible within the building to support essential functions and missions?	REFERENCE: FPC: 65 ANNEX F INTEROPERABLE COMMUNICATIONS.	

Section 14	Vulnerability Questions	Guidance	Observations
COOP Facility: Additional Concerns			
14.6	Test, Training and Exercises: Has there been annual testing of primary and backup infrastructure systems and services at alternate operating facilities (e.g., power, water, fuel)?	Tests and exercises serve to assess, validate, or identify for subsequent correction, specific aspects of COOP plans, policies, procedures, systems, and facilities used in response to an emergency situation. Periodic testing also ensures that equipment and procedures are maintained in a constant state of readiness. REFERENCE: FPC: ANNEX I TEST, TRAINING AND EXERCISE PROGRAM, PARA 1, D.	
14.7	Test, Training and Exercises: Have physical security capabilities been tested / exercised annually and shown to able to be in place within 12 hours of COOP plan activation?	REFERENCE: FPC: 65 ANNEX E ALTERNATE OPERATING FACILITIES PLANNING CONSIDERATIONS, PARA. 8.	
14.8	Planning Requirements: Is the alternate operating facility located in an area where power, telecommunications, and internet grids are distinct from those of the primary facility?	Alternate operating facilities must be located in areas where the ability to initiate, maintain, and terminate continuity operations is maximized. REFERENCE: FPC: PARA 9, F & G.	
14.9	Planning Requirements: Is the distance between the primary facility and the alternate operating facility sufficient to allow it to continue essential agency functions?	COOP planning is an effort to ensure that the capability exists to continue essential agency functions across a wide range of all hazard emergencies. REFERENCE: FPC: PARA 9, I.	
14.10	Planning Requirements: Has the organization identified which essential services and functions that can be continued from remote locations (e.g., home facilities or other alternative workplaces) and those that need to be performed at a designated department or agency operating facility?	Alternate operating facility planning should take maximum advantage of existing agency field infrastructures and give consideration to other options, such as telecommuting locations, work-at-home, virtual offices, and joint or shared facilities. REFERENCE: FPC: PARA 9, H.	

Section 14	Vulnerability Questions	Guidance	Observations
COOP Facility: Additional Concerns			
14.11	Planning Requirements: Does the alternate facility have detailed site preparation and activation plans or have pre-positioned supplies and resources in order to achieve full operational capability within 12 hours of notification?	Cross Reference the alternate operating facility essential functions and resource requirements on the Site Information form. REFERENCE: FPC: 65 ANNEX E ALTERNATE OPERATING FACILITIES PLANNING CONSIDERATIONS, PARA. 10.	
14.12	Planning Requirements: Is the COOP facility able to accommodate all emergency relocation group members in a safe and efficient manner?	REFERENCE: FPC: 65 ANNEX A PLANS AND PROCEDURES	
14.13	Planning Requirements: Does the COOP facility contain the sufficient amount of phones, computers, and necessary equipment needed to sustain COOP operations?	REFERENCE: FPC: 65 ANNEX A PLANS AND PROCEDURES	
14.14	Vital Records: Has the organization identified vital records needed to perform its essential functions during a COOP event?	REFERENCE: FPC 65 ANNEX G VITAL RECORDS AND DATABASES, PARA. 2.	
14.15	Vital Records: Do emergency response group members have access to their vital records at the alternate facility? Are they available within 12 hours or less of a COOP plan activation.	REFERENCE: FPC: 65 ANNEX G VITAL RECORDS AND DATABASES, PARA. 2.	
14.16	Vital Records: Are periodic review / updates of the vital records program conducted to address any new security issues, identify problem areas, and identify additional vital records that may result from new agency programs or functions?	REFERENCE: FPC: 65 ANNEX G VITAL RECORDS AND DATABASES, PARA. 10.	

Section 14	Vulnerability Questions	Guidance	Observations
COOP Facility: Additional Concerns			
14.17	Vital Records: Are there separate COOP servers? Are they placed in a secure area? Are there backup procedures?	REFERENCE: FPC: 65 ANNEX G VITAL RECORDS AND DATABASES, PARA. 2.	
14.18	Vital Records: Has a risk assessment of vital records been performed to determine: a. Identify risks involved if vital records are retained in their current location and medium, and the difficulty reconstituting them if they are destroyed. b. If off-site storage is necessary? c. Determine if alternative storage media is advisable? d. Determine if it is necessary to duplicate records to provide a vital records copy?	REFERENCE: FPC: 65 ANNEX G VITAL RECORDS AND DATABASES, PARA. 4, A-D.	
14.19	**Human Capital:** Is adequate Personal Protective Equipment available for all emergency response group members while on-site?	REFERENCE: FPC: 65 ANNEX H HUMAN CAPITAL.	
14.20	**Human Capital:** Are there sufficient quantities of Personal Protective Equipment for emergency response group members to sustain operations for 30 or more days?	REFERENCE: FPC: 65 ANNEX H HUMAN CAPITAL.	

Section 14	Vulnerability Questions	Guidance	Observations
COOP Facility: Additional Concerns			
14.21	**Human Capital:** Are medical facilities, proper caregivers, and first aid kits available for emergency response group members if and when needed?	REFERENCE: FPC: 65 ANNEX H HUMAN CAPITAL.	
14.22	**Human Capital:** Is there access to essential resources such as food, water, fuel and municipal services at the facility?	COOP Evaluation Tool, Office of National Security Coordination, FEMA, DHS	
14.23	**Security:** Does the site provide physical security that meets all requirements established by annual threat assessments and physical security surveys?	REFERENCE: FPC: 65 ANNEX E ALTERNATE OPERATING FACILITIES PLANNING CONSIDERATIONS, PARA. 8.	