UFC 4-026-01
4 March 2020

UNIFIED FACILITIES CRITERIA (UFC)

DESIGN TO RESIST FORCED ENTRY

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

UNIFIED FACILITIES CRITERIA (UFC)

DESIGN TO RESIST FORCED ENTRY

Any copyrighted material included in this UFC is identified at its point of use.
Use of the copyrighted material apart from this UFC must have the permission of the copyright holder.

Indicate the preparing activity beside the Service responsible for preparing the document.

U.S. ARMY CORPS OF ENGINEERS

NAVAL FACILITIES ENGINEERING COMMAND (Preparing Activity)

AIR FORCE CIVIL ENGINEER CENTER

Record of Changes (changes are indicated by **1**\ ... /**1**/)

Change No.	**Date**	**Location**

FOREWORD

The Unified Facilities Criteria (UFC) system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with USD (AT&L) Memorandum dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate. All construction outside of the United States is also governed by Status of Forces Agreements (SOFA), Host Nation Funded Construction Agreements (HNFA), and in some instances, Bilateral Infrastructure Agreements (BIA). Therefore, the acquisition team must ensure compliance with the most stringent of the UFC, the SOFA, the HNFA, and the BIA, as applicable.

UFC are living documents and will be periodically reviewed, updated, and made available to users as part of the Services' responsibility for providing technical criteria for military construction. Headquarters, U.S. Army Corps of Engineers (HQUSACE), Naval Facilities Engineering Command (NAVFAC), and Air Force Civil Engineer Center (AFCEC) are responsible for administration of the UFC system. Defense agencies should contact the preparing service for document interpretation and improvements. Technical content of UFC is the responsibility of the cognizant DoD working group. Recommended changes with supporting rationale may be sent to the respective DoD working group by submitting a Criteria Change Request (CCR) via the Internet site listed below.

UFC are effective upon issuance and are distributed only in electronic media from the following source:

- Whole Building Design Guide web site http://www.wbdg.org/ffc/dod.

Refer to UFC 1-200-01, *DoD Building Code (General Building Requirements)*, for implementation of new issuances on projects.

AUTHORIZED BY:

CHRISTINE T. ALTENDORF, PhD, P.E., SES
Chief, Engineering and Construction
U.S. Army Corps of Engineers

R. DAVID CURFMAN, P.E.
Chief Engineer
Naval Facilities Engineering Command

NANCY J. BALKUS, P.E., SES
Deputy Director of Civil Engineers
DCS Logistics, Engineering &
Force Protection (HAF/A4C)
HQ United States Air Force

MICHAEL McANDREW
Deputy Assistant Secretary of Defense
(Facilities Management)
Office of the Assistant Secretary of Defense
(Sustainment)

UNIFIED FACILITIES CRITERIA (UFC)
NEW DOCUMENT SUMMARY SHEET

Document: UFC 4-026-01, *Design to Resist Forced Entry*

Superseding: MIL-HDBK-1013/1A, *Design Guidelines for Physical Security of Facilities,* dated 15 December 1993.

Description: Provide a unified approach to the development of protective measures intended to protected assets from a forced entry attack.

Reasons for Document:

- This document is one of a series of security engineering criteria documents covering physical countermeasures for the current threat environment.
- The design of physical security measures is a specialized technical area that does not fall in the normal skill record and resume of commanders, architects, engineers, and project managers. This document provides guidance to those parties tasked with implementing existing and emerging physical protection system requirements for assets.

Impact:

- No additional cost impacts are anticipated by the publication of this document. This document should reduce the design and coordination efforts for design of systems that protect against forced entry.

Unification Issues

There are no unification issues.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION 1
1-1 PURPOSE AND SCOPE. 1
1-1.1 Purpose. 1
1-1.2 Scope. 1
1-2 APPLICABILITY. 1
1-3 SECURITY ENGINEERING UFC SERIES. 1
1-3.1 DoD Minimum Antiterrorism Standards for Buildings. 1
1-3.2 DoD Security Engineering Facilities Planning Manual. 2
1-3.3 DoD Security Engineering Facilities Design Manual. 2
1-3.4 Security Engineering Support Manuals. 2
1-3.5 Security Engineering UFC Application. 2
1-4 VULNERABILITY AND RISK ASSESSMENT. 4
1-5 PRESCRIPTIVE VS. RISK-BASED DESIGN REQUIREMENTS. 4
1-5.1 Prescriptive Design Requirements. 4
1-5.2 Risk-Based Requirements. 4
1-6 GENERAL BUILDING REQUIREMENTS. 5
1-7 CYBERSECURITY. 5
1-8 HISTORIC PRESERVATION COMPLIANCE. 5
1-8.1 Security and Stewardship. 5
1-8.2 Compliance with Laws. 5
1-8.3 Compliance with DoD Standards. 5
1-9 GLOSSARY. 6
1-10 REFERENCES. 6
CHAPTER 2 DESIGN CRITERIA 7
2-1 INTRODUCTION. 7
2-2 FORCED ENTRY TACTIC. 7
2-2.1 Tools and Effects. 7
2-2.2 Employment of Tools. 8
2-2.3 Hand Tools. 8
2-2.4 Power Tools. 9
2-2.5 Thermal Tools. 9
2-2.6 Explosives. 10

2-3 PROJECT DESIGN CRITERIA. 12
2-3.1 Assets. 12
2-3.2 Threat Severity Level. 13
2-3.3 Level of Protection. 13
2-3.4 Design Constraints. 13
CHAPTER 3 DESIGN GUIDANCE TO RESIST FORCED ENTRY 15
3-1 GENERAL DESIGN STRATEGY. 15
3-2 SPECIFIC DESIGN STRATEGIES. 15
3-2.1 Low Level of Protection. 16
3-2.2 Medium Level of Protection. 16
3-2.3 High Level of Protection. 16
3-2.4 Very High Level of Protection. 17
3-3 DESIGN PROCEDURES. 17
3-4 PROTECTIVE SYSTEM. 17
3-5 SECURITY IN DEPTH. 17
3-6 DEFENSE LAYERS. 18
3-7 CONTROL ZONES. 19
3-8 LAYOUT CONSIDERATIONS. 19
3-8.1 Multiple Assets. 20
3-8.2 Multiple Buildings in Project. 20
3-8.3 Multiple Aggressor Tactics. 20
3-8.4 Multiple Defense Layers with Common Roofs or Ceilings. 21
3-9 ESTABLISHING REQUIRED PROTECTIVE SYSTEM DELAY TIME. 21
3-9.1 Delays for Multiple Assets. 21
3-9.2 Establish Minimum and Maximum Response Times. 21
3-9.3 Establish Required Protective System Delay Times. 21
3-10 EVALUATING SYSTEM DELAY IN PRELIMINARY DESIGN. 22
3-10.1 Physical Delay Ratings. 24
3-10.2 Outermost Defense Layer. 25
3-11 DESIGN ADJUSTMENT. 25
CHAPTER 4 SITEWORK. 27
4-1 INTRODUCTION. 27
4-2 SITEWORK ELEMENTS. 27

4-3 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN. 27
4-3.1 Natural Access Control. 28
4-3.2 Natural Surveillance. 28
4-3.3 Territorial Reinforcement. 28
4-4 SITE LAYOUT CONSIDERATIONS. 28
4-5 SECURITY FENCING. 29
4-5.1 Gates for Fences. 29
4-5.2 Utility Openings in Fence Lines. 29
4-5.3 Walls in Fence Lines. 29
4-6 CLEAR ZONES AND UNOBSTRUCTED SPACE. 30
4-6.1 Clear Zones. 30
4-6.2 Unobstructed Space. 30
4-7 SITE PERIMETER ENTRY CONTROL. 31
4-8 DETECTION. 31
4-9 SECURITY LIGHTING. 31
CHAPTER 5 BUILDING ELEMENTS 33
5-1 INTRODUCTION. 33
5-2 BUILDING LAYOUT. 33
5-3 BUILDING COMPONENTS. 34
5-4 FORCED ENTRY RESISTANT BUILDING COMPONENT TABLES 34
5-4.1 Data Formulation. 34
5-4.2 Advantages of Composite Components. 35
5-4.3 Data Application. 35
5-4.4 Using the Tables. 36
5-4.5 References to Explosives Use. 36
5-5 NEW CONSTRUCTION. 36
5-5.1 Walls. 36
5-5.2 Roofs. 47
5-5.3 Ceilings and Floors. 52
5-5.4 Personnel Entrances. 54
5-5.5 Doors (Non-Entry). 61
5-5.6 Emergency Exit Hardware. 64
5-5.7 Vehicle Access Doors. 65

5-5.8 Windows. 66
5-5.9 Utility Openings. 72
5-6 RETROFIT CONSTRUCTION. 77
5-6.1 General. 77
5-6.2 Walls. 77
5-6.3 Roofs. 86
5-6.4 Ceilings and Floors. 87
5-6.5 Personnel Entrances. 89
5-6.6 Doors, Frames and Locks (Non-Entry). 89
5-6.7 Windows. 89
5-6.8 Utility Openings. 90
CHAPTER 6 PROTECTED AREAS 91
6-1 INTRODUCTION. 91
6-2 PROTECTED ASSET TYPES. 91
6-2.1 High-Risk Personnel. 91
6-2.2 Classified Information and Material. 91
6-2.3 Sensitive Compartmented Information. 92
6-2.4 Special Access Program Information and Equipment. 92
6-2.5 Communications Security (COMSEC) Materials. 92
6-2.6 Arms, Ammunition, and Explosives. 92
6-2.7 Chemical Agents. 93
6-2.8 Biological Agents. 93
6-2.9 Nuclear Weapons. 93
6-2.10 Controlled Substances. 93
6-2.11 Funds. 94
6-3 SECURE ROOMS. 94
6-3.1 Walls, Floor, and Roof. 94
6-3.2 Ceiling. 94
6-3.3 Door and Frame. 94
6-3.4 Locks. 95
6-3.5 Windows. 95
6-4 FUNDS STORAGE ROOMS. 95
6-4.1 Walls, Floors, and Ceilings. 95

6-4.2 Doors. 95
6-4.3 Door Frames and Hardware. 96
6-4.4 Windows and Other Openings. 96
6-4.5 Security Lighting. 97
6-4.6 Locks and Keys. 97
6-4.7 Intrusion Detection Systems. 97
6-5 SECURE STORAGE STRUCTURES. 97
6-5.1 Walls. 97
6-5.2 Floor and Ceiling. 98
6-5.3 Doors. 98
6-5.4 Windows. 99
6-6 VAULTS. 100
6-7 CLASS A VAULTS. 101
6-7.1 Walls. 101
6-7.2 Floor. 102
6-7.3 Roof and Ceiling. 102
6-7.4 Door and Frame. 102
6-7.5 Locks. 104
6-7.6 Miscellaneous Openings. 104
6-8 CLASS C VAULTS. 104
6-8.1 Walls. 104
6-8.2 Floor and Ceiling. 104
6-8.3 Door and Frame. 104
6-8.4 Locks. 104
6-8.5 Miscellaneous Openings. 104
6-9 MODULAR VAULTS. 105
6-9.1 Advantages of Modular Vaults. 105
6-9.2 Construction. 105
6-9.3 Availability. 106
6-10 ARMS, AMMUNITION, AND EXPLOSIVES AREAS. 107
6-10.1 Magazines. 109
6-10.2 Arms Rooms. 109
6-10.3 General. 109

6-10.4 Walls. 110
6-10.5 Roofs and Ceilings. 110
6-10.6 Floors. 110
6-10.7 Existing Wall, Ceiling, Roof, and Floor Reinforcement. 110
6-10.8 Doors. 111
6-10.9 Door Frames and Hardware. 111
6-10.10 Locks. 114
6-10.11 Miscellaneous Openings. 114
6-10.12 Other Storage Options. 115
6-10.13 Other Requirements. 115
6-10.14 Retrofit of Existing Arms Rooms. 115
6-11 STORAGE CONTAINERS. 115
CHAPTER 7 EQUIPMENT AND SYSTEMS 117
7-1 INTRODUCTION. 117
7-2 DISPENSABLE BARRIER SYSTEMS. 117
7-2.1 Typical Dispensable Barrier System. 117
7-2.2 Barrier Activation. 118
7-2.3 Command and Control Hardware. 118
7-2.4 Dispensable System. 118
7-2.5 Dispensing Hardware. 119
7-2.6 Response Force Time. 119
7-3 SHUTTERING SYSTEMS. 119
7-3.1 Automated Shuttering Systems. 120
7-3.2 Use of Automated Shuttering Systems. 120
APPENDIX A GLOSSARY 121
A-1 ACRONYMS. 121
A-2 DEFINITION OF TERMS. 123
APPENDIX B REFERENCES 129

FIGURES

Figure 1-1 Security Engineering UFC Application 3
Figure 3-1 Defense Layers 18
Figure 3-2 Control Zones 19
Figure 3-3 Six-Sided Approach 20
Figure 3-4 Forced Entry Design Worksheet 23
Figure 4-1 Site Areas 30
Figure 5-1 Delay times for Solid Core Filled and Reinforced CMU Walls 38
Figure 5-2 Delay times for Conventional Reinforced Concrete Walls 39
Figure 5-3 Delay times for SFR Concrete Walls 40
Figure 5-4 Door Hinge-Side Protection Threat Severity Levels II and III 59
Figure 5-5 Door Anti-Pry Strips for Threat Severity Level III 60
Figure 5-6 Vent and Duct Hardening Barriers 75
Figure 5-7 Vent Pipe and Chase Protection 76
Figure 5-8 Retrofit Hardening of 8-inch (200mm) CMU Wall (1 of 4) 79
Figure 5-9 Retrofit Hardening of 8-inch (200mm) CMU Wall (2 of 4) 80
Figure 5-10 Retrofit Hardening of 8-inch (200mm) CMU Wall (3 of 4) 81
Figure 5-11 Retrofit Hardening of 8-inch (200mm) CMU Wall (4 of 4) 82
Figure 5-12 Wood/Metal Composite Masonry Design Option 83
Figure 5-13 Welded and Riveted Steel Grating 84
Figure 6-1 Class 5 Vault Door 103
Figure 6-2 Simple Modular Vault Panel and Door Arrangement 106
Figure 6-3 Hinge Side Protection Using a Pin-in Socket 112
Figure 6-4 Hinge Side Protection Using a Forward Doorstop with Steel Angle 112
Figure 6-5 Hinge Side Protection Using an Angle Stop 113
Figure 6-6 Hinge Side Protection Using a Bar Stop 113
Figure 6-7 Internal Locking Devices 114
Figure 6-8 Storage Containers 116

TABLES

Table 2-1 Forced Entry Tool Sets 7
Table 3-1 Level of Protection Delay Times for Forced Entry 22
Table 5-1 Reinforcement Rebar Index for Concrete Masonry Walls 41
Table 5-2 Reinforcement Rebar Index for Concrete 42
Table 5-3 Reinforced Concrete Designs for Threat Severity Level V 43
Table 5-4 Wall Materials 44
Table 5-5 Roof Materials 49
Table 5-6 Floor or Ceiling Materials 53
Table 5-7 Personnel Door Panel/Edge Details, Threat Severity Level II 55
Table 5-8 Personnel Doorframe Details, Threat Severity Level II 55
Table 5-9 Door Hardware for Threat Severity Levels II and III 56
Table 5-10 Door Panel/Edge Details for Threat Severity Level III 57
Table 5-11 Doorframe Details for Threat Severity Level III 58
Table 5-12 Door Materials 61
Table 5-13 Vehicle Access Door Construction 65
Table 5-14 Glazing Specifications - Threat Severity Level II 66
Table 5-15 Frame Specifications - Threat Severity Level II 67
Table 5-16 Miscellaneous Specifications - Threat Severity Level II 67
Table 5-17 Glazing Specifications -Threat Severity Level III 68
Table 5-18 Frame Specifications - Threat Severity Level III 68
Table 5-19 Miscellaneous Specifications - Threat Severity Level III 69
Table 5-20 Window Materials 70
Table 5-21 Time Required for Making a Man-Passable Opening in Grilles 71
Table 5-22 Utility Opening Materials 72
Table 5-23 Stud-Girt Construction Retrofit Options for Threat Level III 78
Table 6-1 Penetration Ratings for Class A Vaults 101
Table 6-2 Security Risk Categories for AA&E (DODM 5100.76) 107

CHAPTER 1 INTRODUCTION

1-1 PURPOSE AND SCOPE.

1-1.1 Purpose.

The purpose of this document is to present engineering guidelines and cost-effective designs to protect assets in fixed facilities against a forced entry and providing egress in compliance with NFPA 101.

1-1.2 Scope.

Project leaders, architects, and engineers must use this UFC when designing facilities to resist aggressor forced entry. Technical information considered generally known to professional designers, architects, or engineers or readily available in existing technical references has not been included.

Designs to resist forced entry must be based on protecting specific assets, the applicable asset values, threat severity, and level of protection, which will be provided to designers as part of the design criteria developed during the security engineering planning and preliminary design phases.

1-2 APPLICABILITY.

This document provides design requirements for only fixed facilities that require forced entry threat mitigation. This UFC applies to all facilities either owned, leased, privatized, or otherwise occupied, managed, or controlled by or for DoD containing assets that required force entry protection pursuant to DOD policy.

1-3 SECURITY ENGINEERING UFC SERIES.

This UFC is one of a series of security engineering unified facilities criteria documents that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. Figure 1-1 illustrates the process from initial planning to the development of facility design requirements. The manuals in this series are designed to be used sequentially by a diverse audience to facilitate development of projects throughout the design cycle. The manuals in this series include the following:

1-3.1 DoD Minimum Antiterrorism Standards for Buildings.

UFC 4-010-01 establishes standards that provide minimum protection against terrorist attacks for the occupants of all DoD inhabited buildings. This UFC is intended to be used by security and antiterrorism personnel and design teams to identify the minimum requirements that must be incorporated into the design of all new construction and major renovations of inhabited DoD buildings. It also includes recommendations that should be but are not required to be incorporated into all such buildings.

1-3.2 DoD Security Engineering Facilities Planning Manual.

UFC 4-020-01 presents processes for developing the design criteria necessary to incorporate security and antiterrorism into DoD facilities and for identifying the cost implications of applying those design criteria. Those design criteria may be limited to the requirements of the minimum standards, or they may include protection of assets other than those addressed in the minimum standards (people), aggressor tactics that are not addressed in the minimum standards or levels of protection beyond those required by the minimum standards. The cost implications for security and antiterrorism are addressed as cost increases over conventional construction for common construction types. The changes in construction represented by those cost increases are tabulated for reference, but they represent only representative construction that will meet the requirements of the design criteria. The manual also addresses the tradeoffs between cost and risk. The Security Engineering Facilities Planning Manual is intended to be used by planners as well as security and antiterrorism personnel with support from planning team members.

1-3.3 DoD Security Engineering Facilities Design Manual.

UFC 4-020-02 provides interdisciplinary design guidance for developing preliminary systems of protective measures to implement the design criteria established using UFC 4-020-01. Those protective measures include building and site elements, equipment, and the supporting manpower and procedures necessary to make them all work as a system. The information in UFC 4-020-02 is in sufficient detail to support concept level project development, and as such can provide a good basis for a more detailed design. The manual also provides a process for assessing the impact of protective measures on risk. The primary audience for the Security Engineering Design Manual is the design team, but it can also be used by security and antiterrorism personnel.

1-3.4 Security Engineering Support Manuals.

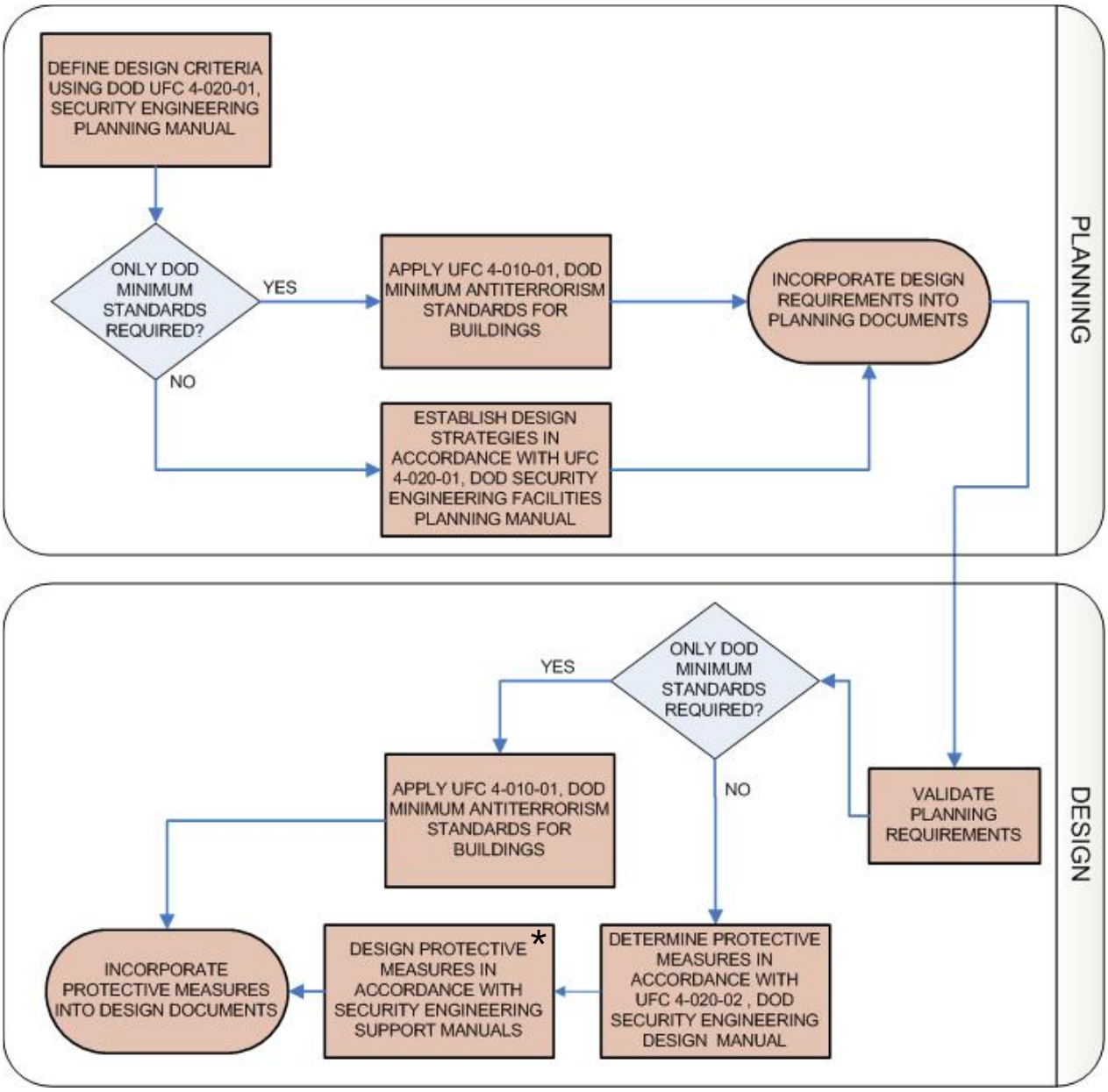
In addition to the standards, planning, and design UFCs mentioned above, there is a series of additional UFCs that provide detailed design guidance for developing final designs based on the preliminary designs developed using UFC 4-020-02. These support manuals provide specialized, discipline specific design guidance. Some address specific tactics such as direct fire weapons, vehicle borne improvised explosive devices, or airborne contamination. Others address limited aspects of design such as resistance to progressive collapse or design of portions of buildings such as mail rooms. Still others address details of designs for specific protective measures such as vehicle barriers or fences. The Security Engineering Support Manuals are intended to be used by the design team during the development of final design packages.

1-3.5 Security Engineering UFC Application.

The application of the security engineering series of UFCs is illustrated in Figure 1-1. UFC 4-020-01 is intended to be the starting point for any project that is likely to have security or antiterrorism requirements. By beginning with UFC 4-020-01, the design

criteria will be developed that establishes which of the other UFCs in the series will need to be applied. The design criteria may indicate that only the minimum standards need to be incorporated, or it may include additional requirements, resulting in the need for application of additional UFCs. Applying this series of UFCs in the manner illustrated in Figure 1-1 will result in the most efficient use of resources for protecting assets against security and antiterrorism related threats.

Figure 1-1 Security Engineering UFC Application



*** NOTE: UFC 4-026-01 is one of the Security Engineering Support Manuals.**

1-4 VULNERABILITY AND RISK ASSESSMENT.

During the pre-design phase of forced entry upgrade projects for existing facilities, a multi-functional security and antiterrorism planning team conducts a vulnerability assessment and develops risk mitigating protection requirements to a level that is both acceptable and cost effective. This document presumes risk analyses are complete prior to beginning the design phase.

For new forced entry projects, a criteria development analysis which addresses risk versus cost is conducted as part of the UFC 4-020-01 planning process.

1-5 PRESCRIPTIVE VS. RISK-BASED DESIGN REQUIREMENTS.

Dynamic conditions drive both vulnerability and risk assessments. Changes in forced entry tactics, technology, and tools of the trade affect residual risk levels. This document and other documents in the UFC series are designed to provide a method of balancing protection, budget, and risk.

The design to resist forced entry may be based on both prescriptive and risk-based requirements that together provide a solution to mitigate risk to an acceptable level.

1-5.1 Prescriptive Design Requirements.

The design for the protection of some assets may require the application of prescriptive measures contained in, or derived from, other non-UFC government regulations. For example, DoDM 5100.76 *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)* contains prescriptive requirements for facility design where arms, ammunition, or explosives are stored. Additionally, UFC 4-010-05 *Sensitive Compartmented Information Facilities Planning, Design, and Construction* contains design criteria for the construction of facilities to protect Sensitive Compartmented Information that is derived from DODM 5105.21, Vol 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security;* and from the IC Tech Spec for ICD/ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities.* (See CHAPTER 6 for further information on Protected Areas.)

1-5.2 Risk-Based Requirements.

Risk-based requirements are developed during the planning phase of the project using the procedures in UFC 4-020-01 and become a part of the project design criteria. When conditions subsequently change the risk level, designers should revisit the design criteria for methods to change or augment how protection is achieved. Not all solutions are sustainable or durable, but those based on current conditions can provide acceptable interventions for a shorter period. At end state, assessments reflect current conditions and protection is achieved at an acceptable risk level.

1-6 GENERAL BUILDING REQUIREMENTS.

Comply with UFC 1-200-01, *DoD Building Code (General Building Requirements)*. UFC 1-200-01 provides applicability of model building codes and government unique criteria for typical design disciplines and building systems, as well as for accessibility, antiterrorism, security, high performance and sustainability requirements, and safety. Use this UFC in addition to UFC 1-200-01 and the UFCs and government criteria referenced therein.

1-7 CYBERSECURITY.

All control systems (including systems separate from an energy management control system) must be planned, designed, acquired, executed, and maintained in accordance with UFC 4-010-06, and as required by individual Service Implementation Policy.

1-8 HISTORIC PRESERVATION COMPLIANCE.

1-8.1 Security and Stewardship.

The Department of Defense remains the lead federal agency in balancing security threats with the protection of historic properties. The Department of Defense abides by federal legislation on protecting cultural resources and issues its own complementary policies for stewardship.

1-8.2 Compliance with Laws.

Implementation of these standards will not supersede DoD's obligation to comply with federal laws regarding cultural resources to include the National Historic Preservation Act and the Archaeological Resources Protection Act. Installation personnel must determine possible adverse effects to historic structures and archaeological resources during project development and consult accordingly. Personnel at installations outside the United States should coordinate with the applicable host nation regarding possible adverse effects to cultural resources.

1-8.3 Compliance with DoD Standards.

Conversely, historic preservation compliance does not negate the requirement to implement other Department of Defense policy. Federal agencies are always the decision-maker in the Section 106 process of the National Historic Preservation Act. An agency should seek to avoid prolonged consultations that conflict with the imminent need to implement security requirements. Preservation considerations and antiterrorism standards are not mutually exclusive, and any compliance conflicts should be quickly and effectively resolved in consultation with appropriate stakeholders.

1-9 GLOSSARY.

APPENDIX A contains acronyms, abbreviations, and terms.

1-10 REFERENCES.

APPENDIX B contains a list of references used in this document. The publication date of the code or standard is not included in this document. Unless otherwise specified, the most recent edition of the referenced publication applies.

CHAPTER 2 DESIGN CRITERIA

2-1 INTRODUCTION.

This chapter describes the forced entry tactic and the design criteria to be used to develop a protective system to address that threat.

2-2 FORCED ENTRY TACTIC.

Forced Entry is a tactic whereby aggressors penetrate a facility through the application of tools, explosives and small arms; then, generate a passageway to operate within the target. Aggressors steal or destroy assets, compromise information, injure or kill occupants, or disrupt operations. Access passageways include walls, roofs, floors, ceilings, doors, windows, and utility portals.

2-2.1 Tools and Effects.

Forced entry tools include hand, power, and thermal tools and explosives that can be carried by one or two aggressors. Categories of forced entry tools are based on levels of sophistication, required skills and risk of detection (observability). Refer to UFC 4-020-01 for the maximum tools and explosives that each threat severity level is projected to employ. When one threat severity level is contained in the design criteria, the threat also includes the tools in all lower threat severity levels. For the purposes of this UFC, weapons are not a tool to breach construction. They are potentially used to overpower guards. (See Table 2-1 for the tools that the aggressor can use for each threat severity level.)

Table 2-1 Forced Entry Tool Sets

THREAT SEVERITY LEVEL	WEAPONS	TOOLS
V	Handguns and sub-machine guns (up to UL 752 Level 3 to overpower guards)	Bulk explosives (up to 20 lbs. /9 kg TNT); linear shaped charges (up to 10,500 grains per foot); unlimited hand, power, and thermal tools
IV		Unlimited hand, power, and thermal tools
III	None	Unlimited hand tools - limited power tools
II		Limited hand tools - low observables

NOTE: For convenience, this table has been derived from information contained in UFC 4-020-01. Information in the current version of that document takes precedence over information in this table.

2-2.2 Employment of Tools.

Forced entry can involve a combination of tools used by different group sizes for varying lengths of time. Six is the maximum number of attackers able to work together effectively when concentrated on a single opening. The high number of possible combinations of factors makes it impossible to completely predict the actual effects of a forced entry attack. Forced entry attacks must be simulated by laboratories experienced in forced entry testing to predict the resistance of specific construction components and assemblies; therefore, the effects of forced entry tool attacks are discussed not in terms of loads on building components, but in terms of the predictable effects of various individual tools.

2-2.3 Hand Tools.

Hand tools include commonly available hand-held tools requiring only manual manipulation and human strength as sources of power. These tools are used for prying, screwing, pulling, shearing, pounding, cutting, sawing, drilling, and wedging. Hand tool effects include disassembly, breaking, deformation, notching, shaving, puncturing, moving, or spalling of components and the removal of fasteners or debris. Hand tools are used for attacks in which the aggressor manipulates either an operable component (prying open a locked door) or stationary components at their intersection or seams (popping metal wall panels away from their anchors). Attacks using hand tools generate relatively less noise than powered tools, but the motion of the aggressor and vibration of the building materials, as well as the noise, might all be detectable. Hand tools can be used to create holes in lighter weight components, such as by breaking glass with a hammer or by smashing plywood or concrete block assemblies with a sledgehammer. Hand tools can also be used in combination with other tools. For example, a bolt cutter can sever steel reinforcing bars after the encasing concrete has been demolished with explosives, or wrecking bars can be used to remove materials crushed but not displaced by more sophisticated tools.

- Limited hand tools carry a low observation profile when employed due to the noise associated with using them and include claw hooks, carpenter saws, hacksaws, bolt cutters, pliers, spanner wrenches, tin snips, and wire cutters. Limited hand tools are readily available and require little skill.
- Unlimited hand tools carry a high observation profile when employed. These include, but are not limited to Kelly tools, Halligan bars, sledgehammers, cutting mauls, shovels, and axes. These tools are less common than limited hand tools and are normally part of a firefighter equipment kit.

2-2.4 Power Tools.

Power tools include electrically powered or gasoline fueled cutting and drilling tools; portable power impact tools; and hydraulic cutting, ramming, and spreading tools. Effects of power tools are breaking (including cutting of anchors and fasteners), deformation, material weakening, notching, spalling, and removal of debris. Attacks using power tools generate detectable evidence during the actual attack that includes noise, motion, vibration of the construction assembly, smoke, heat, dust, and debris. Because these tools require fuel or a power source such as a battery, they are heavier and more awkward to transport than most hand tools. Many power tools also require adequate space in which to effectively manipulate the tools. Aggressors might use power tools to sever the anchors of components, to cut locks or closing devices, or to cut or pry openings through construction materials. Power tools can be used in combination with other tools. For example, a saw might be used to cut through a concrete wall and then a ramming device can be used to displace the severed material to create an opening.

- Limited power tools operate from a self-contained power source like batteries and hydraulics. The hydraulic jack is a self-contained manually operated spreading device that works quietly.
- Unlimited power tools operate from external electric, gasoline, hydraulic pump, or compressed air power sources.

2-2.5 Thermal Tools.

Thermal tools generate flames capable of burning through steel and concrete. They include thermal cutting devices such as an oxyacetylene torch, oxygen-fueled devices such as the Kerie Cable, and the burn bar (thermal lance). Oxygen-fueled cutting devices are used to swiftly cut openings in materials, including reinforced concrete or masonry. Effects of thermal tools include material weakening, breaking, burning, cutting, and melting. Different effects are obtained depending upon the composition of the materials attacked. For example, fiberglass might melt or deform, glass might shatter due to thermal stresses, and flame-resistant materials might resist actual destruction, but the fumes or smoke produced can inhibit further efforts to destroy the assembly. Materials likely to yield to thermal attack, such as wood or plywood assemblies, might resist oxygen-fueled cutting tools longer than other assemblies. Detectable evidence yielded by thermal tools during attacks includes heat, smoke, and light. Some of these tools require oxygen and acetylene fuel tanks, which contributes to the total weight of the tool kit, and they require adequate space and ventilation. In some instances, aggressors would need to use protective safety clothing or other gear to execute an attack with these tools.

2-2.6 Explosives.

Explosives are used as forced entry tools to breach obstacles. Explosive tools include linear shape charges (LSC) and untamped and tamped breaching charges. Refer to UFC 4-020-01 for limits imposed on explosives used as forced entry tools. LSC focus energy from the explosion directly underneath the strip. The practice of backing up a charge with mass to direct the explosive effect is tamping the charge.

Explosive weights are expressed as weights that have the equivalent explosive effect as the expressed weight of trinitrotoluene (TNT). The actual explosive compound may be but is unlikely to actually be TNT.

2-2.6.1 Linear Shaped Charges.

An LSC consists of a copper v-shaped liner embedded in a similarly shaped high-explosives charge. The purpose of an LSC is to sever material. Upon detonation of the explosives, the liner collapses and a high-velocity metallic linear jet is formed. Because of its high kinetic energy, the jet can cut through materials upon impact. Typically, four lengths of LSC are placed in a picture frame arrangement on the element to be breached. Commercially available LSC have explosive weights ranging from 100 to 30,000 grains of TNT per linear foot of charge.

2-2.6.1.1 Homogeneous Materials.

Experimental data shows that the thickness of mild steel that can be severed by an LSC can be reasonably estimated by using Equation 2-1.

Equation 2-1. LSC Delay Calculation Based on Weight of Explosives

$$t = 0.027 * W^{0.547}$$

Where:
t = the thickness in inches of mild steel that can be severed by a given charge weight.
W = the weight of explosives charge in grains per foot (gpf) (linear).

To obtain the severance capability of a linear shape charge against material other than mild steel, multiply the result of Equation 2-1 by the appropriate factor from Table 2-2. The thickness given by Equation 2-1 is the limit for complete severance. If a section is only slightly thicker than the thickness given by the equation and modification factors, it can probably be severed with only minimal effort using hand tools. Because the LSC is a very debilitating tool, it is in the threat severity level V tool kit. When combined with the other tools at this severity level, custom components or materials may need to be developed and tested for the project. Example: Applying the formula to the 10,500 gpf design charge results in a 4.3-inch (109-mm) severance capability for mild steel.

Table 2-2 Mild Steel Severance Factors for Various Materials

MATERIAL	FACTOR
Mild Steel	1.00
Lead	0.67
Steel Armor	0.80
Granite	1.20
Aluminum	1.40
Rock	1.40
Concrete	1.60
Water	2.24
Green Wood	2.88
Earth	4.80
Kiln-Dried White Oak (12% moisture)	5.36

2-2.6.1.2 Composite Construction.

The adequacy of an assembly made of layers of different materials can be determined by converting the thickness of each layer to an equivalent thickness of mild steel. Divide the actual thickness of each material by the appropriate factor from Table 2-2 and sum the results for all materials in the assembly. This total equivalent mild steel thickness is then compared to the result of Equation 2-1 for the given charge weight to determine the adequacy of the composite element.

2-2.6.2 Breaching Charges.

A breaching charge is an explosive placed in direct contact with an element and detonated. The explosive materials used are typically dynamite or plastic explosives such as composition C-4 (U.S.) or Semtex (Czech Republic). Breaching charges are very effective against concrete, masonry, and thin steel elements; however, steel reinforcing bars, if present in concrete or masonry elements, usually remain intact and must be removed with bolt cutters, saws, or thermal tools after the explosion.

Tamped breaching charges are placed on the surface of the target. They are tamped by covering explosives with tightly packed sand, clay, or other dense material.

2-2.6.3 Platter Charges.

Platter charges are not included in this UFC and not identified as a forced entry tool by UFC 4-020-01. A platter charge is a sheet of explosive (either rubberized sheet explosive or a thin sheet of plastic explosive) backed by a plate of copper or steel. When the explosive detonates, the blast wave is largely projected away from the backing plate. If another lighter weight plate or disk is placed on the opposite face of the explosive charge, it will be projected like a missile in the opposite direction.

A platter charge used as a breaching tool may cut and remove most or all the reinforcing material, depending on its configuration. This will minimize the need to cut reinforcing bars with hand, power, or thermal tools after the explosive attack. A platter charge requires more explosives by weight than would be required if a regular explosive charge were used to remove the same mass of concrete. Also, size and weight of the platter, material (copper or steel), size and type of the explosive charge, and the barrier design all play critical roles in how a platter charge will perform against a specific barrier cross section. These factors plus the technical complexity, the possibility of destroying the entire structure or target, and the potential risk to the adversary, makes the use of platter charges for forced entry penetration questionable. Consequently, the following designs in this UFC are based on the use of bulk explosives in combination with hand, power, and thermal tools.

2-3 PROJECT DESIGN CRITERIA.

The project design criteria that was produced by the procedures in UFC 4-020-01 include the assets to be protected, the threat severity level, and the level of protection to be achieved in the final design of the project. These criteria dictate the elements of the protective system that must be provided in the final design.

2-3.1 Assets.

A protective system is designed to protect specific assets within a facility rather than the facility itself. Forced entry assets are those to which the aggressor must gain access for the purpose of stealing, damaging / destroying, or otherwise compromising them; examples include sensitive information, funds, controlled substances, arms, ammunition, and explosives (AA&E). The project design criteria will list the assets to be protected against a forced entry.

2-3.2 Threat Severity Level.

A threat severity level defines the composition of an aggressor team and the tools, weapons, or explosives that the team can potentially use against a facility. Threat severity levels are designated as I, II, III, IV, and V with V being the most severe. Resistance to forced entry does not require protection against threat severity level I. The project design criteria will assign one threat severity level to each asset requiring protection. When the project design criteria contain more than one asset, the facility design can protect all assets at the highest threat severity level; but, protection of each asset at the assigned threat severity level will commonly result in the most cost-effective solution.

2-3.3 Level of Protection.

The level of protection is the degree to which the protective system must defend an asset against the threat severity level. Levels of protection can be designated as very low, low, medium, high, or very high. The higher the level of protection, the lower the risk of asset compromise. The project design criteria specify the level of protection to be provided for each asset. Since the associated cost increases as the level of protection increases, the level of protection must balance risk at a reasonable cost.

Levels of protection for the forced entry tactic relate to the probability that the aggressors will be intercepted by a response force before the assets are compromised. The probability of the intercept is composed of the probability of detecting the aggressors and the probability of the response force arriving in time. The probability of intercept is increased by increasing the number of detection layers, or by increasing the delay time provided by protection measures between the point of detection and the asset. Delay that occurs prior to a detection layer may provide a deterrent to low level aggressors but does little to improve the probability of intercept. The response time that must be met with delay elements varies from the minimum to the maximum expected time depending on the level of protection. Refer to UFC 4-020-01 for the levels of protection for the forced entry tactic. The probability of intercept is also a function of the sophistication and design of the detection system.

2-3.4 Design Constraints.

The project design criteria may include constraints on the protective system design based on the project user’s operational or functional considerations and constraints imposed by regulations.

This Page Intentionally Left Blank

CHAPTER 3 DESIGN GUIDANCE TO RESIST FORCED ENTRY

3-1 GENERAL DESIGN STRATEGY.

The general design strategy for the forced entry tactic is to detect aggressors either prior to their reaching barriers or as they attempt to breach them and then to provide sufficient delay to forced entry in the construction of those barriers to allow responding forces to arrive and defeat the aggressors before they can compromise assets. Inherent in this strategy, therefore, is that there is an intrusion detection system that provides an alarm to a monitoring station in response to intrusion and that there is a response force that can respond to an alarm and reach its location before aggressors are able to breach the barriers between that point and the assets being protected.

3-2 SPECIFIC DESIGN STRATEGIES.

The specific design strategies associated with the different levels of protection vary by the amount of delay provided and the sophistication of the intrusion detection. Note that the levels of protection have specific delay times associated with them. Those delay times are generalized goals, but if the planning team is confident that response times are either more or less than those associated with the applicable levels of protection, the applicable delay times may have to be adjusted. All building elements in the protective envelope that provides the delay time must provide at least the minimum delay time associated with the applicable level of protection based on the assumption that aggressors will always be able to identify the weakest element in the envelope. That protective envelope may be all in one layer, such as the shell of a room or the exterior of a building, or it may encompass multiple layers such as the building exterior and multiple rooms arrayed in rings around the asset. The detection element of the protective system may also include closed circuit television (CCTV) to assess the validity of alarms. The criteria associated with the levels of protection are summarized in Table 3-1 and described below.

Table 3-1 Forced Entry Levels of Protection Summary

LEVEL OF PROTECTION	PERFORMANCE
Low	Provide construction that provides at least 1 minute of delay and provide intrusion detection sensors at all operational openings.
Medium	Provide construction that provides at least 5 minutes of delay and provide a complete ring of intrusion detection sensors
High	Provide construction that provides at least 15 minutes of delay and provide a complete ring of intrusion detection sensors with two different sensor phenomenologies
Very High	Provide construction that provides at least 30 minutes of delay and provide a complete ring of intrusion detection sensors with two different sensor phenomenologies

3-2.1 Low Level of Protection.

The specific design strategy associated with this level of protection incorporates an envelope of building elements (walls, roofs, floors, ceilings, doors, windows) surrounding an asset that provides a delay time to the specified threat tools of at least 1 minute. In addition, the protective system incorporates intrusion detection sensors at all operable openings. Entry though other building elements would be detected through operational procedures, such as roving patrols.

3-2.2 Medium Level of Protection.

The specific design strategy associated with this level of protection incorporates an envelope of building elements (walls, roofs, floors, ceilings, doors, windows) surrounding an asset that provides a delay time to the specified threat tools of at least 5 minutes. It also incorporates a complete ring of detection covering all possible approaches through the protective envelope.

3-2.3 High Level of Protection.

The specific design strategy associated with this level of protection incorporates an envelope of building elements (walls, roofs, floors, ceilings, doors, windows) surrounding an asset that provides a delay time to the specified threat tools of at least 15 minutes. It also incorporates a complete ring of detection covering all possible approaches to the asset. That ring must include two different sensor phenomenologies covering each approach.

3-2.4 Very High Level of Protection.

The specific design strategy associated with this level of protection incorporates the same delay and detection elements as the high level of protection, but the delay time is at least 30 minutes.

3-3 DESIGN PROCEDURES.

If the project is for new construction, review Paragraph 3-4 through Paragraph 3-8 of this document; then, use Chapters 4 through 7 to develop preliminary layout and design of the facility. Following preliminary layout and design, follow the procedures for calculating system delay starting in Paragraph 3-9. If the project is for an existing facility, review Paragraph 3-4 through Paragraph 3-8; then, follow the procedures for delay calculations starting in Paragraph 3-9.

3-4 PROTECTIVE SYSTEM.

Provide an integrated and layered protective system for the facility that is designed to deter, and if that fails, provide detection and physical barriers that provide enough delay time for a response force to defend/defeat the aggressor.

The protective system must operate on the principles of deter, detect, delay, deny, defend/defeat as defined in UFC 4-020-01.

- Deter is the prevention of an action by the existence of a credible threat of unacceptable counteraction or belief that the cost of action outweighs the perceived benefits.
- Detect is to assess possible aggressor action, or sensor/alert transmission that an event has occurred.
- Delay is the capability to interrupt or neutralize an aggressor's activities.
- Deny prevents an aggressor from access, theft or generating casualties.
- Defend / defeat prevents unauthorized access and safeguards assets.

3-5 SECURITY IN DEPTH.

Security in Depth (SID) is a combination of layered and complementary security controls sufficient to deter, detect, and document unauthorized entry and movement within the installation and/or facility and the ability to delay and respond with force. Refer to UFC 4-020-01 for additional information on SID.

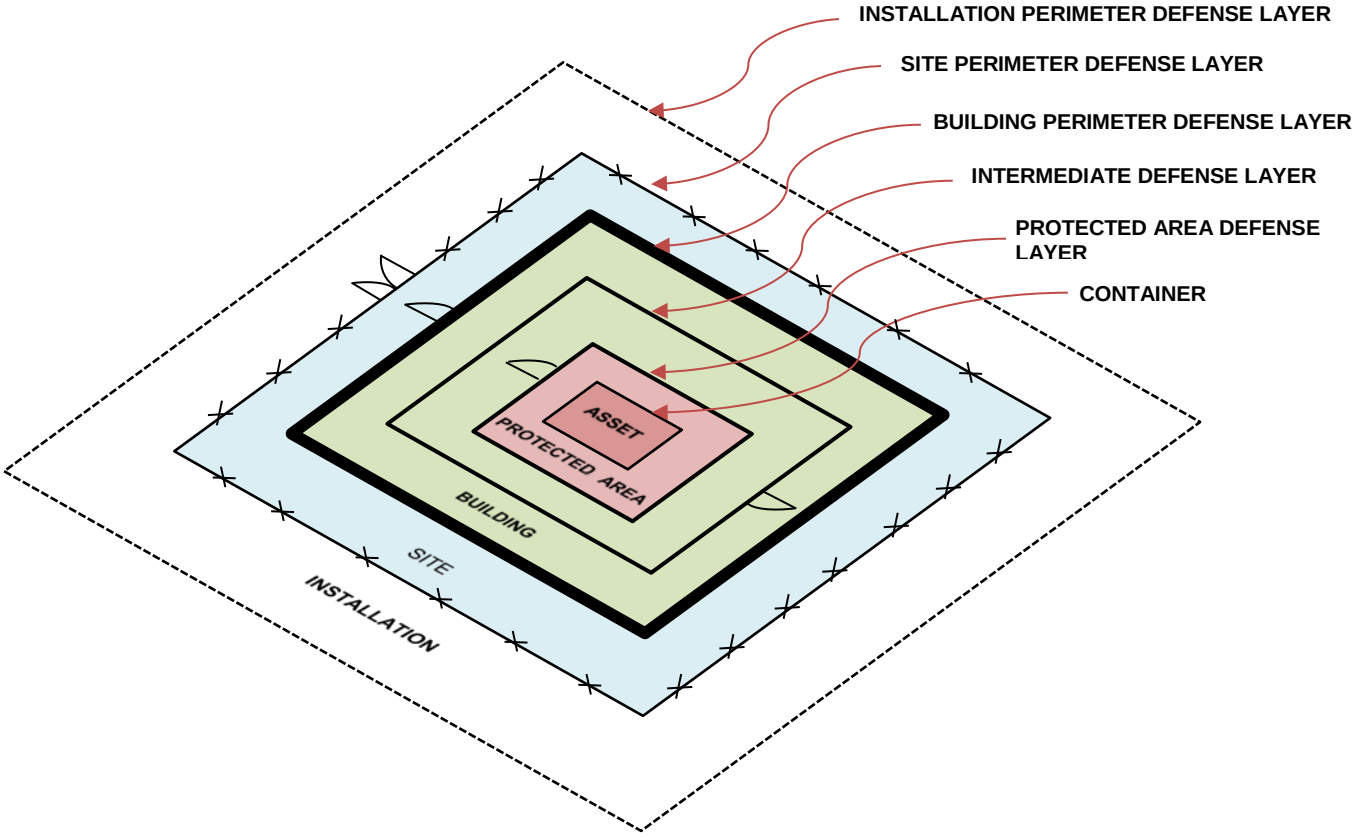
The project protective system should provide SID; and, when possible, consist of multiple defense layers and complementary control zones. If the project is being located within a larger installation, SID begins at the installation boundary.

3-6 DEFENSE LAYERS.

Each defense layer must consist of physical barriers that will delay the aggressor attempt to penetrate the layer and detection measures to provide early warning of the aggressor attempt. Detection measures may use electronic security systems (ESS) to provide the early warning or rely on visual observation by installation personnel or roving guards.

Figure 3-1 illustrates a protective system with multiple defense layers. Defense layers in the illustration are identified as installation perimeter, site perimeter, building perimeter, intermediate, protected area, and container.

Figure 3-1 Defense Layers

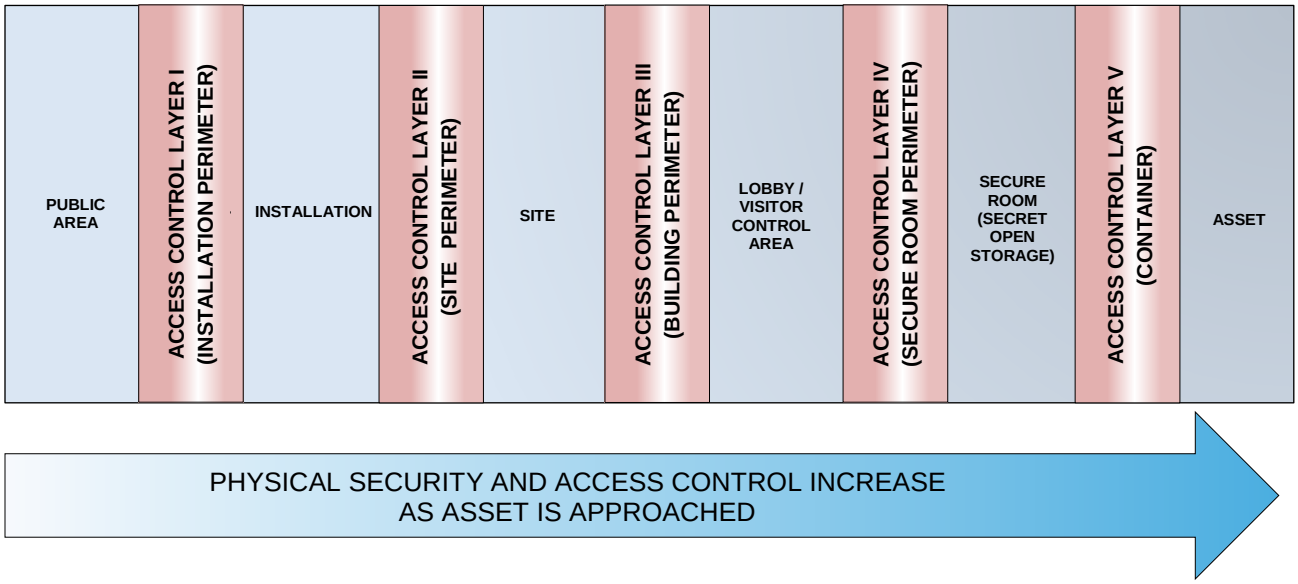


3-7 CONTROL ZONES.

Control zones are groupings of functional areas where access to a zone is restricted to site or building inhabitants who are required to work in the zone. If configured correctly, having multiple access control layers within an installation or facility can enhance the security of the higher security zones. This is accomplished by requiring personnel to transition through increasingly secure access control layers prior to accessing the protected area with the high value asset. Control zones may include installation access, site access, building access, restricted access, or protected area access.

Figure 3-2 illustrates a model for establishing control zones within a layered defense using an installation perimeter, site perimeter, building perimeter, secure room (protected area), and container.

Figure 3-2 Control Zones

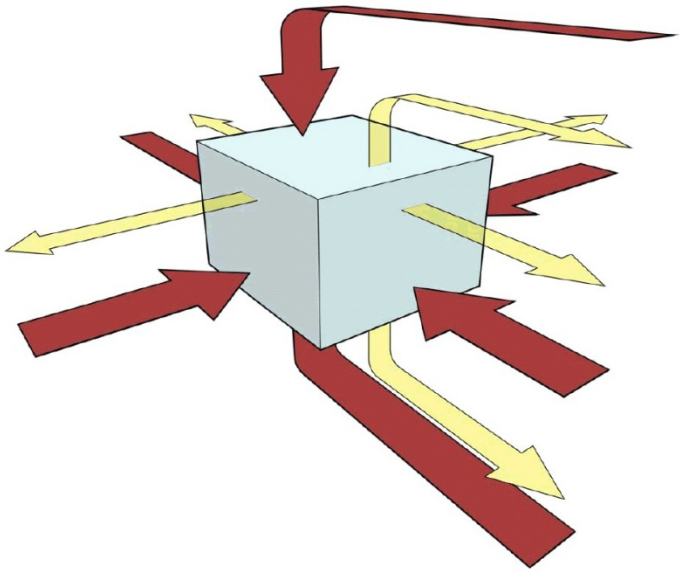


3-8 LAYOUT CONSIDERATIONS.

Except for a site perimeter, use a six-sided approach when designing each defense layer. The walls, floor, roof or ceiling, and any penetrations of the defense layer must be designed so that all elements meet the delay rating for the layer. See Figure 3-3 for a diagram of the six-sided approach.

Chapter 4 describes detailed site layout and design. Chapter 5 describes detailed building layout and design.

Figure 3-3 Six-Sided Approach



3-8.1 Multiple Assets.

Since the design basis threat is focused on assets, not all assets will require the same threat severity level and levels of protection. If there are multiple assets, evaluate each asset and the design criteria associated with it and factor that into how the building is laid out.

When the design criteria contain multiple assets to be protected, consider grouping the protected areas containing those assets together unless prohibited by prescriptive requirements such as a minimum interspatial distance required for explosives.

3-8.2 Multiple Buildings in Project.

When the design project contains more than one building, consider locating assets in a building near the center of the complex.

3-8.3 Multiple Aggressor Tactics.

When the design criteria contain multiple aggressor tactics, each tactic will have a threat severity level and an associated level of protection. Provide design features that protect the assets against the forced entry tactic and associated level of protection, enhanced by requirements to protect against other aggressor tactics and associated levels of protection.

When there are multiple applicable tactics, each tactic will have to be addressed separately and the resulting protective measures will have to be integrated into a comprehensive solution that addresses all tactics. In doing so, the tactics should be addressed in order from the one that has the greatest potential impact on building

construction to the tactic with the least impact. For example, construction to protect against explosives related tactics may require heavy construction that may be a greater requirement than the forced entry resistance but may prove to be advantageous to forced entry resistance.

3-8.4 Multiple Defense Layers with Common Roofs or Ceilings.

Some forced entry projects may necessitate that two or more defense layers have common roofs or ceilings. The pathway to the asset may be through the roof and ceiling, the floor or through the walls and doors. Either pathway must meet the required system delay.

3-9 ESTABLISHING REQUIRED PROTECTIVE SYSTEM DELAY TIME.

An effective protective system requires that any aggressor attempt to attack the facility must be detected so that response forces can interrupt and neutralize the aggressor's attack before his goal can be achieved. Since it is usually not feasible to maintain a response force to provide immediate protection for all assets, a comprehensive aggressor detection and delay plan is needed.

3-9.1 Delays for Multiple Assets.

When the design criteria list multiple assets to be protected, each with an applicable level of protection, delay can be provided for the protection of all assets at the highest level of protection, but a more cost effective design may entail providing delay for each asset listed according to the level of protection assigned to that asset.

3-9.2 Establish Minimum and Maximum Response Times.

Minimum or maximum response time refers to the minimum or maximum possible time in which the response force can reach an engagement area. Consult with facility operations personnel, facility security personnel, and the base Facility Antiterrorism Officer to establish response force tactics including potential engagement areas and the minimum and maximum response times for each asset. For some assets, such as Sensitive Compartmented Information, response time is dictated by policy.

3-9.3 Establish Required Protective System Delay Times.

Defense layers surrounding an asset must collectively provide detection and enough physical delay for a response force to intercept the aggressors, either before the asset is compromised or before the aggressor escapes.

Calculate the required collective protective system delay time based on the minimum or maximum response times using the requirements in Table 3-2.

Table 3-2 Level of Protection Delay Times for Forced Entry

LEVEL OF PROTECTION	REQUIRED DELAY TIME
Very Low	Delay does not apply to this level of protection.
Low	The required delay time is greater than the minimum possible response time.
Medium	The required delay time is greater than the minimum possible response time.
High	The required delay time is greater than the maximum possible response time.
Very High	The required delay time is 25% greater than the maximum possible response time.

3-10 EVALUATING SYSTEM DELAY IN PRELIMINARY DESIGN.

Use the Forced Entry Design Worksheet, Figure 3-4, to document the delay times included in the preliminary design for each asset. Enter the project and asset descriptions; date; minimum/maximum response times, level of protection, and threat severity level assigned to the asset in boxes 1 through 5b.

Enter the protective system delay time calculated in Paragraph 3-9 in Box 5c of the Forced Entry Design Worksheet.

Figure 3-4 Forced Entry Design Worksheet

1. PROJECT / BUILDING IDENTIFICATION	2. ASSET IDENTIFICATION	3. DATE

4a. MINIMUM RESPONSE TIME	4b. MAXIMUM RESPONSE TIME	5a. LEVEL OF PROTECTION	5b. THREAT SEVERITY LEVEL	5C. REQUIRED DELAY

6. DEFENSE LAYER	7. LAYER ELEMENT	8. ELEMENT PHYSICAL DELAY RATING	9. LAYER PHYSICAL DELAY RATING	10. OUTER-MOST DEFENSE LAYER?
CONTAINER				
PROTECTED AREA				
INTERMEDIATE LAYER				
BUILDING PERIMETER				
SITE				

ESTIMATED AGRESSOR ESCAPE TIME	12.	SYSTEM DELAY RATING	11.	

3-10.1 Physical Delay Ratings.

The physical delay rating for a defense layer (construction) element is the time it takes for the aggressor to breach and pass through the element. This rating will include the attack time, the tool penalty, and the skill penalty, as applicable. For traditional elements such as walls, door, and windows used in both new and retrofit construction design, these delay ratings, based on threat severity levels can be found in Chapters 5 and 6.

Additionally, Chapter 7 discusses the use of dispensable barrier and shuttering systems that can be used to further delay a forced entry attempt. For use of these systems, consult with subject matter experts in coordination with facility operations and security personnel.

3-10.1.1 Defense Layer Element Physical Delay Ratings.

Enter the construction elements for each defense layer used in the preliminary design in the appropriate spaces in column 7. For example, building perimeter elements might include walls, roofs, floors, ceilings, doors, windows, and utility openings.

Enter the corresponding delay rating for each element in column 8. If there is no entry in Chapters 5 or 6 for a design element at the required threat severity level, use the delay time for the next lower threat severity level for which data is available.

3-10.1.2 Layer Physical Delay Ratings.

Ideally, all element delay ratings within a layer will be equal, providing a consistent defense; however, aggressors will exploit the weakest element in a defense layer. Thus, the layer delay rating for a given defense layer equals the least delay time among the elements of that layer. Determine the layer delay rating for each defense layer and enter that rating in the appropriate space in column 9.

3-10.1.3 System Delay Rating.

The total system delay is the sum of the defense layer delay ratings in Column 9. Enter the total system delay time in box 11.

3-10.1.4 Aggressor Escape Time.

If the goal in protecting an asset is to keep it from being removed from the facility rather than to deny access to the asset, enter an estimate of the time necessary for an aggressor to escape from the facility in box 12. Note that the escape delay time through each layer will likely be significantly shorter than for entry because of use of emergency exits or use of penetrations created during initial breaching of the layer.

3-10.2 Outermost Defense Layer.

The outermost defense layer is the layer at which the sum of the delay ratings for that layer and layers interior to it is equal to or greater than the required delay time (box 5c). Column 10 of the Forced Entry Design Worksheet is used to indicate the calculated outermost defense layer. The outermost defense layer is the point at which detection is achieved. Where electronic security systems (ESS) are used as part of the protective system, it is the point at which sensors will be placed. Refer to UFC 4-021-02 for design of ESS.

3-11 DESIGN ADJUSTMENT.

If the system delay rating (box 11 of the Forced Entry Design Worksheet) is less than the required delay time (box 5c) or if the outermost defense layer is at an unacceptable location, add defense layers or upgrade layer components. It is usually more efficient to upgrade layers closer to the asset because the size of the inner layers is smaller as is the resulting protected area volume. To upgrade existing defense layers, start with the component with the least delay rating. Select different construction components if the facility is new construction. Replace or retrofit vulnerable existing construction components. Fill out a new Forced Entry Design Worksheet if significant changes are made to the initial defensive system.

This Page Intentionally Left Blank

CHAPTER 4 SITEWORK

4-1 INTRODUCTION.

This chapter applies when the design criteria require that the project establish a building compound with a dedicated site perimeter and open areas between the site perimeter and the building housing the asset to be protected. When required, the building compound may provide the first opportunity for forced entry delay.

a. Not all resistance to forced entry projects will require the establishment of a building compound. In that case, the building perimeter provides the first defense layer; refer to Chapter 5 for building designs.

b. Not all resistance to forced entry projects will be located on an existing Government installation. When the establishment of a building compound is required by the design criteria, this UFC is applicable for both a site located on an existing installation and a stand-alone site.

c. This UFC does not address the design of installation perimeters.

4-2 SITEWORK ELEMENTS.

Sitework elements such as chain-link fences, gates, and entry portals are not likely to delay a small group of well-equipped and dedicated aggressors; however, managing the site perimeter and open areas external to buildings:

- assists in building access control,
- minimizes hidden spots and concealed avenues of approach for an aggressor,
- provides opportunities for observation and detection, and
- may provide a platform for sensors (such as fence mounted sensors).

4-3 CRIME PREVENTION THROUGH ENVIRONMENTAL DESIGN.

Crime prevention through environmental design (CPTED) is the proper design and effective use of the built environment that can lead to a reduction in the fear and incidence of crime, and an improvement in the quality of life. Consider using CPTED concepts in the design of the projects to make the facility less attractive to aggressors considering forced entry. The main features of CPTED are natural access control, natural surveillance, and territorial reinforcement.

For further information on CPTED, See:

- Publications by the National Institute of Law Enforcement and Criminal Justice.
- Crowe, Timothy D., *Crime Prevention Through Environmental Design*. National Crime Prevention Institute (1991).

4-3.1 Natural Access Control.

Natural access control includes design features that clearly indicate public routes and discourage access to private structural elements. These features decrease an opportunity for crime by creating in an offender a perception of unacceptable risk when attempting access to private areas, which marks the stranger as a possible aggressor. Such design features include placement of entrances and exits, fencing, and landscaping to control traffic flow.

4-3.2 Natural Surveillance.

Natural surveillance includes design features that increase the visibility of a property. These features maximize the ability of persons in the area to see persons in the vicinity and avoid trouble and allow external activities to be seen from adjacent building structures by persons who could call for help. Such design features include landscaping, lighting, window and stairway placement, and building entrance and garage layouts.

4-3.3 Territorial Reinforcement.

Territorial reinforcement includes design features that clearly indicate public and private structural elements of a property. An individual will develop a sense of territoriality for a space with frequent activities in an area, a sense of ownership. With this feeling of ownership, the individual will want to defend his environment. This ownership does not necessarily mean legal ownership; it maybe a perceived ownership, such as the sense of ownership that employees feel for the office in which they work. The sense of territory and ownership by an individual is reinforced through regularly scheduled activities, inspections, and maintenance.

4-4 SITE LAYOUT CONSIDERATIONS.

To optimize the site layout for security and function, architects, engineers and security personnel must work together to understand the layout of operational spaces within the site such as parking, landscape and drainage features, lighting, and trash collection areas in addition to visitor and vehicle access and escort requirements. This takes an integrated design approach that balances the site's operational and space requirements. If space permits, the site layout should be designed to provide early detection of aggressor movement toward the building. See Paragraph 4-6 for application of clear zones and unobstructed space.

The following are site-related layout considerations:

- Establish a well-defined perimeter using fences, walls, or a combination of both.
- Provide an intrusion detection system (IDS) at site perimeter to detect aggressor attempt to penetrate site.
- Provide only one personnel entry control point (ECP) and one vehicle ECP into the site.

- Locate facility within view of other occupied facilities.
- Locate assets stored outside of the facility within view of occupied rooms of the facility.
- Eliminate potential hiding places for aggressors.
- Minimize or eliminate signs or other indicators of asset location.
- Illuminate building exterior or exterior sites where assets are located.

4-5 SECURITY FENCING.

Security fencing is effective at delineating a boundary and at keeping honest people honest, but ineffective for preventing a forced entry. The design strategy for forced entry is based on delaying the aggressor, and any serious aggressor could climb a fence in less than four seconds or can cut through a fence in less than ten seconds; however, fences can provide an important role in the early detection of an aggressor's forced entry attempt. An aggressor must make an overt action to breach the fence, which allows them to be intercepted in accordance to the rules of engagement. Refer to UFC 4-022-03 for the functions and design of security fences.

4-5.1 Gates for Fences.

Gates control authorized pedestrian and vehicular traffic and flow. They establish entry and exit points into an area defined by fences. They are a component of the perimeter fence and must be as effective as the associated fence in order to provide an equivalent deterrent. Gates normally require additional hardening features for hinges and locking mechanisms due to their operation and inherent vulnerability. Use designs in UFC 4-022-03 for gates and hardware. When required, design ESS in accordance with UFC 4-021-02 for associated alarms.

4-5.2 Utility Openings in Fence Lines.

Drainage ditches and culverts may pass through or under a perimeter fence. If those openings create a cross-sectional area greater than 96 square inches (619 cm^2) and a smallest dimension greater than 6 inches (150 mm), they must be protected using designs in UFC 4-022-03. Ensure that any addition of grilles or pipes to culverts or other drainage structures is coordinated with civil engineers so that they can compensate for the diminished flow capacity and additional maintenance that will result from the installation.

4-5.3 Walls in Fence Lines.

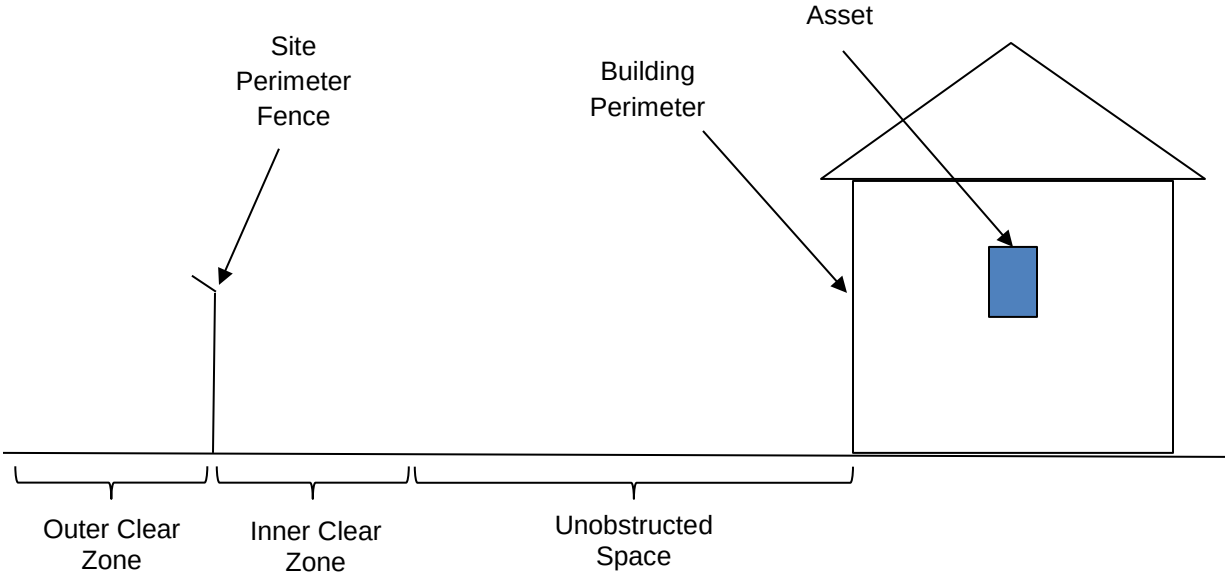
Walls can be used to replace part, or all, of a security fence in the site perimeter. Alternatively, a short wall topped by a fence can be used in the site perimeter.

Walls and walls topped with a fence should provide security features equivalent to that of a security fence. Refer to UFC 4-022-03 for the functions and design of security fences.

4-6 CLEAR ZONES AND UNOBSTRUCTED SPACE.

The space between the site perimeter (security fence) and the facility buildings consists of an inner clear zone and an unobstructed space (Figure 4-1). Additionally, there may be an outer clear zone that is outside of the site perimeter.

Figure 4-1 Site Areas



4-6.1 Clear Zones.

When a site perimeter fence is required, clear zones are areas established on both outer and inner sides of a security fence to provide an unobstructed view to enhance detection and assessment. Refer to UFC 4-022-03 for application of clear zones at fence lines and UFC 4-010-01 for application of clear zones around inhabited buildings.

4-6.2 Unobstructed Space.

Unobstructed Space is an area around inhabited buildings in which there are no opportunities for concealment from observation of explosive devices 6 inches (150 mm) or greater in height or width. Refer to UFC 4-010-01 for minimum requirements for unobstructed space.

4-7 SITE PERIMETER ENTRY CONTROL.

Depending on the project, entry control points may be required in the site perimeter. Consult with facility operations personnel and facility security personnel for entry control requirements for the project perimeter.

4-8 DETECTION.

For forces to respond to an attempted forced entry, the threat must be detected. This may be accomplished by visual observation, IDS, or CCTV. Initial threat detection should occur at the outermost defense layer, either at the site perimeter or at the building perimeter. Refer to UFC 4-021-02 for additional information and designs for IDS and CCTV employment at the outermost defense layer.

4-9 SECURITY LIGHTING.

Security lighting provides illumination during periods of darkness or in areas of low visibility to aid in the detection, assessment, and interdiction of aggressors by security forces. Lighting may also be a deterrent to some aggressors.

Consult with facility operations and facility security personnel, including ESS specialists, for security lighting requirements. When required, design lighting in accordance with UFC 3-530-01.

This Page Intentionally Left Blank

CHAPTER 5 BUILDING ELEMENTS

5-1 INTRODUCTION.

Building elements include the building layout, walls, roofs, ceilings, floors, doors, windows, and utility openings. Designs for each element type are presented in separate sections within this chapter.

5-2 BUILDING LAYOUT.

Effective building layout enhances resistance to forced entry by making assets harder to find and more time-consuming to reach, by making escape more difficult, and by taking advantage of inherent monitoring opportunities by occupants. Some related considerations also influence building layout. Several defense layers surrounding an asset may be more cost-effective than a single layer that provides the total delay time. Minimizing the actual protective volume (all sides of a space must be considered) around an asset reduces construction and detection system costs and surveillance requirements. Deciding whether to consider delay time in terms of the aggressor's ingress time only (time required from detection until the aggressor reaches an asset) or ingress plus egress time (including escape time after compromising or stealing an asset) can also influence building arrangement. Finally, design the building such that interior signage, which may indicate an asset's existence or location is unnecessary.

To optimize the building layout for security and function, the designer must understand the various secure spaces in the facility, the security clearances of the occupants, visitor access and escort requirements and the separations or adjacencies required. This takes an integrated design approach that balances the occupant's operational and space requirements, visitor control requirements, security-in-depth and the concept of control zoning. If building operations permit, the building layout should be designed to complicate aggressors' movement toward the asset by requiring that they be forced to take complicated routes and be equipped with a number of different tools and skills. In developing the building layout:

- Maximize the vertical and horizontal separation between the lowest and highest security areas.
- Maximize grouping of secure areas to enhance floor/ceiling security and to minimize locations of secure elements.
- In large facilities, locate the highest security area in the building center, on an upper floor, or in the basement.
- When a facility has multiple security levels and functionally compatible missions, access to the highest security area should be through the area with the next lower security level.

5-3 BUILDING COMPONENTS.

Defense layers consist of construction components and assemblies including walls, roofs, floors and ceilings, doors, windows, and utility openings, which delay an aggressor from reaching an asset. Consider building components that may be attacked horizontally or vertically from all sides of a space. The penetration delay time for any layer equals the least penetration delay time for any single component of that layer.

The materials from one type of component can be used for another type of component; for example, wall materials can be used for ceilings or window materials can be used for skylights. When making these substitutions, penetration delay times must be adjusted since horizontal and vertical attacks on the same materials yield different penetration delay times; for example, the penetration delay time for a downward attack on a 6-inch (150-mm) concrete roof slab is lower than a similar attack on a 6-inch (150-mm) concrete wall.

5-4 FORCED ENTRY RESISTANT BUILDING COMPONENT TABLES.

This Chapter provides a series of tables containing forced entry resistant building components and the delay times they provide against the four possible threat severity levels for the forced entry tactic. There are separate tables for walls, doors, windows, roofs, floors, and utility openings. Each component table is located within the paragraph of this chapter devoted to the respective component.

5-4.1 Data Formulation.

The tables contain only components which have been tested or otherwise analyzed for forced entry resistance. Although the components in the tables are representative, they are not the only components available. New technology is used to develop improved components, and testing may have been performed that is not reflected in the tables. Users of this manual must therefore supplement it with whatever other data is available to them; however, only data based on actual testing or formal analysis should be used. Manufacturers' data may be based on limited testing or assumptions and may not accurately reflect the tools associated with the threat severity levels discussed in this manual.

The data in these tables was derived from actual tests and on estimates based on such tests. The total delay time consists of three elements: (1) the attack time, (2) the tool penalty, and (3) the skill penalty.

5-4.1.1 Attack Time.

The attack time is the actual time that it took the person or persons performing the test to make a man-passable opening of 96 square inches (619 cm^2) in the designated building component under laboratory conditions. Some data is based on estimates or delay times based on tests of similar materials with the same tools.

5-4.1.2 Tool Penalty.

The tool penalty is an additional delay time added to the attack time to account for difficulties associated with using some tools. It does not apply for all tools.

5-4.1.3 Skill Penalty.

The skill penalty is an additional delay time added to the attack time and tool penalty to reflect an unskilled user's inefficiency in using the tools. Again, the skill penalty does not apply to all tools.

5-4.2 Advantages of Composite Components.

A composite construction component such as a wall, floor, ceiling, or door built with two or more types of materials such as wood, metal, concrete, or foam provides significant delay over a component built with a single material since it requires aggressors to use multiple tools to breach the component.

Thermal tools can cut through metal but do not work well on wood, and power tools commonly get fouled up by foams. Explosives can blast holes in concrete but generally leave the reinforcing bars intact, requiring the aggressors to switch to cutting tools to complete the breach. Note that many of the entries in the tables in this chapter include such cross sections.

5-4.3 Data Application.

The attack time and the tool and skill penalties are already incorporated into the total delay times shown in the tables. All three quantities are applied to arrive at the total delay time for the threat severity levels II and III. The skill penalty is not applied for the threat severity level IV because aggressors operating at that threat severity level are assumed to be skillful at using the tools they select; they may still select tools which are difficult to use, and they are therefore still assigned a tool penalty. The aggressors to whom the threat severity level V applies are assumed to be skillful at using the tools they select and to select only tools which are not too difficult for them to use; therefore, no penalties are associated with the threat severity level V.

5-4.4 Using the Tables.

The tables provide the delay times for building components for the four possible threat severity levels applicable to the forced entry tactic. The second column in each table provides a description of each component with which a delay time is associated. Components may be used as a stand-alone application in new construction or as a retrofit. The third through sixth columns on the tables indicate the total delay times in minutes for various threat severity levels. Each identified building component resists the tools associated with the forced entry threat severity level for the time indicated. Where there are no entries under a given threat severity level, no testing or analysis has been done for that component for that level. In those cases, either select another component or use the next higher threat severity level for which data is available. Using higher threat severity levels will always be conservative.

5-4.5 References to Explosives Use.

The threat severity level V includes the potential for the use of explosives. The delay times associated with explosives are indicated by an asterisk (*). Where testing was done on a building component at threat severity level V without using explosives, that value is also indicated. In such cases the delay time entry will appear as two numbers, such as 10/<1*. The 10 refers to the delay without explosives and the <1* refers to the delay assuming the use of explosives. If the aggressor is unlikely to use explosives due to their noise, their potential for damaging the asset, or for any other reason the planning team establishes, use the value which does not include explosives.

5-5 NEW CONSTRUCTION.

This section provides design options for hardening a new building against forced entry penetration. The objective is to identify construction choices that assure a balanced security design between all building components; approximately equal penetration delays against a given threat severity level.

5-5.1 Walls.

Solid plywood or expanded metal construction can be used to resist a low severity threat. For threat severity levels III and IV, the choices are limited to grout-filled and reinforced concrete-masonry unit (CMU) for lower delay time requirements, and conventional or steel-fiber-reinforced (SFR) concrete for higher delay time requirements. Protection against threat severity level V will require sacrificial areas, multiple barriers, or reinforced concrete barriers.

5-5.1.1 Walls to Resist Threat Severity Level II.

Since conventional wall construction such as stud-girt construction using less than 3/4-inch (19-mm) plywood, stucco, gypsum, composite, light sheet metal, and conventional masonry provides a delay of less than one minute against threat severity level II, use one of the wall types shown in Table 5-4.

5-5.1.2 Walls to Resist Threat Severity Levels III and IV.

Use solid-filled and reinforced CMU; conventional reinforced concrete; SFR concrete; or masonry, wood, metal, and plastic composite walls.

Solid core, filled, and reinforced CMU, conventional, SFR concrete wall construction options and corresponding minimum penetration delay for threat severity levels III and IV are shown in Figure 5-1 through Figure 5-3. Note in Figure 5-1 through Figure 5-3 that the minimum penetration delay times are presented as a function of the thickness of the cross section and the size and spacing of reinforcing bars. Different combinations of reinforcing bar size and spacing are identified by capital letters from Table 5-1 for masonry and in Table 5-2 for reinforced concrete. In general, a required penetration delay time can be achieved either by providing a thicker cross section or by adding more reinforcement. Table 5-4 provides options that can be considered based on structural and cost considerations.

5-5.1.2.1 Security Threat Level III.

a. CMU walls: As shown in Figure 5-1 and Table 5-1, penetration delay times up to about 5.5 minutes are achievable using mortar filled CMU. The use of reinforcing bars in the core is required for higher penetration delay times.

b. Conventional Reinforced Concrete. As shown in Figure 5-2 and Table 5-2, penetration delay times up to 7.5 minutes are achievable with 6 inches (150 mm) of reinforced concrete with the B-curve reinforcing bar combination.

c. SFR Concrete. As shown in Figure 5-3 and Table 5-2, penetration delay times up to about 11 minutes are achievable with 6 inches (150 mm) of SFR concrete with the B-curve conventional reinforcing bar combination. The steel fiber is at least 5 percent by volume of the concrete mix.

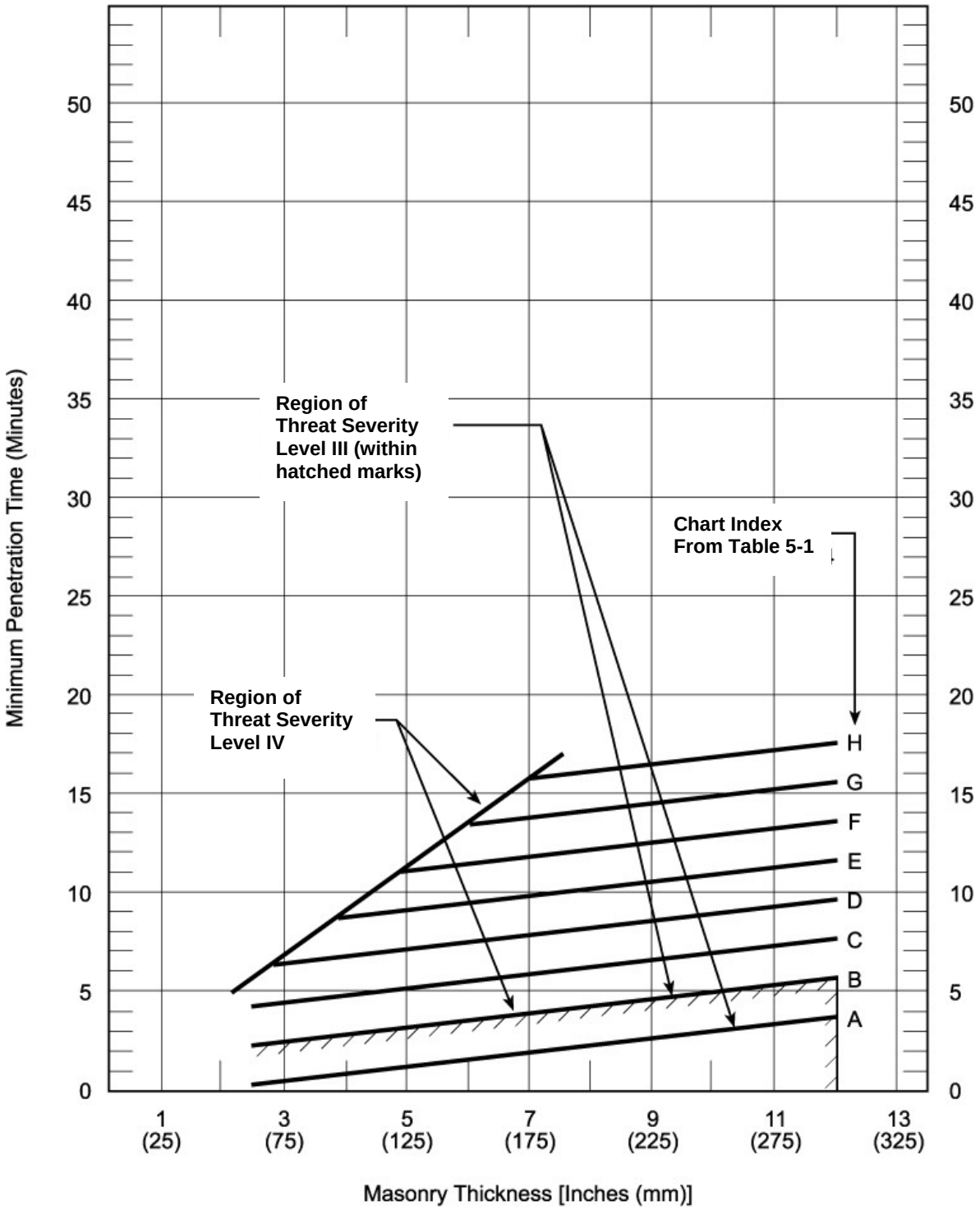
5-5.1.2.2 Security Threat Level IV.

a. CMU walls: Figure 5-1 with Table 5-1, gives CMU and reinforcing bar combinations that can provide penetration delay times up to 18 minutes.

b. Conventional Reinforced Concrete. Figure 5-2 with Table 5-2, gives conventional concrete thickness and reinforcing bar combinations that can provide penetration delay times up to 35 minutes.

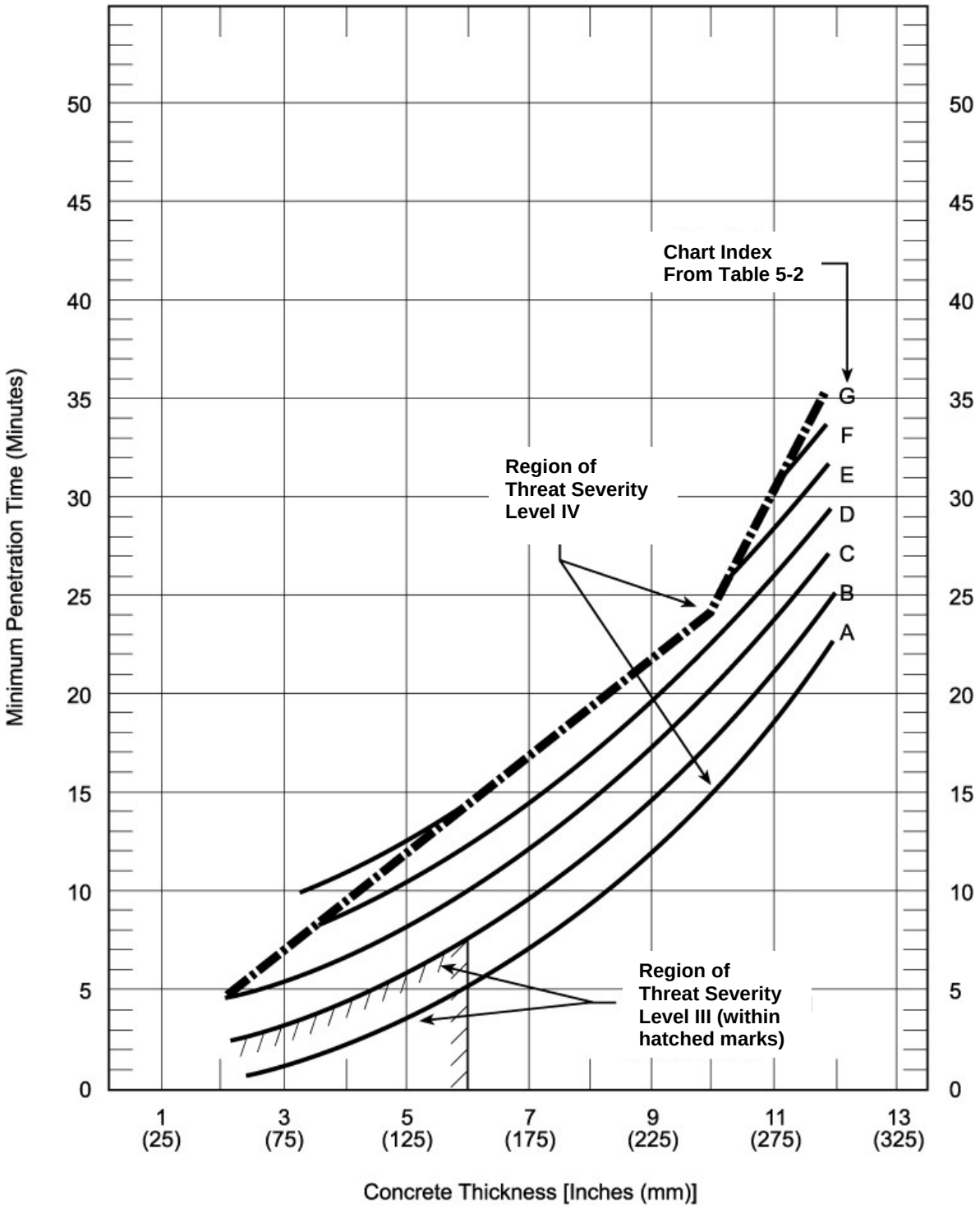
c. SFR Concrete: Figure 5-3 with Table 5-2, gives SFR concrete thickness and conventional reinforcing bar combinations that can provide penetration delay times up to 50 minutes.

Figure 5-1 Delay times for Solid Core Filled and Reinforced CMU Walls



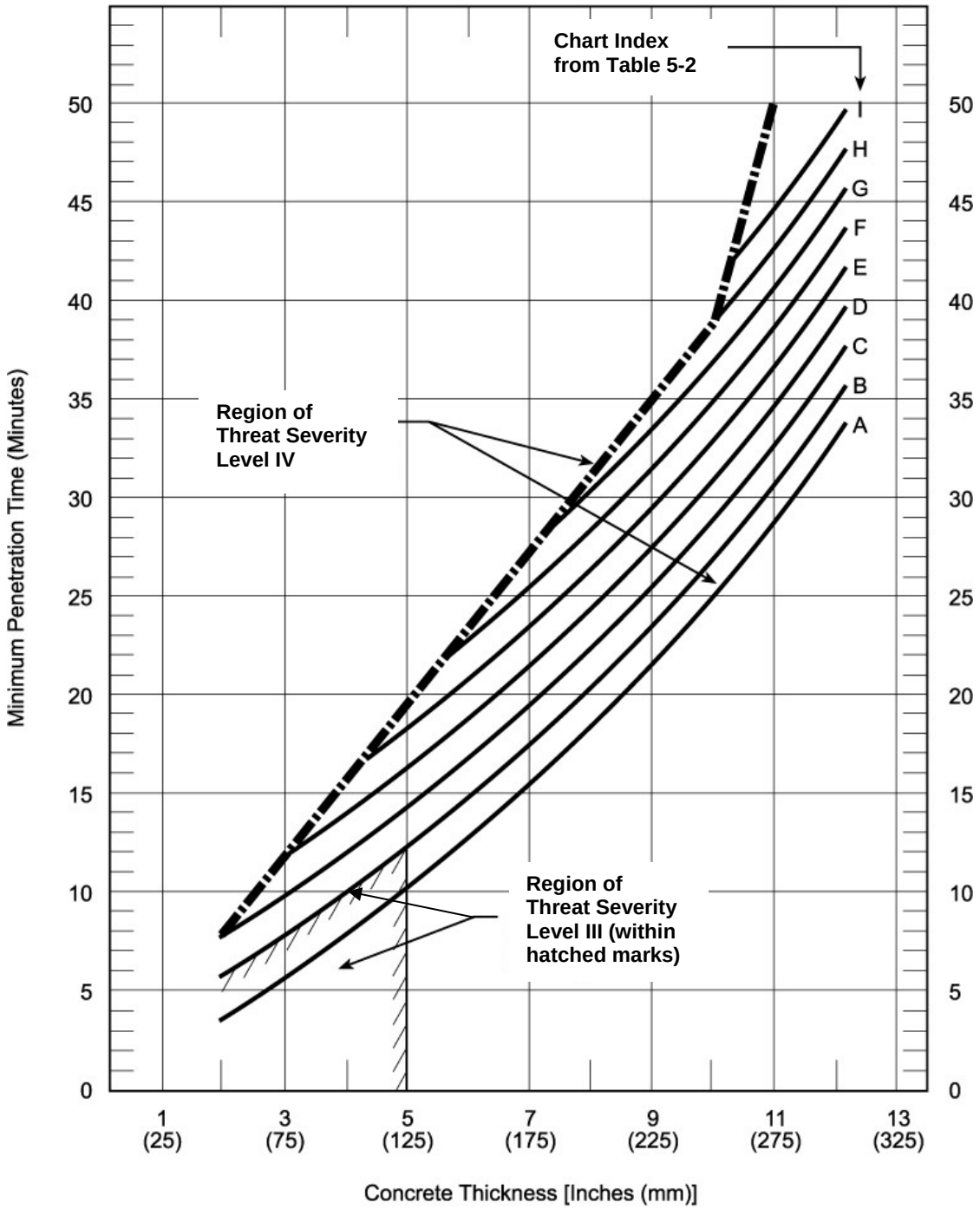
Note: the penetration times are minimum values based on the proper selection and optimal use of the attack tools. In this figure, the regions identified as threat severity level III assumes that only hand powered tools and some limited battery powered tools are used. For these cases, the thickness and/or reinforcing bar combination required is less than for the threat severity level IV where power and thermal tools also may be used.

Figure 5-2 Delay times for Conventional Reinforced Concrete Walls



Note: the penetration times are minimum values based on the proper selection and optimal use of the attack tools. In this figure, the regions identified as threat severity level III assumes that only hand powered tools and some limited battery powered tools are used. For these cases, the thickness and/or reinforcing bar combination required is less than for the threat severity level IV where power and thermal tools also may be used.

Figure 5-3 Delay times for SFR Concrete Walls



Note: the penetration times are minimum values based on the proper selection and optimal use of the attack tools. In this figure, the regions identified as threat severity level III assumes that only hand powered tools and some limited battery powered tools are used. For these cases, the thickness and/or reinforcing bar combination required is less than for the threat severity level IV where power and thermal tools also may be used.

Table 5-1 Reinforcing Bar Index for Concrete Masonry Walls

USING A SINGLE LAYER OF REINFORCING BARS							
HORIZONTAL SPACING IN INCHES (MM)	REINFORCING BAR SIZE						
	NONE	#3	#4	#5	#6	#7	#8
3 (75)	A	B	B	C	C	D	E
3-1/2 (90)	A	B	B	C	C	D	E
4 (100)	A	B	B	B	C	C	D
4-1/2 (115)	A	B	B	B	C	C	D
5 to 9 (125 to 225)	A	B	B	B	B	B	C
>10 (250)	A	A	A	A	A	A	A
USING A DOUBLE LAYER OF REINFORCING BARS							
HORIZONTAL SPACING IN INCHES (MM)	REINFORCING BAR SIZE						
	NONE	#3	#4	#5	#6	#7	#8
3 (75)	A	C	C	D	E	G	H
3-1/2 (90)	A	C	C	D	E	F	H
4 (100)	A	B	C	C	D	E	G
4-1/2 (115)	A	B	C	C	D	E	F
5 to 9 (125 to 225)	A	B	B	B	C	C	D
>10 (250)	A	A	A	A	A	A	A

NOTE: Vertical spacing at 8 inches (200 mm).

Table 5-2 Reinforcing Bar Index for Concrete

USING A SINGLE LAYER OF REINFORCING BARS							
SPACING ON CENTER EAH WAY, INCHES (MM)	REINFORCING BAR SIZE						
	NONE	#3	#4	#5	#6	#7	#8
3 (75)	A	B	B	C	C	D	E
3-1/2 (90)	A	B	B	C	C	D	E
4 (100)	A	B	B	B	C	C	D
4-1/2 (115)	A	B	B	B	C	C	D
5 to 9 (125 to 225)	A	B	B	B	B	B	C
>10 (250)	A	A	A	A	A	A	A
USING A DOUBLE LAYER OF REINFORCING BARS							
SPACING ON CENTER EACH WAY, INCHES (MM)	REINFORCING BAR SIZE						
	NONE	#3	#4	#5	#6	#7	#8
3 (75)	A	C	C	D	E	G	I
3-1/2 (90)	A	C	C	D	E	F	H
4 (100)	A	B	C	C	D	E	G
4-1/2 (115)	A	B	C	C	D	E	F
5 to 9 (125 to 225)	A	B	B	B	C	C	D
>10 (250)	A	A	A	A	A	A	A

5-5.1.3 Walls to Resist Severity Level V.

The only two ways to harden a structure against these types of threats are to construct massive reinforced concrete or sacrificial barrier walls.

The use of bulk explosives or LSCs designed to direct energy, can be especially effective in breaching barriers and producing holes large enough for an aggressor to crawl through. While bulk explosives can produce large holes, even in thick concrete walls, they will not cut internal reinforcing material. The shock waves produced by an explosion propagate throughout the concrete, resulting in internal fragmentation and spalling (breaking off) of the inner and outer surfaces. The pressure of the explosive will force concrete fragments out of a wall creating a relatively clean hole. Cutting and removing the reinforcing material to create a crawl hole creates most of the delay.

a. Thick, heavily reinforced concrete walls can provide significant penetration resistance. Use reinforced concrete 18 to 48 inches (0.46 to 1.2 m) thick. Table 5-3 presents the estimated minimum penetration delay times provided by varied thicknesses of reinforced concrete that has a compressive strength of at least 5,000 psi (35,500 kPa).

   Table 5-4 provides options that can be considered based on structural and cost considerations.

Table 5-3 Reinforced Concrete Designs for Threat Severity Level V

CONCRETE THICKNESS, INCH (M)	REINFORCING BAR LAYERS – NO. 6 (19 MM) ON 6-INCH (150-MM) CENTERS	MINIMUM PENETRATION DELAY TIME (MINUTES)[a]
≤8 (≤0.2)	1	≤1
12 (0.3)	2	2
18 (0.46)	3	3
24 (0.6)	4	4.5
36 (0.9)	6	8
48 (1.2)	8	13

[a] Use of bulk explosives to remove the concrete and using power and thermal tools to cut the reinforcing bars.

b. Sacrificial barriers can be employed above, below, and around the critical area in the building. The walls, doors, and other features of this sacrificial area may be damaged but will provide cumulative delay created by the necessity to breach multiple barriers, transport breaching tools through each barrier, and retreat to a safe distance before the next barrier is breached. In general, the critical area should be internal to the building, and away from exterior walls and roofs.

Table 5-4 Wall Materials

ITEM NUMBER	WALL MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
1	4” CONCRETE 6000 POUNDS PER SQUARE INCH (PSI) WITH #5 REINFORCING BARS AT 5” ON CENTER (OC) EACH WAY (EW)		9	5	3*
2	4” CONCRETE WITH #5 REINFORCING BARS AT 5” OC EW	6	6		1*
3	6” CONCRETE WITH #4 REINFORCING BARS AT 8” OC EW	9		2	2*
4	8” CONCRETE WITH #4 REINFORCING BARS AT 9” OC EW EACH FACE (EF)			15	14
5	8” CONCRETE WITH #5 REINFORCING BARS AT 6” OC EW			11	9/2*
6	8” CONCRETE WITH #6 REINFORCING BARS AT 6” OC EW				2*
7	8” CONCRETE 6000 PSI WITH #5 REINFORCING BARS AT 5” OC EW			6	5
8	8" CONCRETE WITH #6 REINFORCING BARS AT 12" OC EW			11	10
9	12" CONCRETE WITH #6 REINFORCING BARS AT 6" OC EF				3*
10	12" CONCRETE WITH #5 REINFORCING BARS AT 6" OC EF			31	3*
11	12" CONCRETE WITH #6 REINFORCING BARS AT 12" OC EF				2*
12	18" CONCRETE, 5000 PSI WITH 5/16" EXPANDED METAL 3" OC				2*
13	4" FIBROUS CONCRETE, 6500 PSI WITH #5 REINFORCING BARS AT 5" OC EW		13		10
14	8" FIBROUS CONCRETE WITH #5 REINFORCING BARS AT 5" OC EW		9	5	<1
15	8" FIBROUS CONCRETE, 6500 PSI WITH #5 REINFORCING BARS AT 6" OC EW				3*

ITEM NUMBER	WALL MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
16	12" FIBROUS CONCRETE, 6500 PSI WITH #5 REINFORCING BARS AT 6" OC EF			7	6
17	4" REINFORCED CMU	2			
18	4" CMU WITH #8 REINFORCING BARS AT 8" OC MORTAR FILLED	2			
19	8" CMU	2			
20	8" CMU WITH #4 REINFORCING BARS EVERY COURSE MORTAR FILLED		8	5	4
21	8" CMU WITH #8 REINFORCING BARS MORTAR FILLED		7	3	
22	12" CMU	2			
23	12" CMU WITH #5 REINFORCING BARS AT 8" OC MORTAR FILLED				1*
24	12" CMU WITH #6 REINFORCING BARS AT 8" OC MORTAR FILLED	21			1*
25	8" CMU WITH #8 REINFORCING BARS AT 8" OC MORTAR FILLED, 4" FIBROUS CONCRETE, 6500 PSI				3*
26	8" CMU MORTAR FILLED, 3" FIBROUS CONCRETE	27		24	
27	8" CMU, WIRE FABRIC, 4" FERROCEMENT	8	8		
28	8" CMU, DIAMOND MESH PLASTER LATH, 2 LAYERS, 1" POLYURETHANE FOAM	3			
29	8" CMU, 3/4" PLYWOOD, #15 ROOFING MATERIAL, 3/4" PLYWOOD		9		
30	8" CMU, 1-1/2" PLYWOOD		9		
31	8" CMU, 3/4" PLYWOOD, 1" POLYURETHANE FOAM, #9 EXPANDED METAL 3/4"			3	
32	4" SOLID BRICK	1			
33	8" BRICK INTERLOCKED	3			

ITEM NUMBER	WALL MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
34	10 GAUGE (GA) HARDENED STEEL, 3/4" PLYWOOD, 10 GA HARDENED STEEL	7			
35	WOOD OR METAL STUDS WITH GYPSUM WALLBOARD (GWB) BOTH SIDES	<1			
36	WOOD STUDS WITH GWB ON INSIDE, STUCCO ON OUTSIDE WOOD STUDS WITH WOOD SIDING	1			
37	WOOD STUDS WITH GWB ON INSIDE, WOOD SIDING ON OUTSIDE	1			
38	2 LAYERS 3/8" GWB, 2” by 4” STUDS @ 16" OC, 1116 STEEL STUDS @ 16" OC, 1/8" MILD STEEL		7		
39	10 GA HARDENED STEEL, 3/4" PLYWOOD,10 GA HARDENED STEEL, 3/4" PLYWOOD, 10 GA HARDENED STEEL	12			
40	1/4" STEEL PLATE, 20 GA ROOF DECK 3", SILICATE FOAM 3", 1" PLYWOOD SHEATHING		12		<1*
41	2 LAYERS 3/8" GWB, 2” by 4” STUDS @ 16" OC, #l7 STEEL STUDS @ 16" OC, 1/4" MILD STEEL		13		1
42	9 GA HARDENED STEEL, 3/4" PLYWOOD, 9 GA HARDENED STEEL	14			5
43	10 GA HARDENED STEEL, #90 ROOF MATERIAL, 3/4" PLYWOOD, 10 GA HARDENED STEEL	20			
44	1/2" STUCCO, CHICKEN WIRE, TAR PAPER, 2” by 4” STUDS @ 16" OC, 1/2" Gypsum Wall Board (GWB)	1			
45	2” by 4” STUDS CONTINUOUS WITH 2” WOOD SIDING (TOTAL 6” THICKNESS NOMINAL)		5		
46	1-1/2" BEVELED CEDAR SIDING, FELT, l by 6 SHEATHING, 2” by 4” STUDS 16" OC, 3/8" GWB, 11 GA WOVEN WIRE 2” by 4” (6 LAYERS), FERROCEMENT 4"	5			
47	1-1/2" BEVELED CEDAR SIDING, FELT, l by 6 SHEATHING, 2” by 4” STUDS 16" OC, 3/8" GWB, 3/4" PLYWOOD, 1/6" SHEET METAL		10		
48	1-1/2" BEVELED CEDAR SIDING, FELT, lx6 SHEATHING, 2” by 4” STUDS 16" OC, 3/8" GWB, 3/4" PLYWOOD, #9 EXPANDED METAL 3/4”, 3/4" PLYWOOD			5	

ITEM NUMBER	WALL MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
49	4-INCH, SOLID-CORE, FILLED AND REINFORCED MASONRY CONSTRUCTION WITH INTERIOR WALL SYSTEM	1	1	1	
50	8-INCH, SOLID-CORE, FILLED CONCRETE MASONRY WITH #3 BARS AT 8 INCHES OC EW	5			1
51	8-INCH, SOLID-CORE, FILLED CONCRETE MASONRY WITH #5 BARS AT 8 INCHES OC EW		5		
52	8-INCH, MORTAR-FILLED CONCRETE BLOCK WITH #6 BARS AT 8 INCHES OC EW	15			
53	8-INCH, REINFORCED CONCRETE WITH # 4 BARS AT 6 INCHES OC EW		15		
54	12-INCH, MORTAR-FILLED, CONCRETE BLOCK WITH #6 BARS AT 8 INCHES OC EW	30			
55	8-INCH, SOLID-CORE, FILLED CONCRETE MASONRY WITH #6 BARS AT 4 INCHES OC VERTICALLY AND 8 INCHES OC HORIZONTALLY			5	
56	12-INCH, REINFORCED CONCRETE WITH # 5 BARS AT 6 INCHES OC EW			15	
57	12-INCH, REINFORCED CONCRETE WITH 2 LAYERS OF # 7 BARS AT 4 INCHES OC EW		30		
58	12-INCH, REINFORCED CONCRETE WITH 5/16 EXPANDED METAL 2½ INCHES OC (4 LAYERS)				5
59	12-INCH, REINFORCED CONCRETE WITH 5/16-INCH, EXPANDED, METAL MESH AT 2½ INCHES OC AND A ¼-INCH BACKING PLATE			30	15
60	18-INCH-THICK REINFORCED CONCRETE WITH 5/16-INCH EXPANDED METAL AT 2- 1/2 INCHES OC AND A 1/4-INCH BACKING PLATE				30

NOTES: For the use of the above table, refer to Paragraph 5-4.
Where not specified in the table, use 3000 psi concrete.

5-5.2 Roofs.

Conventional roof construction offers little resistance to downward forced entry attack, except where reinforced concrete slabs form the structure.

5-5.2.1 Roofs to Resist Threat Severity Level II.

Solid plywood roof construction provides a delay of less than one minute against threat severity level II. Since greater delay is required, use one of the roof types shown in Table 5-5.

5-5.2.2 Roofs to Resist Threat Severity Levels III and IV.

Protection against threat severity levels III and IV requires the use of conventional or fiber reinforced concrete. Use one of the concrete thickness options in Figure 5-2 and Figure 5-3 combined with the reinforcing bar options in Table 5-2 for roof designs; however, for a downward attack on a roof, penetration delay times are lower for a similar attack on a wall; therefore, to achieve the same delay rating, use an additional thickness of 1-inch (25-mm) concrete, or the same concrete thickness and increase the reinforcement by 2 bar sizes.

Table 5-5 contains several additional design options that provide delays from 2 to 30 minutes.

5-5.2.3 Roofs to Resist Threat Severity Level V.

Threat severity level V requires sacrificial areas, multiple barriers, or massive reinforced concrete. For the reinforced concrete design, use one of the options in Table 5-5 with entries for the threat severity level V.

Sacrificial barriers can be employed above the protected area in the building. The features of these sacrificial areas may be damaged but will provide cumulative delay created by the necessity to breach multiple barriers, transport breaching tools through each barrier, and retreat to a safe distance before the next barrier is breached. Any type of construction for the sacrificial barrier is acceptable if the barrier provides an equivalent level of penetration resistance to lower threat severity levels.

Table 5-5 Roof Materials

ITEM NUMBER	ROOF MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
1	GRAVEL ON ASPHALT, 2" INSULATION ON 2-1/2" CONCRETE	3			
2	5-1/2" CONCRETE, #4 REIFORCING BARS 8" by 12" OC			13	
3	GRAVEL ON ASPHALT, 2" INSULATION ON 2" CONCRETE ON 6' by 24" PRECAST SINGLE T-BEAM	4	4		
4	GRAVEL ON ASPHALT, 3" CONCRETE, 2" INSULATION ON 6' by 24" PRECAST SINGLE T-BEAM WITH 2"-4" TAPER	4	4	3	
5	20 GA SHEET METAL ON 3/4" FIBERGLASS INSULATION	2	2		
6	24 GA SHEET METAL, 1-1/2" FIBERGLASS INSULATION ON 1/8" STEEL MESH 8" BELOW SHEET METAL			2	
7	24 GA SHEET METAL, 1-1/2" FIBERGLASS INSULATION ON 1/8" STEEL WIRE BELOW SHEET METAL	2	2		
8	GRAVEL ON ASPHALT, 2" INSULATION ON 16 GA SHEET METAL	3			
9	GRAVEL ON ASPHALT, 2" INSULATION ON 22 GA SHEET METAL, WITH 12" STEEL MESH BELOW' SHEET METAL			6	
10	GRAVEL ON ASPHALT, 2" INSULATION ON 22 GA SHEET METAL		7	3	
11	GRAVEL ON ASPHALT, 2" INSULATION ON 4" 3500 PSI CONCRETE WITH #4 REINFORCING BARS @ 6" OC EW, 22 GA SHEET METAL		29		
12	GRAVEL ON ASPHALT, 2" INSULATION ON 4" 3500 PSI CONCRETE WITH #4 REINFORCING BARS 6" OC ONE WAY, EXPANDED METAL ON 22 GA SHEET METAL		26		
13	GRAVEL ON ASPHALT, 2" INSULATION ON 2-1/2" CONCRETE WITH 10 GA 6" by 6" WOVEN WIRE FABRIC ON 22 GA SHEET METAL		15		
14	GRAVEL ON ASPHALT, 2" INSULATION ON 2-1/2" CONCRETE WITH 10 GA 6" by 6" WOVEN WIRE FABRIC ON 22 GA SHEET METAL DECK WITH SCREEN MESH 8" BELOW SHEET METAL		10		
15	GRAVEL ON ASPHALT, 2" INSULATION ON 2-1/2" CONCRETE WITH 10 GA 6" by 6" WOVEN WIRE FABRIC ON 22 GA SHEET METAL DECK YITH SCREEN MESH 12" BELOW SHEET METAL	5	5		

ITEM NUMBER	ROOF MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
16	GRAVEL ON ASPHALT, 2" INSULATION ON 2" CONCRETE OVER #4 6" EXPANDED METAL ON 6” by 24" PRECAST SINGLE T-BEAM	5			
17	GRAVEL ON ASPHALT, 2" INSULATION ON 2" CONCRETE ON 16 GA SHEET METAL	4	4	4	
18	BUILT-UP ROOF WITH GRAVEL AND RIGID INSULATION ON STEEL DECKING	5	1	1	
19	BUILT-UP ROOF WITH GRAVEL AND RIGID INSULATION AND 4-INCH LIGHTWEIGHT CONCRETE WITH #5 BARS AT 8 INCHES OC EW ON STEEL DECKING				1*
20	4-INCH, REINFORCED CONCRETE WITH 6 BY 6 WELDED WIRE MESH, 10-GAGE REINFORCING ON STEEL DECKING AND A BUILT-UP ROOFING SYSTEM		5		
21	6-INCH, REINFORCED CONCRETE WITH #4 BARS AT 8 INCHES ON CENTER EACH WAY ON STEEL DECKING AND WITH BUILT-UP ROOFING	15			
22	6-INCH, REINFORCED CONCRETE WITH # 4 BARS AT 6 INCHES ON CENTER EACH WAY ON STEEL DECKING AND WITH A BUILT-UP ROOFING SYSTEM		15		
23	8-INCH, REINFORCED CONCRETE WITH #4 BARS AT 8 INCHES ON CENTER EACH WAY ON STEEL DECKING AND WITH BUILT-UP ROOFING	30			
24	6-INCH, REINFORCED CONCRETE WITH 6 BY 6 WELDED WIRE MESH, 10-GAGE REINFORCING ON STEEL DECKING AND A BUILT-UP ROOFING SYSTEM			5	
25	10-INCH, REINFORCED CONCRETE WITH # 5 BARS AT 6 INCHES ON CENTER EACH WAY ON STEEL DECKING AND WITH A BUILT-UP ROOF			15	
26	10-INCH, REINFORCED CONCRETE WITH 2 LAYERS OF #5 BARS AT 6 INCHES ON CENTER EACH WAY ON STEEL DECKING AND WITH A BUILT-UP ROOFING SYSTEM		30	30	5*
27	10-INCH, REINFORCED CONCRETE WITH 5/16 EXPANDED METAL 2½ INCHES ON CENTER ON STEEL DECKING WITH A BUILT-UP ROOFING SYSTEM				15*

ITEM NUMBER	ROOF MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
28	12-INCH-THICK, REINFORCED CONCRETE WITH 5/16-INCH EXPANDED METAL AT 2½ INCHES ON CENTER, ¼-INCH STEEL DECKING, AND BUILT-UP ROOFING				30*

NOTES: For the use of the above table, refer to Paragraph 5-4.
Where not specified in the table, use 3000 psi concrete.

5-5.2.4 Roof-Mounted Equipment.

Roof-mounted equipment, such as air-supply fans, exhaust fans, gravity ventilators, and filter banks, are usually welded or bolted to an equipment curb, duct system, or foundation and can be removed with simple hand tools. Openings uncovered when equipment is removed can provide entry to the interior of the building. In many installations, the removal of a small number of bolts, plus the removal of the equipment, can provide access. For protection of an exposed opening consider on the following alternatives:

- When possible, limit the exposed opening to less than 96 square inches (619 cm^2) with no dimension greater than 6 inches (150 mm).
- Provide grilles constructed of metal bars to provide delay. See Table 5-21 for the size and spacing of bars for the defense layer penetration delay time.
- Provide a hardened equipment cover to house the machinery. Equipment cover penetration delay time will depend on structural components, doors, and other openings. Specific penetration delay times can be estimated by the same methods described for structures throughout this manual. The use of the equipment cover option must be weighed against the probability, likelihood, and logistics involved with removal of the roof-mounted equipment.

5-5.2.5 Structural Openings.

Structural openings, such as skylights, roof hatches, scuttles, elevator shafts, ash dumps, rubbish chutes, fire escapes, and roof access ladders, offer access to aggressors and should be considered in hardening plans. The approach to upgrading miscellaneous openings is dictated by the structural elements involved (design of walls, roofs, doors, and locking mechanisms).

5-5.2.6 Other Openings.

Secure all hatches, penthouses, and exterior ladders.

5-5.2.7 Roof Styles and Railings.

Use steeply pitched roof structures where possible to make movement difficult and to minimize concealment opportunities provided by flat roofs.

For flat roofs, use railings instead of solid parapets to minimize concealment opportunities.

5-5.3 Ceilings and Floors.

Floor and ceiling assemblies are the horizontal (top and bottom) components of the 6-sided intermediate defense layers. Floors may be exposed to exterior forced entry if the asset is in the space above the floor and the aggressors gain access to the space below; and, ceilings may be exposed to forced entry if the asset is in the space below the ceiling and the aggressors gain access to the space above. Select floor and ceiling construction which provides the required delay time where applicable.

5-5.3.1 Ceilings and Floors to Resist Threat Severity Level II.

Conventional construction of 3/4 inch (19 mm) plywood on wood joists for ceilings and floors can be used to provide the required one minute of penetration delay.

5-5.3.2 Ceilings and Floors to Resist Threat Severity Levels III and IV.

Threat severity levels III and IV necessitate the use of conventional or fiber reinforced concrete. Use one of the concrete thickness options in Figure 5-2 and Figure 5-3 combined with the reinforcing bar options in Table 5-2 for ceiling and floor designs. Table 5-6 contains several additional design options that provide delays from 2 to 30 minutes.

In general, for reinforced concrete walls less than 12 inches (30 cm) thick, the following rules of thumb for companion ceilings will apply. Penetration delay times for an upward attack on a ceiling (floor of upper level) will be higher than the same attack on a wall; therefore, use the next lowest thickness of 1-inch (25-mm) concrete or use the same concrete thickness and decrease the reinforcement by 2 bar sizes. For a downward attack on a roof, penetration delay times are lower for a similar attack on a wall; therefore, to achieve the same delay rating, use an additional thickness of 1-inch (25-mm) concrete, or the same concrete thickness and increase the reinforcement by 2 bar sizes.

5-5.3.3 Ceilings and Floors to Resist Threat Severity Level V.

Thick, heavily reinforced concrete ceilings and floors can provide significant penetration resistance. Use reinforced concrete 18 to 48 inches (0.46 to 1.2 m) thick. Table 5-3 presents the estimated minimum penetration delay times provided by varied thicknesses of reinforced concrete that has a compressive strength of at least 5,000 psi (507,000 kPa). Table 5-6 provides options that can be considered based on structural and cost considerations.

Table 5-6 Floor or Ceiling Materials

ITEM NUMBER	FLOOR OR CEILING MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
1	PLYWOOD ON WOOD JOISTS	1	1	1	1
2	PLYWOOD ON WOOD JOISTS W/INSULATION	1		1	<1*
3	4-1/2" REINFORCED CONCRETE (#4 BARS @ 18" EW) AND 16 GA SHEET METAL	6			2*
4	5-1/2” REINFORCED CONCRETE (10 GA STEEL MESH)	6			
5	8" REINFORCED CONCRETE (#4 BARS @ 9" EW)			12	11/<2*
6	12" REINFORCED CONCRETE (#5 BARS @ 6" EW, EF)			23	22/<3*
7	3" CONCRETE, #10 6" STEEL MESH, 2-1/2" CONCRETE PLANK	6		2	
8	CARPET, 1-1/2" PLYWOOD, 3" SILICATE INSULATION		5	1	<1*

NOTES: For the use of the above table, refer to Paragraph 5-4.
Where not specified in the table, use 3000 psi concrete.

5-5.3.4 Slabs on Grade.

Use minimum 6-inch thick reinforced concrete with #4 bars (1/2-inch, 13 mm) reinforcing bars spaced at 6 inches OC, EW.

5-5.4 Personnel Entrances.

The number of entrances to a defense layer should be limited to one personnel entrance and the minimum number of emergency exit doors required for life safety per National Fire Protection Association (NFPA) 101.

5-5.4.1 Specifying Door Assemblies.

When specifying door assemblies, ensure that the threat severity level and required penetration delay time is included. Refer to UFGS-08 34 63 for design and installation requirements.

5-5.4.2 Personnel Entrances to Resist Threat Severity Level II.

Use doors and frames that are built and installed according to National Association of Architectural Metal Manufacturers/ Hollow Metal Manufacturers Association (NAAMM/HMMA) Hollow Metal Manual standards. Doors and frames meeting these requirements will provide at least a 1-minute penetration delay time against a threat severity level II. If more delay time is needed, use multiple doors placed in series.

Personnel door and frame details for severity threat level II are shown in Table 5-7 and Table 5-8. The frame is designed for installation in a wood-stud frame wall. Hinge-side protection should be provided as shown in Figure 5-4.

Table 5-7 Personnel Door Panel/Edge Details, Threat Severity Level II

COMPONENT	REQUIREMENT
Size	3 feet by 80 inches by 1-3/4 inches (0.9 m by 2 m by 44 mm).
Applicable Specifications	NAAMM/HMMA, Hollow Metal Manual – 1995., UFGS-08 34 01.
Type	Type A, full-flush with continuous welded-edge seams. Design F, full-panel flush door.
Panel	Steel-stiffened.
Face Sheet	16-gauge (1.6 mm) steel.
Stiffeners	Hat section, 16-gauge (1.6 mm) steel; maximum distance between stiffeners 4 inches (100 mm) OC.
Edge Construction	14-gauge (1.9 mm) steel channel, recessed.

Table 5-8 Personnel Doorframe Details, Threat Severity Level II

COMPONENT	REQUIREMENT
Applicable Specifications	Construct per NAAMM/HMMA, Hollow Metal Manual – 1995 except as noted, UFGS-08 34 01.
Frame Design	Single door, butt-type, double-rabbet type; 14-gauge (1.9 mm) steel, fully welded.
Jamb Depth	4 inches (100 mm).
Special Features	(See Figure 5-4 for hinge side protection.)
Frame Installation	Install per NAAMM/HMMA, Hollow Metal Manual – 1995. Install frame into a wood-stud frame wall.
Hardware Preparation	Prepare hardware per NAAMM/HMMA, Hollow Metal Manual – 1995.

Table 5-9 Door Hardware for Threat Severity Levels II and III

COMPONENT	REQUIREMENT
Mortise Lock	American National Standards Institute/Building Hardware Manufacturers Association (ANSI/BHMA) A156.13 Series 1000 Security Grade, with dead bolt and latch bolt.
Auxiliary Rim Lock	ANSI/BHMA A156.5, Security Grade drop bolt lock operated by key from inside and outside. Lock selected must conform to mounting bolt tensile test [12,000 pounds (5,450 kg)]. This lock should be used in conjunction with anti-wedge and anti-drill plates. To comply with life safety requirements, this lock should only be used during those hours when the space is unoccupied.
Hinges	ANSI/BHMA A156.1. Heavy Weight. Note: security door systems for threat severity level III require some form of hinge side protection. Some hinge manufacturers provide this type of protection in the form of shear plugs incorporated into the hinge or hinge pins that are not removable. If these types of hinges are not used, then some form of hinge side protection should be engineered into the door system. For added protection against door sag, surface-mounted continuous hinges can be used.
Panic Hardware	American Society for Testing and Materials (ASTM) F571, Grade 1, Mortise exit device. Use panic type exit devices as required by life safety codes in lieu of this mortise lock; however, to ensure resistance to threat severity level III, use in conjunction with an auxiliary rim lock.
Other Hardware	If the use of additional hardware such as closing devices and electric strikes, among others, is required, ensure that the hardware selected meets ANSI/BHMA requirements, and does not interfere with the security devices on the door systems. Consult with the DoD Lock Program, NAVFAC Engineering and Expeditionary Warfare Center, Toll Free: (800) 290-7607 Comm: (805) 982-1212, if there are any questions.

5-5.4.3 Personnel Entrances to Resist Threat Severity Level III.

Use doors and frames that are built and installed according to ANSI/NAAMM HMMA 863-14. Doors and frames meeting these requirements will provide at least a 4-minute penetration delay time against threat severity level III. If more delay time is needed, use multiple doors placed in series.

Personnel door and frame details for threat severity level III are shown in Table 5-10 and Table 5-11. The frame is designed for installation in a reinforced CMU wall. Hinge-side protection should be provided as shown in Figure 5-4.

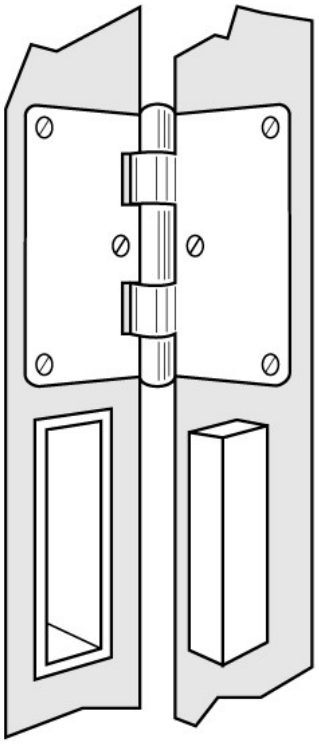
Table 5-10 Door Panel/Edge Details for Threat Severity Level III

COMPONENT	REQUIREMENT
Size	3 feet by 80 inches by 1-3/4 inches (0.9 m by 2 m by 44 mm).
Applicable Specifications	ANSI/NAAMM HMMA 863-14.
Type	Type A, full flush with continuous welded-edge seams. Design F, full-panel flush door.
Panel	Steel-stiffened.
Face Sheet	14-gauge (1.9 mm) steel.
Stiffeners	Hat section, 14-gauge (1.9 mm) steel; maximum distance between stiffeners 4 inches (100 mm) OC.
Edge Construction	12-gauge (2.7 mm) recessed steel channel.
Special Features	(See Figure 5-4 for the hinge side protection configuration and Figure 5-5 for the 7-gauge (4.5 mm) anti-pry strips).

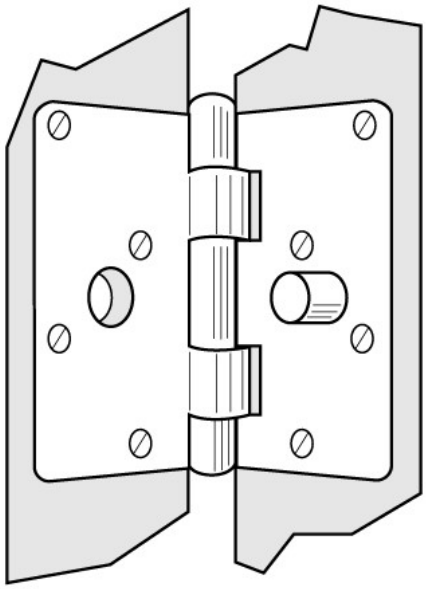
Table 5-11 Doorframe Details for Threat Severity Level III

COMPONENT	REQUIREMENT
Frame Thickness	12 gauge (2.7 mm)
Applicable Specifications	Construct per HMMA 863-14 except as noted.
Frame Design	Single door, butt-type, double-rabbet type; 10-gauge (3.4 mm) steel, fully welded.
Jamb Depth	8 inches (200 mm)
Special Features	(See Figure 5-4 for details on hinge-side protection.)
Frame Installation	Install per HMMA 863-14 and NAAMM HMMA, Hollow Metal Manual
Hardware Preparation	Prepare for hardware per HMMA 863-14. Use one of the two cases below for selecting installation hardware: Frame to be installed in a CMU wall with the frame installed and the wall built to the frame. Provide adjustable 2- by 10-inch (50- by 254-mm) corrugated 12-gauge (2.7 mm) frame side. Ensure that the reinforcing bars of the CMU wall tie into the interior of the frame. Fill frame with a grout of compressive strength not less than 3,000 psi (21,000 kPa). Frame is to be installed in a prepared opening in a CMU wall. Frame must be punched and countersunk for expansion bolt anchors (four per side) and provided with 12-gauge (2.7 mm) hat shaped reinforcements secured in place with at least four spot welds each. Fill frame with a pour type grout with a compressive strength of not less than 3,000 psi (21,000 kPa).

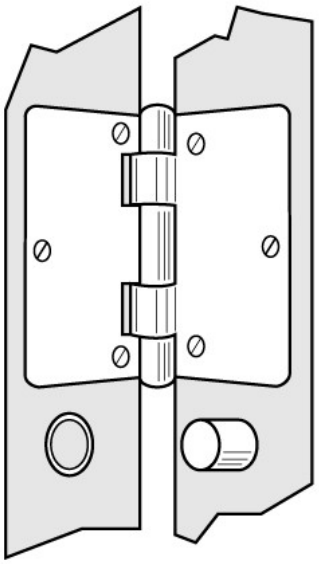
Figure 5-4 Door Hinge-Side Protection Threat Severity Levels II and III



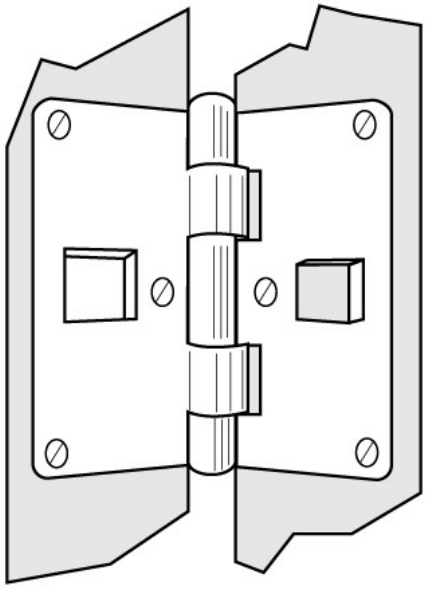
A) Metal lug and receptacle system.



B) Addition of a metal dowel-pin and socket to the existing hing.



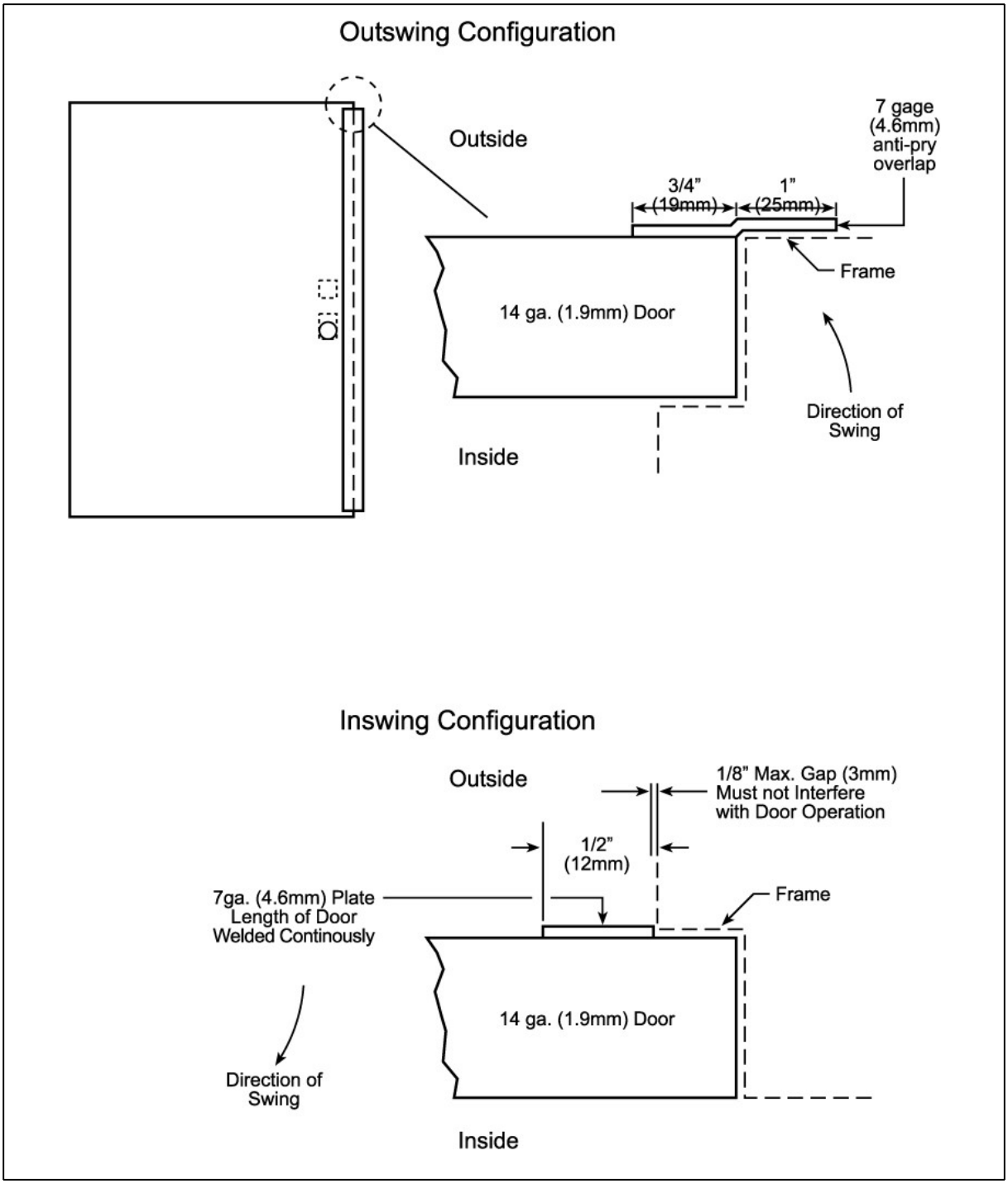
C) Installation of a metal dowel-pin in the door and reinforcing metal cup in the door frame.



D) Hinge with lug and matching socket formed into hinge at factory.

Note: Lugs, dowel-pins, etc. should be 1-inch-diameter (25.4mm) minimum.

Figure 5-5 Door Anti-Pry Strips for Threat Severity Level III



5-5.4.4 Personnel Entrances to Resist Threat Severity Levels IV and V.

There are no personnel doors rated to resist threat severity levels IV and V. Use multiple threat severity level III personnel doors mounted in series or use a vault door. Consider using a day gate during daytime operations.

5-5.5 Doors (Non-Entry).

The number of doors needed to secure a defense layer should be minimized. In cases where more than one door exists, only one (personnel entrance) should be provided with exterior mounted locks. All other non-entry doors to the defense layer must present blank, flush surfaces to the outside and have internal locking or bolting mechanisms to reduce the vulnerability to attack.

5-5.5.1 Door Panel Construction (Non-Entry).

Table 5-12 shows options for door panel construction to resist all threat severity levels. Although the penetration delay time through the door surface can usually be increased by use of thicker or composite materials, such hardening may be constrained by weight, functional requirements (disability access requirements or safety), mounting hardware, or locking system vulnerability. There is no value in hardening a door surface beyond the attack resistance of the available mounting hardware and locking system technology.

Table 5-12 Door Materials

ITEM NUMBER	DOOR MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
1	2 LAYERS 10 GA HOT-ROLLED STEEL, 1 LAYER 3/4" EXTERIOR PLYWOOD	6			
2	3 LAYERS 10 GA HOT-ROLLED STEEL, 2 LAYERS 3/4" EXTERIOR PLYWOOD	12			
3	2 LAYERS 9 GA ASTM A1008 HARDENED STEEL, 1 LAYER 3/4" EXTERIOR PLYWOOD	14			
4	2-LAYERS 9 GA ASTM A1008 HARDENED STEEL, 1 LAYER 3/4" EXTERIOR PLYWOOD, 2 LAYERS OF 90- LB GRAVEL FINISH ROOF PAPER	20			
5	9 LAYERS 3/4" PLYWOOD, 8 LAYERS 10 GA 27 STEEL PLATE	27			

ITEM NUMBER	DOOR MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
6	3 LAYERS 10 GA ASTM A1008 HARDENED STEEL, 2 LAYERS 1/2" ACRYLIC (TOTAL THICKNESS 1-1/4")	20			
7	3 LAYERS 10 GA ASTM A1008 STEEL, 2 LAYERS 1/2" POLYCARBONATE GLAZING	20			
8	2 LAYERS 1/4" HARDENED STEEL, 2 LAYERS URETHANE FOAM 3", 1/4" PERFORATED STEEL PLATE, 1-1/2" OAK				16/ <1*
9	1/4" TYPE 304 STAINLESS STEEL PLATE, 1/2" POLYCARBONATE, 10 GA ASTM A1008 STEEL SHEET (TOTAL THICKNESS 0.88")	11			
10	1/2" HARDENED STEEL, 1-1/4" OAK, l/2" PLWOOD, 1/4" HARDENED STEEL (2 LAYERS)				12/ <1*
11	3/8" STEEL, 3" REDWOOD, 0.036" STEEL	6			
12	3/8" A-36 STEEL PLATE (2 LAYERS), 4" POLYURETHANE FOAM, 3" OAK				18/ <1*
13	3/8" A-36 STEEL PLATE (2 LAYERS), 4" SILICATE FOAM, 3" OAK				23/ <1*
14	3/8" A-36 STEEL PLATE (2 LAYERS), POLYURETHANE FOAM 2.125, 1/4" PERFORATED STEEL PLATE, 2-1/2" OAK				17/ <1*
15	3/8" A-36 STEEL PLATE (2 LAYERS), 3" OAK, 4" SILICATE FOAM				19/ <1*
16	5/16" STEEL PLATE, 1" INSULATION, 22 GA SHEET METAL (2 LAYERS)				3/<1*
17	CLASS 5 VAULT DOOR	4			2
18	1/4" STEEL PLATE, PADLOCK	2	2		2/<1*
19	3/4" STEEL PLATE, 3" RIGID INSULATION, 1/8" STEEL PLATE	2			4/<1*
20	3/4" STEEL PLATE, 1/4" STEEL PLATE		10		4
21	3/4" STEEL PLATE, 3" REDWOOD IN CENTER, 1/4" STEEL PLATE		26		17
22	3/8" DRILL-RESISTANT STEEL, GSA CLASS 6 VAULT DOOR		22		
23	3/8" STEEL PLATE, 1/4" STEEL PLATE		14		4/<1*

ITEM NUMBER	DOOR MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
24	3/8" STEEL PLATE, .036" (20 GA) STEEL PLATE, 2 PADLOCKS	1		1	
25	16 GA SHEET METAL, PANIC HARDWARE, FULL SURFACE HINGE	2	2		2/<1*
26	16 GA SHEET METAL, PANIC HARDWARE, PANIC BAR PLATE, CYLINDER LOCK, BUTT HINGE, NONREMOVABLE PINS, HINGE Z STRIP, FRONT PRY STRIP	2			
27	STANDARD INDUSTRIAL VEHICLE DOOR 16 GA CORRUGATED SHEET METAL ROLL-UP	1			1*
28	STANDARD INDUSTRIAL VEHICLE DOOR, HOLLOW STEEL PANEL, 16 GA	1			<1*
29	CLASS FS FILING CABINET DRAWER			4	
30	16 GA HOLLOW STEEL	2			
31	STANDARD 16-GAGE, HOLLOW, METAL DOOR (3 FEET BY 7 FEET) WITH HINGE-SIDE PROTECTION, ANTI-PRY STRIP, AND DRILL-RESISTANT DEAD BOLT LOCK	5	1	1	1
32	12-GAGE, HOLLOW, METAL DOOR (3 FEET BY 7 FEET) WITH HINGE-SIDE PROTECTION, ANTI-PRY STRIP, AND DRILL-RESISTANT DEAD BOLT LOCK		5		
33	12-GAGE, HOLLOW, METAL DOOR WITH HINGE-SIDE PROTECTION, ANTI-PRY STRIP, DRILL-RESISTANT DEAD BOLT LOCK, AND FILLED WITH LIGHTWEIGHT FIREPROOFING			5	
34	12-GAGE, HOLLOW, METAL DOOR FILLED WITH LIGHTWEIGHT CONCRETE (3 FEET BY 7 FEET) WITH HINGE-SIDE PROTECTION, ANTI-PRY STRIP, AND DRILL-RESISTANT DEAD BOLT LOCK	15			
35	12-GAGE, HOLLOW, METAL DOOR (3 FEET BY 7 FEET) WITH HINGE-SIDE PROTECTION, ANTI-PRY STRIP, DRILL-RESISTANT DEAD BOLT LOCK, AND MULTIPOINT (3) LOCKING SYSTEM	30			
36	SWINGING DOOR (6 INCHES THICK) WITH 1/2-INCH PLATE INSIDE AND OUT, LIGHTWEIGHT CONCRETE FILL, AND AN INTERNAL LOCKING SYSTEM		30		

ITEM NUMBER	DOOR MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
37	SLIDING DOOR (6 INCHES THICK) FILLED WITH LIGHTWEIGHT CONCRETE THAT HAS BEEN REINFORCED WITH EXPANDED METAL MESH WITH A 3/4-INCH STEEL FRONT PLATE, 1/4–INCH BACK PLATE, AND AN INTERNAL LOCKING SYSTEM				5
38	SWINGING DOOR (10 INCHES THICK) WITH 1/2-INCH PLATE INSIDE AND OUT INTERNAL LOCK		15		
39	SWINGING DOOR (10 INCHES THICK) WITH 1/2-INCH PLATE INSIDE AND OUT, LIGHTWEIGHT CONCRETE FILL, AND AN INTERNAL LOCKING SYSTEM			15	
40	SWINGING DOOR (10 INCHES THICK) WITH 1/2-INCH PLATE INSIDE AND OUT, LIGHTWEIGHT CONCRETE FILL REINFORCED WITH EXPANDED METAL MESH, AND AN INTERNAL LOCKING SYSTEM			30	15
41	SWINGING DOOR (10 INCHES THICK) WITH 1/2-INCH PLATE INSIDE AND OUT, LIGHTWEIGHT CONCRETE FILL REINFORCED WITH EXPANDED METAL MESH, AND AN INTERNAL LOCKING SYSTEM WITH A WELDED C-STEEL GRATING VESTIBULE AROUND THE DOOR FOR STANDOFF PROTECTION				30

NOTE: For the use of the above table, refer to Paragraph 5-4.

5-5.6 Emergency Exit Hardware.

When the area is to be occupied and emergency exit hardware is required for fire protection requirements, use a light industrial door with an intrusion sensor and provide forced entry resistance interior to the door.

Since drilling a small hole large enough to pass a wire hook through is all that is required to trip emergency exit hardware, for unoccupied areas, auxiliary rim locks or mortise locks can be used to secure the doors.

5-5.7 Vehicle Access Doors.

Table 5-13 provides a summary of the door construction choices applicable to vehicle access doors for the threat severity levels II and III. There are no commercial vehicle access doors available that will provide penetration resistance equivalent to wall systems designed for threat severity threat level IV or V. If used for threat severity level IV or V, consider separating vehicle access areas from the protected asset. In this configuration delay time calculations may be layered beginning at the barrier system beyond the vehicle storage area and the vehicle storage area can be used as a detection buffer for the secure area.

5-5.7.1 Threat Severity Level II.

For threat severity level II, use a standard 18-gauge (1.2-mm) galvanized steel overhead coiling door with interlocking slats. Refer to UFGS-08 33 23 for installation details.

5-5.7.2 Threat Severity Level III.

For threat severity level III, use a 1-3/4-inch (44-mm) thick hollow metal door with 12-gauge (2.7-mm) skins and stiffeners on 6-inch (150-mm) vertical spacing similar to a sliding magazine door. Refer to UFC 4-420-01 for designs.

The trailing edge of the sliding magazine door must be restrained using a 4-foot (1.2-m) high, 8-inch (20-cm) diameter concrete filled steel bollard along the outside trailing edge to prevent wedging attacks that move doors away from walls.

Table 5-13 Vehicle Access Door Construction

THREAT SEVERITY LEVEL	CONSTRUCTION	PENETRATION DELAY TIME (MINUTES)
II	18-gauge (1.2-mm) galvanized steel with interlocking slats.	1
III	1-3/4-inch (44-mm) thick hollow metal door with 12-gauge (2.7-mm) skins and stiffeners on 6-inch (150-mm) vertical spacing.	4

5-5.8 Windows.

Because forced entry resistant window enhancements are costly, minimize windows where possible in defense layers that are counted on for penetration delay. Security glazing systems are commercially available that will meet the requirements for threat severity levels II, III, and IV (up to 5 minutes of delay). There are no cost-effective glazing cross sections available for threat severity levels V. For commercially available windows use the anchoring method prescribed by the window certification.

Consider the placement of windows in relation to doors. Even a small window in or next to a door could allow an aggressor to reach through and unlock the door. Use obscured glazing materials, blinds, shutters, or drapes to eliminate asset visibility.

5-5.8.1 Specifying Window Assemblies.

When specifying window assemblies, ensure that the threat severity level and required penetration delay time is included.

5-5.8.2 Windows to Resist Threat Severity Level II.

Glazing, frame, and anchor designs for windows to resist threat severity level II are provided in Table 5-14 through Table 5-16 for one minute of penetration delay. These designs are for installation in a wood frame wall. Other options for window components are available in Table 5-20.

Table 5-14 Glazing Specifications - Threat Severity Level II

TYPE	MINIMUM THICKNESS	CROSS-SECTION
Air Gap	1 inch (25 mm)	1/4 inch (6 mm) Laminated Annealed Glass, 1/4 inch (6 mm) AIR, 1/2 inch (13 mm) Laminated Polycarbonate
Extruded Ionomer	13/16 inch (20 mm)	3/16 inch (5 mm) Annealed Glass, 1/2 inch (13 mm) extruded IONOMER, 1/8 inch (3 mm) Annealed Glass
Glass-Clad Polycarbonate	11/16 inch (17 mm)	3/16 inch (5 mm) Annealed Glass, 3/8 inch (10 mm) Polycarbonate, 3/16 inch (5 mm) Annealed Glass
Monolithic Polycarbonate	3/8 inch (10 mm)	3/8 inch (10 mm) Polycarbonate

Table 5-15 Frame Specifications - Threat Severity Level II

COMPONENT	SIZE, INCH (MM)
Minimum Frame Thickness	1/4 inch (6 mm) Steel
Minimum Removable Stop Thickness	3/16 inch (5 mm) Steel
Minimum Bite Depth	1 inch (25 mm)
Minimum Glazing Rabbet Depth	1-1/4 inches (32 mm)
Maximum Width Between Frame Members	42 inches (107 cm)

Table 5-16 Miscellaneous Specifications - Threat Severity Level II

COMPONENT	REQUIREMENTS	
Anchor Lag Bolt	Minimum Diameter: 3/8 inch (10 mm)	Minimum Embedment: 3 inches (75 mm)
Lag Bolt Spacing	Frame Corner to Bolt - Maximum Spacing: 9 inches (230 mm)	Between Adjacent Bolts -Maximum Spacing: 18 inches (460 mm)
Removeable Stop Anchorage: Shouldered Bolt	Minimum Size: 3/8 inch (10 mm)	Minimum Number per Side: 2
Removeable Stop Bolt Spacing	Frame Corner to Bolt - Maximum Spacing: 9 inches (230 mm)	Between Adjacent Bolts - Maximum Spacing: 18 inches (460 mm)

5-5.8.3 Windows to Resist Threat Severity Level III.

Glazing, frame, and anchor designs for threat severity level III are provided in Table 5-17 through Table 5-19 for 4 minutes of penetration delay time. These designs are for installation of windows in grout-filled CMU and reinforced concrete walls. Other options for window components are available in Table 5-20.

Table 5-17 Glazing Specifications -Threat Severity Level III

TYPE	MINIMUM THICKNESS	CROSS-SECTION
Air Gap	1-3/4 inches (44 mm)	1/4 inch (6 mm) Laminated Annealed Glass, 1/4 inch (6 mm) AIR, 1-1/8 inches (28 mm) Laminated Polycarbonate
Extruded Ionomer	2-1/8 inches (54 mm)	7/8 inch (22 mm) Laminated Annealed Glass, 1 inch (25 mm) extruded IONOMER, 3/32 inch (4 mm) Annealed Glass
Glass-Clad Polycarbonate	15/16 inch (24 mm)	3/16 inch (5 mm) Strengthened Glass, 1/4 inch (6 mm) Annealed Glass, 3/8 inch (10 mm) Laminated Polycarbonate
Laminated Polycarbonate	1-1/4 inches (32 mm)	1-1/4 inches (32 mm) Laminated Polycarbonate

Table 5-18 Frame Specifications - Threat Severity Level III

COMPONENT	SIZE
Minimum Frame Thickness	1/4 inch (6 mm) Steel
Minimum Removable Stop Thickness	3/16 inch (5 mm) Steel
Minimum Bite Depth	1 inch (25 mm)
Minimum Glazing Rabbet Depth	1-1/4 inches (32 mm)
Maximum Width Between Frame Members	42 inches (107 cm)

Table 5-19 Miscellaneous Specifications - Threat Severity Level III

COMPONENT	REQUIREMENTS	
One-Piece Expansion Sleeve	Minimum Diameter: 1/2 inch (13 mm)	Minimum Embedment: 3 inches (75 mm)
Taper Bolt	Minimum Diameter: 3/8 (10 mm)	Minimum Embedment: 3 inches (75 mm)
Taper Bolt Spacing	Frame Corner to Bolt -Maximum Spacing: 6 inches (150 mm)	Between Adjacent Bolts - Maximum Spacing: 12 inches (300 mm)
Removeable Stop Anchorage: Shouldered Bolt	Minimum Size: 3/8 inch (10 mm)	Minimum Number per Side: 2
Removeable Stop Bolt Spacing	Frame Corner to Bolt -Maximum Spacing: 9 inches (230 mm)	Between Adjacent Bolts - Maximum Spacing: 18 inches (460 mm)

5-5.8.4 Windows to Resist Threat Severity Level IV.

There are few commercially available glazing systems that provide forced entry resistance against threat severity level IV. See Table 5-20 for window component options.

5-5.8.5 Windows to Resist Threat Severity Level V.

There are no commercially available glazing systems that provide forced entry resistance against threat severity level V. When the threat severity is established at level V, windows should be eliminated, sized below the man-passable threshold, or designed as slat windows (long narrow windows less than 6 inches (150 mm) wide).

Table 5-20 Window Materials

ITEM NUMBER	WINDOW MATERIAL DESCRIPTION	THREAT SEVERITY LEVEL			
		II	III	IV	V
1	1/2" POLYCARBONATE GLAZING	3	1		
2	1/4" ACRYLIC IN ALUMINUM FRAME	1	1		
3	1/8" PLATE GLASS, 1/2" A-36 STEEL BARS @ 6" EW		5		
4	1/8" PLATE GLASS, 10 GA STEEL MESH 6” by 6” COVER	2			
5	1/4" LAMINATED GLASS IN ALUMINUM FRAME	2			
6	1/4" WIRE GLASS IN ALUMINUM FRAME	1			
7	1/4" TEMPERED GLASS	1			
8	9/16" LAMINATED GLASS IN ALUMINUM FRAME	2			
9	1/2" ACRYLIC	1			
10	11/16-INCH, GLASS-CLAD WITH 3/8-INCH POLYCARBONATE CORE	1	1	1	
11	13/16-INCH, GLASS-CLAD WITH 1/2-INCH POLYCARBONATE CORE	15	5	5	
12	15/16-INCH, GLASS-CLAD WITH 3/4-INCH POLYCARBONATE CORE	30			

NOTE: For the use of the above table, refer to Paragraph 5-4.

5-5.8.6 Grilles and Grates.

Alternatives to the use of glazing systems may be grilles or gratings over the window openings. Combinations of glazing and grilles can also be used to increase delay time. Note that the use of grilles or grates over windows that can be used as fire exits must comply with the Life Safety Code.

Table 5-21 shows that penetration delay time is directly related to the diameter and spacing of the protective bars. If, for example, No. 5 (16mm) bars are spaced 3 inches (75 mm) apart (both vertically and horizontally) to form a grille, a penetration delay time of about 2.5 minutes can be achieved. When bars are used to delay penetration, properly anchoring them to the wall is critical, since it may be easier to break them loose than to cut them. Bar type grills should only be used with concrete walls, ceilings, roofs, slabs, or CMU walls. They must be embedded at least 6 inches (150 mm) into the wall, welded to a steel frame with concrete anchors, and cast in place during construction.

Table 5-21 Time Required for Making a Man-Passable Opening in Grilles

BAR SIZE	3/8 INCH (10 MM)	1/2 INCH (13 MM)	5/8 INCH (16 MM)	3/4 INCH (19 MM)
	SEVERITY THREAT LEVELS II and III		SEVERITY THREAT LEVEL IV	
SPACING	TIME (MINUTES)	TIME (MINUTES)	TIME (MINUTES)	TIME (MINUTES)
3 inches (75 mm)	1.2	1.7	2.5	3.5
3.5 inches (90 mm)	0.8	1.2	1.6	2.3
4 inches (100 mm)	0.8	1.2	1.6	2.3
4.5 inches (115 mm)	0.8	1.2	1.6	2.3
5-9 inches (125-225 mm)	0.4	0.6	0.8	1.2

NOTES: Estimated times are for a single-layer grille composed of steel bars of the diameter shown, equally spaced both horizontally and vertically.

Times shown are total time measured in minutes required to provide a man-passable opening of at least 96-square-inch (619 cm^2) or with a single rectangular dimension greater than 6 inches (15 cm).

All reinforcing bar should be embedded at least 6 inches (15 cm) into the surrounding concrete wall and welded at intersections.

5-5.9 Utility Openings.

Utility openings, manholes, tunnels, air conditioning ducts, filters, or equipment access panels can provide aggressors with an easily accessible entrance or exit route. These passages can also circumvent existing IDS. Such openings must be eliminated or kept below the man-passable 96 square inches (619 cm^2) threshold. For long utility conduits, it is not always necessary to hold to the minimum man-passable threshold. For these cases, the threshold can be increased to 144 square inches (930 cm^2) depending on the configuration of the conduit. Bends in long utility runs effectively impede movement through the conduit. Where exits from a utility conduit (manholes and junction boxes, among others) can be effectively sealed from the secure side, the size of the conduit is immaterial unless direct access to the secure space and bypass of the IDS is possible. Ensure that mechanical designers are aware of any restrictions of utility openings being designed so they can adjust air flow designs to accommodate the restrictions; this is particularly import for HVAC designers.

5-5.9.1 Utility Opening Treatments to Resist Threat Severity Levels II and III.

When it is not feasible to hold to the minimum man-passable 96 square inches (619 cm^2) threshold, use single or multiple gratings or grilles for threat severity levels II and III. Protect man-passable openings with the treatments shown in Table 5-21 and Table 5-22 to provide the indicated delay times. Delay times in the tables are for a single layer.

Table 5-22 Utility Opening Materials

Item Number	Utility Opening Material Description	Threat Severity Level			
		II	III	IV	V
1	1/4" DIAMETER A-36 STEEL BARS 1-1/4" EW	15	7		
2	3/8" DIAMETER A-36 STEEL BARS 1-1/4" EW		8		
3	3/8" HARDENED STEEL BARS @ 4"V 8"H		5	1	
4	1/2" HARDENED STEEL BARS @ 4"V 8"H		5	2	<1
5	1/2" A-36 STEEL BARS @ 4"V 8"H	1	1		<1
6	1/2" A-36 STEEL BARS @ 4"V, 3/8" by 1-1/4" A-36 STEEL BARS @ 8"H	2	2		<1
7	1/2" A-36 STEEL BARS @ 4"V, l/8" by 1-1/2" A-36 STEEL BARS @ 8"H	2	2		<1
8	1/2" HARDENED STEEL BARS @ 6" EW		4	2	<1

Item Number	Utility Opening Material Description	Threat Severity Level			
		II	III	IV	V
9	1/2" A-36 STEEL BARS @ 6" EW		4		<1
10	1/2" A-36 STEEL BARS @ 2-1/4" EW	21	9		
11	7/8" HARDENED STEEL BARS@ 4"V, 3/8" by 2·1/4" HARDENED STEEL BARS @ 8"H		7		<1
12	7/8" A-36 STEEL BARS @ 4"V, 3/8" by 2-l/4" A-36 STEEL BARS @ 8"H		5		<1
13	#5 STEEL WIRE 3/4" EW		6		
14	#8 STEEL WIRE 5/8" EW		6		
15	22 GA SHEET METAL DUCT, DIFFUSER, 1/2" DIAMETER A-36 STEEL BARS 6" EW	3			1*
16	22 GA SHEET METAL DUCT, 36" DIAMETER, 20-FOOT VERTICAL		14		
17	24 GA SHEET METAL DUCT 24" by 24", 8-FOOT HORIZONTAL		6		

NOTE: For the use of the above table, refer to Paragraph 5-4.

5-5.9.2 Utility Opening Treatments to Resist Threat Severity Level IV.

Use grilles constructed with larger size bars (No. 5 (16 mm) or greater) and various constrictive barrier designs for threat severity level IV. Options are shown in Table 5-21.

5-5.9.3 Utility Opening Treatments to Resist Threat Severity Level V.

Threat severity level V requires sacrificial enclosing structures around openings.

5-5.9.4 Special Treatments for Utility Openings.

The following describes typical utility openings and protective design options for hardening them when they cannot be eliminated or sized below the man-passable threshold.

5-5.9.4.1 Sewers and Manholes.

Providing multiple pipes, each less than the man-passable opening threshold, is more desirable than a single large pipe. If a large passageway is required, structural walls, floors, and foundations that are accessible from underground passageways should provide penetration delay times equivalent to the basic structure. Access points from sewer lines into secure structures should be equipped with IDS that can detect intrusion activities. The use of grilles in storm and sanitation systems should be avoided because of the operation and maintenance problems caused by such structures. Where grilles are required on storm sewers, inlet filter screens are highly recommended to prevent clogging.

5-5.9.4.2 Pipe Chases.

Pipe chases are horizontal or vertical framed-in passageways that vary in size. They are typically constructed of studs and gypsum board. If unprotected, vertical chases connecting adjacent floors or horizontal chases running through walls may provide access to secure areas. Horizontal chases may provide little resistance to movement except obstacles such as internal equipment, piping, cable, and the entrance door(s). Chases provide entrance and exit points to overhead crawl spaces. Pipe chases that provide man-passable access to HVAC ducts and maintenance crawl spaces larger than the man-passable opening threshold should be alarmed or barriers inserted to prevent free movement through the pipe chase.

5-5.9.4.3 Exhaust Vents.

Exhaust vents through roofs and walls are usually protected by the associated equipment. Because the ductwork and dampers are usually constructed of light sheet metal, penetration can be easily accomplished with a low severity threat tool mix. Typical exhaust ducts range in size up to 4 by 8 feet (1,200 by 2,400 mm). The discussion of hardening techniques under gravity vents, ventilation ducts, and air distribution fixtures generally applies in the case of exhaust vents.

5-5.9.4.4 HVAC Ductwork and Vent Pipes.

If maintenance access is not required, filling duct openings with a 2-foot (0.6-m) length (minimum) of steel pipe, welded together and anchored securely in place by a welded steel plate on the inside (secure side) of the structure as shown in Figure 5-6 is an option. The honeycomb material should be made of steel. For this barrier system, penetration delay time will result from the length of the honeycomb and the necessity for multiple long cuts and debris removal in the relatively restricted space of the duct. If possible, such a barrier should be located at a sharp turn to further restrict the use of cutting tools. This arrangement can also be used for tunnels with electrical lines, since maintenance personnel can have access to both sides of the impediment (constriction), and cables can be threaded through the relatively short constriction.

An alternative option is to weld the steel pipes front and back at least 3 inches (75mm) on each end and at each point where the steel pipes intersect. No steel pipe diameter inside the pipe should be greater than the man-passable threshold opening. A second approach is to eliminate the center steel pipe and to connect the remaining pipes inside the tunnel with continuous welds; however, if this approach is taken, the designer should be careful to ensure that the area in the center, which would have been filled by the seventh center pipe, as shown in Figure 5-7, is not a man-passable opening. These constrictions should be located at secure walls with equivalent penetration resistance. The length of the constriction will force an aggressor to attack and remove each barrier separately. The confined working space and the necessity for debris removal further add to penetration delay time.

Figure 5-6 Vent and Duct Hardening Barriers

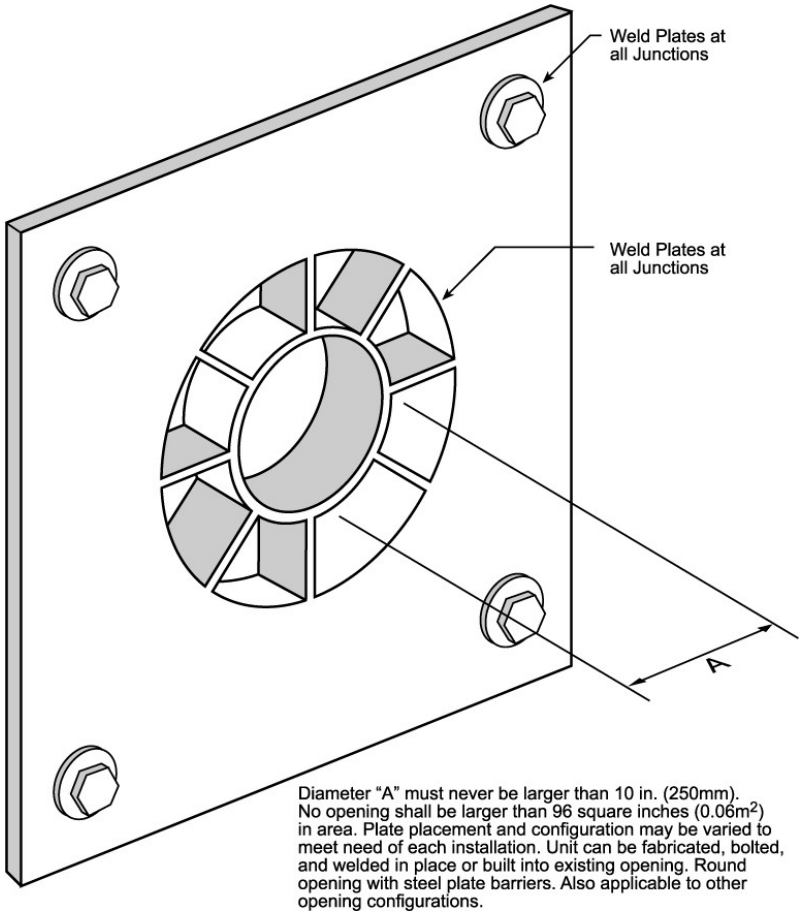
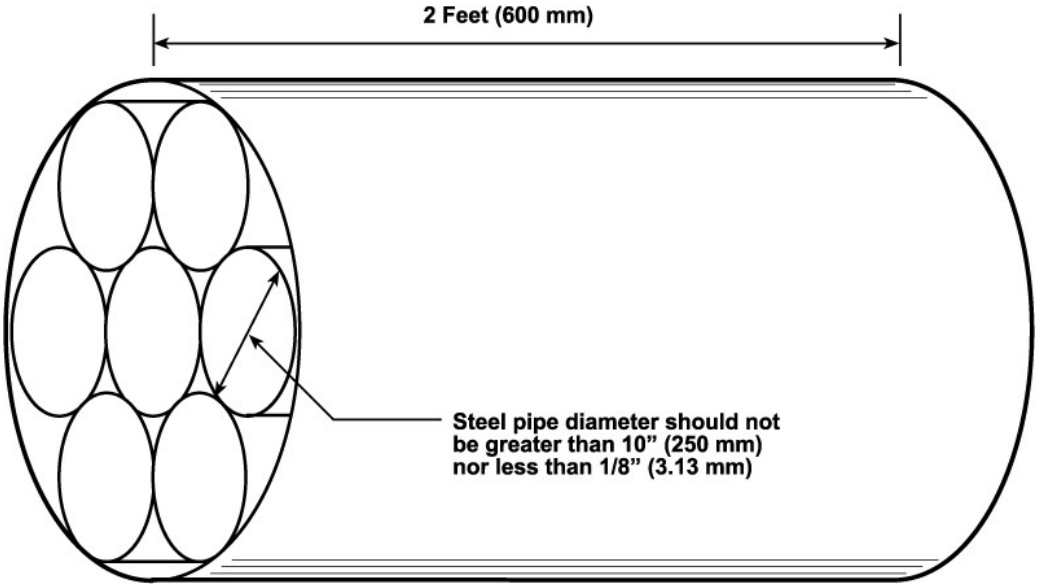


Figure 5-7 Vent Pipe and Chase Protection



5-5.9.4.5 Sleeves and Trays.

Sleeves are pipe penetrations through walls, roofs, and ceilings. Trays are removable, sheet-metal-covered conduits. Sleeves and trays that penetrate security walls should be less than the man-passable opening threshold. Penetrations should be angled upward and, to the extent practical, contain sharp turns to prevent the easy introduction of hooks, cables, or explosive devices. Penetration resistant barriers are similar to those used to protect pipe chases.

5-5.9.4.6 Ducts.

Ducts are round or square sheet metal or fiberglass conduits that may vary in size. Ducts constructed of sheet metal, usually 28 gauge (0.4 mm) through 14 gauge (1.9 mm), can readily be cut with hand tools and light power tools. These ducts do not present a significant barrier to penetration. Penetration resistance is, however, sometimes enhanced using ducts of less than man-sized cross section and the inclusion of required apparatus, such as turning vanes, dampers, pressure plates, and final air distribution fixtures. Duct dimensions should be kept at less than a man-passable cross section. Penetration resistant barriers are similar to those used to protect pipe chases.

5-5.9.4.7 Filter Banks.

Filter banks are unlikely to offer any significant penetration delay time. A hardened enclosure, with one of the vent or duct-hardening techniques should be used to prevent aggressor entry.

5-6 RETROFIT CONSTRUCTION.

This section provides design options for retrofitting an existing building against forced entry attack. The objective of the design is to increase the penetration resistance of the existing building using retrofit options that provide the required penetration delay against the threat severity level for the building. The design should also provide a balanced design between all building components. The following paragraphs provide forced entry delay expected from the existing construction followed by the penetration delay time enhancement of various retrofit options.

5-6.1 General.

Determine if the existing structure and foundations will support the additional weight of the enhanced construction. If not, the use of additional defense layers may be an alternative to retrofit.

5-6.2 Walls.

Solid plywood construction can be used to resist a low severity threat. For severity threat levels III and IV, the choices are limited to grout-filled and reinforced CMUs for lower delay time requirements, and conventional or SFR concrete for higher delay time requirements. Threat severity level V will require sacrificial areas, multiple barriers, or reinforced concrete barriers.

The following paragraphs provide information for estimating the penetration delay times for walls in existing facilities and retrofit options for hardening these walls if additional delay time is required.

5-6.2.1 Penetration Delay Times for Existing Walls.

Table 5-23 shows the maximum penetration delay times for representative stud-girt walls. If existing wall types are not represented in the table, either take credit for the closest type or take no credit.

For conventional concrete materials, the penetration delay times range from about 2 minutes to greater than 60 minutes.

5-6.2.2 Walls to Resist Threat Severity Level II.

If an existing stud-girt wall construction uses a combination of plywood, stucco, or gypsum that meets, or exceeds, 3/4-inch (19-mm) in thickness; light sheet metal; or conventional masonry, it will provide the required one minute penetration delay time against a threat severity level II attack. Otherwise, add materials to the inside of the wall to achieve the one minute penetration delay time or take no credit for delay.

Note that in cases where materials such as expanded metal are applied to a wall, it is common practice to cover those materials with gypsum wallboard for aesthetic purposes.

5-6.2.3 Walls to Resist Threat Severity Level III.

5-6.2.3.1 Stud-Girt Walls.

Table 5-23 shows recommended treatments for existing stud-girt walls to provide resistance to threat severity level III.

Table 5-23 Stud-Girt Construction Retrofit Options for Threat Level III

CONSTRUCTION		PENETRATION DELAY TIME (MINUTES)
1	2- by 4-inch (50- by 100-mm) wood stud frame at 16 inches (400 mm) on center w/bevel siding at 1.5-inch (37.5-mm) lap joints. One-layer No. 15 felt paper, and 1- by 6-inch (25- by 150-mm) sheathing diagonally and 3/8-inch (10-mm) GWB. Attach the following to secure side (opposite from attack side): • 3/4-inch (19-mm) plywood, No. 9 expanded metal and 3/4-inch (19-mm) plywood.	5.0
2	1-inch (25-mm) tongue-and-groove layered with 1/2-inch (13-mm) plywood. Attach either of the following to secure side (opposite from attack side): • 9-gauge (3.8-mm) chain-link fence fabric nailed to wall • 3/16-inch (4.7-mm) steel plate attached to wall with lag bolts.	 1.8 1.9

5-6.2.3.2 Masonry Walls.

Several techniques for hardening both hollow and mortar-filled 8-inch (200-mm) CMU block are illustrated in Figure 5-8 through Figure 5-12. Note that the retrofit hardening layers are applied to the interior (secure side) of the cross section. These options were specifically designed and tested to provide enhanced attack resistance. The CMU sections vary in the type of retrofit materials used.

Figure 5-8 Retrofit Hardening of 8-inch (200mm) CMU Wall (1 of 4)

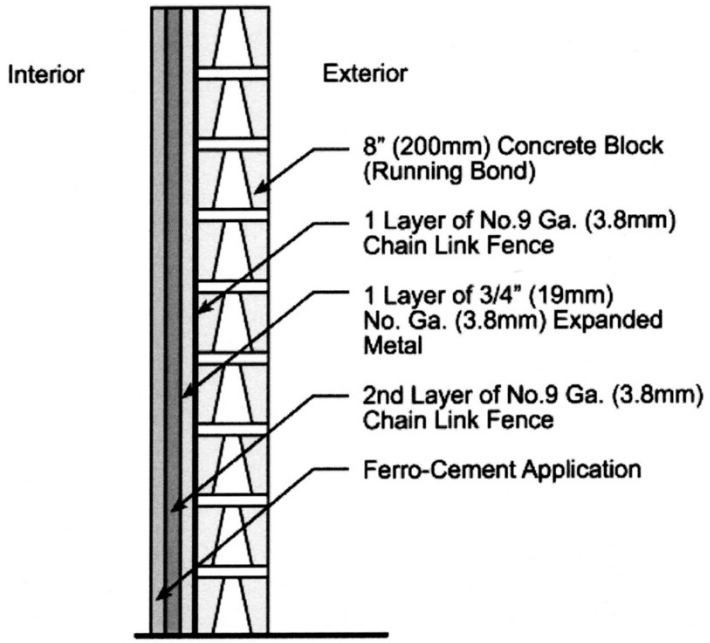
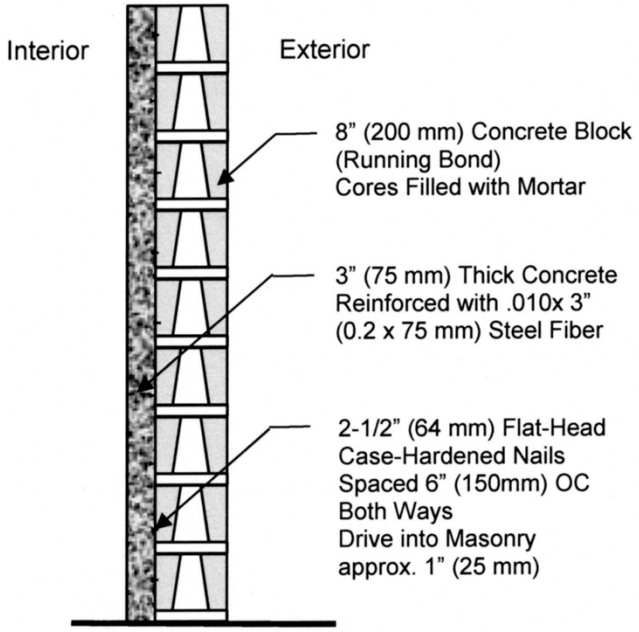
CONSTRUCTION	PENETRATION TIME (MINUTES)	
	III	IV
	8	4
	28	23

Figure 5-9 Retrofit Hardening of 8-inch (200mm) CMU Wall (2 of 4)

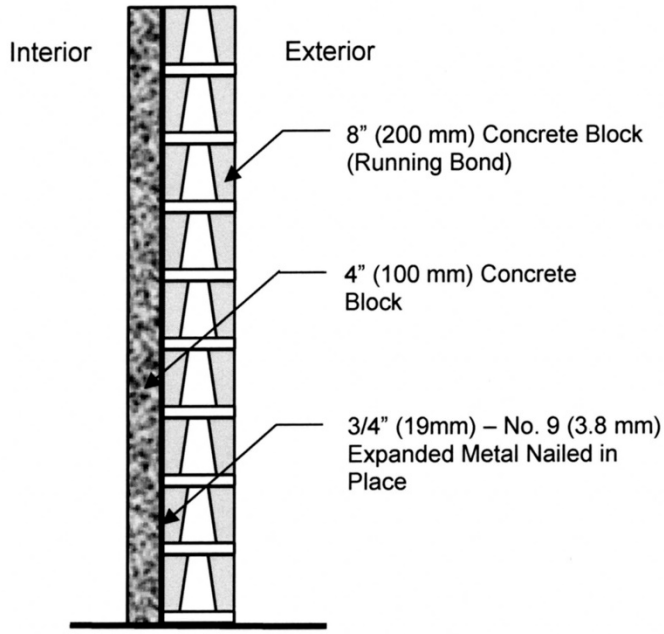
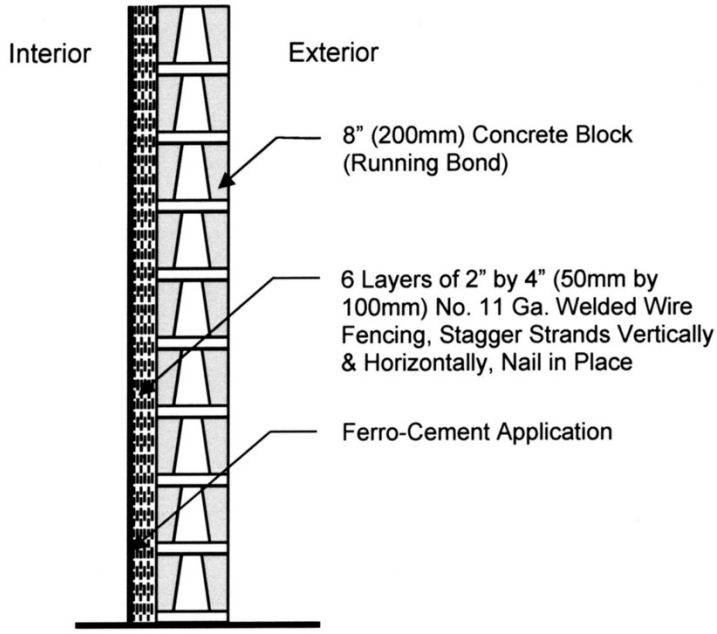
CONSTRUCTION	PENETRATION TIME (MINUTES)	
	III	IV
	4	4
	7	6

Figure 5-10 Retrofit Hardening of 8-inch (200mm) CMU Wall (3 of 4)

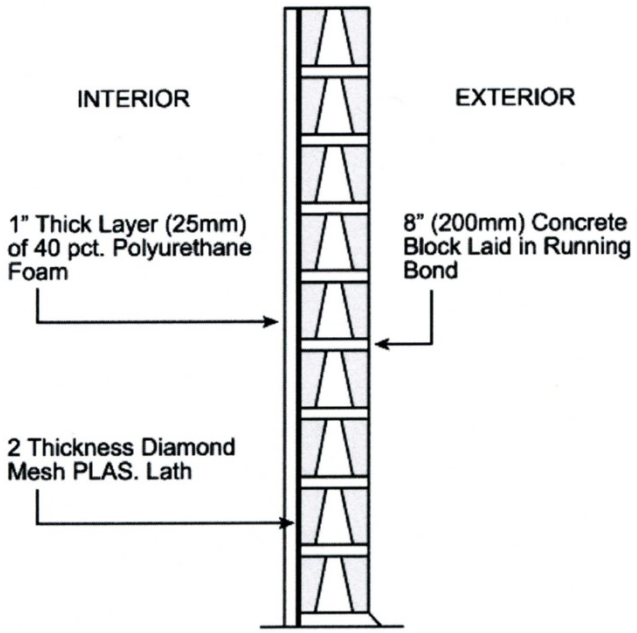
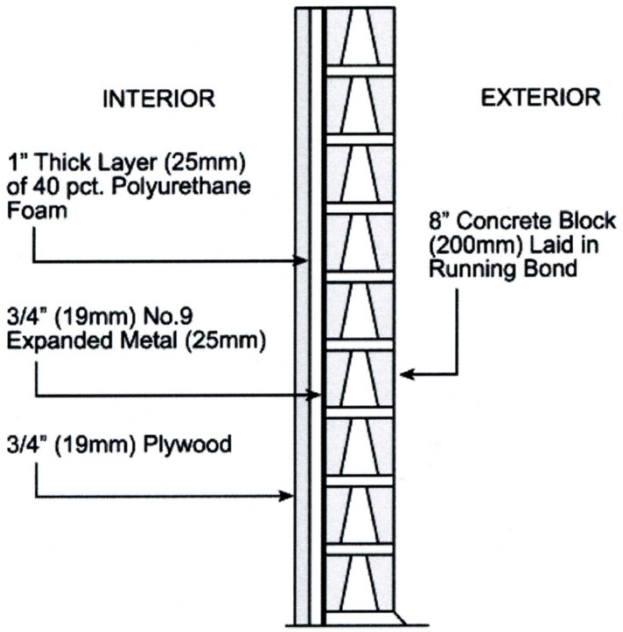
CONSTRUCTION	PENETRATION TIME (MINUTES)	
	III	IV
	2	2
	3.5	3.5

Figure 5-11 Retrofit Hardening of 8-inch (200mm) CMU Wall (4 of 4)

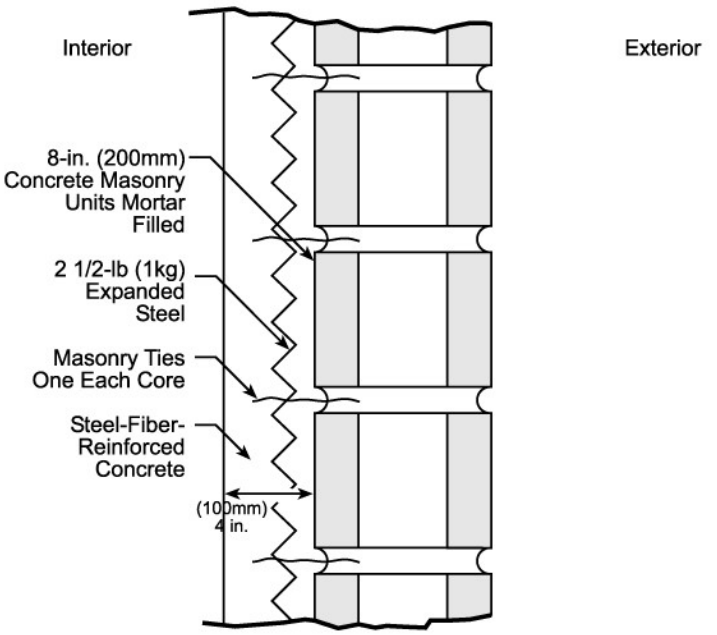
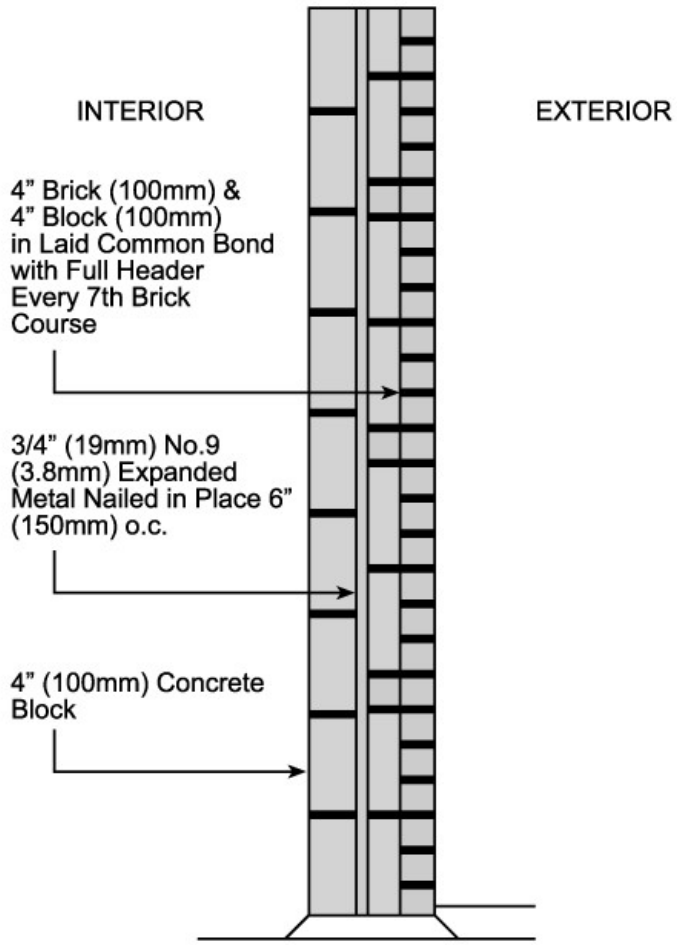
CONSTRUCTION	PENETRATION TIME (MINUTES)	
	III	IV
	(a)	30
(a) Not possible to penetrate at the indicated threat severity level		

Figure 5-12 Wood/Metal Composite Masonry Design Option

CONSTRUCTION	PENETRATION TIME (MINUTES)	
	III	IV
	3	3

5-6.2.3.3 Reinforced Concrete Walls.

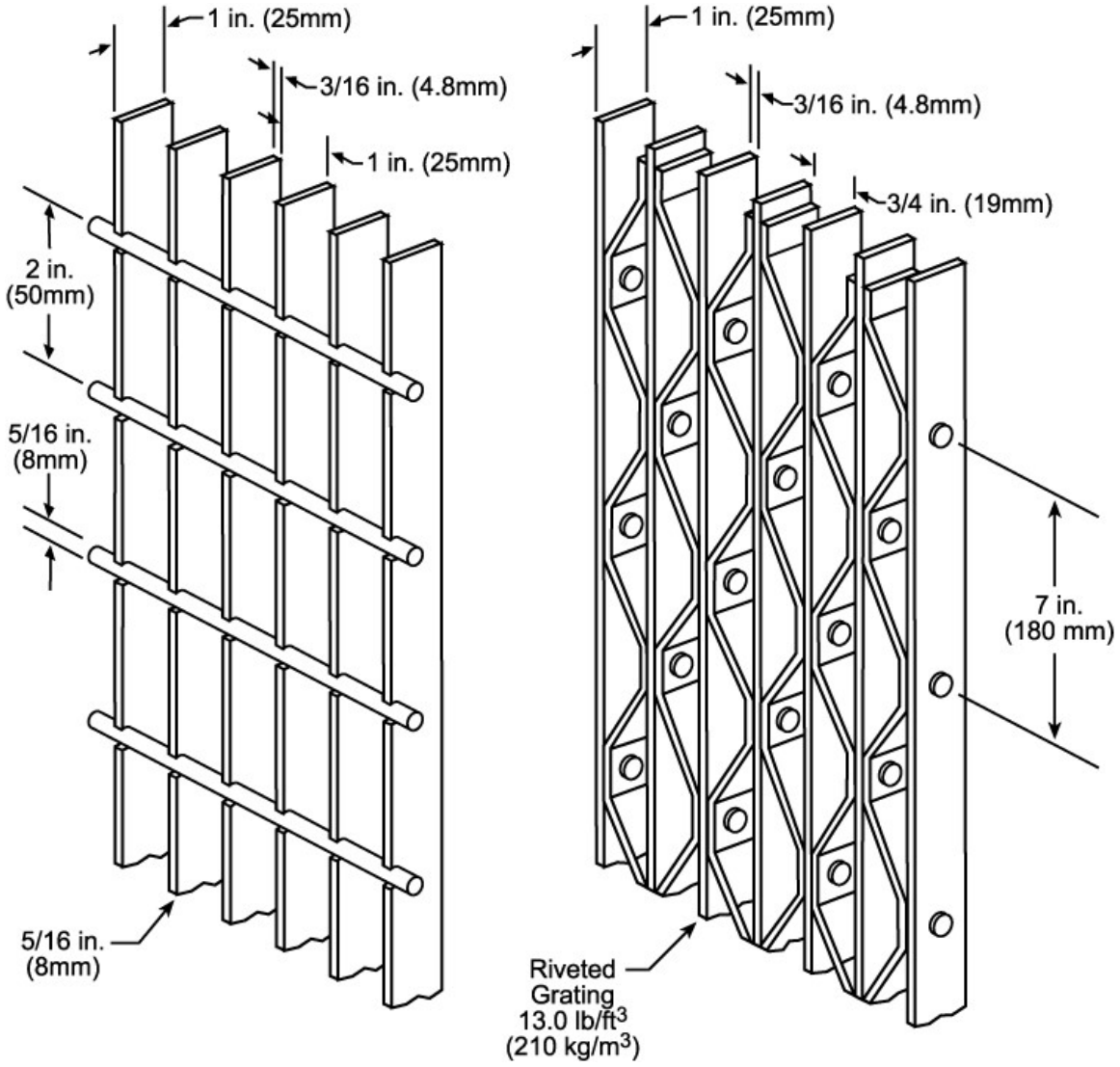
Reinforced concrete 6 inches (150 mm) thick with the "B" reinforcing bar combination (Table 5-2) provides minimum penetration delay times up to about 7.5 minutes for threat severity level III. If the concrete thickness and reinforcing bar combination is outside the threat severity level III region shown in Figure 5-2, using hand-held attack tools alone is not practical. In this case, the existing wall will provide penetration resistance. If the delay time provided by existing concrete construction is inadequate, penetration delay time can be doubled from the values shown in Figure 5-2 by bolting 10-gauge (3.4-mm) standard sheet steel to the interior surface of the wall using taper bolts or expansion sleeve anchors. This effect is gained by preventing internal spalling of the concrete.

5-6.2.4 Walls to Resist Threat Severity Level IV.

5-6.2.4.1 Stud-Girt Walls.

The riveted or welded steel grating shown in Figure 5-13 can be attached to the interior of a stud-girt wall with lag or through bolts to increase the delay time. Additional penetration times against threat severity level IV are approximately 2 minutes minimum for the riveted and 1 minute minimum for welded grating.

Figure 5-13 Welded and Riveted Steel Grating



5-6.2.4.2 Masonry Walls.

The retrofit designs in Figure 5-8 through Figure 5-10 can be used for resistance to threat severity level IV. In addition, the penetration delay times for solid core CMU block walls can be doubled by attaching 10-gauge (3.4-mm) sheet steel to the interior surface with taper bolts or expansion sleeve anchors.

If the penetration delay time is still not adequate, steel-plywood options can be used. Use a layer of 3/4-inch (19-mm) plywood sandwiched between two layers of 10 gauge (3.4-mm) hot-rolled steel to provide about 6 minutes of additional penetration delay time. The penetration delay time can be increased by about five minutes with the addition of another wood and steel layer. This rule of thumb can be applied to the addition of more layers until the desired penetration delay time is reached. Penetration delay time for steel-plywood systems can be increased by changing the steel material to 9-gauge (3.8-mm) ASTM A1008, Class 2, high-strength, low-alloy steel. One layer of 3/4-inch (19-mm) plywood sandwiched between two layers of this steel will provide 14 minutes of penetration delay time. Adding layers of 90-pound (200-kg) gravel finish roofing paper between the plywood and steel further increases the penetration delay time to about 20 minutes. These times are added to the increased penetration delay time provided by preventing internal spalling of the concrete (approximately double the initial penetration delay time).

5-6.2.4.3 Reinforced Concrete Walls.

If the delay time provided by existing concrete construction is inadequate, penetration delay time can be doubled by bolting (taper bolts or expansion sleeve anchor) 10-gauge (3.4-mm) standard sheet steel to the interior surface of the wall. This effect is gained by preventing internal spalling of the concrete.

If the penetration delay time is still not adequate, steel-plywood options as described in Paragraph 5-6.2.4.2 can be used. Standard welded and riveted steel grating can also be used to provide additional delay time. This grating is available in standard 2- by 10-foot (0.6- by 3-m) panels and can be attached to the secure side concrete walls with taper bolts or expansion sleeve anchors. They can also be assembled in a variety of free-standing configurations of any length (in 2-foot (0.6-m) increments). Additional penetration delay times against threat severity level IV are approximately two minutes minimum for the riveted and one minute minimum for welded grating, plus additional time gained by preventing spallation if attached to the secure side of the wall (approximately double the initial penetration delay time).

5-6.2.5 Walls to Resist Threat Severity Level V.

The use of bulk explosives can be effective in quickly producing man-passable openings. Only a reinforced concrete structure 12 inches (305 mm) or more in thickness can provide penetration delay times greater than one minute. In general, the options that will protect existing construction from an explosive penetration attack are retrofit prohibitive because of the weight restrictions and cost implications of retrofitting existing facilities. The only choice is to move the critical asset being protected away from exterior walls and roofs and develop one or more intermediate defense layers. The exterior of the building will then serve as a sacrificial barrier that will force the aggressor to penetrate multiple barriers and limit the use of explosives inside the structure.

5-6.3 Roofs.

Conventional roof construction offers little resistance to downward forced entry attack, except where reinforced concrete slabs form the structure.

5-6.3.1 Roofs to Resist Threat Severity Level II.

Since solid plywood or metal roof construction provides a delay of less than one minute against threat severity level II, replace the existing roof with one of the roof types shown in Table 5-5.

5-6.3.2 Roofs to Resist Threat Severity Levels III and IV.

Conventional or fiber reinforced concrete roofs are required to resist threat severity levels III and IV. If the existing roof is of stud-girt construction, the only choice is to move the critical asset being protected away from exterior walls and roofs and develop one or more intermediate defense layers. The exterior of the building will then serve as a sacrificial barrier that will force the aggressor to penetrate multiple barriers. Figure 5-2, Figure 5-3, and Table 5-2 can be used to estimate penetration times for existing reinforced concrete construction of roofs. In general, for reinforced concrete walls less than 12 inches (30 cm) thick, penetration delay times for a downward attack on a roof will be lower than a similar attack on a wall; therefore, use the next lowest thickness 1 inch (2.5 cm) of concrete in Figure 5-2 to determine the existing penetration delay rating.

If the penetration delay rating for the existing roof is not adequate, add a layer of 3/4-inch (19-mm) plywood sandwiched between two layers of 10 gauge (3.4-mm) hot-rolled steel to provide about 6 minutes of additional penetration delay time. The penetration delay time can be increased by about five minutes with the addition of another wood and steel layer. This rule of thumb can be applied to the addition of more layers until the desired penetration delay time is reached. Penetration delay time for steel-plywood systems can be increased by changing the steel material to 9-gauge (3.8-mm) ASTM A1008, Class 2, high-strength, low-alloy steel. One layer of 3/4-inch (19-mm) plywood sandwiched between two layers of this steel will provide 14 minutes of penetration delay time. Adding layers of 90-pound (200-kg) gravel finish roofing paper between the plywood and steel further increases the penetration delay time to about 20 minutes. These times are added to the increased penetration delay time provided by preventing internal spalling of the concrete (approximately double the initial penetration delay time).

5-6.3.3 Roofs to Resist Threat Severity Level V.

The use of bulk explosives or platter charges can be effective in quickly producing man-passable openings. Only a reinforced concrete structure 12 inches (305 mm) or more in thickness can provide penetration delay times greater than one minute.

In general, the options that will protect existing construction from an explosive penetration attack are retrofit prohibitive because of the weight restrictions and cost implications of retrofitting existing facilities. The only choice is to move the critical asset being protected away from exterior walls and roofs and develop one or more intermediate defense layers. The exterior of the building will then serve as a sacrificial barrier that will force the aggressor to penetrate multiple barriers and limit the use of explosives inside the structure.

5-6.3.4 Roof Equipment and Openings.

For retrofit projects, use the designs in Paragraphs 5-5.2.4 through 5-5.2.6. to secure roof-mounted equipment and utility openings. Eliminate skylights or use tested grille arrangements shown in Figure 5-13 to protect openings where required. Secure all hatches, penthouses, exterior ladders, and fire escapes.

5-6.4 Ceilings and Floors.

Floor and ceiling assemblies are the horizontal (top and bottom) components of the 6-sided intermediate defense layers. Floors may be exposed to exterior forced entry if the asset is in the space below; and, ceilings may be exposed to forced entry if the asset is in the space above. Select floor and ceiling construction which provides the required delay time where applicable.

5-6.4.1 Ceilings and Floors to Resist Threat Severity Level II.

Existing conventional floor and ceiling assemblies of 3/4-inch (19-mm) plywood on wood joists provide at least one minute of penetration delay, they are adequate for resistance to the threat severity level II.

5-6.4.2 Ceilings and Floors to Resist Threat Severity Levels III and IV.

Reinforced stud-girt or reinforced concrete ceilings and floors are required to resist threat severity levels III and IV. Figure 5-2, Figure 5-3, and Table 5-2 can be used to estimate penetration times for existing reinforced concrete construction of ceilings and floors. Penetration delay times for an upward attack on a ceiling (floor of upper level) will be higher than the same attack on a wall; therefore, use the next lowest thickness of concrete 1 inch (2.54 cm) or use a less compact configuration of reinforcing bar size and spacing. For a downward attack on a floor (ceiling of lower level), penetration delay times are lower for a similar attack on a wall; therefore, use the next highest thickness of concrete 1 inch (2.54 cm) or use a configuration with more layers of reinforcing bar size and spacing.

If the existing ceiling or floor is of stud-girt construction, the existing reinforced concrete ceiling or floor cannot provide an adequate penetration delay time, and supporting walls can bear the additional weight, use a layer of 3/4-inch (19-mm) plywood sandwiched between two layers of 10 gauge (3.4-mm) hot-rolled steel to provide about 6 minutes of additional penetration delay time. The penetration delay time can be increased by about 5 minutes with the addition of another wood and steel layer. This rule of thumb can be applied to the addition of more layers until the desired penetration delay time is reached. Penetration delay time for steel-plywood systems can be increased by changing the steel material to 9-gauge (3.8-mm) ASTM A1008, Class 2, high-strength, low-alloy steel. One layer of 3/4-inch (19-mm) plywood sandwiched between two layers of this steel will provide 14 minutes of penetration delay time. Adding layers of 90-pound (200-kg) gravel finish roofing paper between the plywood and steel further increases the penetration delay time to about 20 minutes. These times are added to the increased penetration delay time provided by preventing internal spalling of the concrete (approximately double the initial penetration delay time).

5-6.4.3 Ceilings and Floors to Resist Threat Severity Level V.

The use of bulk explosives or platter charges can be effective in quickly producing man-passable openings. Only a reinforced concrete structure 12 inches (305 mm) or more in thickness can provide penetration delay times greater than one minute. In general, the options that will protect existing construction from an explosive penetration attack are retrofit prohibitive because of the weight restrictions and cost implications of retrofitting existing facilities. The only choice is to move the critical asset being protected away from exterior walls and roofs and develop one or more intermediate defense layers. The exterior of the building will then serve as a sacrificial barrier that will force the aggressor to penetrate multiple barriers and limit the use of explosives inside the structure.

5-6.5 Personnel Entrances.

Existing personnel entrances should provide the same penetration delay times as the other components of the defense layer.

Refer to Table 5-7 through Table 5-12 for evaluating the penetration delay times for existing personnel entry doors. Where existing doors do not provide adequate penetration delay times, they must be upgraded or replaced. As an alternative, additional doors can be added in a vestibule layout to force aggressors to attack multiple doors in sequence before they can penetrate the defense layer.

5-6.6 Doors, Frames and Locks (Non-Entry).

If the existing building or intermediate defense layer perimeters have non-entry doors, perform a life safety evaluation to determine if any non-entry doors can be eliminated. If non-entry doors can be eliminated, fill in the walls to match existing materials.

Refer to Table 5-7 through Table 5-12 for evaluating the penetration delay times for existing doors. Where existing non-entry doors do not provide adequate penetration delay times, they must be upgraded or replaced.

5-6.7 Windows.

Conventional windows provide little resistance to even the lowest threat severity levels of the forced entry tactic. With special glazing materials and frame and anchorage design, forced entry resistant windows can resist the threat severity level II. With specially constructed grille or shutter enhancements, window openings can resist the threat severity levels III and IV. Refer to Table 5-14 through Table 5-20 for evaluating penetration delay times for existing windows. If existing window types are not in the tables, assume they offer no protection against attempted forced entry. Where existing windows do not provide adequate penetration delay times, they must be upgraded; replaced; or, because forced entry resistant window enhancements are costly, eliminated. Removal of existing windows will provide enhanced penetration delay time if the retrofit is accomplished properly. The most straightforward method is to seal the window opening with the same construction used in the wall where it is mounted.

Do not design man-passable window openings in defense layers where the threat severity level V applies. Also consider the placement of windows in relation to doors. Even a small window in or next to a door could allow an aggressor to reach through and unlock the door. Use obscured glazing materials or blinds, shutters, or drapes to eliminate asset visibility.

5-6.8 Utility Openings.

In conventional building designs, utility openings, manholes, tunnels, HVAC ducts, filters, and equipment access panels with openings greater than a man-passable 96 square inches (619 cm^2) provide aggressors with fast ingress and egress routes and provide no penetration delay time. Such openings must be eliminated, or their penetration delay times increased significantly to provide a consistent level of delay for a defense layer.

Methods for hardening man-passable utility openings are described in Paragraph 5-5.9.

CHAPTER 6 PROTECTED AREAS

6-1 INTRODUCTION.

Protected Areas contain the assets; their perimeters are the innermost defense layer and the last layer to provide delay to the aggressors' attempt to reach the assets. Paragraph 6-2 identifies protected asset types and the type of structure to be used to protect them. Construction design requirements for each type of structure is either covered in detail in this UFC; or, when other UFCs or DoD documents exist that contain those requirements, they are summarized, and references provided for the other documents. Paragraphs 6-3 through 6-11 provide the design requirements for structures not covered in other documents.

This UFC does not supersede any of the guidance in other regulatory publications. This UFC is intended to summarize the construction requirements in those documents and provide guidance if additional construction measures are required to protect the assets. If there are any inconsistencies between this UFC and any of the applicable references, the most stringent requirements will control.

6-2 PROTECTED ASSET TYPES.

The following asset types are those most likely to be identified as forced entry targets. Where an asset is identified in the design criteria that is not listed here, use the prescriptive protection requirements from the DoD regulatory documents that govern that asset.

6-2.1 High-Risk Personnel.

High-Risk Personnel (HRP) are DoD personnel who are likely to be terrorist or criminal targets based on their grade, assignment, symbolic value, criticality, and threat and vulnerability assessment. DoDI O-2000.22 defines High Risk Billets and HRP levels; assigns responsibilities; and establishes policy, processes, and procedures for the designation and protection of DoD HRP.

The project design criteria will identify if there are requirements for the protection of HRP including any need for safe havens. UFC 4-010-03 contains the minimum design requirements for the protection of HRP. UFC 4-023-10 contains the design requirements for safe havens.

6-2.2 Classified Information and Material.

The protection of classified information, which is governed by DoDM 5200.01, Volume 3 requires that classified information be secured under conditions adequate to prevent access by unauthorized persons. The storage requirements in DoDM 5200.01 are the same for all classification levels. Classified information and materials can be stored in General Services Agency (GSA)-approved storage containers, secure rooms, or vaults. For service specific regulatory requirements refer to AFI 31-101, AFI 16-1404, AR 380-5, and SECNAVINST M-5510.36.

(See Paragraph 6-11 for Class 5 GSA Storage Cabinets, Paragraph 6-3 for Secure Room design, and Paragraph 6-7 for Class A Vault design.)

6-2.3 Sensitive Compartmented Information.

Sensitive Compartmented Information is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal control systems. The handling and storage of Sensitive Compartmented Information must be confined to a Sensitive Compartmented Information Facility (SCIF). Physical security standards for the construction and protection of SCIFs is governed by DoDM 5105.21, Volume 2.

Use the physical design requirements in UFC 4-010-05 as the minimum requirements for construction of a SCIF.

6-2.4 Special Access Program Information and Equipment.

A Special Access Program is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. Physical security standards for the construction and protection of a Special Access Program Facility (SAPF) is governed by DoDM 5205.07, Volume 3.

Use the physical design requirements in UFC 4-010-05 as the minimum requirements for construction of a SAPF.

6-2.5 Communications Security (COMSEC) Materials.

COMSEC materials are used to secure or authenticate sensitive telecommunications. The protection of COMSEC materials is governed by DoDI 8523.01. COMSEC materials can be stored in security containers, secure rooms, or vaults in accordance with DoDM 5200.01 to the appropriate classification level.

(See Paragraph 6-11 for Class 5 GSA Storage Cabinets, Paragraph 6-3 for Secure Room design, and Paragraph 6-7 for Class A Vault design.)

6-2.6 Arms, Ammunition, and Explosives.

Security of AA&E is governed by DoD 5100.76-M. Storage requirements include security containers, arms rooms, modular vaults, or magazines. Classified AA&E are stored in accordance with DoDM 5200.01. For service specific regulatory requirements refer to AFI 31-101, AR 190-11, MCO 5530.14, and OPNAVINST 5530.13.

UFC 4-215-01 contains minimum design requirements for armories and arms rooms. For forced entry protection of AA&E, use design requirements in Paragraph 6-10.

6-2.7 Chemical Agents.

Chemical weapons storage is governed by DoDI 5210.65. In general, chemical agents are stored within Chemical Exclusion Areas in magazines or rooms constructed to vault standards and with an IDS. The Chemical Exclusion Area needs to be fenced with a perimeter IDS. Research and development level quantities of chemical agents can be stored in security containers within vaults or secure rooms. Classified agents are stored in accordance with DoDM 5200.01. AR 190-59 provides additional Army guidance.

For magazines to store chemical weapons, use the design requirements in UFC 4-420-01. For forced entry protection of research and development level quantities of chemical agents, use the design requirements in Paragraph 6-7.

6-2.8 Biological Agents.

Biological agent security is governed by DoDI 5210.88. That instruction requires agents to be stored in secure containers, including refrigerators, freezers, or other approved storage devices secured with GSA-approved locking devices located within Biological Restricted Areas. Those Biological Restricted Areas must be equipped with an IDS, at least two access control devices, and the entrance must be under constant surveillance.

For forced entry protection of biological agents, use the design requirements in Paragraph 6-7.

6-2.9 Nuclear Weapons.

Nuclear weapons physical security is governed by DoDD 5210.41/AFMAN 31-108. The weapons are stored similarly to chemical weapons within fenced weapons storage areas with a perimeter IDS. Storage is in magazines or rooms constructed to vault standards and with IDS.

6-2.10 Controlled Substances.

Controlled substance storage is governed by 21 CFR 1301.72 for all DoD components except for the Army. Army storage of controlled substances is governed by AR 190-51. In all cases, small quantities of controlled substances can be stored in safes or security containers as described in Paragraph 6-11. Greater quantities of controlled substances need to be stored in vaults. Pharmacy construction standards are in AR 190-51 and AFI 31-101.

For forced entry protection of large quantities of controlled substances, use the design requirements in Paragraph 6-7.

6-2.11 Funds.

The security of DoD funds is governed by DoDR 7000.14. Storage of funds in excess of $100,000 requires special construction for rooms in which funds storage containers are stored. Requirements for the Air Force are reflected in AFI 31-101.

For forced entry protection of funds in excess of $100,000, use the design requirements in Paragraph 6-4.

6-3 SECURE ROOMS.

Secure rooms are options for the storage of classified information and lower levels of COMSEC materials. Secure room construction can also be used for the storage of sensitive items such as funds, and small quantities of controlled substances; however, a secure room cannot be used to simultaneously store both classified information and sensitive items. Their construction is governed by DoDM 5200.01, Volume 3, which includes requirements for all the building elements associated with the perimeter of the room. A secure room may require an IDS if the area is not occupied on a twenty four-hour/seven-day basis; consult with facility security personnel for guidance.

The following paragraphs contain the minimum design requirements for a secure room; they provide little resistance to forced entry. If the secure room requires resistance to forced entry, use construction components from Chapter 5.

6-3.1 Walls, Floor, and Roof.

The walls, floor, and roof construction of secure rooms must be of permanent construction materials such as plaster, GWB, metal panels, hardboard, wood, plywood, or other materials offering resistance to, and evidence of, unauthorized entry into the area. Walls must be extended from the true floor to the true ceiling; and, if not, attached with permanent construction materials, mesh, or 18-gauge (1.2 mm) expanded steel screen.

6-3.2 Ceiling.

The ceiling must be constructed of plaster, GWB, hardboard or other acceptable material.

6-3.3 Door and Frame.

All doors in the secure room perimeter must be substantially constructed of wood or metal. The hinge pins of outswing doors must be peened, brazed, or spot-welded to prevent removal.

6-3.4 Locks.

The access door must be equipped with a built-in GSA-approved combination lock meeting FS FF-L-2740. Emergency exit doors should not have any external hardware installed.

6-3.5 Windows.

Windows that are less than 18 feet above the ground measured from the bottom of the window or are easily accessible by means of objects placed beneath the windows, must be constructed from or covered with materials that will provide protection from forced entry. The protection provided to the windows must provide the same penetration delay time as the contiguous walls.

Secure rooms which are located within a controlled compound or equivalent may eliminate the requirement for forced entry protection if the windows are made inoperable either by permanently sealing them or equipping them on the inside with a locking mechanism and they are covered by an IDS (either independently or by motion detection sensors within the area). This must be approved by the secure room's Security Manager.

6-4 FUNDS STORAGE ROOMS.

A funds storage room is a space specifically selected for containing a funds storage container during non-duty hours. The following construction requirements apply.

6-4.1 Walls, Floors, and Ceilings.

Walls, floors, and ceilings must be constructed or reinforced to provide protection equal to or greater than that of doors and windows. Effectively, most permanent construction will provide protection equal to or greater than that provided by the required windows and doors. Consider any concrete or masonry construction to be at least equivalent. Lightweight construction such as Exterior Insulating Finishing System may not provide equivalent protection, however. Add 5/16-inch expanded metal mesh to at least the walls of such construction. Add it to the floors and ceilings as well if they are constructed of something other than concrete.

6-4.2 Doors.

Doors should be constructed of 1-3/4 inch (44 mm) solid or laminated wood with US 12-gauge (2.7 mm) steel plate on the outside face; or standard 1-3/4 inch (44 mm) hollow metal, industrial type construction with minimum US 14-gauge (1.9 mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches maximum on center. A class 5 steel vault door with a changeable combination may be used instead of other doors and locks.

6-4.3 Door Frames and Hardware.

Door bucks, frames, and keepers should be rigidly anchored and provided with anti-spread space filler reinforcement to prevent disengagement of the lock bolt by prying or jacking the door frame. Also, the frames and locks for both interior and exterior doors should be designed and installed to prevent removal of the frame which faces the built-in locking mechanism. Frames should also be designed to prevent spreading sufficiently to disengage the lock bolt from outside the protected room when the door is closed and locked. Construction requirements for door frames and thresholds must be exacting as those for the door. For example, where metal doors are used, the frame and thresholds must also be metal.

When choosing the proper type of hinge for secure area doors, apply the following criteria:

- The hinge must be strong enough to withstand the rigors of constant use and the unusual weight of the door.
- Hinges should have fixed pins.
- Exposed hinges should be peened, or spot welded, or otherwise protected to prevent removal.
- Hinge mounting screws should not be exposed to the outside unless they are spot welded or peened to prevent removal.

6-4.4 Windows and Other Openings.

Windows should be filled in and sealed with material comparable to that forming the adjacent walls and otherwise limited to the essential minimum. Windows, ducts, vents, or similar openings large enough to permit entry [96-square-inch (619 cm^2) or with a single rectangular dimension greater than 6 inches (150 mm)] must be equipped with bars or mesh of one of the types below. Bars and steel mesh should be securely embedded in the structure of the building or welded to a steel frame that will be securely attached to the wall with fastenings inaccessible from the exterior of the facility.

- 3/8 inch (10 mm) or larger hardened steel bars, if the vertical bars are no more than 4 inches (100 mm) apart with horizontal bars welded to the vertical bars so that the openings do not exceed 32 square inches (206 cm^2).
- High carbon manganese steel mesh [US Number 8-gauge (4.0 mm)] with 2-inch (50-mm) diamond grid. (US Number 6-gauge (5.0 mm) steel mesh may be used if 8 gauge is unavailable.)

6-4.5 Security Lighting.

Interior and exterior security lighting is required for all government funds facilities and encouraged for all other funds facilities. The lighting must be bright enough to allow persons observing the structure or facility to recognize illegal acts. The following additional criteria apply.

- Locate switches for exterior lights so they are not accessible to unauthorized persons.
- Motion sensor lights may be installed to save energy.

Refer to UFC 3-530-01 for security lighting designs.

6-4.6 Locks and Keys.

Equip doors used for entry to funds storage rooms with, as a minimum, key actuated deadbolt locks with at least a 1-inch (25-mm) throw.

6-4.7 Intrusion Detection Systems.

AFI 31-101 requires accounting and finance offices and facilities storing $100,000 or more to have an IDS.

6-5 SECURE STORAGE STRUCTURES.

Army Regulation 190-51 identifies a class of storage facilities referred to as secure storage structures. They may be used to store a variety of asset types but cannot be used to store classified information or AA&E. The regulation has requirements for all building components in the perimeter of the space. The requirements vary by risk level as determined using DA Pamphlet 190-51.

6-5.1 Walls.

6-5.1.1 Risk Level I.

Walls should be constructed of at least 1/2–inch (13-mm) plywood, 1–inch (25-mm) tongue–in–groove wall boards, or 26–gauge (0.45 mm) steel siding.

6-5.1.2 Risk Level II.

Walls should be constructed of 4–inch (100-mm) minimum thickness brick and stud construction or of 8–inch (200-mm) minimum thickness concrete masonry (unreinforced). Alternatively, walls may be designed to provide delay equal to or greater than the actual response time.

6-5.1.3 Risk Level III.

Walls should be constructed of 8–inch (200-mm) minimum thickness core-filled concrete masonry reinforced with #6 (19 mm) reinforcing bars at 4 inches OC vertically and 8 inches (200 mm) OC horizontally, or 4–inch (100-mm) minimum thickness concrete reinforced with #5 (16 mm) reinforcing bars at 5 inches (125 mm) OC EW. Alternatively, walls may be designed to provide delay equal to or greater than the actual response time.

6-5.2 Floor and Ceiling.

The following requirements do not apply to slab on grade floors. No special requirements apply for such floors.

6-5.2.1 Risk Level I.

Floors and ceilings should be constructed of at least 1/2–inch (13 mm) plywood, 1–inch (25-mm) tongue–in–groove wall boards, or 24–gauge (0.6 mm) steel deck.

6-5.2.2 Risk Level II.

Floors and ceilings should be constructed as for Risk Level I with the addition of 5/16–inch (8 mm) expanded metal mesh or 10–gauge (3.4 mm) 6 inch by 6 inch (150 mm by 150 mm) woven wire fabric. Alternatively, floors and ceilings may be designed to provide delay equal to or greater than the actual response time.

6-5.2.3 Risk Level III.

Floors and ceilings should be constructed of 4–inch (100 mm) minimum thickness concrete reinforced with #5 (16 mm) reinforcing bars at 5 inches OC EW. Alternatively, floors and ceilings may be designed to provide delay equal to or greater than the actual response time.

6-5.3 Doors.

6-5.3.1 Risk Level I.

Doors should be a minimum of 1 3/4–inch (44 mm) thick solid core wood or hollow steel. Hollow steel doors will be industrial type construction with at least 20–gauge (0.88 mm) skin plate thickness and will be internally reinforced with continuously spaced stiffeners.

Door frames should be constructed of a minimum of 18–gauge steel. Doors with locking systems exposed to the outside should be kept to the absolute minimum number needed based on operational considerations. In addition, the doors should meet the following installation requirements:

- Door hinge mounting screws should not be exposed to the exterior of the facility. If screws are exposed, they should be spot welded, peened, covered, or filled with material in a way to prevent easy removal. Nails should not be used to mount hinges or any other door hardware.
- Door hinge pins should not be exposed to the exterior of the facility. If they are, they should be spot welded, covered, filled, or otherwise secured to prevent easy removal.
- Doors secured from the inside should be secured with a deadbolt locking device, crossbar, or similar locking device resistant to jimmying and manipulation from the outside. Latch style door locks should not be used.

6-5.3.2 Risk Level II.

Doors should be a minimum of 16–gauge (1.6 mm) hollow steel construction with a minimum of frame construction of 16–gauge (1.6 mm) steel. Installation requirements for Risk Level I also apply. Alternatively, doors or pairs of doors may provide delay time equal to or greater than the actual response time.

6-5.3.3 Risk Level III.

Doors should be a minimum of 1 3/4–inch (44 mm) solid core wood with wood block cores and 12–gauge (2.7 mm) minimum thickness steel plate on both sides or doors should be 12–gauge (2.7 mm) minimum thickness hollow steel doors reinforced with vertical stiffeners at 6 inches (150 mm) on center. Door frames should be constructed of 16–gauge (1.6 mm) steel minimum and be grouted full. Alternatively, doors or pairs of doors may provide delay time equal to or greater than the actual response time.

6-5.4 Windows.

The following apply to all first-floor openings, except doors, in excess of 96 square inches (619 cm^2) that are located less than 12 feet (3.7 m) from the ground level and to similar openings above the first floor which can be reached from an elevated portion of the structure or from an adjacent structure which provides ground level access. Long narrow openings with the shortest dimension measuring less than 6 inches (150 mm) are exempt from these requirements. If window air conditioning is used, bar, mesh, or fence fabric assemblies should completely enclose the air–conditioning unit protruding from the building or storage room exterior. If the window air conditioner is mounted through the wall, measures should be taken to ensure that it cannot be removed from the outside.

6-5.4.1 Risk Level I.

Operable windows should have adequate individual locking devices. Windows should also be covered with 1/2–inch (13 mm) diameter bars spaced at 6 inches (150 mm) on center each way, with 5/16–inch (8 mm) expanded metal mesh, or with 9–gauge (3.8 mm) chain link fabric.

6-5.4.2 Risk Level II.

Windows should be inoperable. They should be covered with bars or mesh as for Risk Level I and the glass should be covered with 4–mil (0.1 mm) fragment retention film or they should have 1/2–inch (13 mm) thick laminated glass or plastic security glazing. Alternatively, windows may provide delay time equal to or greater than the actual response time.

6-5.4.3 Risk Level III.

Windows should be inoperable, and they should be covered with bars or mesh as for Risk Level I and have 1/2–inch (13 mm) thick laminated glass or plastic security glazing. Alternatively, windows may provide delay time equal to or greater than the actual response time.

6-6 VAULTS.

Federal Standard 832 provides requirements for three classes of vaults for the storage of classified material and equipment: A, B, and C.

- Class A vaults provide penetration delay against threat severity levels II to IV. (See Paragraph 6-7 for the minimum construction requirements for Class A vaults.)
- Class B vaults provide penetration delay against threat severity levels II and III. Construction of a Class B vault must be in accordance with FS AA-V-2737. The door and frame of a Class B vault must conform to Federal Specification AA-D-600.
- Class C vaults offer no protection against a forced entry but may be used where unique structural circumstances do not permit concrete wall construction. They cannot be used as a defense layer unless substantially upgraded with designs from Chapter 5. (See Paragraph 6-8 for the minimum construction requirements for Class C vaults.)
- A lightweight, portable modular vault equivalent to a Class B vault that meets FS AA-V-2737 may also be used to store classified material and equipment. (See Paragraph 6-9 for modular vault design requirements).

DoD instructions on the protection of classified information and weapons systems require that vaults used to protect these assets must be cast-in-place reinforced concrete with a GSA-approved vault door that meets the requirements of FS AA-D-600. As alternatives within existing buildings where the use cast-in-place reinforced concrete is not structurally feasible, either a Class C vault or a GSA-approved modular vault can be used in place of a reinforced concrete structure.

6-7 CLASS A VAULTS.

This paragraph contains the minimum construction requirements for Class A vaults. (See Table 6-1 for penetration delay times provided by Class A vaults.)

Table 6-1 Penetration Ratings for Class A Vaults

MINIMUM CONSTRUCTION REQUIREMENT		MINIMUM PENETRATION DELAY TIME (MINUTES)			
		II	III	IV	V
Walls	8-inch (200-mm) Reinforced Concrete	(a)	(a)	12	<1
Floors	8-inch (200-mm) Reinforced Concrete	(a)	(a)	18 (b)	<1
Roof / Ceiling	8-inch (200-mm) Reinforced Concrete	(a)	(a)	10 (c)	<1
Door / Frame	Class 5 (FS AA-D-600)	(a)	10	2	<1

(a) Not practical to attack at this threat severity level.
(b) Penetration delay time is for an upward attack for other than floors on grade. Floors on grade not practical to attack.
(c) Penetration delay time is for a downward attack.

6-7.1 Walls.

Use 8-inch (200-mm) thick reinforced concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa). Reinforce concrete with 5/8-inch (16-mm) reinforcing bars, 6 inches (150 mm) on center each way, staggered each frame. Extend the reinforcement to the underside of the roof or ceiling slab above. Tie wall reinforcement into floor and ceiling or roof. When vault walls are part of the exterior walls, set the vault wall back from the exterior part of the exterior wall to allow 4 inches (100mm) for the normal wall facing to cover the vault wall.

6-7.2 Floor.

Use 8-inch (200-mm) thick reinforced concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa). Reinforce concrete with 5/8-inch (16-mm) reinforcing bars, 6 inches (150 mm) on center each way, staggered each frame. These requirements do not apply to slab on grade floors because these are not practical to attack; no special requirements apply for such floors.

6-7.3 Roof and Ceiling.

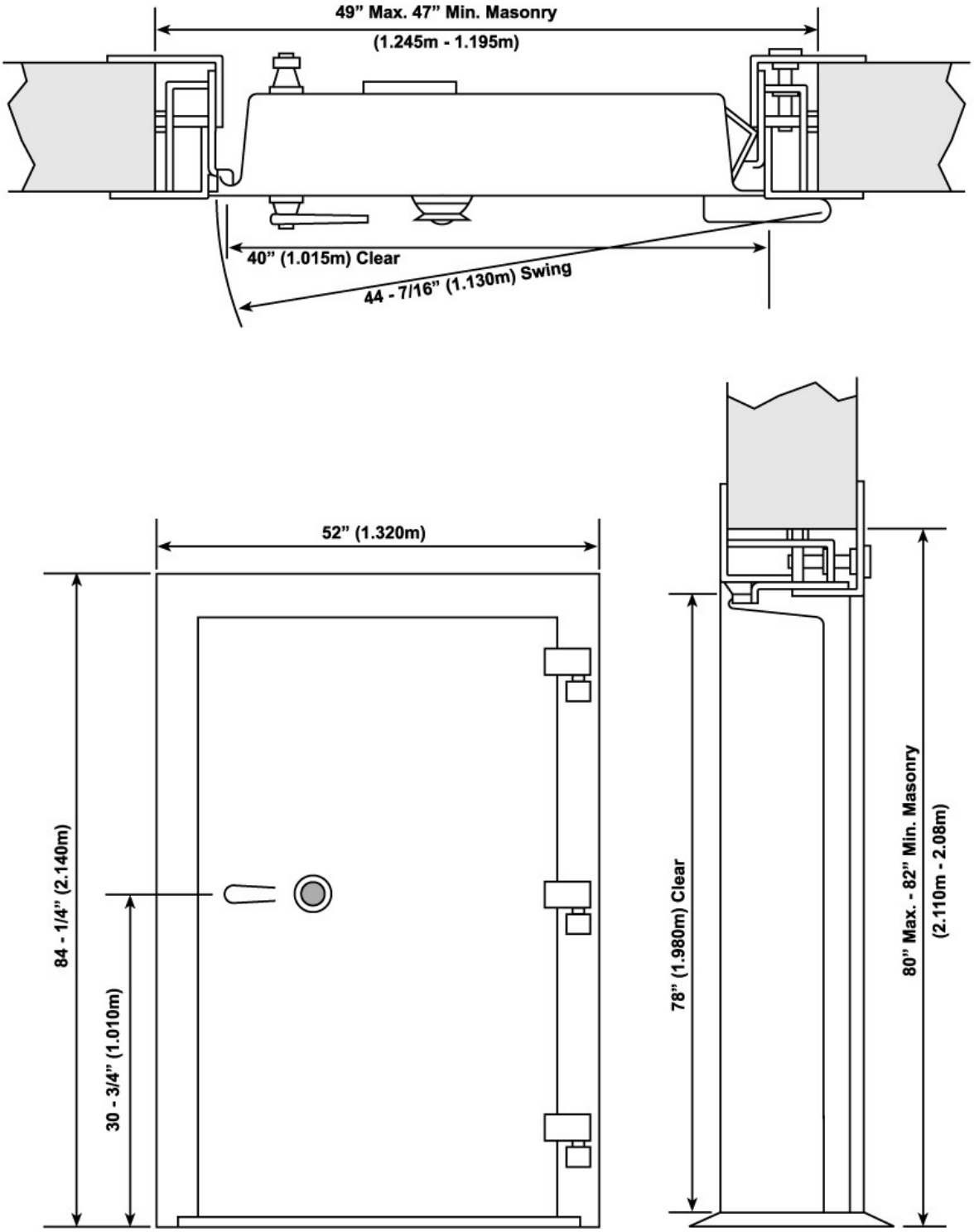
Use 8-inch (200-mm) thick reinforced concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa). Reinforce concrete with 5/8-inch (16-mm) reinforcing bars, 6 inches (150 mm) on center each way, staggered each frame.

6-7.4 Door and Frame.

Since vault doors are more vulnerable to attack than the vault enclosure itself, there should be only one entrance into a vault area. When a vault exceeds 1,000 square feet (93 m^2) in floor space, or will have more than eight occupants, it should have a minimum of two exits for safety purposes. When more than one entrance is required, each must be equipped with an approved vault door with only one used for normal access. Where continued use of an entry barrier is required at a vault door, a day gate may be provided for the primary entrance to preclude undue wear of the door during operating hours.

Vault doors, frames, and locks must conform to FS AA-D-600. Doors other than those secured with locks meeting FF-L-2740 must be secured from the inside with deadbolt emergency egress hardware, a deadbolt, or a rigid wood or metal bar that extends across the width of the door. Figure 6-1 shows the dimensional requirements for a Class 5 vault door.

Figure 6-1 Class 5 Vault Door



6-7.5 Locks.

Use vault door locks that meet the requirements of FS FF-L-2740.

6-7.6 Miscellaneous Openings.

Install barriers in any miscellaneous openings, open ducts, pipes, register, sewers in excess of 96 square inches (619 cm^2) in area and over 6 inches (150 mm) in its smallest dimension. Acceptable barriers are 9 gauge expanded metal mesh, or rigid (steel) bars at least 1/2-inch (13-mm) in diameter, welded vertically and horizontally 6 inches (150 mm) on center. Securely fasten the rigid metal bars at both ends to preclude removal. Use crossbars to prevent spreading of the bars.

6-8 CLASS C VAULTS.

Class C vaults may be used in existing buildings where unique structural circumstances do not permit construction of a Class A concrete vault.

6-8.1 Walls.

Use 1/4-inch (6-mm) thick steel alloy-type metal plates having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor or ceiling of reinforced concrete, they must be firmly affixed to a depth of one-half the thickness of the floor and ceiling.

6-8.2 Floor and Ceiling.

If the floor and/or ceiling construction is less than six inches of reinforced concrete, use a steel liner with the same characteristics as the walls to form the floor and ceiling of the vault. Weld seams together where the steel plates meet horizontally and vertically.

6-8.3 Door and Frame.

Use a vault door and frame that conforms to F S AA-D-600.

6-8.4 Locks.

Use vault door locks that meet the requirements of FS FF-L-2740.

6-8.5 Miscellaneous Openings.

Equip any miscellaneous openings, open ducts, pipes, registers, sewers in excess of 96 square inches (619 cm^2) in area and over 6 inches (150 mm) in its smallest dimension with barriers. Acceptable barriers are 9-gauge (3.8-mm) expanded metal mesh, or rigid metal (steel) bars at least 1/2 inch (13 mm) in diameter, welded vertically and horizontally 6 inches (150 mm) on center. Securely fasten the rigid metal bars at both ends to preclude removal. Use crossbars to prevent spreading of the bars.

6-9 MODULAR VAULTS.

Modular vaults provide a minimum of 15 minutes of forced entry resistance against a multilevel tool attack up to threat severity level III. Modular vaults provide only minimal delay to threat severity levels IV and V.

An advantage of modular construction is that a modular vault can be reconfigured or disassembled and relocated as needed.

6-9.1 Advantages of Modular Vaults.

Advantages of using modular vaults instead of poured in place reinforced concrete vaults include:

- Ability to construct a new vault in a few hours rather than days or months.
- Ability to construct a new vault without the use of concrete forms and resulting construction debris.
- Lighter weight (up to 70 percent less) depending on the class of vault.
- Lower cost (up to 50 percent less) depending on the extent of structural modifications that would be required.
- Flexibility for installing a vault in or removing a vault from an existing operational building (depending on the extent of structural modifications required).
- Reduction in space required because the walls are up to 70 percent thinner.

6-9.2 Construction.

Vaults are made of modular panels, which are assembled to form a six-sided structure. The floor may be the concrete slab of the building, or it may consist of modular panels. Figure 6-2 shows a representative configuration of a modular vault.

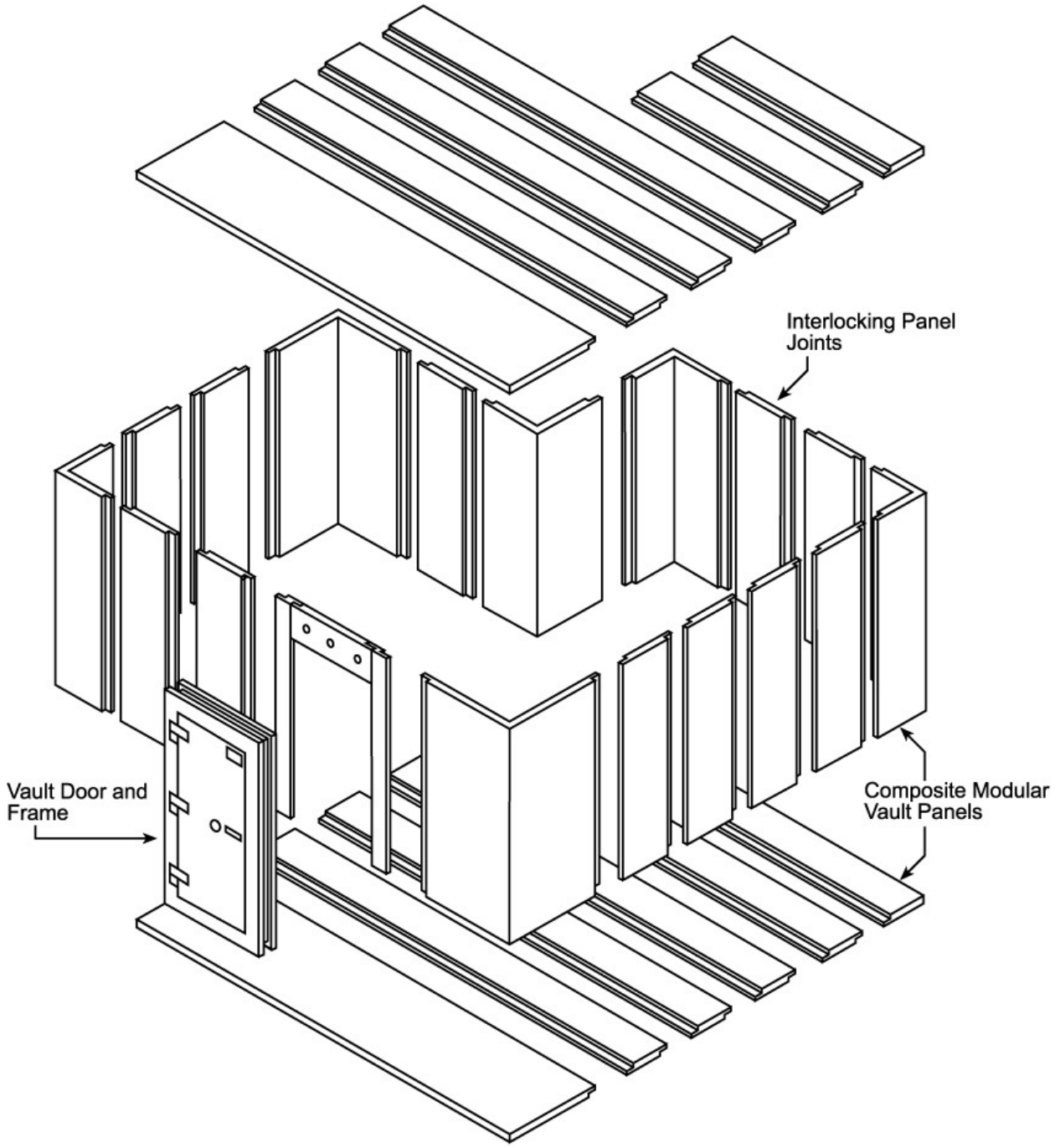
FS AA-V-2737 covers panels that may be assembled to form a GSA-approved modular vault. The vault must use a Class 5 GSA-approved vault door meeting requirements of FS AA-D-600.

Modular vault panels are either lightweight (less than 30 pounds per square foot) or heavyweight (unlimited weight). Lightweight panels are laminated of various materials which together provide the forced entry resistance time of at least 15 minutes against threat severity level IV. Heavyweight panels are typically made of concrete.

6-9.3 Availability.

Modular vaults are available from a variety of American manufacturers. Additional information is available from the Naval Facilities Engineering and Expeditionary Warfare Center (EXWC) Code CI8 Port Hueneme, CA, 93043 and from GSA.

Figure 6-2 Simple Modular Vault Panel and Door Arrangement



6-10 ARMS, AMMUNITION, AND EXPLOSIVES AREAS.

AA&E can be stored in magazines, arms rooms, or vaults depending on the risk category and quantities and use of the AA&E.

Table 6-2 lists AA&E Risk Categories and their application.

- All Risk Category I AA&E must be stored in standard magazines.
- AA&E Risk Categories II through IV must be stored in a structure with a minimum forced entry resistance of 10 minutes against threat severity level III including arms rooms or permanent and modular vaults with a Class 5 approved vault door.

Table 6-2 Security Risk Categories for AA&E (DODM 5100.76)

CATEGORY	WEAPONS	AMMUNITION & EXPLOSIVES
I	Nonnuclear man-portable missiles and rockets in a ready to fire configuration; for example, Redeye, Stinger, Dragon, Javelin, light antitank weapon (66mm), shoulder–launched multi–purpose assault weapon rocket (83 mm), and AT–4 anti–armor launcher and cartridge (84 mm). Also included are the tube–launched, optically tracked, wire–guided missile (TOW) weapon and the Hellfire missile.	Explosive complete rounds for Category I missiles and rockets
II	Light automatic weapons up to and including 0.50 caliber (13 mm), M16A2 rifle, M4 rifle, Squad Automatic Weapon, M60 machine gun, and 40mm MK 19 grenade launcher. Silencers, mufflers and noise suppression devices.	High explosive hand or rifle grenades and white phosphorous. Mines, antitank or antipersonnel with an unpacked weight of 50 pounds (23 kg) or less. Explosives used in demolition operations, C-4, military dynamite and TNT with an unpacked weight of 100 pounds (45 kg) or less. Critical binary munitions components containing “DF “and “QL” when stored separately from each other and from the binary chemical munition bodies in which they are intended to be employed.

CATEGORY	WEAPONS	AMMUNITION & EXPLOSIVES
III	Launch tube and grip stock for the Stinger missile. Launch tube, sight assembly and grip stock for Redeye missiles. Tracker for the Dragon missile. Mortar tubes up to and including 3.2 inch (81 mm). Grenade launchers. Rocket and missile launchers (unpacked weight of 100 pounds (45 kg) or less). Flame throwers. Launcher, missile guidance, or the optical sight for TOW.	Ammunition, .50 caliber (12.7 mm) and larger, with explosive filled projectile (unpacked weight of 100 pounds or less each). Grenades, incendiary, and fuses for high explosive grenades. Blasting caps. Supplementary charges (uninstalled or installed in projectiles in a manner allowing easy removal without special tools or equipment). Bulk explosives. Detonating cord.
IV	Shoulder-fired weapons other than grenade launchers, not fully automatic. Handguns. Recoilless rifles up to and including 4.2 inches (106 mm).	Ammunition with non–explosive projectile (unpacked weight of 100 pounds or less each). Fuses, except for those in Category III. Grenades, illumination, smoke, and tear gas (CS)/chloroacetophenone (CN) (tear–producing). Incendiary destroyers. Riot control agents, 100-pound package or less. Ammunition for weapons in Category III.

6-10.1 Magazines.

Refer to UFC 4-420-01 for construction requirements for ammunition and explosives storage magazines.

6-10.2 Arms Rooms.

Arms rooms are governed by DoDM 5100.76; they are similar in construction to vaults. They are treated as six-sided rooms, but there are door options in addition to vault doors. Unlike vaults, however, arms rooms must both meet minimum construction requirements and provide a minimum of 10 minutes of forced entry resistance against threat severity level III.

- Army arms rooms are constructed according to the requirements of AR 190-11; these are facilities, similar in function to the weapons storage spaces of armories, with very limited maintenance and repair facilities.
- Air Force arms rooms are governed by AFI 31-101 and AFMAN 32-1084. Air Force weapons repair and maintenance facilities are normally located in a Combat Arms Facility.
- Navy arms rooms must comply with OPNAVINST 5530.13.
- Marine Corps arms rooms must comply with MCO 5530.14.

6-10.3 General.

Permanently constructed arms rooms are normally cast-in-place concrete. Precast concrete of similar construction may be used, but it would have to be tested to ensure that the joints and connections meet the required delay time. Alternatively, precast panels meeting the requirements in Paragraph 6-10.4, and in which there are cast-in-place segments between panels, may be allowed if the continuity of reinforcement between panels and between floors or foundations and roofs or ceilings is maintained. In all cases, the construction in the paragraph below constitutes minimum requirements.

Structural requirements may require greater thicknesses and reinforcement. Use concrete in walls, floors, ceilings, and roofs with 3000 psi (20.7 MPa) minimum compressive strength. Use ASTM A615, Grade 60 for reinforcing bars and comply with ASTM A1064 for welded wire fabric. Reinforcement should be installed in accordance with ACI 318. Note that the reinforcing bars outside the United States may not be of the same dimensions or yield strengths as those in ASTM A615 and ASTM A1064. In those cases, use the closest greater diameter and tensile strength.

6-10.4 Walls.

Use a minimum of 8-inches (200 mm) thick concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa) reinforced with a minimum of #4 (1/2-inch, 13 mm) reinforcing bars in both directions on each face, spaced at 9 inches (225 mm), and staggered each face such that they form a projected grid approximately 4-1/2 inches (115 mm) square. Thinner cross sections can be used if heavier reinforcing is selected. For example, a 6-inch (150-mm) cross section could be used if there are two layers of #5 (16-mm) reinforcing bar spaced at 4-1/2 inches (115 mm) each way. Tie reinforcement in walls into ceilings and floors.

6-10.5 Roofs and Ceilings.

For roofs and ceilings, use a minimum of 8-inches (200-mm) thick concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa) reinforced with a minimum of #4 (1/2-inch, 13-mm) reinforcing bars in both directions spaced such that they form a grid such that the areas of any openings between bars will not exceed 96 square inches (619 cm^2). If the ceiling or roof must be pan-joist construction, the thinnest part may not be less than 6-inches (150-mm) and the clear space between joists may not exceed 20-inches (500-mm).

6-10.6 Floors.

Floors, if on grade, must be a minimum of 6-inches (150 mm) thick reinforced concrete with a minimum 28-day compressive strength of 3,000 psi (20.7 MPa) reinforced with minimum of 6-inch x 6-inch (150-mm x 150-mm) W4 x W4 welded wire fabric. Alternatively, use a minimum of #4 (1/2-inch, 12.5 mm) reinforcing bars in both directions spaced such that they form a grid such that the areas of any openings between bars will not exceed 96 square inches (619 cm^2). Bar spacings in each direction of 10 inches (254 mm) would result in a clear area between bars less than the minimum area.

Where floors of arms rooms are ceilings of spaces below them, follow the ceiling standard.

6-10.7 Existing Wall, Ceiling, Roof, and Floor Reinforcement.

Where existing construction is not up to the standards above, use any of the reinforcing methods listed below. When any of these are applied, fasten them to the existing structure so that destruction of the existing and reinforcing materials is required to remove them.

- Steel bars: Use 3/8-inch (10 mm) steel bars, 4 inches (100 mm) apart with bars in one direction welded to the bars in the opposite direction so that the openings do not exceed 32 square inches (0.02 m2). Ends of the steel bars must be embedded securely in the structure of the building or welded to a steel frame securely fastened to the building.
- Steel landing mat: Use Marsten, Irving, or pierced steel planking.

- Expanded metal: Use 3/16-inch (5 mm) thick expanded metal with a maximum grid opening of 1 inch by 3 inches (25 mm by 75 mm) and weighing a minimum of 4.27 pounds per square foot (20.8 kg/m2).
- Steel plate: Use 1/4-inch (6.4 mm) steel plate.
- Steel mesh: Use Number 8–gauge (4.1 mm) high carbon manganese steel, or for existing facilities, number 6–gauge (4.1 mm) cold drawn steel wire with a grid of not more than 2 inches (50 mm) center to center. The number 6–gauge (4.1 mm) wire is not authorized for future upgrading.
- Sheet metal: For existing facilities, use 16–gauge (1.6 mm) steel sheets or plates securely fastened together. This material is not authorized for future upgrading.

6-10.8 Doors.

Only the GSA-approved Class 5 Armory Door provides the required 10 minutes of delay; therefore, only that door is allowed for new construction. The Class 5 Armory Door is specified using FS AA-D-600.

The following doors are authorized for existing construction by DoDM 5100.76:

- 1-3/4-inch (44 mm) solid or laminated wood with 12-gauge (2.7 mm) steel plate on the exterior face.
- 1-3/4-inch (44 mm) hollow metal, industrial type construction with minimum 14-gauge (1.9 mm) skin plate thickness, internally reinforce vertically with continuous steel stiffeners spaced 6-inches maximum on-center.
- Solid hardwood or laminated wood of at least 2 inches (50 mm) thickness with a 1/4-inch (6 mm) thick steel plate on the outside face.
- A door constructed with a 3/8-inch (10 mm) thick steel plate or combines thickness of outside and inside surfaces of at least 3/8-inch (10 mm) steel.

6-10.9 Door Frames and Hardware.

For doors other than the Class 5 Armory Doors, door bucks, frames, and keepers must be rigidly anchored and provided with anti-spread filler reinforcement to prevent disengagement of the lock bolt by prying or jacking of the door frame. Door frames must be designed and installed in a manner that prevents removal of the frame facing. Their construction requirements must be as exacting as those for the doors themselves. For example, where metal doors are used, the frame and thresholds must also be metal. Door hinges must be located on the inside and must be of the fixed-pin security type or equivalent. Figure 6-3, Figure 6-4, Figure 6-5, and Figure 6-6 show designs of acceptable hinge side protection.

Figure 6-3 Hinge Side Protection Using a Pin-in Socket

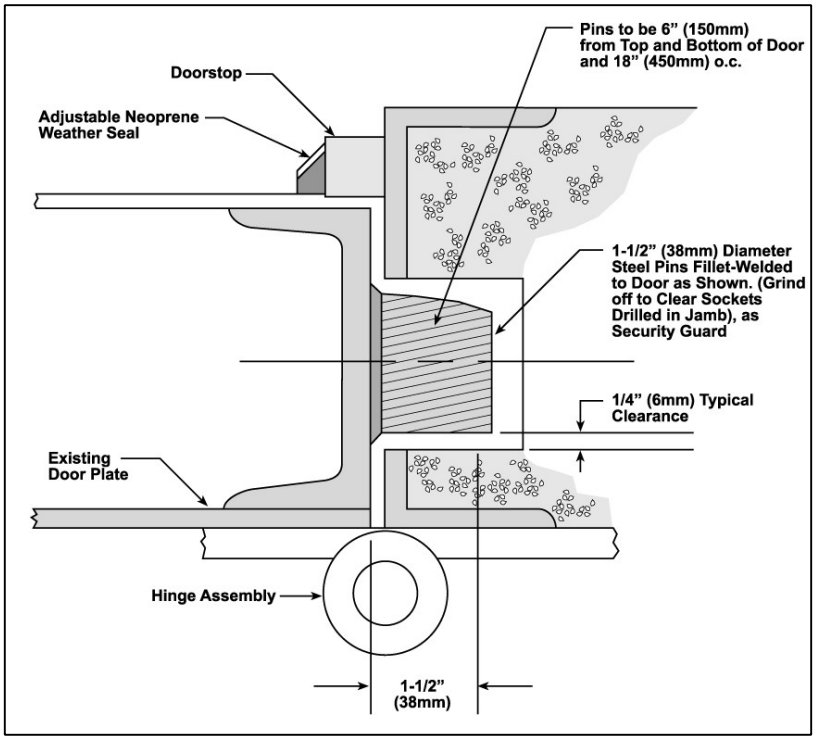


Figure 6-4 Hinge Side Protection Using a Forward Doorstop with Steel Angle

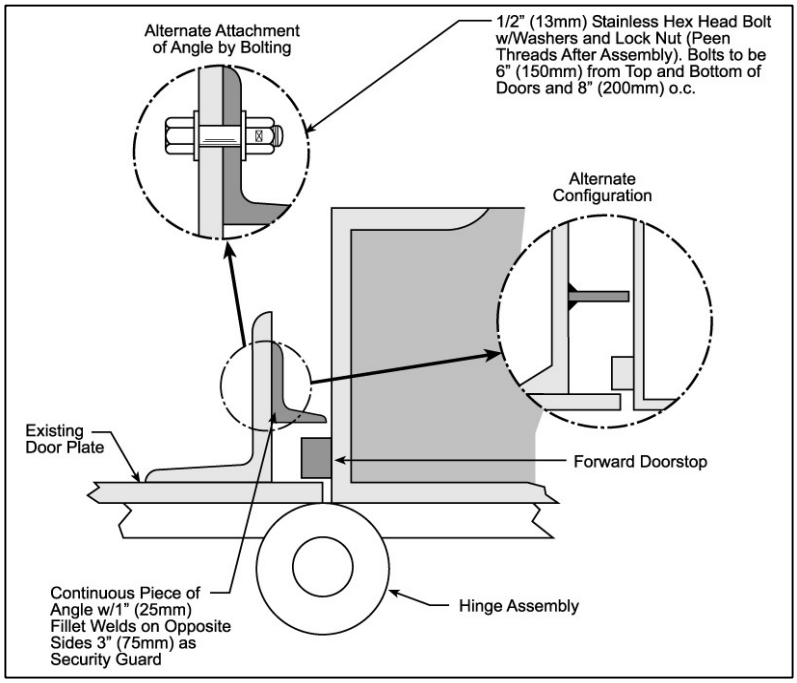


Figure 6-5 Hinge Side Protection Using an Angle Stop

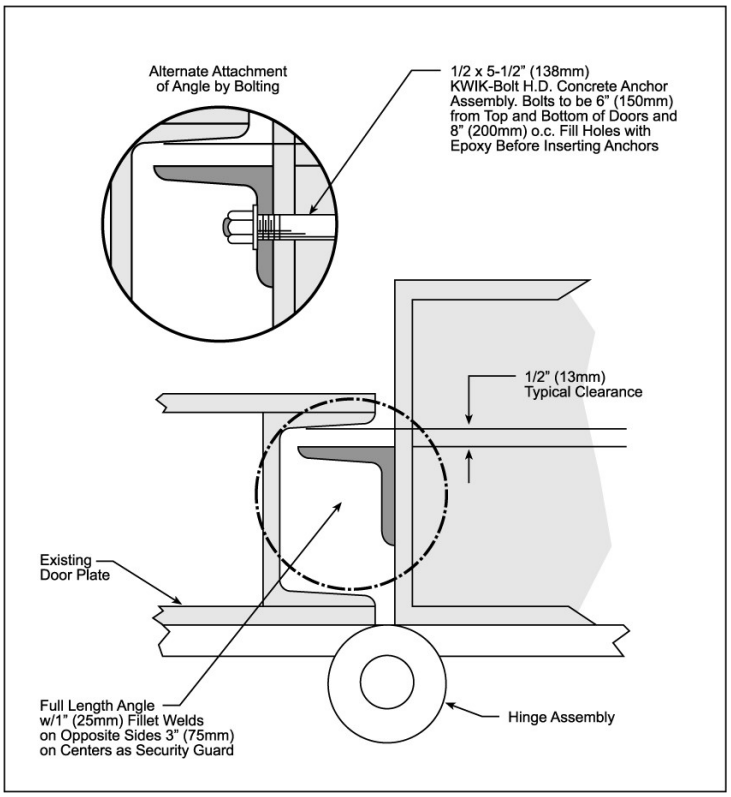
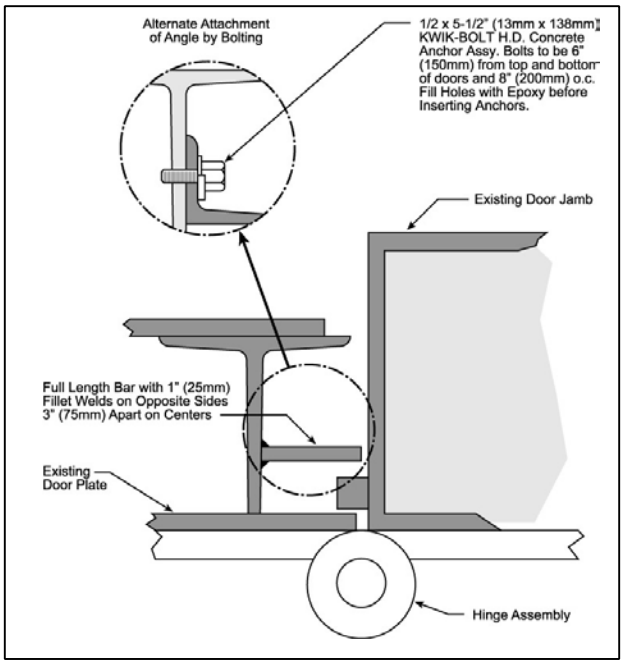


Figure 6-6 Hinge Side Protection Using a Bar Stop

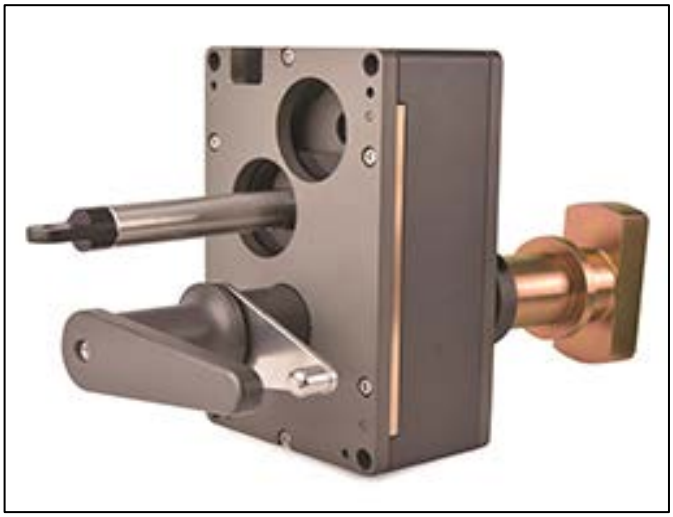


6-10.10 Locks.

Locks for Class 5 Armory Doors are covered in FS AA-D-600. They are combination locks that are listed in accordance with Group 1 of UL 768. Locks for new construction and upgrades of Category I and II AA&E areas must be the Internal Locking Device (See Figure 6-7 for all doors except for Class 5 Armory Doors.)

Figure 6-7 Internal Locking Devices

ILD Gen I



ILD Gen II

6-10.11 Miscellaneous Openings.

In general, windows and other openings must be kept to a minimum. Windows are not authorized for new construction for Army arms rooms. Where any openings are greater than 96 square inches (619 cm^2) with a least dimension greater than 6-inches (150 mm) one of the following can be used to secure them:

- Minimum 3/8-inch (10 mm) hardened steel rods with a maximum spacing of 4-inches (100 mm) and with horizontal bars attached to no openings exceed 32 square inches (0.02 square meters).
- Riveted steel grating weighing 13.2 lbs/square foot (64.4 kg/m^2) or welded steel grating weighing 8.1 lbs/square foot (39.6 kg/m^2) with 1 by 3/16-inch (25 by 5 mm) bearing bars.

6-10.12 Other Storage Options.

A vault that meets the requirements for arms rooms can be used to store all categories of Risk Category II, III and IV arms and ammunition depending on explosive safety restrictions. Modular vaults can also be used.

Security containers that meet the requirements of Federal Specification AA-F-363, Class 5, or Federal Specification AA-C-2859, can be used to store small quantities of Risk Category II, III and IV arms.

6-10.13 Other Requirements.

Unless a weapons storage site is continuously guarded, an IDS is required for Risk Category I and II AA&E storage areas. Refer to UFC 4-021-02 for IDS designs. Risk Category I and II AA&E must be fenced separately. Refer to UFC 4-022-03 for fencing and gate designs. Exterior lighting is required for Risk Category I and II AA&E only.

6-10.14 Retrofit of Existing Arms Rooms.

Existing facilities can be effectively upgraded to meet the AA&E storage requirement for ten minutes of penetration resistance against threat severity level III. To upgrade these facilities, reinforce walls, ceilings and floors as necessary using a layer of 3/4-inch (19-mm) plywood sandwiched between two layers of 10 gauge (3.4-mm) hot-rolled steel to provide about 6 minutes of additional penetration delay time. The penetration delay time can be increased by about five minutes with the addition of another wood and steel layer. This rule of thumb can be applied to the addition of more layers until the desired penetration delay time is reached. Penetration delay time for steel-plywood systems can be increased by changing the steel material to 9-gauge (3.8-mm) ASTM A1008, Class 2, high-strength, low-alloy steel. One layer of 3/4-inch (19-mm) plywood sandwiched between two layers of this steel will provide 14 minutes of penetration delay time. Adding layers of 90-pound (200-kg) gravel finish roofing paper between the plywood and steel further increases the penetration delay time to about 20 minutes. These times are added to the increased penetration delay time provided by preventing internal spalling of the concrete (approximately double the initial penetration delay time).

6-11 STORAGE CONTAINERS.

Class 5 storage containers are allowed as options for the storage of many of the assets that are governed by the regulatory documents described in Paragraph 6-2. They are not considered to be parts of facilities; however, they can provide resistance to forced entry at threat severity level II. Class 5 storage containers provide 10 man-minutes of delay against threat severity level II; they provide no delay against higher threat severity levels. See Figure 6-8 for storage container examples.

Storage containers must be approved by GSA. They are specified using one of the following Federal Specifications (FS) based on what is being stored inside them. The Federal Specifications include container construction and testing requirements as well as locking device specifications.

- FS AA-F-358, Filing Cabinet, Letter and Legal Size, Uninsulated, Security
- FS AA-F-363, Filing Cabinet, Security, Maps and Plans, General Filing and Storage
- FS AA-C-2859, Cabinet, Security, Weapons Storage
- FS AA-C-2786, Cabinet, Security, Information Processing System Storage, Class 5.

Figure 6-8 Storage Containers

FS AA-F-358 Filing Cabinet, Letter and Legal Size, Uninsulated, Security	FS AA-C-2859 Cabinet, Security, Weapons Storage

CHAPTER 7 EQUIPMENT AND SYSTEMS

7-1 INTRODUCTION.

This chapter contains information on systems that can be considered to supplement the barrier designs in Chapter 5 for high and very high levels of protection combined with threat severity levels IV and V.

7-2 DISPENSABLE BARRIER SYSTEMS.

Dispensable barriers are activated manually or automatically in response to attack. Such systems include sticky foam and cold smoke. Sticky foam is an aggressively tacky thermoplastic resin stored under pressure in canisters or wall panels. When punctured by tools or bullets, or when the system's detectors are tripped, the foam shoots out of the panels. The foam expands and adheres to whatever it contacts. Aggressors must be extricated from the foam with a solvent. The foam must also be cleaned off surfaces with the solvent. Because sticky foam may result in the death of the aggressor or anyone else who accidentally triggers it, apply it only where the use of deadly force is authorized. This system provides a minimum delay time of 15 minutes against motivated aggressors (according to the manufacturer). It is most effective when used in hallways. Cold smoke is a particulate material, which fills a room with a persistent dense cloud when activated. Aggressors cannot see in the cloud and therefore have difficulty locating assets. To be effective, both activated barrier systems must by sized for the volume of the protected space.

Dispensable barriers can, on command, stop or delay aggressors from accomplishing their objective. Several types are being developed and tested. This section identifies the major components of a dispensable barrier system and describes some of the attributes of dispensable materials. The information in this paragraph was developed by Sandia National Laboratories, Albuquerque, NM.

7-2.1 Typical Dispensable Barrier System.

A typical dispensable barrier system includes:

- A process for decision making to determine when the dispensable barrier is to be activated.
- Command and control hardware to implement this decision.
- The material that is deployed to physically deny access.
- The dispensing mechanism.
- A response force located on site.

7-2.2 Barrier Activation.

The dispensable barrier may be activated by a member of the response force, some form of intrusion sensing, or by the combined action of both the security force and sensors.

The major compromise is between assurance that activation can and will occur in an aggressor attack (reliability) and assurance that the probability of inadvertent activation is low (premature activation). Hardware design and effective operational procedures can reduce the probability of inadvertent activation to as low a value as required.

7-2.3 Command and Control Hardware.

The command and control hardware accepts the activation decision and operates the dispensing hardware. Command and control hardware stands between the decision mechanism and the dispensing hardware. Because the activation decision mechanism and the dispensing hardware may be separated by large distances, electromagnetic radiation, lightning, earthquakes, power surges, and other possible severe environments must be considered in the design. The command and control hardware improves personnel safety and assures that, if inadvertent activation occurs, authorized personnel in the area have time to exit.

7-2.4 Dispensable System.

7-2.4.1 Types of Dispensable Barriers.

Specific dispensable materials and associated dispensing hardware that are being developed and tested include:

- Rigid polyurethane foam.
- Stabilized aqueous foam.
- Obscurants smoke.
- Sticky thermoplastic foam.
- Various entanglement devices.
- Irritants.

7-2.4.2 Compact Storage and Rapid Expansion.

The dispensable material is normally stored in a compact form, and through a chemical or physical reaction, is expanded to provide additional delay. These properties that permit compact storage and rapid expansion make activated delay systems attractive in applications where operational considerations are dominant or where there are weight issues in the protective system design. For example, pyrotechnic and chemical obscurants have an expansion ratio of approximately 50,000 to 1, whereas most foams range from 50 to 1 to 500 to 1 for aqueous foams.

7-2.5 Dispensing Hardware.

Dispensing hardware consists of storage tanks, activation valves, pressure regulators, safety valves, filters, power sources, and plumbing hardware. The specific hardware design is unique for each material and application, but many of the components are similar. This uniqueness of design and limited application are factors that increase the cost of the dispensing hardware.

7-2.6 Response Force Time.

Dispensable barrier systems will only delay an adversary for a finite time. At some point in time, the aggressor will defeat any delay mechanism; therefore, either guards or the response force must respond and achieve control in a shorter time than the barrier delay time.

An effective dispensable barrier can reduce the critical need for an immediate reaction by the response force. This may allow the use of response personnel who are not always dedicated to security and therefore reduce overall protection system costs. In addition, the dispensing hardware requires that the adversary must be capable of doing more than just neutralizing the response force. This increased requirement on the aggressor can significantly increase the probability that the overall physical protection system will perform as desired.

7-3 SHUTTERING SYSTEMS.

Shuttering systems are doors, screens, or other barriers that can be used to supplement defense layer protection of assets. While these barriers provide only limited delay to a forced entry attempt, they do cause the aggressor to take time to breach them, thereby allowing additional time for a response force to deploy.

7-3.1 Automated Shuttering Systems.

Shuttering systems such as fire barrier doors and security shutters can be automatically deployed in response to detection devices such as smoke detectors, heat detectors, or intrusion detection sensors. They can also be deployed though commands from a guard or monitoring station.

During normal operations, fire barrier doors can be held open by magnetic door holders but released by remote command from fire alarm panels (automatic) or from a security command center. The doors also close upon loss of power. Security shutters are normally open until a command is received from the ACS (in response to sensor activation) or from a security command center. Shutters would remain open during loss of power.

7-3.2 Use of Automated Shuttering Systems.

Automated shuttering systems can be used to delay aggressors along predicable paths from building entrances to the protected areas containing the asset. Consider using them at personnel entrances and in hallways for high and very high levels of protection combined with threat severity levels IV and V.

APPENDIX A GLOSSARY

A-1 ACRONYMS.

AA&E	Arms, Ammunition, and Explosives
ACI	American Concrete Institute
ACP	Access Control Point
ACS	Access Control System
AFCEC	Air Force Civil Engineer Center
AFI	Air Force Instruction
ANSI	American National Standards Institute
AR	Army Regulation
ASTM	American Society for Testing and Materials
AT&L	Acquisition, Technology, and Logistics
BHMA	Building Hardware Manufacturers Association
BIA	Bilateral Infrastructure Agreement
CCR	Criteria Change Request
CCTV	Closed-Circuit Television
cm	Centimeter
cm^2	Square Centimeter
COMSEC	Communications Security
CMU	Concrete Masonry Unit
DBT	Design Basis Threat
ECP	Entry Control Point
EF	Each Face
ESS	Electronic Security System

EW	Each Way
GA/ga	Gauge
GWB	Gypsum Wall Board
GSA	General Services Agency
HMMA	Hollow Metal Manufacturers Association
HNFA	Host Nation Funded Construction Agreement
HQUSACE	Headquarters, United States Army Corps of Engineers
HRP	High Risk Personnel
HVAC	Heating, Ventilating, and Air Conditioning
IC	Intelligence Community
ICD	Intelligence Community Directive
IDS	Intrusion Detection System
in	Inch
kPa	Kilopascal
lbs	Pounds
LSC	Linear Shaped Charge
Mil-Std	Military Standard
m	Meter
mm	Millimeter
mm^2	Square Millimeter
MPa	Megapascal
NAAMM	National Association of Architectural Metal Manufacturers
NAVFAC	Naval Facilities Engineering Command
NFPA	National Fire Protection Association

OC On Center

psi Pounds per square inch

SAPF Special Access Program Facility

SCI Sensitive Compartmented Information

SCIF Sensitive Compartmented Information Facility

SECNAVINST Secretary of the Navy Instruction

SFR Steel-Fiber-Reinforced

SOFA Status of Forces Agreement

TNT Trinitrotoluene

UFC Unified Facilities Criteria

UL Underwriters Laboratories

A-2 DEFINITION OF TERMS.

Access Control: For the purposes of this document, any combination of barriers, gates, electronic security equipment, and/or guards that can deny entry to unauthorized personnel or vehicles.

Aggressor: Any person seeking to compromise an asset. Aggressor categories include protesters, criminals, terrorists, and subversives.

Antiterrorism: Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces.

Assessment: Visual verification of the validity of an alarm from an electronic security system.

Asset: A resource requiring protection.

Biological Agents: Pathogens and toxins that can be used to contaminate air or water.

Breaching: Making a hole completely through a building surface using tools or explosives.

Building: A structure, usually enclosed by walls and a roof, constructed to provide support or shelter for an intended occupancy. Note that other structures, such as canopies, are not considered buildings for the purposes of this UFC.

Building Compound: A controlled area established around a building or group of building that has a perimeter defined by fences or walls, and an open area between the perimeter and the buildings.

Building Elements: Components of buildings and countermeasures associated directly with building interiors and exterior surface features.

Building Hardening: Enhanced conventional construction that mitigates threat hazards where standoff distance is limited. Building hardening may also be considered to include the prohibition of certain building materials and construction techniques.

Chemical Agents: Chemicals, including toxic industrial chemicals, toxic industrial materials, and military chemical agents that can be used to contaminate air or water.

Controlled Perimeter: A physical boundary at which vehicle access is controlled at the perimeter of an installation, an area within an installation, or another area with restricted access. A physical boundary will be considered as a sufficient means to channel vehicles to the access control points. At a minimum, access control at a controlled perimeter requires the demonstrated capability to search for and detect explosives. Where the controlled perimeter includes a shoreline and there is no defined perimeter beyond the shoreline, the boundary will be at the mean high-water mark.

Critical Asset: Any facility, equipment, service or resource considered essential to DoD operations in peace, crisis, and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation, or destruction, and timely restoration. Critical assets may be DoD assets or other government, or private assets Critical assets include traditional physical facilities and equipment, non-physical assets (such as software systems), or “assets” that are distributed in nature (such as command and control networks, wide area networks or similar computer-based networks).

Critical Infrastructure: Infrastructure deemed essential to DoD operations or the functioning of a Critical Asset.

Delay Time. The time an adversary must work to breach a security barrier to gain access to a secured resource. Total delay time is the sum of penetration and ingress times by one or more barriers separating an aggressor from a secured asset required to breach and travel between barriers. Total delay time can include egress time required to load the asset and exit the facility.

Design Basis Threat: The threat upon which a system of countermeasures protecting assets is based. The design basis threat includes the aggressor tactics and the associated weapons, explosives, tools, and agents.

Design Criteria: For the purposes of this document, the basis for defining a protective system that mitigates vulnerabilities to assets. Design criteria include assets, threats, levels of protection, and design constraints.

DoD Building: Any building or portion of a building (permanent, temporary, or expeditionary) owned, leased, privatized, or otherwise occupied, managed, or controlled by or for DoD. DoD buildings other than leased buildings are categorized within these standards as low occupancy, inhabited, primary gathering, high occupancy family housing, and billeting.

DoD Personnel: Any U.S. military, DoD civilian, or family member thereof, host-nation employees working for DoD, or contractors occupying DoD buildings. For the purposes of these standards, non-DoD visitors to DoD owned or controlled visitor centers, visitor control centers, museums, and similar facilities will be included in DoD personnel populations of those facilities. Visitor counts will be based on routine visitor levels.

Egress Time: The interval required for an aggressor to load and carry stolen assets when theft is the purpose of the penetration. The egress time varies depending upon the interior layout of the facility; the availability of doors, windows, and utility ports that can be opened; and the weight and volume of the assets being stolen. In general, egress time increases with layout complexity and any limitation on the number of doors, windows, and utility openings available as exits.

Entry Control Point. A continuously or intermittently manned station at which entry through a perimeter is controlled.

Equipment: As part of a protective system, countermeasures such an electronic security system elements and other devices used by personnel for detection and assessment of threats or weapons, tools, explosives, or chemical, biological, or radiological agents.

Explosive Safety: The practice of providing the maximum possible protection to personnel and property, both inside and outside the installation, from the damaging effects of potential accidents involving DoD ammunition and explosives.

Ferrocement or **ferro-cement:** Also called thin-shell concrete or ferro-concrete; is a system of reinforced mortar or plaster (lime or cement, sand and water) applied over layer of metal mesh, woven expanded-metal or metal-fibers and closely spaced thin steel rods such as reinforcing bars.

Forced Entry Penetration Delay Time: Barrier penetration time is defined as the time interval during which an aggressor can create a man-passable opening through a barrier (such as a wall, roof, floor, door, or window) by forced entry. The penetration delay time is based on working time rather than elapsed time. Working time accounts for the interval that an attack tool is used to attack the barrier. Working time excludes the time required to change tools, change operators, rest, and transfer tools, and for personnel to pass through the barrier. In not accounting for these interruptions, the penetration delay time is inherently conservative. In the case of multiple barriers, the total penetration delay time is the sum of the individual penetration delay times provided by all barriers.

Fragment: For the purposes of developing protective systems, pieces of the materials surrounding an explosive that may be propelled at high velocity toward a building or other target as a result of an explosion of a bomb or a warhead.

Gravity Vent: Strategically placed opening in the building to take advantage of prevailing winds and thermal buoyancy or stack effect to remove heat from a building.

Halligan Bar: A tool used in fire and rescue service for forcible entry and other prying and striking tasks.

Historic Preservation: Protection afforded to districts, sites, buildings, structures, or objects listed on or eligible for inclusion on the National Register of Historic Places in accordance with the National Historic Preservation Act.

Incendiary Devices: Devices designed to spread fire.

Ingress Time: The sum of all-time intervals required for an aggressor to traverse from barrier to barrier within a site or facility. This includes the time required to climb (up or down) through horizontal barriers (for example, roofs or floors) and the time to traverse between vertical barriers (for example, walls or fences). In general, ingress time increases with increasing site or facility size, number of barriers separating the secured area from the exterior, and size and types of tools and equipment that must be transported between barriers. The designer can increase ingress time by properly laying out the exterior and interior of the facility.

Inhabited Facilities: Buildings or portions of buildings routinely occupied by 11 or more DoD personnel and with a population density of greater than one person per 430 gross square feet (40 gross m^2). This density generally excludes industrial, maintenance, and storage facilities, except for more densely populated portions of those buildings such as administrative areas. The inhabited building designation also applies to expeditionary and temporary structures with similar population densities. In a building that meets the criterion of having 11 or more personnel, with portions that do not have sufficient population densities to qualify as inhabited buildings, those portions that have sufficient population densities will be considered inhabited buildings while the remainder of the building may be considered uninhabited, subject to provisions of these standards. An example would be a hangar with an administrative area within it. The administrative area would be treated as an inhabited building while the remainder of the hangar could be treated as uninhabited.

Kerie Cable: A long flexible spiral cable with the center strand pulled out to allow for oxygen passage used as an exothermic cutting tool.

Kelly Tool: A tool used in fire and rescue service for forcible entry and other prying and striking tasks. The predecessor of the Halligan bar, it has largely been superseded by the latter, but still sees some use.

Level of Protection: The degree to which an is protected against injury or damage from an attack.

Man-Passable Opening: A man-passable opening is defined as the minimum area required for an aggressor to physically pass through a barrier and enter a secured area. DoDM 5100.76 defines man-passable as an opening of 96 square inches (619 cm^2), which is at least 6 inches (150 mm) wide or high. These values have been established to standardize laboratory test procedures and provide a built-in level of conservatism for the final test results. The forced entry test data presented in this UFC are based on tests and are conservative. The conservative nature of this approach is even more evident where the avenue of physical entry involves passage through a thick barrier, such as an 18-inch (450-mm) reinforced concrete wall, or a long passageway, such as a 20-foot (6-m) ventilation duct.

Manpower: Countermeasures that relate to the use of guards or other personnel necessary to implement or operate elements of the protective system.

Passive Perimeter Barriers: Vehicle barriers that are permanently deployed and do not require a response to be effective and fences, walls, screens, landforms, and lines of vegetation applied along an exterior perimeter used to obscure vision, hinder personnel access, or hinder or prevent vehicle access.

Penetration: Relating to bullets or fragments, entry into a material without passing all the way through.

Planning Team: A team of people with responsibilities relating to a project that is formed to develop design criteria and review material from all phases of the design process.

Protected Asset: An asset identified in the project design criteria that requires protection against a forced entry attack.

Protective System: An integrated system of countermeasures designed to protect assets against threats to specific levels of protection. Protective systems include building elements, sitework elements, equipment, and manpower and procedures.

Procedures: Countermeasures that relate to actions taken by people, including guards and building occupants, to implement or operate elements of the protective system.

Risk: A means to quantify the combined issues of the value of an asset or the impact of its loss, the likelihood of the asset being attacked, and the effectiveness of the protection afforded the asset that can be used as a tool in making decisions about asset protection.

Risk Analysis: The process of determining risk levels for assets.

Risk Management: The process of evaluating how changes in countermeasures application affect risk levels and costs for the purpose of decision making.

Sitework Elements: Countermeasures that are applied beyond 1.5 meters (5 feet) from a building, excluding countermeasures categorized under equipment.

Spall: The condition in which pieces of a material are broken loose from the inner surface of a wall, roof, or similar element by tensile forces that are created when a compression shock wave travels through the body and reflects from the surface.

Specific Design Strategy: The approach to applying general design strategies based on the applicable levels of protection.

Tactics: The specific methods of achieving the aggressor's goals to injure personnel, destroy assets, or steal materiel or information.

TNT Equivalent Weight: The weight of TNT (trinitrotoluene) that has an equivalent energetic output to that of a different weight of another explosive compound.

Unobstructed Space: Space within 10 meters (33 feet) of an inhabited building that does not allow for concealment from observation of explosive devices 150 mm (6 inches) or greater in height.

Vulnerability: Any weakness in the design or operation of a protective system for an asset that can be exploited by an aggressor to disrupt, damage, destroy, injure, or otherwise compromise the asset.

APPENDIX B REFERENCES

CODE OF FEDERAL REGULATIONS

https://www.deadiversion.usdoj.gov/21cfr/cfr/1301/1301_72.htm

21 CFR 1301.72*, Physical Security Controls for Non-Practitioners; Narcotic Treatment Programs and Compounders for Narcotic Treatment Programs; Storage Areas*

DEPARTMENT OF DEFENSE PUBLICATIONS

https://www.esd.whs.mil/directives/issuances/dodi/

DoDD 5210.41/AFMAN 31-108, Volumes 1–3*, Security Policy for Protecting Nuclear Weapons / The Air Force Nuclear Weapon Security Manual*

DoDI O-2000.22, *Designation and Physical Protection of DoD High Risk Personnel*

DoDI 5210.65, *Security Standards for Safeguarding Chemical Agents*

DoDI 5210.88, *Security Standards for Safeguarding Biological Select Agents and Toxins (BSAT)*

DoDI 8523.01*, Communications Security (COMSEC)*

DoDM 5100.76, *Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (AA&E)*

DoDM 5105.21, Volume 2, *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*

DoDM 5200.01, Volume 3, *DoD Information Security Program: Protection of Classified Information*

DODM 5205.07/AFMAN 16-703, Volume 3, *DoD Special Access Program (SAP) Security Manual: Physical Security / Air Force Special Access Program (SAP) Security Manual: Physical Security*

DEPARTMENT OF AIR FORCE PUBLICATIONS

https://www.e-publishing.af.mil/Product-Index/#/?view=org&orgID=10141&catID=1&isForm=false&modID=449&tabID=131

AFI 16-1404, *Air Force Information Security Program*

AFI 31-101, *Integrated Defense*

AFMAN 32-1084, *Facility Requirements*

DEPARTMENT OF ARMY PUBLICATIONS

https://armypubs.army.mil/

AR 190-11, *Physical Security of Arms, Ammunition, and Explosives*

AR 190-51, *Security of Army Property at Unit and Installation Level*

AR 190-59, *Chemical Agent Security Program*

AR 380-5, *Information Systems Security*

DEPARTMENTS OF NAVY AND MARINE CORPS PUBLICATIONS

https://www.secnav.navy.mil/doni/default.aspx

MCO 5530.14, *Marine Corps Physical Security Program Manual*

OPNAVINST 5530.13, *Physical Security Instruction for Conventional Arms, Ammunitions, and Explosives*

SECNAV M-5510.36, *Information Security Program*

FEDERAL SPECIFICATIONS (FS)

https://www.gsa.gov/buying-selling/purchasing-programs/requisition-programs/gsa-global-supply/supply-standards/index-of-federal-specifications-standards-and-commercial-item-descriptions

FS AA-C-2859, *Cabinet, Security, Weapons Storage, Class 5*

FS AA-C-2786, *Cabinet, Security, Information Processing System Storage*

FS AA-D-6OO*, Security Vault Door*

FS-AA-F-358, *Filing Cabinet, Letter and Legal Size, Uninsulated, Security*

FS-AA-F-363, *Filing Cabinet, Security, Maps and Plans, General Filing and Storage*

FS-FF-L-2740, *Lock, Combination*

FS AA-V-2737, *Modular Vault Systems*

UNIFIED FACILITIES CRITERIA AND UNIFIED FACILITIES GUIDE SPECIFICATIONS PUBLICATIONS

http://www.wbdg.org/ffc/dod

UFC 1-200-01, *DoD Building Code (General Building Requirements)*

UFC 3-350-01, *Interior and Exterior Lighting Systems and Controls*

UFC 4-010-01, *DoD Minimum Antiterrorism Standards for Buildings*

UFC 4-010-03, *Security Engineering: Physical Security Measures for High-Risk Personnel*

UFC 4-010-05, *Sensitive Compartmented Information Facilities Planning, Design, and Construction*

UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*

UFC 4-020-01, *Security Engineering Facilities Planning Manual*

UFC 4-020-02, *Security Engineering Facilities Design Manual*

UFC 4-021-02, *Electronic Security Systems*

UFC 4-022-03, *Security Fences and Gates*

UFC 4-023-10, *Safe Havens*

UFC 4-215-01, *Armories and Arms Rooms*

UFC 4-420-01, *Ammunition and Explosives Storage Magazines*

UFGS-08 33 23, *Overhead Coiling Doors*

UFGS-08 34 01, *Forced Entry Resistant Components*

UFGS-08 34 63, *Detention Hollow Metal Frames, Doors, And Door Frames*

NON-GOVERNMENT PUBLICATIONS

AMERICAN CONTRETE INSTITUTE (ACI), 38800 COUNTRY CLUB DRIVE, FARMINGTON HILLS, MI 48331

https://www.concrete.org/topicsinconcrete/topicdetail/318

ACI 318-14, *Building Code Requirements for Structural Concrete and Commentary*

AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI), 11 WEST 42ND STREET, NEW YORK, NY 10036

https://webstore.ansi.org/Info/Sdolist

ANSI 297.1, *Safety Glazing Materials Used in Buildings-Safety Performance Specifications and Methods of Test*

ANSI/BHMA 156.1, *Butts and Hinges*

ANSI/BHMA 156.5, *Cylinder and Input Devices for Locks*

ANSI/BHMA 156.13, *Mortice locks*

ANSI/NAAMM HMMA 863-14, *Guide Specifications for Detention Security Hollow Metal Doors and Frames*

AMERICAN SOCIETY FOR TESTING AND MATERIALS (ASTM), 1916 RACE STREET, PHILADELPHIA, PA 19103

https://www.astm.org/

ASTM A615, *Standard Specification for Deformed and Plain Carbon-Steel Bars for Concrete Reinforcement*

ASTM A1008, *Standard Specification for Steel, Sheet, Cold-Rolled, Carbon, Structural, High-Strength Low-Alloy, High-Strength Low-Alloy with Improved Formability, Solution Hardened, and Bake Hardenable*

ASTM A1064, *Standard Specification for Carbon-Steel Wire and Welded Wire Reinforcement, Plain and Deformed, for Concrete*

ASTM F571, *Standard Practice for Installation of Exit Devices in Security Areas*

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA), PUBLICATIONS DEPT., 60 BATTERY MARCH ST., BOSTON, MA 02110

https://www.nfpa.org/

NFPA 101, *Safety to Life from Fire in Buildings and Structures*

UNDERWRITERS LABORATORIES (UL) INC., PUBLICATIONS STOCK, 333 PFINGSTEN ROAD, NORTHBROOK, IL 60062

https://www.ul.com/

UL 752, *Bullet-Resisting Equipment*

UL 768, *Combination Locks*