

BUILDING DESIGN FOR HOMELAND SECURITY

Unit I

Building Design for Homeland Security



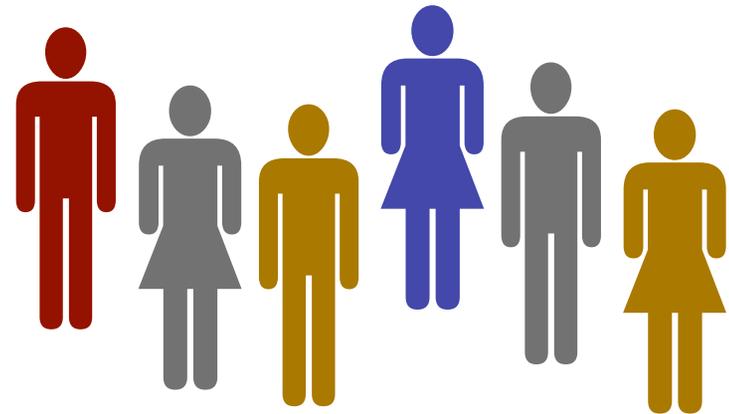
FEMA

Participant Introductions

Name

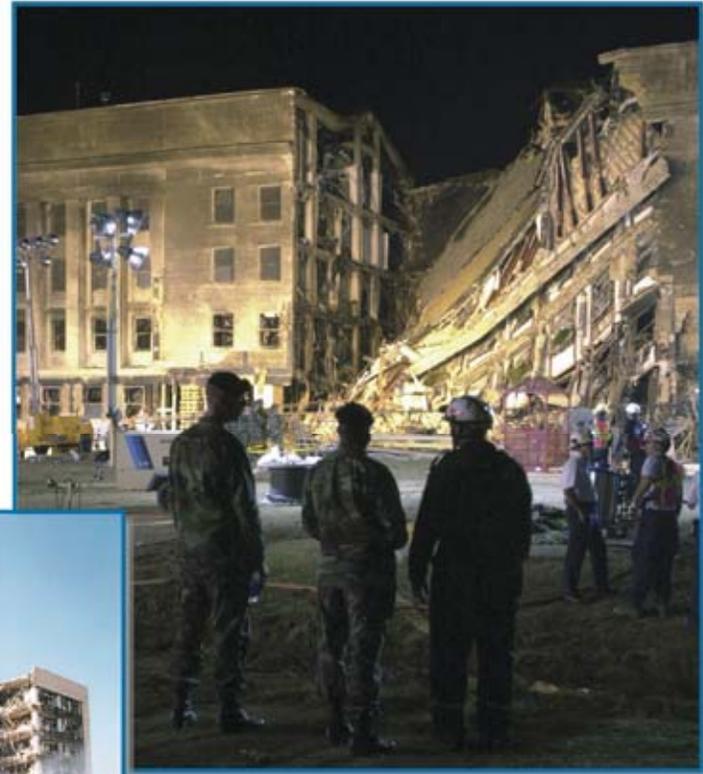
Affiliation

Area of Concentration



Course Goal

To enhance student understanding of the measures and technology available to reduce risk from terrorist attack.



FEMA



U.S. AIR FORCE



FEMA

Course Objectives

Participants will be able to:

1. **Explain** the basic components of the assessment methodology.
2. **Appreciate** the different assessment methodology approaches that can be used.
3. **Perform** an assessment for a building by identifying and prioritizing assets, threats, and vulnerabilities and calculating relative risk.



Course Objectives

4. **Identify** available mitigation measures applicable to the site and building envelope.
5. **Understand** the technology limitations and application details of mitigation measures for terrorist tactics and technological accidents.
6. **Perform** an assessment for a given building by identifying vulnerabilities using the Building Vulnerability Assessment Checklist in FEMA 426.



FEMA

Course Objectives

7. **Select** applicable mitigation measures and prioritize them based upon the final assessment risk values.
8. **Appreciate** that designing a building to mitigate terrorist attacks can create conflicts with other design requirements.



FEMA

Course Overview – Day 1

Unit I – Introduction and Course Overview

Unit II – Asset Value Assessment

Unit III – Threat/Hazard Assessment

Unit IV – Vulnerability Assessment

Unit V – Risk Assessment/Risk Management

Day 1 Wrap-up



FEMA

Course Overview – Day 2

Day 1 Review and Day 2 Overview

Unit V – Risk Assessment/Risk Management (continued)

Unit VI – Explosive Blast (physics and mitigation)

Unit VII – Chemical, Biological, and Radiological Measures (physics and mitigation)

Exam

Unit VIII – Site and Layout Design Guidance

Day 2 Wrap-up



Course Overview – Day 3

Day 2 Review and Day 3 Overview

Unit IX – Building Design Guidance

Unit X – Electronic Security Systems

Unit XI - Finalization of Case Study Results

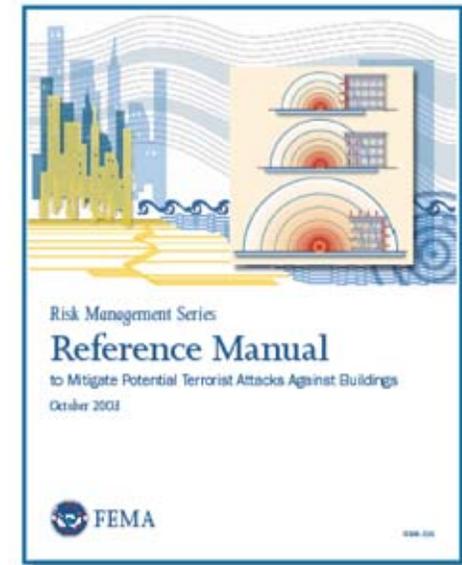
Unit XII - Course Wrap-up



Course Materials

FEMA Publication 426

Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings



FEMA 426 Reference Manual

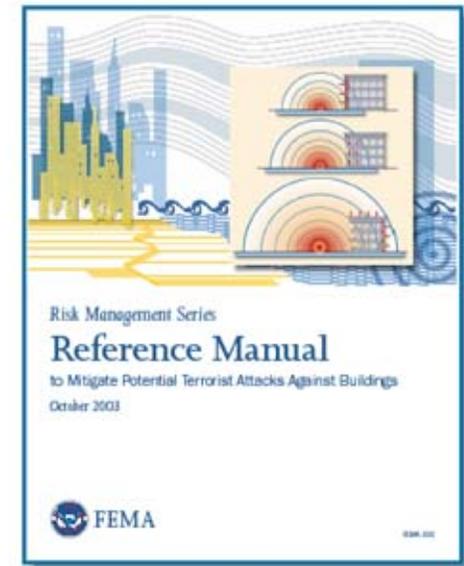
Chapter 1 – Asset Value, Threat/Hazard, Vulnerability, and Risk

Chapter 2 – Site and Layout Design Guidance

Chapter 3 – Building Design Guidance

Chapter 4 – Explosive Blast

Chapter 5 – CBR Measures



FEMA 426 Reference Manual

Appendix A – Acronyms

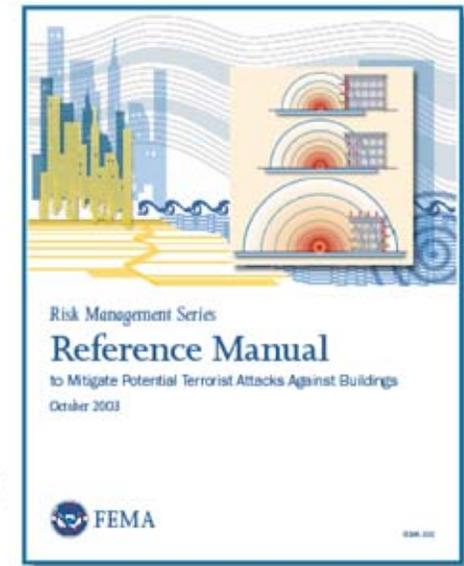
Appendix B – General Glossary

Appendix C – CBR Glossary

Appendix D – Electronic Security Systems

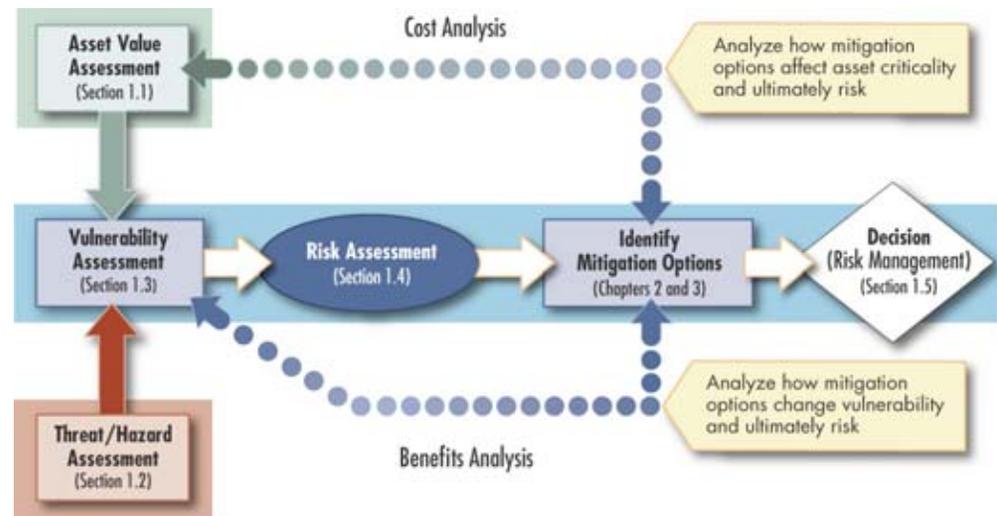
Appendix E – Bibliography

Appendix F – Associations and Organizations



FEMA 426 – Chapter 1

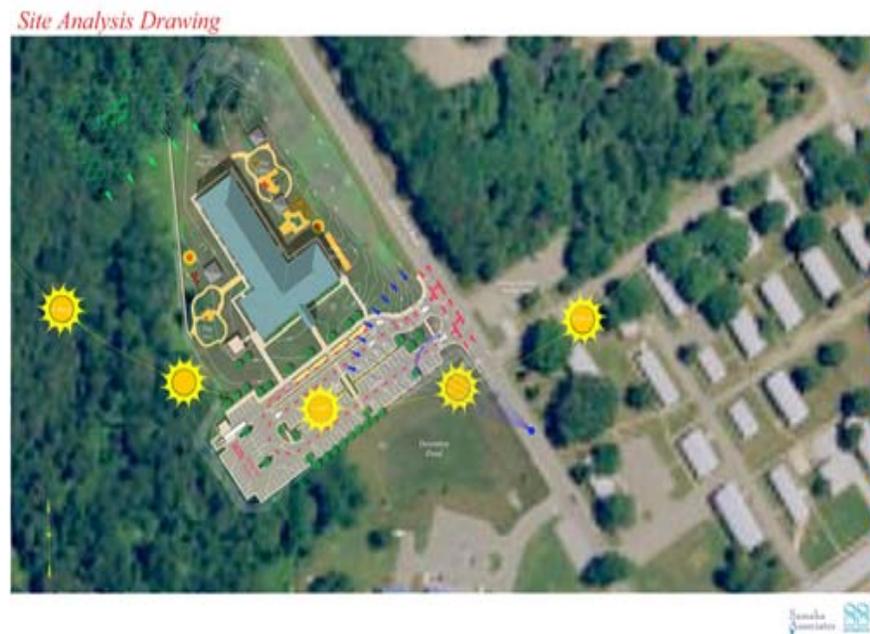
- Asset Value Assessment
- Threat/Hazard Assessment
- Vulnerability Assessment
- Risk Assessment
- Risk Management
- Building Vulnerability Assessment Checklist



FEMA 426 – Chapter 2

Site and Layout Design

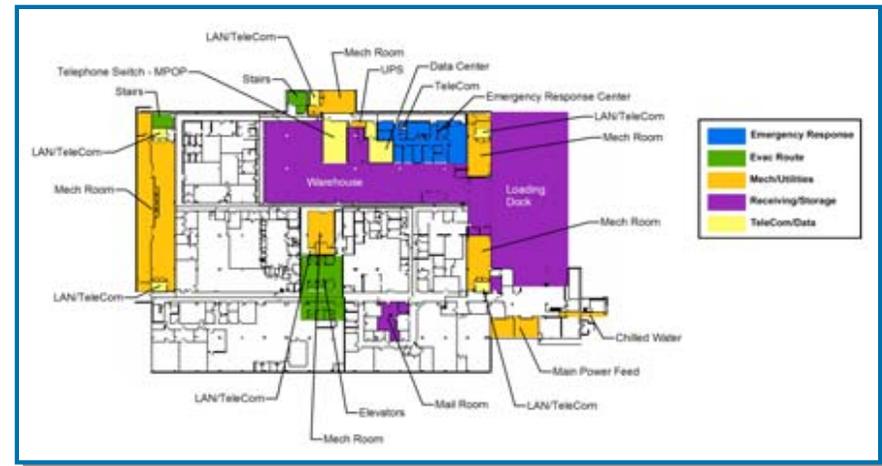
- Layout Design
- Siting
- Entry Control/Vehicle Access
- Signage
- Parking
- Loading Docks
- Physical Security Lighting
- Site Utilities



FEMA 426 – Chapter 3

Building Design Guidance

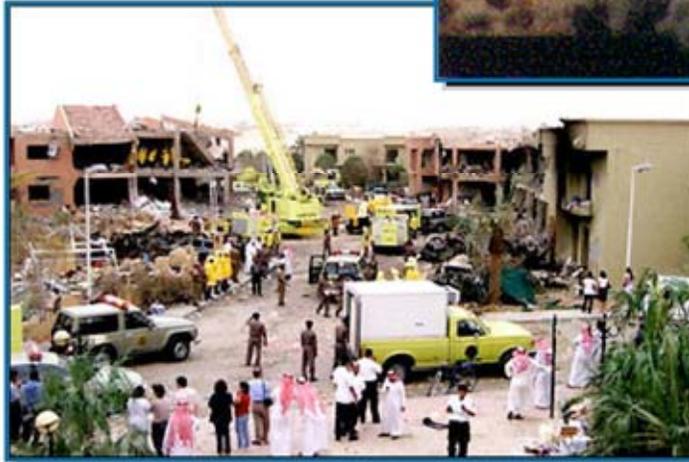
- Architectural
- Building Structural and Nonstructural Considerations
- Building Envelope considerations
- Other Building Design Issues
- Building Mitigation Measures



FEMA 426 – Chapter 4

Explosive Blast

- Blast Effects and predictions
- Stand-off Distance
- Progressive Collapse



FEMA

FEMA 426 – Chapter 5

CBR Measures

- Evacuation
- Sheltering in Place
- Personal Protective Equipment
- Filtering and Pressurization
- Exhausting and Purging



Summary

FEMA 426 is intended for building sciences professionals.

Manmade hazards risk assessments use a “Design Basis Threat.”

Site and building systems and infrastructure protection are provided by layers of defense.

Multiple mitigation options and techniques.

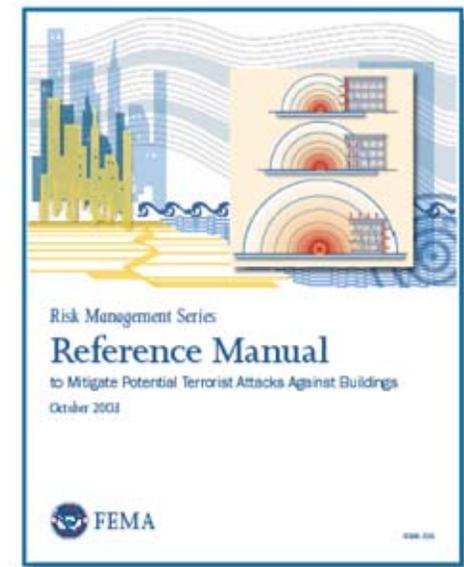
Use cost-effective multihazard analysis and design.



Case Study Activities

In small group settings, apply concepts introduced in the course.

Become conversant with contents and organization of FEMA 426.



Unit I Case Study Activity

Hazardville Information Company Case Study Overview

Requirements

Briefly review HIC case study materials.

As a group, complete the worksheet.

Use only the case study data to answer worksheet questions.



HAZARDVILLE INFORMATION COMPANY (HIC)

Case Study



Hazardville Information Company



Hazardville Information Company (HIC)



FEMA

HIC Mission

Regional Computer Center

- Real-time IT support
- Backup services
- 24 x 7 operations

Customers

- Government and commercial
- Some classified work

Layout

- Downstairs: Computers, Communications, Staff
- Upstairs: Executive offices
- Highway loading dock



FEMA

HIC Threat Analysis

Terrorist Threat

Intelligence Threat

Criminal Threat



FEMA

HIC Hazard Analysis

HazMat

- Facilities
- Highway
- Rail

Liquid Fuels



Air Traffic



Natural Hazards



FEMA

HIC Building Data

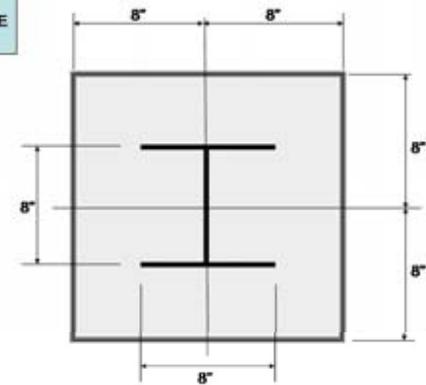


FEMA

HIC Building Structure

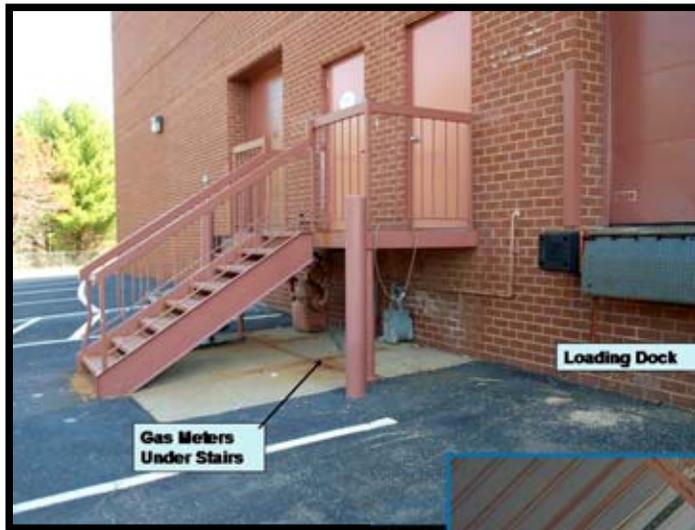


COLUMN ENCLOSURE DETAIL



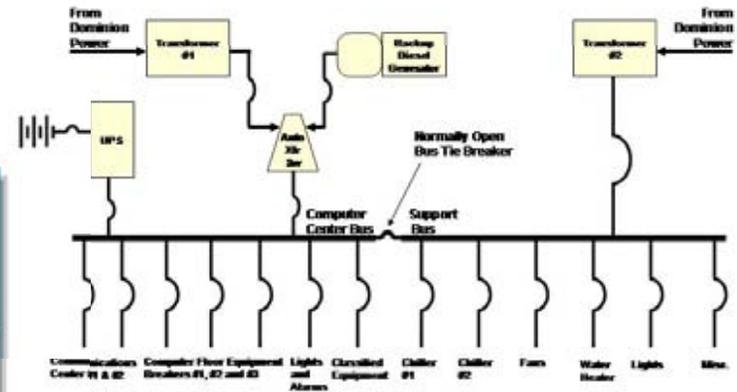
FEMA

HIC Mechanical Systems



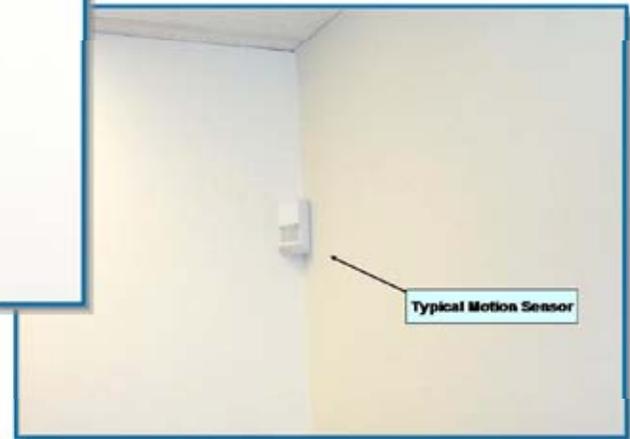
FEMA

HIC Electrical Systems



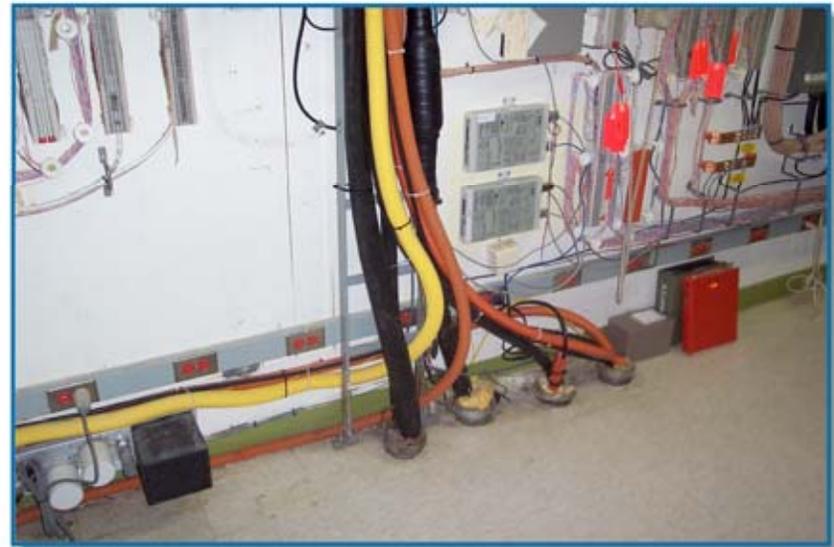
FEMA

HIC Physical Security



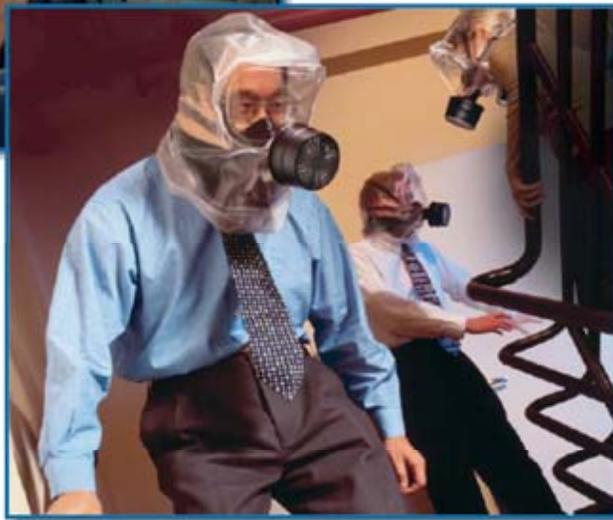
FEMA

HIC IT Systems



FEMA

HIC Emergency Response



FEMA

Design Basis Threat

Explosive Blast: Car Bomb 250 lb TNT equivalent. Truck Bomb 5,000 lb TNT equivalent (Murrah Federal Building class weapon)

Chemical: Large quantity gasoline spill and toxic plume from the adjacent tank farm, small quantity (tanker truck and rail car size) spills of HazMat materials (chlorine)

Biological: Anthrax delivered by mail or in packages, smallpox distributed by spray mechanism mounted on truck or aircraft in metropolitan area

Radiological: Small “dirty” bomb detonation within the 10 mile radius of the HIC building



Design Basis Threat

Criminal Activity/Armed Attack: High powered rifle or handgun exterior shooting (sniper attack or direct assault on key staff, damage to infrastructure [e.g., transformers, chillers, etc.])

Cyber Attack: Focus on IT and building systems infrastructure (SCADA, alarms, etc.) accessible via Internet access



Levels of Protection and Layers of Defense

Levels of Protection for Buildings

- GSA Interagency Security Criteria Level II Building
- DoD Low Inhabited Building

Elements of the Layers of Defense Strategy

- Deter
- Detect
- Deny
- Devalue



Summary

FEMA Publication 426

Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings

