INCH-POUND

MIL-HDBK-1013/1A
15 DECEMBER 1993
SUPERSEDING
MIL-HDBK-1013/1
9 OCTOBER 1987

MILITARY HANDBOOK

DESIGN GUIDELINES FOR PHYSICAL SECURITY OF FACILITIES

AMSC N/A

DISTRIBUTION STATEMENT A. APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

AREA FACR

ABSTRACT

This manual provides guidance to ensure that appropriate physical security considerations are included in the design of facilities. The pre-design phase, including physical security threats, are discussed initially, followed by an overview of the design phase. Specific technical sections include exterior site physical security, building physical security, ballistic attack hardening, standoff weapon hardening, and bomb blast hardening.

FOREWORD

This military handbook has been developed from an evaluation of facilities in the shore establishment, from surveys of the availability of new materials and construction methods, and from selection of the best design practices of the Naval Facilities Engineering Command, other DOD services and Government agencies, and the private sector. It uses, to the maximum extent feasible, national professional society, association, and institute standards. Deviations from this criteria, in the planning, engineering, design, and construction of facilities, cannot be made without prior approval of respective military departments.

Design cannot remain static any more than can the functions it serves or the technologies it uses. Accordingly, recommendations for improvement are encouraged and should be furnished to the Naval Facilities Engineering Service Center (NFESC), Code ESC12, 560 Center Drive, Port Hueneme, CA 93043-4328, telephone (805) 982-9640.

THIS HANDBOOK SHALL NOT BE USED AS A REFERENCE DOCUMENT FOR PROCUREMENT OF FACILITIES CONSTRUCTION. IT IS TO BE USED IN THE PURCHASE OF FACILITIES ENGINEERING STUDIES AND DESIGN (FINAL PLANS, SPECIFICATIONS, AND COST ESTIMATES). DO NOT REFERENCE IT IN MILITARY OR FEDERAL SPECIFICATIONS OR OTHER PROCUREMENT DOCUMENTS.

DESIGN GUIDELINES FOR PHYSICAL SECURITY OF FACILITIES

CONTENTS

			Page
Section 1		INTRODUCTION	1
	1.1	Purpose and Scope.	1
	1.2	Cancellation.	1
	1.3	Using the Handbook.	1
	1.4	Related Technical Documents.	2
Section 2		PRE-DESIGN PHASE	3
	2.1	Introduction.	3
	2.1.1	Objective.	3
	2.1.2	Design Team.	3
	2.1.3	Section Organization.	3
	2.2	Physical Security Planning Policy and Requirements.	3
	2.2.1	DoD Directive 5200.8-R: Security of DoD Installations and Resources.	3
	2.2.1.1	Security System Elements and Performance Objectives.	4
	2.2.1.2	Physical Security Threat and Prioritization of Assets.	4
	2.2.1.3	Protective Design and Military Construction	4
	2.2.2	MIL-HDBK-1190: Facility Planning and Design	4
	2.2.3	DoD 5200.1-R: DoD Information Security Program Regulation of 30 May 1986; DoD 5200.2-R: DoD Personnel Security Program Regulation of 16 December 1986; and DoD 5230.24: Distribution Statements on Technical Documents.	5
	2.2.4	DoD 4270.1M: Policy Guidelines for Installation, Planning, Design, Construction and Upkeep.	5
	2.3	Establishing the Security System Design Threat.	7
	2.3.1	Overview.	7
	2.3.2	Design Threat.	7
	2.3.3	Aggressor Characteristics.	9
	2.3.3.1	Aggressor Objectives.	9
	2.3.3.2	Aggressor Types.	9
	2.3.3.3	Aggressor Tactics.	10
	2.3.4	Design Threat Selection.	11
	2.3.4.1	Overview.	11
	2.3.4.2	Identifying Asset Types.	11
	2.3.4.3	Correlate Asset to Aggressor Types.	13
	2.3.4.4	Correlate Attack Type and Severity to Aggressor Type.	13

Page

	2.3.4.5	For Asset Category Determine Whether Threat Ingress or Egress Denial Must be Provided by the Security System.	16
	2.4	Establishing Guard Force Operating Procedures and Response Times.	16
	2.4.1	Purpose.	16
	2.4.2	Guard Types/and Operating Procedures.	17
	2.4.2.1	Fixed Location.	17
	2.4.2.2	Mobile.	17
	2.4.2.3	Reaction Force.	17
	2.4.2.4	Combinations.	18
	2.4.3	Estimating the Guard Response Time.	18
	2.5	Other Constraints and Requirements.	18
Section	3	DESIGN PHASE	22
	3.1	Introduction.	22
	3.1.1	Objectives.	22
	3.1.2	Design Team	22
	3.1.3	Section Organization.	22
	3.2	Basic Integrated Security System Design Concepts.	22
	3.2.1.	Security System Functional Elements.	22
	3.2.1.1	Real-Time Operating Systems.	22
	3.2.1.2	Integrated Functional Performance.	24
	3.2.1.3	Deterrence Associated with a Security System.	24
	3.2.2	Real-Time Security System Operating Modes.	25
	3.2.3	Security Denial/Containment Zones.	26
	3.2.4	Balancing System Response and Intruder Timelines.	26
	3.2.5	Barrier Penetration Performance.	29
	3.2.5.1	Forcible Entry Barrier Penetration.	29
	3.2.5.2	Ballistic or Standoff Weapon Barrier Penetration.	29
	3.2.5.3	Vehicle Barrier Penetration.	29
	3.2.6	Intrusion Detection.	29
	3.2.6.1	Exterior Detection Along the Site Perimeter.	29
	3.2.6.2	Detection at the Building Surface.	31
	3.2.6.3	Detection Within Building Interiors.	31
	3.2.7	Entry Control.	31
	3.2.8	Threat Assessment.	31
	3.2.9	Security Lighting.	31
	3.3	Key Terms and Definitions.	31
	3.3.1	Introduction.	31
	3.3.2	Delay Time.	31
	3.3.3	Barrier Forced Entry Penetration Time.	32
	3.3.4	Ingress Time.	32
	3.3.5	Egress Time.	32
	3.3.6	Man-Passable Opening.	32

		Page
3.3.7	Intrusion Detection System.	33
3.3.8	Restricted Area.	33
3.4	Security Design Procedure	33
3.4.1	Overview.	33
3.4.2	Design Approach.	33
3.4.3	Design Procedure.	42
3.4.3.1	Design Worksheets.	42
3.4.3.2	Design Activity Chart	42
Section 4	EXTERIOR SITE-RELATED PHYSICAL SECURITY	54
4.1	Introduction.	54
4.2	Exterior Site Work and Layout	54
4.2.1	Introduction.	54
4.2.2	Installation-Wide Security Considerations.	54
4.2.2.1	Existing Site Security.	54
4.2.2.2	Collocate Facilities of Similar Asset Criticality On Site.	55
4.2.2.3	Routes of Travel.	56
4.2.2.4	Security Area Designation.	57
4.2.3	Facility-Specific Exterior Site Layout.	58
4.2.3.1	Maintaining an Adequate Standoff Blast Zone for Vehicle Bomb Threats.	58
4.2.3.2	Limit or Blocking Against Direct Line-of-Sight Weapons.	58
4.2.3.3	Maximize Exterior Site Forced-Entry Threat Ingress/Egress Distances.	60
4.2.3.4	Maintaining Clear Zones for Guard and/or CCTV Observation.	60
4.3	Exterior Site Perimeter Barriers	60
4.3.1	Introduction.	60
4.3.2	Security Fences	61
4.3.3	Vehicle Barriers.	63
4.4	Exterior Site Entry Control	68
4.4.1	Introduction.	68
4.4.2	Function and Location.	68
4.4.3	Minimum Requirements.	69
4.4.4	Gates to Perimeter Fences	69
4.4.4.1	Overview.	69
4.4.4.2	Personnel Gates.	70
4.4.4.3	Vehicle Gates	71
4.4.5	Entry Control Point (ECP) Layout and Traffic Control	72
4.4.6	Types of Entry Control Systems	73
4.4.6.1	Overview.	73
4.4.6.2	Personnel Access Control System for Explosives, Metal and Special Nuclear Materials (SNM) Detection.	74
4.5	Exterior Perimeter Intrusion Detection Systems	75
4.5.1	Introduction.	75
4.5.2	Function and Location	75

Page

4.5.2.1	Overview.	75
4.5.2.2	Exterior IDS Layout and System Compatibility.	78
4.5.3	Minimum Requirements for Exterior IDS.	78
4.5.4	Exterior IDS Options for Detection Along Site Perimeter Fences	79
4.5.4.1	Most Commonly Deployed Sensors.	79
4.5.4.2	Other Exterior IDS Sensor Candidates.	82
4.5.5	Exterior IDS Detection at Building Exteriors.	83
4.5.5.1	Ported Coaxial Cable Sensors.	83
4.5.5.2	Vibration Sensors.	83
4.5.5.3	Grid Wire Sensors.	83
4.6	Exterior Closed-Circuit Television (CCTV)	83
4.6.1	Introduction.	83
4.6.2	CCTV Function and Location	84
4.6.2.1	Threat Assessment.	84
4.6.2.2	Surveillance.	84
4.6.2.3	Location.	84
4.6.3	Minimum Requirements.	84
4.6.4	Elements of a CCTV Assessment System.	85
4.6.4.1	Camera Types.	85
4.6.4.2	CCTV Monitors.	87
4.7	Exterior Security Lighting	87
4.7.1	Introduction.	87
4.7.2	Function and Location.	87
4.7.3	Standard Exterior Lighting Configurations.	87
4.7.3.1	Continuous Lighting.	87
4.7.3.2	Standby Lighting.	88
4.7.4	Minimum Lighting Illumination Specification	89
4.7.4.1	Guard Visual Surveillance.	89
4.7.4.2	Lighting for CCTV Surveillance.	89
4.7.5	Lighting Energy Considerations.	90
4.7.5.1	Overview.	90
4.7.5.2	Restrike Time.	91
4.8	Maintaining Essential Security Support Functions	91
4.8.1	Overview.	91
4.8.2	Security Power Supply.	91
4.8.3	General Installation Power Supply.	91
4.8.4	Communications.	91
4.8.5	Security Control Center.	92
Section 5	BUILDING PHYSICAL SECURITY AGAINST FORCED AND COVERT ENTRY	93
5.1	Introduction.	93
5.2	Threat Severity Levels for Forced and Covert Entry Design	93
5.2.1	Forced Entry.	93
5.2.2	Covert Entry.	94

		Page
5.3	Integrated Security System Elements for the Building	94
5.3.1	Overview	94
5.3.2	Building Layout and Barrier Design	95
5.3.3	Building Access Control	96
5.3.3.1	Introduction	96
5.3.3.2	Function and Location	96
5.3.3.3	Minimum Requirements	97
5.3.3.4	Personnel Identity Verification Systems	97
5.3.3.5	Materials Access Control	99
5.3.4	Building Located Intrusion Detection Systems	100
5.3.4.1	Function and Location	101
5.3.4.2	Minimum Requirements	101
5.3.4.3	Detection at the Barrier	101
5.3.4.4	Detection Within Building Interior Volumes	102
5.3.4.5	Duress Switches	103
5.3.5	Closed-Circuit Television (CCTV)	103
5.3.5.1	Introduction	103
5.3.5.2	Function and Location	104
5.3.5.3	Minimum Requirements	104
5.3.5.4	Available Technology	104
5.4	Minimum Construction Requirements	105
5.4.1	General	105
5.4.2	Vaults	105
5.4.2.1	Class A Vaults	105
5.4.2.2	Class B Vaults	108
5.4.2.3	Modular Vaults	108
5.4.3	Strongrooms	110
5.4.3.1	Minimum Construction	110
5.4.3.2	Penetration Times	110
5.4.4	Arms, Ammunition and Explosives (AA&E) Facilities	110
5.4.4.1	Minimum Requirements for AA&E Facilities	110
5.4.5	Nuclear Weapons Facilities	116
5.4.5.1	Minimum Construction	116
5.4.5.2	Penetration Times	116
5.4.6	Sensitive Compartmented Information Facilities (SCIF)	116
5.4.6.1	Minimum Construction	116
5.4.6.2	Penetration Times	116
5.5	New Construction Design	120
5.5.1	Introduction	120
5.5.1.1	Overview	120
5.5.1.2	Summary of Design Choices	120
5.5.2	Designing for the Very High-Severity Threat	121
5.5.2.1	Sacrificial Areas	121
5.5.2.2	Barriers to Counter an Explosive Attack	121
5.5.3	New Wall Construction for Low- to High-Severity Threats	122
5.5.3.1	Summary	122
5.5.3.2	Low-Severity Threat	123

Asset Categories | Ingress Denial | Egress Denial |

		Page
5.5.3.3	Medium- and High-Severity Threat.	123
5.5.4	New Roof/Floor Construction for Low- to High-Severity Threats	129
5.5.4.1	Summary.	129
5.5.4.2	Low-Severity Threat Level.	129
5.5.4.3	Medium- and High-Severity Threat Levels.	129
5.5.5	New Door Construction	134
5.5.5.1	Summary.	134
5.5.5.2	Personnel Doors.	135
5.5.5.3	Vault Doors.	141
5.5.5.4	Magazine Doors.	146
5.5.5.5	Vehicle Doors.	147
5.5.6	New Window Construction	151
5.5.6.1	Summary.	151
5.5.6.2	Low-Severity Threat Level	152
5.5.6.3	Bars and Grills.	154
5.5.7	Utility Openings for New Construction - Low- to High-Severity Threats	155
5.5.7.1	Overview.	155
5.5.7.2	New Construction Design Considerations.	155
5.6	Retrofit Construction Design	161
5.6.1	Introduction.	161
5.6.2	Considerations Related to the Very High-Severity Threat.	161
5.6.3	Wall Retrofit Construction for Low- Through High-Level Threats	161
5.6.3.1	Summary.	161
5.6.3.2	Low-Security Threat Level.	162
5.6.3.3	Medium- and High-Security Threat Levels	162
5.6.4	Roof/Floor Retrofit Construction for Low to High Threats	172
5.6.4.1	Summary.	174
5.6.4.2	Low-Security Threat Level.	174
5.6.4.3	Medium- and High-Security Level Threats.	175
5.6.5	Door Retrofit Construction	182
5.6.5.1	Personnel, Vehicle, and Vault Doors.	182
5.6.5.2	Magazine Doors	183
5.6.6	Window Retrofit Construction.	186
5.6.7	Utility Opening Retrofit Construction	186
5.6.7.1	Overview.	186
5.6.7.2	Hardening Utility Openings for Conventional Buildings.	186
5.6.7.3	AA&E Ventilation Openings	186
Section 6	BALLISTIC ATTACK HARDENING	194
6.1	Introduction.	194
6.2	Ballistic Threat Characteristics.	194
6.2.1	Caliber.	194
6.2.2	Bullet Characteristics.	194

		Page
6.2.2.1	Armor-Piercing (AP)	194
6.2.2.2	Ball	194
6.2.2.3	Other Characteristics	194
6.2.3	Ballistic Limit	195
6.2.4	Oblique Attack Affects	195
6.2.5	Projectile Energy	195
6.2.6	Multiple Impacts	195
6.3	Ballistic Threats	198
6.3.1	Low-Severity Threat	198
6.3.2	Medium-Severity Threat	198
6.3.3	High-Severity Threat	198
6.3.4	Very High-Severity Threat	198
6.4	Overview of Ballistic-Resistant Materials and Defeat Mechanisms	198
6.4.1	Ballistic Resistance	198
6.4.2	Transparent Armor	200
6.4.3	Opaque Armor	200
6.4.3.1	Common Structural Materials	200
6.4.3.2	Fibrous Materials	200
6.4.3.3	Ceramic Composite Materials	200
6.4.3.4	Inorganic Nonmetallic Materials	201
6.4.3.5	Metallic Materials	201
6.5	Ballistic Hardening Option Recommendations	201
6.5.1	Threat Severity Levels of Protection	202
6.5.2	Protection Measures: New Construction	202
6.5.2.1	Siting Measures	202
6.5.2.2	Building Measures	203
6.5.3	Protection Measures: Retrofit	210
6.5.3.1	Walls	210
6.5.3.2	Doors	212
6.5.3.3	Windows	213
Section 7	STANDOFF WEAPONS HARDENING	214
7.1	Introduction	214
7.2	The RPG Threat	214
7.2.1	RPG Characteristics	214
7.2.2	RPG Jet Formation	214
7.2.3	RPG Jet Penetration	214
7.3	RPG Defeat Mechanism	217
7.3.1	Material Density	217
7.3.2	Material Strength	217
7.3.3	Rebound Defeat Mechanisms	217
7.3.4	Oblique Attack Effects	217
7.3.5	RPG Defeat By Predetonation and Standoff	217
7.4	Hardening Design Options	217
7.4.1	New Construction	217
7.4.1.1	Site Layout	217
7.4.1.2	Sacrificial Areas	218

Page

7.4.1.3 Barrier Construction and Predetonation Screens 218
7.4.2 Retrofit Construction. 220
7.4.2.1 Retrofit of Walls 222
7.4.2.2 Retrofit of Roof and Floors. 222
7.4.2.3 Windows. 222
7.4.2.4 Retrofit of Doors. 223

Section 8 BOMB BLAST HARDENING 226
8.1 Introduction. 226
8.2 Design Threats 226
8.2.1 Stationary Bomb Threats. 226
8.2.2 Moving Vehicle Bomb Threat. 226
8.3 Standoff/Hardening and Protection Levels. 227
8.3.1 Protection Levels for New Construction. 228
8.3.2 Protection Levels Existing Structures. 228
8.4 Design Approach 229
8.4.1 Introduction. 229
8.4.2 Design of New Construction 230
8.4.2.1 Structure Hardening. 230
8.4.2.2 Vehicle Barriers for Maintaining Moving Vehicle Standoff. 231
8.4.3 Retrofit Hardening of Existing Construction 233
8.4.3.1 Required Standoff for Level of Building Protection. . . 233
8.4.3.2 Vehicle Barriers. 233

APPENDIX

APPENDIX A Physical Security Design Worksheets 238

FIGURES

Figure 1 Physical Security Threat Matrix (DoD 5200.8-R) 5
2 Resource and Asset Priorities (DoD 5200.8-R) 6
3 Checklist of Other Design Constraints and Requirements 19
3 Checklist of Other Design Constraints and Requirements (Continued) 20
3 Checklist of Other Design Constraints and Requirements (Continued) 21
4 Integrated Physical Security System. 23
5 Role of Barriers in a Physical Protection System Against a Forced Entry Attack 25
6 Defense Layers for Asset 27
7 Example of Forcible Entry Intruder Timeline 28
8 Ingress Time Between Barriers (from Barrier Technology Handbook, Sandia National Laboratories, SAND 77-077 and MRC Report NSF/RA-770207) 30
9 Detailed Design Flowchart 34
10 Multiple Barrier Designs 50

Page

11	Checklist of Minimum Site Work Protective Consideration.	55
12	Example of Collocating Facilities of Similar Criticality	56
13	Exterior Site Blast Zone	59
14	Fabric With Barbed Wire Outriggers Fence Configuration (MIL-HDBK 1013/10)	64
15	Security Fence Configuration for Nuclear Weapons (DoD C5210.41-M)	65
16	Optional Barbed Roll Topping for Nuclear Weapons (DoD 5210.41-M)	66
17	Concrete Culvert Grill (MIL-HDBK 1013/10)	67
18	Removable Grating for Culverts (MIL-HDBK 1013/10)	67
19	Bar Grill Embedded in Concrete (MIL-HDBK 1013/10)	68
20	Large Culvert with Short Honeycomb Pipes (MIL-HDBK 1013/10)	70
21	Turnstile (Rotational) Personnel Gate (MIL-HDBK 1013/10)	71
22	Single Wheel-Supported (V-Groove) Sliding Gate (MIL-HDBK 1013/10)	72
23	Single Cantilevered Gate (MIL-HDBK 1013/10)	73
24	Example Entry Control Point (MIL-HDBK 1013/10)	74
25	Nuclear Weapons Storage Site Entry Control Facility (MIL-HDBK 1013/10)	76
26	Example Portal Structure for Access Control	77
27	CCTV Camera Components	86
28	Checklist of Minimum Building-Related Layout Considerations	95
29	Class 5 Vault Door Dimensions	107
30	Example Sacrificial Area Design For Very High Level Threats	122
31	Penetration Times For Solid Concrete Masonry Walls	125
32	Wood/Metal Composite Masonry Construction.	128
33	Penetration Times For Conventional Reinforced Concrete Walls/Roofs	130
34	Penetration Times For Fiberous Reinforced Concrete Walls/Roofs	131
35	High-Severity Threat Level Penetration Times for Reinforced Conventional and Fibrous-Concrete Floors Based on an Upward Attack	133
36	Personnel Door Hinge Side Protection for Low- and Medium-Severity Threat	142
37	Personnel Door, Representative Medium-Security Hinge-Side Protection	143
38	Personnel Door Anti-Pry Strips For Medium-Security Applications	144

space time is required between each interior layer and the last concrete incr

Page

39	Personnel Door, Auxiliary Rim-Lock Strike Reinforcement	145
40	Shrouded Key Operated Shackle Padlock Per MIL-P-43607	148
41	Shrouded Hasp For Padlocks MIL-H-29181	149
42	Magazine Door Panel Cross Section For Very High-Severity Threat	150
43	Window Barrier System For High-Severity Threat	153
44	Example of Large Vent Pipe and Chases Rendered Non-Man-Passable by a Honeycomb of Welded Sections of Pipe of Non-Man-Passable Diameter	157
45	High Security Can Be Provided by Vent Frame Hardening as Shown	160
46	Ten-Gauge (3.4-mm) Hot-Rolled Steel Combinations (MIL-HDBK-1013/5)	165
47	Nine-Gauge (3.8-mm) Hot-Rolled Steel Combinations (MIL-HDBK-1013.5)	166
48	Polycarbonate Combinations (MIL-HDBK-1013/5)	167
49	Typical Gratings (MIL-HDBK-1013/4)	168
50	Retrofit Hardening Options For Hollow 8-inch CMU Wall Construction	171
51	Retrofit Hardening Options For Mortar-Filled 8-inch CMU Wall Construction	173
52	Hinge Side Protection Plan for Using a Pin-In-Socket Technique	184
53	Hinge Side Protection for Doors Using a Forward Doorstop with Angle	185
54	Hinge Side Protection for Hardening Typical Thick Doors by Using an Angle Stop	187
55	Hinge Side Protection for Hardening Typical Thick Doors by Using an Angle Stop	188
56	Riveted Steel Grating	189
57	Security Intrusion Protection Plan for Hardening a Typical Door Ventilator	191
58	Installation Details of Hardening a Typical Riveted Steel Grating and Shrouded Louver for Walls or Ceilings	192
59	Security Intrusion Protection Plan for Hardening a Typical Wall or Ceiling	193
60	Ballistic Limit Criteria	196
61	Distance to Penetrate 1 to 4 Inches (25 to 100 mm) Versus Angle of Obliquity	197
Figure 62	Sightlines Blocked From Potential Vantage Points	202
Figure 63	Wall Arrangement to Block Sightlines	205
Figure 64	Walls to Block Sightlines at Doors	207
Figure 65	Oblique Window Openings	208
Figure 66	Example of High-Severity-Ballistic-Threat Bullet-Resistant Glass Cross Section	209

Page

67	Parapets to Block Sightlines	211
68	Example Antitank Grenade Launcher Weapon—the Soviet RPG-7	216
69	RPG Hardening—Concrete/Sand Thickness Versus Standoff Distance	219
70	ASP Walling System	221
71	Building Layout Example	222
72	Building Layout Example	223
73	Building Layout Example	223
74	Standard Sand-Grid Materials	224
75	Retrofit Hardening—Concrete/Sand Thickness Versus Distance	225
76	Blast Wave Geometry	228
77	Pressure Levels Versus Standoff Distance	229
78	Reinforced Concrete Wall Design For 220-Pound (100-kg) Explosive Effects (Army Security Engineering Manual)	230
79	Example Minimum Thickness [feet (meters)] of Thermal-Tempered Glass Glazing to Resist Reflected Overpressusre	231
80	Application of Traffic Obstacles	234
81	Security Barrier	234
82	Moving Vehicle Impact Energy Versus Velocity (Passive Barriers)	235
83	Moving Vehicle Impact Energy Versus Velocity (Active Barriers).	236
84	Repair Levels Versus Standoff Distance For Various Charge Weights	237

TABLES

Table 1	Design Threat Parameters	8
2	Asset Types	12
3	Checklist of Asset Categories and Potential Aggressor Types	14
4	Checklist of Design Threat for Aggressor Categories	15
5	Checklist of Asset Category Versus Security System Ingress or Egress Denial	17
6	Common Chain Link Fence Materials (MIL-HDBK-1013/10)	62
7	Typical Exterior Sensor Types (Most Commonly Used Sensors are Underlined)	79
8	Minimum Lighting Criteria for Unaided Guard Visual Assessment	89
9	Relative Efficiencies and Restrike Times of Light Sources (From IES Lighting Handbook, J.E. Kaufman, ed.)	90

Page

10	Minimum Construction Requirements for Class A Vaults (DIAM 50-3)	106
11	Minimum Construction Requirements For Class B Vaults (DoD 5200.1-R)	109
12	Minimum Construction Requirements For Strongrooms (DOD 5200.1-R)	111
13	Minimum Construction Requirements For Risk Categories I Through IV (DoD 5100.76-M)	112
14	Minimum Construction Requirements for Risk Categories II Through IV Arms, and Non-Earth-Covered Magazines (DoD 5100.76-M)	113
14	Minimum Construction Requirements for Risk Categories II Through IV, Arms and Non-Earth Covered Magazines (Continued)	114
15	Security Risk Categories (DoD 5100.76-M)	115
16	Typical Magazine Doors Panels For Explosive Safety For Risk Categories I Through IV For Ammunition and Explosives.	117
17	Minimum Construction Requirements For Nuclear Weapons Maintenance Facilities (DoD 5210.41-M)	118
18	Minimum Construction Requirements For Sensitive Compartmented Information Facilities	119
19	Reinforced Concrete Wall Designs For Very High Threat Levels	123
20	Wall Construction Choices For New Construction	124
21	Penetration Time Chart Index For Figure 31, Reinforced Concrete Masonry Walls	126
22	Penetration Time Chart Index For Figures 33 and 34	127
23	Penetration Time Chart Index For Figure 35	134
24	Personnel Door Penetration Times	136
25	Personnel Door Panel/Edge Details, Low Security.	137
26	Personnel Door Frame Details, Low Security	137
27	Personnel Door Hardware Notes For Low- and Medium-Severity Threat	138
28	Personnel Door Panel/Edge Details, Medium Security	139
29	Personnel Door Frame Details, Medium Security	140
30	Vault Door Options and Penetration Times	141
31	High-Security Magazine Door	146
32	Very High-Security Magazine Construction	146
33	Vehicle Door Construction	147
34	Time and Number of Cuts Required to Open a Man-Passable Entry in Grills Composed of Various Size Bars and Bar Spacings	151
35	Recommended Glazing System Installed In a Low-Security Wall (Wood Frame) for a Low-Severity Threat Attack	152

Page

36	Recommended Glazing System Components Installed in a Medium-Security (CMU) Wall for a Medium-Severity Threat Attack	154
37	Existing Wall Construction Achievable Penetration Times	162
38	Steel-Ply Retrofit Installations for the High-Severity Level Attack	164
39	Representative Existing Stud-Girt Construction	175
40	Stud-Girt Construction Retrofit Options For Medium Threat Levels	176
41	Existing Roof/Floor Construction Achievable Penetration Times	177
42	Existing Roof/Floor Concrete Construction	179
43	Existing Roof/Floor Wood Construction	180
44	Maximum Penetration Times (Minutes) by Threat Security Levels, Existing Metal Roofs and Floors	183
45	Firearm Ballistic Threats	199
46	Construction for Ballistic Resistance	204
47	Wall Construction Capable of Defeating the MIL-SAMIT Very High Threat	205
48	Transparent Armor Capable of Defeating the High-Severity Threat.	210
49	Upgraded Walls for High-Severity Threat	212
50	Retrofit Construction Capable of Defeating the Very High-Severity Level	213
51	Example Operational Characteristics of an RPG (Soviet RPG-7)	215
52	Predetonation Screen Effectiveness	219
53	Stationary Bomb Threats	226
54	Moving Vehicle Transported Bomb Threats	227

BIBLIOGRAPHY 251

REFERENCES 261

GLOSSARY 265

INDEX 267

Section 1: INTRODUCTION

1.1 Purpose and Scope. This handbook is to be used during the engineering design of Department of Defense (DoD) facilities to assure appropriate physical security is included. The guidelines are based upon the best currently available research and test data, and will be revised or expanded as additional research results become available. The contents include procedures for planning and designing an integrated physical security system for new facilities as well as the retrofit of existing facilities. The focus is on construction choices for protection against forced entry, and ballistic and standoff weapons. Design procedures are also summarized for vehicle bomb blast protection, referencing appropriate sources for details.

1.2 Cancellation. This handbook supersedes Military Handbook (MIL-HDBK) 1013/1, Design Guidelines for Physical Security of Fixed Land-Based Facilities, dated 9 October 1987.

1.3 Using the Handbook. This handbook is divided into eight major sections and four appendices. Sections 2 and 3 contain procedures to follow during the planning and design phases of a project to assure adequate security. Sections 4 through 8 contain supporting detailed design data and instructions. The appendices contain physical security system design worksheets. The content of each major section is summarized as follows:

Section 2 - Pre-Design Phase: Specific requirements and criteria for the security system are established during the pre-design phase. The section begins with a brief overview of DoD directives and instructions defining physical security related planning policies and requirements. This is followed by a procedure to establish: (1) the design threat, (2) the operating procedures and expected alarm response times of the security guard forces, and (3) other requirements and constraints that may affect the security system design.

Section 3 - Design Phase: The objective of this phase is to design an integrated physical security system that meets the requirements and criteria identified during the pre-design phase. The section begins with a discussion of the elements of a physical security system followed by the definitions of certain key terms. It then provides a step-by-step procedure for designing the security system for a new facility or the retrofit design of an existing facility using the detailed information in Sections 4 through 8.

Section 4 - Exterior Site-Related Physical Security: This section addresses the design of the outermost elements of the security system. The exterior area involved lies between the perimeter of the site and the facility containing the assets to be protected. Exterior physical security contributes to the effectiveness of an integrated security system design in the choice of: (1) site layout, including facility location relative to fences and vehicle barriers to enhance protection against forced entry, bomb blast, standoff weapons and ballistic threats; (2) access control at site points of entry to

protect against covert entry threats; (3) exterior intrusion detection sensors or guards to detect perimeter crossover points; (4) closed-circuit television (CCTV) or guards to assess an alarm as a threat; (5) security lighting to support the threat detection and assessment function; and (6) other essential functions that must be maintained to support the above elements. Each of these elements is addressed referring to other sources for more details when appropriate.

Section 5 - Building Physical Security Against Forced and Covert Entry: This section begins with a description of the threat severity levels for forced and covert entry followed by an overview of the important elements required to achieve an effective integrated security system design including building layout, access control, interior intrusion detection system, and CCTV. Minimum prescribed DoD security construction requirements for vaults and strongrooms; sensitive compartmented information facilities; and arms, ammunition, and explosive (AA&E,) and nuclear weapons facilities are then provided, including related penetration delay times. For those cases where the minimum prescribed designs do not provide sufficient delay relative to guard response times, or when there are no prescribed designs for a given facility type, see Section 5.5 (for new construction) or Section 5.6 (for retrofit construction) for design options that achieve the required delays.

Section 6 - Ballistic Attack Hardening: This section begins with a description of the small arms and military ballistic threats and the general hardening mechanisms by which they can be stopped. Hardening design options available for both new and retrofit construction are then presented.

Section 7 - Standoff Weapons Hardening: This section begins with a description of the standoff Rocket Propelled Grenade (RPG) threat and the general mechanisms by which RPGs can be stopped. Hardening design options available for both new and retrofit construction are then presented.

Section 8 - Bomb Blast Hardening: This section summarizes the design approach for hardening against vehicle-transported bomb blast effects for both new and existing construction.

1.4 Related Technical Documents. Use this handbook to address specific design problems relative to specific subject areas (doors, vehicle barrier, etc.). Related technical documents are identified appropriately within the text for each unique subject area.

Section 2: PRE-DESIGN PHASE

2.1 Introduction

2.1.1 Objective. The objective of the pre-design phase is to establish specific requirements and criteria for the design of a security system for either a new or retrofit facility. These requirements and criteria include: (1) the design threat the security system must protect against; (2) the operating procedures, including response time, of the security guard force; and (3) any physical, functional, or budgetary constraints associated with the site or building that can affect the security system design. These requirements must also consider the specific planning policies and procedures reflected in related military directives and instructions. Establishing security requirements during the pre-design phase allows security to be addressed early at the start of a project allowing it to be integrated into the total design of the building efficiently and cost effectively.

2.1.2 Design Team. The design team should include representatives from the intended facility users, as well as the designated military installation intelligence officers, operational officers, security or law enforcement officials, and engineering and planning personnel. The facility user can help identify special operational or logistical requirements as well as the relative criticality of the asset contained in the facility. Intelligence personnel can provide input on historical or projected future threats and their likely targets. Operations personnel can provide information on the criticality of assets from the overall installation or activity level. Security personnel can help establish the response capabilities of the security guard forces as well as identify potential criminal threats. Engineering and planning personnel should organize the effort and consolidate all facility information into the appropriate documents.

2.1.3 Section Organization. Paragraph 2.2 is a brief overview of DoD directives and instructions defining physical security related planning policies and requirements. Paragraph 2.3 is a general discussion of the steps to be taken during the pre-design phase to establish the design threat. Paragraph 2.4 addresses the response operating procedures and related alarm response time of the security guard force. Paragraph 2.5 presents other requirements and constraints that can affect the security system design.

2.2 Physical Security Planning Policy and Requirements. This section provides a brief overview of a number of DoD and other directives and instructions defining physical security related planning policies and requirements.

2.2.1 DoD Directive 5200.8-R: Security of DoD Installations and Resources. This directive prescribes minimum standards and policies related to the physical protection of personnel, installations, and assets of the DoD. The objective is to minimize damage or reduce loss or theft to assets, and to ensure that war-fighting capabilities are maintained. Specific areas

addressed include what constitutes the DoD physical security program, the responsibilities for overseeing the program, security system elements and performance objectives, generic threat types, prioritization of assets, physical security planning and system acquisition, and protective design and military construction related policies. These general policies are followed by more specific policies related to facility access and circulation control, the security of weapons systems and platforms, bulk petroleum products, as well as communication systems and material, including controlled inventory items such as drugs and precious metals. The following briefly summarizes some key elements of this directive as it relates to this handbook.

2.2.1.1 Security System Elements and Performance Objectives. DoD 5200.8-R indicates that the objective of a security system is to preclude or reduce the potential for sabotage, theft, trespass, terrorism espionage or other criminal activity. The following functional elements of the security system must perform in an integrated manner to achieve these objectives:

1) Detection alerts security personnel to possible threats and attempts at unauthorized entry at or shortly after time of occurrence.

2) Assessment through use of video subsystems, patrols, or fixed posts, assists in localizing and determining the size and intention of an unauthorized intrusion or activity.

3) Command and control through diverse and secure communications ensures that all countermeasures contribute to preventing or containing sabotage, theft, or other criminal activity.

4) Delay, through the use of active and passive security measures, including barriers, impedes intruders in their efforts to reach their objective.

5) Response through the use of designated, trained, and properly equipped security forces. Detection and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene.

2.2.1.2 Physical Security Threat and Prioritization of Assets. The general threat types in DoD 5200.8-R are summarized in Figure 1. Prioritization of assets and related level of security are given in Figure 2. These threats and asset types are addressed further in par. 2.3.

2.2.1.3 Protective Design and Military Construction. DoD 5200.8-R specifies that MIL-HDBK-1013/1 or other approved security engineering guidance be used.

2.2.2 MIL-HDBK-1190: Facility Planning and Design Guide. This document indicates that physical security threat definition should be part of the Master Planning and Siting Criteria process (Chapter 3) and references DoD

Threat Type	Threat Description	Threat Example
Maximum	Individuals in organized and trained groups alone or with assistance from an insider; skilled armed and equipped intruders with penetration aids.	Terrorists and special purpose forces; highly trained intelligence agents.
Advanced	Individual(s) working alone or in collusion with an insider; skilled or semiskilled without penetration aids.	Highly organized criminal elements; terrorists or paramilitary forces; foreign intelligence agents with access.
Intermediate	Individual(s) or insider(s) working alone or in small groups; some knowledge or familiarity of security system.	Career criminals; organized crime; white collar criminals; active demonstrators; covert intelligence collectors; some terrorist groups.
Low	Individual(s) or insider(s) working alone or in a small group.	Casual intruders; pilferers and thieves; overt intelligence collectors; passive demonstrators.

Figure 1
Physical Security Threat Matrix (DoD 5200.8-R)

5100.76-M for arms, ammunition, and explosives and DoD 5210.41-M for nuclear weapons security.

2.2.3 DoD 5200.1-R: DoD Information Security Program Regulation of 30 May 1986; DoD 5200.2-R: DoD Personnel Security Program Regulation of 16 December 1986; and DoD 5230.24: Distribution Statements on Technical Documents. These documents provide operational security guidance associated with personnel and classified material. Minimum physical security requirements are also specified.

2.2.4 DoD 4270.1-M: Policy Guidelines For Installation, Planning, Design Construction and Upkeep. This Manual is written for installation commanders to help new facility construction as well as maintenance, repair, and renovation of existing permanent and temporary facilities so that the installation can accomplish its mission now and in the future. With regard to security, the Manual provides general policy guidance that protection is required against espionage, sabotage, terrorism, and theft for facilities that include: aircraft shelters; ammunition and weapons storage facilities; command and control facilities; communications facilities; petroleum, oils,

Security System Level	Asset Definition	Asset Example
A Integrated electronic security systems, entry and circulation control, barrier systems, access delay and denial systems, dedicated security forces, designated immediate response forces.	The loss, theft, destruction or misuse of this resource will result in great harm to the strategic capability of the United States.	Nuclear and chemical weapons and alert/mated delivery systems. Critical command, control and communications facilities and systems. Critical intelligence gathering facilities and systems. Nuclear reactors and category I and II special nuclear materials. Research, development and test assets.

Security System Level	Asset Definition	Asset Example
B Electronic security systems, entry and circulation control, barrier systems, dedicated security forces, designated response forces.	The loss, theft, destruction or misuse of this resource could be expected to gravely harm the operational capability of the United States.	Alert systems, forces, and facilities. Essential command, control and communications facilities and systems. Category I arms, ammunition, and explosives. Research, development and test assets.

Security System Level	Asset Definition	Asset Example
C Electronic security systems, entry and circulation control, barriers, security patrols, designated response forces.	The loss, theft, destruction or misuse of this resource could impact upon the tactical capability of the United States.	Nonalert resources and assets. Precision guided munitions. Command, control, and communications facilities and systems. Category II arms, ammunition and explosives. POL/power/water/supply storage facilities. Research, development and test assets.

Security System Level	Asset Definition	Asset Example
D Electronic security systems, access control, barriers, dedicated response forces.	The loss, theft, destruction or misuse of this resource could compromise the defense infrastructure of the United States.	Arms, ammunition, and explosives. Exchanges and commissaries, fund activities. Controlled drugs and precious metals. Training assets. Research, development and test assets.

Figure 2
Resource and Asset Priorities (DoD 5200.8-R)

and lubricants (POL) facilities; and other facilities when a requirement is established by the responsible Military Department.

It is indicated that planning and design of military installations and facilities should consider the vulnerability to these threats, using the assessments of intelligence community agencies, and should provide installation land use, facility sites, site development, and facilities design

appropriate to the assessed threat. In addition, the use of fencing to enclose military installations or to enclose and separate areas within a military installation should be limited to those conditions requiring physical security or protection of life, except as stipulated for family housing.

2.3 Establishing the Security System Design Threat

2.3.1 Overview. The "design threat" comprises the specific types of attacks and their relative severity levels which could be directed at the facility and assets during its life cycle. Based on historical patterns and trends, the general categories, characteristics, and relative severity levels of attacks shown in Table 1 have been compiled for use in this handbook. Which of these apply to the facility being designed depends on the types of hostile aggressors in the area of the facility and their objectives. The following outlines the major factors one must consider in the selection of a proper design threat.

2.3.2 Design Threat. A clear distinction must be maintained between what is meant by a "design threat" (as shown in Table 1) and a threat "estimate." As used here a design threat is inherently concerned with the broad range of attack possibilities over the life cycle of the facility. A threat estimate is a more focused prediction of the immediately probable. Threat estimates are essentially short-term predictions of the likelihood of particular threats based on recent "intelligence" information. They are relatively important to operational security personnel, particularly security guard commanders, because they relate to the desired state of readiness. Threat estimates are particularly important in situations where physical security has not previously been designed into a facility. If physical security has been properly implemented into a facility to meet an appropriate design threat, threat estimates are presumed included within the design threat selected.

The choice of design threat must be based upon the assets being protected. There is as much potential for diseconomies by selecting a design threat that is too severe as there is for selecting one that is much too low. Choice of any design threat, particularly a severe one, will almost always influence the actual threat experience because the threat will respond to the physical security design, appropriately, in the personnel, equipment, tactics, and timing selected.

Table 1
Design Threat Parameters

Aggressor Tactics	Severity Level	Equipment/Weapons
Forced Entry	Low	Limited hand tools - low observables
	Medium	Unlimited hand tools - limited power tools
	High	Unlimited hand/power/thermal tools
	Very High	50-pound (lb) (22-kilogram (kg)) man-portable explosives, unlimited hand/power/thermal tools
Covert Entry or Insider	Low	Personnel
	Medium	Personnel and contraband
	High	Personnel, arms, contraband
	Very High	Personnel, explosives, arms, contraband
Firearms/ Ballistics	Low	ANSI/UL - Medium-power small arms (MPSA)
	Medium	ANSI/UL - Super-power small arms (SPSA)
	High	Military high-power rifle • 7.62-millimeter (mm) (30-caliber) North Atlantic Treaty Organization (NATO) Ball
	Very High	MIL-SAMIT - Military small arms multiple impact threat
Standoff Weapon	Very High	Rocket-propelled grenades
Stationary Bombs (Vehicle or Package)	Low	50 lb (22 kg)
	Medium	220 lb (100 kg)
	High	500 lb (227 kg)
	Very High	1,000 lb (454 kg)
Moving Vehicle Bombs	Low	50 lb (22 kg) trinitrotoluene (TNT), 4,000-lb (1,800-kg) car at 15 miles per hour (mph) (24 kilometer/hr (km/h))
	Medium	220 lb (100 kg) TNT, 10,000-lb (4,540-kg) car at 15 mph (24 km/h)
	High	500 lb (227 kg) TNT, 4,000-lb (1,800-kg) truck at 50 mph (80 km/h)
	Very High	1,000 lb (454 kg) TNT, 10,000-lb (4,540-kg) truck at 50 mph (80 km/h)

In the most general case the selection of a lower limit for the design threat depends upon the asset being protected, the existence of similar assets representing alternative targets in the vicinity of the facility, and the degree of security provided at these alternative targets. These alternative targets may exist in the civil sector off base or on the military installation or activity itself. Data on the historical threat precedent can be obtained from civil and military law enforcement officials. Threat historical precedent data from such sources will likely represent situations below the proper design threat. In general, the lower limit of design threat is dependent upon the "supply" of the asset and the relative "risk" for obtaining or destroying the asset to a given aggressor type.

The upper limit of the design threat severity depends upon the perceived "degree of reward" resulting from a successful attack to the facility relative to the risk, which in turn depends upon the "demand" for the protected asset. This demand will vary with the objectives and degree of motivation of the threat, for example, a theft by an unsophisticated criminal as opposed to a dedicated terrorist threat against an AA&E storage magazine. In this regard then, the design threat selection process must evaluate the major aggressor types (criminal, terrorists, protestors, etc.) and asset types. Each aggressor type has special motives against certain assets and will favor only certain types of the attacks shown in Table 1.

2.3.3 Aggressor Characteristics. Aggressors are people who perform hostile acts against military assets including equipment, personnel, or operations. Possible aggressor objectives and how they relate to the general categories of aggressor follow.

2.3.3.1 Aggressor Objectives. Possible aggressor objectives include:

1) Inflict injury or death on people
2) Destroy or damage facilities, property, equipment, or resources
3) Steal equipment, material, or information (espionage)
4) Create adverse publicity

2.3.3.2 Aggressor Types. DoD 5200.8-R categorizes the threat types into: (1) Maximum, (2) Advanced, (3) Intermediate, and (4) Low, having the characteristics shown in Figure 1. The threat examples shown in this figure are as follows:

1) Criminals. Criminals fall into one of three possible groups based on their degree of skill. Unsophisticated pilferers and thieves; sophisticated, organized career criminals; and highly organized criminal groups. The objective for all three is theft of assets.

2) Protestors. Protestors or demonstrators are considered to be an intermediate threat if active or violent, a low threat if passive. Active protesters include the two general groups of vandals/activists and extremist protesters. Both groups are politically or issue-oriented and act out of

frustration, discontent, or anger against the actions of other social or political groups. The primary objectives of both groups include destruction and publicity.

3) Terrorists. Terrorists are ideologically, politically, or issue-oriented. They commonly work in small, well-organized groups or cells. They are sophisticated, skilled with weapons and tools, and possess efficient planning capability. Terrorist objectives include death, destruction, theft, and publicity. Terrorist groups are identified based on their areas of operation. Those operating within the continental United States (CONUS) are typically political extremists consisting primarily of ethnic and white supremacy groups such as Macheteros (Puerto Rican) and Aryan Nations. They are considered intermediate-level threats. Terrorist operations outside the United States (OCONUS) are typically better organized and equipped, and their attacks more severe. Those operating in Europe, such as the Red Brigades, are less violent and may be intermediate to advanced. Groups operating in the Middle East and North Ireland have shown paramilitary capabilities and have used a broad range of military and improvised weapons. They have historically staged the most serious terrorist attacks, including suicidal attacks. They are frequently state-sponsored and include such organizations as the Palestine Liberation Organization, the Islamic Jihad, and the Irish Republican Army. These are maximum- or advanced-level threats.

4) Subversives. Subversives include aggressors from foreign governments or from groups trying to overthrow the Government by force. They include saboteurs and spies (hostile intelligence agents at the advanced or maximum levels as well as covert or overt agents at the low and intermediate levels.)

2.3.3.3 Aggressor Tactics. Aggressors can employ a wide range of offensive tactics to achieve their goals. Categorization of these tactics allows facility planners to define threats in standardized terms usable by facility designers in the development of design solutions to resist the particular tools or weapons identified in Table 1. The primary tactics addressed in this manual follow.

1) Forced Entry. The aggressor enters a facility using forced entry tools. The aggressor uses the tools to create a man-passable opening in the facility's walls, roof, windows, doors, or utility openings. Small arms may be used to overpower guards. The aggressor's goal is to steal or destroy assets, compromise information, or disrupt operations.

2) Covert Entry. The aggressor attempts to covertly enter a facility or portion of a facility by false credentials, etc. Objectives are similar to the forced entry tactic above.

3) Insider Compromise. A person with authorized access to a facility, such as an "insider," attempts to compromise a security system and/or assets by taking advantage of that accessibility.

4) Ballistics Attack. The aggressor fires various small arms, such as pistols, submachine guns, and rifles, from a distance determined by the firearm's range. The aggressor's goal is to kill facility occupants or to damage or destroy assets.

5) Standoff Weapons Attack. Military weapons or improvised versions of military weapons are fired at a facility from a significant distance. These include direct and indirect line-of-sight weapons such as antitank rocket-propelled grenade weapons. The aggressor's goal is to injure or kill the facility's occupants, and to damage or destroy assets.

6) Moving Vehicle Bomb. An aggressor drives an explosives-laden car or truck into a facility and detonates the explosives. The aggressor's goal is to destroy the facility and kill people within the blast area.

7) Stationary Bomb. An aggressor places a package or parks an explosives-laden car or truck near a facility. The aggressor then detonates the explosives either by time delay or remote control.

2.3.4 Design Threat Selection

2.3.4.1 Overview. In selecting a design threat from Table 1, the designer must be concerned with the broad range of attack possibilities over the life cycle of the facility. The choice of design threat must consider the assets to be protected, and the presence and likely motivation of an aggressor in directing an attack of a given severity against the asset. In general, the designer must identify the types of assets to be protected, the potential aggressor types that might be interested in a given asset and, from these, the most likely attacks and severity levels that these aggressors might direct at the asset. It should be noted that more than one attack type and severity level shown in Table 1 may be directed at a given asset. The objective is to establish all the attack types and severity levels for all the assets likely to be associated with the facility.

2.3.4.2 Identifying Asset Types

1) Overview. The design team shall select the key assets in the facility requiring protection. Table 2 provides a list of general asset categories. This is intended to serve as a checklist to help the designer elicit the opinion of the sponsors or operational user of the facility. In general, the assets shown in Table 2 can be divided broadly into military-related assets funded by Congressionally appropriated funds, high-value assets purchased with nonappropriated funds, and military and civilian personnel. Each of these are addressed briefly in the following.

Table 2
Asset Types

Category	Examples
A. Pilferables	(Man-Portable)
	Merchandise, supplies, televisions, tools, personal, computers, typewriters, liquor, stereos
B. Money	Cash, other negotiable instruments
C. Drugs	Controlled substances, medically sensitive items
D. Vehicles	Automobiles/motorcycles, aircraft, tactical vehicles, boats/ships
E. Arms, ammunition, and explosives (AA&E)	Rifles, small arms, bulk explosives, nuclear
F. Information	Classified records, personnel, records, financial records, inventory records, proprietary
G. Mission-critical personnel/officials	High-ranking officers/commanders; command, control, communications, and intelligence operators; weapons storage; area response force
H. Military/ Civilian personnel	(Crowds or Groups)
	Housing-family, unaccompanied, etc., recreation facilities, exchange/commissary, officer and enlisted clubs, schools, childcare centers, churches, headquarters buildings
I. Equipment/Machinery/ Buildings(1)	(Non-Portable)
	Large/heavy automated data processing equipment, large/heavy merchandise, electrical distribution/heating, ventilation, and air conditioning equipment, transmission equipment, manufacturing equipment, water treatment equipment, POL tank/pump station, radio equipment and antennae, buildings(1)

(1)Consider buildings as assets only where the building itself is the ultimate target of the attack. Vandals/activists, extremist protestors and terrorists are the primary aggressors that target buildings rather than assets housed in the building.

2) Military Critical Assets. Military critical assets are those which support war-fighting capability. For example, if the facility is an operational armory in the Middle East supporting a rapid wartime dispersal of units, it will likely contain a predictable set of weapon types, medical supplies, and other important supplies and equipment. Other examples of military critical assets and facilities are shown in Figure 2. The design team should also consult with the facility sponsor or user to determine the type of assets to be protected.

3) Nonappropriated Fund Assets. Nonappropriated fund assets are those contained in commissaries, housing, or other personnel support facilities. These assets can run the full gambit from low- to high-value items. For the most part, the threat directed at such assets is likely to be criminals whose objective is theft. The levels of protection required for such assets are, thus, a strong function of their utility or economic value to the aggressor.

4) Personnel Assets. Each facility type will contain military and civilian operating personnel. In this case the designer must be concerned with the affiliation and/or rank of the personnel, since this will directly affect the potential attacks. For example, in the Middle East, high-ranking military personnel will be a more probable target of an assassination or kidnapping than a foreign national working in the same facility. The designer should consult with the facility sponsor or user to determine the type of personnel requiring protection.

2.3.4.3 Correlate Asset to Aggressor Types. Table 3 provides a checklist of potential aggressor types (as described in par. 2.3.2) correlated to the general asset categories shown in Table 2. Implicit in the correlations in Table 3 is the objective of the threat. For example, criminals are likely to be more interested in theft of money, drugs, etc., not destruction, while terrorists are interested in the selected destruction of military assets rather than drugs, etc.

2.3.4.4 Correlate Attack Type and Severity to Aggressor Type. Table 4 provides a checklist of attack types and severity (as defined in Table 1) to aggressor types. In reviewing Table 4, note that certain aggressor types are more likely to commit to an attack at a given level of severity than other types. For example, a casual criminal would most likely resort to a low-level, forced-entry or ballistic attack, while a terrorist in the Middle East might use very high-severity level, forced-entry, ballistic, standoff weapon, or car bomb attacks. The design team should consult with operational, security, and intelligence personnel to assess the attack likelihoods. In this regard the following factors should be considered:

1) The likelihood of an attack of a given severity level occurring depends upon whether: (a) there is a past history of similar attacks in the area, or areas elsewhere with similar geopolitical and demographic characteristics, or (b) intelligence sources indicate a strong possibility of

Table 3
Checklist of Asset Categories and Potential Aggressor Types

Asset Categories	Criminal			Protestors	Terrorists			Subversives	
	Casual	Career	Highly Organized		CONUS	OCONUS	Mideast N. Ireland	Saboteurs	Spies
A. Pilferables	X	X							
B. Money	X	X	X		X	X			
C. Drugs	X	X	X		X	X			
D. Vehicles		X		X					
E. Arms, ammunition, & explosives (AA&E)			X			X	X	X	
F. Information									X
G. Mission-critical personnel/officials				X	X	X	X	X	
H. Military/Civilian population				X	X	X	X	X	
I. Equipment/Machinery/Buildings			X	X	X	X	X	X	X

such attacks.

2) Intelligence sources are normally based on assessing the likelihood of an attack and depend on whether: (a) aggressor types are in the geographical area, (b) the aggressor's objective warrants the use of a given attack at that severity level, and (c) the aggressor has access to the required resources to carry through the attack.

3) Threat accessibility to the required resources includes the necessary: (a) equipment (attack tools, weapons, and supporting equipment); (b) manpower (numbers and skill level); and (c) logistics required to carry through the attack (i.e., the site and facility is directly accessible to the aggressor and the skill, coordination, and timing required to carry through the attack exist).

4) Whether the attack is warranted by the objectives of the threat (i.e., either personnel injury, asset destruction, theft, espionage, or political embarrassment) depends upon whether a given objective is relevant to the aggressor (considering the type of asset involved), and whether the aggressor might be deterred by the protective measures at asset's facility.

5) Whether a given objective is attractive to an aggressor depends, in turn, on whether: (a) the asset is perceived as valuable by the aggressor (i.e., either because of its military criticality, high economic value, or high political embarrassment impact); (b) the aggressor has reason to believe

the asset is in the given facility; and (c) the risk at other similar facilities with the asset in the area (either on site or off) is perceived as higher. The last implies that alternative facilities with similar assets are in the area, and that their protective measures are perceived by the aggressor as more difficult to penetrate.

Table 4
Checklist of Design Threat for Aggressor Categories

Aggressor Tactics	Severity Level	Criminal			Protestors	Terrorists			Subversives	
		Casual	Career	Highly Organized		CONUS	OCONUS	Mideast N. Ireland	Saboteurs	Spies
Forced Entry	Low	X			X					X
	Medium		X							X
	High		X							
	Very high			X			X	X	X	
Covert Entry/Insider	Low	X	X		X					X
	Medium		X							X
	High			X		X	X	X		
	Very high			X		X	X	X	X	
Firearms/ Ballistics	Low	X								
	Medium		X			X	X		X	
	High		X	X		X	X	X	X	
	Very high			X				X		
Standoff Weapons	Very high						X	X	X	
Car/Truck Bombs	Low					X			X	
	Medium					X	X		X	
	High						X	X	X	
	Very high						X	X	X	
Stationary Bomb	Low					X			X	
	Medium					X	X		X	
	High						X	X	X	
	Very high						X	X	X	

6) Whether the aggressor is deterred by a given set of protective measures depends on: (a) if a specific aggressor's motivation is known to be high, or (b) there is a history (either locally, or elsewhere) of a given attack not being deterred by the given protective measures.

7) Whether a given aggressor's motivation is high, in turn, depends on whether they perceive both the reward for success and the probability of success as high.

8) In turn, whether an aggressor may perceive the probability of attack success as high depends on a history of successes; or if the manpower, equipment, and opportunity available to the aggressor is perceived by them as sufficient to accomplish their objectives and to escape.

2.3.4.5 For Asset Category, Determine Whether Threat Ingress or Egress Denial Must be Provided by the Security System. In the case of a forced entry or covert entry threat, a security system can be designed to operate in the following modes of operation:

- Ingress Denial. Unauthorized persons are prevented from entering (or destroying) some exclusion region containing the assets at risk.

- Egress Denial. Unauthorized persons (or weapons effects) are prevented from exiting some containment zone with the assets.

Depending upon the assets, one or both of the above security operational modes may be used. For example, security for arms, ammunition, and explosives assets may require ingress denial to assure that an intruder never gains access to the weapons because of the potential engagement advantage the weapons provide, or because of political embarrassment. On the other hand egress denial may be more appropriate for property-type assets when the objective is theft and not sabotage. In this case allowance can be made for intruder ingress and egress from the facility to achieve a more cost-effective design. Table 5 provides a checklist of suggested security system operating modes by category types.

2.4 Establishing Guard Force Operating Procedures and Response Times

2.4.1 Purpose. The guard force operating procedures and related response times are important factors in the operation of an integrated security system. They control the amount of delay that must be designed into the barriers and other elements of the security system. Paragraph 3.2 discusses in detail an integrated security system design that includes the proper choice of: (1) site and building layout and barrier hardening to delay the intruder, (2) access control at points of entry, (3) intrusion detection sensors and alarm to detect an attack on or within the facility, (4) CCTV or guards to assess whether an alarm is actually a threat, and (5) guards to respond to the location of a real threat. All these elements are equally important. None of them can be eliminated or compromised if an effective security system is to be achieved. Detection encompassing intrusion detection and entry control is an important element since any delay offered by a barrier can eventually be penetrated, and without detection the response force would not be alerted. The delay offered by the site and building design must provide sufficient time after detection for threat assessment and guard force response. In this regard, DoD 5200.8-R is very explicit in requiring adequate

> "... response, through the use of designated, trained and properly equipped security forces. Detection and delay must provide sufficient warning and protection to the asset until the response force can be expected to arrive at the scene."

Table 5
Checklist of Asset Category Versus Security System Ingress or Egress Denial

Asset Categories	Security System	
	Ingress Denial	Egress Denial
A. Pilferables		X
B. Money		X
C. Drugs		X
D. Vehicles o Military critical o Other	X	 X
E. Arms, ammunition, & explosives (AA&E)	X	
F. Information	X	
G. Mission-critical personnel/officials o Assassination o Kidnapping o Hostage	 X X	 X
H. Military/Civilian population o Kidnapping o Hostage		 X X
I. Equipment/Machinery/Buildings o Military critical o Other	X	 X

2.4.2 Guard Types/and Operating Procedures. Security forces at military installations are typically composed of one or more of the following: (1) DoD civilian police, (2) DoD civilian guards, (3) General Services Administration guards, (4) contract guards (commercial security services) or military guards. These guards are deployed in operating configurations that include the following.

2.4.2.1 Fixed Location. These guards normally remain at one point within a specific area (such as gates and towers at facilities).

2.4.2.2 Mobile. These guards (roving or response) are either on foot or in vehicle patrols that rove within a specified area, responding as required to alarms.

2.4.2.3 Reaction Force. These guards are dedicated to protect special assets or facilities and are housed at some central facility. They only respond to designated facilities or asset alarms.

2.4.2.4 Combinations. Combinations of the above guards are also possible. For example, a roving patrol may be dispatched on an alarm to conduct a preliminary assessment followed by a full response from a reaction guard if a real threat presents itself. In this case, the overall response time of the security system is much longer than if a real-time assessment using on-site guards or CCTV is provided, or if the initial guard response includes the full reaction force. The specific guard operating procedures for the facility of interest shall be established with the help of installation operational and security personnel on the design team.

2.4.3 Estimating Guard Response Time. The maximum likely response time required is the sum of those times it takes after an alarm has occurred to correctly assess that a threat is present, plus the time it takes for a guard force to arrive at the scene. In this regard, threat assessment may be accomplished by a CCTV system, or by simply dispatching a guard for direct observation, with the actual full guard response occurring once a real threat has been detected. Once the guard types, their locations, and operating procedures applicable to the facility are established, it is possible to estimate the likely response time. It is recommended that the maximum likely time, considering adverse weather conditions or other factors, be used. To aid in this determination, Public Works may have maps from which response distances and, thus, response time can be estimated using (conservatively) a 30-mph response speed. Alternatively, simple timing measurements with a stop watch can be conducted under actual conditions.

2.5 Other Constraints and Requirements. While security engineering is an important aspect of facility design, it is only a part of the total project. Project planners and designers concerned with security must also consider such issues as installation master planning requirements, safety, fire protection, facility operational and functional issues, energy conservation, seismic criteria, barrier-free handicapped access, and aesthetics. Protective measures may actually enhance energy conservation or seismic survivability, but safety requirements or barrier-free access may hinder the objectives of the protective system. In general, these constraints may be unique to a specific asset, site, facility, or entire installation. Conflicts need to be recognized and priorities established in the planning programming stage to guide designers toward appropriate and optimal solutions. Figure 3 provides a checklist of items to be considered by the design team. These are broadly classified as: (1) political, (2) financial, (3) regulatory, (4) procedural or operational, and (5) facility- and site-related.

(1) Political Considerations. The relationship with the public, including on-post and off-post personnel.

(a) Adjacent Landowners or Other Tenant Organizations. Assess potential problems, such as high-intensity security lighting's impact on neighbors, the safety of neighbors, and inconveniences such as traffic restrictions. Identify any neighbors requiring special consideration.

(b) Appearance. Consider the public perception of the appearance of a proposed security facility, site, or area. For example, public perception of a "fortress" may be either desirable or undesirable.

(c) Public Access. Identify restrictions on limiting public access to a facility, a site, or an area of an installation.

(d) Political Climate. Consider how the local situation influences facility design or land use decisions. Politically unpopular decisions may actually attract acts of aggression to completed facilities.

(2) Financial Considerations. Establish funding limitations for security based on such criteria as regulations, available budget, or the planning team's judgement of a reasonable limit for security costs. Describe limitations in terms of actual cost or percentage of facility cost.

(3) Regulations. Consider other government regulations which pertain to design. Ensure that all pertinent regulations are cited and identify any which are not. Also consider requirements imposed by the installation's physical security plan, local building codes, life safety, and occupational safety and health codes or regulations.

(4) Procedural or Operational Considerations. Installation or facility user requirements related to operations in either normal or heightened threat conditions. Examples include:

(a) Deliveries. Requirements related to how and where deliveries or pickups are to be made, e.g., mail, supplies, material, and trash, service or construction vehicles.

Figure 3
Checklist of Other Design Constraints and Requirements

(b) Restricted Areas. Areas within facilities or the installation which require restricted access.

(c) Access Controls. Who or what is to be controlled, to what degree and where and when the controls apply, e.g., personnel identity and weapons checks, vehicle checks, and checks of packages.

(d) Functional Requirements. How the user will operate the facility including relationships between organizations or components of organizations, work schedules, types of operations to be performed, and special requirements for facility layout or construction.

(5) Facility and Site Constraints. Examine the installation's Master Plan, existing facilities, and the proposed project (if using standard definitive designs) to identify requirements related to site or facility layout or construction. Potential constraints include:

(a) Occupancy Requirements. Identify space requirements, ventilation and window ratios, and other occupancy-related design constraints.

(b) Life Safety Considerations. Egress requirements related to fire safety constraints, protective measures, and building layout.

(c) Occupational Safety and Health Concerns. Whether personnel safety measures conflict with or inhibit security measures.

(d) Barrier-Free Accessibility. Public facilities and facilities which shelter military dependents or civilians must conform to the Uniform Federal Accessibility Standards which may constrain security-related design.

(e) Parking Lots and Roads. Requirements for parking lots and roads which could impact security, e.g., how close to the protected building vehicles may be allowed to approach or park with and without entry control.

(f) Fences and Lighting. Identify restrictions for installation of fences or security lighting.

Figure 3
Checklist of Other Design Constraints and Requirements (Continued)

(g) Intrusion Detection Systems (IDS). Identify any restrictions for IDS including CCTV, access control equipment, and intrusion sensors.

(h) Architectural Design. Restrictions on the construction materials or architectural style to be used for the building. Some installations provide architectural guidelines which define appropriate styles and limit construction materials.

(i) Existing Facilities. Whether layout, proximity, construction, or operations of existing facility constrain new projects.

(j) Miscellaneous. Design constraints imposed by landmark status of buildings or areas, floodplain restrictions, endangered wildlife or plant species, or any other design considerations.

Figure 3
Checklist of Other Design Constraints and Requirements (Continued)

Section 3: DESIGN PHASE

3.1 Introduction

3.1.1 Objectives. The objective is to design an integrated physical security system (Figure 4), for either a new facility or existing facility. This security system must meet the requirements and criteria identified during the planning phase (Section 2) including protecting against the full range of design threats in a manner that also accounts for the security guard force operating procedures and response times, and accounts for the physical, functional, and budgetary constraints associated with the site or building.

3.1.2 Design Team. The design team consists of the architects, security specialists and the civil, structural, mechanical, and electrical engineers responsible for the design of the facility.

3.1.3 Section Organization. Paragraph 3.2 discusses the basic concepts and important elements of an integrated physical security system design. Paragraph 3.3 provides definitions of key terms. Paragraph 3.4 provides a step-by-step process for designing the security system for a new facility, or the retrofit of an existing facility.

3.2 Basic Integrated Security System Design Concepts. This section describes basic design concepts associated with: (1) the functional elements of an integrated security system (par. 3.2.1); (2) the operating modes of a security system (par. 3.2.2); (3) security exclusion/containment zones (par. 3.2.3); (4) balancing system response and intruder timelines (par. 3.2.4); (5) barrier penetration performance (par. 3.2.5); (6) intrusion detection (par. 3.2.6); (7) entry control (par. 3.2.7); (8) threat assessment (par. 3.2.8); and (9) security lighting (par. 3.2.9).

3.2.1 Security System Functional Elements

3.2.1.1 Real-Time Operating Systems. Four basic functional elements must operate in an integrated and timely manner to achieve an overall effective security system that defeats the design threats. These include:

1) Intrusion detection and access control. Intrusion detection and access control sensors and/or guards are required to detect any unusual occurrence or disturbance around, at the entrance to, or within a secured site or facility. The detecting and assessing functions also require a communication system to transfer information to security control in a timely manner.

2) Threat assessment. A CCTV or guards are required to assess whether the detected event or disturbance is actually a threat.

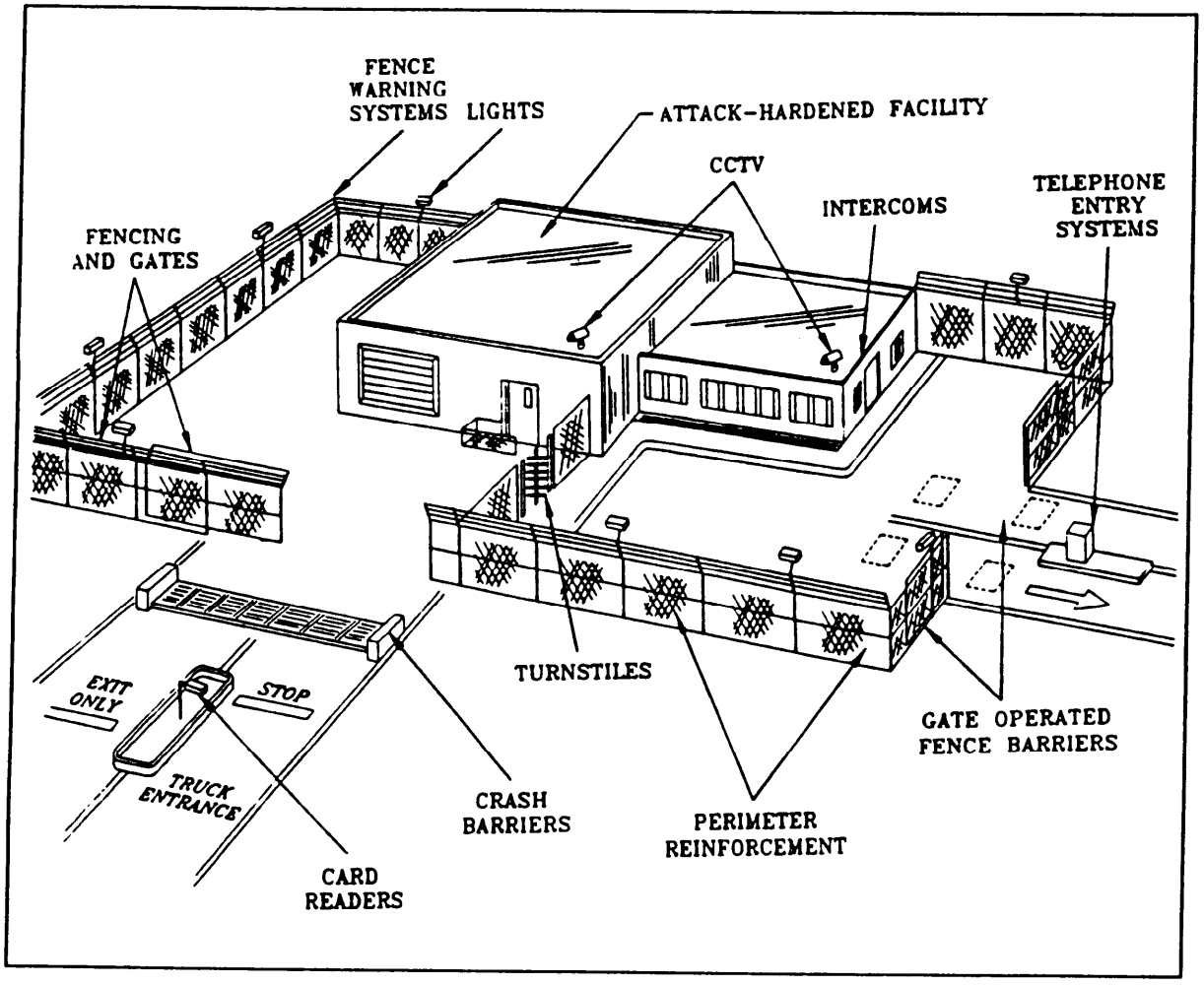


Figure 4
Integrated Physical Security System

3) Barriers. Appropriately designed and located barriers are required to delay a forced entry threat or to stop a standoff, ballistic, or vehicle bomb attack. In the case of forced entry, the delay must be sufficient to allow the system time to detect, assess, and react appropriately.

4) Responding Guards. Guards must respond to the location of the alarm, applying restraining or, in the limit, deadly force.

The above functional elements can be accomplished using people, hardware, or some combination. For example, detection may be accomplished by roving guards or intrusion detection sensors. Assessment may involve response force guards, CCTVs, or some combination. The delay function may involve either one or more

passive structural barriers such as: attack hardened walls; active, roving guard patrols with small arms; or some combination. System response normally involves a security guard response force, but could involve some form of active defensive hardware.

3.2.1.2 Integrated Functional Performance. All of the above system elements are equally important and must operate in an integrated manner. None can be eliminated or compromised if an effective security system is to be achieved. Detection is important, since any resistance and delay offered by a barrier can eventually be penetrated without detection. Moreover, the delay must be sufficient to allow time after detection for threat assessment and guard force response. A simple graphical method of illustrating the timely interplay of these four basic elements, particularly the role of barriers in delaying the threat, is shown in Figure 5. At some point in time, labeled T sub o in Figure 5, an attack or unauthorized action by an adversary begins. The upper line in Figure 5 reflects the actions and time required for the intruder to complete his goal including the delay caused by the barriers associated with the security system. At time T sub o, a sensor is triggered which initiates the active protection system elements. Commencing at time T sub o, a time race begins between the adversary and the response elements. The protection system objective is to ensure that the sensor alarm is quickly and correctly assessed and that sufficient response forces are alerted and arrive at the proper location in time to prevent the adversary from accomplishing his goal. The role of barriers is to increase the intruder time after the detection system sensor is triggered. This increase in time is accomplished by introducing sufficient barriers along all possible adversary paths to provide the needed delay for the response forces to arrive and react.

3.2.1.3 Deterrence Associated with a Security System. All security systems offer some level of deterrence which depends on the level of dedication and sophistication of the intruder and the relative value and/or criticality of the assets at risk. Casual thefts of opportunity against noncritical assets may be deterred by nominal investments in such things as alarm systems or bars on the windows of a facility. On the other hand, the integrated real-time security system described above may be required to deter dedicated and sophisticated intruders intent on stealing or destroying critical assets.

Examples of deterrent security measures include: (1) visible guard forces with rapid response or frequent patrol intervals, (2) high traffic densities in or near a structure to increase the perceived likelihood of detection, (3) an inventory control system that is updated frequently to deter insider theft, and (4) lighting systems to increase the perception of nighttime detection.

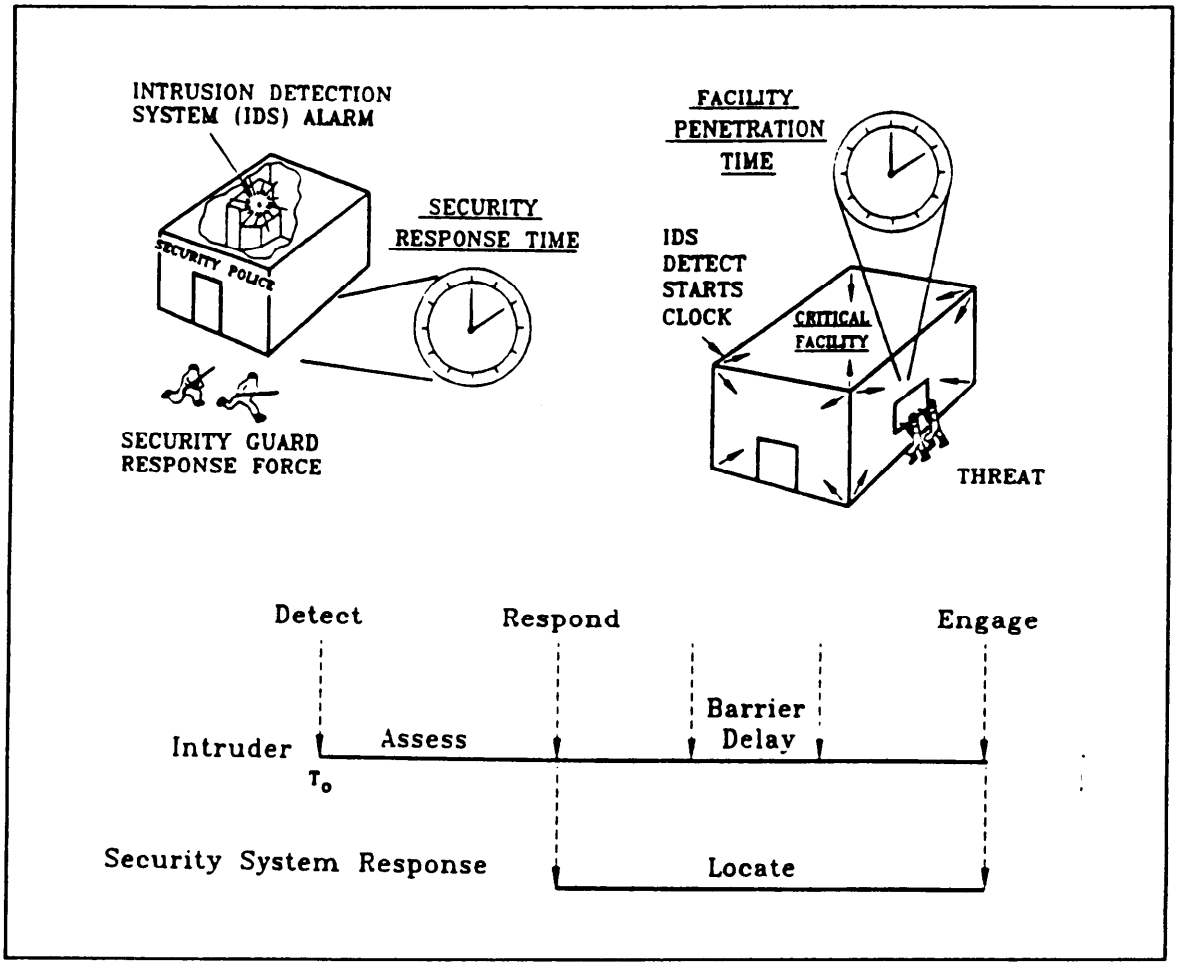


Figure 5
Role of Barriers in a Physical Protection System
Against a Forced Entry Attack

3.2.2 Real-Time Security System Operating Modes. An integrated real-time security system can be designed to operate in the following modes of operation:

- Ingress Prevention - Unauthorized persons (or weapons effects) are prevented from entering (or destroying) the denial zone containing the assets at risk.

- Egress Prevention - Unauthorized persons are prevented from exiting with the assets.

Depending upon the assets, one or both of the above security operational modes may be used. For example, security for arms, ammunition, and explosives-type assets may require ingress prevention to assure that an intruder never gains access to the weapons because of potential engagement advantages against the guards offered by the weapons, or because of political embarrassment, or other considerations. On the other hand, egress prevention may be more appropriate for property assets when the objective is theft and not sabotage. In this case allowance can be made in the timeline calculations and design for intruder ingress and egress from the facility. When both of the above operating modes are combined into one integrated system, we say that the system has in-depth (i.e., backup) security capability.

3.2.3 Security Denial/Containment Zones. In the most general case, the spatial regions described as the "denial" and "containment" area or zone are three-dimensional. Depending upon its physical extent, an exclusion or a containment zone can be further characterized as either a "perimeter" or a "point" zone. "Perimeter" zones tend to have large, extended volumes characterized by a well-defined perimeter or boundary such as the exterior of a large fenced-in site or a building. On the other hand, a "point" zone is characterized by a very small or limited volume, e.g., a single vault in the interior of a building or perhaps a secured cabinet containing classified information. In this regard, one may have a building containing a security system that relies on multiple defensive shells or layers of hardened perimeter type barrier zones culminating in a single container point zone. Figure 6 shows such a multilayered defensive configuration. The first, or innermost, layer may be a container, a prefabricated magazine, a vault, or simply a room containing the asset. These are followed by other interior rooms, the exterior of the facility, and the site perimeter fence. Note that although the outer perimeter fence shown in Figure 6 offers little penetration delay (see par. 4.3.2.1), it does limit the amount of tools, etc., that can be easily transported by the threat.

3.2.4 Balancing System Response and Intruder Timelines. In general, the time for detecting, assessing, and responding must be less than, or at least match, the intruder's time accounting for delays introduced by the barriers. Depending on the design threat, the system design may have to be flexible enough to handle anything from very "compressed" times for high-speed vehicle intruders to more extended times for slower on-foot intruders. Also, the timing and the performance of the real-time system elements must be designed to complement each other. For example, if the responding function involves an inherently long time (e.g., guards on foot), the detecting, assessing, and delaying functions must be designed to detect, confirm, and delay the threat in a time frame that matches these system delays.

It is also important to note that unless the threat is detected before, at, or near the outside of the barrier, the delay stemming from the penetration of the barrier cannot be accounted for when balancing against the guard force response time. The guard force can only begin to respond after detection and assessment. Consideration must be given to installing barriers so that they

are encountered after detection. In general, the critical assets to be protected should be located at a central point well within the interior of a building presenting as many intermediate barriers to the intruder's path as possible. An example of a building layout involving multiple barriers or shells is illustrated in Figure 6. In general, the total delay time associated with the site and building should equal the guard response time. The total delay time, in turn, is the sum of the penetration times associated with each barrier plus the intruder ingress/egress time between all barriers where the timeline starts at the first point of intrusion detection. In this regard, if the building is surrounded by a fence or other exterior site-related barrier having an exterior intrusion detection system (IDS), this can be considered the first layer of defense followed by the exterior of the building and then any interior rooms, vaults, or containers housing the asset. If there is no exterior fence IDS, the timeline can only start with that barrier which immediately is preceded by a building interior IDS that can detect the intruder. Finally, it is important to note that in order to be effective, each component comprising a given shell (i.e., walls, roof, floor, door, etc.) must offer an equivalent penetration delay time so as not to create any weak links into the shell.

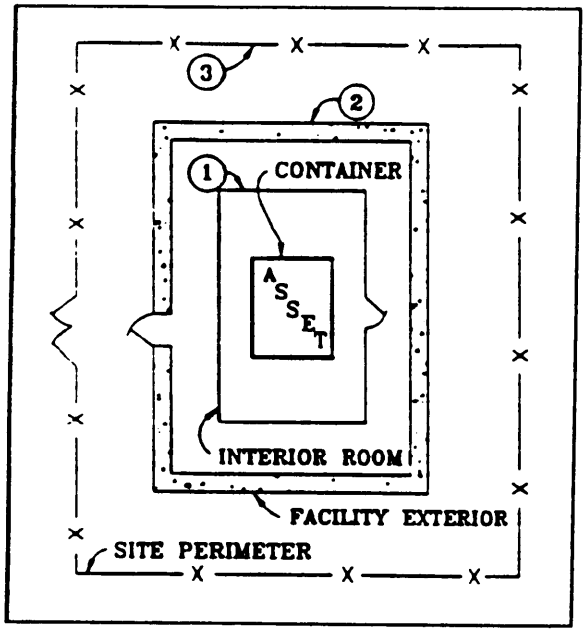
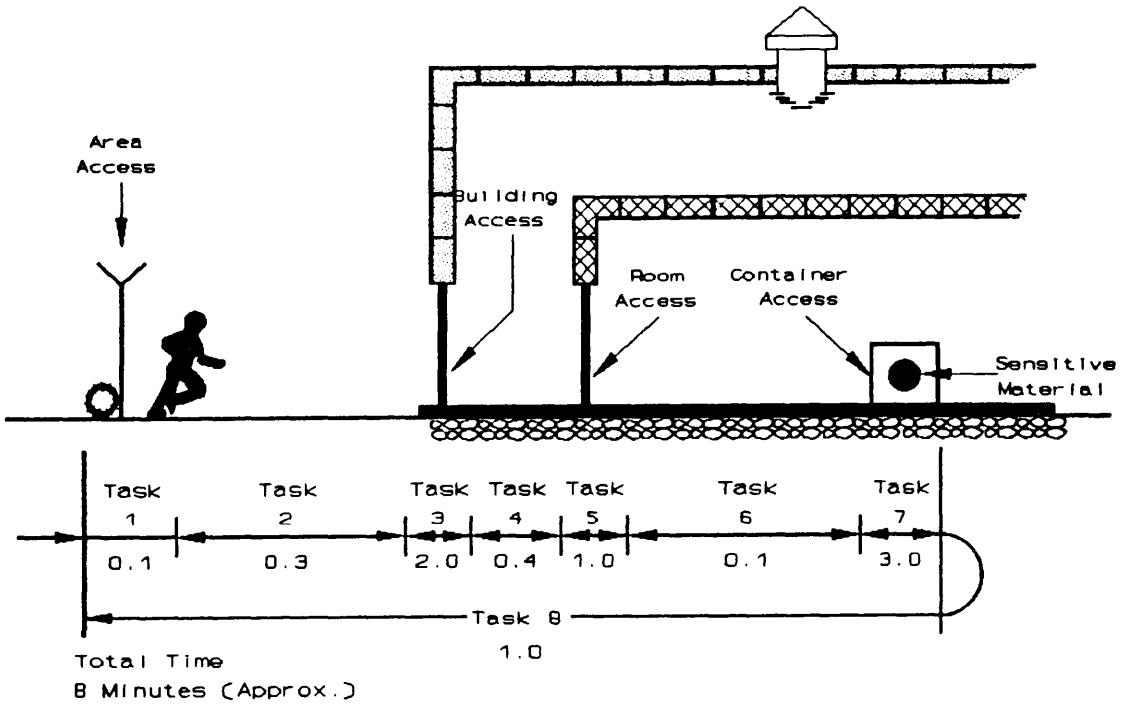


Figure 6
Defense Layers for Asset

Figure 7 presents a graphic example of a simple scenario for an industrial-type facility which uses conventional barriers. This example illustrates how individual barrier penetration times can be combined with threat ingress times to establish total intruder scenario times. The scenario starts with the intruder just outside the fenced area and ends when the adversary has exited the fenced area with the stolen material. In this example, the adversary can accomplish the theft in about 3 minutes, if not interrupted by guards. Guards, of course, will not be available to interrupt the intruder unless he is detected at some point in the scenario, an alarm is sounded, and the guards have time to respond.

To illustrate the guard response times needed for various protection system goals, assume that a fence perimeter detection system with an immediate alarm capability exists at the fence in the example facility. If the goal is to intercept the intruder before he can penetrate the building, the guards must arrive within about 2 minutes of the alarm. If the goal is to intercept the intruder before he can get his hands on the sensitive material (for possible sabotage), the guards must arrive at that location within about 6 minutes of



Time Estimate		
Task	Mean Time (min)	Task Description
1	0.1	Climb over fence
2	0.3	Run 250 feet (76mm)
3	2.0	Force door
4	0.4	Walk 150 feet (46mm)
5	1.0	Force lock
6	0.1	Walk to container
7	3.0	Open container
8	1.0	Gather material and escape
9	7.9	Total (approx. 8 min)

Figure 7
Example of Forcible Entry Intruder Timeline

the alarm. If the goal is to prevent removal of the sensitive material from the fenced area, the guards must intercept the adversary within 8 minutes of the alarm.

3.2.5 Barrier Penetration Performance

3.2.5.1 Forcible Entry Barrier Penetration. A barrier is penetrated when an intruder can pass through, over, under, or around the structure. Penetration time includes the time to create a man-passable opening [96 square inches (0.06 square meter (sq m))] and traverse the barrier. Barrier penetration time is a function of the selected attack mode which is governed by the equipment required. Categories of attack tools are described in par. 2.3.2.4.

As an intruder encounters a series of barriers, it becomes increasingly difficult to transport and set up bulky or sophisticated tools. This is especially true if it is necessary to pass through a series of small openings. The accessibility of the restricted area to vehicular traffic may also be affected. When the adversary is forced to carry heavy equipment for long distances without the aid of vehicles, the delay times may become significantly longer.

Section 5 presents penetration time information to be used in evaluating or selecting barriers to protect against forced entry.

3.2.5.2 Ballistic or Standoff Weapon Barrier Penetration. A barrier is penetrated by a standoff or ballistic weapon, when a shaped-charge jet or bullet either penetrates or causes sufficient secondary spall to kill or injure personnel on the other side of the barrier. Section 6 addresses methods for hardening against ballistics, and Section 7 against standoff weapons.

3.2.5.3 Vehicle Barrier Penetration. A vehicle barrier can be considered penetrated when the ramming vehicle has passed through the barrier and is still functioning, when a second vehicle can be driven through the breached barrier, or when the vehicle barrier has been removed or bridged and a vehicle has passed through or over the barrier. Vehicle barriers designed to prevent penetration are addressed in Section 8.

3.2.6 Intrusion Detection. The detection of an intruder can be accomplished using either on-site guards, IDS, or some combination: (1) at the exterior perimeter fence line of the site, (2) at or on the surface of barriers associated with the building, or (3) within the interior volume of all or part of the building.

3.2.6.1 Exterior Detection Along the Site Perimeter. Locating guards in towers or deploying sensors along extended fence lines adds to the intruder's ingress/egress time to cover the distance from the fence to the building, i.e., the clock starts earlier with detection along the fence. This option, though, typically involves high operating costs for guards or, if sensors are

Recommended only if required by

used, high initial purchase, installation, and maintenance costs. The cost-effectiveness of using exterior detection along extended perimeters to gain added intruder ingress/egress time must be weighed against the cost of hardening the building more and installing IDS in a smaller area at or within the building. Figure 7 shows that the time to penetrate or climb over a perimeter fence is only a few seconds (about 0.1 minute). Figure 8 also shows that the ingress time for an intruder carrying up to 35 pounds (16 kg) of tools covering distances of up to 400 feet (122 m) between the fence and building is less than a minute. Given the nominal amount of time gained relative to the expense involved, the use of guards or IDS on extended fence perimeter is recommended only if required by DoD regulation. Exterior IDS options are discussed in par. 4.5.

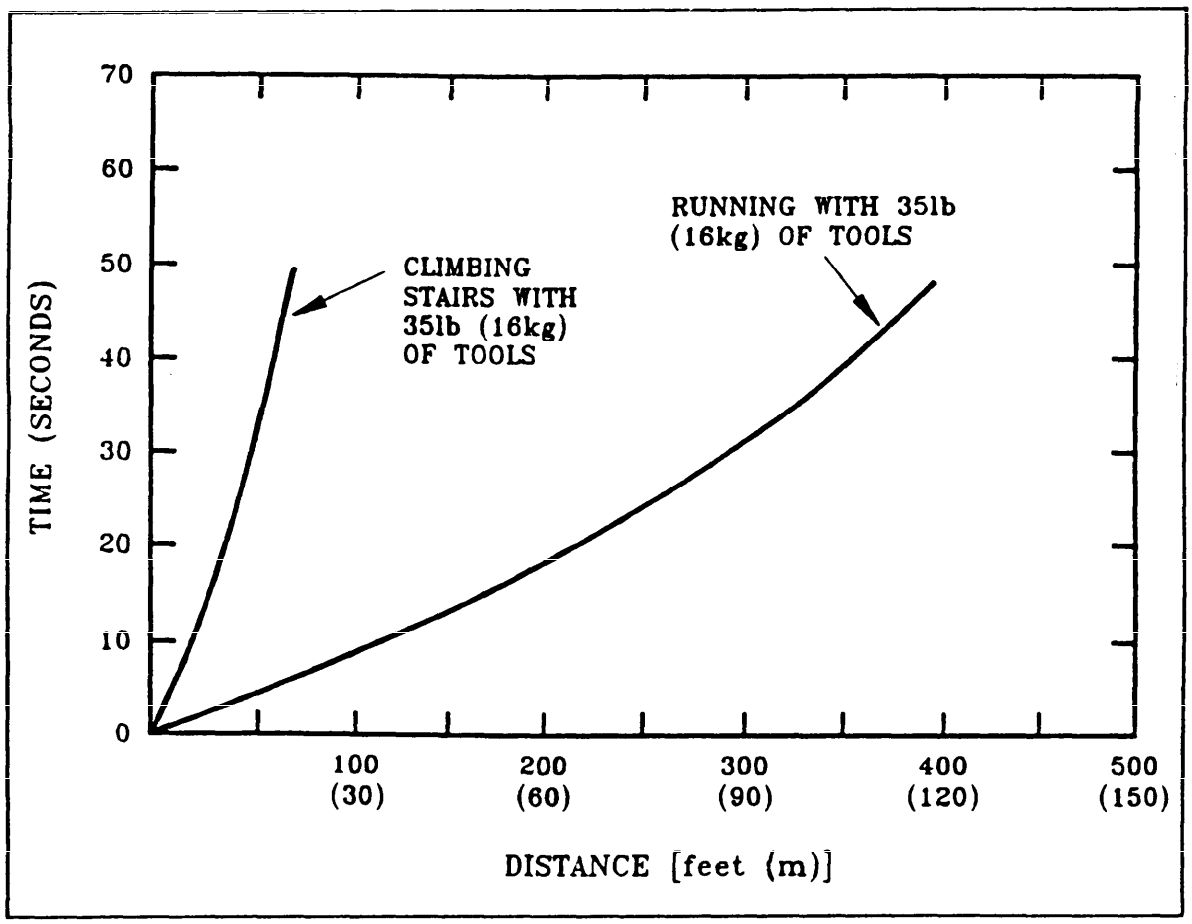


Figure 8
Ingress Time Between Barriers (from Barrier Technology Handbook, Sandia National Laboratories, SAND 77-077 and MRC Report NSF/RA-770207)

3.2.6.2 Detection at the Building Surface. Guards or sensors may be located on site at the building to detect a threat before penetrating a barrier surface. As noted, for a barrier to be effective in delaying an intruder, detection must occur before penetration of the barrier has occurred. Surface sensor systems, such as vibration sensors, etc., are usually more cost-effective than stationing guards. These IDS options are addressed further in par. 5.3.4.

3.2.6.3 Detection Within Building Interiors. Guards or sensors for threat detection may be located within the building. For example, intruder detection may be limited to an area around the outside of a vault. The deployment must ensure that the detection occurs before the vault is penetrated. Interior IDS systems are also used to detect covert entry or insider threats. Barrier surface sensors as well as volumetric sensors can be used. These are described in par. 5.3.4.

3.2.7 Entry Control. Entry control is the security function whereby personnel, vehicles, and material are identified and screened to discriminate authorized from unauthorized personnel and vehicles, and to detect explosives contraband, etc. Entry control also includes supervising the flow and routing of traffic, both pedestrian and vehicular. Control is not limited to the site boundary or main gate, but extends to all controlled areas of the activity, e.g., parking areas, building entrances, and even interior rooms and safes. Exterior site-related entry control options at gates, etc., are addressed in par. 4.4, and building entry control-related options in par. 5.3.3.

3.2.8 Threat Assessment. Threat assessment can be accomplished by roving or depot guards dispatched to investigate an alarm, or directly by tower guards along the site perimeter or guards or personnel located at the building. Alternatively, a CCTV system may be used. Assessment may occur: (1) along the perimeter fence line of the site, (2) the exterior of the building, or (3) within the interior of the building. The first two options are addressed in par. 4.6, and the third in par. 5.3.5.

3.2.9 Security Lighting. Security lighting provides lights during periods of darkness or in areas of low visibility to aid threat detection, assessment, and interdiction by guards or CCTV. Security lighting is typically located along site or building perimeter boundaries and entry points. Security lighting is addressed in par. 4.7.

3.3 Key Terms and Definitions

3.3.1 Introduction. The following provides specific definitions for key terms.

3.3.2 Delay Time. Delay time is the total time an intruder is prevented from gaining access to a secured resource. Delay time includes the penetration time provided by one or more structural barriers separating an intruder from a secured resource, and the ingress time required for travel

to define the surveillance region or an exterior regulation. fences are used

from barrier to barrier to get to the secured resource. Delay time can also include egress time required to load the secured resource and exit the facility.

3.3.3 Barrier Forced Entry Penetration Time. Barrier penetration time is defined as the time interval during which an intruder succeeds in creating a man-passable opening through a barrier (i.e., a wall, roof, floor, door, window, etc.) by forced entry. The penetration time is based on working time rather than elapsed time. Working time only accounts for the interval that an attack tool is actually used. This excludes the time required to change tools, change operators, rest operators, and transfer tools, and enable personnel to pass through the barrier. In not accounting for these interruptions, the penetration time is inherently conservative. The penetration times presented in Sections 4 and 5 apply to single barriers only. In the case of multiple barriers, the total penetration time is the sum of the individual penetration times provided by all barriers.

3.3.4 Ingress Time. Ingress time is the sum of all time intervals required for an intruder to traverse from barrier to barrier within a site or facility. This includes the time required to climb (up or down) through horizontal barriers (e.g., roofs or floors) and the time to traverse between vertical barriers (e.g., 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 facilities engineer can increase ingress time by properly laying out the exterior and interior of the facility.

3.3.5 Egress Time. Egress time is the interval required for an intruder to load and carry stolen assets from a secure area when theft is the purpose of the penetration. The egress time may be short or long 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 that are 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.

3.3.6 Man-Passable Opening. A man-passable opening is defined as the minimum area required for an intruder to physically pass through a barrier and enter a secured area. DoD 5100.76-M defines man-passable as an opening of 96 square inches (0.06 sq m), which is at least 6 inches (150 mm) wide or high. In limiting the definition of a man-passable opening to 96 square inches (0.06 sq m), the definition is inherently conservative, particularly 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.

3.3.7 Intrusion Detection System. This is a system designed to detect and alarm the approach, intrusion, or presence of an intruder by reaction of a mechanical or electronic detector.

3.3.8 Restricted Area. A restricted area is an area to which entry is subject to special restrictions or control for security reasons, or to safeguard property or material. This does not include those designated areas restricting or prohibiting overflight by aircraft. Restricted areas may be of different types depending on the nature and varying degree of importance of the security interest, or other matter contained therein. Restricted areas must be authorized by the installation/activity commander, properly posted, and shall employ physical security measures.

3.4 Security Design Procedure

3.4.1 Overview. Figure 9 presents a design activity flow chart outlining a recommended procedure for designing an integrated physical security system for a facility. This procedure is intended to be used with the information and data contained in Sections 4 through 8. With the exceptions noted, the same general procedure applies to the design of a security system for a new facility or the retrofit of an existing facility. Note that a single box in the flow chart represents a design activity, while one or more boxes preceded by a circle (an "or") means an either/or design option. Finally, a diamond represents a decision point. The number appearing at the top of a box or diamond is the section (or paragraph) number in this handbook containing related guidelines and data. Since the more severe design threats are likely to control the selection of building elements, the procedure focuses first on the vehicle bomb, standoff weapon, and ballistic weapon attacks, followed by the forced and covert entry threats. The forced-entry design segment addresses the exterior site security elements first, followed by building security elements. These security elements include barrier construction, intrusion detection sensors, CCTV, lighting, etc. The covert threat segment addresses the selection of sensors and entry control to counter these threats.

3.4.2 Design Approach. The objective is to identify an integrated physical security system design that achieves a cost-effective application of security system resources. This usually means identifying and securing the innermost and smallest volume possible. In general, securing large extended volumes of a building or a fenced-in site perimeter around a building is necessary only: (1) if required by a DoD regulation, (2) to establish an adequate blast zone for a vehicle bomb attack, or (3) as a sacrificial area for standoff weapon protection. In most other situations, the design should harden and secure the smallest volume comprising the innermost interior shell layer surrounding the critical asset. Outer security hardened barriers are included in the design only if necessary to achieve additional required delay time.

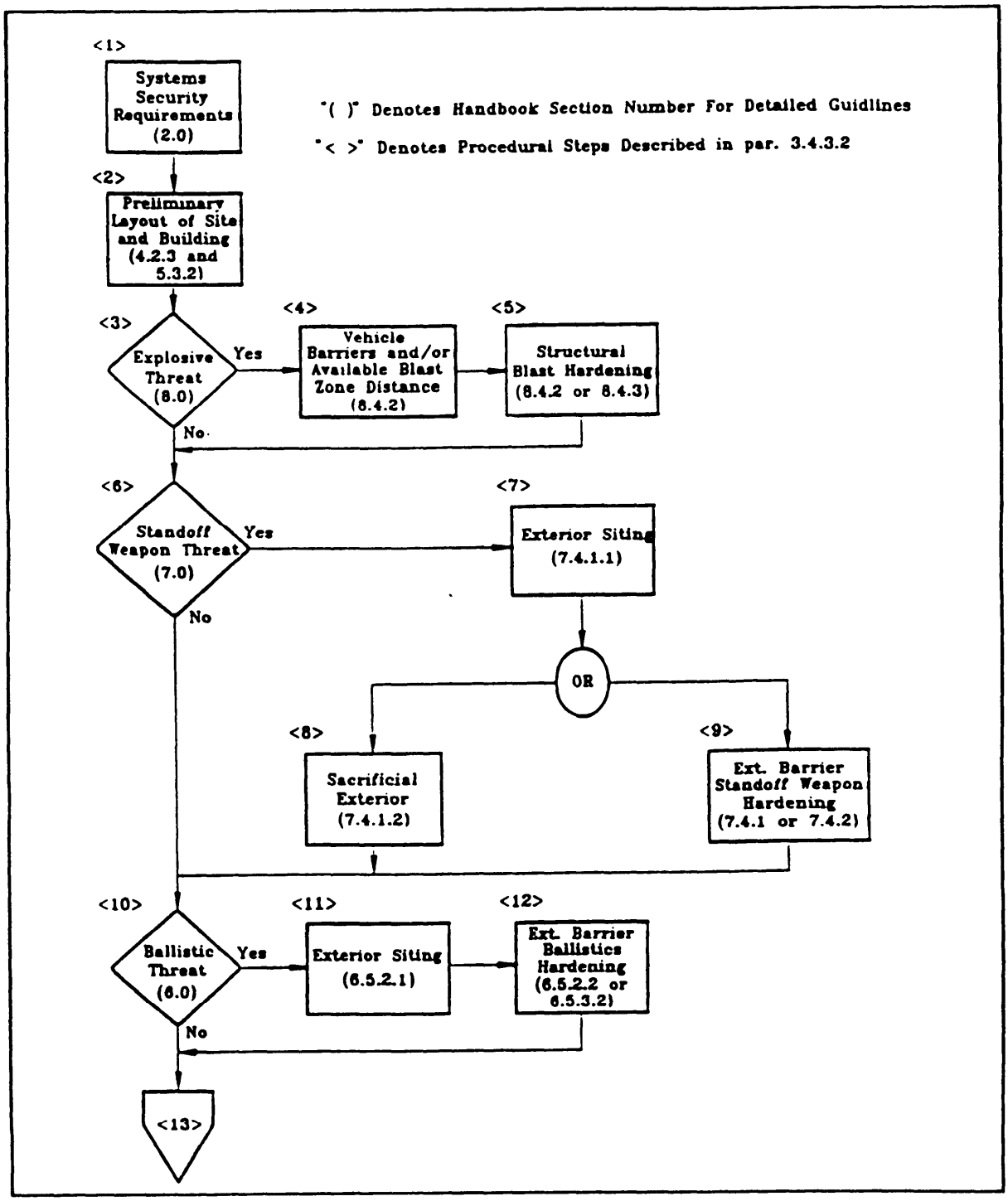


Figure 9
Detailed Design Flowchart

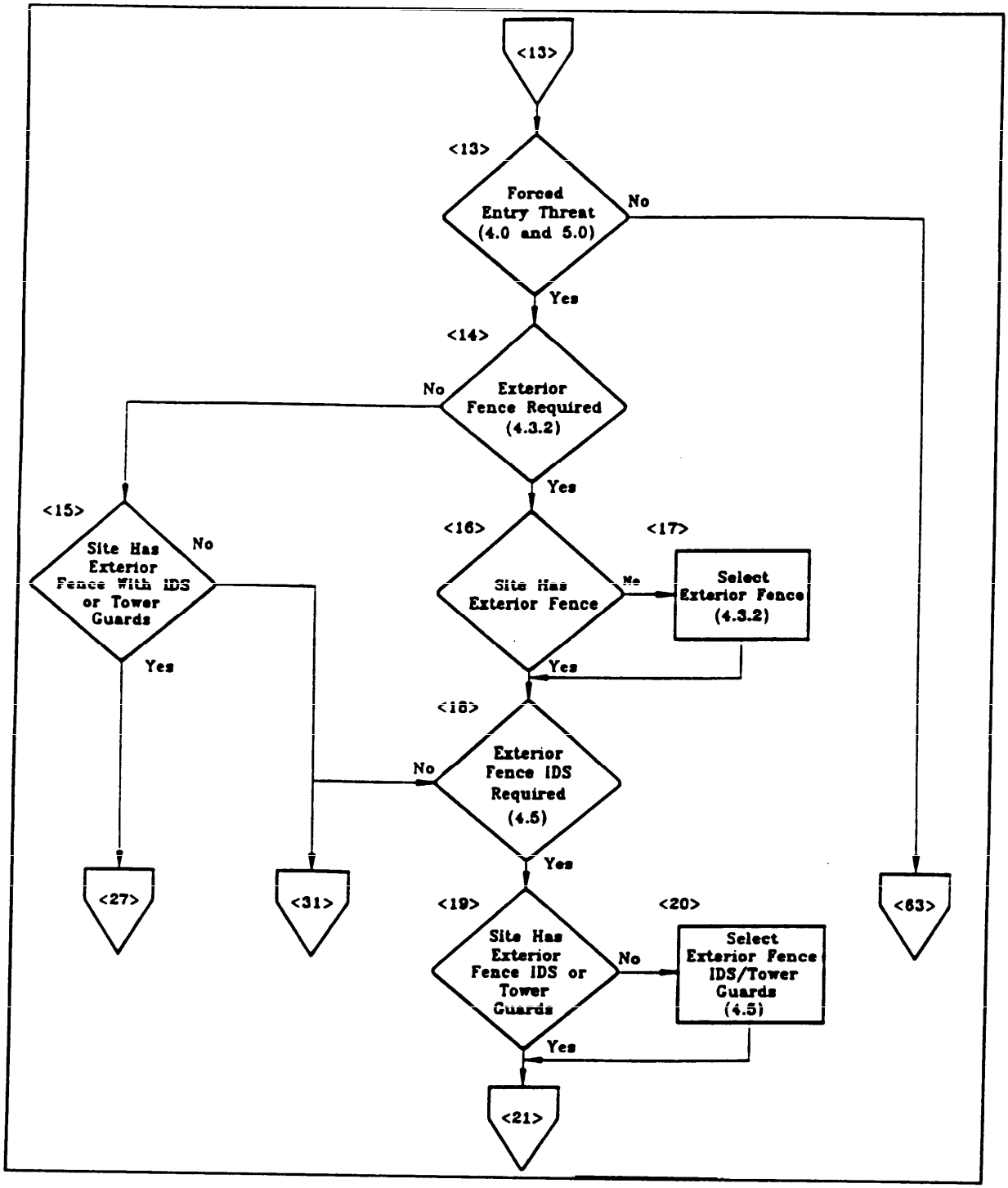


Figure 9
Detailed Design Flowchart (Continued)

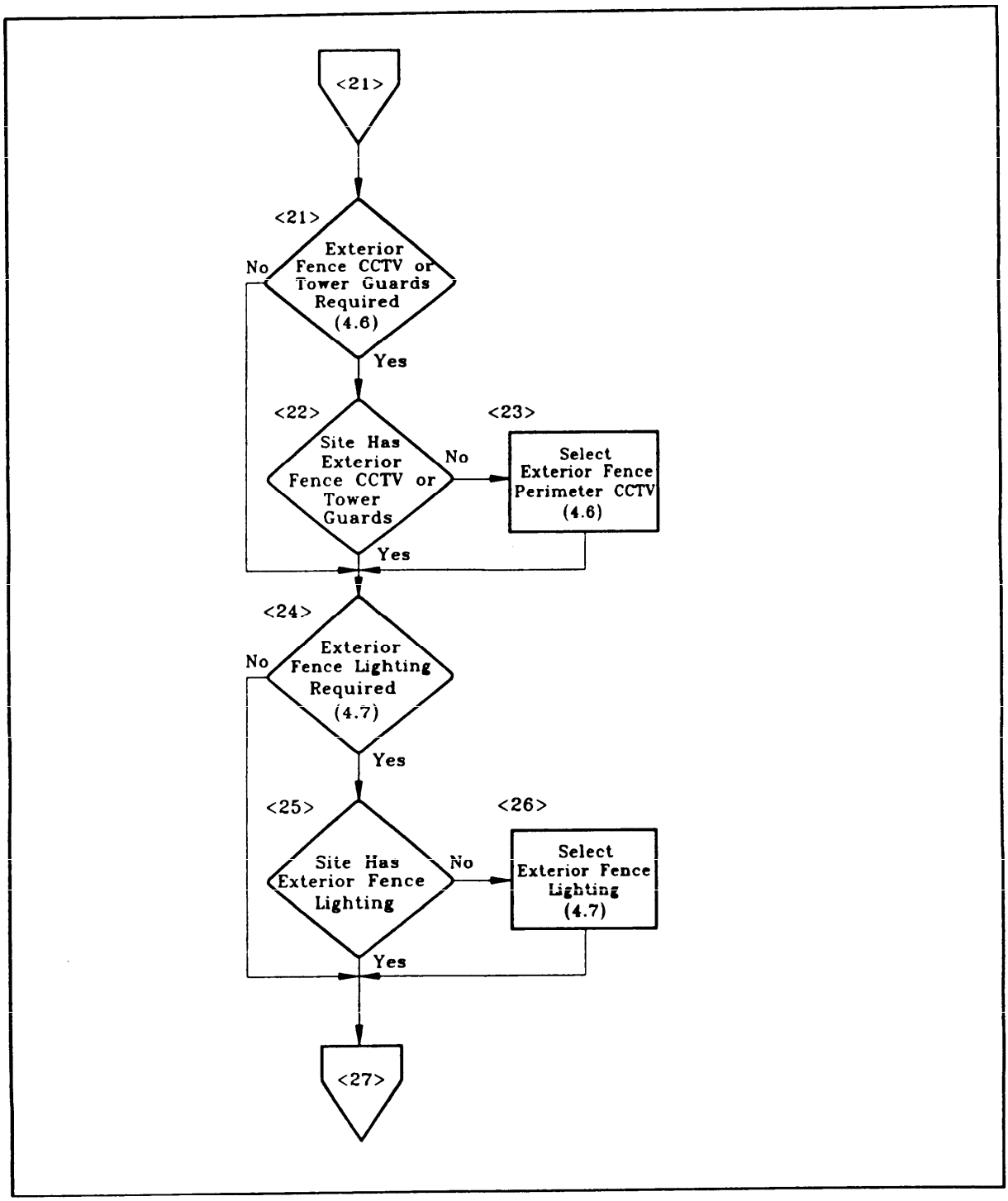


Figure 9
Detailed Design Flowchart (Continued)

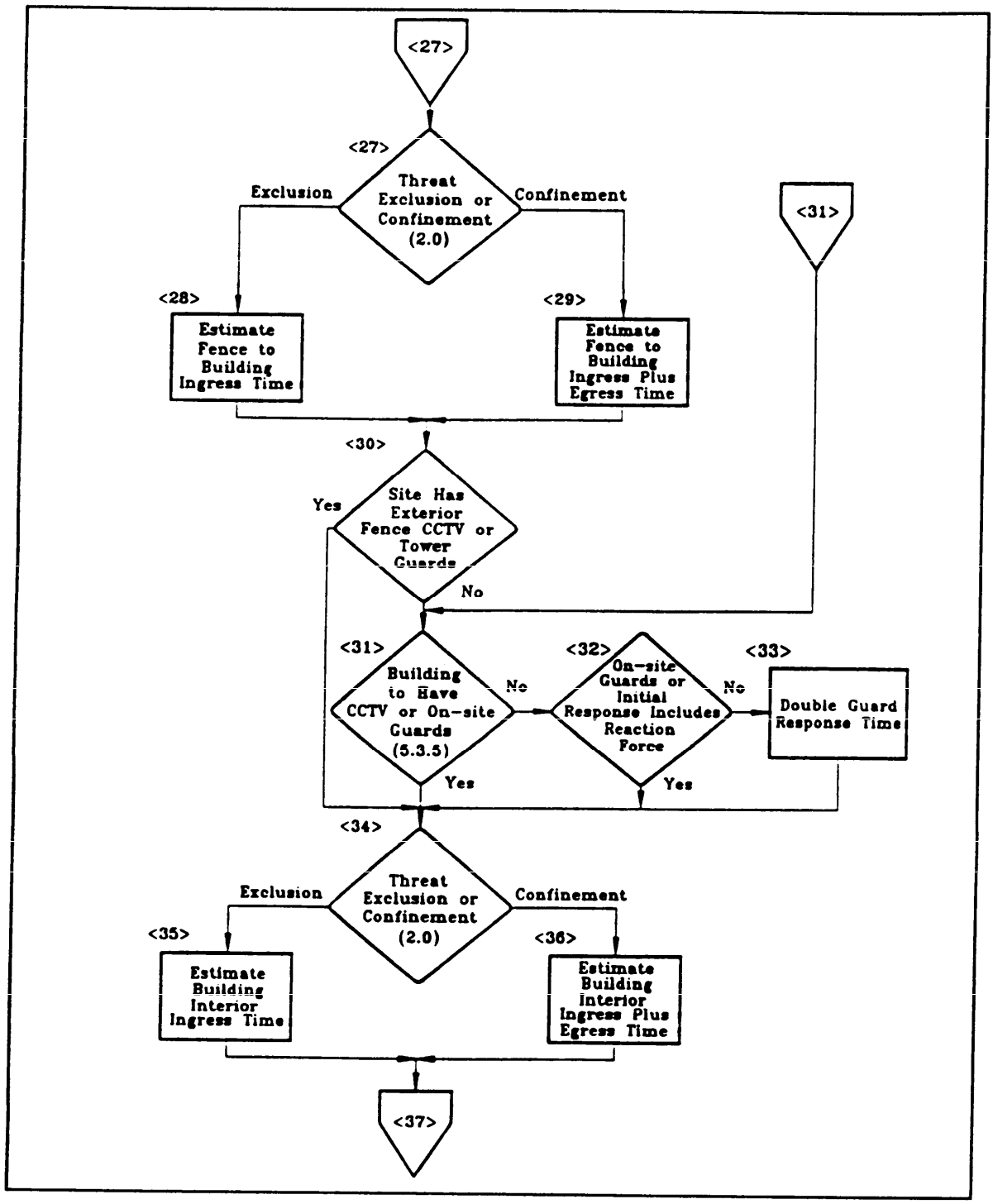


Figure 9
Detailed Design Flowchart (Continued)

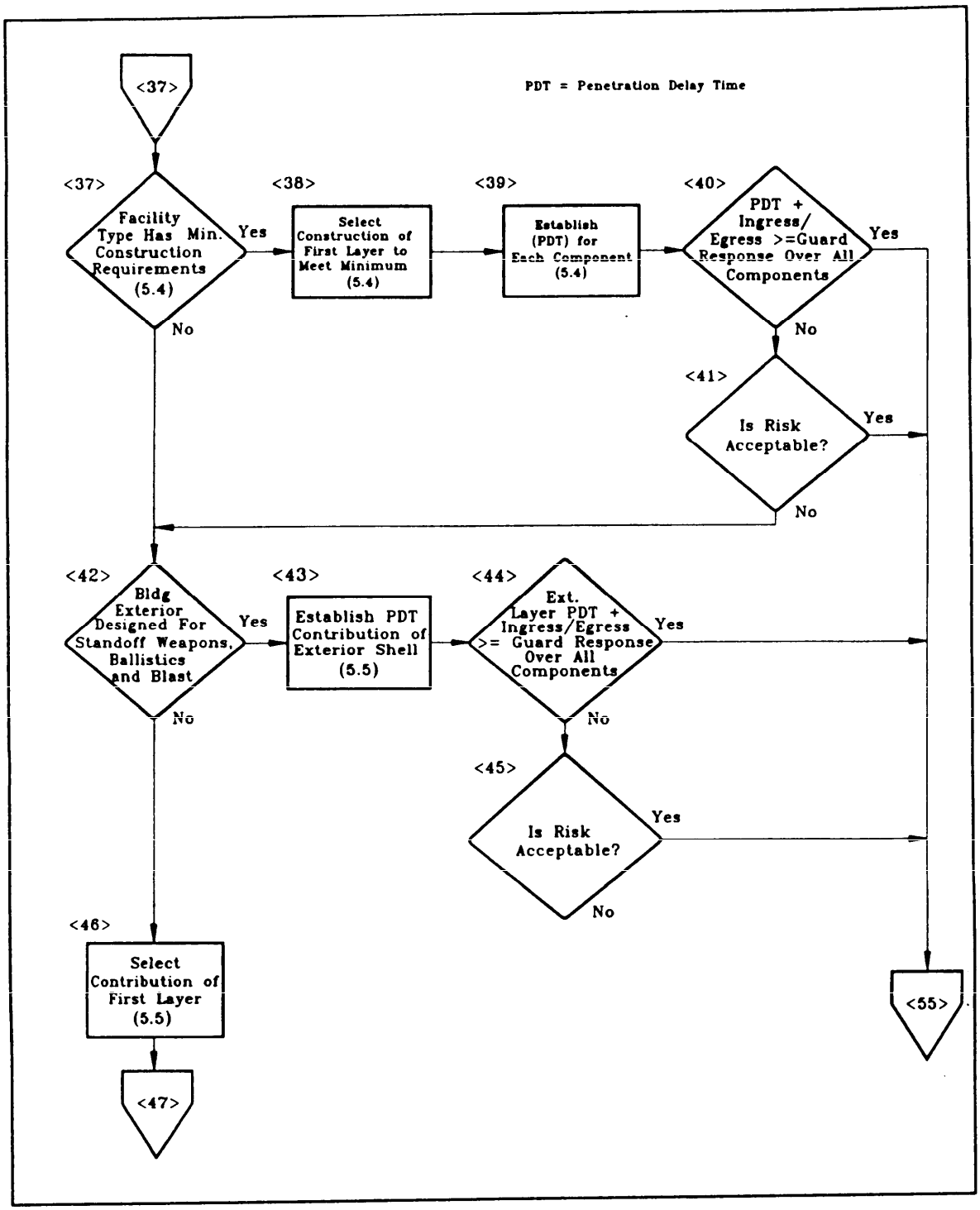


Figure 9
Detailed Design Flowchart (Continued)

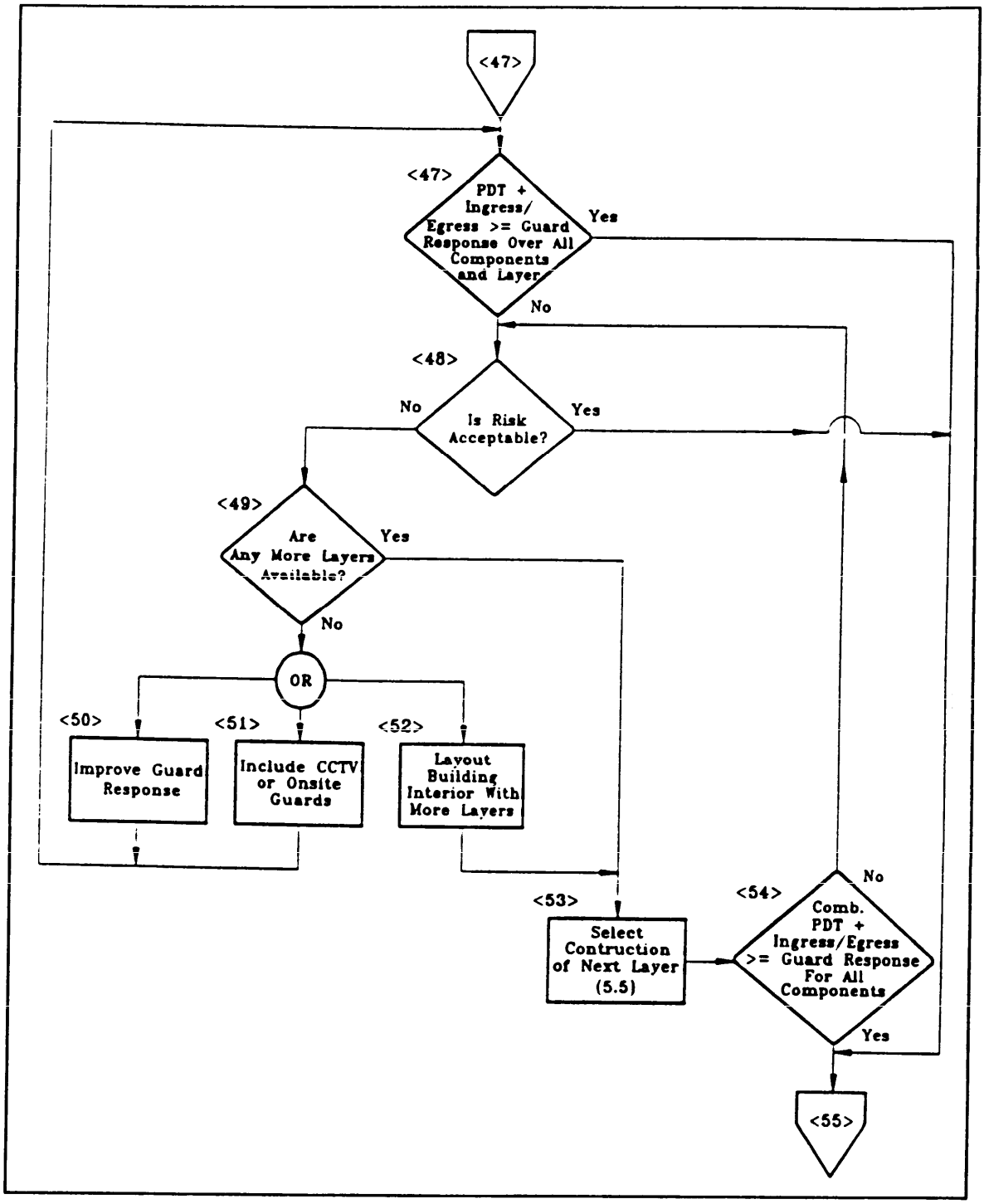


Figure 9
Detailed Design Flowchart (Continued)

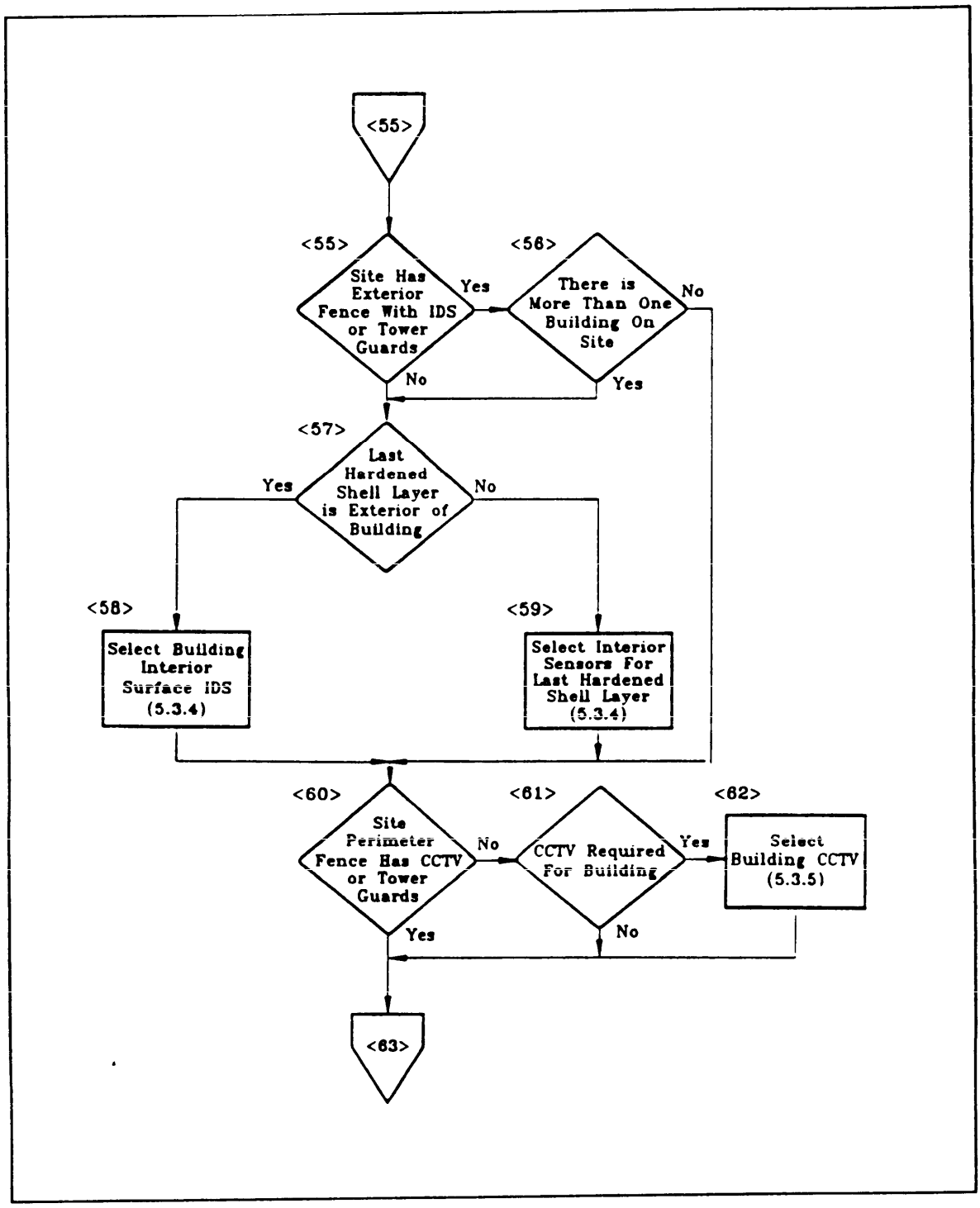


Figure 9
Detailed Design Flowchart (Continued)

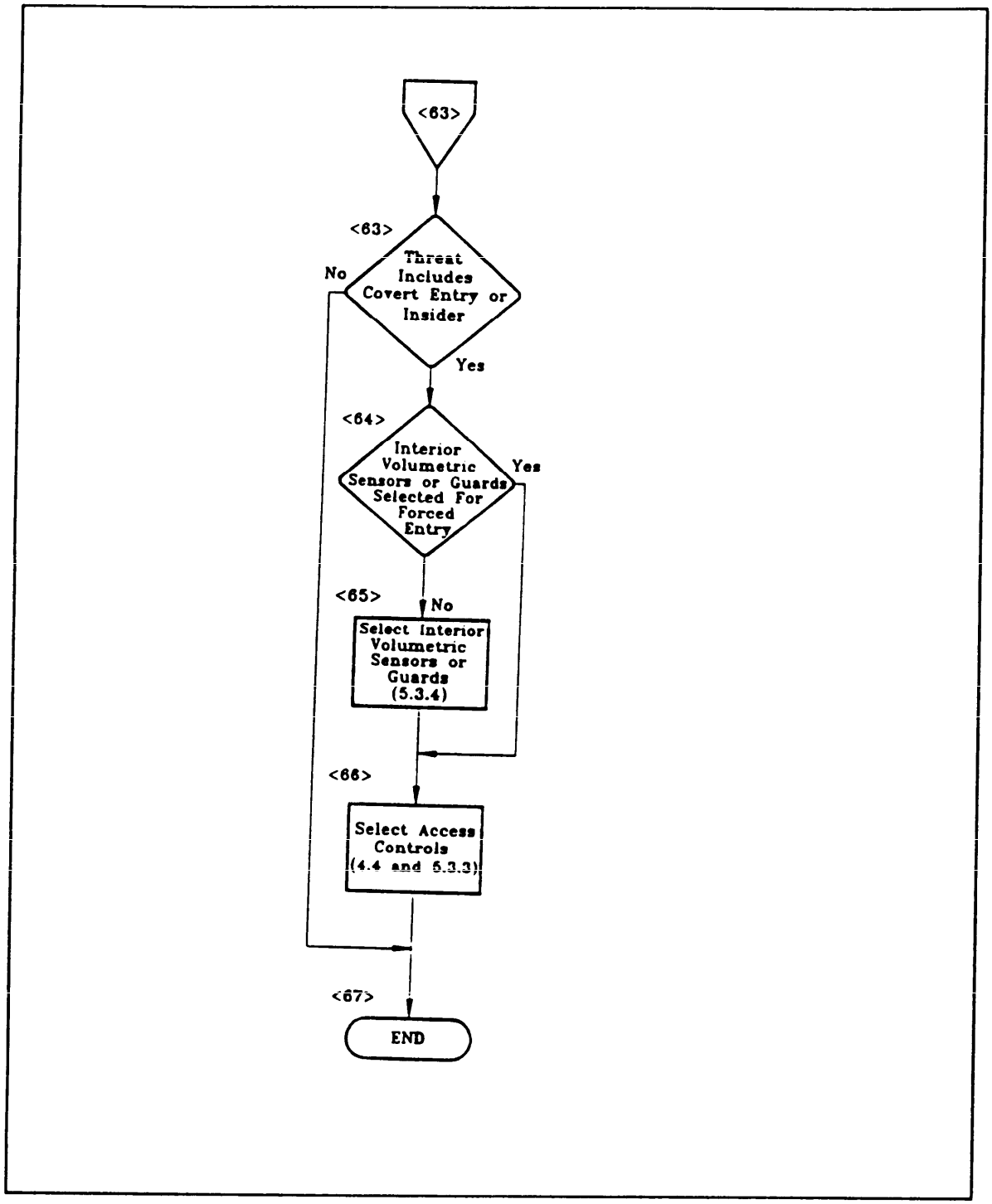


Figure 9
Detailed Design Flowchart (Continued)

3.4.3 Design Procedure

3.4.3.1 Design Worksheets. Worksheets to aid the design are contained in Appendix A. Table A-1 applies to a new facility and Table A-2 to the retrofit of an existing facility. These worksheets provide a convenient format for entering and evaluating site and building construction options with corresponding penetration times and ingress/egress times to allow comparison with the threat assessment and guard response times.

3.4.3.2 Design Activity Chart. The paragraphs that follow describe each element of the flow chart in Figure 9. The identifying number within (( )) appearing outside each box in the figure corresponds to the paragraph number below:

⟨1⟩ Establish security system requirements. The procedures outlined in Section 2 of this handbook should to followed to establish the:

a) Design threat the security system must protect against. The specific tactics and security levels should be checked under Item 3 of the worksheet (Appendix A).

b) Minimum delay time required if the design threat includes a forced entry. This should at least equal the maximum anticipated guard force response time. This time should be entered as Item 4 of the worksheet (Appendix A).

c) Other constraints and requirements. Any physical, functional, or budgetary constraints associated with the site or building that may affect the security system design. This includes the required area of the secured area, etc. (see Section 2).

⟨2⟩ Complete a preliminary layout of the exterior site and building interior. Guidelines for the layout of the site are provided in par. 4.2.3, and par. 5.3.2 for the building interior. In general, although an existing facility may already have a fixed site and interior layout, some flexibility may still be possible in adjusting this layout. If possible, new buildings should be located on the site to enhance the visual observation by guards, to limit or preferably block vantage points for line-of-site weapons, to maximize the threat ingress/egress time from the outer perimeter of the site, and/or to provide adequate blast standoff against vehicle-transported bombs. Within the building, the critical assets should be located in the smallest volume possible at a central point well within the interior of the building away from exterior walls, etc. presenting as many intermediate barriers to the intruder's path as possible (consistent with operational and functional requirements). For example, if there is a basement in the facility, the secured area should be located there. If the facility is multistoried, the secure area should be located in the approximate center away from all exterior walls roofs and floors.

⟨3⟩ Is there an explosive bomb threat? If the design threat includes explosives, the activity chart branches to Elements ⟨4⟩ and ⟨5⟩. Section 8 summarizes the procedures for selecting vehicle barriers to stop the threat at an adequate standoff as well as to design the building to sustain any resulting blast effects from that distance.

⟨4⟩ Establish vehicle barriers and available blast zone distance. Paragraph 8.4.2 summarizes design approach for the structural hardening new construction, and par. 8.4.3 does the same for retrofit against bomb blast. This includes the exterior walls, roofs, doors, windows, and frame of the building. The construction chosen for these components should be entered in the "Facility Exterior" portion of the worksheet (Appendix A).

⟨5⟩ Establish structural blast hardening. Paragraph 8.4.2 summarizes the structural hardening design approach for new construction, and par. 8.4.3 does the same for retrofit against vehicle bomb blast at the given design threat. This includes the exterior walls, roofs, doors, windows and frame of the building. The construction chosen should be entered in the "Facility Exterior" portion of the worksheet.

⟨6⟩ Is there a standoff weapon threat? If the design threat includes standoff weapons, the flow chart branches to Elements ⟨7⟩ and ⟨8⟩. Section 7 summarizes procedures for hardening a building against a standoff rocket propelled grenade (RPG) attack.

⟨7⟩ Exterior siting for standoff weapons. Paragraph 7.4.1.1 presents facility siting considerations to limit or block RPG attack sight lines.

⟨8⟩ Sacrificial exterior design for standoff weapons. Paragraph 7.4.1.2 presents guidelines for designing a sacrificial exterior shell as an option to reduce the effectiveness of an RPG attack.

⟨9⟩ Exterior barrier standoff weapon hardening for standoff weapons. Paragraphs 7.4.1 and 7.4.2 provide guidelines for designing barriers (both new and retrofit) to stop an RPG attack. The construction selected should be entered into the "Facilities Exterior" portion of the appropriate worksheet (Appendix A).

⟨10⟩ Is there a ballistics threat? If the design threat includes ballistic weapons, the flow chart branches to Elements ⟨11⟩ and ⟨12⟩.

⟨11⟩ Exterior siting for ballistic weapons. Paragraph 6.5.2.1 presents facility siting considerations to limit or block firearm attack sight lines.

⟨12⟩ Exterior barrier ballistic hardening measures. Paragraph 6.5.2.2 provides barrier hardening design options to counter a given ballistic

design threat. The construction selected should be entered into the "Facilities Exterior" portion of the appropriate worksheet (Appendix A).

⟨13⟩ Is there a forced entry threat? If the design threat includes forced entry, Elements ⟨14⟩ through ⟨62⟩ of the flow chart should be followed. If not, the chart branches to Element ⟨63⟩. Elements ⟨14⟩ through ⟨29⟩ address exterior security associated with the site on which the building is located referring to appropriate material in Section 4. Elements ⟨30⟩ through ⟨62⟩ address security associated with the building referring to appropriate material in Section 5.

⟨14⟩ Exterior fence required? In general, security fences or other barriers around the site perimeter act to deter casual intruders only. They can be easily scaled, crawled under, or cut through. A dedicated threat will be neither deterred nor significantly delayed by a perimeter barrier. Security fences may be required by DoD regulations for certain facility types, and/or to maintain an adequate blast zone for a vehicle bomb attack. Paragraph 4.3.2 provides guidance as to when security fences are required. If required, the flow chart branches to ⟨16⟩, otherwise to ⟨15⟩.

⟨15⟩ Does the site have an exterior fence with IDS or tower guards? Even though a fence may not be required by DoD regulation or otherwise, the facility may still be located in an existing fenced enclave containing other buildings. If this fence also has an IDS system or tower guards for threat detection, one can take advantage of the ingress/egress time of the threat from the fence to the building. In this case, the flow chart branches to Element ⟨26⟩, otherwise to Element ⟨31⟩.

⟨16⟩ Does the site have an exterior fence? Although par. 4.3.2 may indicate that the facility requires a fence, it may be that this facility is to be located in an existing fence enclave with other buildings. If so, the flowchart branches to Element ⟨18⟩, otherwise to Element ⟨17⟩.

⟨17⟩ Select exterior fence. For facilities requiring an exterior fence, the information contained in par. 4.3.2 can be used to aid its selection. The fence construction should be entered under "Site Perimeter" in the worksheet. In general, the penetration time through the fence is negligible (~0.1 minutes). This is already reflected in Item 9 of the worksheet. On the other hand, a fence can limit the amount of tools, etc., that can be easily transported by a threat.

⟨18⟩ Exterior fence IDS required? In general, an exterior IDS or tower guard on an extended fence perimeter around a site is costly to install and maintain. The added threat ingress/egress time gained may not justify these costs. It is generally more cost effective to limit the size of the secured area to the building and provide the hardness and threat detection there. In some cases, DoD regulations may require a fence perimeter IDS or tower guards. Paragraph 4.5 provides guidelines as to when this might be

required. If not required, the flow chart branches to Element ⟨31⟩, otherwise to Element ⟨19⟩.

⟨19⟩ Site has exterior fence IDS or tower guards? If the building requiring a fence IDS or tower guards is to be located in an existing fenced enclave already having an IDS or tower guards, the flow chart branches to Element ⟨21⟩, otherwise to Element ⟨20⟩.

⟨20⟩ Select exterior fence IDS/tower guards. Paragraph 4.5 summarizes the available perimeter fence-related threat detection options referring the user to appropriate sources for more details.

⟨21⟩ Exterior fence CCTV or tower guards required? Paragraph 4.6 provides guidelines as to when CCTV or tower guards are required along perimeter fences for threat assessment by DoD regulation.

⟨22⟩ Site has exterior fence CCTV or tower guards. If the facility requiring a site perimeter CCTV or tower guard is to be located in an existing fenced enclave already so equipped, the flow chart branches to Element ⟨24⟩, otherwise to Element ⟨23⟩.

⟨23⟩ Select exterior perimeter fence CCTV. Paragraph 4.6 summarizes the available exterior fence CCTV options referring the user to appropriate sources for more details.

⟨24⟩ Exterior fence lighting requirements. Paragraph 4.7 provides guidelines as to when lighting is required to aid threat detection and assessment along perimeter fences.

⟨25⟩ Site has exterior fence lighting? If a facility requiring a site perimeter lighting system is to be located in an existing fenced enclave already having perimeter lighting, the flow chart branches to Element ⟨27⟩, otherwise to Element ⟨26⟩.

⟨26⟩ Select exterior fence lighting. Paragraph 4.7 summarizes lighting requirements and available options.

⟨27⟩ Threat exclusion or confinement? In cases where a perimeter fence with IDS exists or is required, the designer can take advantage of the time it takes the threat to go from the fence to the facility. If the threat is to be excluded from the critical asset, the designer can only account for the ingress time from the fence to the building. If the threat is to be contained within the site, the egress time from the building to the fence can also be accounted for. For the case of threat exclusion, the flow chart branches to Element ⟨28⟩, and containment to Element ⟨29⟩.

⟨28⟩ Estimate fence-to-building ingress time. The on-foot ingress time between the fence and the building exterior can be estimated using Figure 8 using an estimate of the distance involved. The distance used should

be the shortest distance between the fence and the building measured using the preliminary site layout plan developed under Element ⟨2⟩. This ingress time should be inserted in the appropriate slot under Column E of the "Facility Exterior" portion of the applicable worksheet (Appendix A).

⟨29⟩ Estimate fence-to-building ingress plus egress time. If threat containment rather than exclusion is permitted, both the site-related threat ingress and egress time can be accounted for. The on-foot ingress time can be estimated using Figure 8. The egress time may be shorter or longer than shown in Figure 8 depending on the weight or volume of the assets being stolen. In both cases, the distance used should be the shortest between the fence and the building established using the preliminary site layout plan developed under Element ⟨2⟩. Insert the ingress and egress times in the appropriate slots under Column E of the "Facility Exterior" portion of the applicable worksheet (Appendix A).

⟨30⟩ Site has an exterior fence CCTV or tower guard? If the site already has, or is required to have, an exterior fence CCTV or tower guard, the flow chart branches to Element ⟨34⟩, otherwise to Element ⟨31⟩.

⟨31⟩ Building to have a CCTV or on-site guard? If the designer has reached this point, no CCTV or tower guards are required along the perimeter fences for threat assessment. This function must occur at the building. At this point a decision is required if threat assessment is to be accomplished by dispatching a guard to the building or by using CCTV. The advantage of using CCTV is that real-time assessment is possible from a remote monitoring location, reducing the overall security system response timeline (see Figure 5). The disadvantage is the cost for purchasing, installing and maintaining the system. Paragraph 5.3.5 summarizes CCTV options referencing appropriate sources for details. If a CCTV is to be provided, the flow chart branches to Element ⟨34⟩, otherwise to Element ⟨32⟩.

⟨32⟩ Initial response includes reaction force? If the designer has reached this point, the use of CCTV for threat assessment is not an option and one must rely on a guard responding to the location of an alarm. If the guard operating procedures allow for an on-site guard, or if the initial response includes the full reaction force to engage and counter the threat, the flow chart branches to Element ⟨34⟩, otherwise to Element ⟨33⟩.

⟨33⟩ Double guard response time. If the designer has reached this point, the dispatch of a guard is required for threat assessment before the full reaction force. The designer should double the "Minimum Delay Time Required to Match Guard Response" in Row (4) of the worksheet (Appendix A).

⟨34⟩ Threat exclusion or confinement. If the threat is to be excluded from the critical asset, one can only account for the ingress time from the building exterior to the innermost shell (Figure 6) containing the asset. On the other hand if the threat is to be contained within the building, the egress time out may also be accounted for. In the case of

threat exclusion, the flow chart branches to Element ⟨35⟩, otherwise to Element ⟨36⟩.

⟨35⟩ Estimate building interior ingress time. The on-foot ingress time between the exterior of the building and each interior shell layer can be estimated using Figure 8. The preliminary building layout plan established under Element ⟨2⟩ can be used to estimate the distances between interior layers. In general, the shortest distance should be used. It is possible that there may be some difference in the time to reach one building component relative to another. For example, attacking and entering through the ceiling of a secured area may mean added time to climb the extra floor relative to a wall or door attack. Generally, the time differences involved are small and one can use the minimum time over all components. On the other hand, a separate ingress time is required between each interior layer and the last. If there is only one interior layer (as shown in Figure 6), then only one time is required between this layer and the exterior of the building. If there are more interior layers, a separate time is required for each. These ingress times should be inserted in the appropriate slots under Column E of the "Interior Layers" portion of the new design worksheet (Table A-1) and Column H of the retrofit worksheet (Table A-2). Note in the worksheet, that Interior Layer No. 1 is the innermost layer, Interior Layer No. 2 is the next, etc.

⟨36⟩ Estimate building interior ingress plus egress time. If threat containment rather than exclusion is permitted, both the ingress into and egress out of the building can be accounted for. The on-foot ingress time can be estimated using Figure 8 with an estimate of the distance involved. The egress time may be shorter or longer than shown in Figure 8 depending on the weight or volume of the assets being stolen. The egress distance may also be different depending on the availability of doors, windows, etc., that may be opened from the inside. A separate ingress and egress time is required between each interior layer and the last. If there is only one interior layer (as shown in Figure 6), then only one time is required between this layer and the exterior of the building. If there are more interior layers, separate ingress and egress times are required for each. These times should be inserted in the appropriate slots under Column E of the "Interior Layers" portion of the new design worksheet or Column H of the retrofit worksheet appropriately. Note in the worksheet that Interior Layer No. 1 is the innermost layer, Interior Layer No. 2 is the next, etc.

⟨37⟩ Does facility type have minimum construction requirements? Minimum prescribed DoD security-related construction requirements exist for vaults and strongrooms; sensitive compartmental information facilities; arms, ammunition, and explosive facilities; and nuclear weapons facilities. If the facility being designed is one of these, the flow chart branches to Element ⟨38⟩, otherwise to Element ⟨41⟩.

⟨38⟩ Select construction of first layer to meet minimum. Paragraph 5.4 presents the minimum prescribed construction for each building component (walls, roof, floor, doors, utility opening). These should be entered into

Column C of the new construction worksheet (Table A-1) under the first layer option (which may or may not be the building exterior depending on the preliminary layout). In the case of a retrofit design, the minimum construction also applies to the first layer which may or may not be the exterior of the building depending on the layout. In some cases, a new interior layer may be required (e.g., a vault). In this case, the minimum construction should be entered in the Retrofit Worksheet (Table A-2) under "Existing" or Row C for each layer element (walls, doors, etc.).

⟨39⟩ Establish penetration delay time (PDT) for each component. The penetration delay time for each prescribed component construction should be obtained from Paragraph 5.4 and entered appropriately into Column D of the New Construction Worksheet (Table A-1) or Row D of the retrofit worksheet (Table A-2). The appropriate forced entry threat severity level identified under the Design Threat Item 3 of the worksheet should be used.

⟨40⟩ Is PDT plus ingress/egress greater than or equal to the guard response overall components? If one or more of the building component PDT plus ingress/egress times (both interior and exterior to the building) does not equal or exceed the guard response time, additional delay is required. In this case, the flow chart branches to Element ⟨41⟩, otherwise to Element ⟨55⟩.

⟨41⟩ Is risk acceptable? If the PDT plus ingress/egress times for one or more of the building components does not equal or exceed the guard response, the designer should decide if the risk is acceptable considering other factors such as the cost of additional hardening, etc.

⟨42⟩ Has the building exterior been designed for blast, standoff weapons, or ballistics? If the facility exterior has been previously designed with specific construction identified under "Facility Exterior" in the worksheet, the flow chart branches to Element ⟨43⟩ to establish the forced entry penetration delay offered, otherwise to Element ⟨46⟩.

⟨43⟩ Establish PDT contribution of exterior shell. The PDT data for each component should be obtained from par. 5.5 for new construction, or par. 5.6 for existing and retrofit construction, and entered appropriately into Column D under "Facility Exterior" of the worksheet for new construction (Table A-1) or Row D and F for existing and retrofit construction (Table A-2).

⟨44⟩ Is exterior layer PDT plus ingress/egress times greater than or equal to the guard response over all components? If one or more of the exterior layer component PDT (Column D in Table A-1, Column G in Table A-2) plus ingress/egress times (both interior and exterior to the building) does not equal or exceed the guard response time, additional delay is required. In this case, the flow chart branches to Element ⟨45⟩, otherwise to Element ⟨55⟩.

⟨45⟩ Is risk acceptable? If the PDT plus ingress/egress times for one or more of the building components does not equal or exceed the guard response, the designer should decide if the risk is acceptable considering other factors such as the cost of additional hardening, etc.

⟨46⟩ Select construction of first layer. If the designer reaches here, it means: (a) the minimum prescribed construction of the innermost layer for one or more building components does not meet delay time requirements; (b) one or more components of the exterior layer design for blast, standoff weapons, etc., does not meet minimum delay time requirements; (c) inner and exterior layers in combination do not meet delay time requirements; or (d) there is no previously prescribed inner or exterior layer construction and the design must start at this point. The data in par. 5.5 provides design options and PDT for new construction and par. 5.6 for existing and retrofit construction. These should be selected and entered appropriately into Columns C and D of the worksheet for new construction (Table A-1) and Rows C, D, E, and F for each component for retrofit construction (Table A-2). If possible, one should identify those choices that achieve an equivalent penetration time over all building components, i.e., walls should be about equally as hard as the roof, doors, etc. In some cases, the use of multiple doors may be required as shown in Figure 10.

⟨47⟩ Is the PDT plus ingress/egress time greater than or equal to the guard response time for all components and layers? If one or more of the building component penetration (Column D for Table A-1, Column 6 for Table A-2) plus ingress/egress times (both interior and exterior to the building) does not equal or exceed the guard response time, additional delay is required. In this case, the flow chart branches to Element ⟨48⟩, otherwise to Element ⟨55⟩.

⟨48⟩ Is risk acceptable? If the penetration delay plus ingress/egress times for one or more of the building components does not equal or exceed the guard response, the designer should decide if the risk is acceptable considering other factors such as the cost of additional hardening, etc.

⟨49⟩ Are any more layers possible? If the preliminary layout of the building permits more layers to be hardened to achieve the needed delay, the flow chart branches to Element ⟨53⟩, otherwise to Elements ⟨50⟩, ⟨51⟩, or ⟨52⟩. Here, the designer has the option of redesigning the layout of the building interior (Element ⟨52⟩), reevaluating the guard operating procedure to reduce the response (Element ⟨50⟩), or adding CCTV to reduce the threat assessment time (Element ⟨51⟩).

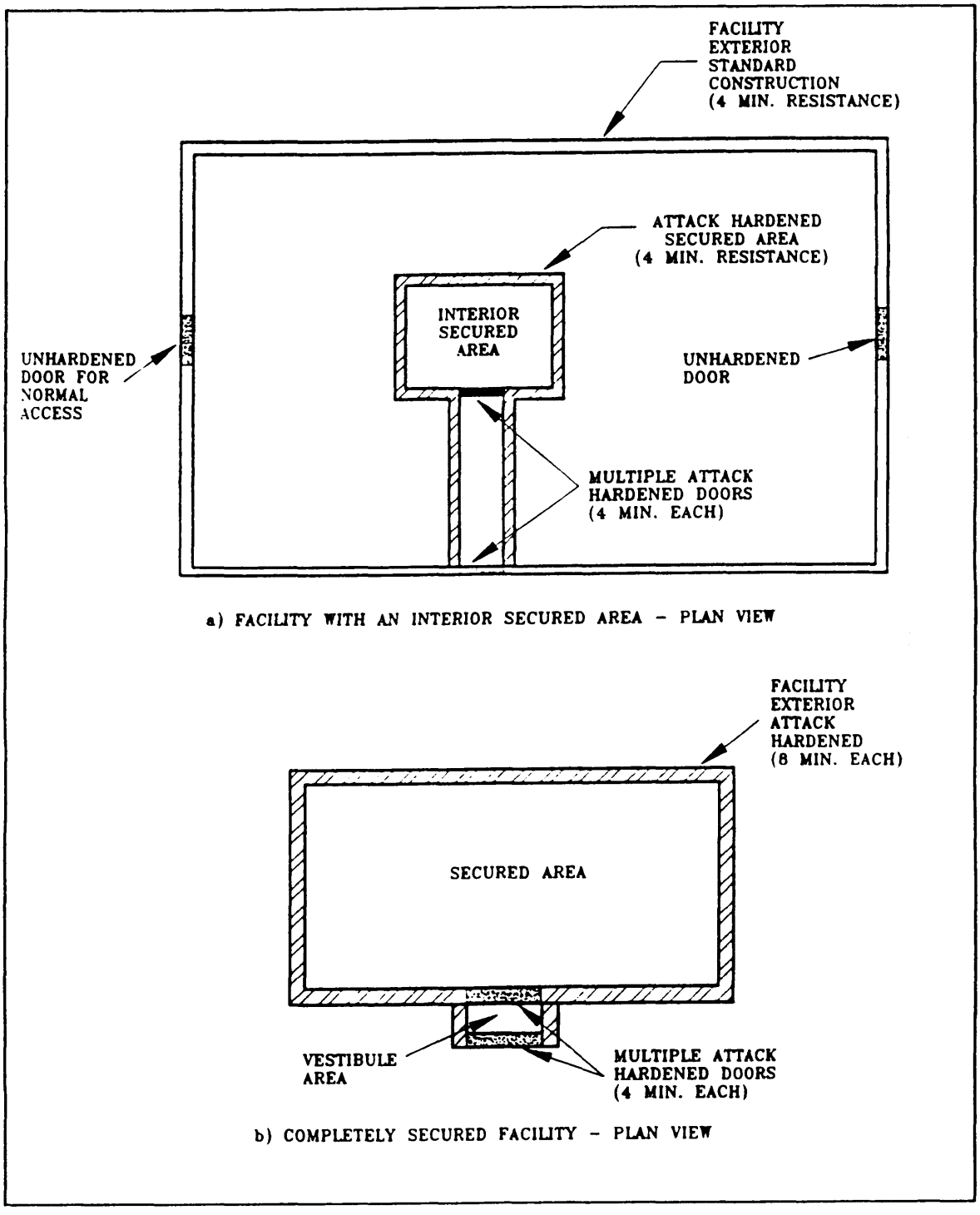


Figure 10
Multiple Barrier Designs

⟨50⟩ Improve guard response time. This may be accomplished by: (a) adding an on-site guard to reduce threat assessment timelines, (b) sending the reaction force on alarm instead of an assessment guard, or (c) seeking other ways of improving the guard response. The response time should be reduced in Item 4 of the worksheet appropriately and the designer should return to Element ⟨47⟩, above.

⟨51⟩ Include CCTV or on-site guard? If not already included, CCTV or on-site guard may be added at the first point of threat detection to reduce threat assessment times. If this is possible, the response time can be reduced in Row 4 of the worksheet by a factor of two and the designer can return to Element ⟨47⟩, above.

⟨52⟩ Re-layout building interior to provide more layers. The preliminary layout can be changed to provide more layers between the building exterior and interior. For example, if a single floor separates the secured area from the ground floor of a multistory building and delay time requirements cannot be met, consider relocating the secured area higher in the building, forcing the intruder to penetrate two or more intermediate floors. To protect the secure area, delay requirements for some components like walls may be achieved without using multiple barriers, while other components, such as doors, may require a multiple barrier approach. A design approach where multiple barriers are placed between the exterior shell of the building and an interior space containing the secured resources is illustrated in Figure 10. If possible, the added layers should be introduced and the designer can move on to Element ⟨53⟩.

⟨53⟩ Select construction of next layer. The construction of the next layer should be selected using the data in par. 5.5 and entered appropriately into Columns C and D of the Worksheet for new construction, or par. 5.6 and Rows C, D, E and F of the worksheet for retrofit construction.

⟨54⟩ Is the combined PDT plus ingress/egress time greater than or equal to the guard response time for all components and layers? If one or more of the building component PDT plus ingress/egress times (both interior and exterior to the building) does not equal or exceed the guard response time, additional delay is required. In this case, the flow chart branches to Element ⟨55⟩, otherwise to Element ⟨48⟩.

⟨55⟩ Does site have an exterior fence with IDS or tower guards? The segment of the flow chart beginning with this element is concerned with the proper selection of an intrusion detection system that takes full advantage of the delay times offered by the barriers. As noted, intruder detection must occur at or before a barrier for it to be considered in the timeline calculation. If the site has perimeter IDS or tower guards, the timeline starts at that point and the flow chart branches to Element ⟨56⟩, otherwise to Element ⟨57⟩.

operation in the event of malfunction.

⟨56⟩ Is there more than one building on site? If there is only one building on site, the flow chart branches to Element ⟨60⟩ since no further IDS is required (i.e., the fence IDS is sufficient). On the other hand, if there are many buildings within a fence enclave, IDS may be required at or within the building to identify which one may be under attack.

⟨57⟩ Is the last hardened shell layer the exterior of the building? If reliance on the delay is offered by the exterior shell of the building, a building interior surface IDS system capable of detecting an intruder before penetration is required. In this case, the flow chart branches to Element ⟨59⟩, otherwise to Element ⟨60⟩.

⟨58⟩ Select building interior surface IDS. If the designer has reached this point, an interior surface IDS capable of detecting an intruder before penetration of the exterior shell of the building is required. These IDS options are addressed in par. 5.3.4.

⟨59⟩ Select interior sensors for last hardened shell. If the designer has reached this point, an interior IDS capable of detecting an intruder before penetrating the last hardened interior shell layer of the building is required. Paragraph 5.3.4 addresses IDS options for this case.

⟨60⟩ Does site perimeter fence have CCTV or tower guards? If it was determined earlier that the perimeter fence has CCTV or tower guards for threat assessment, the flow chart branches to Element ⟨63⟩, otherwise to Element ⟨61⟩.

⟨61⟩ Does building require CCTV? If it was determined earlier that the building requires CCTV to reduce threat assessment related timelines, the flow chart branches to Element ⟨62⟩, otherwise to Element ⟨63⟩.

⟨62⟩ Select building CCTV. Paragraph 5.3.5 summarizes the CCTV selection guidelines and refers the designer to other sources for more detail.

⟨63⟩ Does threat include covert entry/insider? If not, the flow chart branches to Element ⟨67⟩, otherwise to Element ⟨64⟩.

⟨64⟩ Have volumetric interior sensors been selected for forced entry? A covert entry or insider threat implies that forced entry tactics are not used to enter a facility. In this case, interior IDS located on the barrier surface may not be effective. Volumetric interior sensors or on-site guards are required to detect such threats. If these were selected earlier, the flow chart branches to Element ⟨67⟩, otherwise to Element ⟨66⟩.

⟨65⟩ Select volumetric interior sensor or guards. Paragraph 5.3.4 summarizes the volumetric interior sensor options referencing the designer to other sources for more details as necessary. If on-site building guards are to be used, the designer can go directly to Element ⟨66⟩.

⟨66⟩ Select access control. Paragraph 4.4 summarizes access control options for the site perimeter, and par. 5.3.3 does so for the building, referring the designer to other sources for more details.

⟨67⟩ End. This element ends the design process for new facilities.

Section 4: EXTERIOR SITE-RELATED PHYSICAL SECURITY

4.1 Introduction. Exterior physical security addresses the outermost elements of a physical security system lying between the site perimeter and the facility containing the assets to be protected. Exterior physical security contributes to the effectiveness of an integrated security system design in the choice of: (1) site layout including facility location relative to fences and vehicle barriers to enhance protection against forced-entry, bomb blast, standoff weapons, and ballistic threats; (2) access control at site points of entry to protect against covert entry threats; (3) exterior intrusion detection sensor or guards to detect perimeter crossover points; (4) CCTV or guards to assess an alarm as a threat; and (5) security lighting to support the threat detection and assessment functions. The following pages provide design guidelines related to each of the above elements: par. 4.2 addresses exterior site layout; par. 4.3, site perimeter fences and vehicle barriers; par. 4.4, site access control; par. 4.5, exterior IDS; par. 4.6, CCTV for threat assessment; and par. 4.7, security lighting. Finally, par. 4.8 addresses essential functions that must be maintained to support all the above elements.

4.2 Exterior Site Work and Layout

4.2.1 Introduction. This section provides design guidelines related to the exterior layout of the site. Only general guidelines can be provided. The application of these general principles to a specific facility must be governed by site-specific factors. Figure 11 provides a checklist of minimum site work measures applicable to any facility regardless of the design threat. The following pages provide more details on these and other important factors. Considerations related to exterior site work include those applicable to the entire installation and those appropriate to a specific facility.

4.2.2 Installation-Wide Security Considerations.

4.2.2.1 Existing Site Security. Although it is highly desirable that the site work incorporate security considerations from the start, doing so may not always be possible. The security designer may find situations where an existing site layout will influence security measures rather than security considerations influencing layout. The security associated with a given facility must be compatible with the military installation's overall security plan including existing security resources and operating procedures. This includes the location and type of: (1) surveillance guard posts and patrols; (2) security response forces; (3) intrusion detection systems; and (4) site-related access control at points of entry. Any existing security should be reviewed and adjusted to enhance the overall surveillance opportunities and to facilitate the guard response to the facility under consideration.

Figure 4

1. Eliminate potential hiding places near the facility.
2. Provide unobstructed view around the facility.
3. Site facility within view of other occupied facilities on installation.
4. Locate assets stored on site outside of the facility within view of occupied rooms of the facility.
5. Minimize need for signage or other indications of asset locations.
6. Minimize exterior signage which may indicate location of assets.
7. Provide adequate facility separation from installation boundary.
8. Eliminate lines of approach perpendicular to building.
9. Minimize vehicle access points.
10. Eliminate parking beneath facilities.
11. Locate parking as far from facility as practical.
12. Illuminate building exterior or exterior sites where assets are located.
13. Secure access to power/heat plants, gas mains, water supplies, electrical service.
14. Locate public parking areas within view of occupied rooms on facilities.
15. Locate construction staging areas away from asset locations.
16. Site facility away from vantage points.
17. Locate the facility away from natural or manmade vantage points.

Figure 11
Checklist of Minimum Site Work Protective Consideration

4.2.2.2 Collocate Facilities of Similar Asset Criticality On Site. Where possible, facilities with assets subject to similar risk should be collocated on the site as shown in Figure 12. Similar security measures can be implemented for these areas having a similar risk. If it can be achieved, collocation reduces costs and improves security effectiveness and efficiency.

electromagnetic waves

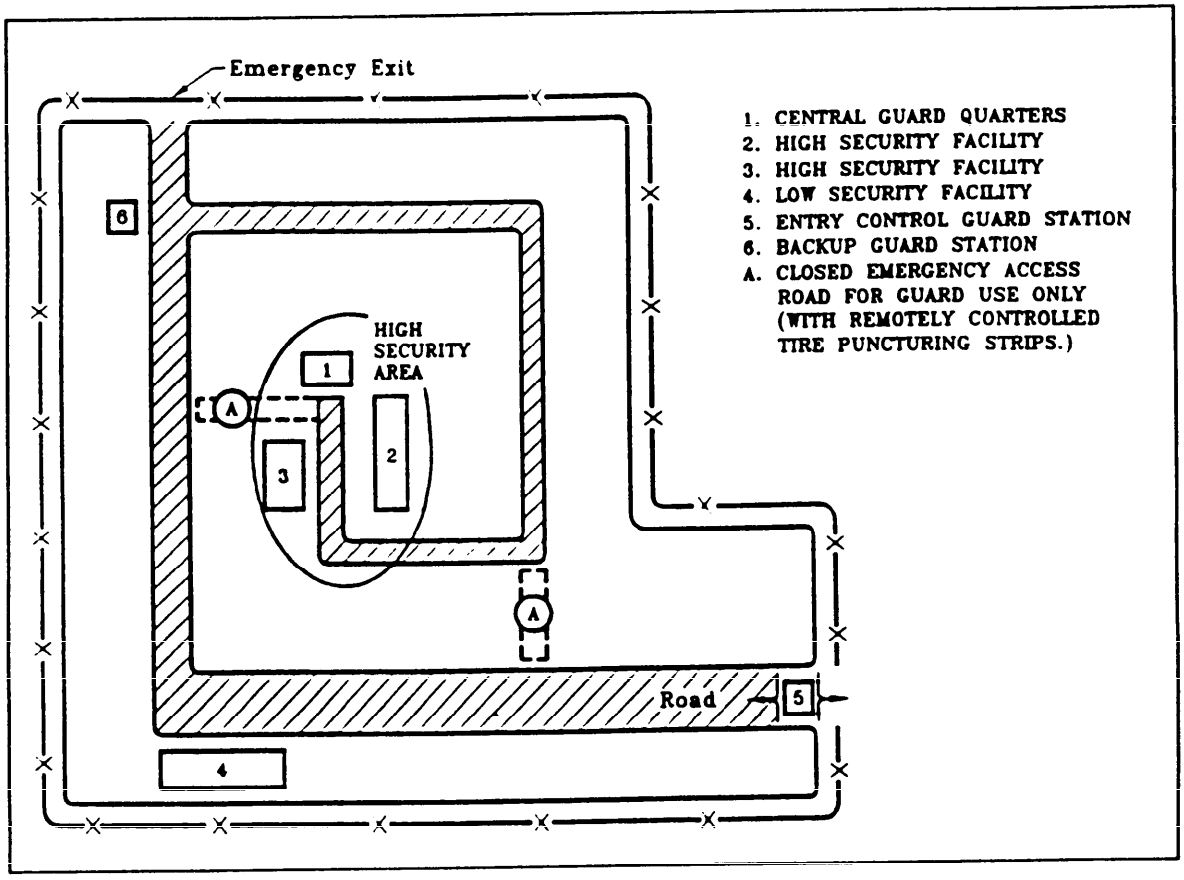


Figure 12
Example of Collocating Facilities of Similar Criticality

4.2.2.3 Routes of Travel. Regulation and direction of routes of traffic on the military installation should be controlled. These routes include pedestrian paths and vehicular road networks. It is desirable to route unauthorized, unofficial traffic away from high-risk protected areas, such as storage magazines. On the other hand, it may be desirable to route as much traffic as possible along main thoroughfares that serve facilities with high traffic densities during duty hours, such as warehouses. In the latter case, the potential observation of intruders by passers-by during nonduty hours might enhance deterrence and identification of intruders. Road networks and facility layout must also account for the needs of the security roving patrols and response forces. For example, multiple approaches to the facility should be available to minimize the predictability of response forces using the same route of approach for either surveillance or response. Access paths to all points around the facility should be provided to allow for intruder assessment and interdiction. The path identified as A in Figure 12 is intended to function in this manner.

4.2.2.4 Security Area Designation. DoD 5200.8-R indicates that different areas and tasks require different degrees of security interest depending upon their purpose, nature of the work performed within and information and/or materials concerned. For similar reasons, different areas within an activity may have varying degrees of security importance. To address these situations and to facilitate operations and simplify the security system, a careful application of restrictions, controls, and protective measures commensurate with varying degrees or levels of security importance is essential. In some cases, the entire area of an activity may have a uniform degree of security importance requiring only one level of restriction and control. In others, differences in the degree of security importance will require further segregation of certain security interests.

1) Designated Areas. Areas are to be designated as either restricted areas or nonrestricted areas. Restricted areas are established in writing by a commanding officer within his/her jurisdiction. These areas are established "pursuant to lawful authority and promulgated pursuant to DoD Directive 5200.8, dated 25 April 1991. Commanding officers are to publish in writing and inform the provost marshal of all areas under his/her control that are designated as vital to or of substantial importance to national security.

2) Restricted Areas. Three types of restricted areas are established in descending order of importance: Level Three, Level Two, and Level One. All restricted areas should be posted simply as Restricted Areas so as not to single out or draw attention to the importance or criticality of an area. While restricted areas often pertain to the safeguarding of classified information, there are other valid reasons to establish restricted areas to protect security interests (e.g., mission sensitivity; protection of certain unclassified chemicals, precious metals, or precious-metal-bearing articles; conventional arms, ammunition, and explosives; funds; drugs; nuclear material; sensitive or critical assets; or articles having high likelihood of theft).

(a) Level Three (Formerly Exclusion Area). Level Three is the most secure type of restricted area. It may be within a less secure restricted area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause grave damage to the command mission or national security. Access to the Level Three restricted area constitutes, or is considered to constitute, actual access to the security interest or asset.

(b) Level Two (Formerly Limited Area). Level Two is the next most secure type of restricted area. It may be inside a Level One area, but is never inside a Level Three area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause serious damage to the command mission or national security. Uncontrolled or unescorted movement could permit access to the security interest.

units separated so that all the

(c) Level One (Formerly Controlled Area). Level One is the least secure type of restricted area. It contains a security interest which if lost, stolen, compromised, or sabotaged would cause unidentifiable damage to the command mission or national security. It may also serve as a buffer zone for Level Three and Level Two restricted areas, thus providing administrative control, safety, and protection against sabotage, disruption, or potentially threatening acts. Uncontrolled movement may or may not permit access to a security interest or asset.

4.2.3 Facility-Specific Exterior Site Layout. The facility should be located on site considering the minimum guidelines summarized in Figure 11. In general, the layout should: (1) provide an adequate blast standoff distance if the design threat includes vehicle-transported bombs, (2) limit or preferably block all sightlines from potential vantage points if the design threat includes line-of-sight standoff or ballistic weapons, (3) maximize the threat ingress/egress time across the exterior site, and (4) enhance the possibility of threat visual observation and interdiction by on-site-stationed or responding guards.

4.2.3.1 Maintaining an Adequate Standoff Blast Zone for Vehicle Bomb Threats. A blast zone is a controlled area that surrounds a facility by a set standoff distance. This standoff distance limits structural damage to the facility if a bomb explodes at that distance. Examples are shown in Figure 13. Vehicular access to a blast zone should be limited only to vehicles operated by the handicapped or maintenance and delivery personnel. This implies adequate entry control into the blast zone where these vehicles can be searched and cleared. Discussion of related exterior barriers and entry control is discussed in pars. 4.3 and 4.4. The required standoff distance associated with the blast zone is directly related to the facility construction and the amount of explosive. This is discussed in Section 8.

4.2.3.2 Limit or Blocking Against Direct Line-of-Sight Weapons. The facility should be sited to limit, or preferably block, attack sightlines from potential vantage points. Options include: (1) the use of natural or manmade obstructions such as trees, fences, land-forms or buildings to obscure sight paths; (2) sighting the facility at a high point, if possible, to force aggressors to fire up toward the target; and (3) causing the threat to strike protective surfaces at an angle, reducing the effectiveness of the attack. Specific standoff weapons and ballistic attacks design options are addressed in Sections 6 and 7, respectively.

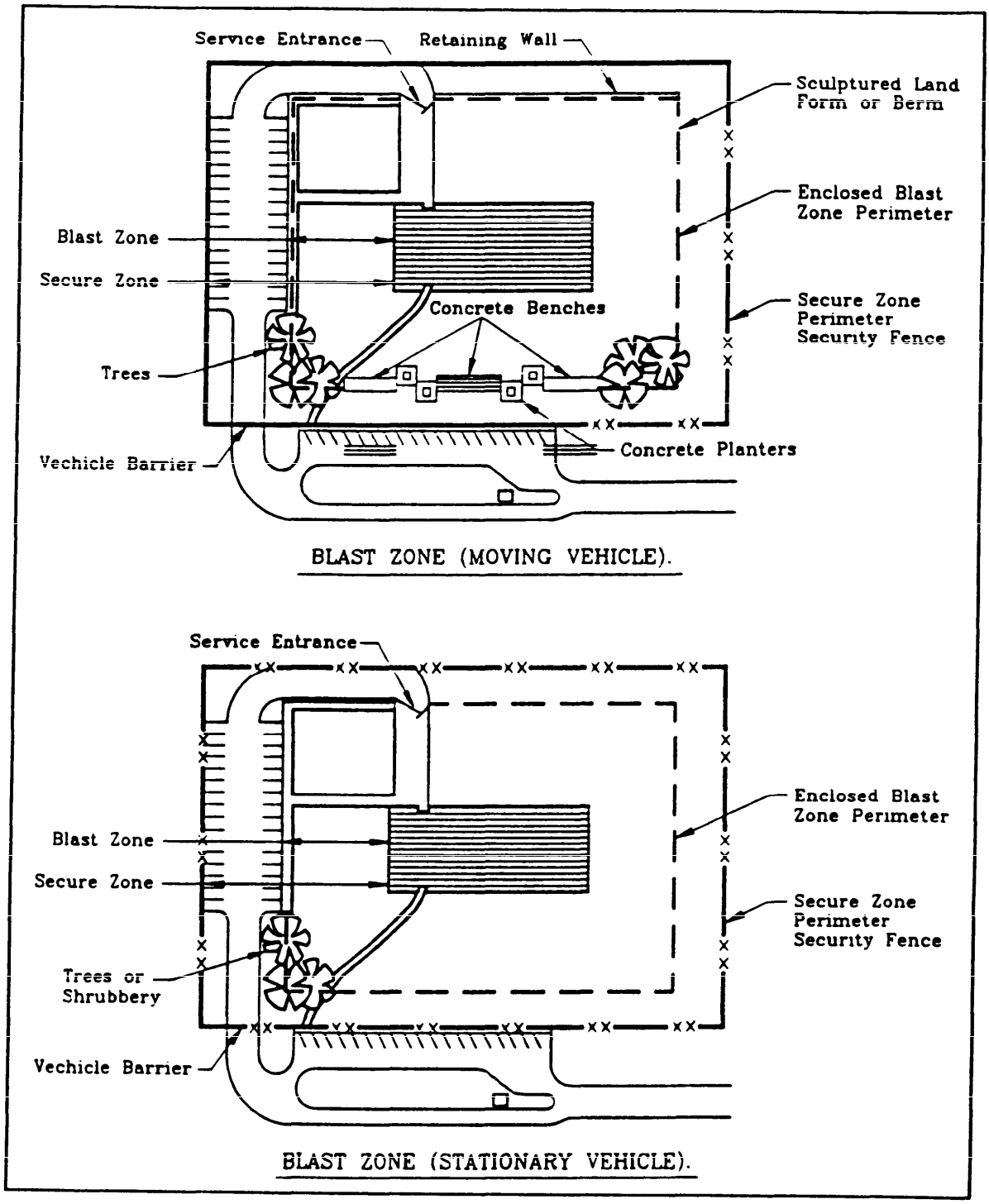


Figure 13
Exterior Site Blast Zone

4.2.3.3 Maximize Exterior Site Forced-Entry Threat Ingress/Egress Distances. In all cases, it is best to locate the facility as far away from installation perimeters as possible. This is the case whether threat detection occurs at the site perimeter or not. Therefore, locating the facility has a deterrent effect making the intruder's job more difficult and enhancing the possibility of being observed. To allow one to account for the exterior-site-related threat ingress/egress in the timeline analysis requires locating guards in towers or deploying sensors along extended site perimeter fence lines. As discussed in par. 3.2.6, this option typically involves high operating costs or (in the case of sensors) high initial purchase, as well as installation and maintenance costs. The cost effectiveness of this must be weighed against the added cost and the intruder ingress/egress time gained relative to the alternative of hardening the building more and installing IDS in a smaller area at or within the building. Paragraph 4.3.2.(2)(b) shows the time to penetrate or climb over a fence is only a few seconds and Figure 8 shows ingress/egress times of less than a minute for site distances up to 400 feet. Installing exterior fence IDS over extended perimeters is not cost effective if only a small amount of additional delay time is gained. It is recommended only if required by DoD regulation. Exterior perimeter IDS options are discussed in par. 4.5.

4.2.3.4 Maintaining Clear Zones for Guard and/or CCTV Observation. In restricted areas the facility should be sited to assure that extended, well-lighted clear zones are maintained surrounding restricted area fences and building exteriors where threat detection and assessment by guards or IDS and CCTV are required. This includes the elimination of all plantings, trees, and shrubs likely to grow over 8 feet (2.4 m) in height as well as any other manmade obscuring features on the site. Minimum clear zone requirements prescribed by military regulation follow.

1) DoD 5210.41-M - Nuclear Weapons Security Manual (Paragraph 3-300). Requires clear zones that extend 30 feet (9.1 m) on the outside and the inside of the perimeter fence when a single fence is used; and 30 feet (9.1 m) on the outside of the outer fence, the entire area between the two fences and 30 feet (9.1 m) inside the inner fence.

2) DoD 5100.76-M - Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (Paragraph 501i). Requires clear zones 20 feet (6.1 m) on the outside and 30 feet (9.1 m) on the inside of the perimeter fence.

4.3 Exterior Site Perimeter Barriers

4.3.1 Introduction. Exterior site fences and vehicle barriers are those located on the perimeter of the site. The following addresses each.

4.3.2 Security Fences

1) Function. A security fence serves the following functions:

a) Restricted area boundary definition. Fences are used to define the outermost boundary of a restricted area to deter accidental or casual intruders from entering.

b) Surveillance region definition. When required by a DoD regulation, fences are used to define the surveillance region of an exterior intrusion detection system (IDS or guards), an assessment system (CCTV or guards), and associated exterior security lights.

c) Timeline initiation. In conjunction with any required exterior perimeter guards or IDS system, fences cause a dedicated forced-entry threat to initiate an overt action which starts the timeline for the security system response.

d) Traffic control. Fences are used to channel and control the flow of personnel and vehicles through designated entries into the site.

2) Security Fence Types

a) Design options. Table 6 and Figure 14 present examples of security fence configuration. In general, security fences are made of either taut wire or standard chain link metal fabric with various enhancements (Table 6). Fence enhancements include different configurations of barbed wire outriggers (Figure 14). Personnel and vehicle fence gates are addressed under entry control in par. 4.4.4. The reader is referred to MIL-HDBK 1013/10 for details on fence design options.

b) Delay times. In general, fences (both with and without enhancements) offer delays of less than 1 minute against low-level threats to as little as 3 to 8 seconds against trained and dedicated high-level intruder teams. The height [up to 8 feet (2.4 m)] of the fence, or the degree of enhancements used (Figure 14) make little difference on this time. In general, fence material can be easily cut, or climbed over. This includes barbed wire which can easily be climbed over with the aid of blankets, etc. However, fences do offer some advantage in limiting the amount of tools, etc., that an intruder can readily carry into the site.

c) Fence selection including minimum requirements. In general, the delay time offered is not a significant factor in selecting a fence. A simple fence without enhancements will be adequate in most cases to define the site boundary, deter the casual intruder, or support an exterior IDS system. The use of fence enhancements offers the increased appearance of impregnability, but this should be weighted in terms of the increased material and maintenance costs. Specific minimum fencing requirements that are prescribed by military regulation include (see also MIL-HDBK 1013/10):

Table 6
Common Chain Link Fence Materials (MIL-HDBK-1013/10)

Component	Options
Specification	Federal Specification RR-F-191.
Gauge/Material	9-gauge (3.8-mm) steel wire mesh.
Mesh	Less than 2 inches (50 mm) per side.
Coating	Zinc coated, aluminum coated, or polyvinyl chloride (PVC) over zinc or aluminum coating.
Tension Wires	Wire, rail, cable (attached at top or bottom).
Support Posts	Steel pipe-formed sections, H-sections, square sections (see Federal Specs RR-F-191/3).
Height with Outriggers	8 feet (2.4 m). 7 feet (2.1) (for AA&E storage sites only).
Fabric Tie-Downs	Buried, 2-inch (50-mm) minimum encased in concrete or staked.
Pole Reinforcement	Buried, encased in concrete.
Gate Opening	Single and double swing, cantilevered, wheel- or overhead-supported.

i) DoD 5210.41-M - Nuclear Weapons Security Manual (Paragraph 3-202). Specifies two 7-foot (2.13-m) physical boundary fences, a minimum of 30 feet (9.14 m) or a maximum of 150 feet (45 m) apart that meet U.S. Federal Specification RR-F-191J/GEN. The configuration is summarized in Figures 15 and 16.

ii) DoD 5100.76-M - Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives (Chapter 5C). Requires fences around the perimeter of Category I and II missiles, rockets, ammunition, and explosives storage areas. Fencing may not be necessary for Category III and IV storage facilities unless an assessment of local threats, vulnerabilities, and cost effectiveness so suggest. The fence requirements are as follows:

- Fence fabric must be chain link (galvanized, aluminized, or plastic-coated woven steel) 2-inch (50-mm) square mesh 9-gauge (3.8-mm) diameter wire, excluding any coating. In Europe, fencing may be North Atlantic Treaty Organization (NATO) Standard Designed Fencing [~0.125-inch (2.5- to 3-mm)-diameter wire, 3-inch (76-mm) grid opening, 6.6 feet (2 m) high with 12.3-foot (3.76-m) post separation].

- Minimum fence height is 6 feet (1.8 m) for new fencing, excluding top guard (outrigger).

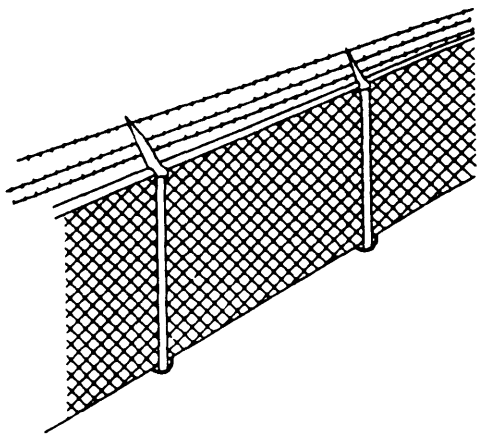
- Posts, bracing, and other structural members should be inside of the fence fabric. Nine-gauge (3.8-mm) galvanized steel tie-wires must be used to secure the fence fabric to posts and other structural members.

- The bottom of the fence fabric should extend to within 2 inches (50 mm) of firm ground. Surfaces should be stabilized in areas where loose sand, shifting soils, or surface waters may cause erosion and thereby assist an intruder in penetrating the area. Where surface stabilization is not possible or is impractical, concrete curbs, sills, or other similar types of anchoring devices extending below ground level should be used.

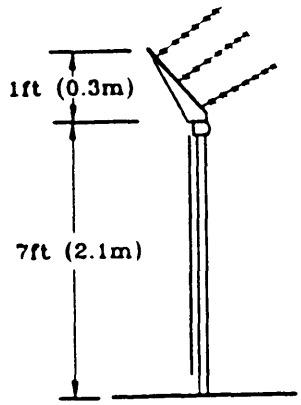
(d) Drainage culverts and utility openings under fences. Special protective measures must be designed for culverts, storm drains, sewers, air intakes, exhaust tunnels and utility openings that pass through cleared areas, traverse under or through security fences, or have a cross-sectional area of 96 square inches (0.06 square meter) or greater with the smallest dimension being more than 6 inches (150 mm). Such openings and barrier penetrations should be protected by securely fastened grills, locked manhole covers, or other equivalent means that provide security penetration resistance of approximately 2 minutes. MIL-HDBK 1013/10 provides detailed design options, some of which are illustrated in Figures 17 through 20. The reader is referred there for details.

4.3.3 Vehicle Barriers. Vehicle barriers are used to stop vehicle bomb threats at a preselected standoff distance (Figure 13) consistent with the hardness of the facility against blast effects. Available barriers are addressed in Section 8 in conjunction with designing the facility to sustain bomb blast. MIL-HDBK 1013/10 also presents enhancements to chain link fences to resist vehicle attacks.

FENCE OF STANDARD CHAIN LINK MESH, WITH ONE OR MORE OUTRIGGERS, USUALLY HOLDING THREE STRANDS OF BARBED WIRE EACH

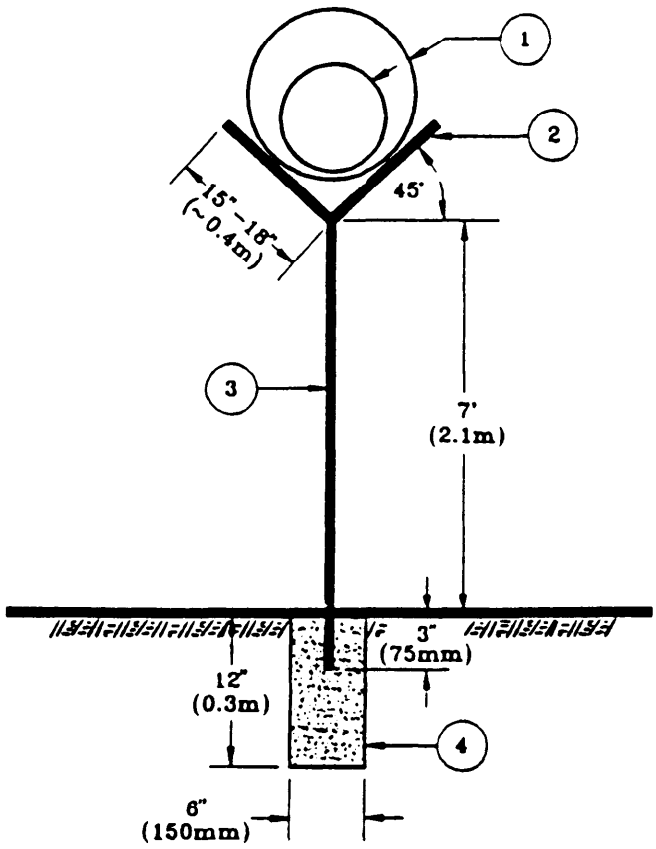


A. GENERAL DESCRIPTION



B. EXAMPLE

Figure 14
Fabric With Barbed Wire Outriggers Fence Configuration
(MIL-HDBK 1013/10)



LEGEND

1. Dual coil [30"/24" (0.7/0.6m)] barbed tape fastened to fence every 24 inches (0.6mm) is optional.

2. Outriggers with 3 strands barbed wire each side are installed at top of fence posts. Length of outrigger may range from 15 inches to 18 inches (~0.4m).

3. Chain-link fence, 2-inch-square (50mm) mesh maximum, 9 gauge (3.8mm) wire fabric minimum. Twisted and barbed salvage at top. Metal fence posts set in concrete every 10 feet (~3m).

4. Concrete footing encasing bottom of fence around entire perimeter. Purpose is to prevent lifting bottom of fence, delay burrowing and diminish erosion. Exact dimensions not critical, therefore where soil conditions permit, concrete may be poured directly in the trench without formwork.

Figure 15
Security Fence Configuration for Nuclear Weapons (DoD 5210.41-M)

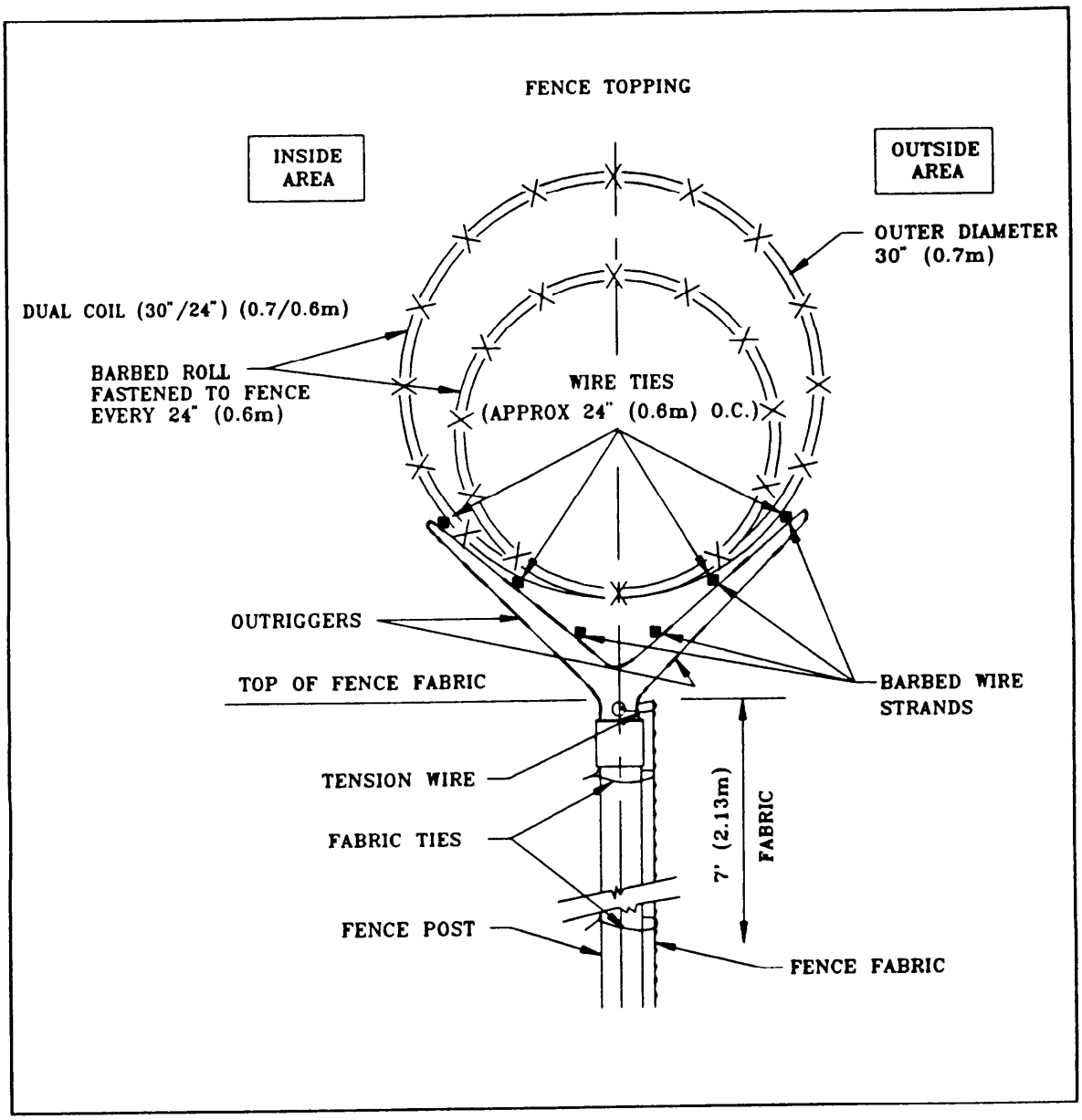


Figure 16
Optional Barbed Roll Topping for Nuclear Weapons (DoD 5210.41-M)

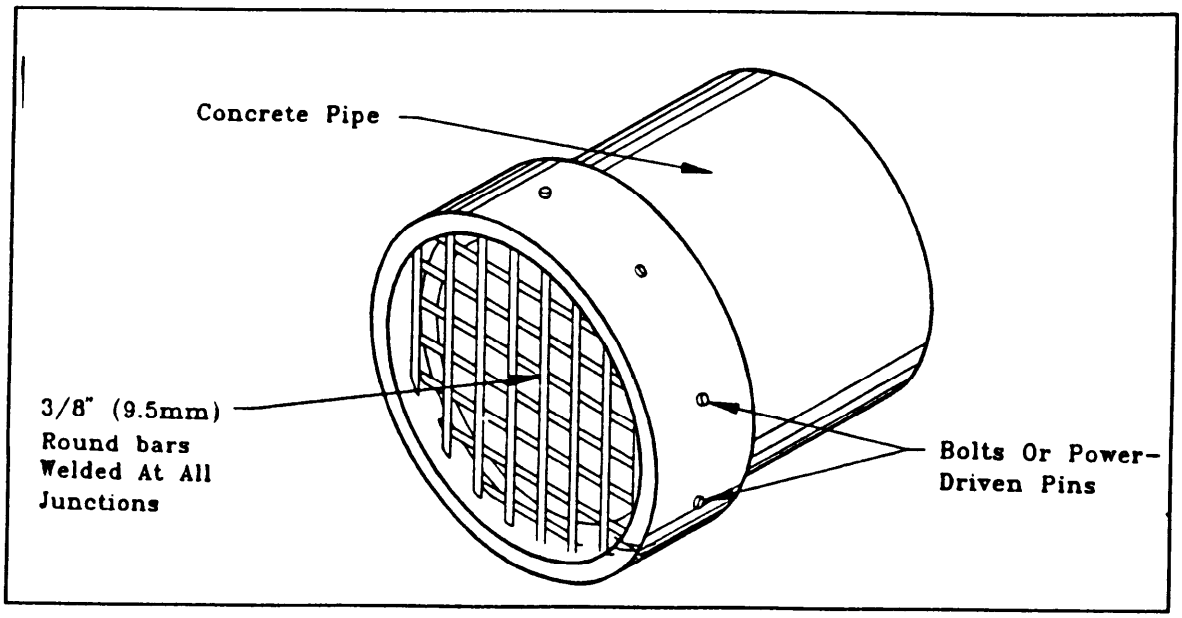


Figure 17
Concrete Culvert Grill (MIL-HDBK 1013/10)

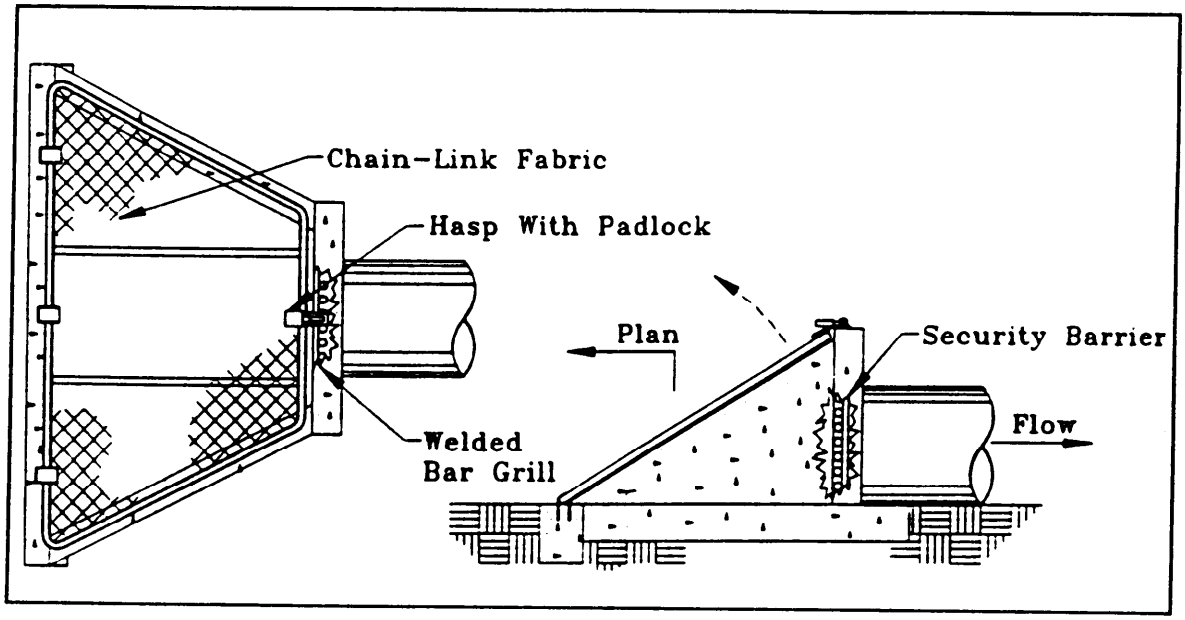


Figure 18
Removable Grating for Culverts (MIL-HDBK 1013/10)

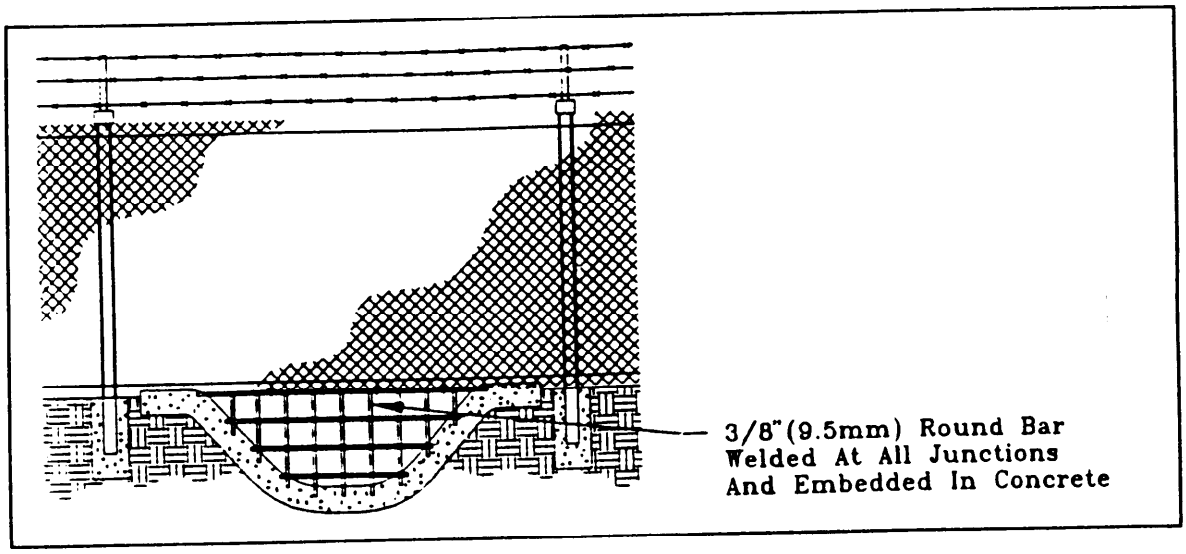


Figure 19
Bar Grill Embedded in Concrete (MIL-HDBK 1013/10)

4.4 Exterior Site Entry Control

4.4.1 Introduction. This section summarizes the function and location of measures for controlling entry into a restricted area, minimum DoD requirements for entry control, and the types of entry control systems available. Sources of detailed information regarding entry control systems are contained in:

- NAVFAC Design Manual 13.02 Commercial Intrusion Detection Systems, September 1986.
- MIL-HDBK 1013/10 Design Guidelines for Security Fencing Gates, Barriers and Guard Facilities, January 1993.
- TM 5-853-4, Security Engineering, Electronic Security Systems Manual, U.S. Army Corps of Engineers, February 1993.
- CEGS 16752 Electronic Entry Control Systems, U.S. Army Corps of Engineers Guide Specifications, April 1991.
- SAND 87-1927 Entry Control Systems Technology Transfer Manual, Department of Energy (DOE)/Sandia Laboratory.

4.4.2 Function and Location. Exterior entry control is that security function whereby personnel, vehicles, and materials are identified and

screened at exterior site perimeters and gates to protect against covert threats, discriminate authorized from unauthorized personnel, detect contraband, etc. Entry control also includes supervising the flow and routing of both pedestrian and vehicular traffic.

4.4.3 Minimum Requirements. DoD 5200.8-R states that military installations develop, establish, and maintain policies and procedures to control access into both the overall installation and designated restricted areas. The following summarizes:

1) Inspection Procedures. Procedures for inspecting persons, their property, and vehicles at entry and exit points of installations or at designated restricted areas and the search of persons and their possessions while on the installation are to be prescribed.

a) Random or Mandatory Inspections. This includes establishing whether searches or inspections are randomly conducted or mandatory for all. DoD 5200.1-R, Chapter 5, Section 3 prescribes inspection procedures for the safeguarding of classified information.

b) Search. Examinations of individuals and their possessions while on the installation for the primary purpose of obtaining evidence is classified as a "search" under the Fourth Amendment and separate guidance regarding the conduct of these searches is to be issued.

c) Legal Sufficiency. All procedures are to be reviewed for legal sufficiency by the appropriate General Counsel or Legal Advisor to the DoD Component prior to issuance. The procedures require Commanders to consult with their servicing Judge Advocate or other legal advisor before authorizing gate inspections.

2) Access Denial. This involves enforcing the removal of or denying access to persons who are a threat to order, security, and the discipline of the installation.

3) Restricted Areas. The command is required to designate restricted areas to safeguard property or material.

4) Randomized Anti-Terrorism Measures. The commander is to establish randomized anti-terrorism measures within existing security operations to reduce patterns, change schedules, and visibly enhance the security profile of an installation. This reduces the effectiveness of pre-operational surveillance by hostile elements.

4.4.4 Gates to Perimeter Fences

4.4.4.1 Overview. Gates facilitate control of authorized traffic and its flow. They establish specific points of entrance and exit to an area defined by fences. They also function to limit or prohibit free flow of pedestrian or

vehicular traffic, while establishing a traffic pattern for restricted areas. Gates, as a part of perimeter fences, must be as effective as their associated fence in order to provide an equivalent deterrent. Gates will normally require additional hardening features due to their location across entrance roads and the inherent vulnerability of their requirements when designing security fencing. MIL-HDBK 1013/10 provides design options for personnel and vehicle gates. The following summarizes the most common gate configurations used in conjunction with security fencing. These include single and double swing, cantilevered wheel-supported (V-groove) sliding gates, and double (biparting) overhead supported gates. While any of these may be used for pedestrian or vehicular traffic, generally single gates are designed for pedestrian traffic and double gates for vehicular traffic.

4.4.4.2 Personnel Gates. Pedestrian gates and turnstiles will be designed so that only one person may approach the guard at a time. For nuclear storage areas, the personnel entry gate complex is to include access and exit routes in accordance with DoD 5210.41-M, Nuclear Weapons Security Manual. For other details see MIL-HDBK 1013/10.

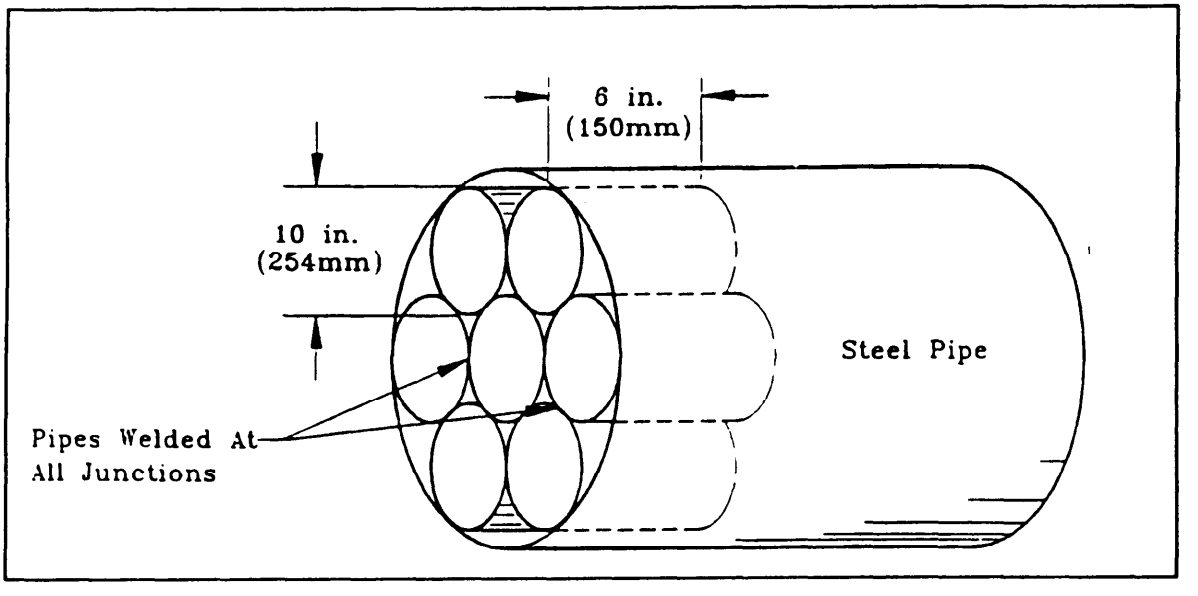


Figure 20
Large Culvert with Short Honeycomb Pipes (MIL-HDBK 1013/10)

1) Turnstile gates. Where access control is required into a restricted area, turnstile gates are recommended for controlling pedestrian traffic (Figure 21). Turnstile gates are also very helpful in relieving requirements for controlling personnel exiting a secured area since they can be set to revolve only in the exiting direction, thereby reducing the guard supervision required. Automated access control systems using coded credentials, such as badges with magnetic stripe, magnetic spot, Wiegand-effect wires, etc., may also be used to access turnstile gates (see par. 4.4.5).

2) Swing gates. While turnstile gates provide security personnel with more positive access control and greater penetration resistance, swing gates are a second alternative when turnstile personnel gates are not practical. Swing type personnel gates may be more economical to procure and fabricate from a hardware aspect; however, both operational and guard personnel requirements should be considered to determine the most economical long-term cost for the facility.

4.4.4.3 Vehicle Gates. Either wheel-supported (Figure 22) or cantilever sliding (Figure 23) gates are the best selection for vehicle security gates followed by overhead sliding gates. Swing gates are a third alternative and lastly, and the least desirable, are overhead ("guillotine") gates. Initially, the designer should begin by evaluating the wheel-supported or cantilever sliding gate. An initial step in the design is to determine the operational requirements for the gate. This includes the daily peak and normal work flow of vehicles; and the operational access control requirements for the secured area, i.e., badging, penetrator threat, magnetic sensor personnel monitoring, package surveillance, type (size) of vehicles to use the gate, etc. These requirements provide the basis for determining the type and size of gates, desirability or requirement for automatic openers, special hardening requirements, etc. In areas known for snow or ice buildup, internal heating should be considered in the gate design. See MIL-HDBK 1013/10 for details.

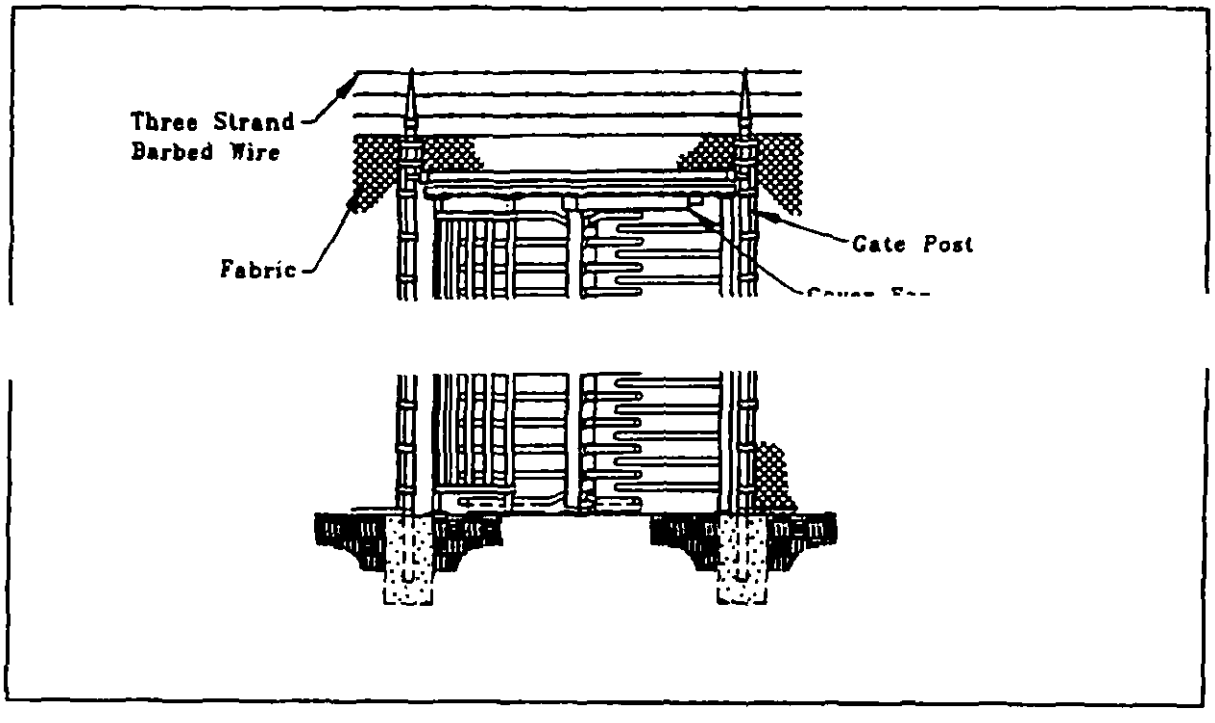


Figure 21
Turnstile (Rotational) Personnel Gate (MIL-HDBK 1013/10)

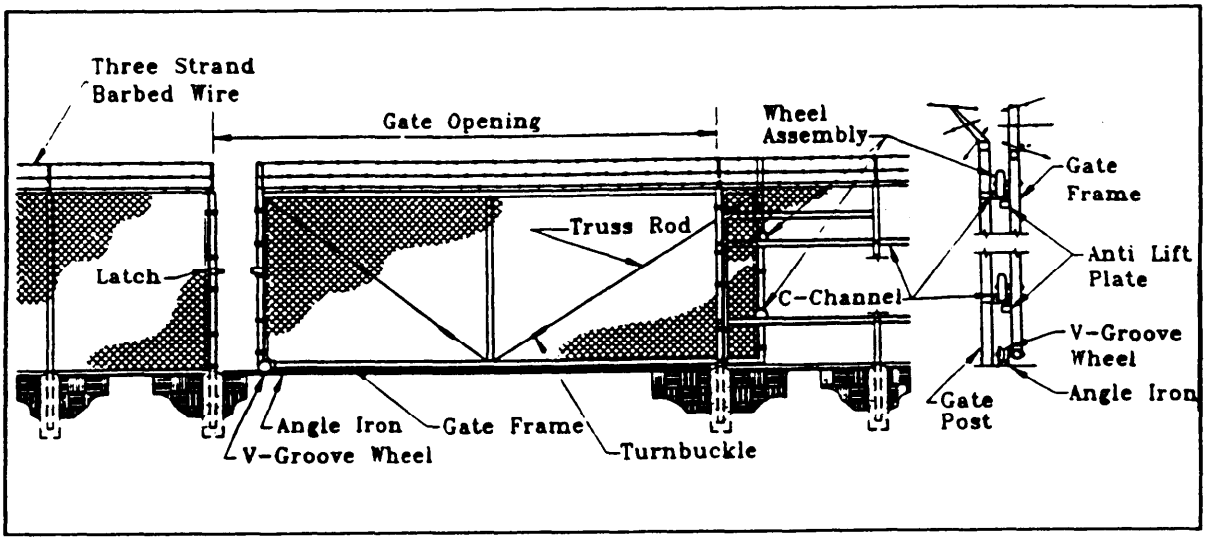


Figure 22
Single Wheel-Supported (V-Groove) Sliding Gate (MIL-HDBK 1013/10)

4.4.5 Entry Control Point (ECP) Layout and Traffic Control. Traffic control into and out of restricted areas during peak hours must be evaluated for both pedestrian and vehicular access when designing the entry control for a complex. Vehicular gates for restricted areas must be set back from any public or military roadway to ensure that temporary delays caused by identification checks will not cause traffic hazards. Sufficient space should also be provided to allow for spot checks, inspections, and searches of vehicles without impeding the flow of traffic.

Entry control design must afford maximum security while minimizing delay in the flow of authorized traffic. Figure 24 provides a characteristic entry control arrangement for a restricted area that has a high volume of assigned personnel and visitors to access daily. Inbound visitors and unauthorized vehicles are diverted from the normal flow entering the restricted area. They have the opportunity to either voluntarily reverse their direction and not approach the ECP or obtain appropriate vehicle and personnel passes to proceed into the restricted area. A second turnaround is provided immediately behind the ECP, but prior to the remotely controlled restricted area gates, so that security personnel can reverse the direction of vehicles or personnel that arrive at the ECP without proper passes or decals prior to accessing the restricted area. As a final security measure, remotely controlled, active (pop-up) vehicle barriers are provided inside of the gates to obstruct forced or high-speed entry into the restricted area. Tire shredders or remotely controlled active vehicle barriers are also provided inside the exit gate to forcibly stop a high-speed entry attack through the exit.

...ner matter contained therein. Restricted areas ... the security interest, or or

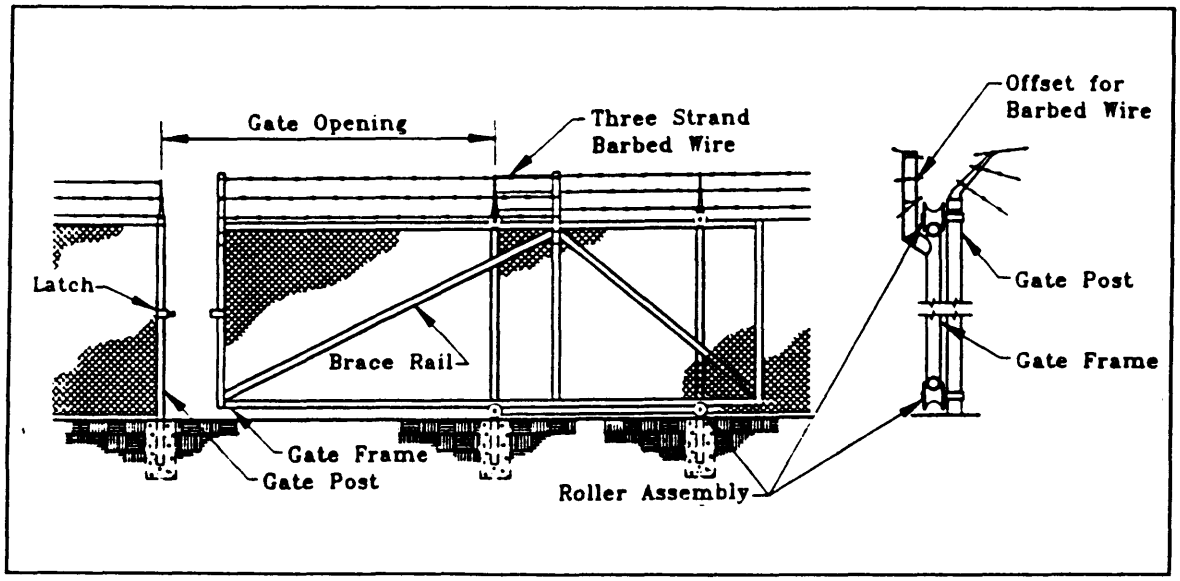


Figure 23
Single Cantilevered Gate (MIL-HDBK 1013/10)

The ECP shown in Figure 25 represents an entry control arrangement for a restricted area securing critical nuclear weapon components but having a low volume of assigned personnel and minimal visitor traffic to access daily. Direct straight-in vehicle access is impeded by a sharp curve and passive vehicle barriers to lessen the possible success of a high-speed vehicle attack. Personnel must pass through turnstiles on foot, one at a time to access the restricted area. Vehicles are processed and inspected in a sally-port gate and personnel turnstiles are paired in-line with the direction of entry so that one must be closed and locked before the other of the pair may be opened. Gate opening and locking system overrides must be provided for emergency vehicles. All opening/locking/emergency controls are contained within the ECP building.

4.4.6 Types of Entry Control Systems

4.4.6.1 Overview. The generic types of systems used to identify and control personnel and materials include: manual, machine-aided manual, and automated systems. Manual systems employ guards to control access based on authorization criteria. Machine-aided manual systems utilize entry control equipment to assist the guard in making decisions to allow or deny access. Automated systems allow personnel to enter and exit without guard intervention unless an alarm occurs. Automated access control that takes advantage of microprocessor technology and recent advances in coded credentials are increasingly used. The employee badge is now the primary access authorization means and the central processor provides alarm display, control, and related system integration functions. A number of badge technologies are available, and described in NAVFAC DM 13.02. A variety of access control systems are

described in the Sandia Entry Control System Handbook (SAND77-1033), and in the U.S. Army Security Manual TM-5-853-4. Additional details are provided in par. 5.3.3 related to building entry control.

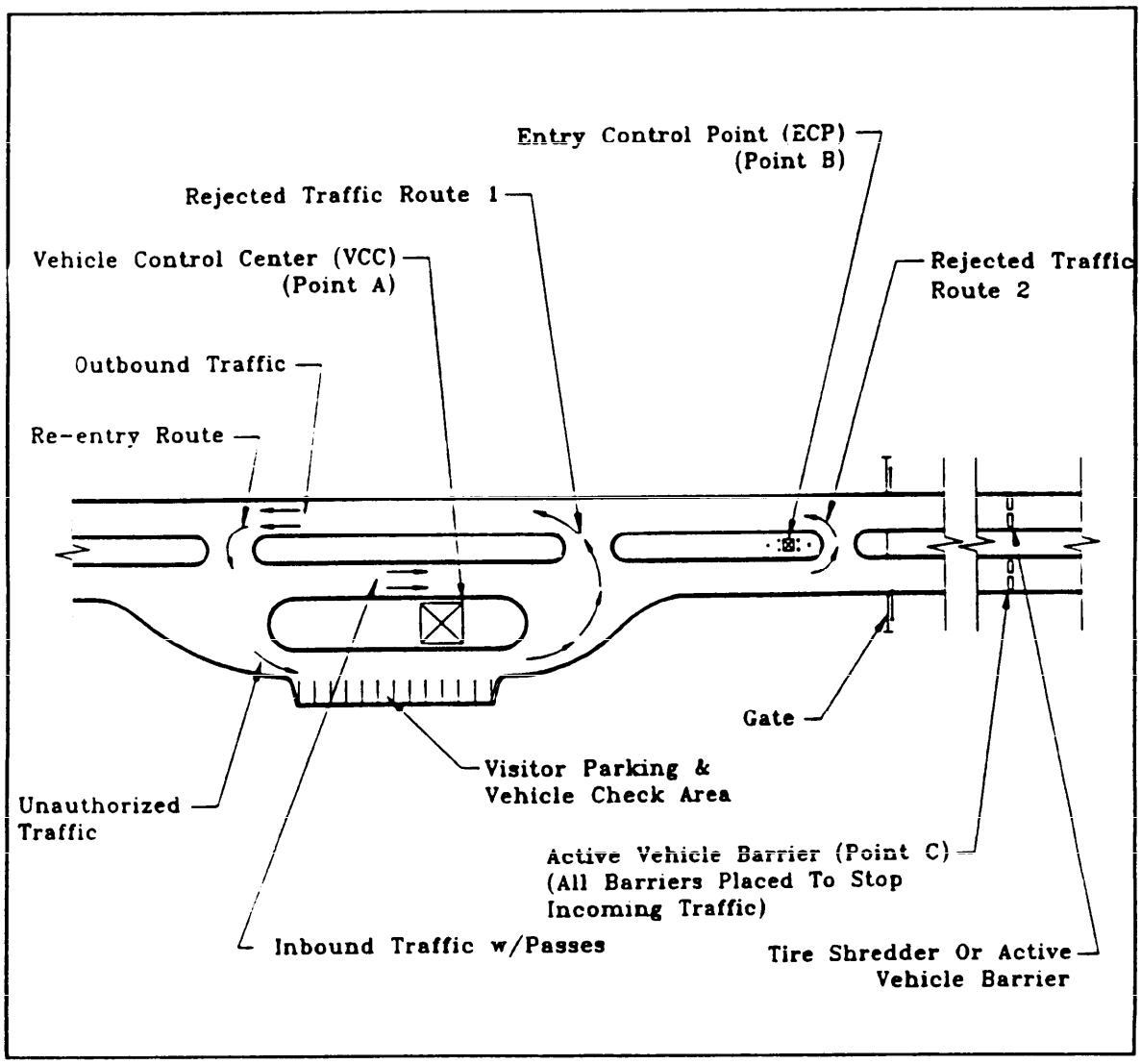


Figure 24
Example Entry Control Point (MIL-HDBK 1013/10)

4.4.6.2 Personnel Access Control System for Explosives, Metal, and Special Nuclear Materials (SNM) Detection. Figure 26 shows an example of a portal structure that can be used to screen personnel attempting to enter a restricted area. The procedure for operation of this system is as follows. An individual approaches the access enclosure and requests entry by pressing an entry request button. The operator at the control console unlocks the door

and watches the individual enter. The person places any hand-carried objects in the material inspection station, steps into the IDS area, and stops in front of the identification console. As the person walks into the IDS area, the SNM and metal detectors take measurements to sense for and indicate to the operator the presence of SNM or metal. While the individual is being identified, the explosives detector samples the air around the individual and indicates to the operator the presence of explosive vapors. After the individual has been identified and if no alarms have been signaled by any of the detectors, exit from the portal is permitted. A material inspection camera can be used to examine material which has caused a metal detector to alarm. The individual removes items from his pockets and places them in the material inspection area. The operator at the control console pushes a button and views the material on the television monitor. The person in the enclosure again passes through the metal detector. The material inspection area is large enough to view lunch boxes, briefcases or packages.

4.5 Exterior Perimeter Intrusion Detection Systems

4.5.1 Introduction. This section provides a summary of the function and placement of exterior fence IDS, applicable minimum requirements, and the types of sensors available and typically deployed. Sources of more detailed design information regarding exterior IDS include:

- DM 13.02, Commercial Intrusion Detection Systems, NAVFAC Design Manual, September 1986.
- TM-5-853-4, Security Engineering, Electronic Security Systems Manual, U.S. Army Corps of Engineers, February 1993.
- SAND 89-123, Exterior Intrusion Detection Systems Technology Transfer Manual, DOE/Sandia National Laboratory.
- ESE-SIT-0001, Siting Criteria for Standardized Electronic Security Equipment, Air Force, March 1991.
- NFGS 16726C, Basic Intrusion Detection Systems, NAVFAC Guide Specification, February 1991.
- NFGS 16727C, Commercial Intrusion Detection Systems, NAVFAC Guide Specification, February 1991.

4.5.2 Function and Location

4.5.2.1 Overview. For security guards to respond to an intrusion, threat detection either by security personnel or remote systems IDS is required. The function of an exterior perimeter IDS is to detect a threat and initiate the security system response timeline at the exterior perimeter of the site. IDS performance parameters of concern include:

- Completeness of coverage.
- False and nuisance alarm rates.
- Probability of detection.
- Zone at which the alarm occurred.

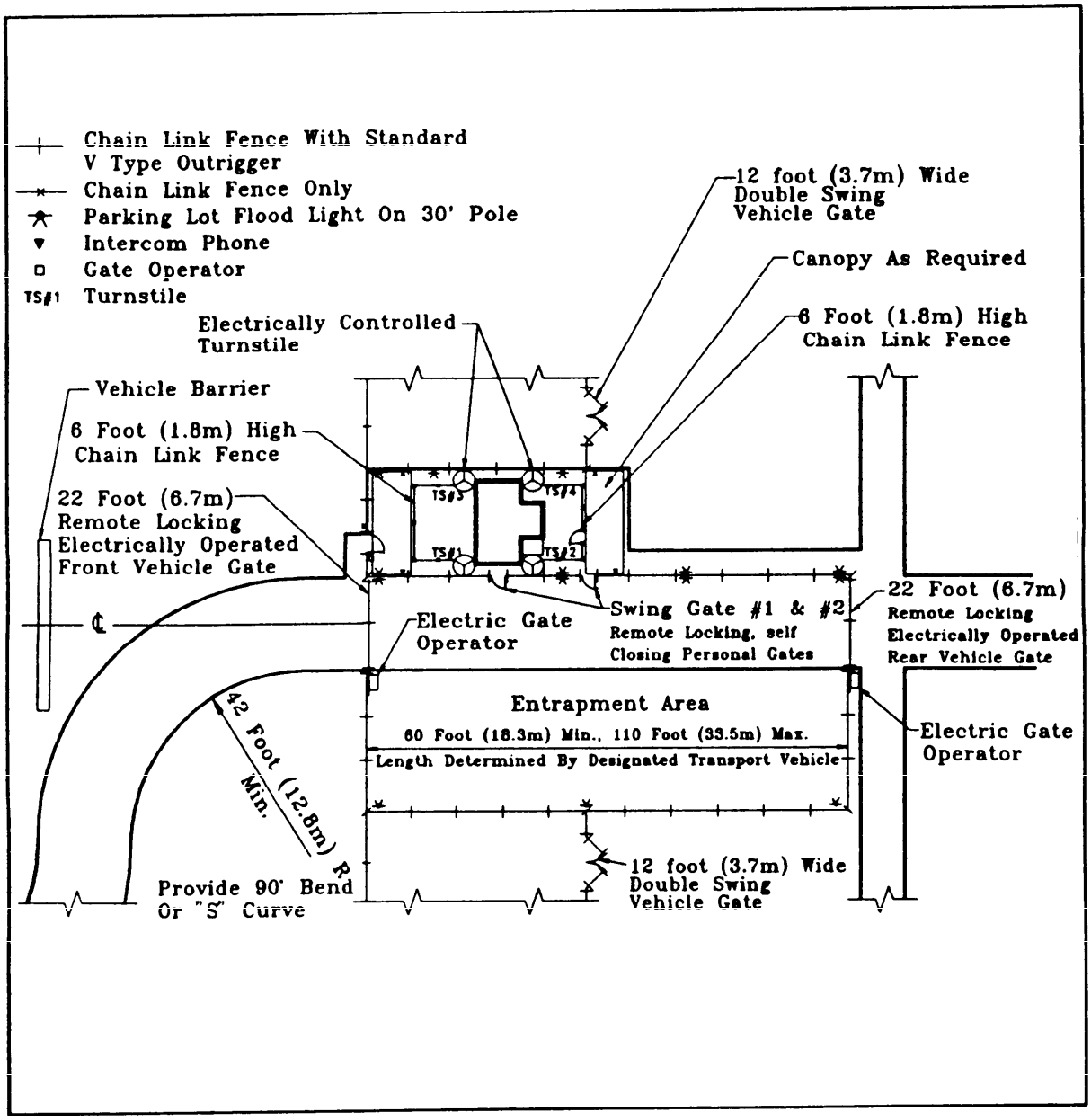


Figure 25
Nuclear Weapons Storage Site Entry Control Facility (MIL-HDBK 1013/10)

Relying on exterior IDS involves inherent risks. In general, deploying sensors along extended site perimeters can be costly. Also, guard requirements for threat assessment may increase because of high false or nuisance alarm rates associated with detection sensors subject to weather and other factors. One way of minimizing the latter problem is to design systems

threat attack.

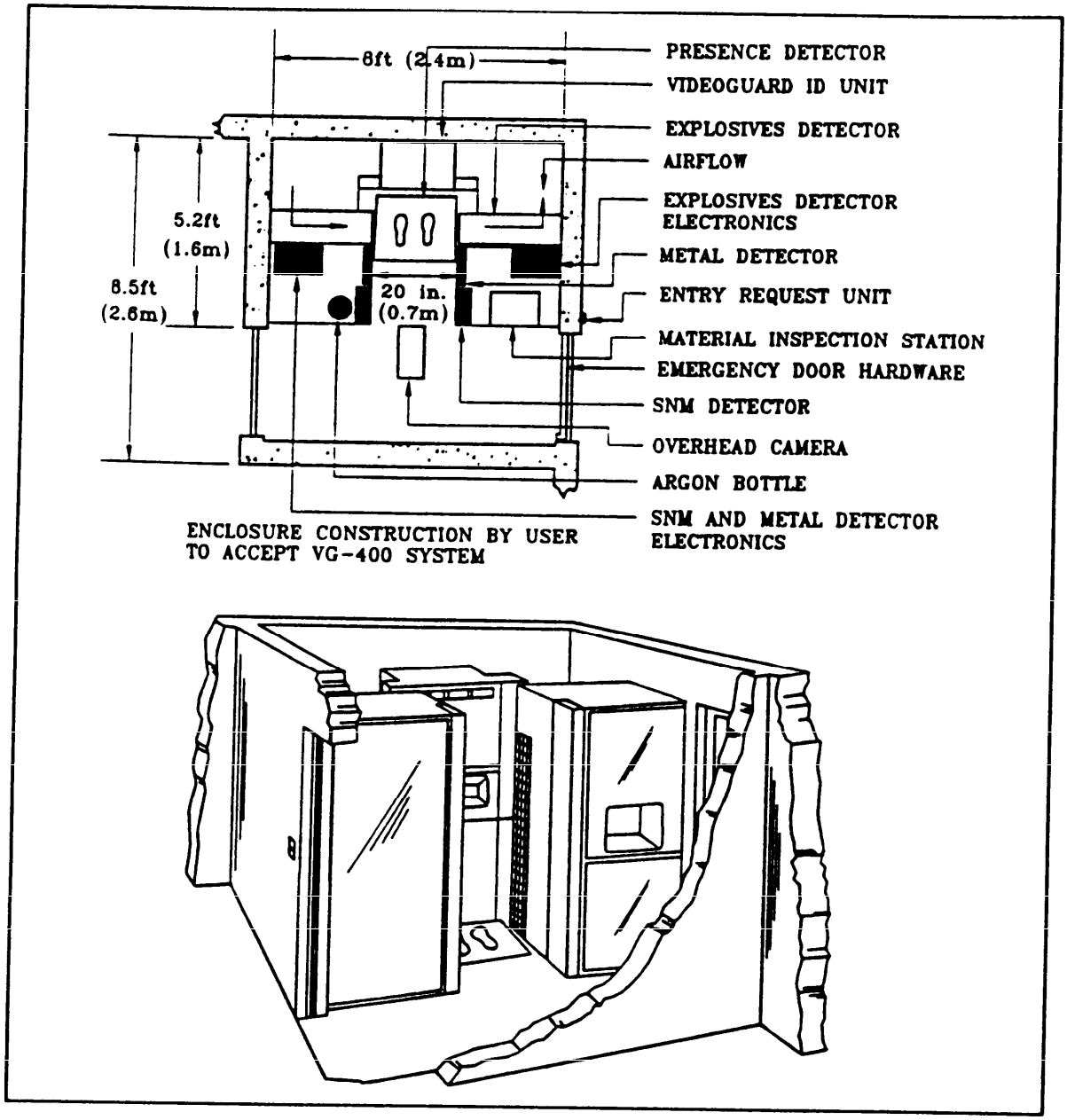


Figure 26
Example Portal Structure for Access Control

for which the disturbance threshold level for activating the sensor is very high, but within the level of that created by an intruder. In general, exterior perimeter IDSs are not recommended unless specifically required by DoD instruction or regulation. This is discussed further in par. 4.5.3 below.

4.5.2.2 Exterior IDS Layout and System Compatibility. Any required exterior site IDS must be identified and included during the planning of the site layout. The IDS required cannot be completely identified until the proposed site layout plan has been established. As noted, an exterior IDS designed to provide detection along a long fence line may result in high system costs for installation, operation and maintenance. Detection and assessment sensors nearer or on the exterior of the facility being protected are often more effective from a performance and cost point of view. In any case, even when intrusion detection sensors and fences are located close to the facility, if the facility delay time is too low the time available for effective security force response may not be adequate. As emphasized in Section 3, ensuring that resources are wisely spent requires that the relationship between exterior sensor location, delay times, and security force response times must be carefully examined.

1) Exterior Site Perimeter Detection. Detectors employed along the perimeter of the site initiate the timeline of an intrusion at that point. Such detectors may be employed on the fence, such as strain-sensitive cable, or between fences, such as buried, ported coax, bistatic microwave, or infrared beam sensors. These sensors are described in par. 4.5.4. CCTV or guard personnel in towers or responding to the site are also needed for threat assessment.

2) Detection at Building Exterior. To take advantage of the delay provided by walls, floors, ceilings, etc., detectors may be employed on or within the surfaces of the building exterior. An example is vibration sensors mounted on walls to detect an intrusion attack. Another is the use of a buried ported coax sensor around the outside of the building. These systems are described in par. 4.4.5.

4.5.3 Minimum Requirements for Exterior IDS. Exterior IDS is required by military regulation only for certain facilities and resources. When required, the exterior IDS should be selected for the best performance considering such prevailing local environmental conditions as soil, topography, weather, and other factors. These factors can adversely affect performance or increase false alarm (an alarm without a known cause) rates. New exterior IDS must be an approved DoD standardized system or utilize commercial equipment. Existing installed IDS not meeting these standards may continue to be used until replacement is necessary. Minimum exterior IDS requirements should be based on security system levels defined in DoD 5200.8-R for facilities and resources (see par. 2.2.1.2, Figure 2).

4.5.4 Exterior IDS Options for Detection Along Site Perimeter Fences

4.5.4.1 Most Commonly Deployed Sensors. Table 7 lists a number of exterior sensors used along fence perimeters. There are three classes: fence-mounted, free-standing, and buried sensors. On-site visits to Navy, Air Force, and Army facilities disclosed that although all of the sensors shown in Table 7 are utilized by DoD, the following are most common:

- Fence-Mounted: Strain-sensitive cable on the fence fabric in combination with a "Y" taut wire on the fence outriggers.
- In Clear Zone Between Fences: Ported Coaxial Cable Sensor (PCCS) or, alternatively, a microwave fence sensor (MFS).
- Threat Assessment: Tower guards or CCTV for threat assessment after one or more of the above sensors have detected the intrusion.

Table 7
Typical Exterior Sensor Types (Most Commonly Used Sensors are Underlined)

- Fence-Mounted
  1. Fence Disturbance Sensor - Mercury Switch.
  2. Strain-Sensitive Transducer Cable.
  3. Inertia Guard Fence Sensor - Shock Sensors.
  4. "Y" Taut Wire Sensor (YTWS).
  5. Vertical Taut Wire Sensor.
  6. E-Flex Cable.
  7. E-Field.
  8. Mechanical Accelerometer.
- Free-Standing at Fence Line
  1. Microwave Fence Sensor (MFS).
  2. Infrared Beam.
  3. Forward-Looking Infrared.
  4. Pyroelectric Vidicon.
  5. Infrared Charged-Coupled Device.
- Buried at Fence Line
  1. Short Ported Coaxial Sensor.
  2. Ported Coaxial Cable Sensor (PCCS).

In general, a double fence perimeter configuration having a strain-sensitive cable taut wire on the inner fence, and MFS or PCCS for detection with a CCTV (for assessment) in the clear zone is used to protect critical military resources such as special weapons or designated Command, Control, and Communications (C3) facilities.

Interviews with representatives from the Navy, Air Force, Army, and USMC showed general agreement with the above most commonly deployed sensor choices. In some cases, it was found that a given military service might interpret differently what constitutes a critical resource requiring the double-fenced configuration.

The following briefly summarizes some important characteristics of the above sensors. Generic configurations are described since the performance of one manufacturer's sensor may differ in detail from another's. Performance is also site- and installation-dependent. Sensors must be evaluated for their capability to detect targets against which they are expected to be used, and for their vulnerabilities to the source of nuisance alarms expected to be encountered. Each sensor has its own vulnerabilities to natural background disturbances and capabilities for target detection. For more details see the sources listed in par. 4.5.1.

1) Strain-Sensitive Cable. This sensor detects intruders by use of a fence-mounted transducer cable which sends analog signals to an electronic signal processor when the cable is disturbed. The transducer is a coaxial cable with shielding (Teflon) between the center conductor and the shield outer conductor. The incoming signal from the sensor cable is fed into a signature filter; signals that closely resemble intrusion signatures pass through the filter, generating a count. If the total count exceeds a preset limit within a preset time, an alarm pulse is generated. The basic system consists of a signal processor and a transducer cable. The transducer cable is typically installed in 328-foot (100-m) sectors, which are monitored by a signal processor. Each sensor sector provides one alarm output. The strain-sensitive cable will not detect threats on the fence outriggers. This requires a taut wire sensor.

2) "Y" Taut Wire Sensor (YTWS) System. The YTWS consists of a fence-outrigger-mounted sensor and control unit that employs a twisted barbed wire pair stretched to about 75 pounds (34 kg). Wire deflections caused by climbing, pulling wires apart, or cutting the wires produce alarms. The YTWS system consists of two sensor arms in a "Y" configuration, each with six sensor switches, dual Expander Isolation Circuit Assemblies, and twelve taut wires running the length of the sensor sector. Each taut wire is connected to a sensor switch at the switch arm so that a switch is actuated and an alarm generated by deflecting any of the taut wires. Slider arms in the outrigger plane at each fence post maintain taut wire separation along the sensor sector.

3) Ported Coaxial Cable Sensor (PCCS). The PCCS is an external line sensor consisting of a coaxial cable with the outer conductor (or sheath) open along the length of the cable. A pair of such cables, one for transmission and the other for reception, and the associated transmitter, receiver, and processor constitute the ported coax system. The cables are buried a few inches below the ground surface. The receiving cable lies in the electromagnetic field surrounding the transmitting line. An intruder entering the field increases the coupling between transmitter and receiver, producing a detectable change of received signal level. Detectable target velocities range from 0.07 to 23 feet/second (f/s) (0.02 to 7 m/s). The PCCS generates an electromagnetic corridor at the boundary of the area and detects intruders in the corridor. Disturbances of the electromagnetic field by intrusions exceeding predetermined thresholds cause an alarm with intrusions pinpointed to a specific zone. An alarm zone can be set from 33 to 5,250 feet (10 to 1,600 m) but is typically 330 feet (100 m). The soil in which the cables are buried can have a large effect on system performance. The soil conductivity will vary greatly from a clay soil (high conductivity) to a sandy soil (low conductivity). A clay soil will not allow as much energy to reach the surface and produces a lower sensitivity than a sandy soil. Different installation techniques are used depending on the soil type and conductivity. A standard 12-inch-square (0.3-m-square) trench can be used only in soils with an average conductivity of 40 MHOS per meter or less, and with an average dielectric constant of 35 or less. Running water resulting from heavy rainfall and wave action on standing puddles which cover or cross the detection zone will increase false alarm rates for the system.

4) Microwave Fence Sensor (MFS). There are a large number of commercially developed microwave sensors currently available. One difficulty with microwave sensors is that the terrain must be extremely flat, roughly 3/8 inch (~9 mm) in elevation/depression over a 10-foot (~3-m) span. Blowing snow and dust can also cause false alarms. The MFS is employed as a bistatic microwave intrusion detector. Its detection zone consists of a narrow region between transmitter and receiver antennas. The received signal is the vector sum of the direct transmitted structures and objects. Moving objects (e.g., humans and vehicles) produce changes in the net vector sum of the received signal. Detection occurs when the resulting received signal crosses a predetermined threshold. The transmitted signal is tone-modulated to eliminate mutual interference when multiple MFS sensors are operated in close proximity to one another. The primary detection mode is the beam-break mode where the target passes directly between the MFS transmitter and receiver antennas. A second and equally important mode is the multipath reflection mode in which the reflected wave from an off-axis target destructively interferes with the direct wave at the receiver. In addition, alarms are produced when the transmitted signal or its modulation is disturbed, when the equipment is jammed, or when the enclosure tamper switches are actuated.

4.5.4.2 Other Exterior IDS Sensor Candidates. The following provides a brief description of other candidate sensors that may be used in conditions when the most commonly deployed sensors are not suited. See the sources identified in par. 4.5.1 for more details.

1) Electric Field Fence Sensor. An electric field fence sensor consists of an alternating current field generator which excites a field wire, one or more sensing wires that couple to the field, and an amplifier and signal processor to amplify and detect changes in signal amplitude generated by intrusions. A human body distorts the coupling between the field and the sensing wires thus generating a signal. This sensor can be employed to follow terrain and is useful over hilly terrain. Supervisory circuits have been designed to detect cutting, shortening, or breaking of wires. Zone lengths are typically 330 feet (100 m).

2) Seismic-Magnetic Buried Line Sensor. This sensor consists of a cable that is sensitive to both seismic and magnetic disturbances and a processor to evaluate signals that are generated in the cable. Detection is based on the fact that seismic disturbances will either move the cables in the earth's magnetic field or strain the magnetic core. Either will generate a voltage in the sensing coil. This sensor is useful in remote areas, but may suffer false alarms from wind-induced ground motion and other localized pressure sources such as moving vehicles and trains.

3) Seismic Buried Line Sensor. There are three types of seismic sensors: piezoelectric sensors, balanced pressure systems, and geophone line sensors. Each are activated by seismic energy generated by intruders and each can follow irregular terrain and crooked sectors. Such sensors can be used in combination with other sensors (such as microwave sensors) to optimize detection capability while minimizing false alarms.

4) Magnetic Buried Line Sensor. This is a passive sensor that is sensitive to disturbances in the local magnetic field caused by nearby movement of ferromagnetic material. When an intruder with ferromagnetic material crosses the loop, the electrical signal generated causes an alarm.

5) Electromechanical Fence Disturbance Sensor. When an attempt is made to climb a fence, the fence moves. This motion can cause a switch mechanism to open or close, generating an alarm. This is called an electromechanical fence disturbance sensor. Electromechanical fence sensors use a set of point transducers to detect fence motion. These point transducers produce an analog signal, rather than a switch closure, and use an electronic signal processor to extract alarm information from the signal.

6) Doppler Radar. A Doppler radar is a monostatic microwave sensor that operates on the principle of target motion generating a frequency change or Doppler shift which is detected by the receiver. Such radars can provide coverage over irregular terrain.

7) Electromagnetic Point Sensor. This device detects a frequency change caused by the reflected impedance of an intruder entering an antenna's field. Two oscillators are tightly coupled to the antenna. A change in antenna impedance results in a change in frequency of each oscillator. This sensor adjusts automatically to changes in the background noise level. As the background noise level increases, the sensitivity is automatically reduced, but detection range is also shortened.

8) Geophone Point Sensor. Geophone sensors are normally buried in the ground to detect seismic disturbances generated by intruders. This sensor is sensitive to seismic and acoustic energy sources and far-field effects must be discriminated against.

9) Magnetic Point Sensor. Magnetic point sensors contain one or more magnetometers that are used to detect the movement of ferrous objects. Using two magnetometers spaced at various distances, it is possible to determine the direction of motion of such ferrous targets.

10) Infrared Beam Sensor. Exterior infrared intrusion detection systems can be active or passive. Passive sensors detect changes in thermal radiation within a specific field of view. Active infrared sensors detect changes in signal power between a transmitter and a receiver. Generally, multiple beams are employed in columns at the ends of a detection zone. An intruder passing through one or more beams causes a "beam-break," thus generating a signal. As this sensor can be defeated by tunneling, seismic sensors should be used as well.

4.5.5 Exterior IDS Detection at Building Exteriors. Several candidate options for use at building exteriors are briefly described here.

4.5.5.1 Ported Coaxial Cable Sensors. In addition to use in the clear zones between perimeter fences, the Ported Coax Cable System (described in par. 4.5.4.1) can also be used around the exterior of buildings.

4.5.5.2 Vibration Sensors. Vibration sensors can be mounted on or within walls and roofs to detect intrusion attempts at facility exteriors. The simplest vibration sensor is a mechanical contact switch designed to actuate when the surface on which the sensor is mounted starts to vibrate.

4.5.5.3 Grid Wire Sensors. Grid wire sensors may be embedded in the walls or roof of a building. When the barrier is penetrated, the wire is broken causing an alarm.

4.6 Exterior Closed-Circuit Television

4.6.1 Introduction. This section provides a summary of the function and placement of CCTV's applicable minimum requirements; and the types of CCTV equipment available. Sources of more detailed design information include:

- NAFAC Design Manual 13.02, Commercial Intrusion Detection Systems, September 1986.

- TM-5-853-4, Security Engineering, Electronic Security Systems, Manual U.S. Army Corps of Engineers, February 1993.

- SAND 89-1924, Video Assessment Technology Transfer Manual, DOE/Sandia National Laboratory.

- ESE-SIT-0001, Siting Criteria for Standardized Electronic Security Equipment, Air Force, March 1991.

- CEGS-16751, Closed Circuit Television Systems, Corps of Engineers Guide Specification, April 1991 .

4.6.2 CCTV Function and Location

4.6.2.1 Threat Assessment. A properly designed CCTV assessment system provides a rapid and cost-effective supplement to guards for determining the cause of intrusion alarms and assessing a potential threat. CCTVs allow evaluations to be made from remote locations. Using video event recorders, events can also be viewed later when multiple alarms or delayed guard force attention occurs. In general, CCTVs increase the efficiency and effectiveness of security personnel and security response timelines. They can be a cost-effective alternative to human on-the-spot assessment, which typically involves extended time delays for guards to respond, or the use of costly on-site guards.

4.6.2.2 Surveillance. CCTVs can also be used for surveillance. As a surveillance system, CCTVs are used at the discretion of and under control of the security center console operator to scan a secured area.

4.6.2.3 Location. CCTVs are typically located:

1) Outdoors, along exterior site perimeter clear zones.

2) Outdoors, at controlled access points to sites or buildings.

3) Outdoors, within a restricted area that overlooks approaches to selected security interests.

4) Indoors, at selected locations within the protected area.

4.6.3 Minimum Requirements. DoD 5200.8-R requires the use of CCTV to provide real time assessment for certain facilities and resources security systems levels (see par. 2.2.1.2, Figure 2). In addition, DoD 5210.41-M specifies the following for nuclear weapons storage site security (quoting directly):

a) "A means is to be provided by which the cause of all alarms generated at the perimeter security system can be assessed in near-real-time, physically (i.e., visually) or remotely through electro-optical (imaging system) or other electronic devices. To the maximum practical extent, electro-optical equipment (imaging systems) or other electronic devices should be utilized, thereby permitting more effective utilization of the security and response forces.

b) Real-time visual assessment may be enhanced by providing an intruder sector indicator at alarm annunciation locations. This optional feature should improve the capability to respond quickly with discriminate application of force, including deadly force.

c) Imaging systems provide a remote visual image of activity occurring in an area under surveillance. CCTV, low-light level television, infrared, and radar are examples of techniques which may be employed. Such equipment can be used for area surveillance beyond and within the perimeter and for assessment of the cause of alarms and other activities.

d) Facilities used for visual assessment shall be hardened against small arms fire. Individual cameras, imaging sensors or scanners do not require hardening."

4.6.4 Elements of a CCTV Assessment System. A typical video system is composed of one or more cameras, a display monitor, and various switching, transmission, and recording systems. Coverage of the desired field of view must be determined through analysis of the camera location, the size and shape of the area to be surveyed, and appropriate light levels. Control circuitry enables either manual or automatic selection of specific video signals for display on television monitors. When an alarm is generated by a perimeter sensor, the view from any given camera is displayed on the television so that the operator can assess the cause of the alarm. Guidance in camera selection and optimization of installation are given in the references of par. 4.6.1. The following summarizes.

4.6.4.1 Camera Types. Equipment includes cameras with automatic iris adjustment to accommodate varying illumination levels. Cameras are also equipped with thermostatically controlled heating elements to compensate for low temperature environments. A variety of lenses ranging in focal length are available. This variety permits adapting to varying fence configurations and blind zone lengths. Supports for the cameras include a tilting cantilevered mast that permits the support to be installed inside the boundary fence while the camera is suspended over the fence, viewing the clear zone. Also included

is a tilting vertical mast that can be used in those situations where the cantilevered mast is not appropriate. Two cameras can be mounted atop a vertical mast. The tilting feature permits the top of the mast to be lowered to working height for maintenance on the ground. Counterweights facilitate the tilting operation of both the cantilevered and vertical masts. One other support is provided that permits mounting a camera to the side of a building or other vertical surface. The following summarizes the available camera types.

1) Standard Video Camera. The standard vidicon tube is the most widely used image tube for CCTV. Conventional cameras are designed primarily for daylight. These cameras typically operate at light levels of 1 lumen per square meter. Their spectral response closely approximates the human eye. In continuous 24-hour use, it will last up to 6 months. A typical CCTV camera is illustrated in Figure 27.

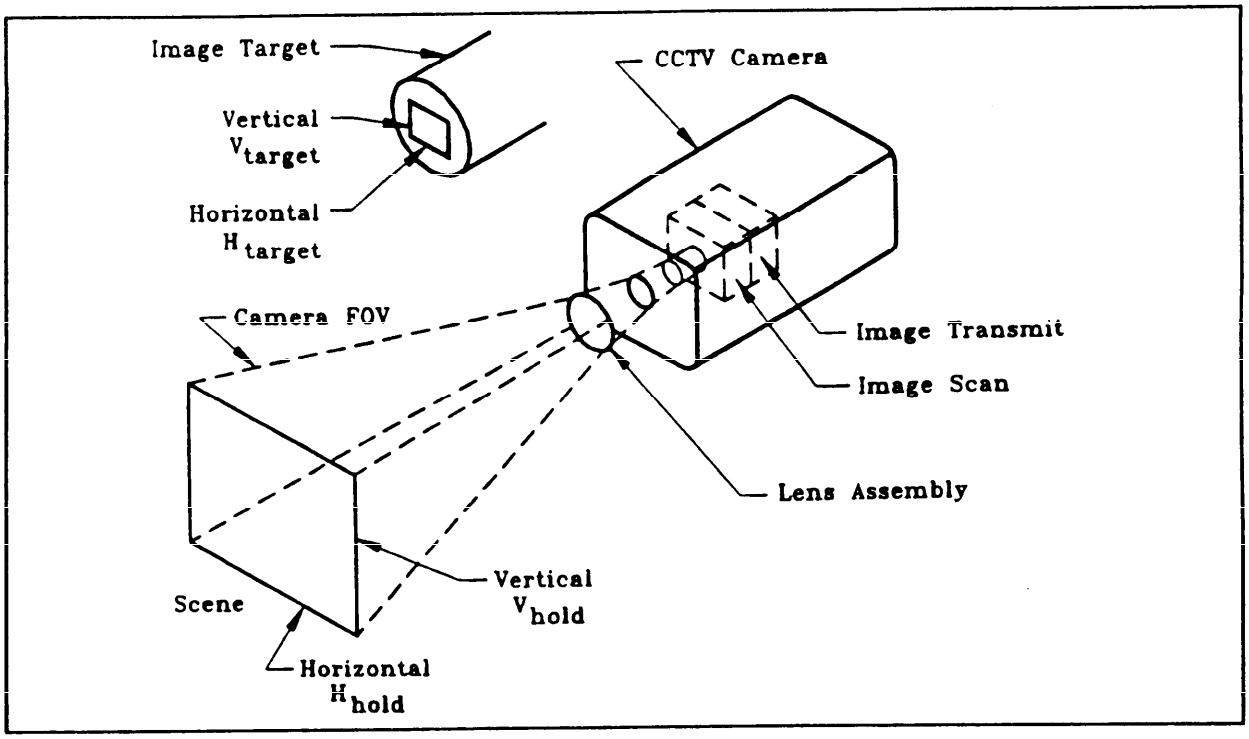


Figure 27
CCTV Camera Components

2) Low-Light Level Camera. Low-light level cameras can be used to provide greater sensitivity when required, i.e., much less lighting than the standard vidicon. These cameras also generally have a longer life. Automatic iris control is needed to prevent "blinding" of the camera in bright light.

3) Very Low-Light Cameras. Very low-light level cameras are also available. Such cameras can function at 2 x 10E-5 lumens per square meter. Very low-light level cameras find application where "blackout" conditions are to be maintained at a facility. Such cameras use Silicon Intensifier Target or Intensified Silicon Intensifier Target tubes. These cameras are expensive, roughly 20 to 30 times the cost of a standard video camera. As a result, it may be more cost-effective to upgrade lighting than to use such tubes. Designers may encounter applications where such cameras fulfill a special requirement.

4) Solid-State Cameras. These cameras use charge-coupled solid-state devices that function like the vidicon tube of a conventional camera. Elimination of the tube increases reliability and minimizes maintenance requirements. Its small size and high reliability are very desirable features.

4.6.4.2 CCTV Monitors. Monitors are devices upon which a CCTV scene is projected and viewed. For access control monitoring, a 19-inch (0.5-m) monitor is preferred. A 9-inch (0.3-m) monitor is typically used for security alarm assessment. One operator can effectively handle up to eight monitors (four sets of two stacked vertically). It is desirable that monitors for alarm assessment remain blank until an alarm occurs. If the system is also being used for surveillance of an area when an alarm occurs, the alarmed zone scene should automatically replace the surveillance scene.

4.7 Exterior Security Lighting

4.7.1 Introduction. This section summarizes the kinds of lighting deployed to enhance the security of DoD facilities. Specifications are provided for both direct guard-visual and CCTV surveillance.

4.7.2 Function and Location. Security lighting aids threat detection, assessment, and interdiction. Lighting may also have value as a deterrent. Security lighting increases the effectiveness of guards and CCTV by increasing the visual range during periods of darkness or by illuminating an area where natural light is insufficient. Exterior security lighting is typically located along exterior perimeters and entry points of the site and buildings. Each facility presents its particular deployment problems based on physical layout, terrain, weather conditions, and security requirements. The remainder of this section discusses standard types of lighting, lighting concepts, lighting for CCTV, and surveillance and related lighting issues (energy and legal).

4.7.3 Standard Exterior Lighting Configurations. Lighting may operate continuously or on a standby basis.

4.7.3.1 Continuous Lighting. Continuous lighting (the stationary luminaire) is the most common security lighting system. It consists of a series of fixed luminaires arranged to flood a given area continuously during

changes are used to generate alarms.

the hours of darkness with overlapping cones of light. The two primary methods of using continuous lighting are glare projection and controlled lighting.

1) Glare Lighting. Glare lighting uses luminaires slightly inside a security perimeter and directed outward. It is considered a deterrent to a potential intruder because it makes it difficult for him to see inside the area being protected. It also protects the guard by keeping him in comparative darkness and enabling him to observe intruders at considerable distance beyond the perimeter.

2) Controlled Lighting. Controlled lighting is used when it is necessary to limit the width of the lighted strip outside the perimeter because of adjoining property or nearby highways, railroads, navigable waters, or airports. In controlled lighting, the width of the lighted strip is controlled and adjusted to fit a particular need, such as illumination of a wide strip inside a fence and a narrow strip outside, or floodlighting a wall or roof. Unfortunately, this method of lighting often illuminates or silhouettes security personnel as they patrol their routes. Controlled lighting may provide direct or indirect illumination.

a) Direct Illumination. This lighting concept involves directing light down to the ground. Its goal is to provide a specified intensity of illumination on intruders, facilitating their detection by CCTV or security patrols.

b) Indirect Illumination. An alternative lighting concept involves backlighting the intruders against a facility. This may be done by placing lighting away from the building and directing it back toward the walls so shadows will be cast on the building by the threat. Such applications are most effective if the luminaires themselves are near ground level. This indirect concept is also aesthetically pleasing, illuminating the architecture during darkness.

4.7.3.2 Standby Lighting. A standby lighting system is different from continuous lighting since its intent is to create an impression of activity. The luminaires are not continuously lighted but are either automatically or manually turned on intermittently or responsively when activity is detected or suspected by the security force or IDS. Lamps with short restrike times are essential if this technique is chosen. This technique may offer significant deterrent value while also offering economy in power consumption.

1) Intermittent Lighting. A lighting system can be developed to turn lights on at random times as a deterrent to some threats. It can use either direct or indirect illumination concepts. While an intermittent lighting system can involve a duty cycle of 10 to 50 percent, it may increase operational and maintenance costs, it may force the use of inefficient lamps, or reduce lamp life. Deterrence can actually be higher for such a system

because of its appearance of activity. Luminaires may be controlled individually or as a group.

2) On-Demand Lighting. Rather than randomly activating the luminaires, an IDS sensor can be used to turn on the lights when an intruder is detected. This type of active lighting system provides maximum deterrent value at a low duty cycle. Such a responsive area system is subject to the same nuisance and false alarms of any sensor system.

4.7.4 Minimum Lighting Illumination Specification

4.7.4.1 Guard Visual Surveillance. Table 8 shows minimum lighting criteria. Lighting levels range from 0.2 footcandles (fc) [2.1 lux] near boundaries and perimeter fencing, increasing to 2 fc (2.1 lux) at entry areas. A lighting specification for visual guard surveillance to specific locations is presented in Table 8. This table provides general guidance for footcandles as a function of location type and for the amount of area that should be illuminated.

Table 8
Minimum Lighting Criteria for Unaided Guard Visual Assessment

Application			Illuminated Width feet (m)		Minimum Illumination	
Type	Lighting	Area	Inside	Outside	Footcandles (lux) (a)	Location
Boundary	Glare	Isolated	25 (7.6)	150 (46)	0.2 (2.1) (b) 0.4 (4.3)	Outer lighted edge At fence
	Controlled	Semi-isolated	10 (3.0)	70 (21)	0.2 (2.1) 0.4 (4.3)	Outer lighted edge At fence
	Controlled	Non-isolated	20-30 (6.1 - 9.1)	30-40 (9.1 - 1.2)	0.4 (4.3) 0.5 (5.4)	Outer lighted edge Within
Inner area	Area	General At Structures	All 50 (15)	-- --	0.2 - 0.5 (c) (2.1 - 5.4) 1 (11)	Entire area Out from structure
Entry point	Controlled	Pedestrian	25 (7.6)	25 (7.6)	2 (21)	Entry pavement and sidewalk
		Vehicular	50 (15)	50 (15)	1 (11)	

(a) Horizontal plane at ground level unless otherwise noted.
(b) Vertical plane, 3 feet (0.9m) above grade.
(c) Use higher value for more sensitive areas.

4.7.4.2 Lighting for CCTV Surveillance. Lighting requirements for CCTV are considerably higher than those required for direct visual surveillance. The entire assessment zone must have an average initial horizontal illumination level of 2 fc (21.5 lux) at 6 inches (150 mm) above the ground. The uniformity of illumination in the assessmment zone must meet the following requirements: (1) the overall ratio of brightest to darkest regions of the assessment zone must not exceed eight to one, and (2) the overall ratio of the

average brightest to darkest regions of the assessment zone must not exceed three to one.

Several methods are presently used in achieving these illumination levels. These employ high pressure sodium vapor roadway luminaires spaced to meet both the CCTV and other security illumination requirements. The most common variety of luminaire is the 250-watt (W) unit, while some facilities employ a 400-W unit. Some installations have opted for 150-W luminaires with an instant restrike capability.

4.7.5 Lighting Energy Considerations

4.7.5.1 Overview. Since the energy shortage of 1973-74, virtually every lighting system has come under scrutiny to identify energy savings. Security lighting systems are no exception. This scrutiny is probably as much related to the conspicuousness of security lighting as to the amount of energy consumed. While the only energy consumption statistics available on lighting pertain to the energy required to maintain street lighting systems, security lighting uses considerably less energy. Recently, the direction of the security community to reduce energy costs in security lighting has resulted in replacing luminaires to increase source efficacy by changing to high-pressure sodium (HPS) lamps. HPS lamps produce more lumens per watt than either mercury vapor or incandescent lamps. The latter two lamps are the most widely used in the United States today. Table 9 presents the relative efficiencies and restrike times of some typical lamps.

Table 9
Relative Efficiencies and Restrike Times of Light Sources
(From IES Lighting Handbook, J.E. Kaufman, ed.)

Lamp Type	Efficacy (Lumens/watt)	Restrike Time (minutes)
Theoretical Maximum	683	---
Ideal White Light	220	---
Incandescent	10-16	<1
Tungsten-Halogen	17-25	<1
Mercury Vapor	30-65	3-7
Fluorescent	33-77	<1
Metal Halide	75-125	up to 15
High-Pressure Sodium	60-140	1 (restrike) 3-4 (warm-up to full output)
Low-Pressure Sodium	180	7-15

for both pedestrian and vehicular access when designing the entry control

4.7.5.2 Restrike Time. The differences in restrike time among the various lamps (see Table 9) influence the selection of security lighting systems and concepts. For example, high-pressure sodium lamps are the primary light source of most security systems because of their efficiency (140 lumens/W). However, these lamps are not without deficiencies. From a cold start, a high-pressure sodium lamp warms up to full light output in about 10 minutes. It will usually restrike in less than 1 minute and warm-up in 3 to 4 minutes. During this warm-up interval, the lamp cannot be expected to operate at full light output, and this reduced capacity may be important in many high-security applications. Because of this restrike interval, incandescent lamps are sometimes used as the emergency backup light source because of their short restrike time. The evaluation of any security lighting system, particularly one requiring continuous illumination, requires careful analysis of lamp life, energy consumption, and restrike time. The security engineer who has determined that short restrike time is a critical performance parameter should determine whether it is economically feasible in relation to increased lamp replacement and energy costs.

4.8 Maintaining Essential Security Support Functions

4.8.1 Overview. Essential exterior site functions that support site and facility security include security power supply, general power supply, communications, and security control.

4.8.2 Security Power Supply. Both regular and standby power sources should be provided for IDS and security lighting. In some cases, dual emergency backup power sources may be required, particularly if power transformer stations are vulnerable. All critical power, communications, and IDS lines should be well protected, usually by burial. In the case of light poles, cabling should be internal to aluminum or steel poles. Standby power sources must be protected from sabotage by facility hardening and IDS coverage. Standby power sources should be configured for automatic activation when required.

4.8.3 General Installation Power Supply. Some of the best tools used for penetrating hardened facilities rapidly are electrically powered. Although a sophisticated attacker will probably not let himself be dependent on facility power sources, it is worthwhile to consider arrangements where the general power supply to a facility exterior and just outside any key interior barriers (other than that required for essential services such as IDS) is either normally shut off during nonworking hours or can be shut off remotely by the security forces. Switch and fuse boxes must be protected.

4.8.4 Communications. To the extent feasible and practical, consideration should be given to hardening both internal and external communications lines so that security forces will not be easily deprived of their use during emergencies. As mentioned above, communication lines essential to IDS alarm assessment should be hardened and protected with fail-safe features. Phone jacks for security personnel should be provided, as

necessary, at external locations. Another possible option is to equip security personnel with hand-held radios.

4.8.5 Security Control Center. A security control center is a continuously manned facility serving one or more of the following functions:

- Alarm annunciation, display, and control.
- Centralized control and communications for base, installation, or facility security operations.
- Quarters for security alert guard force.
- Monitoring of a remote entry control or surveillance system, such as closed circuit television, electronic locking devices and systems, and similar systems.
- Control of entry to restricted area.
- Housing, storage, or parking for guard force support equipment including arms, ammunition, portable communications and observation equipment, and vehicles.

Depending on the size of a facility or installation, the security control center can vary from an assigned and physically isolated area within a building to a structure designed and constructed especially for the purpose. These facilities must also be protected against a possible attack.

Section 5: BUILDING PHYSICAL SECURITY AGAINST FORCED AND COVERT ENTRY

5.1 Introduction. This section begins with a review of the threat severity levels for forced and covert entry (par. 5.2) followed by a description of the important elements required to achieve an effective integrated security system design for the building to counter these threats (par. 5.3). Minimum prescribed Department of Defense (DoD) security construction requirements for vaults and strongrooms; compartmental information facilities; arms, ammunition, and explosive facilities; and nuclear weapons and sensitive compartment information facilities are then provided in par. 5.4 including related penetration delay times. For cases where the minimum prescribed designs do not provide sufficient delay relative to guard response times, or when there are no prescribed designs for a given facility type, the reader is referred to par. 5.5 (for new construction) or par. 5.6 (for retrofit construction) for design options.

5.2 Threat Severity Levels for Forced and Covert Entry Design

5.2.1 Forced Entry. Forced entry threat severity is defined in terms of the relative energy level of the tools selected by an intruder to penetrate a barrier and gain entrance to a facility. The four basic threat severity levels are:

- Low Level - Low-observable, hand-powered tools only.
- Medium Level - Unlimited hand-powered tools and limited battery-powered tools.
- High Level - Unlimited hand, power, or thermal tools.
- Very High Level - Up to 50 pounds (23 kg) of explosives together with unlimited hand, power, and thermal tools.

As one proceeds from the low to very high severity levels, the technical skill or sophistication level of the threat also increases. Examples of the kinds of tools associated with the above threat levels are:

- Hand Tools. High-observable tools include the hammer, sledgehammer, cutting maul, shovel, pry axe, and pick head axe. Low-observable tools include claw tool, carpenter's saw, hacksaw, Kelly tool, bolt cutters, pliers, spanner wrench, tin snips, wrecking and pry bar, and wire cutters.
- Power Tools. Electric- or gasoline-powered circular or reciprocating saw with steel, diamond, carbide-tipped blade, or abrasive wheel; hydraulic bolt cutters; chain saw; sabresaw; drill or chisel rotohammer; rescue tools; and electric drill.

• Thermal Tools. Oxyacetylene, electric arc, or oxygen-fed cutting torch; oxygen lance; power lance; burning bar; and rocket torch.

• Explosives. Bulk TNT or plastic explosive either by itself or in combination with a tamper or flyer plate driven by the explosive to create a hole in a barrier.

The threat severity level applicable to a given facility depends on the assets in the facility and the relative technical skill, objectives, and motivation of potential threats. This level is established as part of the planning process (described in Section 2). Barrier penetration time data are provided for each threat severity level in par. 5.4 for the minimum prescribed construction, in par. 5.5 for new construction, and in par. 5.6 for retrofit construction.

5.2.2 Covert Entry. The covert entry threat attempts to enter a facility or portion of a facility using false credentials, etc. Objectives are similar to the forced entry tactic above. The aggressor may also attempt to compromise an intrusion detection and entry control system using stealth or saturation and deception to carry weapons or explosives into the facility. The four basic threat severity levels are:

- Low Level - Personnel.
- Medium Level - Personnel and contraband.
- High Level - Personnel, arms, contraband.
- Very High Level - Personnel, explosives, arms, contraband.

5.3 Integrated Security System Elements for the Building

5.3.1 Overview. The security elements associated with the building to ensure the effectiveness of an integrated security system design are: (1) barrier layout and construction to delay the intruder; (2) access control at points of entry to protect against covert entry threats; (3) intrusion detection sensors and alarms to detect an attack on or within the facility, and/or unauthorized insiders after hours; (4) CCTV to assess whether an alarm is actually a threat; and (5) guards to respond to the location of a real threat. All these elements are equally important. None of them can be eliminated or compromised if an effective security system is to be achieved. Also, without detection, the response force would not be alerted. In addition, the delay offered by the building components must provide sufficient time after detection for threat assessment and guard force response. The following provides a brief overview of each of these critical system elements referencing appropriate sources for their proper selection. The focus here is on how these various system elements complement and support the barrier design, which is the main subject of this handbook and which is addressed in detail in pars. 5.4, 5.5, and 5.6.

1. Locate critical assets on interior of facility in smallest volume possible.
2. Minimize window area.
3. Glass doors in foyers are to be backed by solid door or wall.
4. Do not allow windows to be next to doors such that aggressors could unlock the doors through them.
5. Layout buildings to conceal assets and make access difficult for intruders.
6. Simplify building configuration to eliminate hiding places.
7. Design circulation to provide unobstructed views from control points or occupied spaces.
8. Arrange building interiors to eliminate hiding places around asset location.
9. Locate assets in spaces occupied 24 hours/day where possible.
10. Locate activities with large visitor populations away from protected assets where possible.
11. Locate protected assets in common areas where they are visible to more than one person.
12. Place mail room on perimeter of facility.

Figure 28
Checklist of Minimum Building-Related Layout Considerations

5.3.2 Building Layout and Barrier Design. Section 3 describes the building layout and design process in detail. Figure 28 provides a summary checklist of minimum building-related layout considerations. In general, the critical assets to be protected should be located in the smallest volume possible at a central point well within the interior of a building presenting as many intermediate barriers to the intruder's path as possible. An example of a building layout that involves multiple barriers or shells is illustrated in Figure 6 (Section 3). As noted in Section 3, the total delay time offered by all these barriers should equal or exceed the anticipated guard response time. The total delay time, in turn, is the sum of the penetration times associated with each barrier plus the intruder ingress/egress time between all

barriers where the timeline starts at the first point of intrusion detection. If the building is surrounded by a fence or other exterior site-related barrier having an exterior IDS (see Section 4), the fence is the first layer of defense followed by the exterior of the building and any interior rooms, vaults, or containers. If there is no exterior fence IDS, the timeline starts with the first building barrier preceded by an interior IDS that can detect the intruder before penetration of this barrier occurs. In order to be effective, each separate element (i.e., exterior and interior walls, roof, floor, door, etc.) must offer an equivalent or balanced penetration delay time with no weak links. Paragraph 5.5 provides choices and barrier penetration delay times for new construction; par. 5.6 does so for retrofit construction.

5.3.3 Building Access Control

5.3.3.1 Introduction. This section summarizes information regarding methods for controlling access of personnel and materials at the entrance to buildings to protect against covert threats. Data sources containing building access control design details are contained in the following sources. The reader is referred there for details.

- NAVFAC Design Manual 13.02, Commercial Intrusion Detection Systems, September, 1986.
- SAND 87-1927, Entry-Control Systems Technology Transfer Manual, DOE/Sandia National Laboratory.
- CEGS 16752, Electronic Entry Control Systems, U.S. Army Corps of Engineers Guide Specification, April 1991.
- TM-5-853-4, Security Engineering Electronic Security Systems Manual, U.S. Army Corps of Engineers, February 1993.

5.3.3.2 Function and Location. The function of building access control is to ensure that personnel and materials entering the building have the proper authorization to do so. Control points are typically located at building entry points. Access controls also complement the role of interior intrusion detection systems. Often, intrusion detectors must be deactivated and placed in a nondetecting mode during normal working hours. During these periods, access controls provide a means to prevent unauthorized persons from entering a protected facility. An intrusion detection system using interior detectors will generally detect any unauthorized person who stays behind after working hours. Access control also restricts free access to those persons whose intent may be to tamper with intrusion detection system components or circuits. Maintaining the effectiveness of access control and intruder detection requires the complementary function of screening personnel for security clearances.

5.3.3.3 Minimum Requirements. DoD 5200.8-R states that a DoD component or installation develop, establish, and maintain policies and procedures to control access to installations. These are summarized in par. 4.4.3.

5.3.3.4 Personnel Identity Verification Systems. The purpose of a personnel identity verification system is to restrict access to only those personnel who have received previous authorization. There are three generic types of systems: manual systems, mechanical locks, and automatic electronic locks. The following summarizes these systems. The reader is referred to the sources identified in par. 5.3.3.1 for details.

1) Manual Systems. Manual systems frequently make use of a security identification badge. The badge is an entry credential which includes a photograph of the person wearing it. The individual keeps the badge and wears it at all times within the facility. Such badges have only low to medium effectiveness. For more control, one can institute a process of "badge exchange." In this method, an individual receives a security identification badge with a second badge retained within the security-controlled area. When access is desired, the security personnel exchange the duplicate badge for the individual's badge. When the individual leaves, the exchange is reversed. This procedure makes counterfeiting difficult because the intruder would have to gain access to the exchange badges. This is the recommended procedure for personnel-based systems.

2) Mechanical Locks. Various mechanical locking equipment can be used to control access without requiring the presence of security personnel. These include:

a) Keyed locks. Keys are the most common and least expensive way to open locked doors. They are also one of the least secure ways since keys are easy to copy. A key lock system is most effective when: (1) few keys are issued per door, (2) master keys are minimized, and (3) two differently keyed locks are used on each door, thus requiring a two-man access policy.

b) Combination locks. Combination locks include a dial or dials onto which an access code is entered activating the lock to open the door. These are inexpensive and allow a high level of personnel throughput. One advantage of access codes is that they cannot be lost and subsequently found by unauthorized people unless written down. Their primary disadvantage is how easily the access code can be passed to unauthorized people.

3) Automated Electronic Locks. Electronic locks are used to control the admission of personnel into protected areas. Electronic locks, however, cannot fulfill all the functions of a human sentry because they monitor only a limited portion of the observables (visual, audible, etc.) that can be observed by humans. The degree of access control afforded by electronic locks varies with the type of device used. Some electronic locks can only identify a code, which is either encoded on a card or badge carried

by the person or is memorized by the individual. The electronic lock that relies on an encoded card or badge offers the least control because cards and badges can be lost or stolen. The more sophisticated types of electronic locks actually identify the person seeking entry on the basis of some physical characteristic, such as fingerprints or dimensions of fingers. Some electronic locks use a combination of code and identification of a personal characteristic, for example, a numerical code and fingerprint identification. Some electronic lock systems may perform such additional functions as initiating an alarm or providing automatic personnel entry/exit inventory. The more common commercially available electronic locks and their applications are digital cipher locks, card locks, hand geometry comparison locks, and fingerprint-comparative locks. Regardless of spohistication, electronic locking systems are convenience locks only and should only be used for personnel ingress and egress.

a) Digital cypher locks. These are similar to the combination locks above except that the access code is entered into a keypad.

b) Card readers. Card readers are a means of electronic entry control which reads authorization information which has been encoded onto a card. Card readers are highly effective access control devices. Cards are difficult to counterfeit and the system has a high level of personnel throughput capability.

c) Video comparator system. This system requires a guard to verify an individual's identity based on visual characteristics. A securely stored image is compared with a real-time image of the individual requesting entry. Such systems are not considered positive personnel identity verification systems but they have the advantage that it is difficult to tamper with the stored image.

d) Fingerprints. Fingerprints are considered one of the most reliable means of personnel identification. Automatic pattern recognition and computerized data processing facilitate fingerprint identification.

e) Speech. Speech is useful for identity verification and well-suited to automated processing. Measurements include: waveform envelope, voice pitch period, relative amplitude spectrum, and vocal trait resonant frequencies.

f) Handwriting. Automated handwriting verification systems are available that utilize handwriting dynamics such as velocity and acceleration as a function of time. Statistical evaluation of these data indicates that an individual's signature is unique and provides a reliable method of verification of identity.

g) Hand geometry. These systems perform computerized statistical analysis of finger length data used in identifying a hand. Hand

geometry is a distinct measureable human characteristic which is unique to individuals.

5.3.3.5 Materials Access Control. Control of materials entering or exiting a building includes special nuclear materials (SNM), metal detectors, explosives, and packages. Detailed information for the following can be found in SAND 87-1927, Entry Control Systems Technology Transfer Manual.

1) Special Nuclear Materials. Monitors are utilized to detect concealed SNM on persons, in packages, or in vehicles exiting a controlled area. An SNM monitor generally consists of a Thermal Neutron Activation detector unit, signal processing electronics, and alarm logic. Thermal neutrons are used to irradiate containers when a search is being made for concealed SNM. The emitted neutrons and gamma rays are coincidentally detected by scintillator sensors to descriminate against source neutrons and gamma radiation. Detection is based on the high nitrogen contents of explosives. There are a number or SNM monitors available. Examples include:

a) Doorway monitors. Most commercially available SNM monitors are doorway monitors. While they provide high throughput, sensitivity is reduced.

b) Portal monitors. Portal monitors detect the presence of SNM within a detection volume that is usually much larger than that of doorway monitors. As a result, throughput times are generally longer than for doorway monitors.

c) Hand-held monitors. Los Alamos Scientific Laboratory (LASL) has developed a hand-held SNM monitor for manual and vehicle search. This monitor has the advantage of significantly lower cost compared to doorway monitors; however, it has the disadvantage of long search times.

d) Vehicle monitors. The primary difficulty in detecting SNM at vehicle entry control portals is the ease with which SNM can be shielded within a vehicle. At present, the most practical method of monitoring vehicles for SNM is a search conducted by guards equipped with hand-held monitors.

e) Sewer monitors. Lawrence Livermore Laboratory has developed a sewage monitor system that detects the deposition of radioactive material into a sewage system. The systems are not limited to sewage, but also can be used with other liquid effluents.

2) Metal Detectors. Metal detectors are used to detect weapons and hand tools intended for sabotage, or for the detection of metal used to shield SNM. Active metal detectors generate a time-varying electromagnetic field and respond to changes in the field caused by the introduction of metallic objects. Such changes are used to generate alarms.

3) Explosive Detection Sensors. Sensors to detect explosives are not capable of detecting all explosives. There are simply too many explosives compounds. Because of this, animals (typically dogs) are used most commonly for this purpose.

a) Vapor detection. One method of detecting explosives is by collecting the vapors emitted by the explosive material. The electron capture detector is the only inanimate means of explosives vapor detection which is currently available commercially. Most explosives vapors have a high electron affinity, that is, there is a high probability that thermalized electrons will attach to explosive vapor molecules. As a result, monitoring the electron concentration provides identification of molecules with high electron affinity.

b) Bulk detection. Detection of the bulk of an explosive is preferable to detection of explosives vapors since there is more physical material to be detected. Unfortunately, there are no commercially available bulk explosives detectors, although several are under development.

4) Package Search Systems. Package search sensors are available to prevent theft of contraband or weapons from entering a facility.

a) X-ray systems. X-ray systems are currently in use by commercial airlines. An image of the contents of packages is obtained by pulsed X-ray techniques. X-ray baggage inspection systems are designed for high throughput search of handbags, briefcases, and luggage. Preferential package orientation may be needed to optimize the probability of detection.

b) Computerized tomography. Computerized tomography (CT) is an X-ray technique which provides two-dimensional images of cross-sectional slices of an object. By combining a number of adjacent slices, a three-dimensional image can be obtained. The CT technique provides maximum sensitivity and accuracy for material detection and identification.

5.3.4 Building Located Intrusion Detection Systems. This section provides a summary of the function and placement of interior intrusion detection systems (IDS). This includes the types of sensors available and typically deployed. The reader is referred to the following sources for more detailed design information:

- NAVFAC Design Manual 13.02, Commercial Intrusion Detection Systems, September 1986.
- Manual TM-5-853-4, Security Engineering, Electronic Security Systems, U.S. Army Corps of Engineers, February 1993.
- ESE-SIT-0001, Siting Criteria for Standardized Electronic Security Equipment, Air Force, March 1991.

- NFGS 16726C, Basic Intrusion Detection Systems, NAVFAC Guide Specification, April 1991.

- NFGS 16727C, Commercial Intrusion Detection Systems, NAVFAC Guide Specification, April 1991.

5.3.4.1 Function and Location

1) Function. In order that security guards can respond to an intrusion, threat detection either by security personnel or by using a remote intrusion detection system (IDS) is required. The function of an IDS is to initiate the system response by detecting an overt attack against the facility, covert entry threats, or unauthorized insiders after hours. IDS performance parameters of concern include: completeness of coverage, probability of detection, the alarm zone resolution, and false and nuisance alarm rates. The use of IDS involves inherent risks. For example, guard requirements for threat assessment may increase because of high false or nuisance alarm rates associated with detection sensors. One way of minimizing the latter problem is to design systems where the disturbance threshold level for activating the sensor is high, but within the level of that created by the intruder.

2) Location. IDS should be located to detect a penetration attempt before any building barriers enclosing the protected area are breached. If this is not done, the delay time offered by the barriers cannot be counted in the overall delay which is compared to the guard force response time. IDS systems are available that can be located on either barrier surfaces, or to cover interior volumes within buildings. These are summarized in the following.

5.3.4.2 Minimum Requirements. Minimum IDS requirements established by DoD relate to exterior IDS systems rather than building interior systems. The reader is referred to par. 4.5.3 for a discussion.

5.3.4.3 Detection at the Barrier. This section summarizes sensors used for detection at the surfaces of walls, floors, ceilings, doors, windows, and utility openings.

1) Walls/Floors/Ceilings

a) Vibration sensors. Vibration sensors, also called "shock" sensors, are mechanical contact switches designed to activate when the surface on which the sensor is mounted starts to vibrate. Rigid materials such as reinforced concrete or masonry make excellent surfaces for this

sensor. Metal surface should be avoided. Installation should always be specified on the inside surface (within the protected area).

b) Grid-wire sensors. Grid-wire sensors are a wire mesh embedded in or affixed to building barriers which cause an alarm to occur when broken. These sensors must be embedded in the barrier to conceal the grid.

2) Doors/Windows/Utility Openings

a) Balanced magnetic switches. Also referred to as door "switches," this sensor is the most commonly used intrusion detection device. The standard magnetic switch sensor consists of two components: one contains contacts that open or close in the presence of a magnetic field, the other contains the magnet which provides the magnetic field. It is possible to defeat a "plain" magnetic switch by placing a strong magnet near the switch, thus preventing the contacts from activating when the normal switch magnet is moved away, as when the door opens. As a result, the only acceptable type of magnetic switch for most DoD applications is the balanced or biased magnetic switch (BMS).

b) Glass breakwire sensor. This type of sensor is used to detect breakage of glass by an intruder. The breakage of glass also causes the breakage of a thin, low tensile strength wire embedded in the window mullions or overlaid on the glass itself. This breakage interrupts a low voltage direct current that runs through the wire, generating an alarm.

c) Window vibration/ultrasonic sensors. Both of these sensors are known as "window bugs." Vibration sensors detect attempts to penetrate windows. Ultrasonic sensors detect the sounds made by forcible intrusions even if the sounds are not audible to the human ear. Such sensors are passive receivers consisting of a microphone and an electronic processor which discriminates between "noise" such as human speech, and the specific frequency associated with forcible entry attempts.

5.3.4.4 Detection Within Building Interior Volumes. Volumetric detectors detect the presence of an intruder within a given volume of space. The following are the most commonly deployed.

1) Ultrasonic. This sensor emits ultrasonic energy (inaudible to the human ear) and sets up a "standing" energy field which is sensed by a receiver. This sensor works on the Doppler principle. That is, any movement in the field produces a frequency change which is detected by the receiver and causes an alarm. Electronics within the sensor permit adjustment of the alarm

threshold. As a result, the sensor can distinguish between movements of both small objects (such as birds) and the larger motions of humans. The pattern should be set up in an area with stable surfaces avoiding objects whose surfaces can vibrate.

2) Microwave. This sensor is a transceiver which transmits and receives a radar frequency wave pattern. The sensor detects changes in the wave pattern generated by movements and results in alarms. The wave pattern will penetrate glass, masonry walls, and other nonmetallic barriers so that the sensor should not be aimed at an outside wall. Sources of nuisance alarms, such as wind-caused movement of metal objects, should be avoided.

3) Passive Infrared. Passive infrared sensors respond to the energy emitted by the human intruder, which is comparable to the heat radiated by a 50-watt light bulb. As infrared energy does not penetrate most building materials, sources located exterior to the facility will not typically generate false alarms. However, local heating effects can lead to false alarms via sunlight through windows. Such geometries should be avoided during sensor placement.

4) Sonic sensors. Sonic sensors can be active or passive. Passive systems in their simplest forms use a microphone and an amplifier to detect sounds generated by an intruder. Active sensors are equivalent to ultrasonic sensors operating at audio frequencies. They detect the Doppler frequencies generated by intruder motion.

5) Capacitance proximity sensor. This interior sensor is used to detect intrusions to metal objects. The sensor detects changes in capacitance between the protected object and ground that are caused by the approach of an intruder. The alarm relay is activated in a fail-safe configuration so that an intruder, loss of power, or breaking of the protection loop will cause an alarm.

5.3.4.5 Duress Switches. Duress switches activate remotely located alarms. They are typically placed in hidden locations and activated by guards or other personnel.

5.3.5 Closed-Circuit Television (CCTV)

5.3.5.1 Introduction. The same CCTV technology discussed under exterior site security (par. 4.6) can also be applied for threat assessment and surveillance on building exteriors or within building interiors. The following briefly describes its application to the building. The reader is referred to par. 4.6 for a summary of the technology. Sources of more detailed design information include:

- NAVFAC Design Manual 13.02, Commercial Intrusion Detection Systems, September 1986.

- Manual TM-5-853-4, Security Engineering, Electronic Security Systems, U.S. Army Corps of Engineers.

- SAND 89-1924, Video Assessment Technology Transfer Manual, DOE/Sandia National Laboratory.

- ESE-SIT-0001, Siting Criteria for Standardized Electronic Security Equipment, Air Force, March 1991.

5.3.5.2 Function and Location. CCTV systems are normally deployed on or within buildings and consist of a television camera, monitor, and electrical circuitry. When an alarm occurs, a CCTV may be triggered automatically or alternatively by personnel at the control center to determine whether response forces should be dispatched to the alarmed area. The following summarizes the functions and typical deployment locations of the CCTV.

1) Threat Assessment. As an alarm assessment system, CCTVs are designed to respond manually or automatically upon receipt of IDS alarms at the Security Center. A properly integrated assessment CCTV system provides a rapid and cost-effective method for determining the cause of intrusion alarms and assessing the threat (see pars. 2.4.1 and 2.4.3). It allows such evaluations to be made from physically remote locations. Recorders can be used to record alarm events for assessment at a later time.

2) Surveillance. CCTVs can also be used for surveillance. As a surveillance system, CCTVs are typically designed to be used at the discretion of and under control of the Security Center console operator.

3) Location. CCTV cameras may be mounted on building exterior walls or roofs to observe outside surfaces. They may also be located at entrances to secure areas to aid access control or within building interior spaces for threat assessment.

5.3.5.3 Minimum Requirements. Minimum DoD requirements for CCTV apply primarily to exterior site perimeter deployment rather than on building exteriors or within interiors. These requirements are described in par. 4.6.

5.3.5.4 Available Technology. The reader is also referred to par. 4.6 for a summary of available CCTV technology.

...ions or certain key terms. It then provides a step-by-step procedure ... derini...

5.4 Minimum Construction Requirements. This section describes minimum DoD security requirements for vaults and strongrooms; arms, ammunition, and explosive (AA&E) facilities; and nuclear weapon and sensitive compartment information facilities. If your facility is not any of these, you may proceed directly to par. 5.5 for new construction, or to par. 5.6 for retrofit construction.

5.4.1 General. DoD requires that sensitive or dangerous material be protected in secure structures. In many instances, specific construction is prescribed for major construction elements such as walls, floors, roofs/ceilings, doors, windows, etc. This section summarizes these prescribed requirements and the minimum penetration times for each forced entry threat severity level. Please note that you should consider these prescribed construction requirements as minimum. In no case shall a design provide a penetration time less than those summarized here. On the other hand, if you find your guard response time requires a higher penetration time for the facility than provided by the prescribed construction, par. 5.5 (for new construction) or par. 5.6 (for retrofit construction) provide design options to meet these added requirements.

5.4.2 Vaults. Minimum security requirements for vaults are specified in DoD 5200.1R, Information Security Program Regulation. There are two classes of vaults for the storage of classified material and equipment: A and B. Class A vaults offer the maximum in protection. Class B vaults offer adequate protection. In some cases, a lightweight, portable "modular vault" may be applicable. The class of vault applicable to your case depends on the classification level of the documents, material, or equipment to be stored. The minimum DoD construction requirements for each class of vault are described as follows.

5.4.2.1 Class A Vaults

1) Minimum Construction. As shown in Table 10, DoD 5200.1-R requires that the walls, floors, roof, and ceilings be a minimum of 8-inch (200-mm)-thick reinforced concrete with the standard reinforcing shown in the table. In addition, the walls are to extend to the underside of the roof slab above. When vault walls are part of exterior walls, the vault wall must be set back from the exterior part of the exterior wall to allow 4 inches (100 mm) for the normal wall facing to cover the vault wall. In addition, a Class 5 door with the dimensions shown in Figure 29 is to be provided. This door shall be equipped with an emergency escape and relocking device (DoD 5200.1-R). The escape device must not be activated by the exterior locking device and must be permanently attached to the inside of the door to permit escape by persons inside the vault.

Table 10
Minimum Construction Requirements for Class A Vaults (DIAM 50-3)

Minimum Construction Requirement		Minimum Penetration Time (minutes)			
		Low	Medium	High	Very High
Walls	8-inch (200-mm) Reinforced Concrete (a)	(c)	(c)	12 (b)	<1
Floors	8-inch (200-mm) Reinforced Concrete (a)	(c)	(c)	18 (b)	<1
Roof/Ceiling	8-inch (200-mm) Reinforced Concrete (a)	(c)	(c)	12 (b)	<1
Door/Frame	Class 5 (Fed Spec AA-D-00600C)	(c)	10	2	<1

(a) Assumes standard reinforcing: The most commonly used to prevent forced entry incorporates No. 5 bars, 6 inches (15 mm) on-center each way, staggered each face.
(b) Penetration time is for an upward attack for other than floors on grade (not practical to attack).
(c) Not practical to attack at this threat severity level.

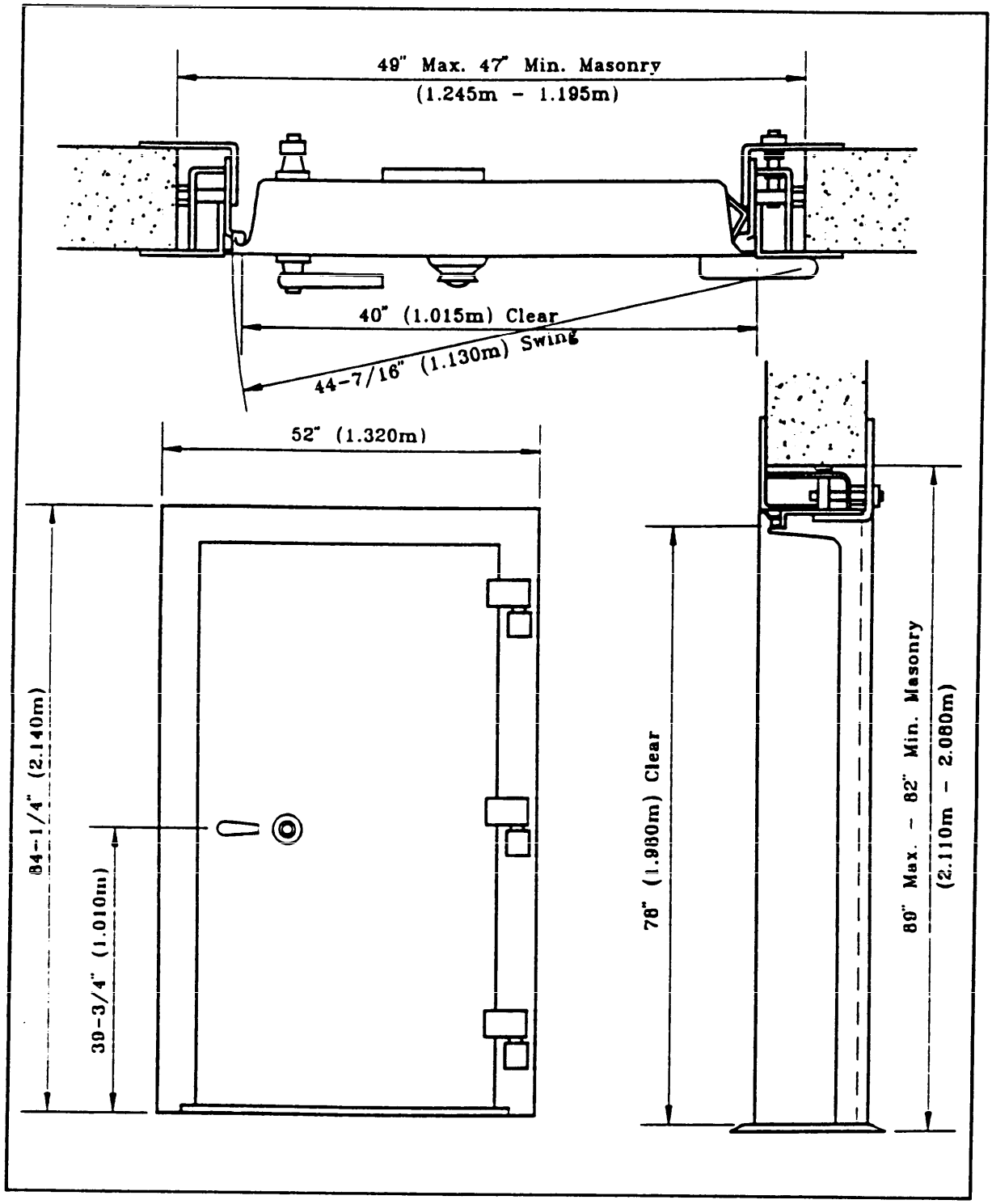


Figure 29
Class 5 Vault Door Dimensions

2) Forced Entry Penetration Times. Penetration times for the four threat severity levels are shown in Table 10. The low level corresponds to the use of simple low-observable, hand-held tools. The medium level consists of all hand-applied and some battery-operated tools. High level threats include power tools such as burn bars, jackhammers, etc. The very high level threat includes explosives. As shown in Table 10, it is not practical to attack the walls, roofs, and ceilings at the low- and medium-threat levels. The doors can be defeated within 10 minutes for medium and 2 minutes for high severity threats. Other openings can be defeated within less than a minute. Minimum penetration times against a high-level attack are 15 minutes for the walls and roof/ceilings. An upward attack on floors from below requires 18 minutes. Floors on-grade are not practical to attack. Against the very high level of attack, the minimum penetration times are all less than 1 minute.

5.4.2.2 Class B Vaults

1) Minimum Construction. Minimum requirements for Class B vaults are summarized in Table 11. As shown, the walls are to be not less than 8-inch (200-mm)-thick brick, or filled concrete block masonry units. Hollow masonry units are to be the vertical-cell type (load bearing) filled with concrete and steel reinforcement bars. Monolithic steel-reinforced concrete walls at least 4 inches (100 mm) thick may also be used. Floors are to be monolithic concrete construction not less than 4 inches (100 mm) thick. The roof is to be monolithic reinforced concrete slab of a thickness to be determined by structural requirements, but not less than 4 inches (100 mm) thick. Class 5 vault door requirements are the same as for Class A vault doors.

2) Penetration Times. Minimum penetration times achieved by the above minimum construction are also shown in Table 11. Walls provide from 2.5 to 4 minutes against medium-level threats and doors provide about 10 minutes against a medium-level threat and 2 minutes against a high-level threat. Roof/ceiling penetration times are about 5 minutes. An upward attack on the floor is about 9 minutes for a high severity threat. Penetration times for the very high threat are all less than 1 minute.

5.4.2.3 Modular Vaults. Although not General Services Administration (GSA) approved for the storage of classified material, the modular vault may be appropriate in selected circumstances. Consult your first echelon command for approved systems. Modular vaults can be procured under Federal Specification AA-V-2737. They are lightweight in comparison to the standard security vault. They are relocatable, easier and quicker to install, have reduced floor loading, and are less expensive. Additionally, they can be custom-designed to meet user specifications in terms of size, shape, and weight. Any number of panels of various sizes can be combined to fit specific space requirements, producing a customized vault with virtually no design restrictions. As of

clear distinction must be maintained between what [illegible] design threat.

this printing, available modular vaults have not passed GSA test requirements. Consult your first echelon command for approved systems.

Table 11
Minimum Construction Requirements For Class B Vaults (DoD 5200.1-R)

Minimum Construction Requirement		Minimum Penetration Time (minutes)			
		Low	Medium	High	Very High
Walls	8-inch (200-mm) brick	(a)	2.5	2.5	<1
	8-inch (200-mm) concrete block masonry units, concrete filled, rebar in each core (b)	(a)	4.0	4.0	<1
	4-inch (100-mm) monolithic, steel reinforced concrete (c)	(a)	3.0	3.0	<1
Floors	Minimum 4-inch (100-mm) monolithic concrete (c)	(a)	(1)	9 (d)	<1
Roof/ Ceiling	Minimum 4-inch (100-mm) monolithic reinforced concrete slab thickness determined by structural requirements. (c)	(a)	5.0	5.0	<1
Door/Frame	Class 5 (Fed Spec: AA-D-00600C)	(a)	10	2.0	<1

(a) Cannot be defeated at this threat severity level.
(b) Assumes No. 4 (12.7-mm) rebar
(c) Assumes 6- by 6-inch (150- by 150-mm) welded wire fabric.
(d) Penetration time is for an upward attack for other than floors on grade (which are not practical to attack).

5.4.3 Strongrooms. A strongroom is an interior space enclosed by, or separated from, other similar spaces by four walls, a ceiling, and a floor, all of which are normally constructed of solid building materials. A strongroom would be appropriate for storage of highly pilferable items and property of high value, e.g., electronics equipment. Classified items are generally stored in vaults.

5.4.3.1 Minimum Construction. Minimum construction requirements for strongrooms are summarized in Table 12.

5.4.3.2 Penetration Times. Minimum penetration times for the four threat levels are also provided in Table 12.

5.4.4 Arms, Ammunition, and Explosives (AA&E) Facilities

5.4.4.1 Minimum Requirements for AA&E Facilities

1) Minimum Construction. Minimum construction requirements are specified in DoD 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives. These requirements are summarized in Table 13 for security Risk Categories I through IV for Ammunition and Explosives. Table 14 applies to Risk Categories II through IV and non-earth-covered magazines. The security risk categories are defined in Table 15.

a) Walls/Floors/Roofs. Walls, floors, and roofs are to be a minimum of 8-inch (200-mm) concrete reinforced with two grids of No. 4 (12.7-mm) rebar on 9-inch (225-mm) centers; or 8-inch (200-mm) filled-concrete block reinforced with No. 4 bars (12.7 mm); or 8-inch (200-mm) interlocked brick. In addition, DoD 5100.76M requires that security Risk Categories I and bulk explosives of II (Table 15) magazine construction be acceptable for storage as specified in DoD 5154.4, the Ammunition and Explosive Safety Standard. To achieve explosive safety based on DoD 5154.4, the following magazine headwall construction is most commonly used:

> 12 inches (300 mm) of concrete reinforced with two grids of No. 6 (19-mm) steel bars spaced 12 inches (300 mm) apart, both horizontally and vertically and staggered each face to form a grid approximately 6 inches (150 mm) square.

Consequently, Risk Category I and II magazines have headwalls that are typically 12 inches (300 mm) or thicker and achieve a penetration delay time of 26 minutes against a high-severity threat.

Table 12
Minimum Construction Requirements For Strongrooms (DoD 5200.1-R)

Minimum Construction Requirement		Minimum Penetration Time (minutes)			
		Low	Medium	High	Very High
Walls	Plaster, gypsum board, metal, handboard, wood or plywood with No. 9 gauge (3.8-mm), 2-inch (50-mm) wire mesh or stronger.	<1	<1	<1	<1
Floors	Use standard structural requirements.	<1	<1	<1	<1
Roof/Ceiling	Plaster, gypsum board, metal hardboard, wood, plywood, No. 9 gauge (3.8-mm), 2-inch (50-mm) wire mesh or stronger.	<1	<1	<1	<1
Door/Frame/ Lock	Metal or solid wood reinforced with a metal panel, louvers/baffle plates reinforced with No. 9 gauge (3.8-mm), 2-inch (50-mm) wire mesh. Built-in, three-position Group 1 or 1R combination lock.	<1	<1	<1	<1
Misc. Openings	If larger than 96 sq in. (0.06 sq m), wire mesh, (No. 18 gauge (1.1-mm), 2-inch (50-mm)-square mesh. USN requires 9 gauge)	<1	<1	<1	<1
	or				
	1/2-inch (12.5-mm) steel bars, 6-inch (150-mm) spacing on bars.	0.6	0.6	0.14	<0.1

b) Doors. Table 16 provides examples of doors for explosive safety in DoD 5154.4. More information on AA&E doors can be found in par. 5.5.5.3.

c) Miscellaneous openings. See Tables 13 and 14.

Table 13
Minimum Construction Requirements For Risk Categories I Through IV
(DoD 5100.76-M)

Minimum Construction Requirement		Minimum Penetration Time (min)			
		Low	Med	High	Very High
Walls	8-inch (200-mm) concrete reinforced with No. 4 (12.7-mm) reinforcing bars, 9 inches (150 mm) on center, in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square.	(a)	(a)	15	<1
	or				
	8-inch (200-mm) concrete block (or concrete masonry unit) with No. 4 (12.7-mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course.	(a)	4.0	4.0	<1
	or				
	at least 8 inches (200 mm) of brick interlocked between inner and outer courses.	(a)	2.5	2.5	<1
Floors	Minimum 6-inch (150-mm) concrete construction reinforced with 6- by 6-inch (150- by 150-mm) W4 by W4 mesh or equivalent bars.	(a)	(a)	18 (b)	<1
Roof/ Ceilings	Reinforcing bar spacing will form a grid using No. 4 (12.7-mm) bars or larger so that the area of any opening does not exceed 96 sq in. (0.06 sq m). If ceiling or roof is of concrete pan-joist construction, the thinnest may not be less than 6 inches (150 mm) and the clear space between joists may not exceed 20 inches (500 mm).	(a)	(a)	7.6	<1
Doors/Frame	Refer to drawings in source, see Table 16 for typical construction.	(a)	(a)	4	<1
Locks/Hasps	High security locks (MIL-P-43607), see Figure 40.	(a)	4	<1	<1
	High security hasp (MIL-H-29181), see Figure 41.	(a)	4	<1	<1
Misc. Openings	Openings of 96 sq in. (0.06 sq m) or more with the least dimension greater than 6 inches (150 mm) will be protected by:				
	Minimum 3/8-inch (9.5-mm) hardened steel rods with maximum 4-inch (100-mm) spacing with horizontal bars so that openings do not exceed 32 sq in. (200 sq mm).	0.8	0.8	0.3	<0.1
	or				
	Riveted steel grating (weight of 13.2 lb/ft^2 (64.5kg/m^2) or welded steel grating (weight of 8.1 lb/ft^2 (39.6kg/m^2) with 1- by 3\16-inch (25.4- by 4.7-mm) bearing bars.	(a)	4.0	1.0	<1

(a) Cannot be defeated at this threat severity level.
(b) Penetration is for an upward attack for other than floors on grade (not practical to attack)

Table 14
Minimum Construction Requirements for Risk Categories II Through IV Arms, and Non-Earth-Covered Magazines (DoD 5100 76-M)

Minimum Construction Requirement		Minimum Penetration Time (min)			
		Low	Med	High	Very High
Walls	8-inch (200-mm) concrete reinforced with No. 4 (12.7-mm) reinforcing bars, 9 inches (150 mm) on center in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm) square.	(a)	(a)	15	<1
	or				
	8-inch (200-mm) concrete block (or concrete masonry unit) with No. 4 (12.7-mm) bars threaded through block cavities filled with mortar or concrete and with horizontal joint reinforcement at every course.	(a)	(a)	4.0	<1
	or				
	at least 8 inches (200 mm) of brick interlocked between inner and outer courses.	(a)	(a)	2.5	<1
Floors	Minimum 6-inch (150-mm) concrete reinforced with 6- by 6-inch (150- by 150-mm) W4 by W4 mesh or equivalent bars.	(a)	(a)	18(b)	<1
Roof/ Ceilings	Reinforcing bar spacing will form a grid using No. 4 (12.7 mm) or larger so that the area of any opening does not exceed 96 sq in. (0.6 sq m). If ceiling or roof is of concrete panjoist construction, the thinnest may not be less than 6 inches (150 mm) and the clear spaces between joists may not exceed 20 inches (500 mm).	(a)	(a)	7.6	<1

(a) Not practical to attack.
(b) Penetration time is for an upward attack for other than floors on grade (not practical to attack)

Table 14
Minimum Construction Requirements for Risk Categories II Through IV, Arms and Non-Earth-Covered Magazines (Continued)

Minimum Construction Requirement		Minimum Penetration Time (min)			
		Low	Med	High	Very High
Door/ Frame	1-3/4-inch (44-mm) solid or laminated wood with 12-gauge (2.7-mm) steel plate on outside face.	(a)	0.8	<1	<1
	or				
	1-3/4-inch (44-mm) hollow metal, industrial type construction with minimum 14-gauge (1.9-mm) skin plate thickness, internally reinforced vertically with continuous steel stiffeners spaced 6 inches (150 mm) maximum on center.	(a)	2	<1	<1
	or				
	GSA Class 5-per Fed Spec: AA-D-00600C	(a)	10	2.0	<1
Locks/ Hasp	High security lock (MIL-P-43607), see Figure 40.	(a)	4	<1	<1
	High security hasp (MIL-P-29181), see Figure 41.	(a)	4	<1	<1
Misc. Openings	Minimum 3/8-inch (9.5-mm) hardened steel rods with maximum 4-inch (100-mm) spacing with horizontal bars so that openings do not exceed 32 sq in. (0.02 sq m).	0.8	0.8	0.3	<0.1
	or				
	Riveted steel grating [weight of 13.2 lb/sq ft (64.5 kg/sq m)] or welded steel grating [weight of 8.1 lb/sq ft (39.6 kg/sq m)] with 1- by 3/16-inch (25.4- by 4.7-mm) bearing bars.	(a)	4.0	1.0	<1

(a) Not practical to attack.
(b) DoD 5100.76-M requires 3/8-inch (9.5-mm) rods as a minimum.

these guards are deployed in operating configurations that include the

Table 15
Security Risk Categories (DoD 5100.76-M)

Class(a)	Arms	Ammunition & Explosives
Cat. I	Not Applicable.	Explosive rounds for non-nuclear missiles and rockets in ready-to-fire configuration. Non-nuclear missiles and rockets in a ready-to-fire configuration.
Cat. II	Light automatic weapons up to and including 0.50 caliber (12.7 mm).	Grenades, high explosives, and white phosphorus; mines, antitank, and antipersonnel (unpacked weight of 100 pounds (45 kg) or less); explosives used in demolition operation; explosive rounds for missiles and rockets other than Category I (unpacked weight of 100 pounds (45 kg) or less).
Cat. III	Launch tube and gripstock for Stinger; launch tube excluding the 4.2-inch; grenade launchers; rocket and missile launchers (unpacked weight of 100 pounds (45 kg) or less); flame throwers; launcher, missile guidance, and/or optical sight for TOW.	Ammunition, 0.50 caliber (12.7 mm) and larger, rocket and missile warheads with explosive-filled projectile with unpacked weight of 100 pounds (45 kg) or less); grenades, incendiary and grenade fuzes; blasting caps; detonating cords; supplementary charges; bulk explosives.
Cat. IV	Shoulder-fired weapons other than grenade launchers; handguns; recoilless rifles up to and including 3.6 inches (90 mm).	Ammunition with nonexplosive projectiles (unpacked weight of 100 pounds (45 kg) or less); fuzes (except grenade fuzes, Category III); grenades, illumination, smoke and practice, CS/CN (tear producing); incendiary destroyers; riot control agents (100-pound (45-kg) package or less); ammunition for arms not otherwise categorized.

(a) As a general rule only arms, missiles, rockets, explosive rounds, mines, projectiles, etc., which have an unpacked unit weight less than 100 pounds (45 kg) or less are classified.

2) Penetration Times. Minimum penetration times for the four threat levels are given in Tables 13 and 14. Table 16 also gives the results of penetration tests showing that current magazine door designs can be opened in about 4 minutes. In general, current door designs offer lower penetration resistance than headwall construction for Risk Categories I and II used today. More information on locks is provided in par. 5.5.6.

5.4.5 Nuclear Weapons Facilities

5.4.5.1 Minimum Construction. Minimum construction requirements are summarized in Table 17 based on DoD 5210.41-M. Walls are to be a minimum of 8-inch (200-mm) concrete reinforced with two grids of No. 4 (12.7-mm) rebar on 9-inch (225-mm) centers in each direction and staggered on each face to form a grid approximately 4-1/2 inches (114 mm); or 8-inch (200-mm) concrete block with 3 inches (75 mm) of fibrous concrete bonded to the inside. Floors and roofs/ceilings have the same requirements as the walls. Doors are to be 1-3/4-inches (44-mm)-thick solid wood with 12-gauge (2.7-mm) steel outer face or 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. Miscellaneous openings use 1-1/4-inch (32-mm) by 3/8-inch (9.5-mm) flat steel bars spaced 8 inches (200 mm) vertically and 1/2-inch (12.5-mm) rods 4 inches (100 mm) apart horizontally or 1-1/2-inch (38-mm) by 3/8-inch (9.5-mm) flat steel bars spaced 8 inches (200 mm) apart vertically and 3/4-inch (19-mm) rods 4 inches (100 mm) apart horizontally.

5.4.5.2 Penetration Times. Table 17 shows the minimum penetration times for the prescribed nuclear weapon facility construction. Note that walls provide up to 25 minutes for the medium-level threat and 22.6 minutes for the high-level threat. Doors and miscellaneous openings can be penetrated in less than 1 minute.

5.4.6 Sensitive Compartmented Information Facilities (SCIF). The term SCIF describes classified information concerning or derived from intelligence sources. The facility contains methods or analytical processes that are required to be handled exclusively within formal access control systems established by the DoD Director of Central Intelligence.

5.4.6.1 Minimum Construction. Minimum construction requirements for SCIFs are summarized in Table 18.

5.4.6.2 Penetration Times. Minimum penetration times for the four threat levels are also provided in Table 18.

Table 16
Typical Magazine Door Panels For Explosive Safety For Risk Categories I Through IV For Ammunition and Explosives (a)

Overall Thickness in (mm)	Steel Plate Faces		Stiffeners		Minimum Penetration Times (minutes)			
	Outside in (mm)	Inside in (mm)	Type	Spacing	LOW	MED	HIGH	VERY HIGH
10.75 (270)	1/2 (12.5)	1/4 (6.25)	10-inch (250-mm) wide flange 49 lb/ft (75 kg/m).	18 inches (450 mm) apart, horizontal spaces	(b)	(b)	4	<1
7.75 (194)	3/8 (9.4)	3/8 (9.4)	7-inch (175-mm) structural Tee from wide flange 17 lb/ft (25 kg/m).	17 inches (425 mm) apart	(b)	(b)	4	<1
4.62 (115)	5/16 (7.8)	5/16 (7.8)	4-inch (100-mm) structural Tee from wide flange 12 lb/ft (18 kg/m).	17 inches (425 mm) apart, horizontal spaces	(b)	(b)	4	<1

(a) Category I and II storage magazines have an IDS requirement.
(b) Cannot be defeated at this threat severity level.

Table 17
Minimum Construction Requirements For Nuclear Weapons Maintenance Facilities (DoD 5210.41-M)

Minimum Construction Requirement		Minimum Penetration Time (minutes)			
		Low	Med	High	Very High
Walls	8-inch (200-mm) concrete reinforced with 2 grids of No. 4 (12.7-mm) bars on 9-inch (225-mm) centers. or 8-inch (200-mm) filled-concrete block with 3 inches (75 mm) of fibrous concrete bonded to block by 2-1/2-inch (62.5-mm) case-hardened nails on 6-inch (35.5-mm) spacing driven 1 inch (25 mm) into block.	(a) (a)	(a) 25	15 22.6	<1 <1
Floors	Same as Walls.	(a)	(a)	18 (b)	<1
Roof/ Ceiling	Same as Walls.	(a)	(a)	see walls above	<1
Door/ Frame	1-3/4-inch (44-mm)-thick solid wood with 12-gauge (2.7-mm) steel outer face. or 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.	(a) (a)	0.8 4	0.8 <1	<1 <1
Misc. Openings	1-1/4-inch (32-mm) by 3/8-inch (9.5-mm) flat steel bars spaced 8 inches (200 mm) vertically and 1/2-inch (12.5-mm) rods 4 inches (100 mm) apart horizontally. or 1-1/2-inch (38-mm) by 3/8-inch (9.5-mm) flat steel bars spaced 8 inches (200 mm) apart vertically and 3/4-inch (19-mm) rods 4 inches (100 mm) apart horizontally.	(a) (a)	2 2	0.2 0.3	<0.1 <0.1
Locks/ Hasps	High security lock (MIL-P-43607) see Figure 40. High security hasp (MIL-P-29181) see Figure 41. AIB Requirement for USN.	(a) (a)	4 4	<1 <1	<1 <1

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

Table 18
Minimum Construction Requirements For Sensitive Compartmented Information Facilities (a)

Minimum Construction Requirement		Minimum Penetration Time (Minutes)			
		Low	Med	High	Very High
Walls	Expanded Metal Reinforcement Construction Reinforced on inside with 9-gauge (3.8-mm) expanded metal.	1	1	<1	<1
	Steel Plate Reinforcement Construction Reinforced on inside with 1/8-inch (3.2-mm) steel plate.				
	• 4-inch (100-mm) reinforced concrete	(b)	(b)	4	<1
	• 8-inch (200-mm) stone or brick	(b)	(b)	4	<1
	Drywall Construction	<1	<1	<1	<1
Floors	Same as walls.				
Roof/ Ceiling	Same as walls.				
Door/ Frame	Class 5 (Federal Spec AA-D-00600C)	(b)	10	2.0	<1
	16 gauge (1.5 mm) with 1-3/4-inch (33-mm) wood	(b)	0.8	0.8	<1
	1-3/4-inch (33-mm) solid core wood	(b)	<0.8	<0.8	<0.8
	1-3/4-inch (33-mm) metal	(b)	4	<1	<1
Vault	8-inch (200-mm) reinforced concrete with 1 grid of 5/8-inch (16-mm) bars horizontally and vertically 6 inches (150 mm) on center.	(b)	(b)	15	<1
	or				
	Minimum 1/4-inch (6.4-mm) steel lining on other construction.	(b)	(b)	1	<1

(a) DIAM 50-3, Physical Security Standards for Construction of Sensitive Compartmented Information Facilities.
(b) Not practical to attack at this threat severity level.

5.5 New Construction Design

5.5.1 Introduction

5.5.1.1 Overview. This section provides design options for hardening a new building against forced entry penetration. Hardening options for the very high-severity threats (explosives in combination with hand, power, or thermal tools) are addressed in par. 5.5.2. This is followed by design options for the low-, medium-, and high-severity threats in par. 5.5.3 for walls, par. 5.5.4 for roofs and floors, par. 5.5.5 for doors, par. 5.5.6 for windows, and par. 5.5.7 for utility openings. The objective is to identify construction choices that assure a balanced design between all building components, i.e., approximately equal penetration delays against a given threat severity level for each with no vulnerable weak links. These penetration delay times for a given severity level must also equal or exceed the guard force response times established in Section 2.

5.5.1.2 Summary of Design Choices. The choices available to the designer are summarized as follows:

1) Walls. Any wall construction can be used for the low-severity threat. For medium- and high-severity threats, the choices are limited to CMU (concrete-masonry unit) for lower delay time requirements, and conventional or steel-fiber-reinforced concrete for higher delay time requirements. Very high-severity threats require sacrificial areas or massive reinforced concrete.

2) Roofs and Floors. Any roof or floor construction can be used for low-severity threats. Medium- and high-severity threats require reinforced concrete. Very high-severity threats require sacrificial areas and reinforced concrete.

3) Doors. Specialized designs are available for low and medium threats for personnel doors, medium and high threats for vaults, and high and very high threats for magazines. Conventional vehicle door designs are available for low, medium, and high threats, but all offer little penetration resistance.

4) Windows. Specialized designs are available for low-barrier, medium-, and high-severity threat levels:

a) Low – Hinged grating and transparent barrier
b) Medium – Transparent barrier
c) High – Opaque rolling barrier.

5) Utility Openings. If possible, all utility openings should be less than the man-passible 96 square inches (0.06 sq mm) of cross-sectional area or less than 10 inches (254 mm) in diameter. Where this is not possible, single or multiple grillworks can be introduced for the low and medium threat

levels. Grillworks of larger size bars [No. 5 (16 mm) or greater] and various constrictive barrier designs are provided for the high threat levels. Very high level threats require sacrificial enclosing structures around openings.

5.5.2 Designing for the Very High-Severity Threat. The use of explosives, either in bulk or augmented with flyer plates, can be especially effective in quickly producing holes large enough for an intruder to crawl through. There are only two ways of hardening against such threats: (1) the use of building sacrificial areas, and/or (2) appropriately designed barriers using massive reinforced-concrete construction.

5.5.2.1 Sacrificial Areas. Sacrificial areas in the building can be employed above, below, and around the critical area in the building to be protected (see Figure 30). The walls, doors, and other features of this sacrificial area may be damaged, but will provide a standoff region to reduce the effectiveness of the blast on the critical area. In general, the critical area should be low, internal to the building, and well away from exterior walls and roof. Any type of construction of the exterior walls, roof, etc., of the sacrificial area is acceptable. Using a lighter construction is more desirable and may preclude the attacker from using large quantities of explosives, reducing the damage to the building.

5.5.2.2 Barriers to Counter an Explosive Attack

1) Construction. The only practical barrier construction to stop a direct explosion is the use of massive reinforced concrete 18 to 48 inches (0.46 to 1.2 m) in thickness. Because of structural considerations, such thick cross sections normally will be limited to the walls in the area protecting the only critical resource. Roofs and doors require the use of sacrificial areas and foyers as shown in Figure 30.

2) Penetration Times. Thick, heavily reinforced concrete walls can provide significant penetration delays. While power, hand, and thermal tools are impractical for removing the large masses of concrete thick walls contain, they can be used to cut and remove the reinforcing material after it is exposed by the explosives.

a) Explosive threats. While explosives can produce large holes, even in thick concrete walls, they do not remove the 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 explosion forces the fragmented concrete out of the wall, and a relatively clean hole results. Cutting and removing the reinforcing material for a crawl hole contributes to most of the delay.

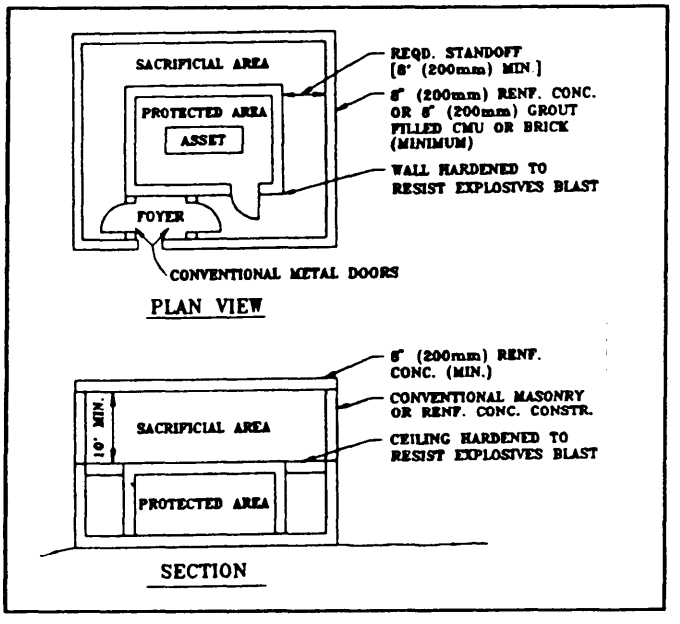


Figure 30
Example Sacrificial Area Design For Very High Level Threats

If an explosive-platter (flyer plate) combination is used as the breaching tool, it may cut and remove most or all the reinforcing material. This combination minimizes the need to cut the rebar with hand or thermal tools after the concrete has been removed by the explosives, in many cases significantly reducing the penetration time. On the other hand, the platter charge requires much more explosive by weight than would be required if a regular explosive charge were used to remove the concrete. This fact, plus the weight of the platter, results in a much heavier configuration as well as the possibility of collapsing or destroying the entire structure or its contents, and makes the use of platter charges questionable. Consequently, the following wall designs are based on the use of bulk explosives only in combination with hand, power, and thermal tools.

b) Concrete wall design. Table 19 presents the estimated minimum penetration delay times offered by various thicknesses of reinforced concrete having a compressive strength of at least 5,000 psi (507,000 kPa).

5.5.3 New Wall Construction for Low- to High-Severity Threats

5.5.3.1 Summary. Table 20 summarizes the maximum penetration delay times achievable for new wall construction options. These include concrete masonry unit (CMU) construction, and conventional and steel-fiber-reinforced concrete. Only these types of construction are recommended for the medium- and high-severity threat levels. Any wall can be used for low-severity threats. Stud-girt construction using standard materials such as wood, light metal, stucco, and gypsum provide only nominal protection (typically less than 2 minutes) and are not recommended for the medium and high level threats. Note in Table 20 that, for concrete thickness up to 12 inches (305 mm), steel-fiber-reinforced concrete is the only design option meeting a single barrier penetration time requirement of up to 50 minutes. Conventional concrete can achieve up to 35 minutes, and CMU construction up to 18 minutes. Where equivalent reinforced concrete or CMU options are possible, the designer should select that which is also compatible with the other building components and also satisfies any cost, functional, dimensional, and aesthetic objectives.

Table 19
Reinforced Concrete Wall Designs For Very High Threat Levels

Concrete Thickness in. (m)	Rebar layers - No. 6 (19 mm) on 6-Inch (150-mm) Centers Each Way	Minimum Penetration Time (min.)(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 power thermal tools to cut the rebar.

5.5.3.2 Low-Severity Threat. In general, it is not practical to attack walls using only a limited set of low-observable hand-held tools. A low level threat would more likely attack the doors, windows, or other more vulnerable part of the facility rather than the walls. Any wall construction can be considered adequate for this threat level.

5.5.3.3 Medium- and High-Severity Threat. CMU, conventional, and steel-fiber-reinforced concrete wall construction options and corresponding minimum penetration times for medium- and high-security threat levels are summarized in Figures 31 through 34 and Tables 21 and 22. Note in Figures 31, 33, and 34 that the minimum penetration times are presented as a function of the thickness of the cross section and the size and spacing of reinforcing. Different combinations of reinforcing size and spacing are reflected in the family of curves identified by A, B, C, etc. These combinations are summarized in Table 21 for masonry and Table 22 for reinforced concrete. In general, a required penetration time can be achieved either by providing a thicker cross section and/or by adding more reinforcing. Which is more appropriate may be decided by structural or other considerations. Note also in Figures 31, 33, and 34 that the penetration times are minimum values based on the proper selection and optimal use of the attack tools. In this regard, the region identified as the "medium-severity threat level" assumes that only hand-powered tools and some limited battery-powered tools are used. For these cases, the thickness and/or rebar combination required is less than the "high-severity threat level" where power and thermal tools also may be used. If the threat is of medium severity and the delay time requirement is within the

Table 20
Wall Construction Choices For New Construction
(Not More Than 12 Inches (305 mm) Thick)

Wall Construction Type (b)	Maximum Penetration Delay Times (minutes) Achievable for Threat Severity Level		
	Low	Medium	High
Concrete Masonry Unit	(a)	5.5	18
Conventional Reinforced Concrete	(a)	7.5	35
Steel-Fiber-Reinforced Concrete	(a)	11.0	50

(a) It is not practical for low level threats to attack walls. Any construction can be considered adequate.
(b) Note: As described in what follows, different cross-section thicknesses and rebar combinations apply to the low-, medium-, and high-severity threat levels.

medium threat cross-hatched region in Figures 31, 33, and 34, the chart can be used to establish the minimum penetration time. On the other hand, if the delay time requirement is outside the medium-severity region, this means a design having a thicker cross section and more rebar is required to preclude only the practical use of hand- or battery-powered tools. In this case, pick a cross section that is just outside the medium-severity region to stop the threat. For example, if the delay requirement is 10 minutes for a medium-severity threat against reinforced concrete (Figure 34), providing something just over 6 inches of concrete will stop the threat.

1) Medium-Severity Threat

a) Concrete Masonry Unit. As shown in Figure 31 and Table 21, penetration delay times up to about 5.5 minutes are achievable against medium-severity threats using mortar-filled CMU. Reinforcing bars in the core are required for higher times. Figure 32 presents some additional masonry/wood/metal composite cross-section design options together with their penetration times.

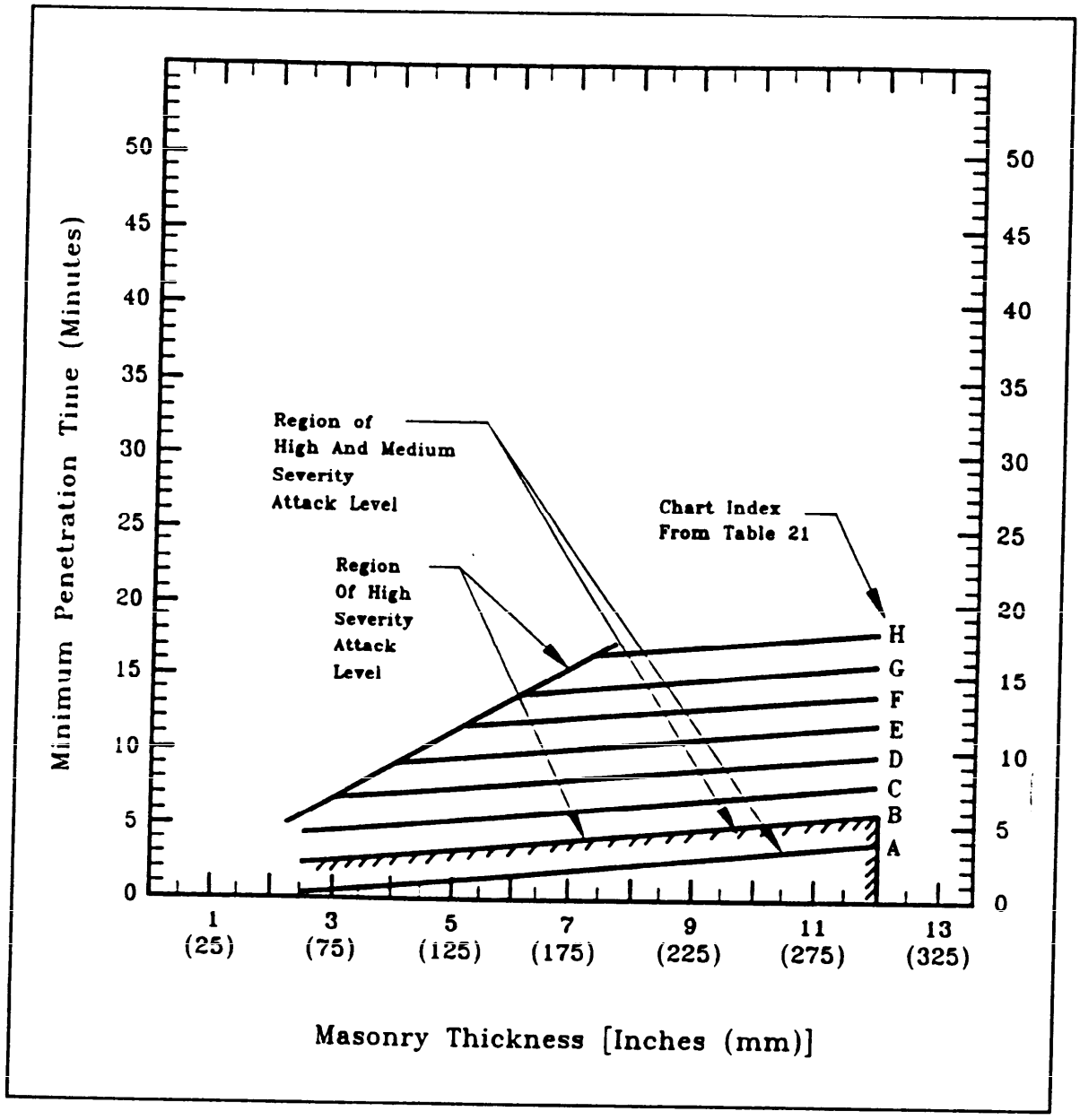


Figure 31
Penetration Times For Solid Concrete Masonry Walls

b) Conventional Reinforced Concrete. As shown in Figure 32 and Table 22, penetration delay times up to 7.5 minutes are achievable against medium-severity threats with 6 inches (150 mm) of reinforced concrete at the "B" rebar combination (Table 22).

Table 21
Penetration Time Chart Index For Figure 31, Reinforced Concrete Masonry Walls

Single Layer of Rebar in Block Cavities.

Spacing Each Way, inches (mm)	Bar Number						
	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

Double Layer of Rebar in Block Cavities.

Spacing Each Way, inches (mm)	Bar Number						
	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

c) Steel-Fiber-Reinforced (SFR) Concrete. Figure 34 shows that penetration delay times up to about 11 minutes are achievable against medium-severity threats with 6 inches (150 mm) of SFR and the "B" rebar combination in Table 22. The steel fiber is at least 5 percent by volume of the concrete mix design.

Table 22
Penetration Time Chart Index For Figures 33 and 34

Single Layer of Rebar.

Spacing Each Way, inches (mm)	Bar Number						
	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

Double Layer of Rebar.

Spacing Each Way, inches (mm)	Bar Number						
	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

2) High-Severity Threat Level

a) Concrete Masonry Unit (CMU). Penetration delay times up to 18 minutes are achievable against high-severity threats using mortar-filled reinforced CMU block (Figure 31 and Table 20) against high-severity threat levels.

b) Conventional Reinforced Concrete. Figure 33 with Table 22 gives concrete thicknesses and rebar combinations that can achieve penetration delay times up to 35 minutes against high-severity threats.

c) Steel-Fiber-Reinforced (SFR) Concrete. Figure 34 with Table 22 gives SFR thickness and rebar combinations that can achieve penetration delay times up to 50 minutes against high-severity threats.

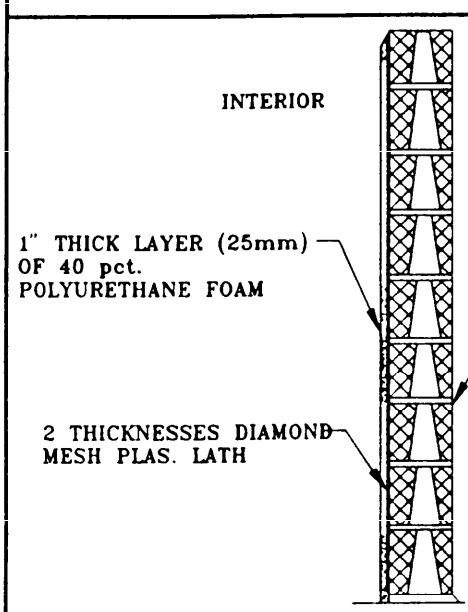
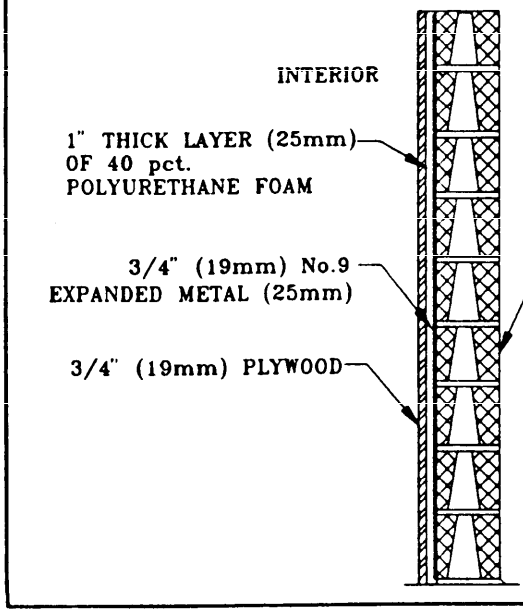
Construction	Penetration Time (min.)	
	Medium	High
	2	2
	3.5	3.5

Figure 32
Wood/Metal Composite Masonry Construction.

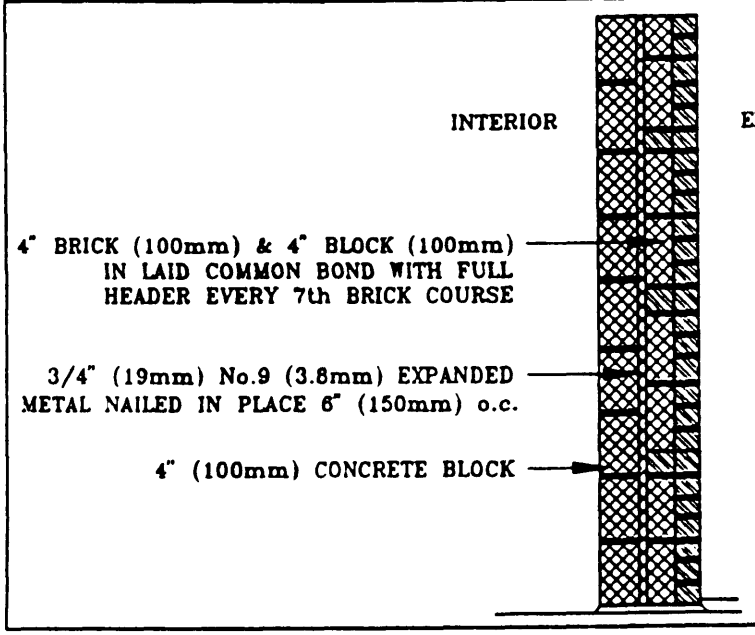
Construction	Penetration Time (Min)	
	Medium	High
	3	3

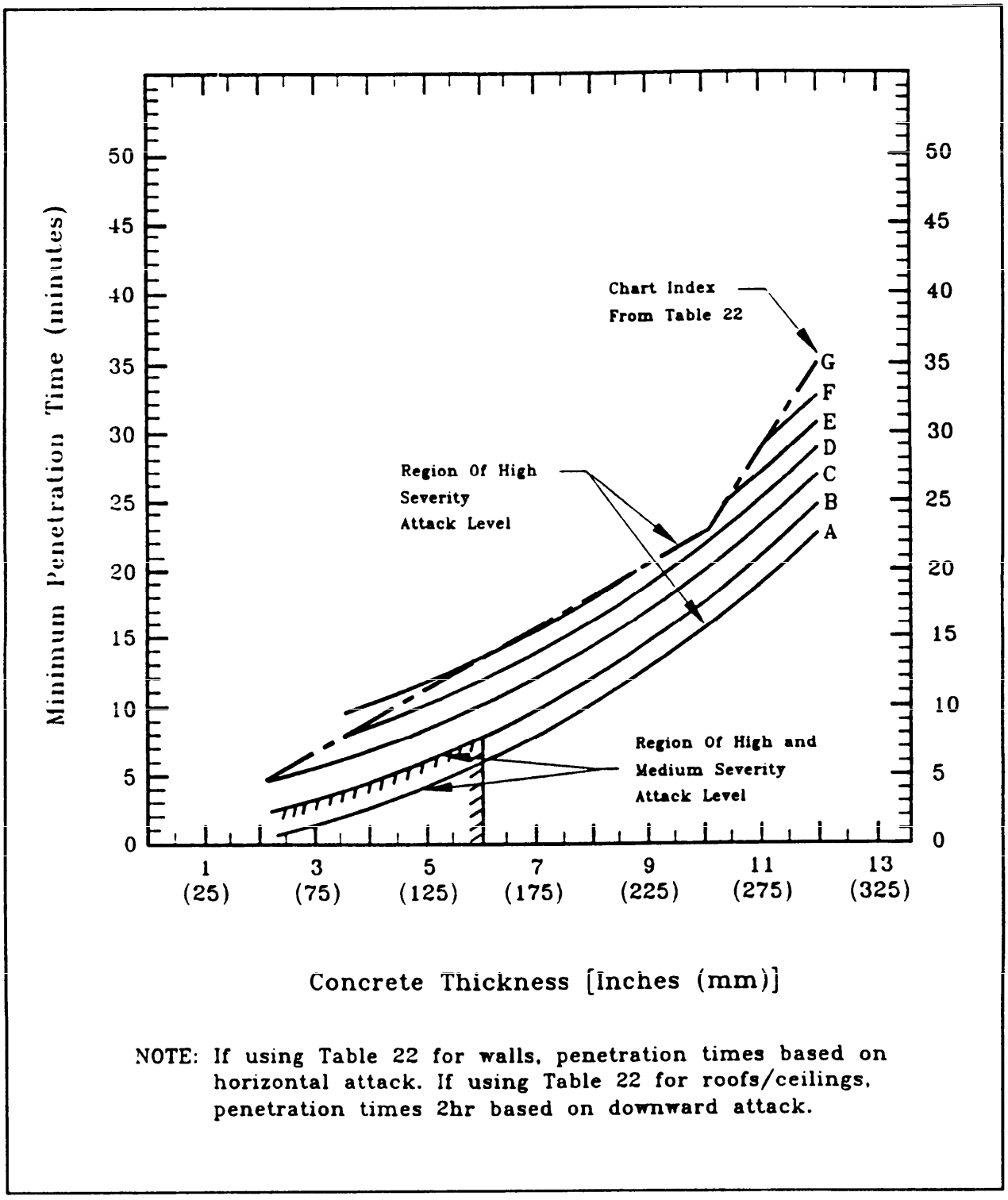
Figure 32
Wood/Metal Composite Masonry Construction (Continued)

5.5.4 New Roof/Floor Construction for Low- to High-Severity Threats

5.5.4.1 Summary. Only conventional or steel-fiber-reinforced concrete construction are recommended for the medium- and high-severity threat levels. Any construction can be used for low-severity threats. Other types of roof/floor construction such as wood frame or metal provide only nominal protection (typically less than 2 minutes) and are not recommended for the medium and high threat levels.

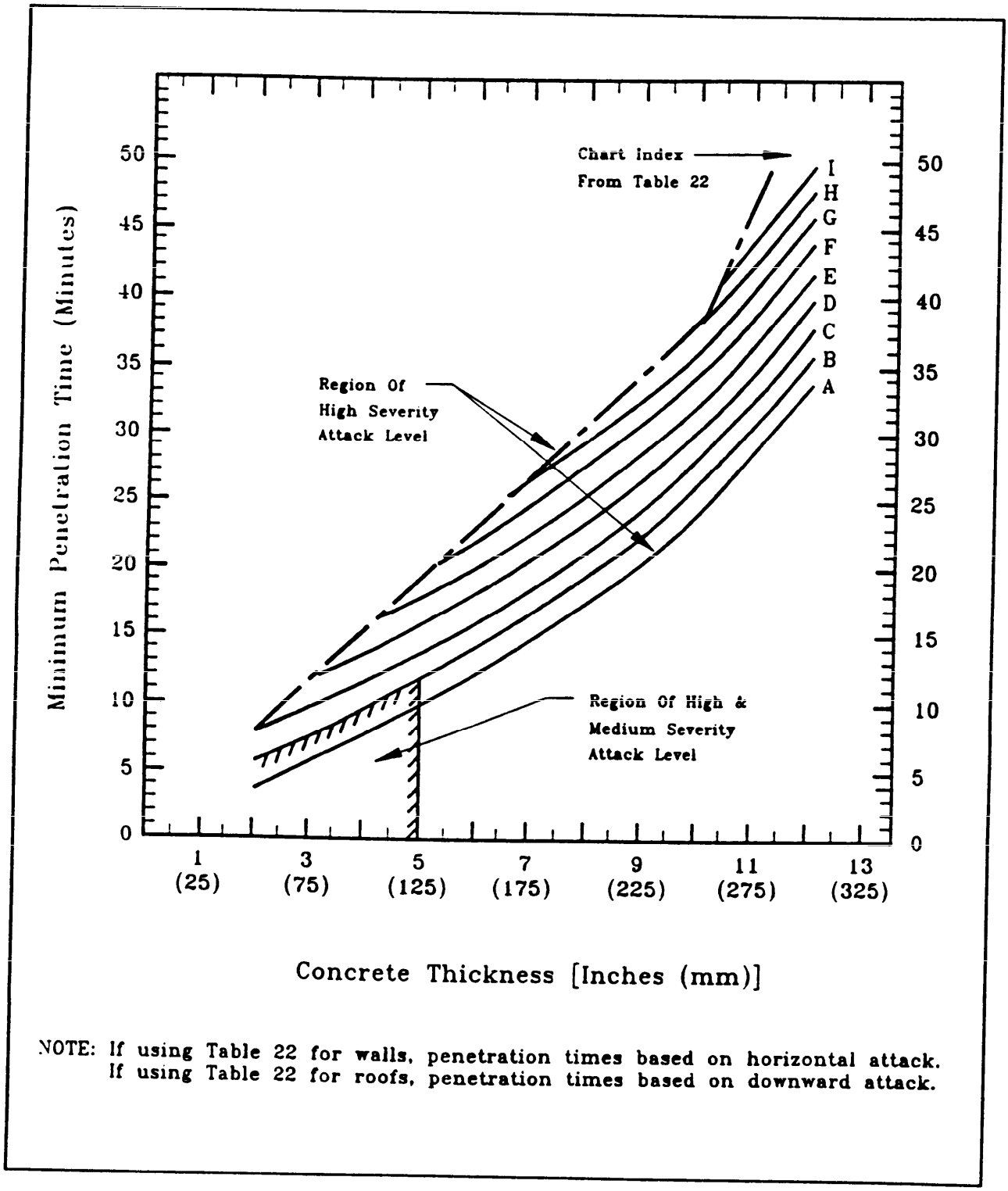
5.5.4.2 Low-Severity Threat Level. In general, it is not practical to attack roofs or floors using only a limited set of low-observable, hand-held tools. A low level threat more likely would attack the doors, windows, or other more vulnerable part of the facility. Consequently, any roof or floor construction can be considered adequate for this threat level.

5.5.4.3 Medium- and High-Severity Threat Levels. Conventional or steel-fiber-reinforced concrete construction options and corresponding minimum penetration times for medium- and high-severity threat levels are summarized in Figures 33 and 34 and Table 22 for a downward attack on roofs or floors. Figure 35 with Table 23 presents data for an upward high-severity attack on the floor. Figure 35 does not include medium-severity attacks because it is



NOTE: If using Table 22 for walls, penetration times based on horizontal attack. If using Table 22 for roofs/ceilings, penetration times 2hr based on downward attack.

Figure 33
Penetration Times For Conventional Reinforced Concrete Walls/Roofs



NOTE: If using Table 22 for walls, penetration times based on horizontal attack.
If using Table 22 for roofs, penetration times based on downward attack.

Figure 34
Penetration Times For Fiberous Reinforced Concrete Walls/Roofs

not practical to conduct an upward attack on floors without power tools. Note in Figures 33 through 35 that the minimum penetration times are presented as a function of the thickness of the cross section and the size and spacing of reinforcing. Different combinations of size and spacing of the reinforcing are reflected in the family of curves identified by A, B, C, etc. These combinations are summarized in Tables 22 and 23. In general, a required penetration time can be achieved by providing either a thicker cross section and by adding more reinforcing. Which is more appropriate may be decided by structural or other considerations. Note also in Figures 33 through 35 that the penetration times are minimum values based on the proper selection and optimal use of the attack tools. In this regard, the region identified as the "medium-severity threat level" for a downward attack in Figures 33 and 34 assumes only hand-powered tools and some limited battery-powered tools are used. For these cases, the thickness and rebar combination required is less than the "high-severity threat level" where power and thermal tools also may be used.

1) Medium-Severity Threat Level

a) Roofs and ceilings. If the threat is of medium severity and the delay time requirement is within the medium threat cross-hatched region in Figures 33 and 34, the chart can be used to establish the minimum penetration time.

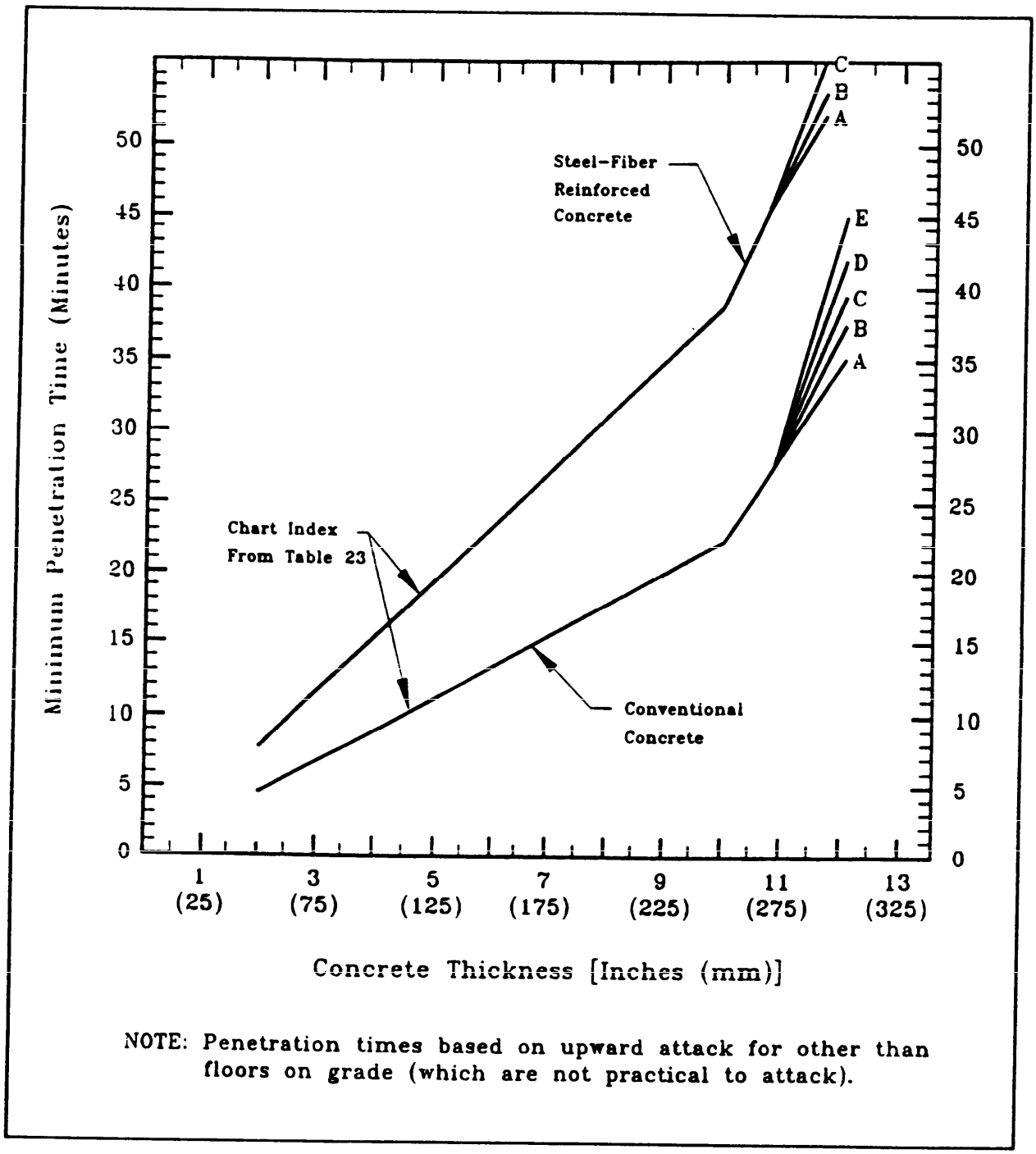
On the other hand, if the delay time requirement is outside the medium-severity region, a design having a thicker cross section and more rebar is required to preclude only the practical use of hand- or battery-powered tools. In this case, pick a cross section that is just outside the medium-severity region to stop the threat. For example, if your delay requirement is 10 minutes for a medium-severity threat against reinforced concrete (Figure 33), providing something just over 6 inches (15 mm) of concrete will stop the threat.

b) Floors. Because an attacker is working against gravity, it is not practical to attack a reinforced concrete floor from below for a medium-severity threat using only hand-held tools. Any thickness or rebar combination is suitable for this case.

2) High-Severity Threat Level

a) Roofs and ceilings. Figures 33 and 34 with Table 22 give concrete thickness and rebar combinations that will achieve a required penetration time for both conventional and SFR concrete.

b) Floors. Figure 35 and Table 23 give concrete thickness and rebar combinations that will achieve a required penetration time for conventional and SFR concrete.



NOTE: Penetration times based on upward attack for other than floors on grade (which are not practical to attack).

Figure 35
High-Severity Threat Level Penetration Times for Reinforced Conventional and Fibrous-Concrete Floors Based on an Upward Attack

Table 23
Penetration Time Chart Index For Figure 35
Single Layer of Rebar.

Spacing Each Way, inches (mm)	Bar Number						
	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

Double Layer of Rebar.

Spacing Each Way, inches (mm)	Bar Number						
	None	3	4	5	6	7	8
3 (75)	A	C	C	D	E	E	E
3-1/2 (90)	A	C	C	D	E	E	E
4 (100)	A	B	C	C	D	E	E
4-1/2 (115)	A	B	C	C	D	E	E
5 to 9 (125 to 225)	A	B	B	B	C	C	D
>10 (250)	A	A	A	A	A	A	A

5.5.5 New Door Construction

5.5.5.1 Summary. As noted, penetration delay time through structure walls and other building sections can be increased by using thicker or composite materials. However, in all structures, the value of the barrier ultimately is determined by its weakest point. All structures, to be useful, require doors for access. Doors, due to their functional requirements and associated hardware, impose design restrictions and are, in many cases, one of the weakest links in a structure. For example, many structures with reinforced

CMU walls provide pedestrian access through commercial hollow steel doors. In such a facility the barrier value of the basic structure, while designed to be relatively high, is weakened by the use of ordinary doors, frames, and hinges. Balanced design dictates the use of doors that provide the delay times commensurate with the structure in which they are installed.

The number of doors to a facility should be reduced to an absolute minimum. In cases where more than one door exists, only one of these should be provided with outside-mounted locks and entry hardware. All others should, as far as practicable, present blank, flush surfaces to the outside to reduce their vulnerability to attack. Exposed locking devices on the exterior (attack side) of the door should be used only on low- or medium-security applications. No matter how secure a door is made, placing the locking device on the exterior of the door cannot provide the level of security required for high-security applications.

Although the penetration time through the door surface usually can be increased by use of heavier or composite materials, such hardening may not provide a complete security solution because of weight constraints, conflicts with functional requirements, mounting hardware limitations, or lock vulnerability. There is no point in hardening a door surface beyond the attack resistance of the available mounting hardware and locking device technology. According to available data, currently used standard or commercial door or door hardware do not provide <u>significant</u> penetration time against a <u>determined</u> intruder.

For example, personnel doors currently are available only for the low- and medium-severity threat levels. Although vehicle doors are available for the low through high threat levels, they provide only nominal penetration times of 1 minute or less. Vault doors are designed for the medium- and high-severity threats and AA&E magazine doors are used for the very high-severity threat. Commercial door manufacturers provide attack- and bullet-resistant doors. When properly installed, these doors may offer a substantial increase in penetration resistance over standard industrial doors. Requirements for each type of door are described in the following paragraphs.

5.5.5.2 <u>Personnel Doors</u>. As shown in Table 24, personnel doors are available for low- and medium-severity threat levels. There are no personnel doors available to defeat the high- and very high-severity threat level. Potential attack areas on doors include the face (surface), hinges, and locking device(s).

1) <u>Low-Severity Threat</u>. Door design for the low-severity threat is summarized in Tables 25, 26, and 27.

Table 24
Personnel Door Penetration Times

Threat Severity Level	Penetration Time (minutes)	Design Details
Low	<1	Tables 25, 26, and 27 Figure 36
Medium	≤4	Tables 27, 28, and 29 Figures 36, 37, 38, and 39
High	N/A	N/A

N/A = Not Available

a) Door Panel Construction. Typical exterior personnel doors used with conventional construction are commonly 1-3/4 inches (45 mm) thick and typically faced with 16- or 18-gauge (1.5- or 1.2-mm) steel. Although some doors are hollow, others commonly are filled with a noncombustible foam or a slab of polyurethane. Locking devices for personnel doors vary; however, they are typically a five- or six-pin tumbler type. Hinges are of mortised design with nonremovable pins. It should be noted that such features are only furnished when specified (as an extra cost option). Estimated penetration times for standard personnel doors are uniformly low.

In evaluating the penetration times of door surfaces, consider doors required to have panic bar hardware as special cases. These doors do not require a man-passable opening to be defeated. Drilling a small aperture to pass a wire hook through is all that is required to open them. The tradeoffs between life safety and security may impact directly upon interior layouts to avoid a design that must be compromised to meet fire protection requirements.

Personnel door panel/edge details for low-severity threat level protection are shown in Table 25. The door panel is constructed of 16-gauge (1.5-mm) steel with 16-gauge (1.5-mm) steel stiffeners. Edge construction is a 14-gauge (1.9-mm) recessed channel. Fully welded construction is employed.

Table 25
Personnel Door Panel/Edge Details, Low Security
1-Minute Penetration Delay Time

Size	3 feet by 80 inches by 1-3/4 inches (0.9 m by 2 m by 44 mm)
Applicable Specifications	Hollow Metal Manufacturer's Association (HMMA) 862-87, 810-87
Type	Type A, full-flush with continuous welded-edge seams. Design F, full-panel flush door.
Panel	Steel-stiffened.
Face Sheet	16-gauge (1.5-mm) steel
Stiffeners	Hat section, 16-gauge (1.5-mm) steel; maximum distance between stiffeners 4 inches (100 mm) on center
Edge Construction	14-gauge (1.9-mm) steel channel, recessed.
Special Features	Not Applicable

Table 26
Personnel Door Frame Details, Low Security
1-Minute Penetration Delay Time

Applicable Specifications	Construct per HMMA 820-87 & 862-87 except as noted.
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 36 for hinge side protection.
Frame Installation	Install per HMMA 840-87, 820-87.
Hardware Preparation	Prepare hardware per HMMA 830-87. Frame is to be built into a wood-stud frame wall.

Table 27
Personnel Door Hardware Notes For Low- and Medium-Severity Threat

Mortise Lock	American National Standards Institute/Building Hardware Manufacturers Associations (ANSI/BHMA) A156.13 Series 1000 Security Grade, with dead bolt and latch bolt.
Auxiliary Rim Lock	ANSI/BHMA A156.5, Security Grade dropbolt lock operated by key from inside and outside. Lock selected must conform to mounting bolt tensile test [12,000 pounds (5,450 kg)] described in Section 10.10. Lock shall be used in conjunction with anti-wedge and anti-drill plates similar to the type shown in this specification. Note: To comply with life safety requirements, this lock shall only be used during those hours when the space is unoccupied.
Hinges	ANSI/BHMA A156.1. Heavy Weight. Note: medium-security door systems require some form of hinge side protection. Some hinge manufacturers provide this in hinges. If these type of hinges are not used, then some form of hinge side protection shall be engineered into the door system (see Figure 36). For added protection against door sag, use surface-mounted continuous hinges, and design the door/frame with hinge-side protection independent of the hinges.
Kick Plates	ANSI/BHMA A156.6
Panic Hardware	ANSI/BHMA A156.3, Grade 1, Mortise exit device. Note: Use of panic type exit devices as required by life safety codes in lieu of mortise lock described above. However, to ensure medium-security rating, use in conjunction with auxiliary rim lock (see note above).
Other Hardware	If the use of other hardware such as closing devices, electric strikes, etc., 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 Naval Civil Engineering Laboratory Security Engineering Division (Code L56) if there are any questions.

Table 28
Personnel Door Panel/Edge Details, Medium Security
4-Minute Penetration Time

Size	3 feet by 80 inches by 1-3/4 inches (0.9 m by 2 m by 44 mm)
Applicable Specifications	HMMA 863-87, 810-87
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) on center
Edge Construction	12-gauge (2.7-mm) steel channel, recessed.
Special Features	Hinge side protection configuration (see Figures 36 and 37) 7-gauge (4.6-mm) anti-pry strips (see Figure 38)

b) Door Frame Construction. Personnel door frame details for the low-severity threat are shown in Table 26. The frame is designed to be installed into a wood-stud frame wall. Hinge-side protection shall be provided in accordance with Figure 36. The security stud shown in section (c) of Figure 36 fits into the frame openings shown in section (b) at the three locations shown in section (a).

c) Door Assemblies. The low-security door includes a continuous hinge, mortise lock with a dead bolt, an auxiliary rim dead bolt lock, and other hardware as may be required. Requirements for these hardware items are shown in Table 27. Doors and frames are to be built and installed per applicable National Association of Metal Manufacturers-Hollow Metal Manufacturers Association (NAAMM-HMMA) standards. All welded 14-gauge (1.9-mm) steel construction is used. Doors meeting these requirements provide 1-minute penetration time. If more delay time is needed, multiple doors placed in series may be provided as shown in Figure 10.

2) Medium-Severity Threat Level. The personnel door design for the medium-severity threat is summarized in Tables 27, 28, and 29. This door consists of a 14-gauge (1.9-mm) steel, and a stiffened face sheet with a frame designed for installation in CMU walls. This design includes either the "security stud" protection shown in Figure 39 or the "lug/dowel pin" option shown in Fig. 37. Lock side protection is accomplished with the 7-gauge

Table 29
Personnel Door Frame Details, Medium Security
4-Minute Penetration Time

Frame Size	12 gauge (2.7 mm)
Applicable Specifications	Construct per HMMA 820-87 & 863-87 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 Figures 36 and 37 for details on hinge-side protection. See Figure 39 for details on special 12- by 1- by 1/4-inch (305- by 25- by 19-mm) plate reinforcement for auxiliary rim-lock strike reinforcement.
Frame Installation	Install per HMMA 863-87, 840-87 and 820-87.
Hardware Preparation	Prepare for Hardware per HMMA 863-87, 830-87. Use one of the two cases below for selecting installation hardware 1) Frame to be installed in a Concrete Masonry Unit (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 rebar system of the CMU wall ties in to the interior of the frame. Grout-fill frame with a grout of compressive strength not less than 3,000 psi (21,000 kPa). 2) Frame is to be installed in a prepared opening in a CMU wall. Frame shall be punched and countersunk for expansion bolt anchors (four per side) and provided with 12-gauge hat-shaped reinforcements secured in place with at least four spot welds each. Grout-fill frame with a pourable type grout with a compressive strength of not less than 3,000 psi (300,000 kPa).

(4.6-mm) anti-pry strip shown in Figure 38 and the auxiliary rim-strike reinforcement shown in Figure 38. This design provides 4 minutes of delay against a medium-severity threat. If more delay time is required, multiple doors installed in series may be used as shown in Figure 10.

3) High-Severity Threat Level. There are no high-severity threat personnel doors. If there is a requirement for a high-severity threat personnel door, use alternative means. For example, use two medium-severity personnel doors mounted in series or use a vault door. Since access control or panic hardware can not be installed on a vault door, consider using both a daytime door and a nighttime door.

5.5.5.3 Vault Doors. Since openings in vaults are more vulnerable to attack than the vault enclosure itself, only one entrance should be provided, where possible. When a vault exceeds 1,000 square feet (90 sq m) 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 shall 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 shall be provided for the primary entrance to preclude undue wear of the door, which eventually could weaken the locking mechanism or cause malfunctioning. Vault doors and frame units shall conform to Federal Specification AA-D-00600C for GSA Class 5 vault doors. Requirements of this specification are summarized in the following paragraphs. Vault door requirements and penetration times are given in Table 30.

Table 30
Vault Door Options and Penetration Times

Attribute	Threat Severity Level		
	Low	Medium	High
Class	N/A	5	8
Specifications	N/A	FED SPEC AA-D-00600C	FED SPEC AA-D-2757
Penetration Time (minutes)	N/A	10	15

N/A = Not Applicable

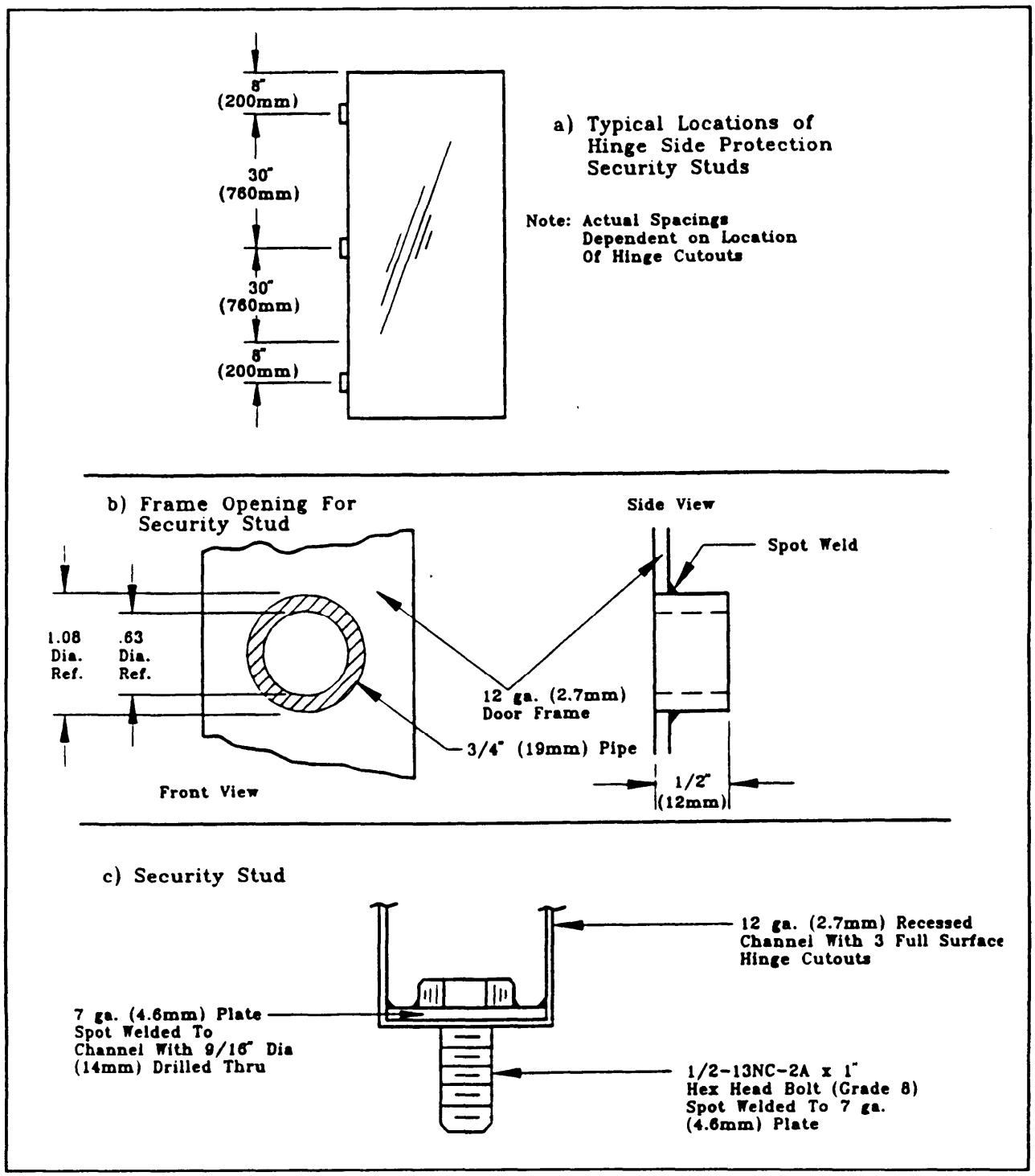


Figure 36
Personnel Door Hinge Side Protection for Low- and Medium-Severity Threat

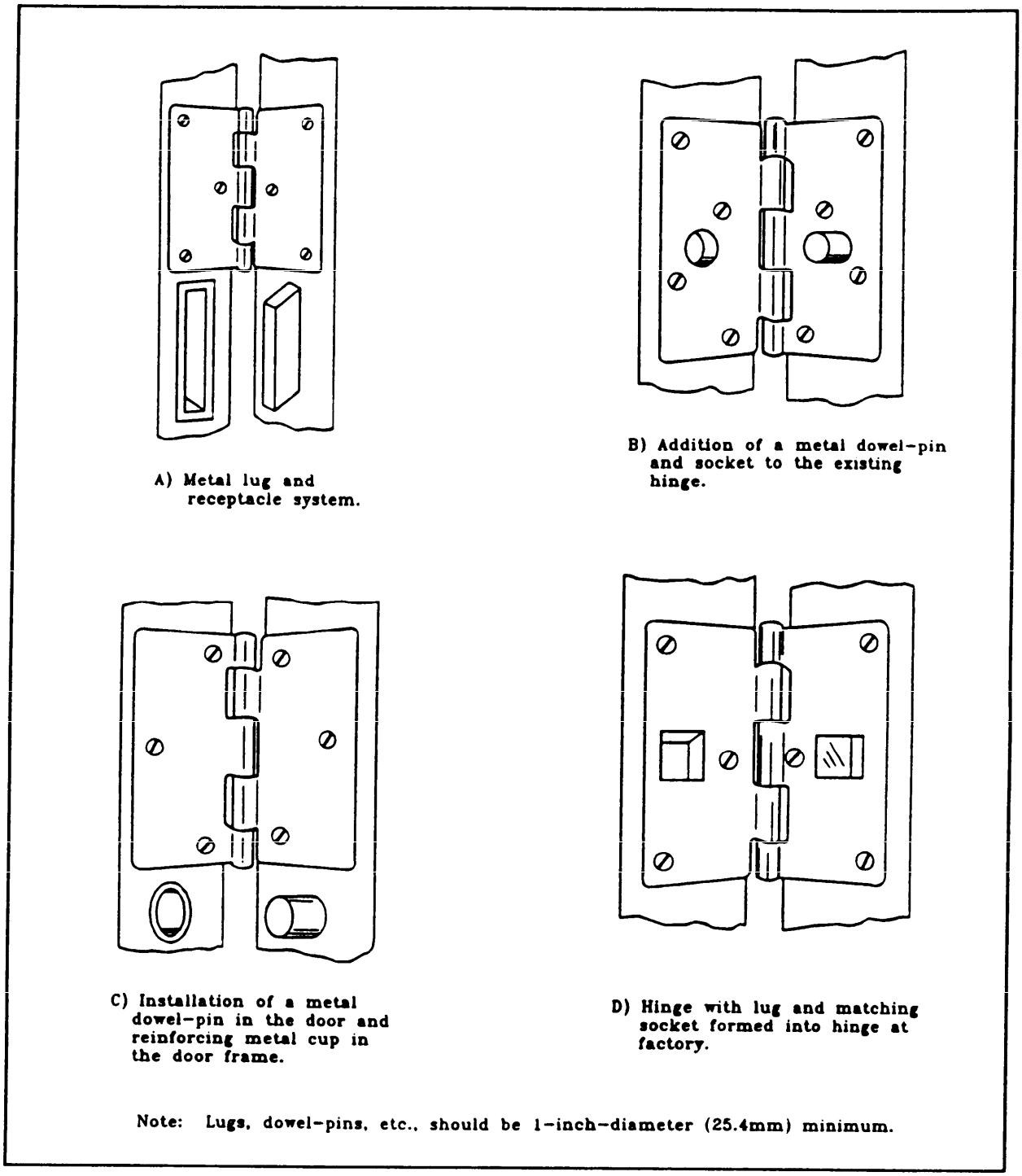


Figure 37
Personnel Door, Representative Medium-Security Hinge-Side Protection

| Special features | Hinge side protection configuration (see |

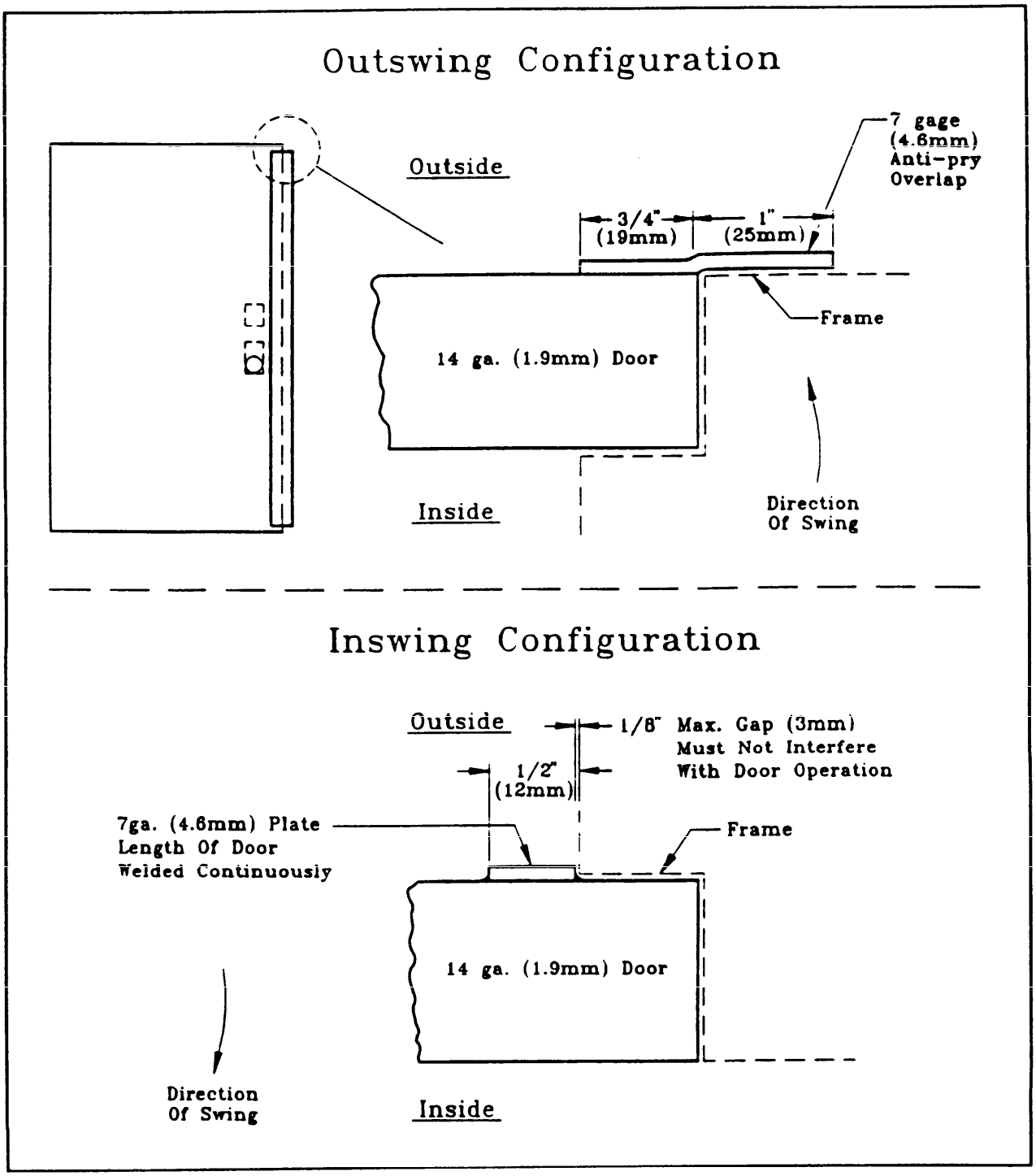


Figure 38
Personnel Door Anti-Pry Strips For Medium-Security Applications

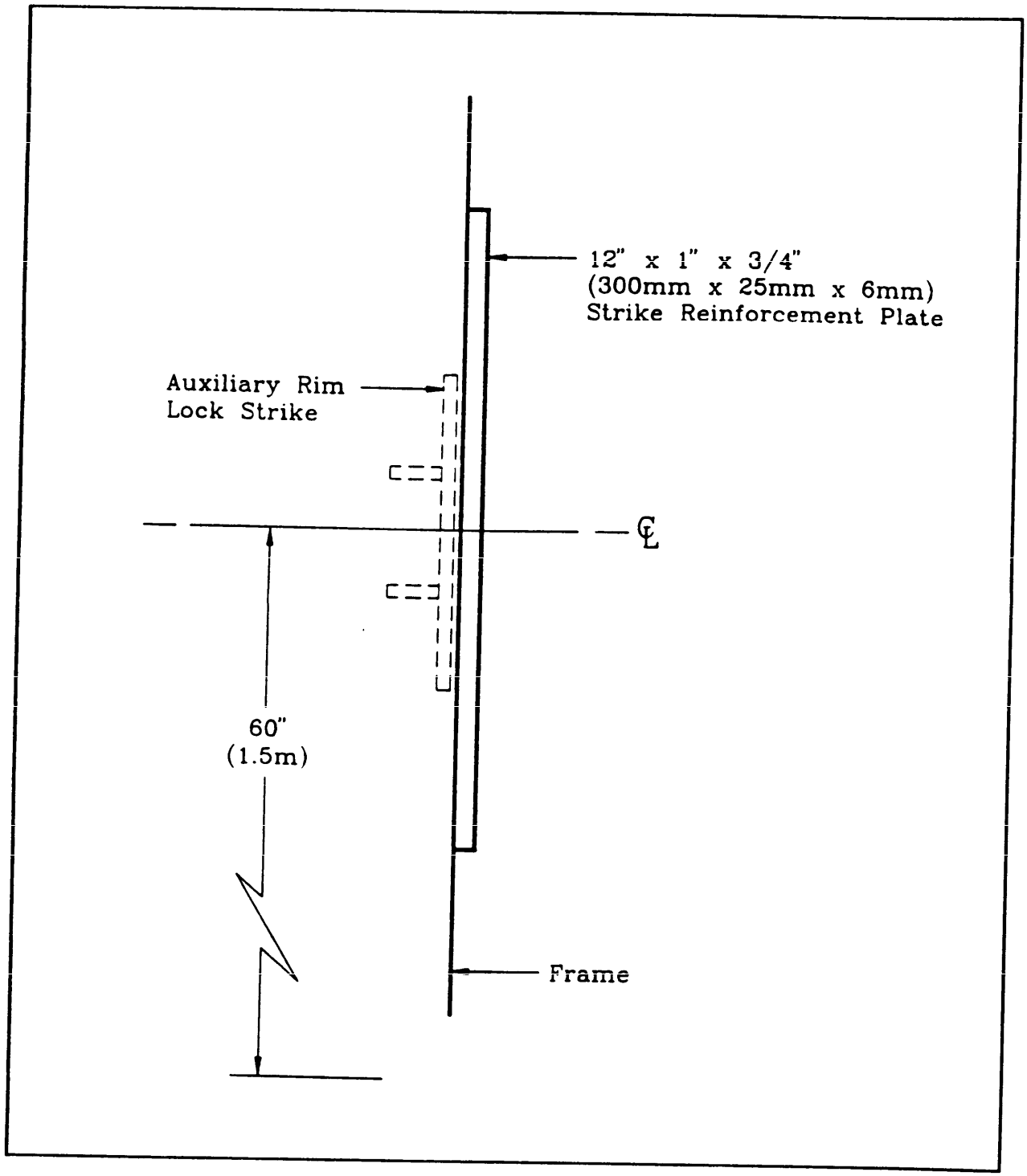


Figure 39
Personnel Door, Auxiliary Rim-Lock Strike Reinforcement

1) Low-Severity Threat. There are no low-severity threat vault doors.

2) Medium-Severity Threat. Vault doors for the medium-severity threat are GSA Class 5 vault doors (see Figure 29) that are designed to comply with Federal Specification AA-D-00600C. They provide a forced-entry penetration delay time of 10 minutes.

3) High-Severity Threat. Vault doors for the high-severity threat are GSA Class 8 vault doors that are designed to comply with Federal Specification AA-D-2757. They provide a forced-entry penetration delay time of 15 minutes.

5.5.5.4 Magazine Doors. Table 31 identifies design data for high-severity threat level AA&E storage facilities. Table 32 identifies magazine door design data for the very high-security threat level.

Table 31
High-Security Magazine Door

Element	Construction	Penetration Time (minutes)
Panel	See Table 16	4
Lock/Hasp	Figures 40 and 41	<1

Table 32
Very High-Security Magazine Construction

Element	Construction (a)	Penetration Time (minutes) (b)
Panel	Figure 42	20
Locking System	High-Security Internal-Locking System	20

(a) Contact the Naval Civil Engineering Laboratory for details.
(b) Penetration time is for hand/power/and thermal tools. Also defeats explosive charges.

1) Low- and Medium-Severity Threats. There are no low- and medium-severity threat doors.

2) High-Severity Threat. Table 16 gives examples of typical door panel construction required by DOD 5154.4 to achieve explosive safety in the storage of Risk Categories I through IV, ammunition and explosives (see Table 15 for a description of risk categories). At present, the shrouded shackle padlock shown in Figure 40 together with the shrouded hasp shown in Figure 41, is to be used with these doors. Note in Table 31, that although the door panel is capable of providing a penetration delay time of 4 minutes, the lock/hasp provides less than 1 minute of delay against a high-severity threat.

3) Very High-Severity Threat. Figure 42 describes a door panel design that will counter a very high-severity threat. This panel should be used with the High-Security Internal-Locking System. The door panel and locking system are described in detail in MIL-HDBK-1013/11 and 1013/6, respectively. When the door panel and locking system are integrated, the resulting barrier will provide 20 minutes of delay against a very high-severity threat level attack.

5.5.5.5 Vehicle Doors. Table 33 provides a summary of the door construction choices applicable to vehicle doors for the low-, medium-, and high-severity threats.

Table 33
Vehicle Door Construction

Threat Severity Level	Construction	Penetration Time (minutes)
Low	18-gauge (1.2-mm) galvanized steel with interlocking slates.	1
Medium	14-gauge (1.9-mm) hollow metal on 3/8-inch (9.5-mm) steel plate.	1
High	See Table 16 and Figures 40 and 41 for magazine door.	4

1) Low-Severity Threat. For the low-severity threat, use the standard 18-gauge (1.2-mm) galvanized-steel roll-up door with interlocking slats.

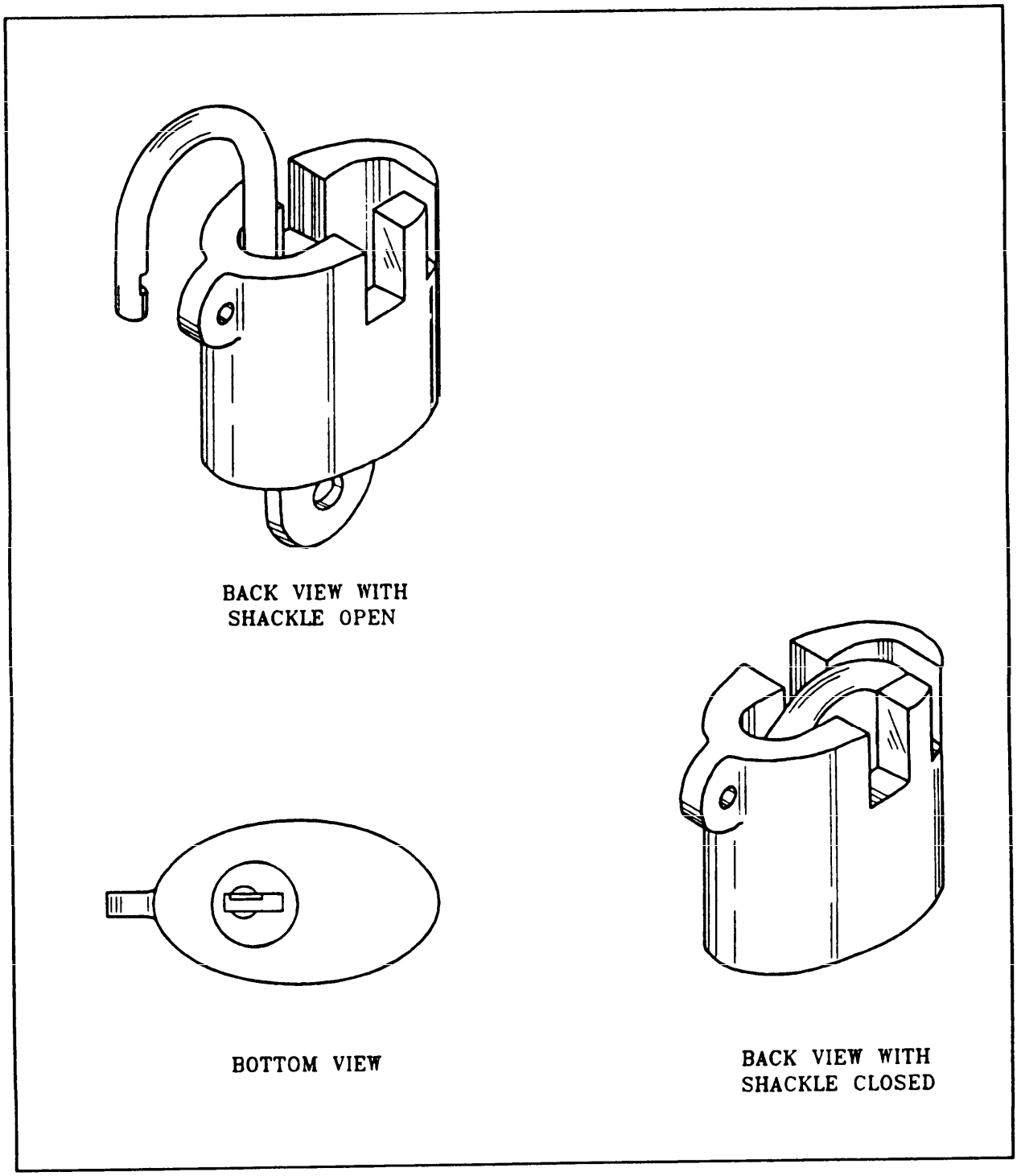


Figure 40
Shrouded Key Operated Shackle Padlock Per MIL-P-43607

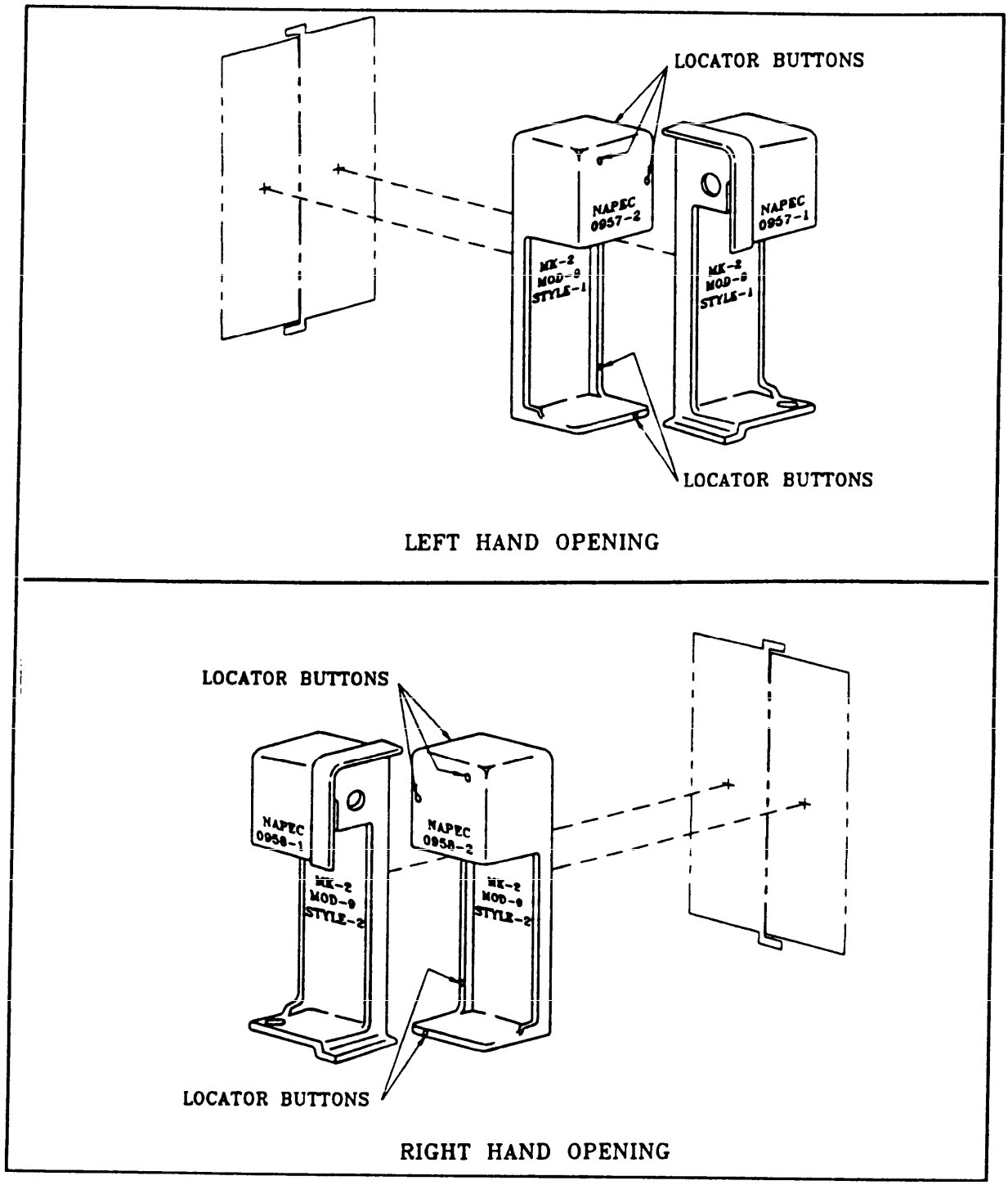


Figure 41
Shrouded Hasp For Padlocks MIL-H-29181

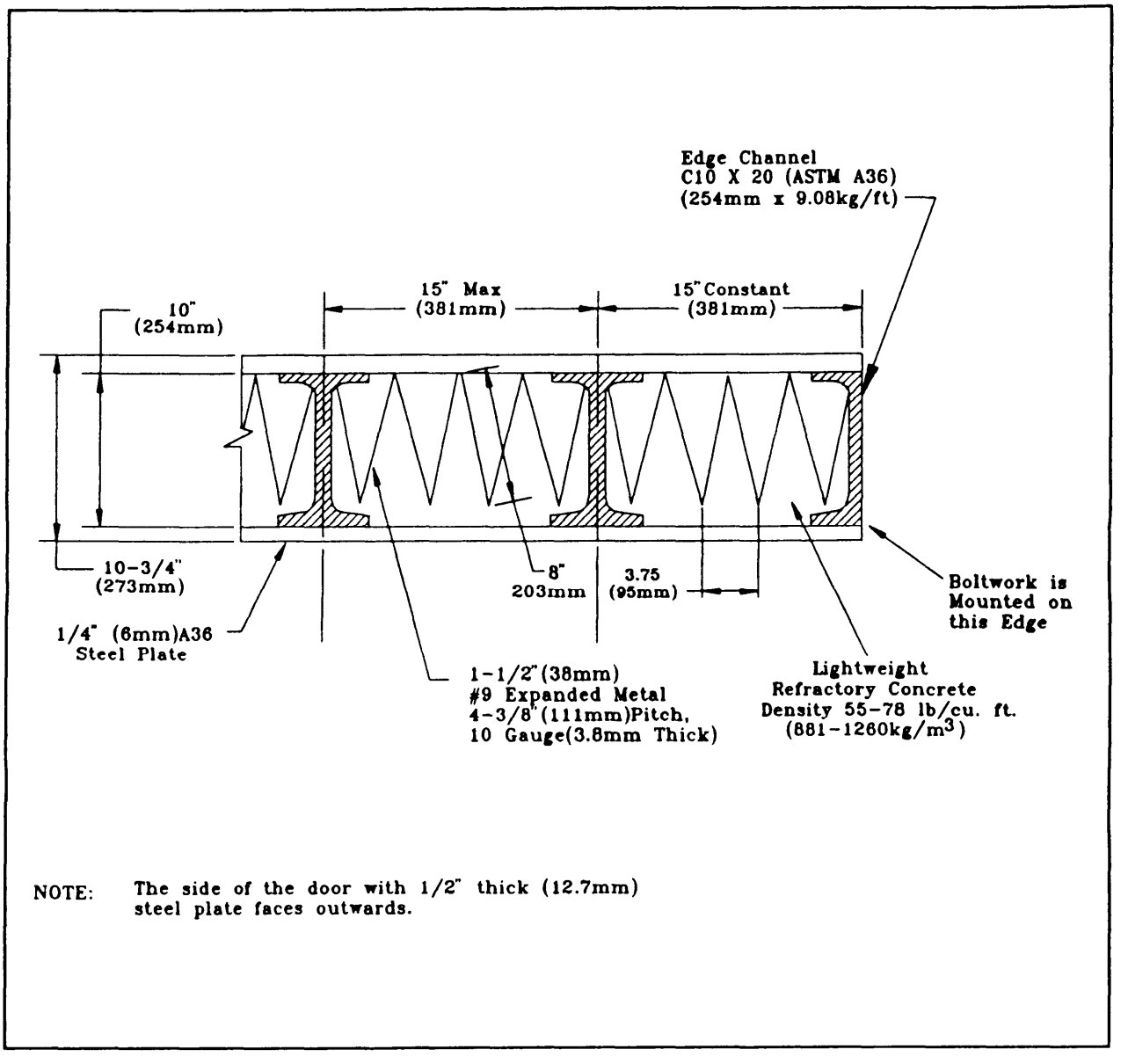


Figure 42
Magazine Door Panel Cross Section For Very High-Severity Threat

2) Medium-Severity Threat. Use 4-inch (100-mm) sliding doors (2) constructed of 14-gauge (1.9-mm) hollow metal or 3/8-inch (9-mm) steel plate.

3) High-Severity Threat. For the high-severity threat, use the magazine door described in Table 16.

5.5.6 New Window Construction

5.5.6.1 Summary. Practical glazing systems presently for the medium-severity level provide up to 4 minutes of delay. None exist for the high- or very high-severity level. An alternative to glazing systems is to use grills over openings. Combinations of glazing and grills are also possible. Table 34 shows the time required and the number of cuts necessary to open man-passable entries in grills as a function of bar size and spacing.

Table 34
Time and Number of Cuts Required to Open a Man-Passable Entry in Grills Composed of Various Size Bars and Bar Spacings

Bar No.	No. 3 (9.5 mm)	No. 4 (12.7 mm)	No. 5 (15.9 mm)	No. 6 (19.1 mm)
Low- and Medium-Severity Threat Level			High-Severity Threat Level	
Spacing in (mm)	Time (minutes)	Time (minutes)	Time (minutes)	Time (minutes)
3(75)	1.2	1.7	2.5	3.5
3.5(90)	0.8	1.2	1.6	2.3
4(100)	0.8	1.2	1.6	2.3
4.5(115)	0.8	1.2	1.6	2.3
5-9(125-225)	0.4	0.6	0.8	1.2
>10(250)	0.0	0.0	0.0	0.0

Notes:
1. Estimates are for a single-layer grill composed of steel bars of the diameter shown, equally spaced both horizontally and vertically.
2. Times shown are total time measured in minutes required to provide a man-passable entry of at least 96 square inches (0.06 sq m).
3. Cuts shown are the minimum total number of bars that must be cut to provide the man-passable entry.
4. All rebar should be embedded 6 inches in concrete and welded at intersections.

Table 35
Recommended Glazing System Installed In a Low-Security Wall (Wood Frame) for a Low-Severity Threat Attack

1 Minute of Penetration Delay

Component	Description
Glazings	1/2-inch (12.7-mm) laminated polycarbonate (a) 11/16-inch (17.4-mm) glass-clad polycarbonate with 3/8-inch (9.5-mm) monolithic polycarbonate 7/8-inch (22.2-mm) glass-clad extruded ionomer with 1/2-inch (12.7-mm) core 1-3/8-inch (35-mm) glass-air gap with 1/2-inch (12.7-mm) laminated polycarbonate (b) 1/4-inch (6.4-mm) laminated glass
Frames	1/4-inch (6.4-mm) minimum total frame thickness 1/4-inch (6.4-mm) minimum thickness of removable stop 1-inch (25.4-mm) minimum bite 1-1/4-inch (32-mm) glazing rabbet depth
Lag Bolts	3/8- by 3-1/2-inch (9.5- by -90-mm) lag bolts

(a) 1/2-inch (12.7-mm) laminated polycarbonate tested in FY90 and FY91.
(b) 1-3/8-inch (35-mm) glass-air gap polycarbonate tested in FY91.

5.5.6.2 Low-Severity Threat Level

1) Low-Severity Threat. Glazing, frame, and anchorage designs for the low-severity threat are summarized in Table 35 for 1 minute of penetration delay. These designs are for installation in a wood-frame wall.

2) Medium-Severity Threat. A glazing, frame, and anchorage design for the medium-severity threat is summarized in Table 36. This design provides 4 minutes of penetration delay.

3) High-Severity Threat. There is no known glazing which will provide high-severity threat integrity. An alternative to a glazing system is a combination of glazing and window barrier over the opening. Figure 43 is a window barrier that will provide 15 minutes of delay against a high-severity threat attack.

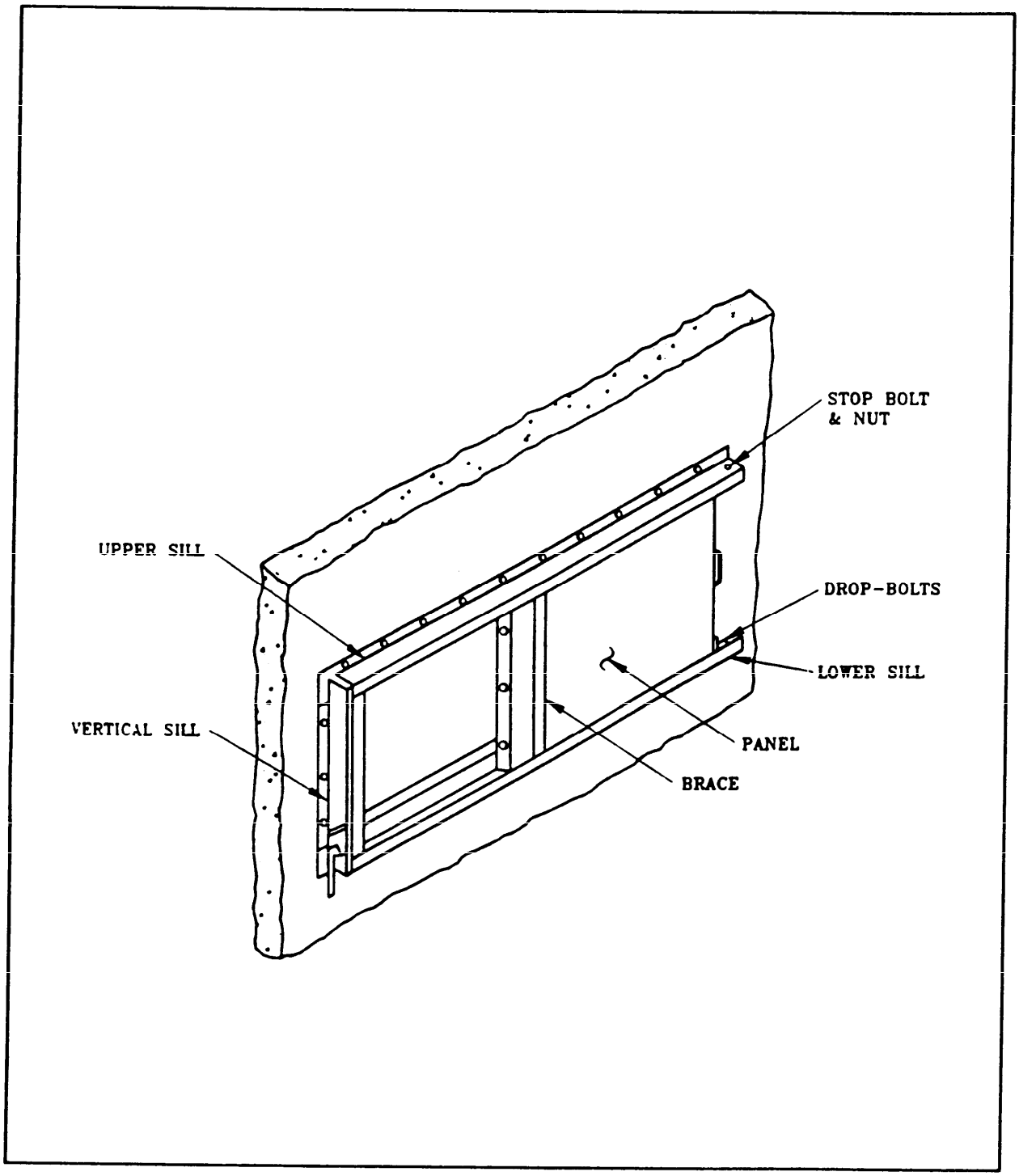


Figure 43
Window Barrier System For High-Severity Threat

Table 36
Recommended Glazing System Components Installed in a Medium-Security (CMU) Wall for a Medium-Severity Threat Attack
Medium Security Level
(4 minutes)

Component	Description
Glazings	1-1/4-inch (32-mm) laminated polycarbonate 15/16-inch (24-mm) glass-clad polycarbonate with 1/2-inch (12.7-mm) laminated polycarbonate 1-3/4-inch (44-mm) glass-air gap polycarbonate with 1-1/4-inch (32-mm) laminated polycarbonate 2-1/8-inch (54-mm) glass-clad extruded ionomer with 1-inch (25-mm) extruded ionomer (a)
Frames	1/4-inch (6-mm) minimum total frame thickness 1/4-inch (6-mm) minimum thickness of removable stop 1-inch (25-mm) minimum bite 1-1/4-inch (32-mm) glazing rabbet depth
Anchor Bolts	1/2- by 4-inch (12.7- by 100-mm) one-piece expansion sleeve 3/8- by 3-inch (9.5- by 75-mm) taper bolt

(a) Glazing tested in FY91.

5.5.6.3 Bars and Grills. Table 34 shows that the penetration time is related directly to the diameter and spacing of the bars. If, for example, No. 5 (16-mm) bars are spaced 3 inches (75 mm) apart (both vertically and horizontally) to form a grill, a penetration time of about 2.5 minutes can be achieved. Use of a double grill of the same construction should increase penetration time to over 5 minutes. More grill layers will provide a proportional increase in penetration time. When bars are used as penetration delay devices, the method of anchoring them to the wall is critical, since it may be easier to tear or pry them loose than to cut them. It is recommended that bars only be used for concrete walls, ceilings, roofs, slabs, or CMU walls and that they be embedded at least 6 inches (150 mm) therein. Alternatively, they may be welded to a steel channel or angle frame which is built into the construction as a unit.

5.5.7 Utility Openings for New Construction - Low- to High-Severity Threats

5.5.7.1 Overview. Utility openings, manholes, tunnels, air conditioning ducts, filters, or equipment access panels can provide intruders with an attractive entrance or exit route. If possible, such openings should be eliminated, or if necessary, kept below the man-passable size of 96 square inches (0.06 sq m). The following briefly describes typical utility openings and design options for hardening them when they can not be eliminated, or must be larger than 96 square inches (0.06 sq m).

5.5.7.2 New Construction Design Considerations. Methods for hardening electrical system conduits, mechanical system conduits for air conditioning, heating, and venting systems, roof-mounted equipment, filter banks, manholes, and other openings are discussed in this section.

1) Electrical and Mechanical Conduits. These consist typically of sewers, manholes, pipe chases, and sleeves and trays.

a) Sewers/manholes. If possible, providing a cluster of pipes, each less than 96 square inches (0.06 sq m) in cross section is more desirable than one large pipe. If a large pipe is required, it is important to ensure that structure walls, floors, or foundations which are accessible from such underground routes provide the required penetration time against penetration attempts. Furthermore, actual entry ports from the sewers to the structure should, if possible, be constricted to make their expansion into a man-passable opening very difficult and time-consuming. Obviously, an effective intrusion detection system capable of detecting pre-intrusion activities (e.g., a seismic system to detect digging) is very important for high-risk situations.

i) Hardening against low- and medium-level threats. Single (or multiple) fixed grills No. 4 (12.7 mm) or smaller bars and with spacings of 3 inches (75 mm) or more can be installed in sewers to provide the penetration times against hand-held tools as shown in Table 34. Figure 17 shows an example of a grill for concrete culvert pipe (see MIL-HDBK-1013/10 for details). Although locked manhole covers may discourage a less-dedicated intruder, typical fastening devices offer little penetration delay times (<1 minute) against a dedicated threat. Manholes should not be accessible to a potential intruder.

ii) Hardening against high-level threats. Single (or multiple) fixed grills with at least No. 5 (15.9-mm) bars and with spacings as shown in Table 34 provide the penetration times indicated.

b) Pipe chases. Pipe chases are horizontal or vertical framed-in passageways that may be as small as 1-foot square (305-mm square) to any desired size. They are typically constructed of studs and gypsum board.

If unprotected, vertical chases connecting adjacent floors may provide unlimited access once an intruder is inside the chase system. Similarly, horizontal chases (walk-throughs) may offer little impedance to movement except that afforded by the internal equipment, piping, cable, and the entrance door(s). Entrances to, or exits from, overhead crawl spaces may also be made from some chases.

i) Hardening against low- and medium-level threats. Single (or multiple) fixed grills with No. 4 (12.7 mm) or smaller bars and with spacing of 3 inches (75 mm) or more can provide limited penetration times against hand-held tools (see Table 34).

ii) Hardening against high-level threats. Single (or multiple) fixed grills with No. 5 (15.9 mm) or larger bars with spacings as shown in Table 34 provide the pentration times indicated. Another option, if maintenance access is not required, is filling the opening with a 2-foot (0.6-m) length of steel pipe, welded together and anchored securely in place by a welded structure on the inside (secure side) of the structure as shown in Figure 44. The honeycomb material should be of a grade of steel reasonably resistant to cutting with hand and thermal tools [at least 1/8-inch (1.6-mm) thick]; however, the penetration time will accrue mainly from the length of the honeycomb and the resultant 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 adjacent turn in the tunnel 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.

Construction can be undertaken in two ways. One approach is to weld the steel pipes front and back at least 3 inches (75 mm) on each end and at each point where the steel pipes intersect. No steel pipe diameter inside the pipe should be greater than 10 inches (250 mm) to ensure a smaller-than-man-passable opening. A second approach is to eliminate the center steel pipe and to connect the remaining six 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 44, is not a man-passable opening. These constrictions should be located at attack-hardened secure walls. The length of the constriction should force the intruder to attack and remove each barrier separately. The confined working space and the necessity for debris removal further add to penetration time.

c) Sleeves and trays. Sleeves are pipe penetrations 1 inch (25 mm) to 8 inches (200 mm) in diameter through walls, roofs, etc. Trays are removable composed of a sheet-metal-covered conduit 3 inches square (75 mm square) or larger. Sleeves and trays should penetrate security walls at a

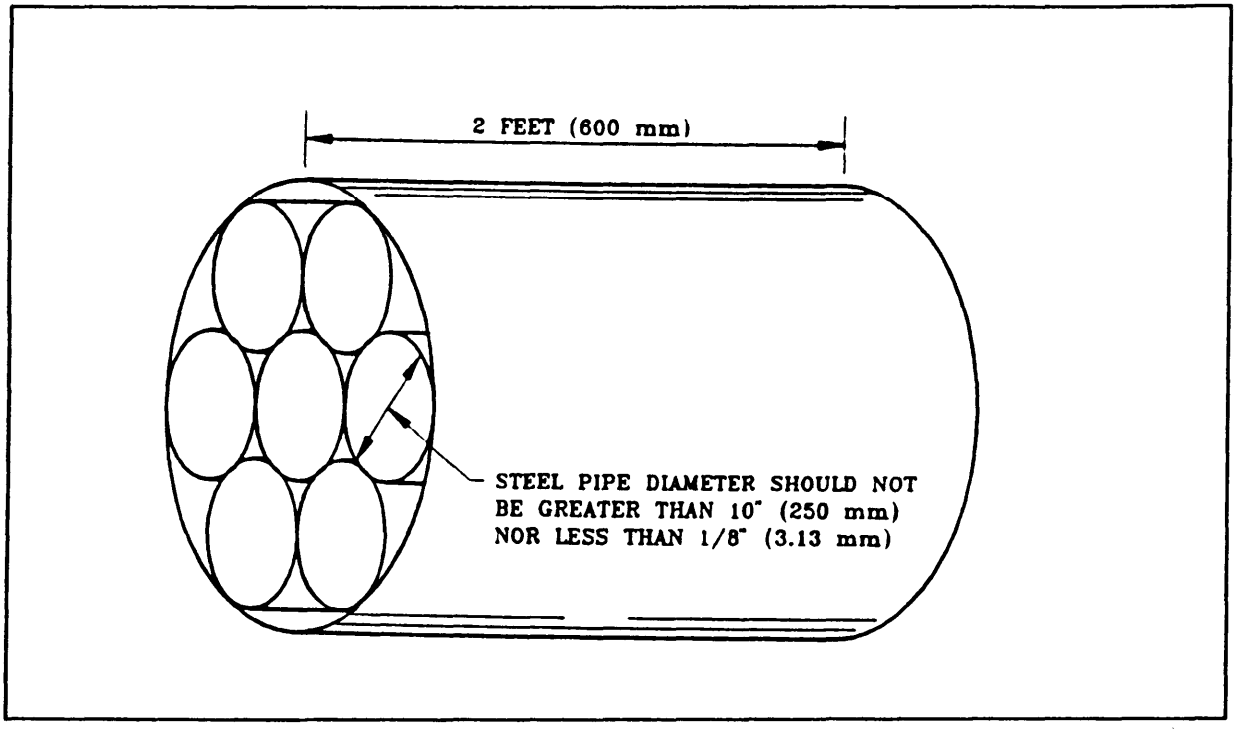


Figure 44
Example of Large Vent Pipe and Chases Rendered Non-Man-Passable by a Honeycomb of Welded Sections of Pipe of Non-Man-Passable Diameter

steep angle so that the length of the opening will be large enough to forestall its use as a convenient entry for a saber saw or other cutting device. Holes should be angled upward and, to the extent practical, contain sharp turns to prevent the easy introduction of hooks, cables, or explosive devices. They should by kept to the minimum possible dimensions.

2) Air-Conditioning, Heating, and Ventilation systems. These systems include ducts, gravity vents, and exhaust vents.

a) Ducts. Ducts are sheet metal or fiberglass conduits, round or square, which may vary from 3 inches (75 mm) on a side, or in diameter up to any required size [e.g., 6 or 8 feet (1,800 or 2,400 mm) on a side]. 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 incidentally enhanced by the use of ducts of less than man-sized cross section and the inclusion of required appurtenances, turning vanes, dampers, pressure plates, or the final air distribution fixture. The standard specification for steel air ventilating grill units for

detention units American National Standards Institute/American Society for Testing and Materials (ANSI/ASTM A 750-84) shows at least one secure design. Duct dimensions should be kept at less than a man-passable cross section. However, airflow capacity requirements and cost can be applied to ducts in an effective manner due to confined working spaces and the possibility of using multiple and widely spaced grills.

i) Hardening against low- and medium-level threats. Single (or multiple) fixed grills with No. 4 (12.7 mm) or smaller bars, and with spacing of 3 inches (75 mm) or more can provide limited penetration times against hand-held tools (see Table 34).

ii) Hardening against high-level threats. Single (or multiple) fixed grills with No. 5 (15.9 mm) or larger bars, and with spacings as shown in Table 34 provide the penetration times indicated. Another option is to insert strategically placed honeycomb sections (similar to those shown in Figure 44) to restrict passages. Although such sections will require care in design to avoid airflow and noise problems, they are feasible. Since duct walls are generally easy to cut through, i.e., 18- to 24-gauge (1.2- to 0.6-mm) sheet steel, the honeycomb must be strategically located so that the intruder cannot bypass it by gaining entrance to the crawl space or "soft" ceilings. It may be necessary to reinforce the duct walls at some locations with high resistance materials such as steel/polycarbonate laminates (see Table 38 and Figures 46 through 48 in par. 5.6.3). The honeycomb sections should be located, if practical, at sharp bends in the ducting. Depending on duct size, cost, and air flow, an alternative approach would be to replace the single duct with a double- or triple-duct system at selected, strategic points. As previously noted, the inclusion of required appurtenances, turning vanes, dampers, pressure plates, or the final air distribution fixture may also add a few minutes to penetration time. This can be further enhanced by anchoring such fixtures securely and by using grills and bar gratings of a dimension and shape that force the use of large and unwieldy tools (see Table 34).

b) Gravity Vents. Gravity vents vary in size from 6 inches (150 mm) to 4 by 8 feet (1,200 by 2,400 mm). Since they terminate inside the building, gravity vents can provide direct entrance if not properly protected. A typical barrier now used in these ducts is a 3/8-inch (9-mm)-thick perforated steel plate welded to an 18-inch-diameter (450-mm-diameter) pipe. A key limiting factor effecting the hardening of a vent is the depth (i.e., volume of space) available for installing barriers.

i) Hardening against low- and medium-level threats. If the vent is simply an aperture in a wall or roof, the problem is analogous to hardening a window with grills or bars. Single (or multiple) fixed grills with No. 4 (12.7 mm) or smaller bars and with spacings of 3 inches (75 mm) or more can provide limited penetration times against hand-held tools (see Table 34).

ii) Hardening against high-level threats. If possible, the vent should be kept to less than man-passable size. Penetrations through vents smaller than the 96-square-inch (0.06-sq-m) man-passable opening require attacking the surrounding wall or roof to enlarge the vent. The vent itself may provide an advantage in such an attack since it can eliminate the necessity of drilling a hole for introducing tools. Any vent, no matter how small, can provide a convenient entry for the blade of a tool used to breach the roof or wall through which the vent passes. Therefore, as a minimum, all vents should be hardened with massive steel collars at the structure interface, as illustrated in Figure 45. If the vent must be kept at a man-passable size, and if space exists behind it, the best approach to increase penetration time is to fill the opening with lengths of steel pipe welded into a "honeycomb" (see Figure 44). This causes the intruder to have to make cuts in depth, which increases cutting time but also seriously interferes with his use of tools. An alternative approach is multiple and widely spaced grilled barriers in the shaft or duct leading from the vent (see Table 34). This approach is only effective, however, if the facility's mechanical layout is such that the intruder cannot cut his way out of the duct or shaft and gain access to the facility before the grilled barriers are reached. Even very small vents must be protected since they can be an easy route for introducing explosive charges. Traps or bends at carefully selected locations can often prevent this.

c) Exhaust vents. Exhaust vents through roofs and walls are generally considered to be protected by the equipment used in conjunction with them. However, if the equipment is removed, the entrance is open. Because the ductwork, damper, etc., are usually contructed of light sheet metal, penetration can be accomplished through the use of hand tools. Typical exhaust ducts range in size from 6 inches (150 mm) 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 (above) generally applies in the case of exhaust vents. Possibilities for reducing vents to less than man-passable size by using multiple honeycombs (Figure 44) should be considered. In some cases, the exhaust system machinery itself may add to penetration time.

3) 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 hand tools. Openings uncovered when equipment is removed can provide an adversary entry to the interior of the facility. In many installations, the removal of only eight bolts, plus the withdrawal of the equipment, can provide access. Although expensive, the only known way of providing extended penetration time for man-passable openings exposed by the removal of roof-mounted machinery is a hardened "penthouse" to house the machinery. Penthouse penetration time will depend on structural components, doors, and openings used. Specific penetration times can be estimated by the same methods described for structures throughout this handbook. The use of

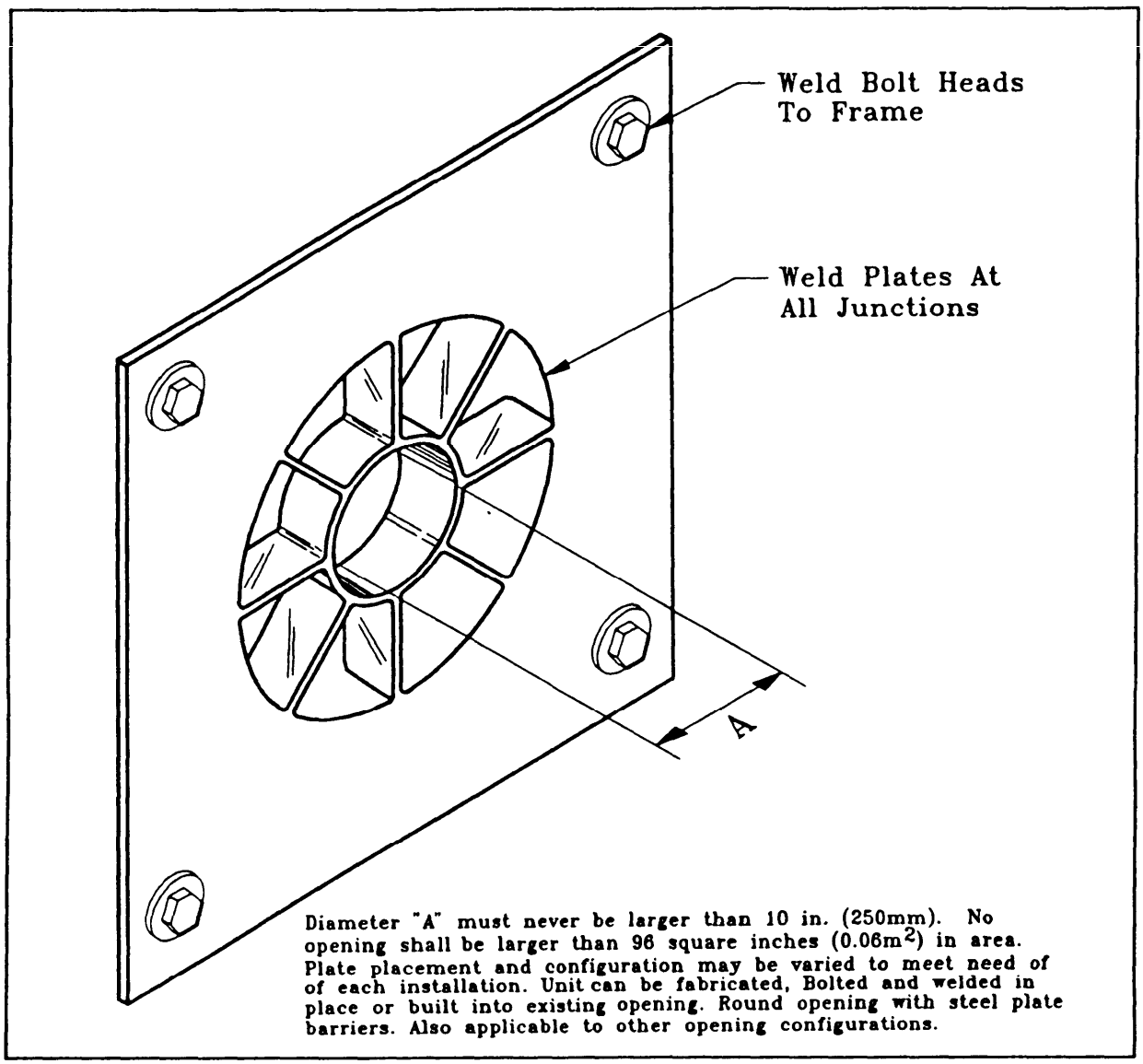


Figure 45
High Security Can Be Provided by Vent Frame Hardening as Shown

multiple small ports in the penthouse structure hardened by multiple grills (see Table 34) might be considered.

4) Filter Banks. The discussion above regarding roof-mounted equipment applies in general to filter banks, except that the banks themselves are unlikely to offer any significant penetration time. A hardened enclosure, with one of the vent or duct hardening techniques, appears to be the best approach.

5) Miscellaneous Openings. Structure openings, such as skylights, roof-hatches, scuttles, elevator shafts, ash dumps, rubbish chutes, fire escapes, and roof access ladders, offer access to intruders and should be considered in hardening plans. One should try to eliminate openings that are not absolutely necessary. The approach to upgrading those that remain will be dictated by the structural elements involved, that is, by appropriate design of walls, roofs, doors, and locking mechanisms.

5.6 Retrofit Construction Design

5.6.1 Introduction. This section provides design options for retrofiting an existing building against forced entry attack. Paragraph 5.6.2 addresses the very high-severity threat involving explosives in comination with hand, power, or thermal tools. This is followed by options to protect against low-, medium-, and high-severity threats involving hand, power, and thermal tools only. Paragraph 5.6.3 provides options for walls, par. 5.6.4 for roofs and floors, par. 5.6.5 for doors, par. 5.6.6 for windows, and par. 5.6.7 for utility openings. The objective of the design is to supplement the penetration time offered by the existing building construction with retrofit options that achieve the required penetration delay times against the design threat severity for the building established in Section 2. The design must also assure a balanced design between all building components. This means approximately equal penetration delays for each with no vulnerable weak links. The following pages provide forced-entry delay times one can expect from the existing construction followed by the penetration-time enhancement afforded by various retrofit design options.

5.6.2 Considerations Related to the Very High-Severity Threat. The use of explosives in bulk or flyer plate form can be especially effective in quickly producing holes large enough for an intruder to enter. Only buildings made of reinforced concrete 12 inches (305 mm) or more in thickness can provide penetration delay times greater than 1 minute (see Table 19). In general, there are no retrofit options that can protect existing construction from an explosive penetration attack. The only choice is to locate the critical area being protected internally and low in the building, well away from exterior walls, roofs, etc. The exterior of the building will serve as a sacrificial barrier forcing the intruder to penetrate multiple barriers.

5.6.3 Wall Retrofit Construction for Low- Through High-Level Threats

5.6.3.1 Summary. Table 37 summarizes the maximum penetration delay times achieved by existing wall construction in use today. Only in the case of reinforced concrete with thicknesses of at least 12 inches (305 mm) do barrier penetration times exceed 30 minutes for high-level threats. Reinforced concrete less than 12 inches (305 mm), offers single barrier penetration times under 30 minutes. Conventionally constructed masonry and stud/girt walls provide penetration times up to 18 minutes and 1.5 minutes, respectively. The following pages contain information to estimate the penetration times offered

by the walls of your existing facility and to retrofit harden these walls if additional delay time is required.

5.6.3.2 Low-Security Threat Level. In general, it is not practical to attack walls using only a limited set of low-observable hand-held tools. A low-level threat would likely attack the doors, windows, or other more vulnerable part of the facility rather than the walls. Consequently, any wall construction can be considered adequate for this threat level.

5.6.3.3 Medium- and High-Security Threat Levels. The general categories of wall construction for existing facilities addressed in the following includes: (1) reinforced concrete, (2) masonry, (3) stud-girt with layered wood, gypsum, stucco, etc., panels. The inherent penetration delay times offered by these walls are provided followed by retrofit options to enhance these delay times.

Table 37
Existing Wall Construction Achievable Penetration Times

Wall Construction Type	Maximum Penetration Delay Times (minutes) Achievable For Threat Severity Level		
	Low	Medium	High
Stud-Girt (a)	<1	1.6	1.5
Masonry (a)	(b)	5.5	18
Reinforced Concrete (a)	(b)	7.5	35

(a) As described in what follows, different cross-section design characteristics apply to the low, medium, and high threat level.
(b) It is not practical for low-level threats to attack walls. Any construction can be considered adequate.

1) Reinforced Concrete

a) Representative existing construction. Representative existing construction includes:

- Cast-in-place walls. The forms are constructed vertically and the concrete poured on-site.

- Tilt-up walls. These are similar to cast-in-place walls except that the walls are poured on the ground and then raised to the vertical.

• Precast walls. These are constructed elsewhere and shipped to the site.

The thickness of typical precast or tilt-up walls may be as low as 3-1/2 inches (90 mm) to as high as 12 inches (300 mm). A cast-in-place wall typically begins at 4 inches (100 mm) and may reach as high as 30 inches (760 mm). The corresponding reinforcement may be as low as a single layer of No. 3 (9.7-mm) steel bars at 12-inch (300-mm) spacing each way, for the 3-1/2-inch (90-mm) or 4-inch (100-mm) wall, to as high as No. 8 (25-mm) bars at 3 inches (75 mm) each way at each face for the 12-inch (300-mm) wall. Concrete with compressive strengths between 3,000 and 6,000 psi [20.7 and 41.4 megaPascal (MPa)] and steel rebar with tensile strengths between 40,000 and 60,000 psi (276 and 414 MPa) are typically used.

b) Penetration times for existing reinforced concrete construction. For conventional concrete materials, the penetration times range from about 2 minutes to more than 60 minutes. At the time this handbook was written (1992), no data for hand, power, and thermal tool attacks on concrete walls exceeding 12 inches (300 mm) in thickness were available. One can expect, though, that these thicker walls will exceed 40 to 45 minutes to penetrate, with a 30-inch (760-mm) wall taking much more than an hour. For walls up to 12 inches (300 mm) thick, Figure 33 and Table 22 (par. 5.5.3) can be used to estimate penetration times for various thicknesses and rebar combinations. It should be noted that the data point on Curve C in Figure 33 with a penetration time of about 15 minutes for 8-inch (200-mm) reinforced concrete walls is the expected penetration time of the 8-inch (200-mm) reinforced concrete wall construction mandated for Category II AA&E storage facilities by DOD 5100.76-M.

c) Retrofit options for medium-severity level threats. Note in Figure 33 that reinforced concrete 6 inches (152 mm) thick with the "B" rebar combination shown in Table 22 achieves minimum penetration times up to about 7.5 minutes for medium-severity level threats. If the concrete thickness and rebar combination is outside the medium threat region shown in Figure 33, using hand-held attack tools alone is not practical. In this case, the existing wall provides adequate security. If the concrete thickness is at least 6 inches (152 mm) and the rebar combinations are at or within the medium threat level region of Figure 33 and more delay time is required, about 14 additional minutes can be gained by attaching a 9-gauge (3.8-mm) flattened expanded steel grate to the interior of the wall.

d) Retrofit options for high-severity threats. If the required delay time is greater than that achievable by the existing construction, this penetration delay time can be doubled from the values shown in Figure 33 by simply fixing a 10-gauge (3.4-mm) sheet steel (ASTM A589) to the interior surface of the wall using lag screws or bolts. If this is still not adequate, the steel-ply options summarized in Table 38 and Figures 46 through 48 or the riveted or welded grating shown in Figure 49 can be used.

Table 38
Steel-Ply Retrofit Installations for the High-Severity Level Attack

Type of Construction	Additional Delay Time (minutes)
Three layers [10-gauge (3.4-mm) ASTM A569 steel - 3/4-inch (19-mm) plywood - 10-gauge (3.4-mm) ASTM A569 steel]	6
Five layers [10-gauge (3.4-mm) ASTM A569 steel - 3/4-inch (19-mm) plywood - 10-gauge (3.4-mm) ASTM A569 steel - 3/4-inch (19-mm) plywood - 10-gauge (3.4-mm) ASTM A569 steel]	11
Three layers [9-gauge (3.8-mm) ASTM A607 steel - 3/4-inch (19-mm) plywood - 9-gauge (3.8-mm) ASTM A607 steel]	14 (a)
Five layers [9-gauge (3.8-mm) ASTM A607 steel - 3/4-inch (19-mm) plywood - 9-gauge (3.8-mm) ASTM A607 steel - 3/4-inch (19-mm) plywood - 9-gauge (3.8-mm) ASTM A607 steel]	Not Tested
Three layers [1/4-inch (6.25-mm) type 304 stainless steel - 1/2-inch (12.5-mm) polycarbonate - 10-gauge (3.4-mm) ASTM A607 steel]	10
Five layers [10-gauge (3.4-mm) ASTM A607 steel - 1/2-inch (12.5-mm) polycarbonate - 10-gauge (3.4-mm) ASTM A607 steel - 1/2-inch (12.5-mm) polycarbonate - 10-gauge (3.4-mm) ASTM A607 steel] (b)	17

(a) Twenty minutes with two layers of 90-pound (41-kg) gravel-finish roofing paper.
(b) Recommended for ballistic protection. Source: MIL-HDBK-1013/5

The steel-ply options, including installation techniques, are described in MIL-HDBK-1013/5. Layered sheet steel and wood combinations can double or triple penetration times (see Table 38). The test data indicate that a layer of 3/4-inch (19-mm) plywood sandwiched between two layers of 10-gauge (3.4-mm) hot-rolled steel provides about 6 minutes of penetration time (Table 38). The penetration time can be increased by about 5 minutes with the addition of another wood/steel layer (Table 38). This rule of thumb can be applied to the addition of more layers until the overall thickness of the wall renders the use of hand and power tools impractical. Better gains in penetration time can be achieved by changing the steel layers to 9-gauge (3.8-mm) ASTM A607 HS low alloy steel.

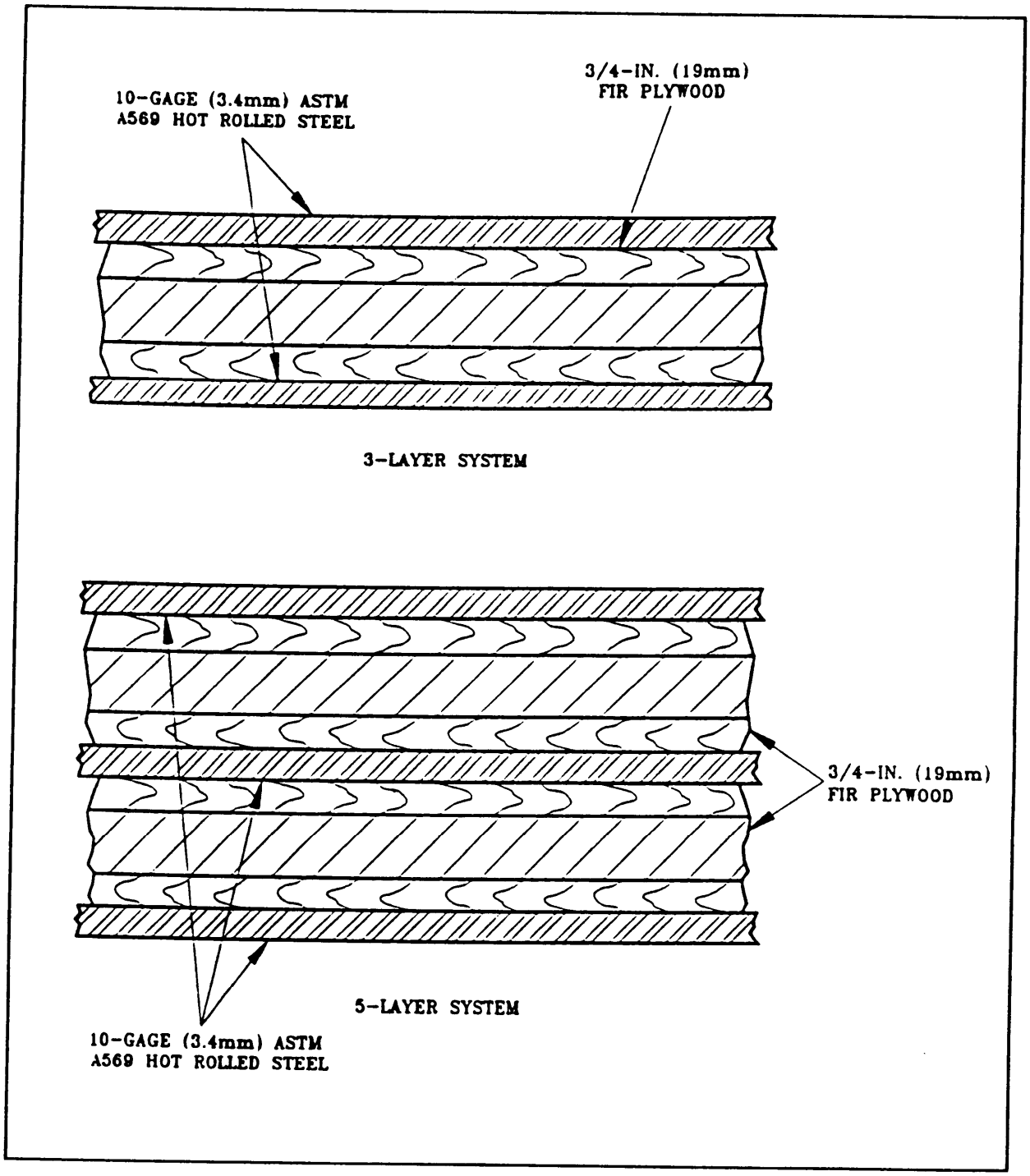


Figure 46
Ten-Gauge (3.4-mm) Hot-Rolled Steel Combinations (MIL-HDBK-1013/5)

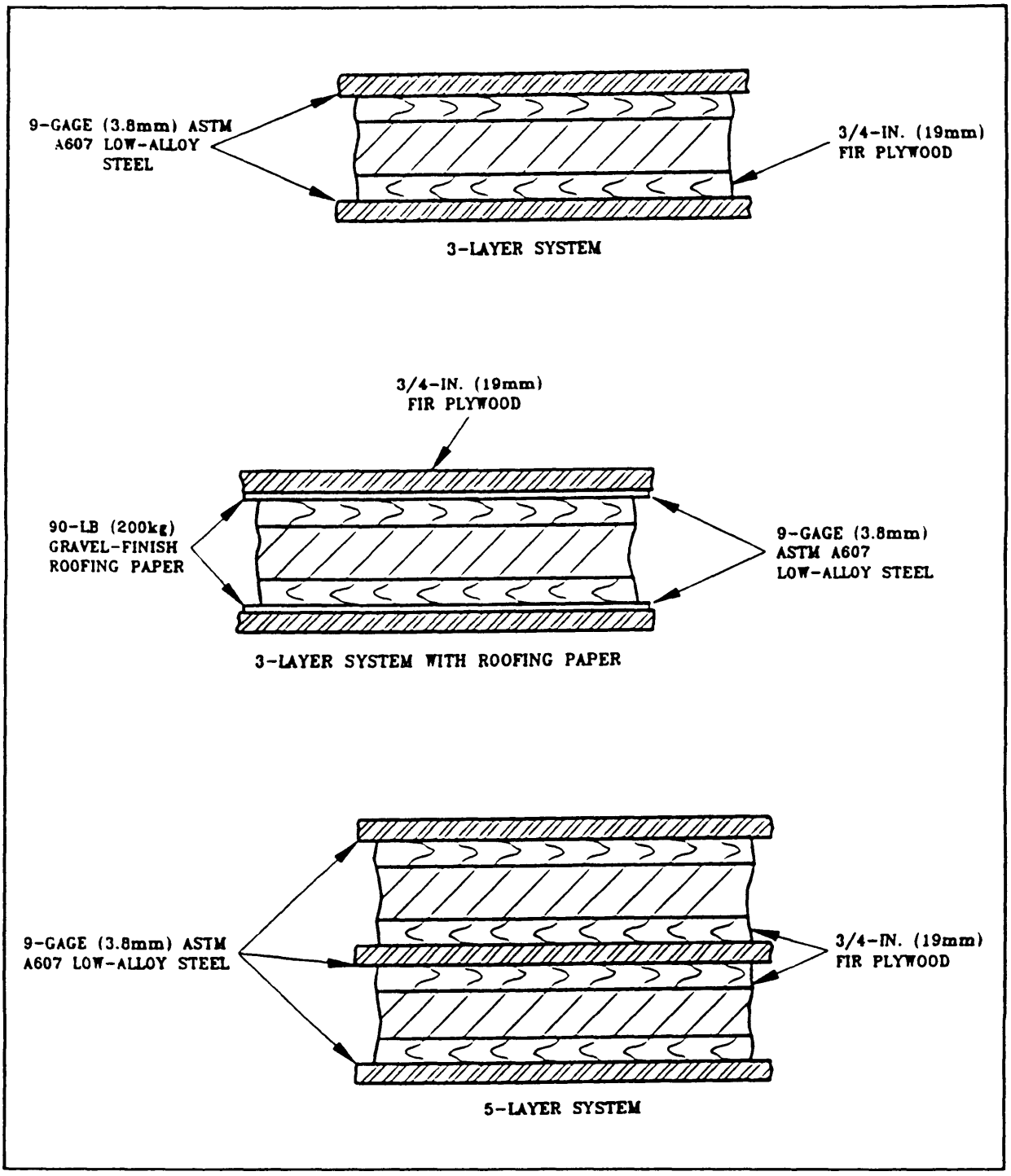


Figure 47
Nine-Gauge (3.8-mm) Hot-Rolled Steel Combinations (MIL-HDBK-1013/5)

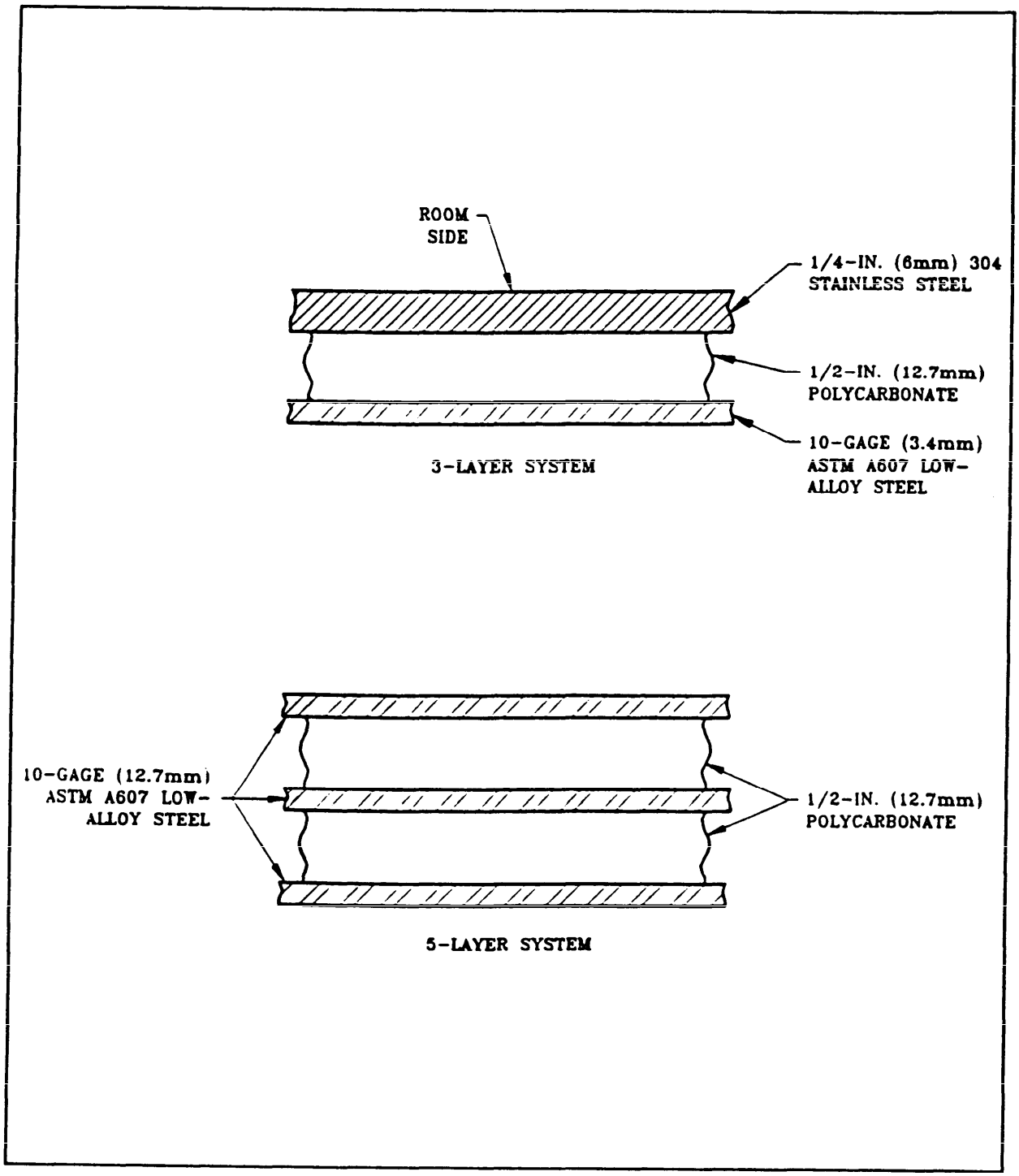


Figure 48
Polycarbonate Combinations (MIL-HDBK-1013/5)

b. Satisfactory. Subcontract does permit optimizing next phase

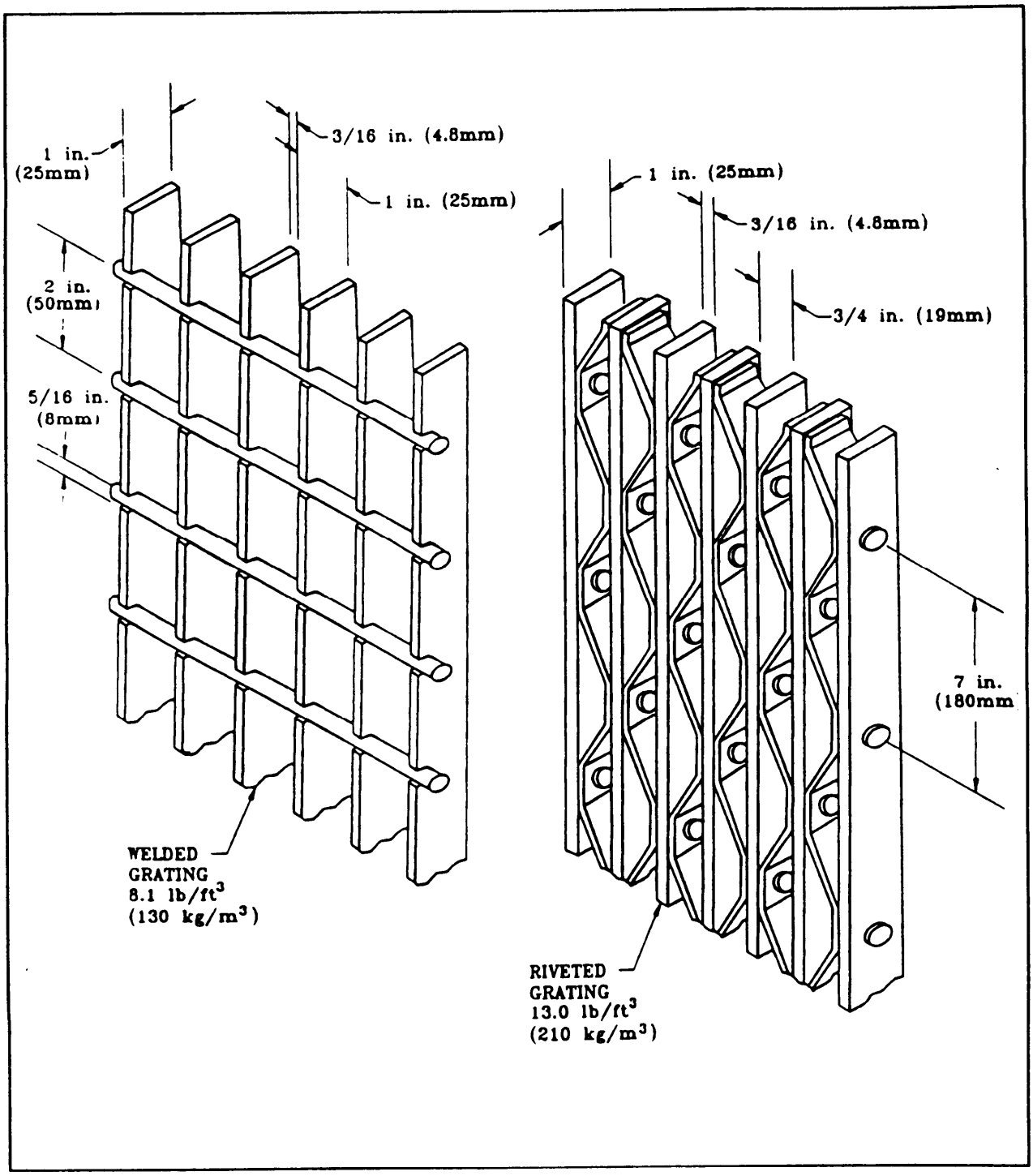


Figure 49
Typical Gratings (MIL-HDBK-1013/4)

One layer of 3/4-inch (19-mm) plywood sandwiched between two layers of this steel provides 14 minutes of penetration time. Adding layers of 90-pound (200-kg) gravel finish roofing paper between the plywood and steel further increases the penetration time to about 20 minutes (Table 38). Alternatively, additional delay time can be obtained by the use of steel grating as shown in Figure 49. This grating is available in standard 2- by 10-foot (0.6- by 3-m) panels and can be affixed to the walls. They can be assembled in a variety of configurations of any length [in 2-foot (0.6-m) increments] as described in MIL-HDBK-1013/4. Additional penetration times offered against high-severity threats are approximately 2 minutes (minimum) for the riveted and 1 minute (minimum) for the welded grading.

2) Masonry Wall Construction

a) Representative existing masonry construction. Masonry walls are typically constructed of one or more of the following materials: concrete masonry unit (CMU), brick, structural tile, or stone. Unreinforced masonry wall construction typically consists of CMU, brick, structural tile, stone, or a combination of these materials. CMU may range from 4 to 12 inches (100 to 300 mm) thick and may be left hollow or grouted solid. Single-wye brick generally comes in widths of 4 to 12 inches (100 to 300 mm). Structural clay tile will typically range from 4 to 8 inches (100 to 200 mm) wide, and stone will usually vary between 6 and 24 inches (150 and 600 mm). As for combinations of these materials, brick or CMU may range from 8 to 16 inches (200 to 400 mm) with masonry ties every second CMU course. Structural clay tile on CMU may be found in widths from 6 to 16 inches (150 to 400 mm) with masonry ties every second course. Brick of structural clay tile may vary from 8 to 12 inches (200 to 300 mm) with ties every sixth brick course. Finally, stone-on-CMU may range from 6 to 16 inches (150 to 400 mm) with ties every second CMU course. Reinforced CMU may vary from 6 to 12 inches (150 to 300 mm) wide, grouted solid with reinforcing ranging from No. 4 rebar (12.7 mm) at 32 inches (800 mm) on-center horizontally and 16 inches (400 mm) on-center vertically, to No. 5 (16 mm) at 16 inches (400 mm) on-center horizontally and No. 8 (25 mm) at 8 inches (200 mm) on-center vertically. Brick-on-stone, double-wye ranges from 10 to 16 inches (250 to 400 mm) thick, grouted solid with No. 6 (19-mm) rebar at 12 inches (300 mm) on-center horizontally and No. 9 (29 mm) at 12 inches (300 mm) on-center vertically. Reinforced CMU with 4-inch (100-mm) stone or brick veneer varies from 10 to 16 inches (250 to 400 mm) wide, grouted solid, with reinforcing ranging from No. 4 (12.7-mm) rebar at 32 inches (800 mm) on-center horizontally and at 16 inches (400 mm) on-center vertically, to No. 5 (16-mm) rebar at 8 inches (200 mm) on-center horizontally and No. 8 (25 mm) at 6 inches (150 mm) on-center vertically.

b) Penetration times for existing masonry construction. Conventional masonry walls provide only limited hardness against forced-entry attacks. They typically offer penetration times ranging from less than 1.5 minutes for hollow masonry to 2 to 5 minutes for solid masonry against medium-severity level attacks (see Figure 31 and Table 21 in par. 5.5.3). For thick solid walls with significant reinforcing, higher penetration times are

achievable against high-severity threat levels (Figure 31). Relative to other forms of construction, masonry walls provide penetration times only slightly greater than stud/girt construction and for the same wall thickness, masonry walls provide penetration times that are much less than reinforced concrete. If additional penetration time is required, consider one or more of the following options depending on the threat severity level.

c) Retrofit options for medium-severity threats. Several techniques for hardening both hollow and mortar-filled 8-inch (200-mm) CMU block are illustrated in Figures 50 and 51. Note that the retrofit hardening layers are applied to the interior 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. The data in Figures 50 and 51 show the penetration times achievable by adding 3 to 4 inches (75 to 100 mm) of steel fiber-reinforced (i.e., ferro-cement) concrete, expanded steel grating, and other options.

d) Retrofit options for high-severity threats. Consider those retrofit options shown in Figures 50 and 51 for 8-inch (200-mm) CMU block. The penetration times can be doubled from the values shown in Figure 33 by simply fixing a 10-gauge (3.4-mm) sheet steel (ASTM A589) to the interior surface of the wall using lag screws or bolts. If this is still not adequate, the steel-ply options summarized in Table 38 and Figures 46 through 48 or the riveted or welded grating shown in Figure 49 can be used. The reader is referred to par. 5.6.3.3(1)(d) for further discussion.

3) Stud/Girt Wall Construction

a) Representative existing construction. Stud walls are used in the construction of wood or light metal frame buildings. The basic frame consists of wood or metal vertical supports, usually 2 by 4 inches (50 by 100 mm) or 2 by 6 inches (50 by 150 mm), placed 12, 16, or 24 inches (300, 400, or 600 mm) on-center. Metal girts are horizontal framing members used in rigid frame systems. They range in depth from 6-1/2 to 9-1/2 inches (165 to 240 mm) and are spaced 2 to 7-1/2 feet (600 to 2,250 mm) on-center. An architectural finish is attached to the exterior side of the stud or girt, and an interior wall finish may be attached to the interior side. The seven basic types of stud/girt wall construction include: stud and stucco, stud and wood siding, stud and plywood siding, stud and shingle siding, stud and composition siding, stud/girt industrial siding, and conventional masonry veneer construction. It should be noted that wood wall construction for permanent buildings is confined primarily to housing and minor structures. Wood construction must be in accordance with the fire protection requirements set forth in MIL-HDBK-1008, Fire Protection for Facilities Engineering, Design and Construction.

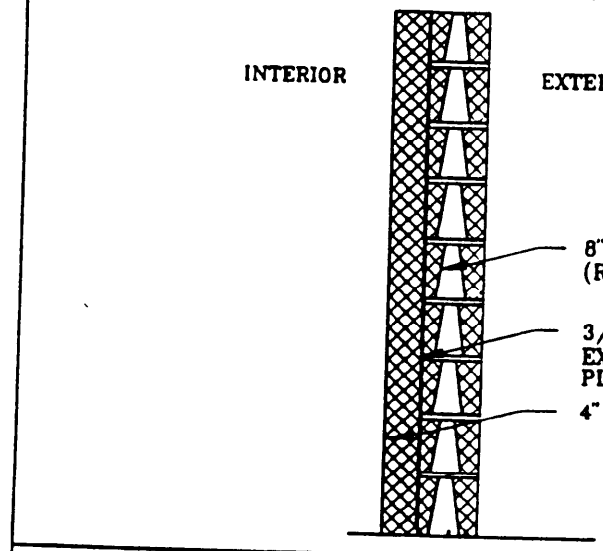
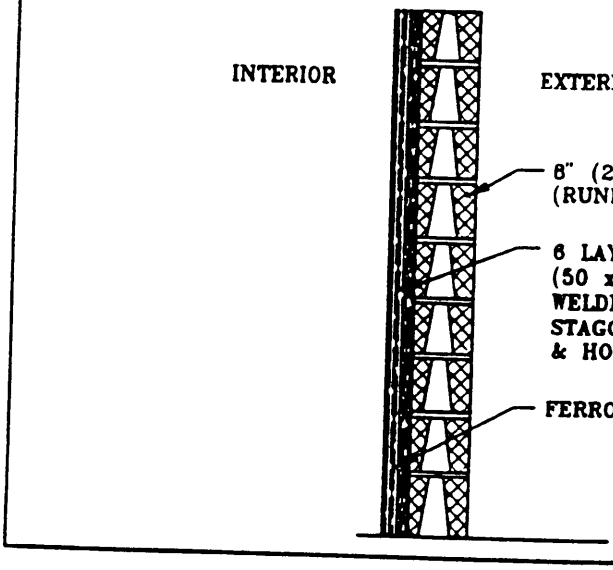
Construction	Penetration Time (min.)	
	Medium	High
	4	4
	7	6

Figure 50
Retrofit Hardening Options For Hollow 8-inch CMU Wall Construction

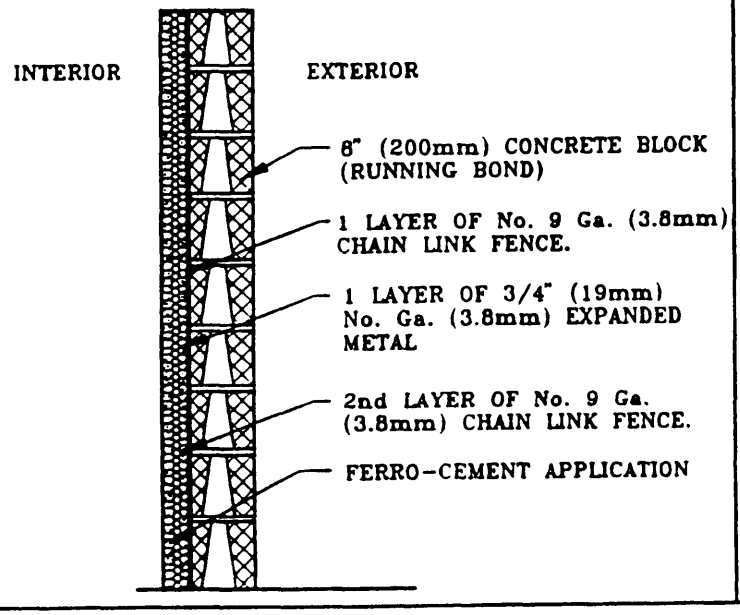
Construction	Penetration Time (min.)	
	Medium	High
	8	4

Figure 50
Retrofit Hardening Options For Hollow 8-inch CMU Wall Construction
(Continued)

b) Penetration times for existing stud/girt construction. Estimated penetration times for the seven basic types of stud/girt walls are all less than 2 minutes (see Table 39).

c) Retrofit options for medium-severity threats. Limited data is available on retrofit options for hardening against medium-level threats. Table 40 shows the delay times achieved by adding 9-gauge (3.8-mm) metal fence material, 1/4- to 3/4-inch (6- to 19-mm) thick plywood, 9-pound (19-kg) expanded metal, or 3/16-inch (4.8-mm) steel plate to a wood panel.

d) Retrofit options for high-severity threats. The steel-ply retrofit options shown in Figure 48 and Table 32 or the riveted or welded steel grating shown in Figure 49 can be affixed to the interior of the stud-girt wall to increase the effective delay time. See par. 5.6.3.3(1)(d) for additional information.

5.6.4 Roof/Floor Retrofit Construction for Low to High Threats

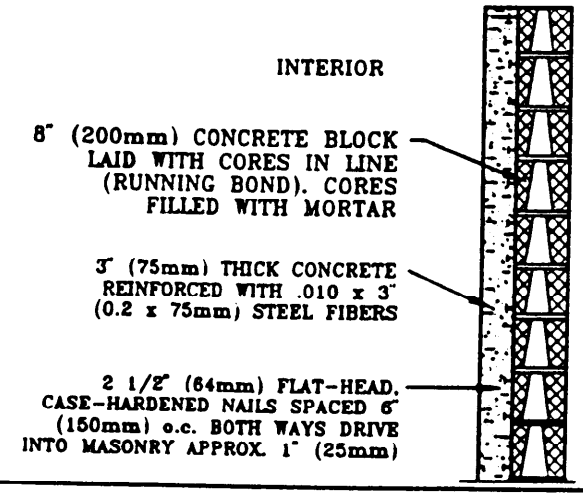
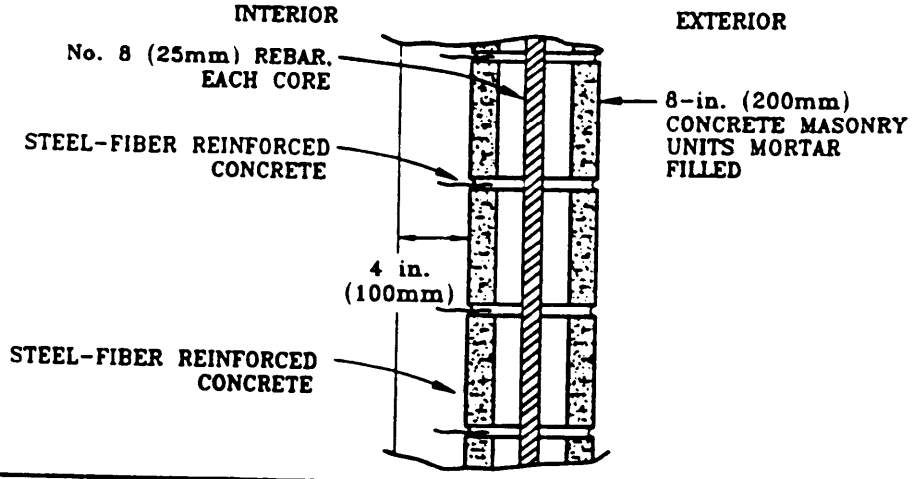
Construction	Penetration Time (min.)	
	Medium	High
	26	23
	(a)	25
(a) It is not possible to penetrate at the indicated threat severity level.		

Figure 51
Retrofit Hardening Options For Mortar-Filled 8-inch CMU Wall Construction

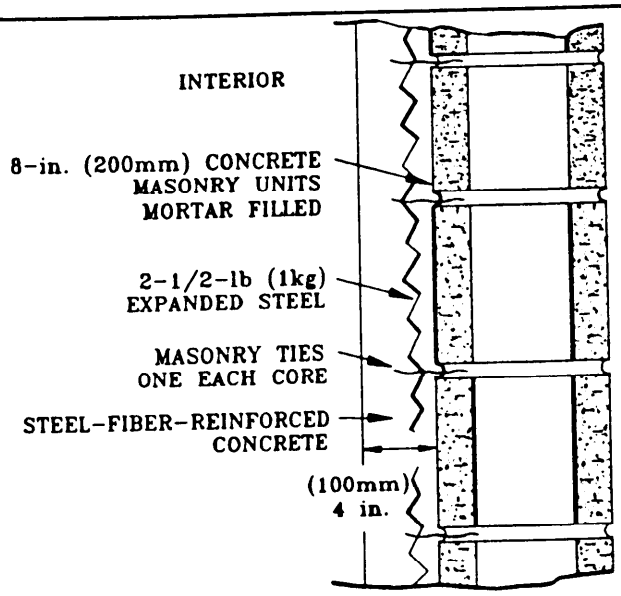
Construction	Penetration Time (min.)	
	Medium	High
	(a)	30
(a) Not possible to penetrate at the indicated threat severity level.		

Figure 51
Retrofit Hardening Options For Mortar-Filled 8-inch CMU Wall Construction
(Continued)

5.6.4.1 Summary. Table 41 summarizes the maximum penetration delay times achieved by floor/roof construction in use today. These times are for the high-level threat. It is not practical to attack these barriers at the low- or medium-level threats. Concrete floors can provide up to about 45 minutes of delay against the high-level threat whereas concrete roofs only provide about 35 minutes. Wood construction provides up to 1.5 minutes against high-level threats and 1.6 minutes against medium-level threats. Metal construction can provide up to about 2 minutes of delay for roofs but up to 15 minutes for floors that use riveted steel gratings.

5.6.4.2 Low-Security Threat Level. As noted, it is not practical to attack roofs/floors with a limited set of hand-held tools. A more reasonable attack would be against more vulnerable parts of the facility such as doors, windows, etc.

Table 39
Representative Existing Stud-Girt Construction

Wood Frame	Penetration Time (minutes)		
	Low	Medium	High
Wood Panel Double 1-inch (25-mm) planking wood siding nailed to 2x4 studs and no interior finish.	(1)	2	1.3
Gypsum Panel 1-inch tongue & groove nailed to exterior side of wood studs 16 inch (400 mm) on center and tar paper & 1/2-inch sheet rock nailed to interior side.	1	0.3	0.3
1-inch (25-mm) tongue & groove nailed to wood studs 16 inches on center, with 1/2-inch (12.5-mm) plywood, tar paper, & 1/2-inch (12.5-mm) sheet rock.	(1)	1.6	1.5
Stucco Panel 1/2-inch (12.5-mm) stucco, chicken wire & tar paper attached to exterior side of wood studs 16 inches (400 mm) on center & 1/2-inch (12.5-mm) sheet rock nailed to inside of studs.	0.5	0.3	0.3
Asbestos Panel 3/8-inch (9.4-mm) corrugated asbestos wall (nonstructural). Note: retrofit can not disturb the asbestos	0.4	0.4	0.4

5.6.4.3 Medium- and High-Security Level Threats. Representative existing construction for roofs and floors include reinforced concrete, wood, and metal. Penetration delay times offered by roofs and floors of the above construction are provided followed by retrofit options to enhance these delay times as required.

1) Reinforced Concrete Roofs and Floors

a) Representative existing construction. The general types of construction include the following:

i) Conventional systems that are cast-in-place on structural members. Slab over open-web steel-joists systems range from 2-1/2 inches (63 mm) thick with No. 3 (9.5-mm-diameter) rebar at 7-1/2 inches (190

Table 40
Stud-Girt Construction Retrofit Options For Medium Threat Levels

Construction	Penetration 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, 1-layer No. 15 felt paper, and 1- by 6-inch (25- by 150-mm) sheathing diagonally and 3/8-inch (9.4-mm) gypsum wallboard. Attach to interior:	
• 3/4-inch (19-mm) plywood, No. 9 expanded metal and 3/4-inch (19-mm) plywood, all attached to interior.	5.0
2. 1-inch (25-mm) tongue-and-groove on 1/2-inch (12.5-mm) plywood.	
Attach to interior:	
• 9-gauge (3.8-mm) metal fence, nailed.	1.8
• 3/16-inch (4.7-mm) steel plate.	1.9

mm) on-center each way up to 6 inches (150 mm) thick with No. 4 (12.7-mm-diameter) rebar at 12 inches (300 mm) on-center.

Composite slab/beam systems range from 6 inches (150 mm) thick with No. 5 (15.9-mm-diameter) rebar at 12 inches (300 mm) on-center each way up to 12 inches (300 mm) thick with No. 5 (15.9-mm-diameter) rebar at 6 inches (150 mm) on-center.

Composite metal deck and slab systems range from 1-1/2-inch (38-mm) thick, 22-gauge (0.8-mm) corrugated steel decking with 2-1/2-inch (63-mm) concrete topping poured with 6- by 6-inch W 1.4 x W 1.4 wire mesh [total 4 inches (100 mm)] up to 3-1/2-inch (90-mm) thick, 22-gauge (0.8-mm) steel decking with 4-1/2-inch (115-mm) concrete topping poured with 6- by 6-inch W 1.4 x W 1.4 wire mesh [total 8 inches (200 mm)].

ii) Conventional systems which are cast-in-place as structural members. One- and two-way slab systems range from 6 inches (150 mm) thick with (minimum) No. 4 (12.7-mm-diameter) rebar at 12 inches (300 mm) on-center up to 18 inches (450 mm) thick with (maximum) No. 5 (15.9-mm) rebar at 3 inches (75 mm) on-center.

The penetration resistance of waffle slab systems should be evaluated on the basis of slab thickness between the reinforcing ribs. The

Table 41
Existing Roof/Floor Construction Achievable Penetration Times

Construction Type(b)	Maximum Penetration Delay Times (minutes) Achievable by Threat Security Level		
	Low	Medium	High
Concrete			
• Roof	(a)	7.5	35
• Floor:			
Downward attack	(a)	7.5	35
Upward attack	(a)	(a)	45
Wood			
• Roof	2.0	1.6	1.5
• Floor	(a)	1.6	1.5
Metal			
• Roof	(a)	(a)	1 to 2
• Floor	(a)	(a)	15

(a) It is not practical for threats at this level to attack the roof or floor.
(b) Different cross-section designs apply to low-, medium-, and high-level threats.

range of normal top slab thickness is between 3 inches (75 mm) and 4-1/2 inches (113 mm) with integral reinforcing ribs 5 to 6 inches (125 to 150 mm) wide spaced 24 or 36 inches (600 or 900 mm) each way. The void spaces between ribs can range between 19 and 30 inches (475 and 750 mm). Total depth of slab plus rib ranges from 11 to 16-1/2 inches (280 to 420 mm) thick. The top slab is reinforced with (minimum) No. 4 (12.7-mm-diameter) rebar at 12 inches (300 mm) on-center up to a maximum of No. 7 (22-mm-diameter) rebar at 6 inches (150 mm) on-center.

iii) Conventional precast prestressed concrete units. Single-tee units range from 3 feet (900 mm) wide by 1-1/2 feet (450 mm) deep up to 10 feet (3,000 mm) wide by 4-1/2 feet (1,400 mm) deep with 6- by 6-inch W 1.4 x W 1.4 wire mesh in 2-inch (50-mm) flanges.

Double-tee units range from 4 feet (1,200 mm) wide by 1-1/8 feet (350 mm) deep up to 8 feet (2,500 mm) wide by 2-2/3 feet (810 mm) deep with 6- by 6-inch W 1.4 W 1.4 wire mesh.

Prestressed deck units range from 8 to 10 inches (100 to 250 mm) thick with tendons at 16 inches (400 mm) on center with 6- by 6-inch W 1.4 x W 1.4 wire mesh.

iv) Conventional post-tensioned cast-in-place flat slabs. One-way slabs range from 4-1/2 inches (113 mm) thick with No. 4 (12.7-mm-diameter) rebar at 36 inches (900 mm) on-center and No. 5 (15.9-mm-diameter) rebar at 12 inches (300 mm) on-center up to 9 inches (225 mm) thick with No. 4 (12.7-mm-diameter) rebar at 24 inches (600 mm) on-center, and No. 6 (19 mm) at 12 inches (300 mm) on-center.

Two-way slabs range from 7 inches (175 mm) thick with No. 4 (12.7-mm-diameter) rebar at 36 inches (900 mm) on-center up to 10-1/2 inches (265 mm) thick with No. 4 (12.7-mm-diameter) rebar at 24 inches (600 mm) on-center and No. 5 (15.9-mm-diameter) rebar at 12 inches (300 mm) on-center.

v) Slabs-on-grade. In general, it is not practical to attack slabs-on-grade. Slabs-on-grade are used for floors only. The thickness may be as low as 4 inches (100 mm) to as high as 12 inches (300 mm). The corresponding reinforcement may be as low as a single layer of No. 3 (9.5-mm-diameter) rebar at 12 inches (300 mm) on-center each way to as high as No. 7 (22-mm-diameter) rebar at 6 inches (150 mm) on-center each way and on each face, or perhaps wire mesh. Concrete with compressive strengths between 3,000 and 6,000 psi (21 and 42 MPa) are typically used.

b) Penetration times for existing construction. Table 42 sumarizes the maximum penetration times for existing concrete construction of roofs and floors. Estimated penetration times for both upward and downward attacks on representative major conventional construction types can be estimated using Figure 33 and Table 22, and Figure 35 and Table 23. A review of the data in Figures 33 and 34 shows that a wide range of penetration times are possible, depending primarily upon the thickness and type of slab, size and spacing of the reinforcement, and the direction of the attack (typical ceiling, roof, and floor covering materials contribute very little to penetration times). The lower bound is less than 2 minutes for very thin, nominally reinforced slabs to more than 60 minutes for very thick slabs [12 inches (300 mm)] with heavy reinforcements. For a downward attack on roof or floor slabs made of up to 12-inch (300-mm)-thick reinforced slab, Figure 33 and Table 22 can be used to estimate penetration times for various thickness and rebar combinations. For an upward attack on floors of various thickness, the conventional concrete family of curves, shown on Figure 35 and cross-referenced to Table 23 can be used. For floors, an upward attack is more difficult and requires a different combination of tools than a downward attack on the same cross section. The result is increased penetration times for the same cross section. The difference is typically 5 to 10 minutes. For upward attacks on floor slabs less than 11 inches (275 mm) thick, the primary factor influencing penetration time is the thickness of the slab. Beyond 11 inches (275 mm), the type, size, and spacing of reinforcing also becomes important. This is shown in Figure 35 for slabs up to 12 inches (300 mm) thick reinforced with rebar. For floors reinforced with mesh rather than rebar (used Curve B in Figures 33 or 35), the mesh spacing or size of wire mesh has a small effect on penetration times. In general, reinforced concrete roofs and floors

provide higher penetration times than those constructed of wood or metal at roughly comparable costs.

Table 42
Existing Roof/Floor Concrete Construction

Building Component (b)	Maximum Penetration Times (minutes) Achievable		
	Low	Medium	High
Concrete Roofs	(a)	7.5	35
Concrete Floors • Downward attack • Upward attack	 (a) (a)	 7.5 (2)	 35 45

(a) It is not practical for threats to attack roofs or floors at this severity level.
(b) As described in what follows, characteristics of construction affect penetration for a given threat level.

c) Retrofit options for medium-severity threats. Figure 33 shows that reinforced concrete 6 inches (150 mm) thick with the "B" rebar option from Table 22 provides minimum penetration times up to about 7.5 minutes for medium-severity threat levels with downward attacks on roofs or floors. If more time delay is required, about 14 additional minutes can be gained by affixing a 9-gauge (3.8-mm) flattened expanded steel grate to the interior of the roof or floor.

d) Retrofit options for high-severity threats. If the required delay time is greater than that achievable by the existing construction, the penetration delay time can be doubled from the values shown in Figure 33 or Figure 35 by fixing 10-gauge (3.4-mm) sheet steel (ASTM A589) to the interior surface using lag screws or bolts. If this is still not adaquate, the steel-ply options summarized in Table 38 and Figures 46 through 48 or the riveted or welded grading shown in Figure 49 can be used. See par. 5.6.3.3(1)(d) for details.

2) Wood Ceilings/Roofs and Floors

a) Representative existing construction. Typical construction for wood roofs and floors includes:

- Wood or plywood on joists.
- Stressed skin plywood on joists.
- Wood deck on beams.

Plywood on joists may include thicknesses from 14 to 1-1/8 inches (6 to 28 mm). The plywood is supported on joists ranging from 2 by 4 inches (50 by 100 mm) up to 2 by 14 inches (50 by 350 mm) on 12-, 16-, or 24-inch (300-, 400- or 600-mm) centers. The stressed skin plywood panels are typically 1/2- to 1-inch (13- to 25-mm) plywood supported on joists of 2- by 4-inch to 2- by 14-inch (50- by 100-mm to 50- by 350-mm) on 12-, 16- or 24-inch (300-, 400- or 600-mm) centers. The ceiling joists are then covered by 3/8-inch (9-mm) plywood. The wood deck-on-beams option consists of 1-, 1-1/8-, or 1-1/4-inch (25-, 28-, or 32-mm) plywood or 2- by 6-inch (50- by 150-mm) wood decking supported on sawn or glue-laminated wood beams on 4- or 8-foot (1,200- or 2,400-mm) centers. Regardless of the degree of security, the choice of wood construction must be in accordance with the fire protection requirements set forth in MIL-HDBK-1008.

Table 43
Existing Roof/Floor Wood Construction

Building Component	Maximumm Penetration Times (minutes) Achievable		
	Low	Medium	High
Wood Roofs	(a)	1.6	1.5
Wood Floors	(a)	1.6	1.5

(a) It is not practical for low-level threats to attack roofs or floors.

b) Penetration times for existing construction. Penetration times for conventional wood roof and floor construction options against optimal combinations of hand and power tools are 1.6 minutes against the medium-level threat and less than 15 minutes against the high-level threat (see Table 43).

c) Retrofit options for medium-level threats. Very little test data is available on retrofit options for hardening against medium-level threats using hand-held and limited battery-powered tools only. Table 40 shows delay times achieved using 9-gauge (3.8-mm) metal fence material, 1/4-inch (19-mm) to 3/4-inch plywood, 9-pound (4.1-kg) expanded metal, and 3/16-inch (4.8-mm) steel plate.

d) Retrofit options for high-severity threats. The steel-ply retrofit options shown in Figures 46 through 48 and Table 38 or the riveted or welded steel grating shown in Figures 49 and 50 can be affixed to

the interior of the roof or floor to increase the effective delay time. See par. 5.6.3.2(1)(d) for additional information.

3) Metal Roofs and Floors

a) Representative existing construction. Typical metal roof construction consists of three types:

- Steel-plate decking
- Ribbed-steel decking
- Corrugated-metal decking

Typical metal floor construction consists of four types:

- Steel-plate decking
- Riveted-steel grate
- Welded-steel grate
- Expanded-steel grate

i) Steel-plate decking. Steel-plate decking typically ranges from a minimum thickness of 1/4 inch (6 mm) to a maximum of 1 inch (25 mm).

ii) Ribbed-steel decking. This decking consists of long, narrow sections with longitudinal ribs from 1-1/2 to 2 inches (38 to 50 mm) deep, spaced 6 inches (150 mm) center-to-center. Special long-span roof-deck sections may also be used. Common gauges used are No. 22, 20, and 18 (0.8, 0.9, and 1.2 mm), while the deep long-span sections are of heavier gauges, ranging from No. 18 to 12 (1.2 to 2.7 mm).

iii) Corrugated-metal decking. This decking is typically made of aluminum, galvanized iron, or protected (rust-inhibited) metal. Corrugated aluminum may be either corrugated sheets, curved corrugated sheets, V-beam sheets, or concealed clip panels. The corrugated sheets and curved corrugated sheets are typically 0.024 or 0.032 inch (0.6 or 0.8 mm) thick with 2.67-inch (68-mm) corrugations 7/8 inch (22 mm) deep. The V-beam sheet has a 4-7/8-inch (120-mm) pitch with 1-3/4-inch (45-mm) deep corrugations with top and bottom flats of 3/4 inch (19 mm). Thicknesses are 0.032, 0.040, or 0.050 inch (0.8, 1.0, or 1.3 mm). Concealed clip panels are 13.35 inches (340 mm) wide by 3 feet (900 mm) up to 39 feet (12 m) long with thicknesses of 0.032, 0.040, or 0.050 inch (0.8, 1.0, or 1.3 mm).

Protected metal is available in corrugated sheets, mansard sheets, or V-beam sheets. The corrugated sheets have 2.7-inch (69-mm) corrugations 9/16 inch (14 mm) deep. Mansard sheets have 6 beads per sheet. The V-beam sheet has a 5.4-inch (135-mm) pitch with 1-5/8-inch (40-mm)-deep corrugations and contains five Vees per sheet. The thickness of all protected metal sheeting ranges from 18 to 24 gauge (1.2 to 0.6 mm).

iv) Riveted-steel grate. Riveted steel grate has a minimum bearing bar size of 3/4 by 1/8 inch (19 by 3 mm) spaced 2-5/16 inches (60 mm) on center and a maximum bearing-bar size of 2-1/2 by 3/16-inches (63 by 5 mm) spaced 3/4 inch (19 mm) on-center. The spacer bars are riveted about 7 inches (175 mm) on-center for average installations or 3-1/2 to 4 inches (90 to 100 mm) for heavy traffic, or where wheeled equipment is used.

v) Welded-steel grate. Welded-steel grate has minimum and maximum bearing-bar sizes of 3/4 by 1/8 inch (19 by 3 mm) and 2-1/2 by 3/16 inches (63 by 5 mm), respectively. The minimum spacing is 15/16 inch (24 mm) on-center, and the maximum spacing is 1-3/16 inch (30 mm) on-center. Spacer bars are typically welded either 2 or 4 inches (50 or 100 mm) on-center.

vi) Expanded-steel grate. The expanded-steel grate has a minimum diamond size of 1.33 by 5.03 inches (35 by 125 mm) and a maximum diamond size of 1.41 by 5.33 inches (36 by 135 mm).

b) Penetration times for existing construction. Table 44 provides the penetration times for existing metal roof and floor construction. In most cases, low- and medium-level threats are not practical against this type of construction. Metal roofs provide only about 1.5 to 2 minutes of delay against medium- to low-level forced-entry threats. In floors, riveted or welded expanded or steel grates provide less than 1 minute of delay against a high-level attack.

c) Low- and medium-severity threats. With the exception of ribbed steel, corrugated metal, and expanded steel grate, it is not practical for a low- or medium-severity threat to attack metal roofs or floors (see Table 44). The existing construction should be adequate. For the above-listed exceptions, riveted, or welded steel grate can be afixed to the underside to enhance the hardness.

d) Retrofit options for high-severity threats. The steel-ply retrofit options shown in Figures 46 through 48 and Table 38, or the riveted or welded steel grating shown in Figure 49 can be affixed to the interior of the roof or underside of the roof or floor to increase the effective delay time. See par. 5.6.3.3(1)(d) for additional information.

5.6.5 Door Retrofit Construction

5.6.5.1 Personnel, Vehicle, and Vault Doors. Where existing personnel, vehicle, and vault doors do not provide adequate penetration delay, it may be possible to replace the existing doors with new ones meeting the desired delay requirements. Refer to par. 5.5.5 for personnel, vehicle, and vault door options and details. Where the existing construction will not support the

door change-out, upgrade of the existing door may be possible. The upgrade should follow the requirements of par. 5.5.5.

Table 44
Maximum Penetration Times (Minutes) by Threat Security Levels, Existing Metal Roofs and Floors

Building Component		Maximumm Penetration Times (min) By Threat Severity Level		
		Low	Medium	High
Roofs	Steel plate 1/4 inch (6.25 mm) to 1 inch (25 mm)	(a)	(a)	1 to 2
	Ribbed Steel 18 to 12 gauge (1.2 mm to 2.7 mm)	2	1.5	<1
	Corrugated Metal 18 gauge (1.2 mm)	2	1.5	<1
Floors	Steel Plate 1/4 inch (6.25 mm) to 1 inch (25 mm)	(a)	(a)	1 to 2
	Riveted Steel Grate	(a)	(a)	<1
	Welded Steel Grate	(a)	(a)	<1
	Expanded Steel Grate	1	1	1

(a) It is not practical for these level threats to attack roofs or floors.

5.6.5.2 Magazine Doors

1) Typical Existing Door Construction. For magazine doors, Table 16 shows examples of typical door panel construction required by DOD 5154.4 to achieve explosive safety in the storage of Risk Categories I through IV ammunition and explosives (see Table 15 for a description of risk categories.) At present, the shrouded shackle padlock shown in Figure 40, together with the shrouded hasp shown in Figure 41, is to be used with these doors. Note in Table 31 that although the door panel is capable of providing a penetration delay time of 4 minutes, the lock/hasp provides less than 1 minute's delay against a high-severity threat.

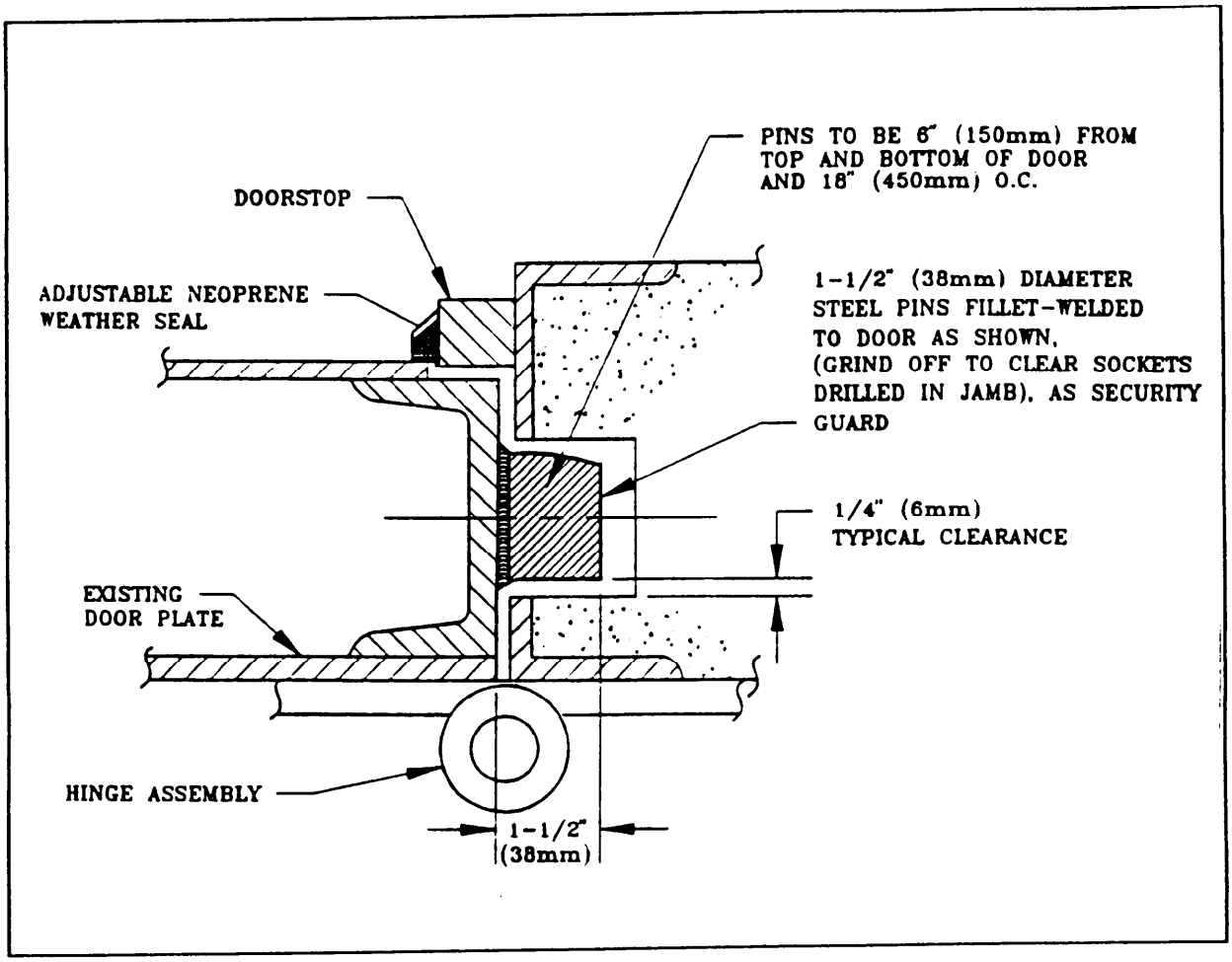


Figure 52
Hinge Side Protection Plan for Using a Pin-In-Socket Technique

2) Hinge-Side Protection. The standard door designs used in existing magazine structures for AA&E storage are, in most cases, vulnerable to physical attack on the hinge side of the door. Attacks consist of cutting the hinge mounting bolts, cutting and driving out the hinge pintle pin, or cutting the hinge assembly. A positive door-to-jamb interlock is, therefore, required. Figures 52 through 55 show the cross sections of hinged doors and door frames. Various options of passive hardware for positive interlocking at the hinge edge are shown that are designed to prevent entry by physical attack at the hinge edge. This approach prevents the hinged edge from being pushed in or pulled out when the door is closed and locked. The design options shown have the advantage of not producing a safety hazard by extending the interlocking hardware into the clear opening of the door.

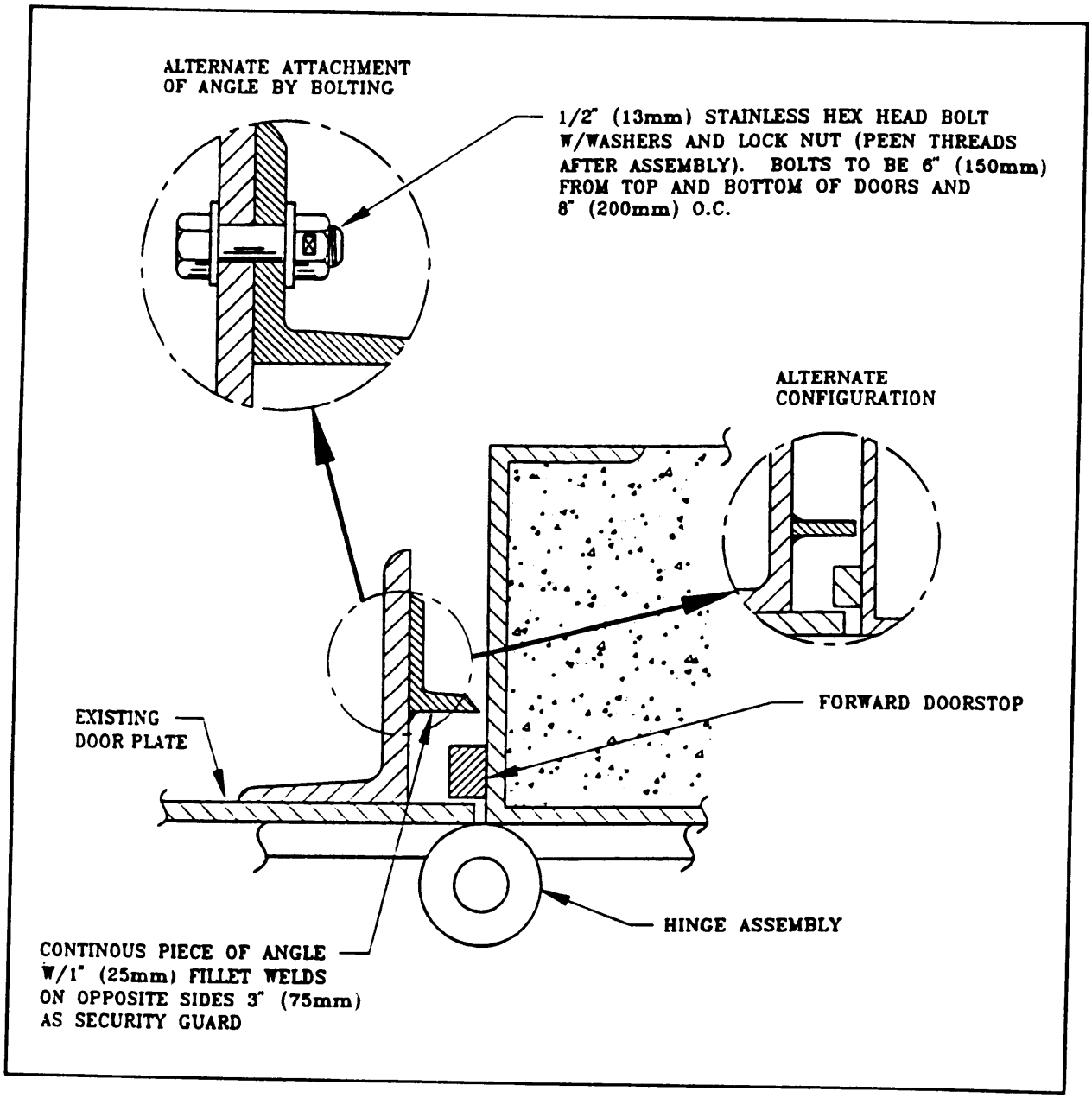


Figure 53
Hinge Side Protection for Doors Using a Forward Doorstop with Angle

5.6.6 Window Retrofit Construction. It may be possible to replace existing windows with new windows; see par. 5.5.6 for window design options. As an alternative, elimination of 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 or building section being sealed.

5.6.7 Utility Opening Retrofit Construction

5.6.7.1 Overview. In conventional building designs, utility openings, manholes, tunnels, air conditioning ducts, filters, and equipment access panels can provide intruders with an attractive entrance or exit route with no significant delay. Either such openings must be eliminated or delay times increased significantly, if consistent physical security integrity of the overall structure is to be provided. The following paragraphs provide a brief description of typical utility openings and the factors and issues that require special consideration in determining and enhancing delay times.

5.6.7.2 Hardening Utility Openings for Conventional Buildings. Methods for hardening utility openings greater than 96 square inches (0.06 sq m) are described in par. 5.5.6 under New Construction. These openings include electrical system conduits, mechanical system conduits for air conditioning, heating, and venting systems, roof-mounted equipment, filter banks, and manholes.

5.6.7.3 AA&E Ventilation Openings

1) Overview. Door, wall, or roof ventilators in an earth-covered arms, ammunition, and explosives (AA&E) storage magazine often provide the best means of penetrating the structure. Any AA&E ventilator that is 96 square inches (0.06 sq m) or larger must, therefore, be secured against high-severity level attacks.

2) Door Ventilators. Most magazine door ventilators are shrouded, shrouded and louvered, or simply louvered. These openings can be quickly and easily penetrated because of inherent weaknesses in the external mounting, quality of the mounting, or because, in some cases, the steel of the ventilator is considerably lighter than the door. All external shrouds should be mounted with a continuous bead-weld along all edges. Many door ventilators can be reinforced on the inside with riveted steel grating, MIL-G-18014 Type A, Class B, as shown in Figure 56. Where design of the door permits, this cover should be welded flush with the inside of the door. If door stiffeners and ventilator frames do not permit flush mounting, this cover should be offset mounted, using 1/4-inch (6-mm) flat bar or angle steel at the minimum possible offset. An alternative to the welding of this grate to the door is to mount it with 1/2-inch (13-mm) steel bolts and a 1/4-inch (6-mm) flat bar in the manner shown in Figure 57, with the ends of the grating extending 6 inches (150 mm) beyond the opening and the bolts and nuts welded to prevent removal.

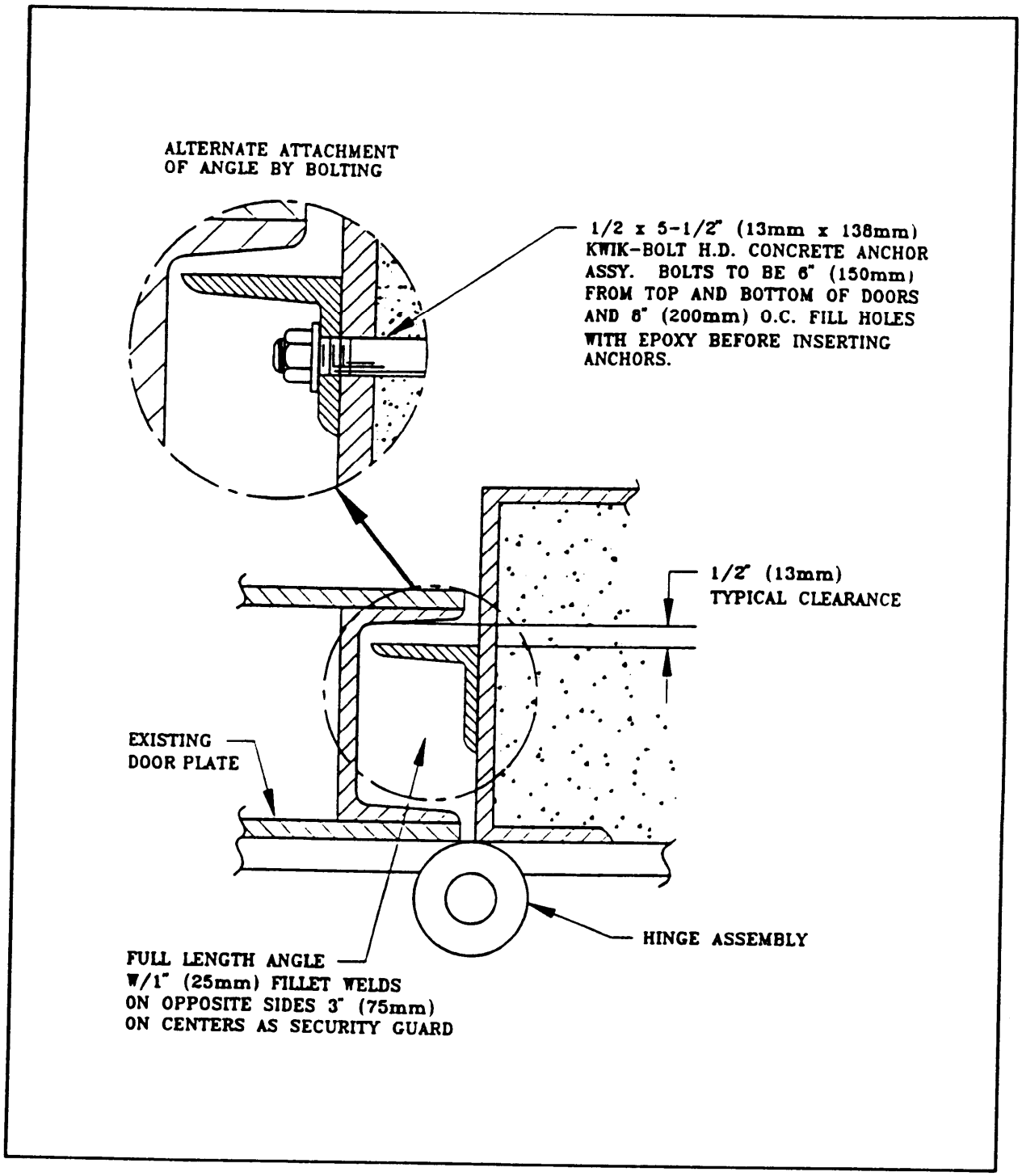


Figure 54
Hinge Side Protection for Hardening Typical Thick Doors by Using an Angle Stop

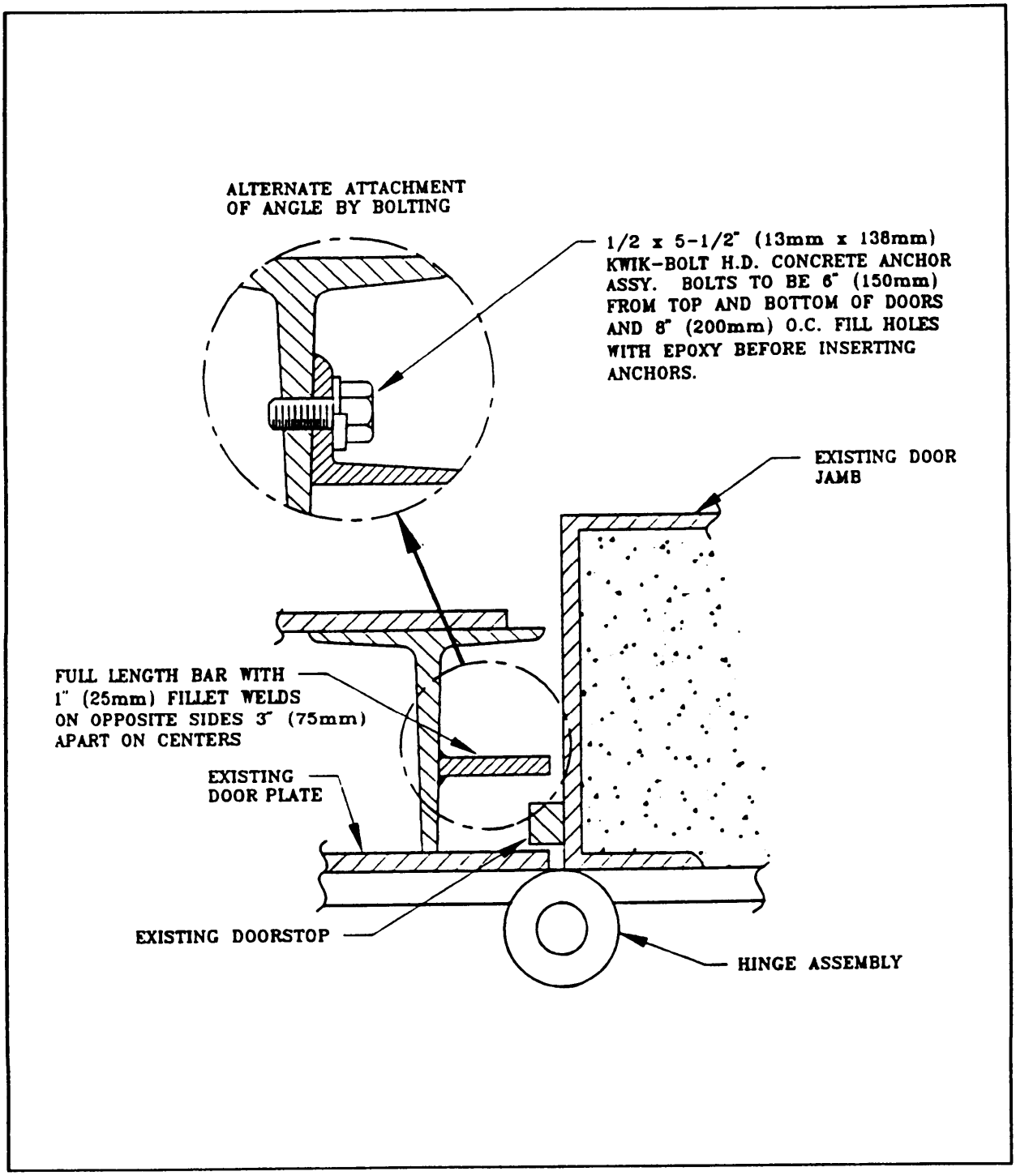
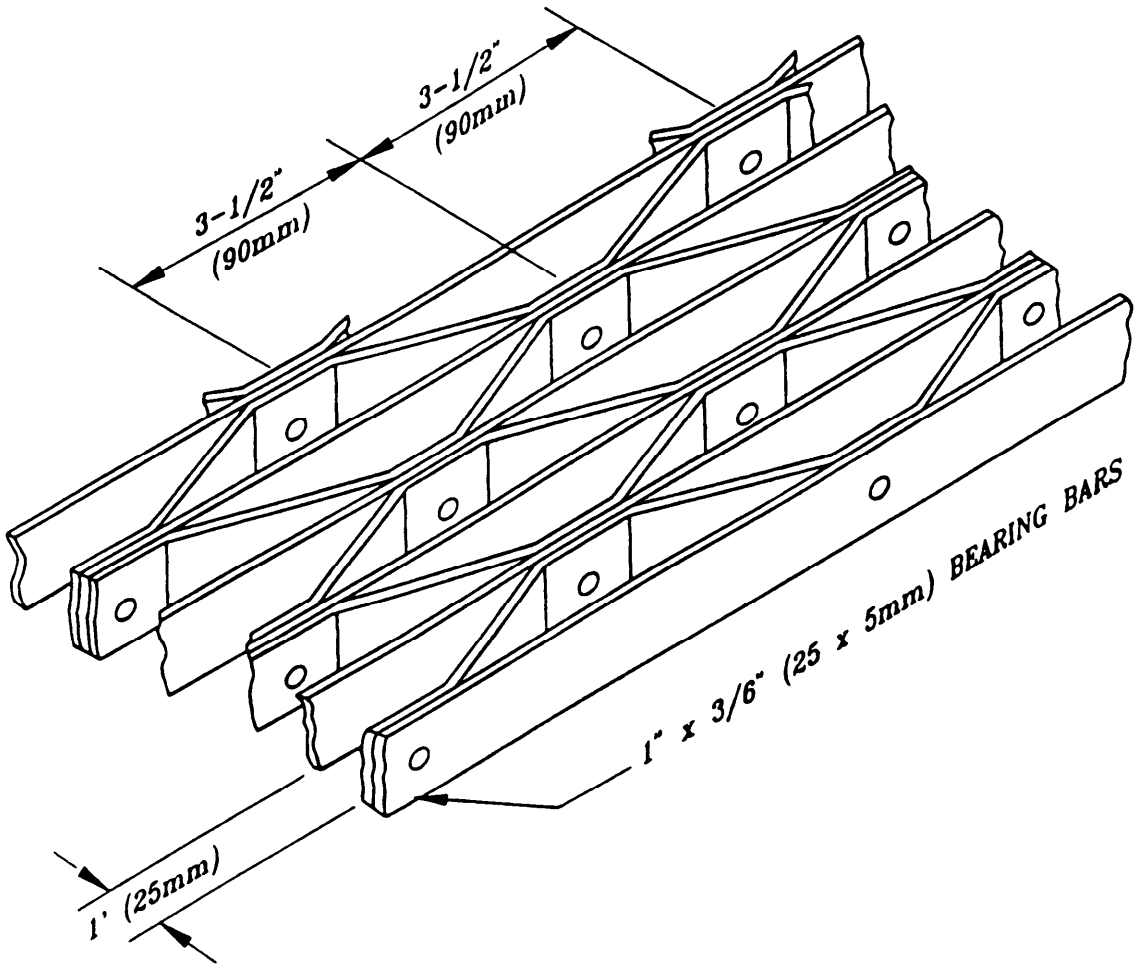


Figure 55
Hinge Side Protection for Hardening Typical Thick Doors by Using an Angle Stop



NOTE: Penetration times of 4.0 minutes against a medium threat and 1.5 minutes against a high severity threat

Figure 56
Riveted Steel Grating

3) Wall Ventilators. All wall ventilators should be externally shrouded using, as a minimum, 3/8-inch (9-mm) steel plate (see Figure 58). The shroud should extend well below the bottom edge of the ventilator, and the minimum possible distance should be between the wall face and the shroud plate. It should be noted, however, that a solid steel plate placed in front of the ventilator will restrict the air flow because of the blockage in front of the open area. Compensation for this air flow reduction should be made. The security engineer should determine whether the distance between the wall face and the shroud plate and the shroud attachment mechanism permits the required air flow. Internally, a cost-effective method of increasing resistance is to use riveted steel grating, MIL-G-18014, Type A, Class B, cut with a minimum 6-inch (150-mm) overlap on all sides of the ventilator opening. Two installation techniques are shown in Figure 58. One technique requires welding the steel grating to an existing steel frame surrounding the vent. The other technique requires no welding. Flat steel bars, 1/4 by 2 inches (6 by 50 mm), drilled to accept 1/2-inch (13-mm) expansion fasteners, should be used to hold the grating to the wall. Any concrete anchor meeting the requirements of ASTM or military specifications may be used. To ensure maximum pullout strength, the holes must be drilled carefully to ensure tight fit of the fastener. The fastener must not be installed closer than 4 inches (100 mm) to the edge of the concrete. The bolt should be welded to the frame.

4) Roof Ventilators. Roof ventilators in older magazines may open directly into the magazine ceiling or may open high on the rear of the magazine wall. These ventilators should be protected through the internally mounted vent covers. The light sheet metal and ceramic tile construction of the older magazine vents precludes reinforcing the roof ventilators at any point other than the inside opening. In concrete arch magazines, use of riveted steel grating mounted as shown in Figure 59, similar to the technique used for wall ventilators, can be used for enhanced penetration resistance.

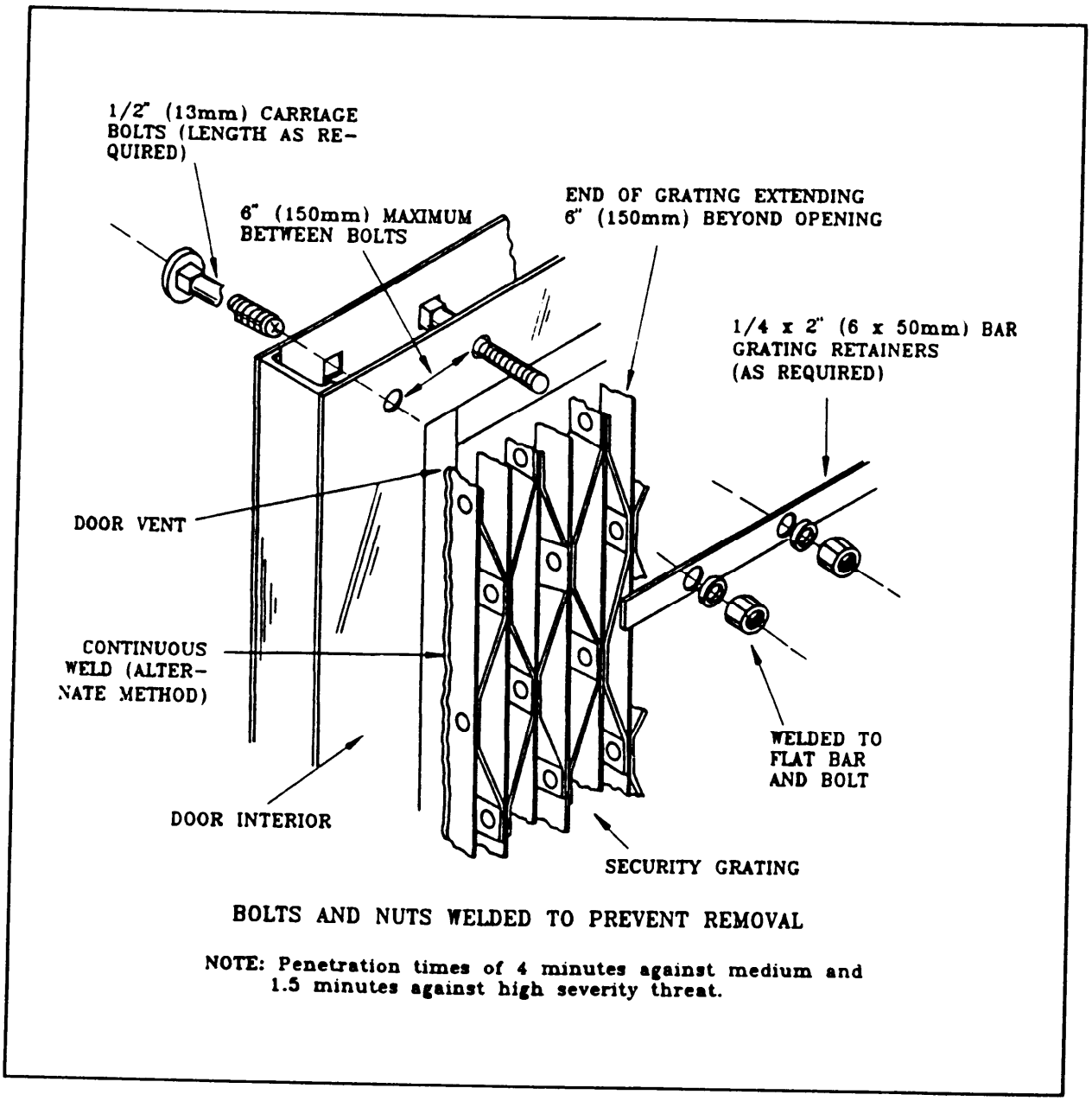


Figure 57
Security Intrusion Protection Plan for Hardening a Typical Door Ventilator

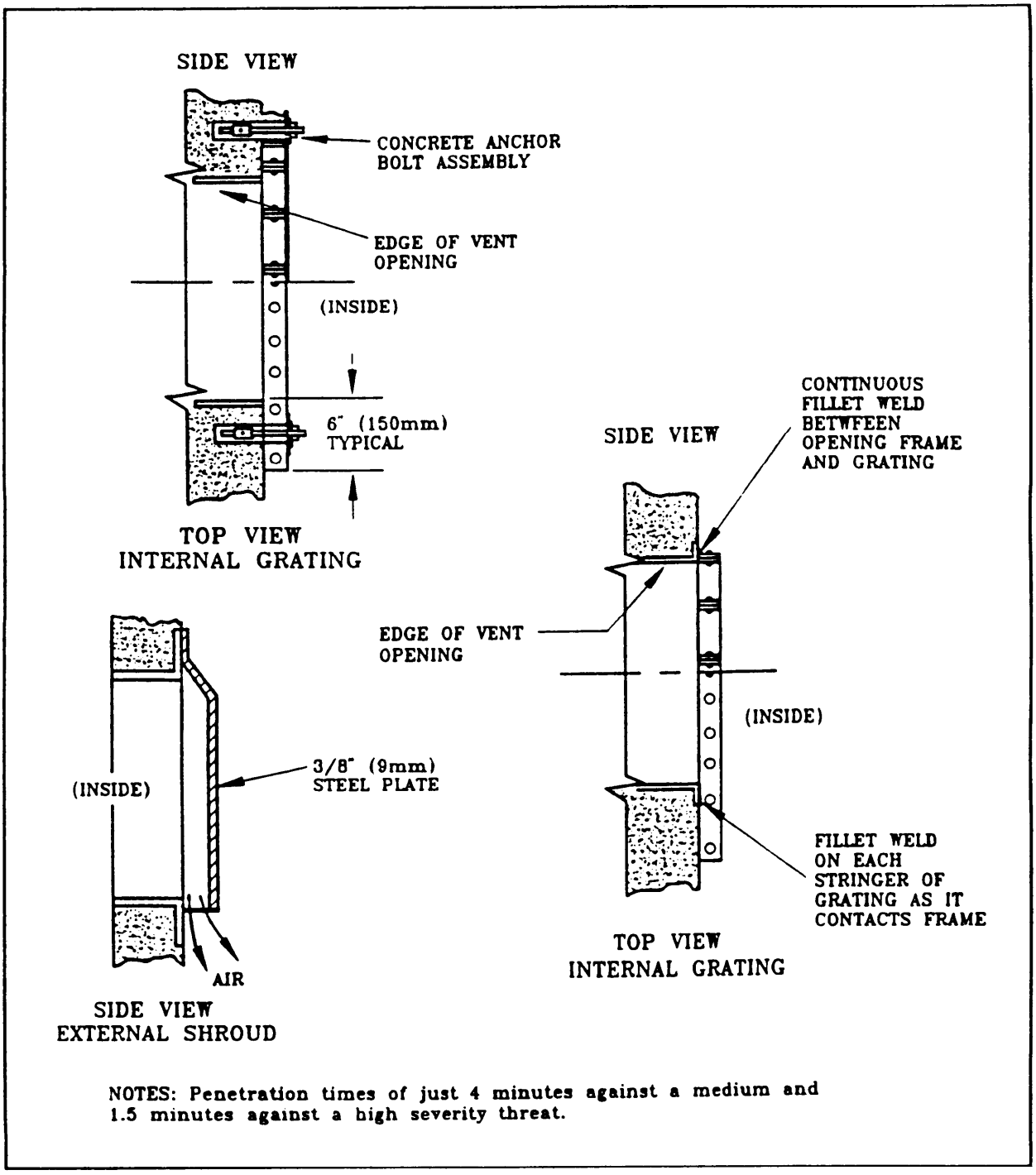
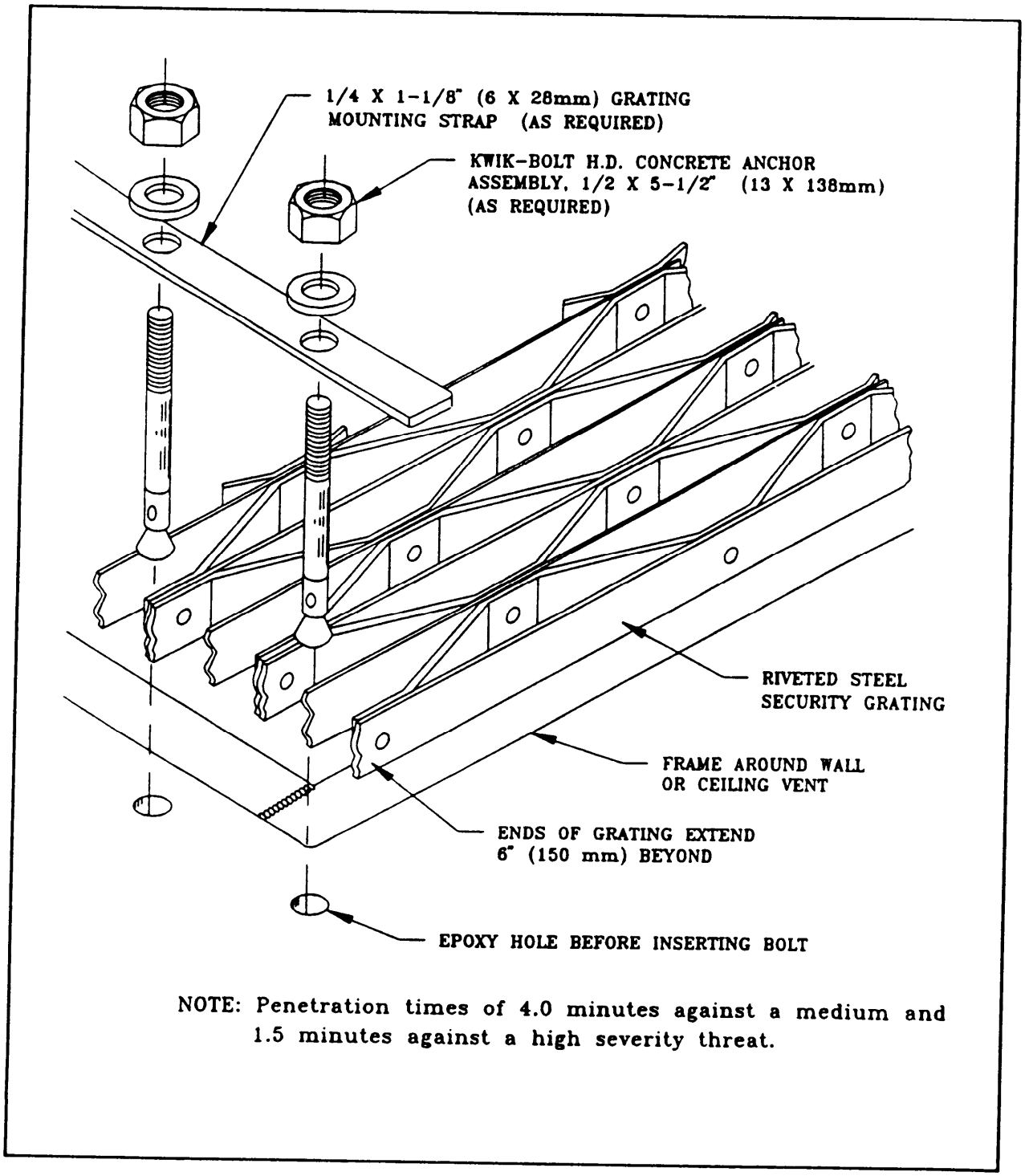


Figure 58
Installation Details of Hardening a Typical Riveted Steel Grating and Shrouded Louver for Walls or Ceilings



NOTE: Penetration times of 4.0 minutes against a medium and 1.5 minutes against a high severity threat.

Figure 59
Security Intrusion Protection Plan for Hardening a Typical Wall or Ceiling

) Surface and Drainage: Track surfaces may be asphalt, concrete

Section 6: BALLISTIC ATTACK HARDENING

6.1 Introduction. This section provides a summary of the available information on the ballistic resistance of commercial construction, structural barriers, doors, and glazing materials against small arms and military threats, i.e., the ballistic attack. In a ballistic attack, the aggressor fires various small arms such as pistols, rifles, submachine guns, and shotguns from a distance determined by the range of the firearm and accessibility to the asset. A ballistic attack requires line-of-sight access to the asset being attacked, at as close a range as practicable. Firearms, which may be civilian or military, are described in terms of ballistic standards developed for testing the resistance of building components to the weapons' effects. These standards generally specify weapons, ammunition, muzzle velocity of the round, and number of rounds fired at the target.

6.2 Ballistic Threat Characteristics. The ballistic threat posed by a bullet depends on its caliber, type, shape and weight, impact velocity, angle of impact, muzzle energy, multiple versus single impact, and target range. The most probable threat is from pistol, rifle, submachine gun, or machine gun fire. Coverage of the ballistic threat in this handbook is limited to bullets or projectiles fired from small arms; the penetration mechanics of these bullets or projectiles, and the architectural application of ballistic-resistant materials or armor. The term "ballistic-resistant" refers to protection against complete penetration, passage of projectile fragments, or spallation (fragmentation) of the protective material to the degree that injury would be caused to an asset or a person standing directly behind the ballistic barrier.

6.2.1 Caliber. The caliber of a bullet refers to its diameter and is expressed either in decimals of an inch or in millimeters. Typical examples include the 0.303-caliber high-power rifle and 7.62-mm NATO rifles.

6.2.2 Bullet Characteristics. Bullets vary in their characteristics.

6.2.2.1 Armor-Piercing (AP). A bullet having a hardened metal core, a soft metal envelope, and a bullet jacket. When the AP bullet strikes armor, the envelope and jacket are stopped, but the armor-piercing core continues forward to penetrate the armor. The AP bullet is characterized by high accuracy in flight and high velocity.

6.2.2.2 Ball. A non-armor-piercing bullet having a lead or mild steel core.

6.2.2.3 Other Characteristics. The different bullet designs are spire point, round nose, flat point, full metal jacket, boat-tail hollow-point, short jacket, cast bullet, and wadcutter. Ballistic performance of a material is sensitive to a projectile's shape and construction, e.g., whether or not the bullet is jacketed, the length, thickness, and hardness of the jacketed material, the presence of a hollow nose, a cavity and hollow base, and the hardness of the lead.

An ogive-shaped projectile would be expected to initiate fracture of the target. By comparison, a flat-nosed projectile would favor "plugging" of the target around the projectile as it advances into the target medium. A lighter bullet will slow down more readily while a heavier bullet will penetrate further into the target. An AP-type bullet has a greater capacity to penetrate than the ball type because the AP bullet has a hardened steel core that resists deformation upon impact.

6.2.3 Ballistic Limit. The ballistic limit of a material is an approximation of the velocity at which 50 percent of the impacts would result in complete penetrations and 50 percent in partial penetrations. Ballistic limit generally is expressed as V sub 50. In evaluating the V sub 50 ballistic limit, it is necessary for the definition of penetration to be specific. Currently, there are three criteria of penetration or ballistic limits: the Navy, the Army, and Protection Ballistic Limit (PBL), illustrated in Figure 60. The PBL has received greater recognition since it defines the limiting velocity at which damage occurs beyond the armor. As the striking velocity is increased from a very low velocity to the ballistic limit of the material, theoretically no complete penetration will occur at least 50 percent of the time. When the impacting or striking velocity is in excess of the ballistic limit, the projectile will pass through the armor with a residual velocity at least 50 percent of the time. When the striking velocity coincides with the ballistic limit, maximum energy is extracted from the projectile by the armor.

6.2.4 Oblique Attack Affects. Armor resistance to penetration is not only affected by the angle at which a plate is mounted but also by the angle at which the projectile strikes the target. The greater the obliquity, the greater the thickness of armor the projectile must travel through to perforate it. Figure 61 illustrates the increasing thicknesses a projectile must travel through at varying obliquities for armors of specific thicknesses.

6.2.5 Projectile Energy. A projectile in motion is stopped when its kinetic energy is dissipated on impact with the armor. The kinetic energy of the projectile is resisted by an impulse equal and opposite to that of the projectile at impact. The rate of projectile energy loss increases as the surface area of the projectile in contact with the armor increases. The application of the kinetic energy of the projectile over the smallest cross-sectional area possible will result in less projectile energy loss. If the armor is rigid and very hard, a portion of the projectile's kinetic energy will be diffused in fragments produced by shattering of the impacting projectiles, and the kinetic energies of these fragments may be enough in themselves to cause damage.

6.2.6 Multiple Impacts. The effect of multiple hits on armor depends on the dispersion of the points of impact and the degree to which the armor is reinforced to offer resistance to later shots. A small area of dispersion such that successive hits fall within the crater of the first projectile is advantageous for the attack and promotes projectile penetration.

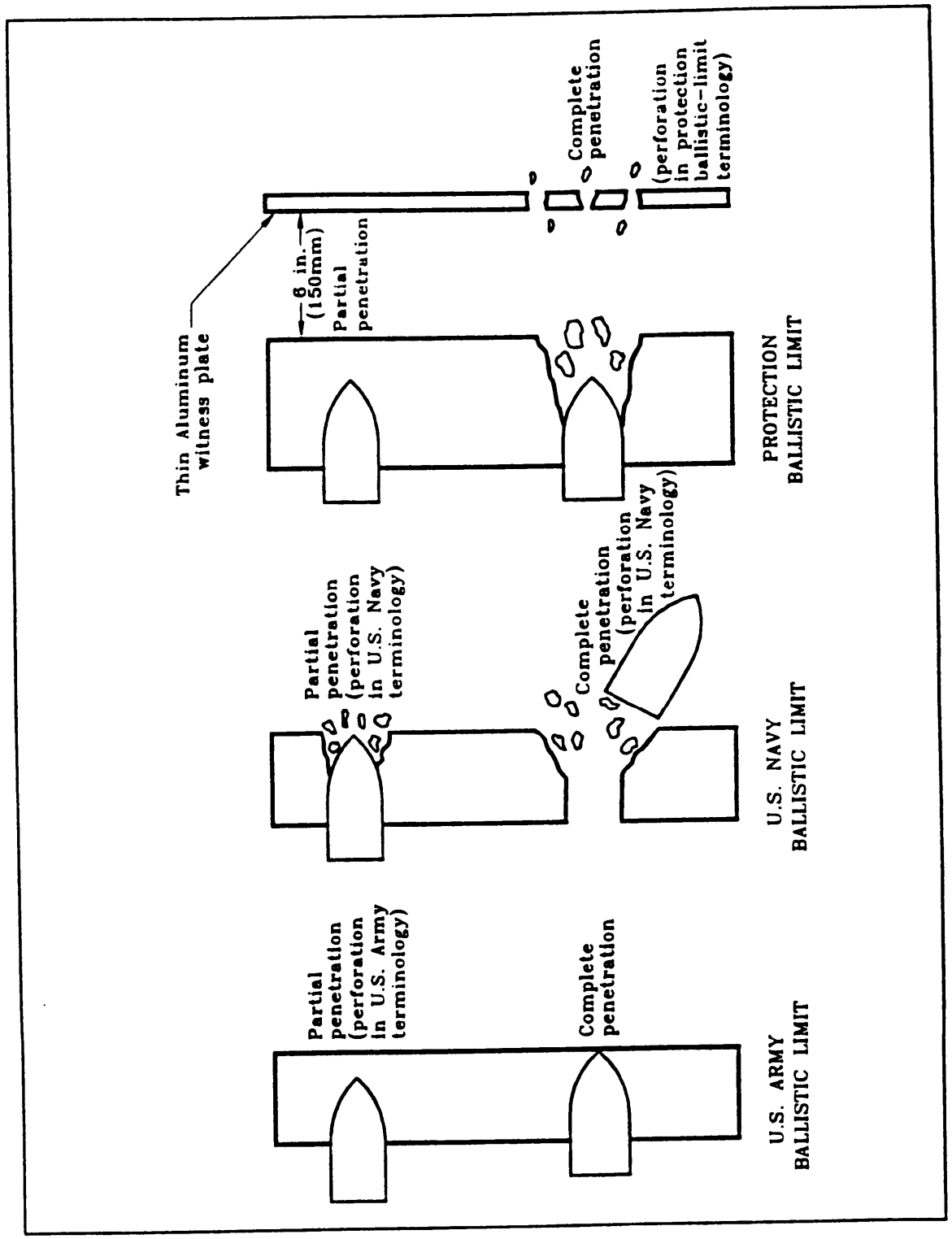


Figure 60
Ballistic Limit Criteria

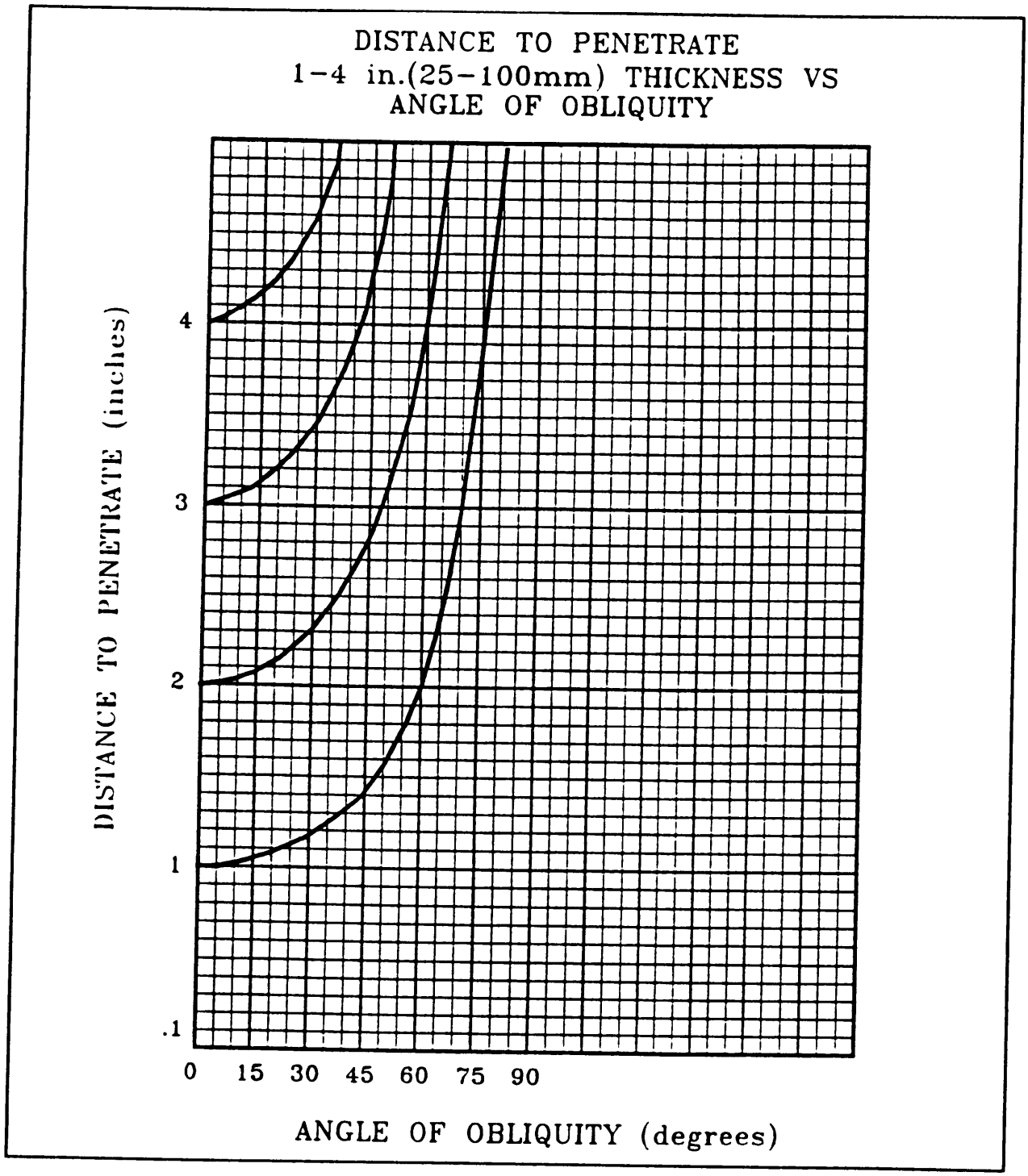


Figure 61
Distance to Penetrate 1 to 4 Inches (25 to 100 mm) Versus Angle of Obliquity

6.3 Ballistic Threats. Four ballistic threat levels are used in this handbook, reflecting their severity level: (1) low, (2) medium, (3) high, and (4) very high. These threats are summarized in Table 45.

6.3.1 Low-Severity Threat. The low-severity threat is the American National Standards Institute (ANSI)/Underwriters Laboratories (UL) Medium-Power Small Arms (MPSA) threat described in ANSI/UL 752. This threat normally would be employed against facilities when the main objective of the attacker is to persuade someone to turn over items of high value such as cash or drugs. This threat also may be employed in a hostage situation.

6.3.2 Medium-Severity Threat. The medium-severity threat is the ANSI/UL Super Power Small Arms (SPSA) threat described in ANSI/UL 752. This threat normally would be employed when the attacker knows that ballistic-resistant glazing is installed, e.g., teller cages.

6.3.3 High-Severity Threat. The high-severity threats are described in the H.P White Laboratory, Inc., (HPW) HPW-TP-0501.00, Ballistic Resistance of Structural Materials (Opaque and Transparent), Test Procedures and Acceptance Criteria.

6.3.4 Very High-Severity Threat. The very high-severity threat is the Military Small Arms Multiple Impact Threat (MIL-SAMIT) described in Naval Civil Engineering Laboratory (NCEL) Report CR 80.025. This threat is defined as 25 rounds of 7.62-mm NATO ball ammunition fired from an M-60 machine gun at a range of 25 yards (22.9 m).

6.4 Overview of Ballistic-Resistant Materials and Defeat Mechanisms. Ballistic-resistant materials include various commercially available structural materials, special armor materials, and composites. These materials are used to improve the ballistic resistance of walls, roofs, ceilings, windows, and doors of structures to protect the contents and the occupants against ballistic attack. Ballistic-resistant materials are divided into two categories: (1) transparent armor, and (2) opaque armor. These are discussed below.

6.4.1 Ballistic Resistance. The term "ballistic resistance" denotes protection against complete penetration, passage of projectiles, or spallation of the protective material to the degree that injury would be caused to a person standing directly behind the bullet-resisting barrier. This definition is set forth in the ANSI/UL Standard for Bullet-Resisting Equipment, ANSI/UL 752. The ANSI/UL definition of bullet-resisting glazing material specifies that there should be no penetration of the projectile, fragments of the projectile, or fragments of the glazing assembly with sufficient force to embed into or damage 1/8-inch (3-mm)-thick corrugated cardboard indicators placed a distance of 18 inches (450 mm) behind the protected side of the test sample. This conforms to the protection ballistic limit described in par. 6.2.3.

Table 45
Firearm Ballistic Threats

Standard Threat Level	Caliber	Weapon	Bullet Weight (grains) & Type	Velocity Range ft/s (m/s)	Number of shots Resisted
LOW-Severity Threat Level					
UL-MPSA	.38 Super (9.6 mm)	Pistol Automatic 5-in. (12.7-mm) Barrel	130 FMJ	1152-1344 (350-410)	3
MEDIUM-Severity Level					
UL-SPSA	.44 Magnum (11.2 mm)	Handgun 6.5-inch (165-mm) Barrel	240 Lead	1323-1544 (403-471)	3
HIGH-Severity Level					
HPW Rifle Standard	7.62x51 mm NATO (M-14) (0.30 caliber)	Rifle	147 M-80 Ball	2700-2800 (823-853)	2 at Specified Locations
VERY HIGH-Severity Level					
MIL-SAMIT	7.62x51 mm NATO (0.30 caliber)	Light Machine gun, 25.5-in. (647 mm) Barrel M60E3 (US)	152 M-60 Ball	2800 (853)	25

ABBREVIATIONS:

AP - Armor Piercing
FMJ - Full Metal Jacketed
HPR - High-Power Rifle
MPSA - Medium-Power Small Arms
SPSA - Super-Power Small Arms
US - United States

BALLISTIC TESTING STANDARDS:

HPW - H.P. White Laboratory, Inc.; HPW-TP-0501.00, Ballistic Resistance of Structural Materials (Opaque and Transparent); Test Procedures and Acceptance Criteria, 1988.

MIL-SAMIT - Military Small Arms Multiple Impact Threat; performance standard developed by the Naval Civil Engineering Laboratory (NCEL).

SD - Department of State; SD-STD-02.01, Ballistic Resistance of Structural Materials (Opaque and Transparent); Test Procedures, 1986.

UL - American National Standards Institute/Underwriters Laboratories, Inc.; ANSI/UL 752-85, Rev. 13, Standard for Bullet Resisting Equipment, 1991, 8th edition with 30 Dec. 91 Rev.

6.4.2 Transparent Armor. Transparent armor is composed of materials with dual properties of being virtually transparent while having a resistance to penetration of small-arms projectiles and fragments. In general, transparent armors are laminate composites of glass and elastomers. Spallation has an important role in the impact process of transparent armors. A potential disadvantage of glass is breakup on projectile impact and the subsequent shattering and formation of sharp, needle-like splinters which can prove to be hazardous. Safety glass, which consists of two or more sheets of tempered glass bonded together by synthetic resin, produces cubical pieces on impact that usually have rounded edges. The energy absorbing mechanics of plastic materials offer an advantage over glass with regard to spallation. Plastics often can be designed not to shatter, and when combined with glass as a spall shield or a laminated glass/plastic configuration, can inhibit the shattering of the glass by containing the glass particles. The suppression of spallation is a powerful method of enhancing impact resistance of transparent armor. A laminated and bonded composite transparent armor consisting of safety glass and polycarbonate layers provides visual clarity and demonstrates resistance to small-arms projectiles.

6.4.3 Opaque Armor. Opaque armor is armor that obstructs transmission of light. Various types of opaque armor are described in the following paragraphs.

6.4.3.1 Common Structural Materials. Various tests have been performed on common structural building elements and concrete walls to determine their ballistic resistance to small-arms fire. Concrete masonry units, reinforced concrete, and steel/plywood wall systems have been ballistically tested against small-arms fire. Examples of these tests are covered later in this section.

6.4.3.2 Fibrous Materials. Fibrous armor is armor which incorporates the use of fibers or fabrics in a plastic matrix. The fibers work as an excellent reinforcing material for polymers. Three types of laminated fabrics include fiberglass, nylon, and Kevlar. Glass-fiber-reinforced-polymer (GRP) laminate consists of a number of laminations of woven rovings of glass fibers bonded with a polyester resin. Its performance at close range is limited mainly to protection against fragmentation. Test data indicate that a 2.5-inch (63.5-mm)-thick GRP can defeat a 0.30-caliber (7.62-mm) AP round at a range of 110 feet (34 m). Kevlar has a high tensile strength compared to nylon, but neither material is considered a satisfactory armor with regard to a 0.30-caliber (7.62-mm) projectile fired at 25 yards (22.9 m). Its principal attribute, as with laminated glass fibers, is to shield against scabbing and fragmentation by absorbing the low kinetic energy of the ballistic threat.

6.4.3.3 Ceramic Composite Materials. Ceramics encompass all inorganic materials except metals and metal alloys. Ceramic composite armor systems usually consist of aluminum oxide or boron carbide tile bonded to a rear panel, usually a GRP laminate, which acts as a shield against ceramic

fragmentation. Ceramic armors can provide ballistic protection at less weight per square foot, but high unit costs have limited their application.

6.4.3.4 Inorganic Nonmetallic Materials. Inorganic nonmetallic armor can range from sand, dirt, and gravel, to snow. Protection of small-arms fire offered by earth materials is available and effective, but costs of equipment and labor present a disadvantage. When gravel is placed in layers between two wooden panels, the impacting bullet usually shatters a piece of gravel in its path. Small gravel lacks the effectiveness of layer gravel or crushed rock since a bullet must be stopped by something comparable to its own mass. For equal thicknesses, the ballistic protection offered by wet sand is about one-half the protection of dry sand. No spalling and ricocheting occurs with snow as armor material. Snow must be packed to be effective, with loose or natural snow providing about one-half the protection of packed snow for resisting small-arms fire.

6.4.3.5 Metallic Materials. The majority of armor materials currently used are metallics. Metal armor falls into three general categories: (1) steel, (2) aluminum, and (3) titanium.

1) Steel Armor. Rolled homogeneous steel armor conforming to specification MIL-S-12560 has become the standard steel armor material, and is used for comparison when considering the ballistic performance of other armors. Homogeneous steel armor should be made as hard as possible for defeating small-arms AP ammunition. However, as steel becomes harder it also becomes more brittle and is more prone to severe fractures. This has formed the basic guidance for improved steel armor, that is, to increase steel armor's hardness without increasing its tendency toward brittle fracture.

2) Aluminum Armor. Aluminum alloys have been considered for potential armor application due to their low weight. Aluminum alloys have been designed for specific armor applications which were strengthened by strain hardening to increase their resistance to fragment penetration. However, as with metallic armor, high-strength aluminum alloys become more brittle as the strength level increases and improved protection against AP ammunition accompanies a reduction in resistance to fragmentation.

3) Titanium Armor. As with aluminum, titanium alloys offer excellent ballistic protection against fragment type ammunition while affording low weight compared to steel. Titanium armor, specified in MIL-T-46077(MR), shows ballistic superiority over the majority of fragmentation and small-arms threats.

6.5 Ballistic Hardening Option Recommendations. The determination of the category of security required against ballistic threats is discussed in Section 2. In general, the level of ballistic-resistant hardening required in a facility design depends upon the type of facility and the category of the threat.

6.5.1 Threat Severity Levels of Protection. Threat severity levels of protection range from low to very high. For the general case, the level of protection will correspond to the threat level described in par. 6.3.

6.5.2 Protection Measures; New Construction. Both siting and building elements or measures are used to negate the effects of the ballistic attack.

6.5.2.1 Siting Measures. Limit sightlines to the asset being protected. The ballistic attack, to be successful, must have uninterrupted line-of-sight visual access to the target. Protective measures are facility siting and obscuration.

1) Facility Siting. The initial site selection should consider the ballistic attack. Obviously, some sites are better than others with respect to conditions related to the ballistic attack. For example, site facilities on high ground to force attackers to shoot upward. Under this condition, targets inside the facility are more difficult to see and as a result, cause the bullets to strike building surfaces at an angle, decreasing their effectiveness. Site facilities away from either natural or manmade vantage points to limit an attacker's ability to see assets. Examples of potential vantage points include nearby structures or elevated land formations.

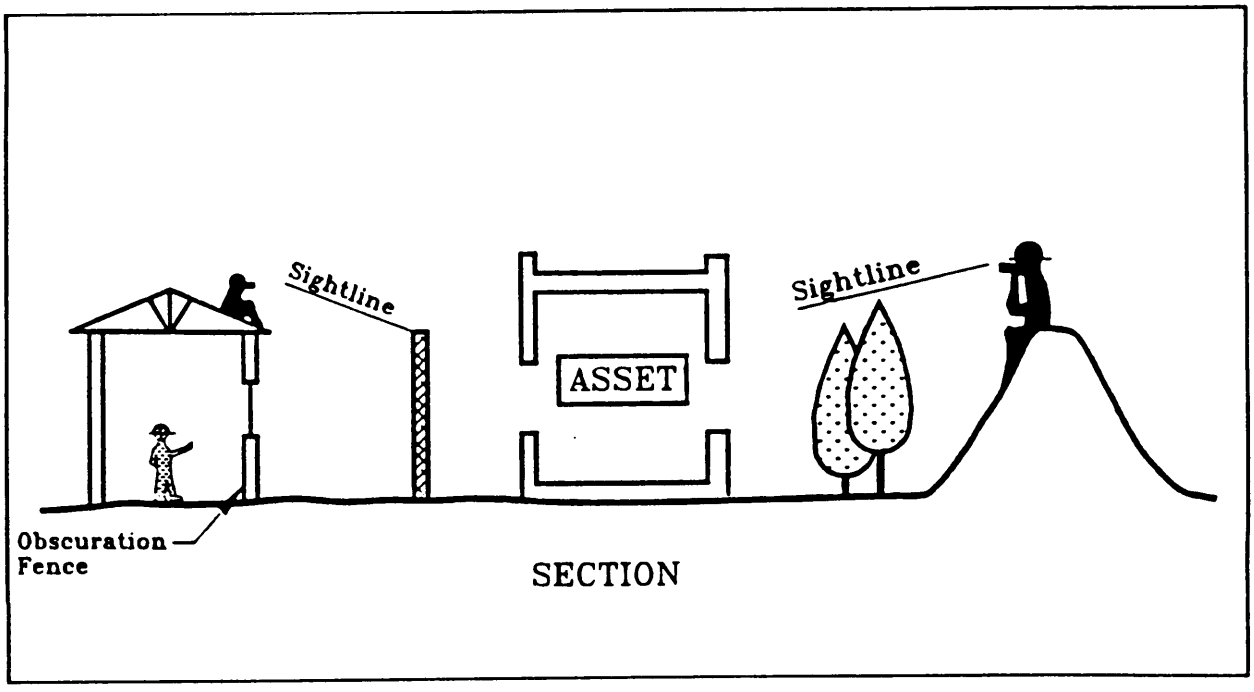


Figure 62
Sightlines Blocked From Potential Vantage Points

2) Obscuration. Block sightlines with landscaping features, obscuration fences, walls, or noncritical structures as illustrated in Figure 62. Consider blocking sightlines with other less critical facilities or earth berms. Obscuration fences include chain-link fences with slats woven through the fence fabric, and wooden fences with minimal spaces between planks. Many other types of fences also could be effective. However, the fence must be constructed and located such that an attacker cannot easily overcome the obscuration features of the fence. If trees are used as part of the landscaping, or if they already exist near the fence, locate them at a sufficient distance from the fence so that attackers cannot use them to scale over the fence.

6.5.2.2 Building Measures. Building elements include the building's layout and its walls, doors, windows, and utility openings. Since bullets are fired from line-of-sight weapons, they ordinarily pose no threat to roofs.

1) Layout. To reduce exposure to bullets, house critical assets at the center of the facility. If assets are effectively concealed, no other protective measures are needed to protect critical assets for the low level of protection. Locate bullet-resistant walls around assets, as shown in Figure 63, to eliminate sightlines through doorways. This arrangement allows conventional doors to be used while providing a complete hardened enclosure around the asset. Arrange entryways to eliminate sightlines.

2) Walls. Wall construction is dependent upon the threat severity. Representative examples of types of wall construction to defeat each threat severity level are described in the following paragraphs.

a) Low level of threat protection. There are no specific wall requirements for the low level of protection. Standard construction, selected for other reasons, applies. Table 46 shows a representative list of materials that could be used for the low-severity threat. Note that all of the materials shown are standard materials that would be appropriate for new construction. Any single material could be used. Or, if a combination of materials is used, such as 4-inch (101.6-mm) grouted CMU with 4-inch (101.6-mm) brick, increased ballistic resistance will result.

b) Medium level of threat protection. Table 46 shows representative wall materials for the medium level of threat. Note that the material thickness increases only slightly over the low-severity threat. Only a 1/2-inch (12.7-mm) increase in thickness is required for reinforced concrete and only an additional 1/16 inch (1.6 mm) is required for steel. Even the bullet-resistant fiberglass thickness only needs to be increased by 1/8 inch (3.2 mm) to defeat the medium level threat.

Chemical Officer, D-7

Table 46
Construction for Ballistic Resistance

Threat Severity	Wall Thickness, inches (millimeters)					
	Reinforced Concrete (3,000 psi) (21,000 kPa)	CMU, Normal Thickness (Grouted)	Brick	Steel Plate		Bullet-Resistant Fiberglass
				Mild	Armor	
Low	2 (50)	4 (100)	4 (100)	1/4 (6m)	3/16 (4.8mm)	5/16 (8)
Medium	2 1/2 (64)	4 (100)	4 (100)	5/16 (8m)	1/4 (6mm)	7/16 (14)
High	4 (100)	8 (200)	8 (200)	9/16 (14.3m)	7/16 (14mm)	1 1/8 (28.4)
Very High	12 (300)	(a)	(a)	13/16 (21mm)	11/16 (17.4mm)	(a)

(a) Not applicable.

c) High level of threat protection. Select wall construction which resists the high-severity ballistics from Table 46. Wall materials include reinforced concrete, CMU, brick, mild steel or rolled homogenous armor plate, or bullet-resistant fiberglass.

d) Very high level of threat protection. The SAMIT threat is difficult to protect against. Effective protection, however, can be provided with appropriate design. Use a 10-gauge (3.4-mm) face plate over suitable cast concrete or filled concrete walls as shown in Table 47. Application of the 10-gauge (3.4-mm) steel plate on the back side of the wall, instead of the front, is not sufficient to stop penetration.

3) Doors. Because openings often are perceived by attackers to be more vulnerable than walls, minimize the number of exterior doors to limit potential targets. Bullet-resistant doors are available in a variety of sizes and styles, but most fit into one of two categories: opaque or transparent doors. Opaque doors normally are constructed of steel or aluminum armor plate and in some cases thicker plates of mild steel. Bullet-resistant plates are either on the face of the door and frame or are part of the core of the door and frame. Door frames normally are constructed of steel or aluminum sections and are filled with metal or plastic to ensure ballistic integrity.

Where a glazed door is required for safety, e.g., to avoid opening a door into a pathway, use the smallest possible glazing area to reduce exposure

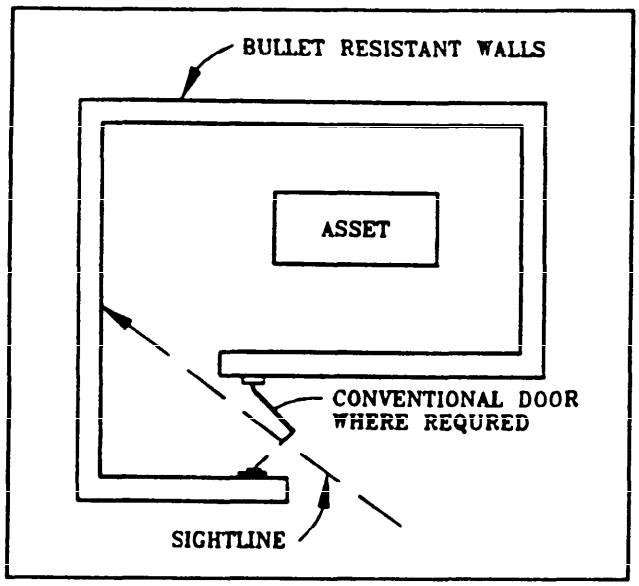


Figure 63
Wall Arrangement to Block Sightlines

of assets. Transparent bullet-resistant doors/frames usually are constructed of steel or aluminum sections with glazing panels of transparent armor consisting of glass, glass/plastic composites, or glass and plastic separated by an air gap. Each of the transparent armor types can be sized to different types of ballistic threats shown in Table 45. Installation (or replacement) of the transparent armor is critical in the overall protection afforded by the door assembly.

A transparent bullet-resistant door is not an attack-resistant door unless specifically designed against a forced-entry threat. Many of the features

Table 47
Wall Construction Capable of Defeating the MIL-SAMIT Very High Threat

Construction
8-inch (203-mm) cast concrete wall. Rebar [5/8 inch (16 mm)] placed in the center of the wall both horizontally and vertically on 6-inch (152-mm) centers. Single sheet of 10-gauge (3.4-mm) steel on the outside face.
10-inch (254-mm) cast concrete wall. Rebar [5/8 inch (16 mm)] placed in the center of the wall both horizontally and vertically on 6-inch (152-mm) centers. Single sheet of 10-gauge (3.4-mm) steel on the outside face.
12-inch (305-mm) grout-filled CMU block. Rebar [5/8 inch (16 mm)] placed the full height of the wall in each block opening. Single sheet of 10-gauge (3.4-mm) steel on the outside face.

incorporated into bullet-resistant doors are very beneficial to resist attack; however, the glazing systems of some transparent bullet-resistant doors are still vulnerable to tool attacks. Tests have shown that some transparent armors and framework can be penetrated within a short time when basic attack tools are used against the glazing.

A bullet-resistant door should provide protection with all door components. The lock area, frame, and sill plate should be armored to protect against the same type of threats as the door itself. Full length hinges or

hinges with self-engaging [1-inch (25-mm)] lock pins should be used with one or more high-security locks and dead bolts. Locks may be surface-mounted on the inside of the door or mortised into and around a cutout in the armor plate. Multiple and different locks and dead bolts should be considered. Grouting or overlapping steel plates also should be specified for the frame-to-wall gap.

Alternatively, for the high level of protection, provide bullet-resistant walls a short distance in front of the door, extending several feet to either side as shown in Figure 64. Use the same wall construction as required for the building exterior.

4) Windows. Minimize the number of windows and the window areas to limit available targets. Windows for the low level of protection depend on concealment to protect assets. For the medium and high levels of protection, provide bullet-resistant window assemblies to protect assets.

a) Low level of threat protection. Provide narrow windows oriented obliquely to the exterior surfaces of the facility as illustrated in Figure 65. Oblique windows limit the line-of-sight into the facility and decrease the window target areas. In the design and in practice arrange furniture and assets within the facility so that no occupants or assets within the facility are within the direct line-of-sight through windows. Provide reflective 0.004-inch (0.1-mm) fragment-retention film on window glass to obscure the interior of the facility from outside visibility during daylight. The film also limits the spread of glass fragments throughout a room if a bullet shatters the window. Provide drapes, shades, or blinds to obscure vision through the windows at night when the film is ineffective. As an alternative to the oblique windows, place all window openings at least 6 feet (1.8 m) above the floor to limit an attacker's ability to see activity below the sightline. Elevated windows also remove the constraints on furniture or asset locations. Provide transparent fragment-retention film on the elevated windows to minimize fragments entering the protected space.

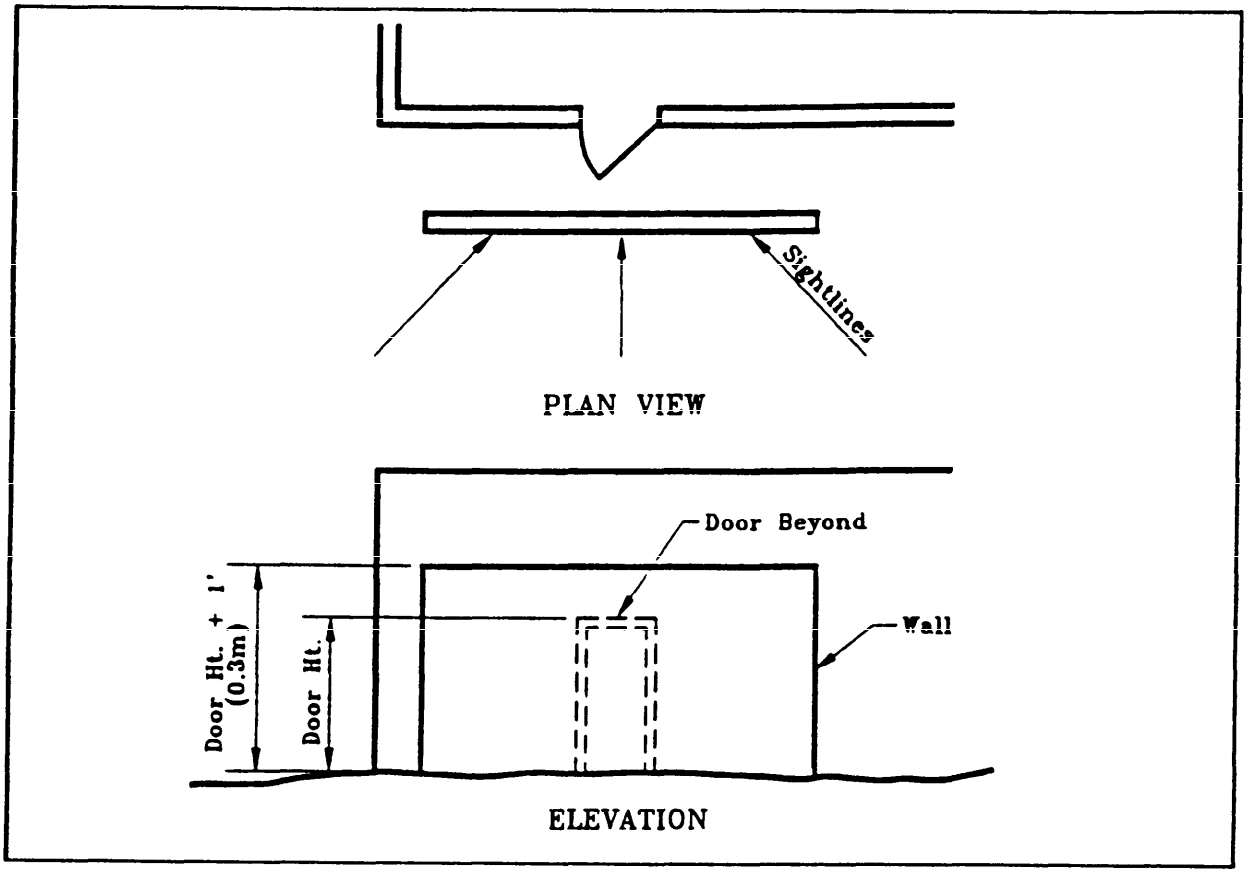


Figure 64
Walls to Block Sightlines at Doors

b) Medium level of threat protection. Follow guidance given for defeating the low-level threat. In addition, specify and provide bullet-resistant window assemblies that are designed to defeat the medium severity threat level shown in Table 45.

c) High level of threat protection. Specify and provide bullet-resistant window assemblies that are designed to defeat the high level threat shown in Table 45. Standard bullet-resistant window assemblies are available from manufacturers of bullet-resistant components. Because bullet-resistant window assemblies are extremely heavy and expensive, minimize their number and size. Coordinate wall construction to ensure adequate structural support for the windows.

Bullet-resistant window assemblies are all similar, employing laminated construction designed to defeat the specified threat. An example is illustrated in Figure 66. This assembly uses laminated glass backed with a 0.5-inch (12.7-mm)-thick polycarbonate spall shield to resist the 0.30-caliber (7.62-mm) high-severity threat. Safety glass laminated with polyvinyl

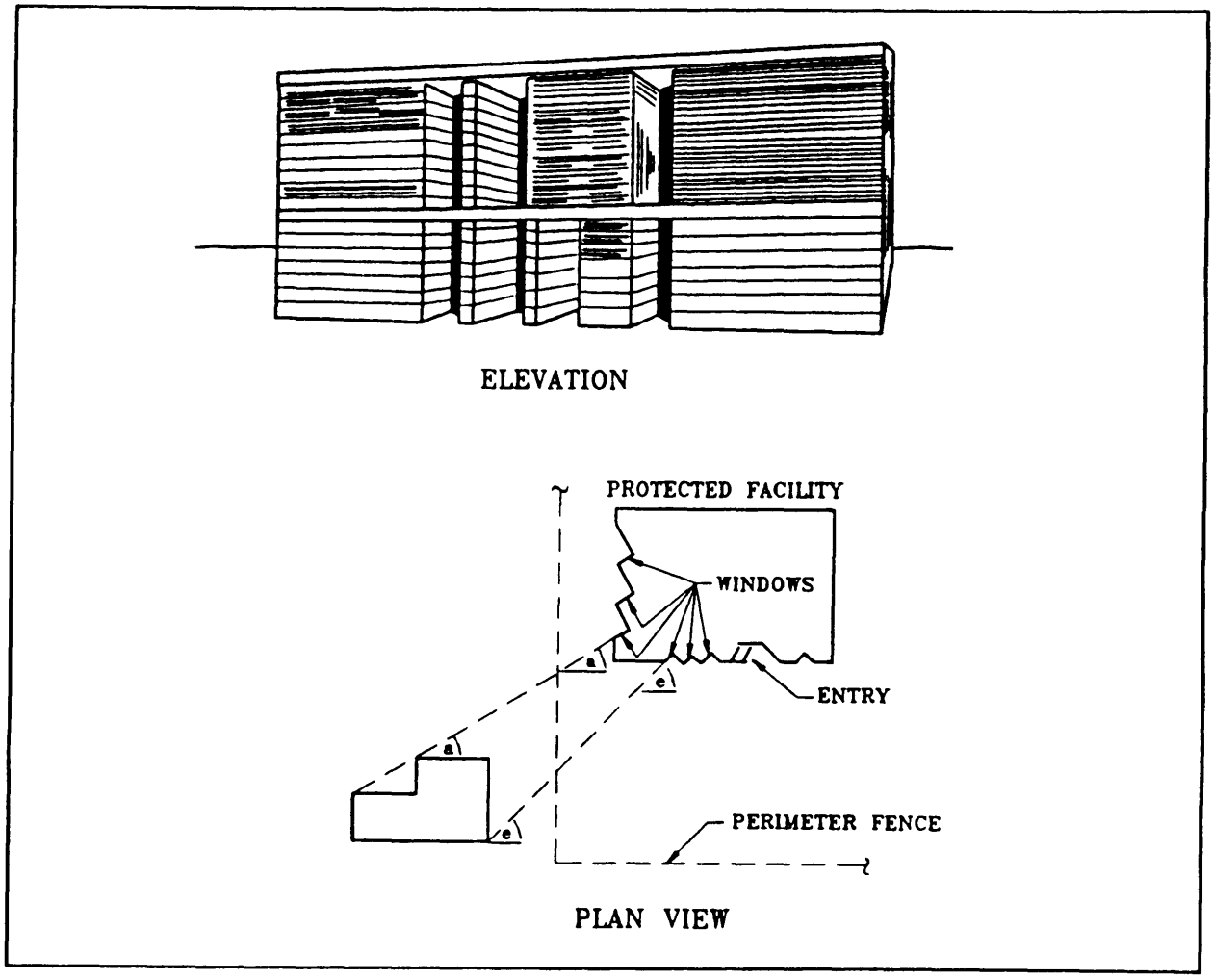


Figure 65
Oblique Window Openings

butyral is used. A space separates the bullet-resistant glass from the spall shield. The number of hits that can be defeated is a function of the number of laminations:

Number of Hits	Minimum Number of Laminations
1	6
2	7
3	8

The bullet-resistant glass and spall shield should be mounted so that it can be removed for cleaning and can be easily replaced if chipped, crazed, of scratched. The same should apply to the protective shield if employed on the exterior of the window. Mounting should be coordinated with the wall

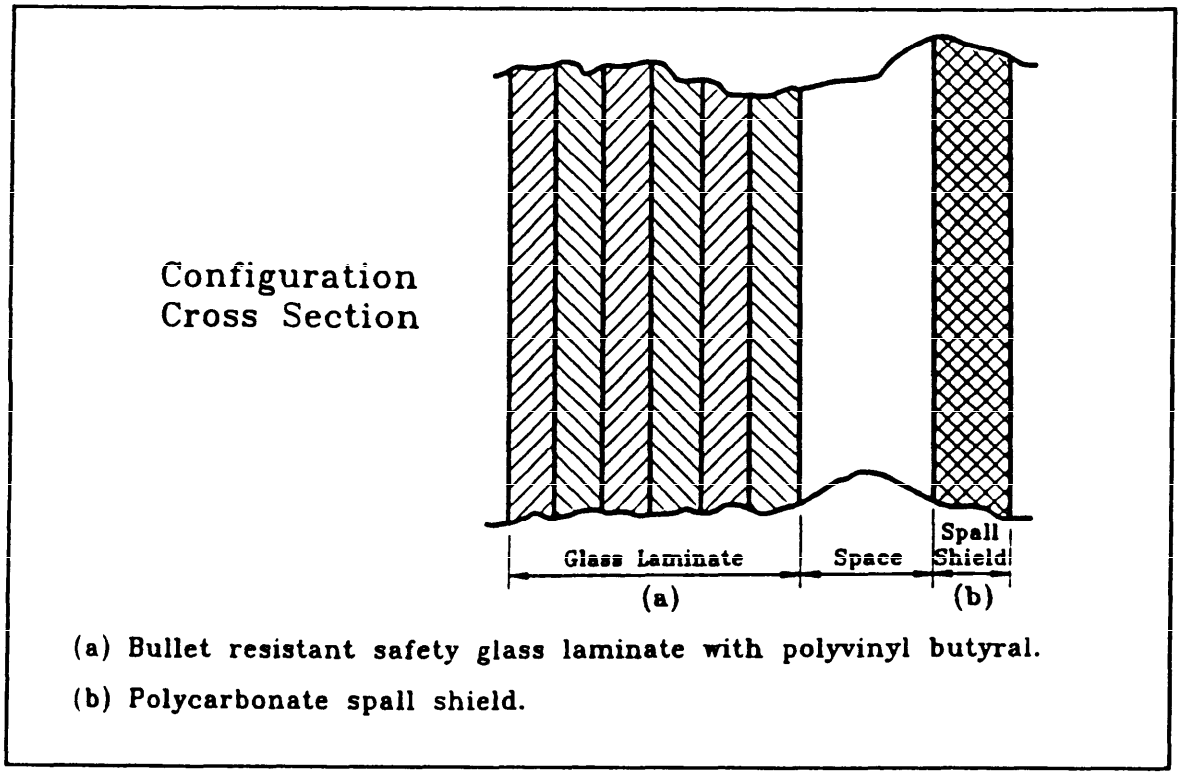


Figure 66
Example of High-Severity-Ballistic-Threat Bullet-Resistant Glass Cross Section

construction to avoid a weak ballistic boundary. Some other examples of bullet-resistant window assemblies designed to defeat the high-severity threat are shown in Table 48.

d) Very high level of threat protection. Eliminate windows in facilities that must withstand the very high-level threat.

5) Utility Openings. Protect utility openings where assets could be targeted through them. Specify sight-proof fixed louvers for all levels of protection. Bullet-resistant louvers or dampers shall be used to resist the appropriate severity level for the higher levels of protection. Coordinate wall construction to ensure adequate structural support for bullet-resistant utility opening protection.

6) Roof Protection. Provide roof protection only where there are potential sightlines to the roof. For the low level of protection, eliminate skylights or obscure sightlines through skylights and use opaque roof scuttles. For the medium through very high levels of protection, harden the roof construction using concrete components which provide equivalent construction to the rated wall assemblies shown in Table 46. Specify bullet-

Table 48
Transparent Armor Capable of Defeating the High-Severity Threat

Thickness	Construction
1.39 inches (35.3 mm)	Goodyear laminated transparent armor (Type 73-30) consisting of two 0.5-inch (12.7-mm)-thick plies of soda-lime plate glass (front) and one 0.25-inch (6-mm)-thick ply of polycarbonate (rear). Total thickness of adhesive between plies is 0.1 inch (2.5 mm). Exterior of rear is coated with 0.04-inch (1-mm)-thick compound to protect polycarbonate from abrasion.
1.75 inches (44.5 mm)	NCEL transparent sandwich (described in 6.5.2.2(4)(c), above) consisting of six 0.25-inch (6-mm)-thick plate glass plies (front), 0.5-inch (12.7-mm)-thick air space, one 0.25-inch (6-mm)-thick Lexan sheet (rear); transparent adhesive (between glass plies) and air space.
2.00 inches (50.8 mm)	Amerada glass (also known as Safe-Ray glass) consisting of eight 0.25-inch (6-mm)-thick plate glass laminae; transparent adhesive between laminae.
2.12 inches (53.8 mm)	Armaglas (series T, level 4) consisting of 0.5-inch (12.7-mm)-thick plate glass laminate (front), 1-inch (25-mm)-thick acrylic (intermediate), and 0.375-inch (9.5-mm)-thick polycarbonate (rear); transparent adhesive between laminae.

resistant roof scuttles and skylights for the required severity threat level or eliminate skylights. As an alternative for the high level of protection, provide high bullet-resistant parapet walls to block sightlines as shown in Figure 67.

6.5.3 Protection Measures; Retrofit. Retrofit protection measures are components and building systems added to the existing facility construction. Moving of assets to more secure or secluded areas is another method for enhancing protection. Retrofit measures are discussed in the following paragraphs.

6.5.3.1 Walls. There are three methods for upgrading existing walls. First, a stand-up reinforced concrete wall section can be added either to the outer or inner surface of an existing wall. A wall thickness equal to the wall section necessary to prevent single-round impacts at published muzzle velocities is recommended, although thinner add-on wall sections could be used if the composite (existing wall plus add-on section) wall is tested against the projectile threat and proven to be effective.

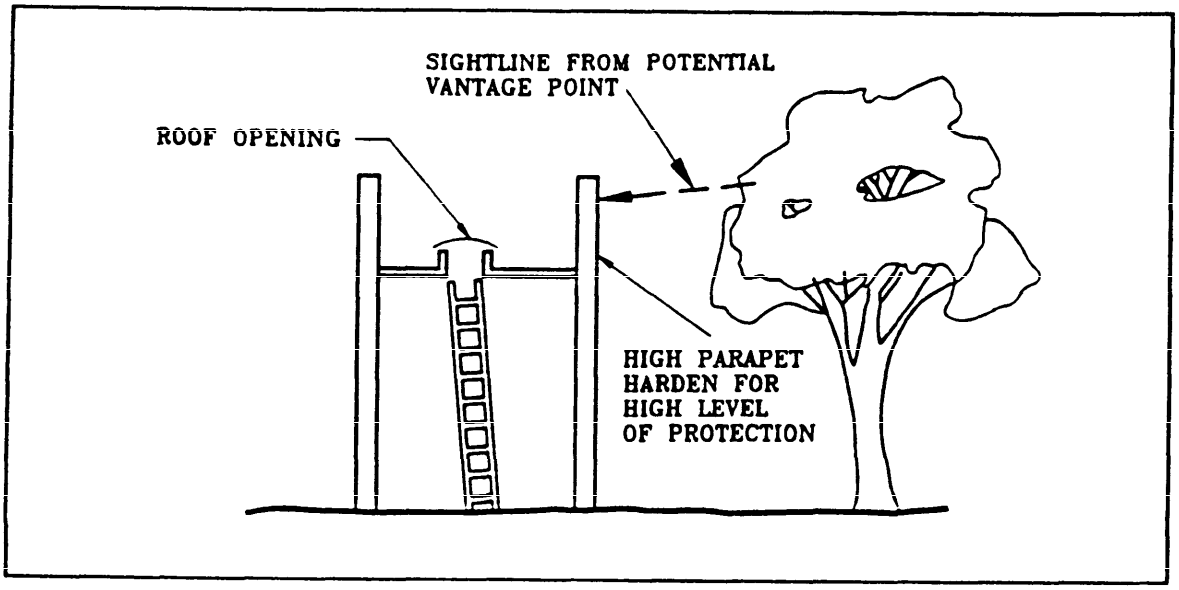


Figure 67
Parapets to Block Sightlines

Second, various other construction materials can be used to upgrade existing walls. These materials include wood, dirt, sand, gravel, brick, and concrete blocks. To upgrade hollow block walls, materials such as dirt, sand, and gravel should be added to a fill height of 6 feet (1.8 m) or more. Other materials such as brick or concrete blocks could be added either to the inside or the outside of existing weak walls to defeat a projectile threat. It appears feasible to upgrade walls with brick or block on the outside because: (1) footers to support the added weight of the new wall can be installed more easily on the outside than the inside; (2) usually fewer obstructions such as pipes, receptacles, vents, or doors are found on the outside of a building rather than the inside; (3) usable work space is not reduced; (4) interference with daily operations of the protected areas is minimal; and (5) the upgraded walls sometimes can improve the appearance of the structure. Conversely, it is possible that the existing structure might be ornate or unusually decorative, in which case upgrading it with brick or blocks could cause some degradation of its appearance.

A third upgrade suggestion is to use steel sheets or plates to achieve the degree of ballistic hardening required, as determined by the selected ballistic threat (Table 45). Some results of tests on upgraded walls using mild steel are shown in Table 49. Other types of steel such as high-hardness, dual-hardness, or rolled-homogeneous steel plates, also could be used.

Table 49
Upgraded Walls for High-Severity Threat

Wall	Upgrade
Hollow 8-inch (200-mm) concrete block	1/8-inch (3-mm) steel(a)
4-inch (100-mm) face brick	3/8-inch (9.5-mm) steel
2-inch (50-mm) concrete T-beam	3/8-inch (9.5-mm) steel

(a)Mild steel per QQ-S-741D.

Although steel armor can be used either on the inside or outside of walls, its use on the inside of a wall appears more appealing because: (1) the armor prevents spalling of the original wall material; (2) it occupies little interior space; (3) it can be cut and fitted at the site; (4) it can be installed with only hand and power tools, or in some cases, with only thermal tools; (5) when installed in a location protected from the weather, it requires very little maintenance; (6) no noticeably hardened areas can be seen by outsiders; and (7) ornate exteriors are not affected by the upgrade. Some disadvantages include: (1) critical cutouts for pipes, vents, receptacles, doors, windows, and switches must be made in the steel; (2) walls and footers may not be strong enough to support the additional load; and (3) daily operations may be affected by the armor installation.

When deciding what type of upgrade options can be applied to existing walls, consideration should be given to the availability of materials and installation hardware, labor requirements (skilled or unskilled), aesthetic appearance, degree of interference with daily operations, structural loads, installation time, and cost. Because of variation in threat definitions, every structure has unique ballistic hardening requirements, but a compromise usually can be made to satisfy both the functional and the protective elements of buildings. Table 50 provides additional examples of retrofit construction.

6.5.3.2 Doors. Eliminating all unnecessary doors is the first step in upgrading existing facilities. Steel pedestrian doors mounted in stamped steel frames frequently are found in existing facilities. While these doors provide little ballistic resistance, they can be upgraded. Steel sheets, described in the previous paragraph, can be used to upgrade these doors.

Table 50
Retrofit Construction Capable of Defeating
the Very High-Severity Level

Construction
8-inch (200-mm) hollow concrete Block, 3 sheets 10-gauge (3.4-mm) steel, 2 sheets 3/4 inch (19 mm)
6-inch (150-mm) cast concrete, No. 5 (15.9-mm) rebar at 6 to 8 inches (200 mm) o.c., to 10-gauge (3.4-mm) steel front and back
8-inch (200-mm) concrete block, No. 5 (15.9-mm) rebar at 8 inches (200 mm) o.c., horizontal joint reinforcement, 10-gauge (3.4-mm) steel front and back

However, it is necessary to provide balanced measures in the upgrade of doors. Suggestions are found in par. 6.5.2.2 (3).

Normally, because of construction constraints, existing doors are not removed and replaced with ballistic-resistant door assemblies. However, such a possibility may exist. The addition of a bullet-resistant wall assembly, such as shown in Figure 64, can be effective in obscuring an attacker's visual access to a door.

6.5.3.3 Windows. See par. 6.5.2.2.4.

Section 7: STANDOFF WEAPONS HARDENING

7.1 Introduction. This section begins with a description of the threat from a standoff Rocket Propelled Grenade (RPG) type of attack, followed by the general mechanisms by which RPGs can be stopped, and ends with hardening design options available for both new and retrofit construction. An RPG attack is a very high-severity level attack directed primarily toward killing or injuring personnel inside a building, although some critical assets might also be subject to destruction. An RPG is not used to gain entrance or cause significant damage to a building. A high-velocity jet of material is created by the RPG which penetrates significant distances and kills or injures by direct impact and spallation. The jet itself creates only a small hole.

7.2 The RPG Threat

7.2.1 RPG Characteristics. An RPG, like the Soviet built RPG-7 antitank grenade, is a rocket-assisted projectile fired from light hand-held launchers (see Figure 68). The grenade is first ejected from the launcher at a velocity of about 390 feet (120 m) per second by a small strip powder charge. Approximately 36 feet (11 m) from the launcher a sustainer rocket ignites and boosts the rocket to a maximum velocity of about 980 to 1310 feet (300 to 400 m) per second. The general characteristics of the weapon are summarized in Table 51. The RPG warhead consists of a conical-shaped charge within an outer steel casing called the ogive. On detonation, the material of the inner lining of the cone of the shaped charge collapses and forms a metallic jet having a very high velocity. The following gives a brief summary of the jet formation and target penetration mechanisms associated with a shaped charge of this type as background.

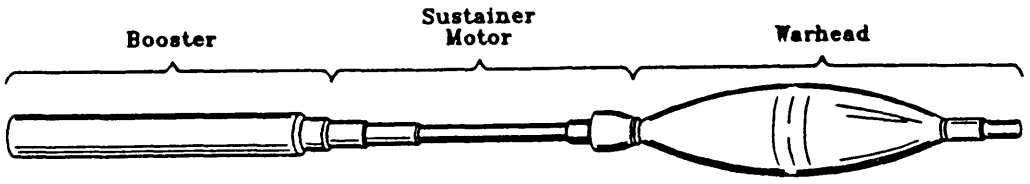
7.2.2 RPG Jet Formation. On detonation of the shaped charge, the metal jet is initially in a continuous stretching condition similar to a wire-drawing process. Because there is more explosive near the tip of the conical liner than around the base, there is an inherent variation in the velocity of each element of the jet. This results in stretching of the jet along its length until it eventually breaks up and separates into a column of small rod-like particles aligned one after another in tandem fashion.

7.2.3 RPG Jet Penetration. When the jet is in its early continuous state, it can penetrate virtually any material regardless of the hardness of that material. The density of the target material is its most significant protective property. However, once the jet is broken into discrete particles, the penetration mechanism changes, and factors such as target hardness become more important to the penetration process. Maximum depth of penetration is achieved when the jet is absolutely straight with each element exactly following its predecessor. As the jet impinges on a target material, the pressure exerted by the jet tip pushes the material away in all directions. The tip is used up continuously and converted into a high-temperature liquid with possibly some vapor formed and pressure generated at the contact point. New jet material continuously comes into contact at the rapidly moving

"working face" as the jet drives through the material. The penetration process continues until either all the jet particles are consumed, the energy of the unused jet particles is insufficient to overcome the target's own strength, the target material rebounds on the jet reducing its effective length, or the particles otherwise impact the side of the penetration cavity due to axial misalignment of the jet.

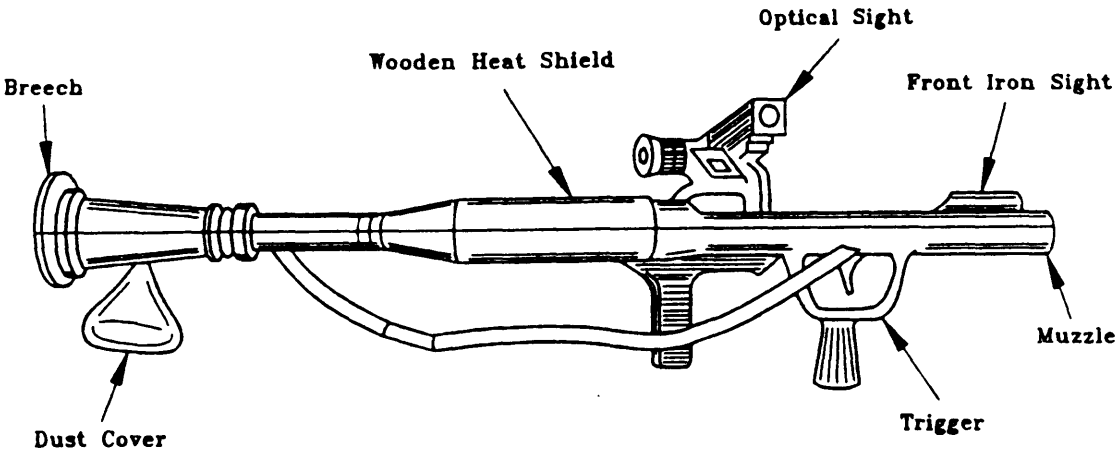
Table 51
Example Operational Characteristics of an RPG (Soviet RPG-7)

Characteristic	Value
Launcher Length	
Unloaded	37.8 inches (960 mm)
Loaded	52.6 inches (1340 mm)
Launcher Weight	
Unloaded	14.5 pounds (32 kg)
Loaded	19.0 pounds (42 kg)
Caliber	
Tube	1.57 inches (40 mm)
Round	3.35 inches (81 mm)
Rate of Fire	4.6 rounds per minute
Grenade	
Length	36.61 inches (930 mm)
Weight	4.6 pounds (10 kg)
Fuse	Point impact with base detonator
Propellant	Smokeless powder
Range	
Arming	16.4 feet (5 m)
Sighting Range (Max.)	1,640 feet (500 m)
Maximum Range	2,950 feet (900 m)
	Self destructs
Velocity	
Initial	384 ft/s (117 m/s)
Rocket Assist	965 ft/s (294 m/s)
Type Warhead	HEAT
Lead Capability	20 mph (32 km/h)



The grenade is carried in two parts: (1) warhead and sustainer motor and (2) booster charge. The two must be screwed together before the grenade is ready to fire.

A. Grenade -- Prelaunch Configuration



B. Launcher

Figure 68
Example Antitank Grenade Launcher Weapon—the Soviet RPG-7

7.3 RPG Defeat Mechanism. Important characteristics that limit the penetration of an RPG jet are primarily material density, strength, and the tendency of certain materials to rebound on the jet. In addition, predetonation of the RPG at a standoff distance from the material or creating an oblique line of attack can limit RPG effects.

7.3.1 Material Density. In general, the amount of penetration achieved by a continuous jet is approximately inversely proportional to the square root of the density of the material. Consequently, materials with greater density have a greater stopping capability.

7.3.2 Material Strength. Material strength becomes increasingly important as the jet slows down and/or becomes particulated, i.e., when the pressure exerted by the jet is no longer large compared to the strength of the target. An approximate indicator of strength is the Brinell Hardness Number (BHN) of the material. In general, materials with higher BHN have better stopping ability.

7.3.3 Rebound Defeat Mechanisms. Rebound or hole "closure" is a phenomena where target material moves back into the cavity caused by a jet and interferes with subsequent portions of the jet, reducing its effective length and penetrating capability. Only certain materials like steel, ceramics, aluminum, and glass-reinforced plastics exhibit rebound. In general, this phenomenon effects jets that have particulated. Rebound occurs when the material flows back toward the cavity axis and closes the hole behind each particle. Thus, the next particle must penetrate the closed cavity before impacting the cavity bottom.

7.3.4 Oblique Attack Effects. Barrier surfaces that are at some angle to the line of attack of the jet create a thicker material cross section for the jet to penetrate.

7.3.5 RPG Defeat By Predetonation and Standoff. Screens can be used to predetonate an RPG at a standoff distance away from the barrier. At large standoffs the jet particulates and slows down before hitting the target and consequently is easier to stop.

7.4 Hardening Design Options. This section provides guidelines for hardening both new construction (par. 7.4.1), as well as the retrofit of existing construction (par. 7.4.2) against an RPG attack.

7.4.1 New Construction. In designing a new building against an RPG attack, one or more of the following should be considered: (1) proper site layout to minimize attack line-of-sight; (2) the use of building sacrificial areas; and (3) appropriately designed barriers with or without predetonation screens.

7.4.1.1 Site Layout. Since the RPG is a line-of-sight (LOS) weapon, the facility should be sited to limit, or preferably block, RPG attack sightlines

from potential vantage points. Options include: (1) the use of natural or manmade obstructions such as trees, fences, land-forms, or buildings to obscure sight paths; (2) siting the facility at a high point, if possible, to force aggressors to fire up toward the target; and (3) causing the RPG to strike protective surfaces at an angle, reducing the effectiveness.

7.4.1.2 Sacrificial Areas. Sacrificial areas in the building can be employed above, below, and around the critical area in the building to be protected. The walls, doors, etc., of this sacrificial area may be damaged, but will provide a standoff region to reduce the effectiveness of the RPG jet for the critical area. In general, to facilitate this the critical area should be low and internal to the building and well away from exterior walls.

7.4.1.3 Barrier Construction and Predetonation Screens

1) Walls. The only practical wall construction material to stop a direct RPG attack is the use of massive concrete in combination with sand and a predetonation screen. The design tradeoffs are shown in Figure 69. In general, the use of sand is more appropriate to a temporary situation where the function of the facility may change and the sand can be removed later. If an RPG threat against the building is likely to be permanent, the use of concrete by itself or in combination with a predetonation screen is more appropriate.

a) Predetonation screens. Predetonation screens may consist of wood fences, chain-link fencing, expanded metal mesh, or heavy woven-fiber fabric. Wood fences can be made of wood slats or plywood panels a minimum of 3/8 inch (9.4 mm) thick. If they are made of slats, the slats should be spaced no more than 1/4 inch (6.4 mm) apart. Spaces in metal fabric screens must be 2 inches (50 mm) by 2 inches (50 mm) maximum and the fabric a minimum of 9 gauge (3.8 mm). The effectiveness of screens of various sizes is shown in Table 52. This data suggests that 2-inch (50-mm) chain link presents the minimum risk of an RPG passing through the screen with no effect. An RPG which strikes a predetonation screen either detonates on impact or is dudded. Dudded refers to a round being damaged so that it will not detonate. The residual effects of a predetonated round on a building are more severe than the effects of a dudded round. Therefore, in the design one need be concerned only with predetonated rounds. After predetonation, the RPG jet and the spent rocket engine from the RPG continue past the screen. The screen should be located away from the wall a standoff distance appropriate to the concrete wall construction (see Figure 68). For other materials allow a minimum of 40 feet (10 m).

b) Predetonation walls. Solid walls constructed of CMU or other material can also be used if they can be constructed at the proper height and location. These are 100 percent effective in predetonating RPGs.

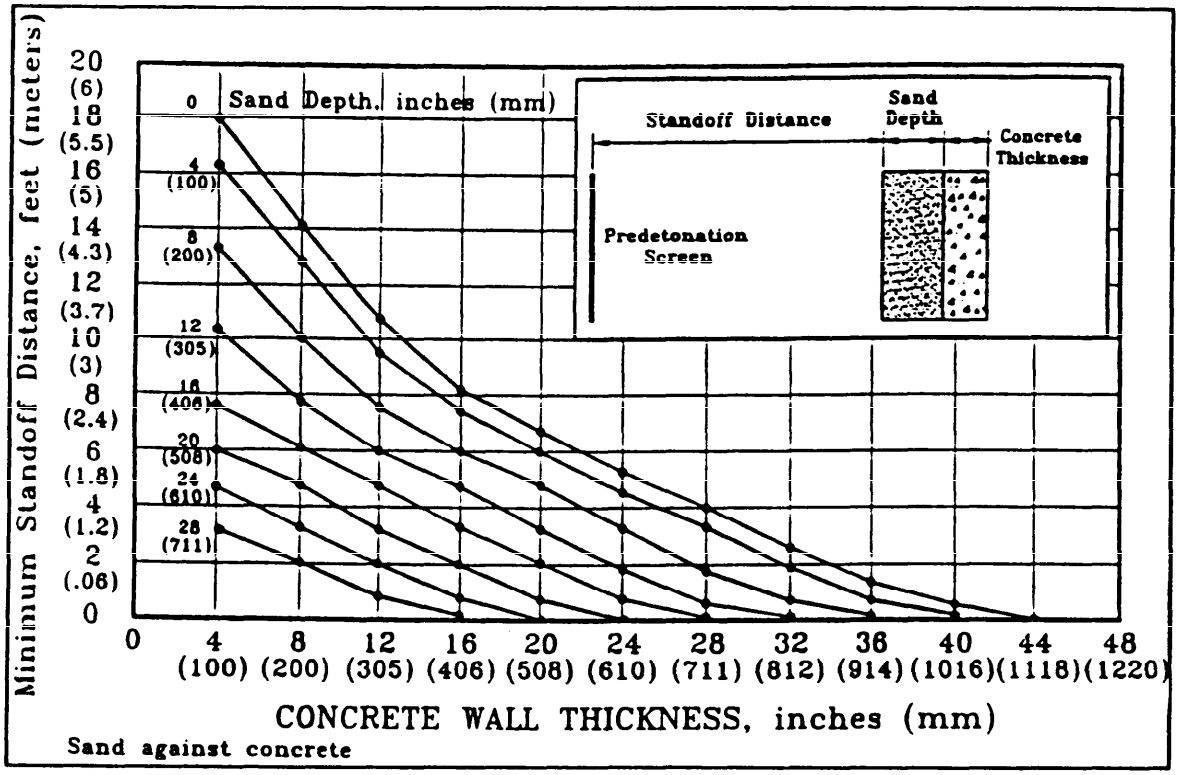


Figure 69
RPG Hardening–Concrete/Sand Thickness Verses Standoff Distance

Table 52
Predetonation Screen Effectiveness

Screen Size	No Effect	Detonating
2-inch (50-mm) Chain Link	36%	64%
3- by 3- by 0.2-inch (76- by 76- by 5-mm) Weld Mesh	48%	52%
3- by 6- by 0.2-inch (76- by 152- by 5-mm) Weld Mesh	58%	42%
3- by 12- by 0.2-inch (76- by 305- by 5-mm) Weld Mesh	62%	38%

c) Wall construction. New construction options for walls include concrete/sand combinations as shown in Figure 69. This figure shows the concrete wall thickness required versus standoff distance for sand depths (if used) ranging from 0 to 28 inches (700 mm). An example of the use of this figure is as follows. If no sand and no predetonation screen are used, about 44 inches (1.1 m) of concrete are required. If the concrete wall thickness is limited to 12 inches (300 mm) and no sand is used, the minimum standoff distance required for the predetonation screen is about 11 feet (3.3 m). If 16 inches (400 mm) of sand is employed, the standoff distance is reduced to 5 feet (1.5 m). These combinations of depths of sand and concrete used with an effective predetonation screen have been found adequate to stop the penetration of the predetonated RPG.

Another wall concept is the 32-inch (810-mm) sandwich ASP Walling design shown in Figure 70. The ASP Walling system consists of formed metal sheets joined together to constitute both the permanent formwork, while at the same time acting as antispalling plates to contain fragments. The basic component of the ASP Walling system is a wall element consisting of interlocked external sheets. The two faces are tied to each other by diagonal lacing panels which, in zig-zag fashion, form a rigid permanent formwork into which 1.5-inch (40-mm) hard stones are placed (see Figure 70).

2) Roofs and Floors. Because of the large quantities of material required to stop an RPG jet, structural considerations will likely preclude their application to roofs or floors open from above and below. In this case, critical assets may only be protected from above and below using sacrificial areas as discussed in par. 7.4.1.2.

3) Windows. Areas to be protected against an RPG attack should be free of any windows.

4) Doors. Foyers should be provided at protected entrances or door openings should be offset so that each door is opposite a solid wall construction associated with a sacrificial area. Examples of possible configurations are illustrated in Figures 71, 72, and 73. The design of exterior concrete walls should be of the same construction as other protected walls. Predetonation screens at the proper standoff can also be provided if necessary (see Figure 69).

7.4.2 Retrofit Construction. The most cost-effective retrofit concept involves the use of sand and predetonation screens or walls. Sand bags or sand-grids used in combination with properly located predetonation screens can stop an RPG from penetrating into high-security areas constructed of concrete and certain CMU construction.

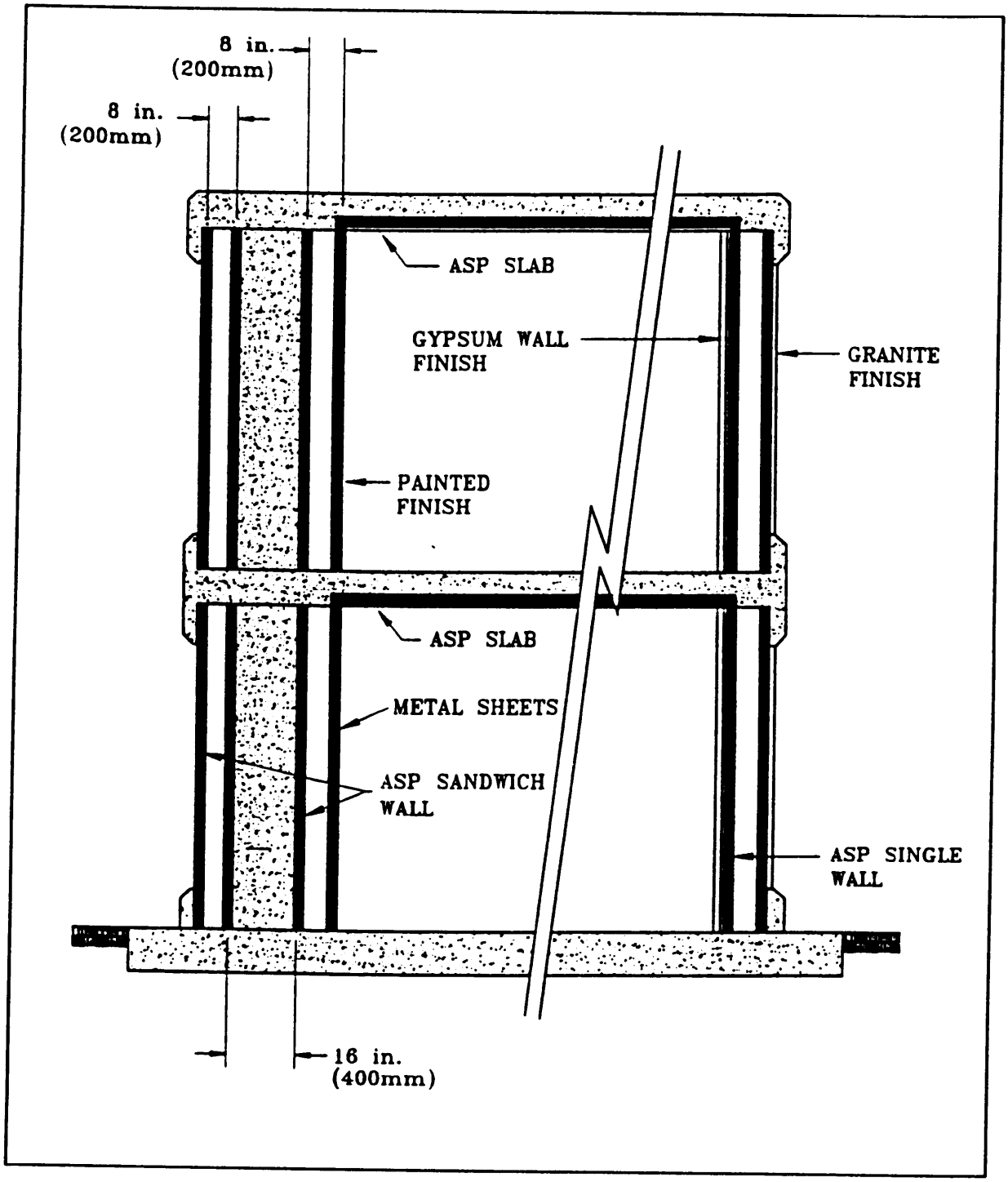


Figure 70
ASP Walling System

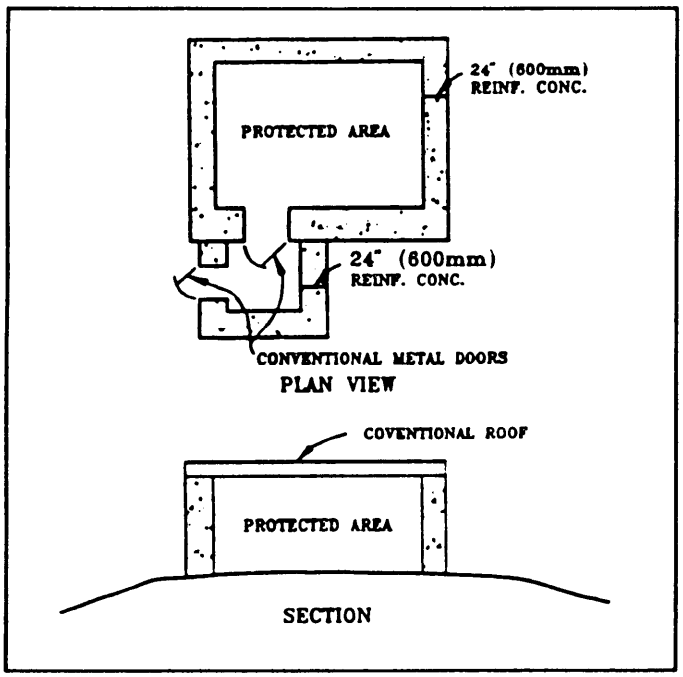


Figure 71
Building Layout Example

7.4.2.1 Retrofit of Walls

1) Concrete Wall Retrofit. Sand in combination with predetonation screens can be used in sandbags or in sand-grid revetments to retrofit concrete walls. Sand-grids (see Figure 74) are more easily transported and require less construction time than sandbags. The expanded configuration shown in Figure 74 is placed in a vertical configuration and filled with sand. The required thickness of sand for concrete and a predetonation screen at various standoffs is summarized in Figure 75. A spall plate consisting of 0.5 inch (12.5 mm) of polyethylene is also employed on the interior wall. This plate reduces the concrete thickness required to stop the RPG from penetrating. Choices of standoff distance, sand depth, and wall thickness will vary with user requirements. Figure 75 allows the user to determine the combinations that best fit his needs.

2) CMU Wall Retrofit. Sand can also be used with CMU to reduce the jet penetration of an RPG. For example, test results for 12-inch (300-mm)-thick CMU require 32 inches (812 mm) of sand on the exterior with 0.5 inch (12.5 mm) of polyethylene on the inside (as a spall plate) to successfully stop the jet. Presently, there is no test data for other CMU wall sizes.

3) Other Materials. Other materials such as wood cannot effectively be retrofit-hardened against an RPG attack.

7.4.2.2 Retrofit of Roof and Floors. Because of the large quantities of material required to stop an RPG jet, structural considerations preclude their application to roofs or floors open from above or below. Critical assets can only be protected from above and below using sacrificial areas as discussed in par. 7.4.1.2.

7.4.2.3 Windows. Areas to be protected against an RPG attack should be free of windows.

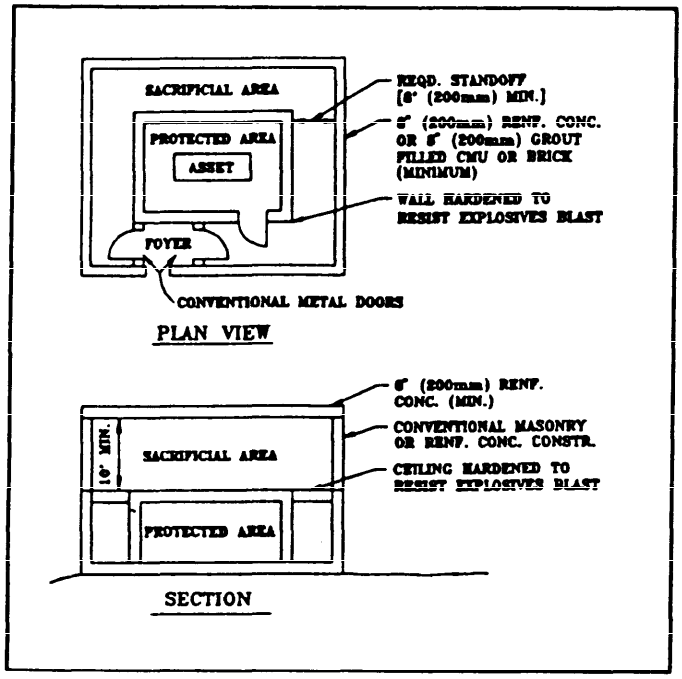


Figure 72
Building Layout Example

7.4.2.4 Retrofit of Doors. Foyers should be provided at protected entrances or openings should be offset such that each door is opposite a solid-wall construction associated with a sacrificial area. Examples are given in par. 7.4.1.3.

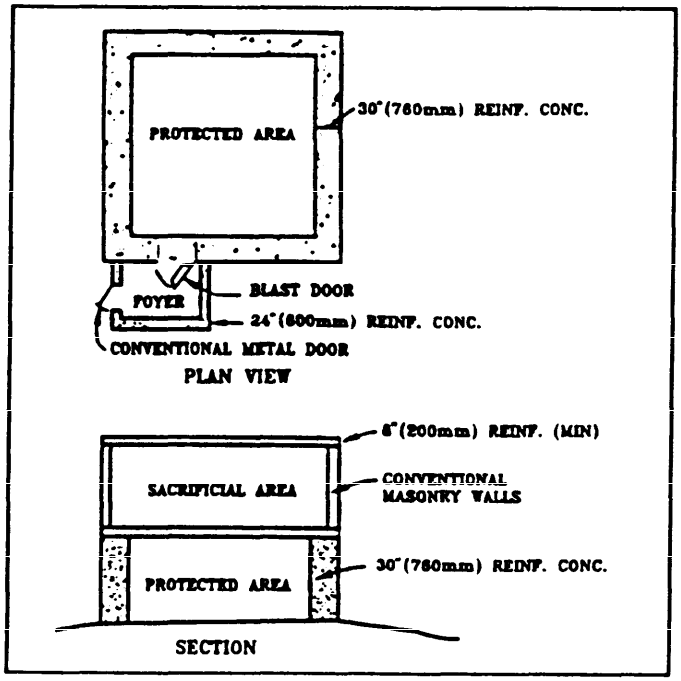


Figure 73
Building Layout Example

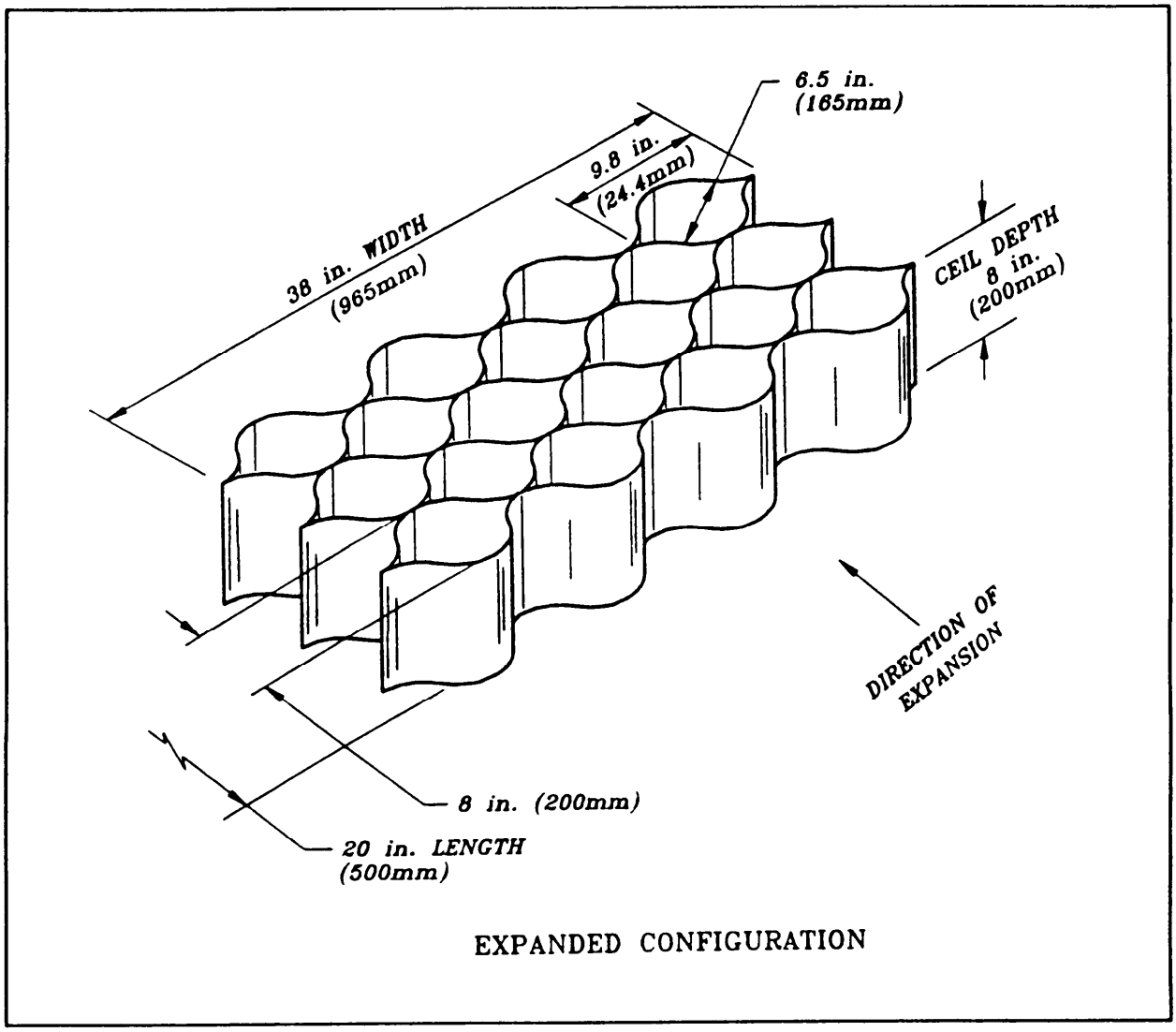


Figure 74
Standard Sand-Grid Materials (from Army Technical Report SL-88-39, Expedient Field Fortifications Using Sand-Grid Construction)

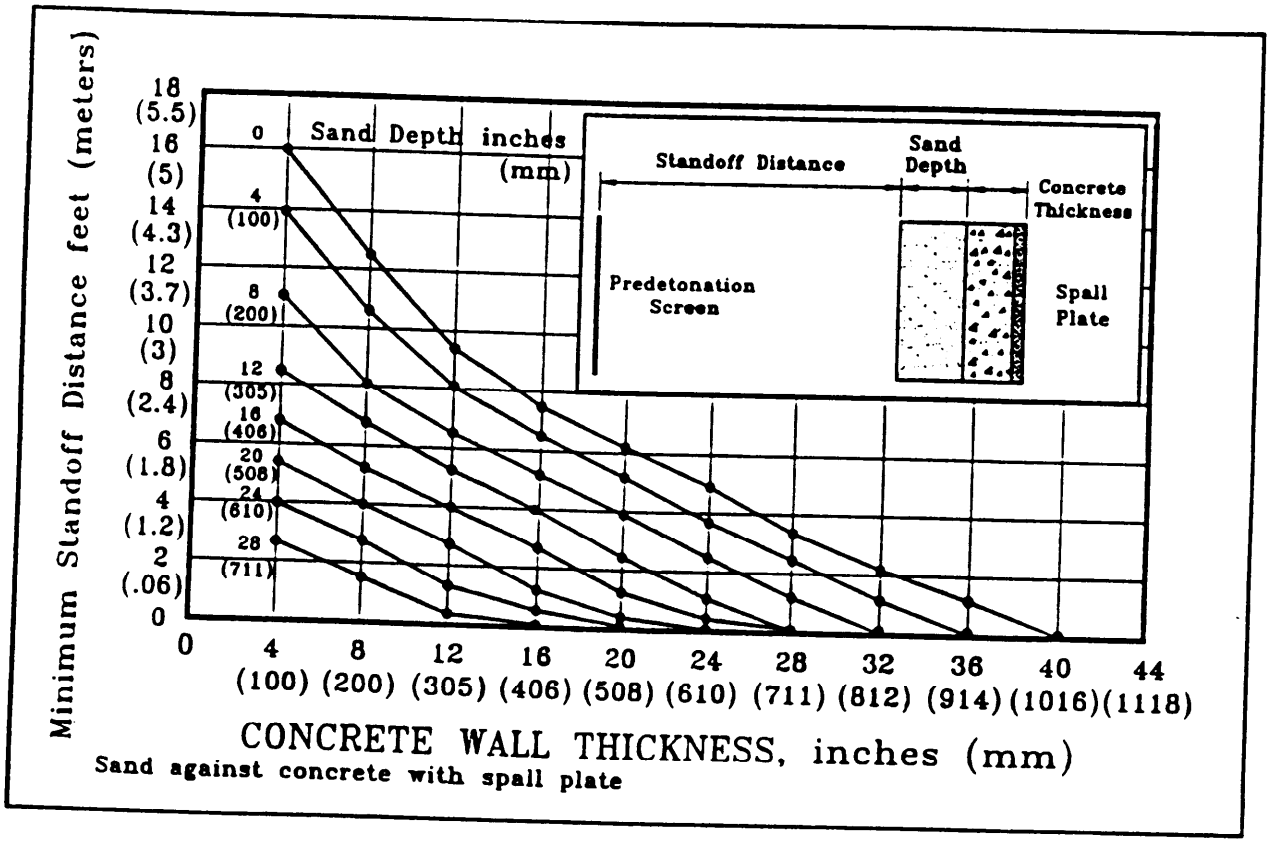


Figure 75
Retrofit Hardening—Concrete/Sand Thickness Versus Distance

Section 8: BOMB BLAST HARDENING

8.1 Introduction. This section summarizes the design approach for hardening against bomb blast effects. A brief summary of design approaches for both new and existing construction is provided. The intent is to illustrate the basic standoff distance versus blast hardening tradeoff for designing against such threats. See the Navy Terrorist Vehicle Bomb Survivability Manual and the Army Security Engineering Manual for details.

8.2 Design Threats

8.2.1 Stationary Bomb Threats. Stationary bomb threats may consist of either a bomb-ladened vehicle parked near perimeter fence lines or entry point areas or dropped-off, concealed packages. In these cases, the design threat explosive level can range from 50 pounds (22.5 kg) of trinitrotoluene (TNT) for the low-level threat up to 1,000 pounds (450 kg) for the high-level threat as shown in Table 53. In this regard, one operational requirement focuses on the higher order threat requiring protection against detonation of 1,000 pounds (450 kg) net explosive weight from at least 400 feet (122 m); however, it is also indicated that this is not absolute, but must be adapted to site conditions.

Table 53
Stationary Bomb Threats

Threat	Explosive Level, lb (kg) of TNT
Low	50 (22.5)
Medium	220 (100)
High	500 (225)
Very High	1000 (450)

8.2.2 Moving Vehicle Bomb Threat. There are also four levels of moving vehicle design threats ranging from low to very high, as shown in Table 54. Explosives range from 50 to 1,000 pounds (22.5 to 450 kg) of TNT. Vehicle weights are 4,000 pounds (1,800 kg) for automobiles and up to 10,000 pounds (4,500 kg) for trucks, with speeds varying from 15 to 50 mph (24 to 80 km/h). In general, the basic tradeoff is to design vehicle barriers to stop such threats at a standoff distance that is consistent with the hardness of the building against blast effects. Kinetic energy (KE) equivalents for the vehicle can be computed using the expression:

EQUATION: $$KE(ft\text{-}lb) = 0.03344\ W\ V^2 \quad (1)$$

where W = vehicle weight in pounds
V = the vehicle velocity in miles per hour
or

EQUATION: $KE(m\text{-}kg) = 0.0497\ WV^2$ (2)

where W = vehicle weight in kilograms
V = vehicle velocity in kilometers per hour

Again, one operational requirement requiring detonation of 1,000 pounds (450 kg) net explosive weight from at least 400 feet (122 m) should be considered; however, it is also indicated that this is not absolute, but must be adapted to site conditions.

Table 54
Moving Vehicle Transported Bomb Threats

Threat Severity	Explosive Level lb (kg) of TNT	Vehicle Transport		
		GVW, lb (kg)	Speed, mph (km/h)	Kinetic Energy Equivalent, ft-lb (kg-m)
Low	50 (22.5)	4,000 (1,800)	15 (24)	30,000 (40,000)
Medium	220 (100)	10,000 (4,500)	15 (24)	75,000 (100,000)
High	500 (225)	4,000 (1,800)	50 (80)	334,000 (450,000)
Very High	1000 (450)	10,000 (4,500)	50 (80)	836,000 (1,140,000)

8.3 Standoff/Hardening and Protection Levels. Figure 76 shows the geometry of a bomb-blast wave. In general, the pressure levels of bomb blasts fall off approximately as the inverse square of the distance from the blast. Consequently, the larger the standoff distance, the lower the pressure delivered to the structure. To illustrate, Figure 77 shows the pressure from a blast wave versus standoff distance for several different charge weights. For example, the pressure from a 100-pound (45-kg) charge at a standoff distance of 10 feet (300 cm) is about 280 psi (1,900 kPa). If the standoff distance is increased to 100 feet, the pressure is reduced to about 2.8 psi (19 kPa).

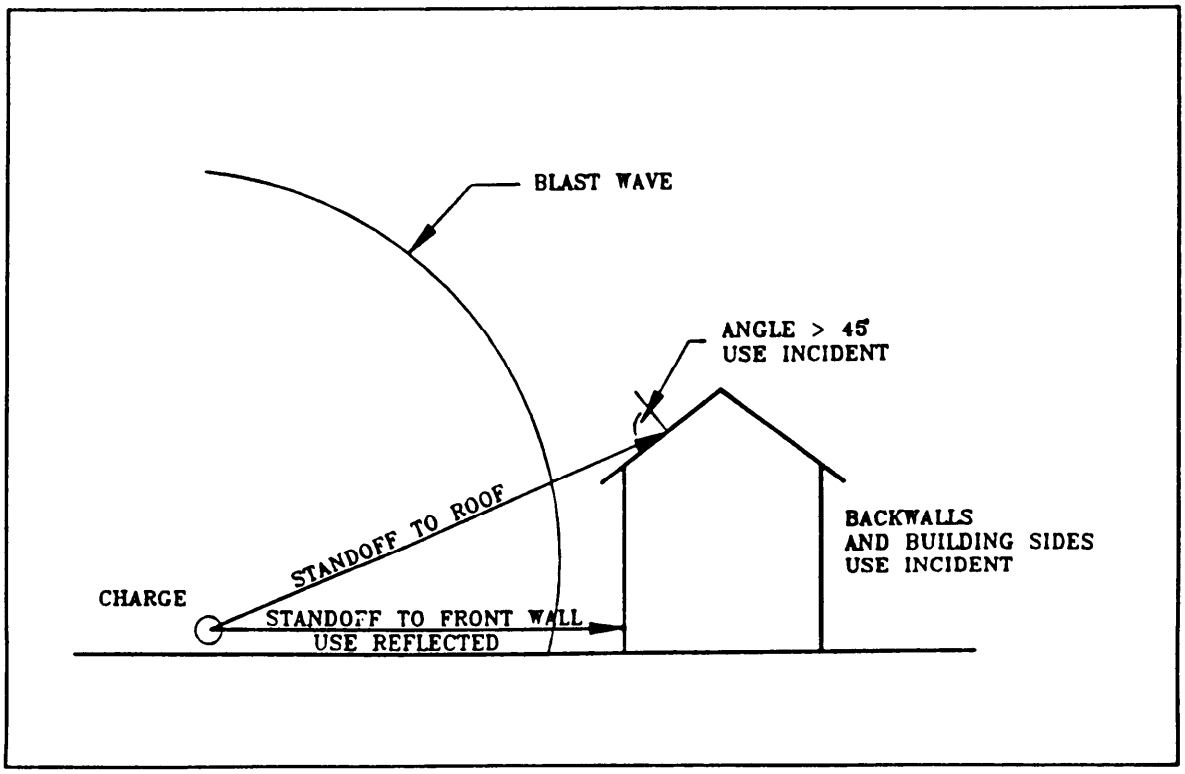


Figure 76
Blast Wave Geometry

8.3.1 Protection Levels for New Construction. In the Army Security Engineering Manual there are three levels of protection to which facilities can be hardened: a low level in which damage is unreparable; a medium level in which the damage can be repaired; and a high level in which the facility suffers only superficial damage.

8.3.2 Protection Levels Existing Structures. The Navy Terrorist Vehicle Bomb Survivability Manual describes two levels of protection for existing structures: Rebuild or Repair. These are provided for charge weights from 1 to 4,000 pounds (0.45 to 1,800 kg) and standoff distances from 1 to 1,000 feet (0.3 to 300 m) for 12 different building types intended to be representative of facilities used by the Armed Services worldwide. Examples are provided in par. 8.4.3.1.

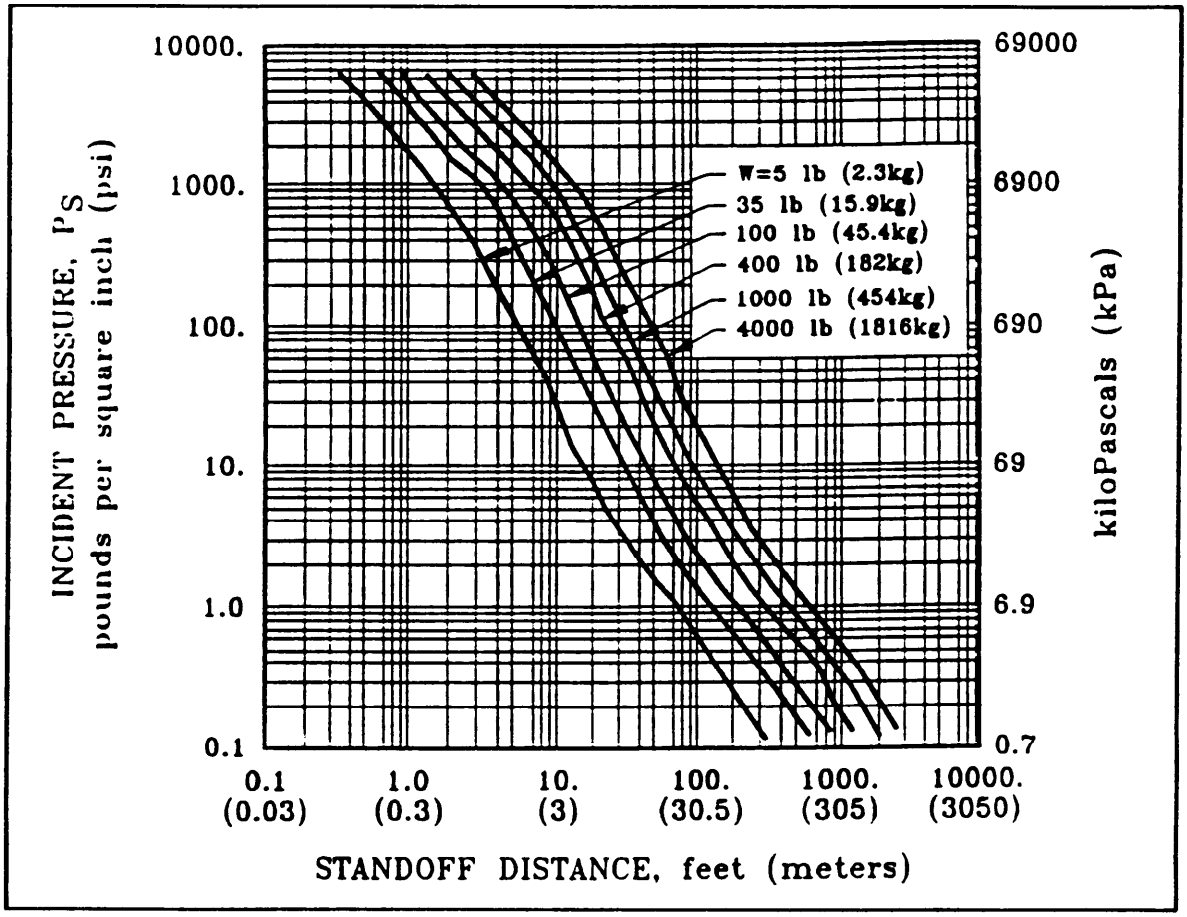


Figure 77
Pressure Levels Versus Standoff Distance

8.4 Design Approach

8.4.1 Introduction. This section summarizes the design approach contained in the Navy Terrorist Vehicle Bomb Survivability Manual and the Army Security Engineering Manual whereby one can establish the level of protection provided by various combinations of standoff distances and structural hardening. Vehicle barriers required to maintain standoff distances are also summarized.

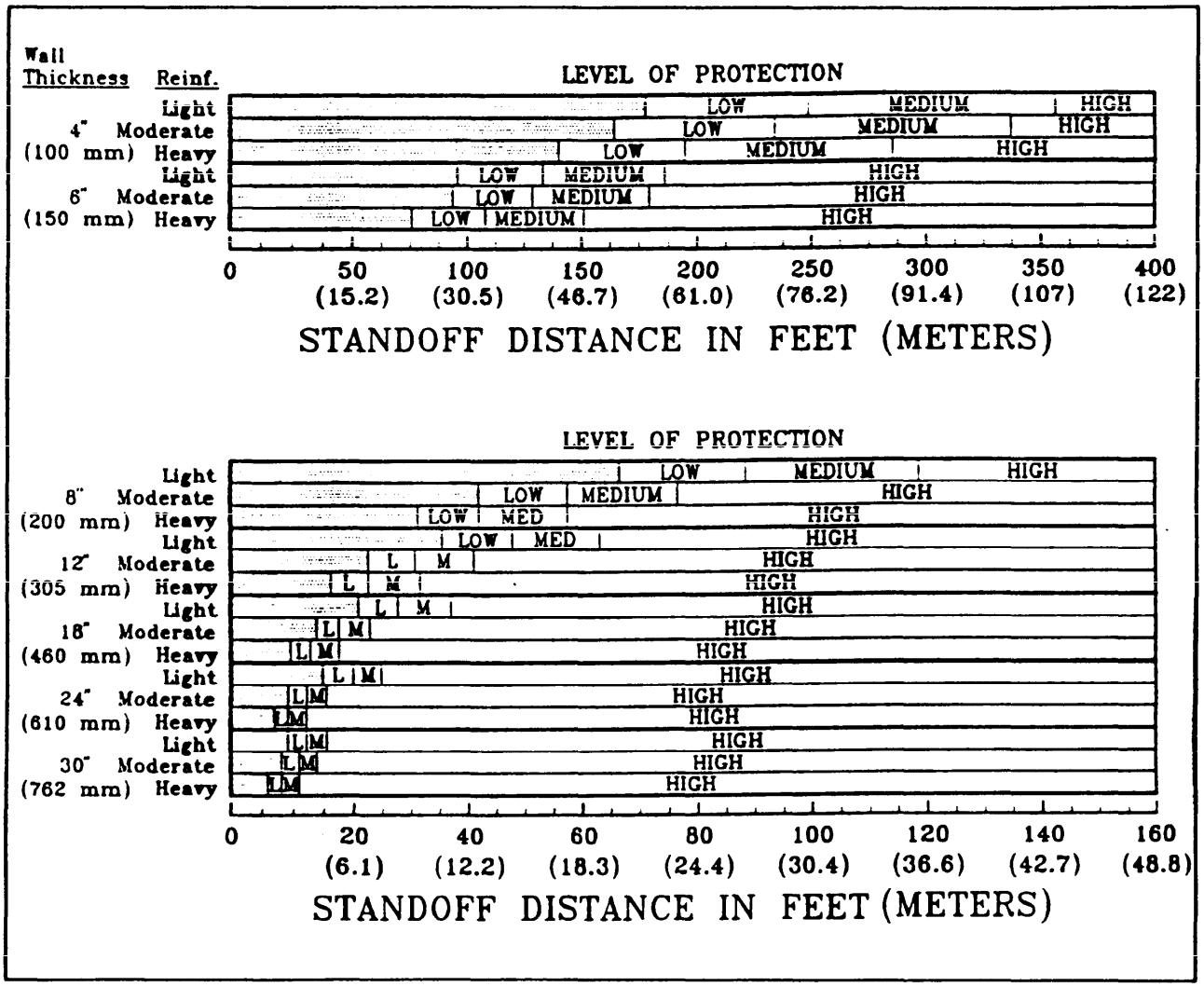


Figure 78
Reinforced Concrete Wall Design For 220-Pound (100-kg) Explosive Effects
(Army Security Engineering Manual)

8.4.2 Design of New Construction

8.4.2.1 Structure Hardening. The Army Security Engineering Manual provides technical data regarding structure hardening for plain and reinforced CMU, and for reinforced concrete structures. Data is available for explosive charges from 50 to 1,000 pounds (22.5 to 900 kg). Figure 78 shows some example results for reinforced concrete walls of thickness from 4 to 30 inches (100 to 762 mm). Three levels of reinforcement are considered: light, moderate, and heavy. Levels of protection are shown versus required standoff distance.

Similar results are available for plain and reinforced CMU. Tabular results are also available for doors, windows, roofs, and frames. Window hardening techniques and tabular results (see Figure 79) of load resistance versus charge weight and standoff distance are also provided in the Navy Terrorist Vehicle Bomb Survivability Manual.

Charge weight = 100 lb (45kg) Aspect Ratio = 1.00									
Plate Dimension inches (meters)		Standoff Distance, feet (meters)							
b	a	25 (7.6)	50 (15)	75 (23)	100 (30)	125 (38)	150 (46)	200 (61)	300 (91)
12 (0.3)	12 (0.3)	60 (18)	16 (5)	9 (3)	7 (2)	7 (2)	7 (2)	7 (2)	7 (2)
14 (0.36)	14 (0.36)	59 (18)	16 (5)	9 (3)	6 (2)	5 (2)	5 (2)	5 (2)	5 (2)
16 (0.4)	16 (0.4)	57 (17)	15 (5)	9 (3)	6 (2)	4 (1)	4 (1)	4 (1)	4 (1)
18 (0.46)	18 (0.46)	56 (17)	15 (5)	9 (3)	6 (2)	5 (2)	4 (1)	3 (1)	3 (1)
20 (0.5)	20 (0.5)	54 (17)	15 (5)	9 (3)	6 (2)	5 (2)	4 (1)	3 (1)	3 (1)
22 (0.56)	22 (0.56)	53 (16)	15 (95)	9 (3)	6 (2)	4 (1)	4 (1)	3 (1)	2 (1)
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

Figure 79
Example Minimum Thickness [feet (meters)] of Thermal-Tempered Glass Glazing to Resist Reflected Overpressusre

8.4.2.2 Vehicle Barriers for Maintaining Moving Vehicle Standoff. Moving vehicles carrying large weights of explosives pose a tremendous problem. Currently, most vehicle barriers are designed to stop vehicles through one or a combination of the following methods. (See the Navy Terrorist Vehicle Bomb Survivability Manual for details.)

1) Vehicle Arrestor. Absorbs virtually all of a vehicle's kinetic energy and applies a low to moderate resistive force to gradually stop a vehicle over a relatively long distance. Examples are weights that are dragged by a vehicle and accumulate with distance traveled, and piles of loose sand.

2) Crash Cushion. Absorbs a large portion of a vehicle's kinetic energy and provides a stiff resistive force to stop a vehicle in a reasonable distance. Examples are liquid-filled plastic containers and arrays of empty steel barrels that are backed by strong supports.

3) Inertia Device. Exchanges momentum and kinetic energy with a vehicle during impact. This device provides a stiff resistive force to stop a vehicle in a reasonable distance. Examples are relatively small concrete shapes and sand-filled barrels that are not anchored.

4) Rigid Device. Provides very high resistive force to stop vehicles in very short distances. The vehicle dissipates almost all of its own kinetic energy as it deforms during impact. Examples include massive concrete shapes and steel structures that are well anchored.

The above general types of barriers may be active or passive. Active barriers require action by personnel or equipment to permit entry. Passive barriers can be used as traffic obstacles as shown in Figure 80. Barriers may also be fixed, movable, or portable. Fixed barriers include hydraulically operated rotating or retracting systems. Movable barriers include 55-gallon (200-liter) drums, highway medians, etc. Portable barriers include ropes, chains, and cables used as temporary barriers. In general, all the above types of barriers have been designed and tested against combinations of vehicle size, weight and velocity. Paragraph 8.2 shows that the kinetic energy (KE) of such vehicles scales as the velocity squared; hence reducing the velocity by a factor of 2 reduces the KE by a factor of 4. Figures 81 and 82 (from the Army Security Engineering Manual) show the effectiveness of both active and passive barriers against threats of various KE. Figure 80 shows an example of one of the hydraulically activated security plate type barriers. This barrier is 31 inches high and comes in a standard width of 10 feet (other widths are also available). Normal operation is 4 to 8 seconds (field-adjustable). This barrier has been crash tested. A 14,980-pound (6,800-kg) vehicle traveling at a velocity of 50.3 mph (80 km/h) failed to penetrate the barrier. For further details on this and other barriers shown in Figures 81 and 83, see the Navy Terrorist Vehicle Bomb Survivability Manual. To use Figures 81 and 82, identify the vehicle approach velocity and move upward to the curve associated with the vehicle weight at the given threat severity. Read across to determine the kinetic energy the barrier must resist. The kinetic energy capacities for the tested barriers shown are indicated by horizontal lines. The barriers will stop any kinetic energy below the associated horizontal lines. Vehicle barriers with capacities below that required to stop the threat vehicle will probably disable the vehicle, but the barrier will be penetrated. The vehicle will then continue moving toward the

facility and may approach close enough to cause damage on detonation of its explosives.

8.4.3 Retrofit Hardening of Existing Construction

8.4.3.1 Required Standoff for Level of Building Protection. Although the windows and doors can be changed for existing structures to increase their blast hardness, the only practical option for the rest of a building is to maintain the required standoff distance between the facility and the point of explosion, i.e., it is not normally practical to structurally harden existing walls, ceilings, etc. The Navy Terrorist Vehicle Bomb Survivability Manual provides a methodology to evaluate the vulnerability of existing structures to bomb blast and to establish the required standoff distance. The reader is referred there for details. Briefly, the maximum standoff distance that can be attained for a given site is established first. Building components such as walls, interior and exterior columns, beams, joists, and roofs are then listed. For the blast design threat level, blast loading in various structural elements is evaluated using data such as that shown in Figure 77. Damage expected is then determined using diagrams as illustrated in Figure 84. The standoff distance can be iterated to obtain a tolerable level of damage. Figure 84 shows a typical example of the rebuild/repair criteria for charge weight versus standoff distance of a typical building. The "rebuild" condition is left of the solid line. The "repair" condition is right of the line. The numerical values on the chart (not on the axes) are percent of damage value, i.e., the further one is away from the solid line, the less the damage.

8.4.3.2 Vehicle Barriers. Vehicle barrier options for existing construction are the same as for new construction, see par. 8.4.2.2.

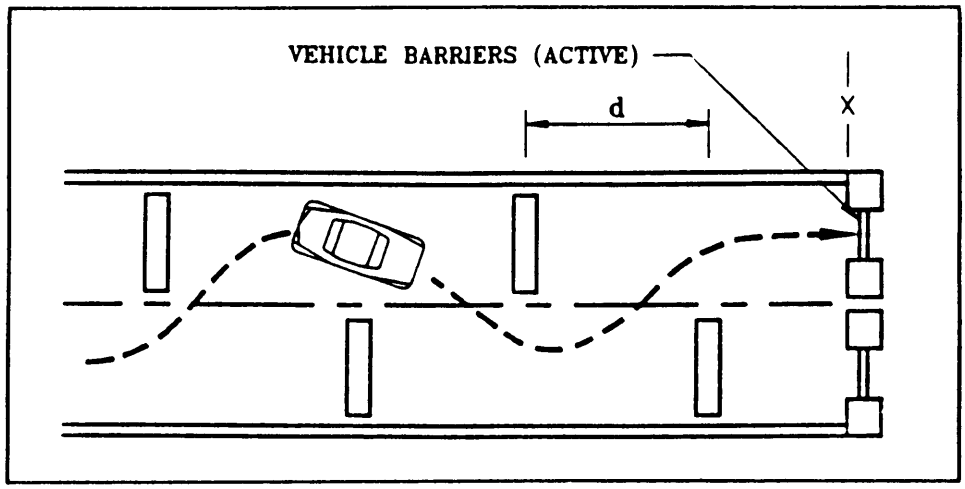


Figure 80
Application of Traffic Obstacles

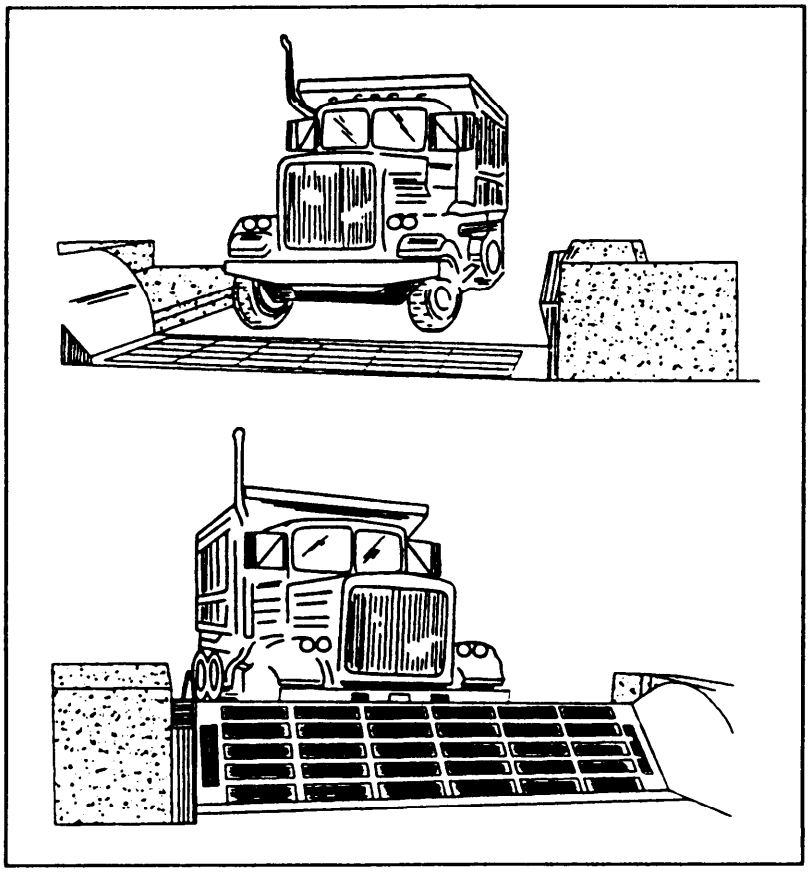


Figure 81
Security Barrier

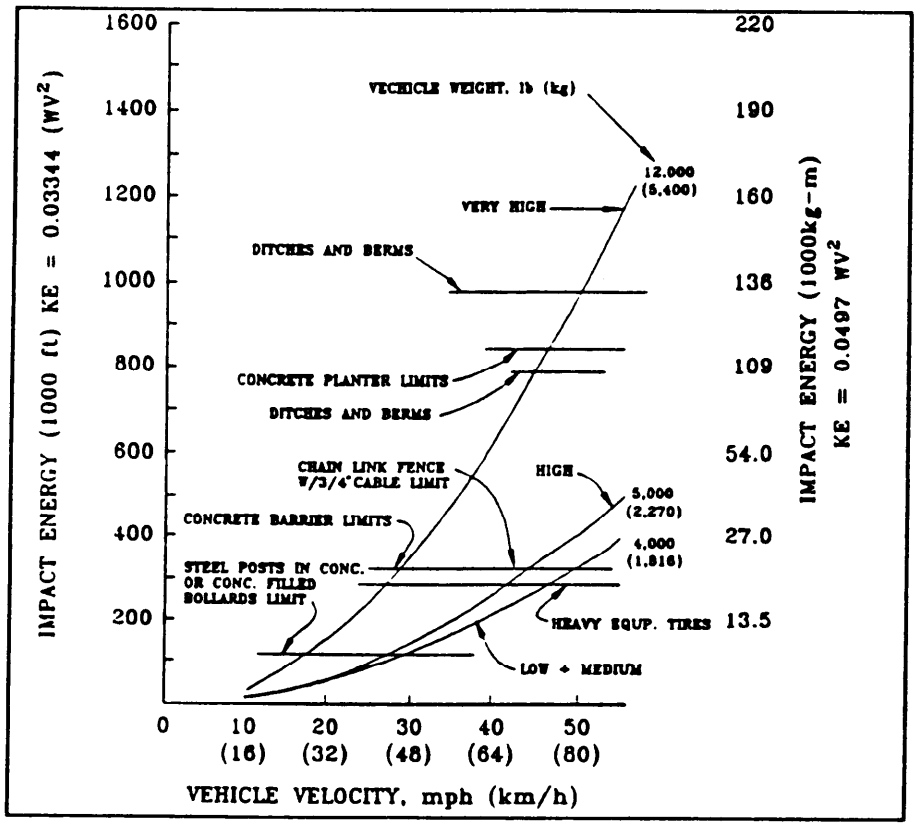


Figure 82
Moving Vehicle Impact Energy Versus Velocity
(Passive Barriers)

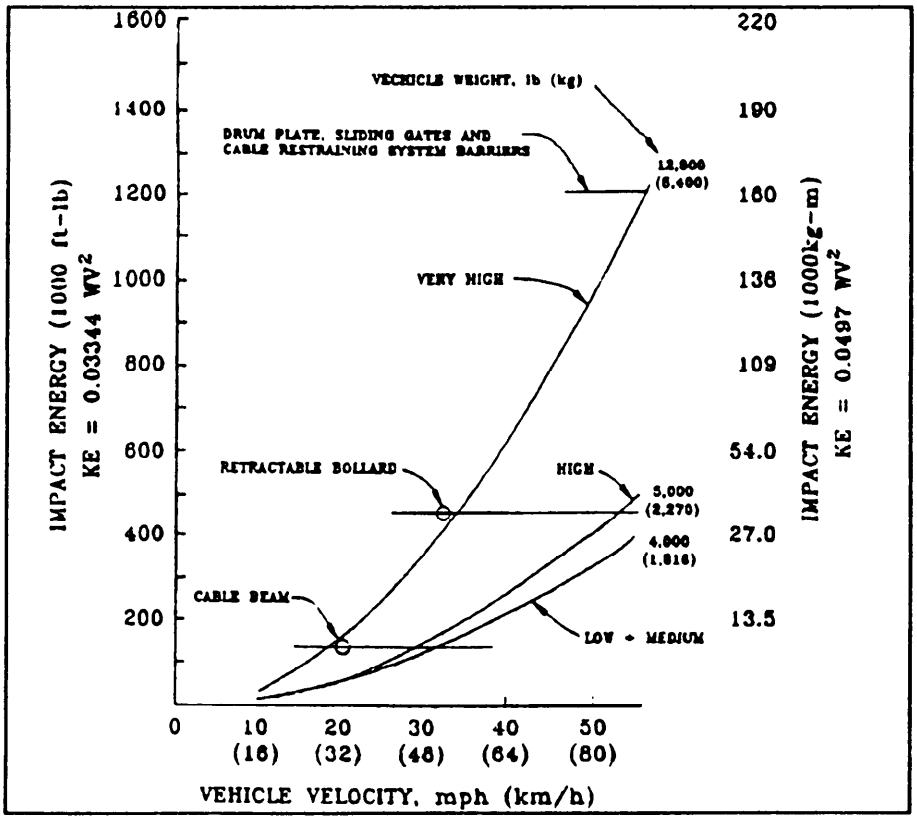


Figure 83
Moving Vehicle Impact Energy Versus Velocity (Active Barriers).

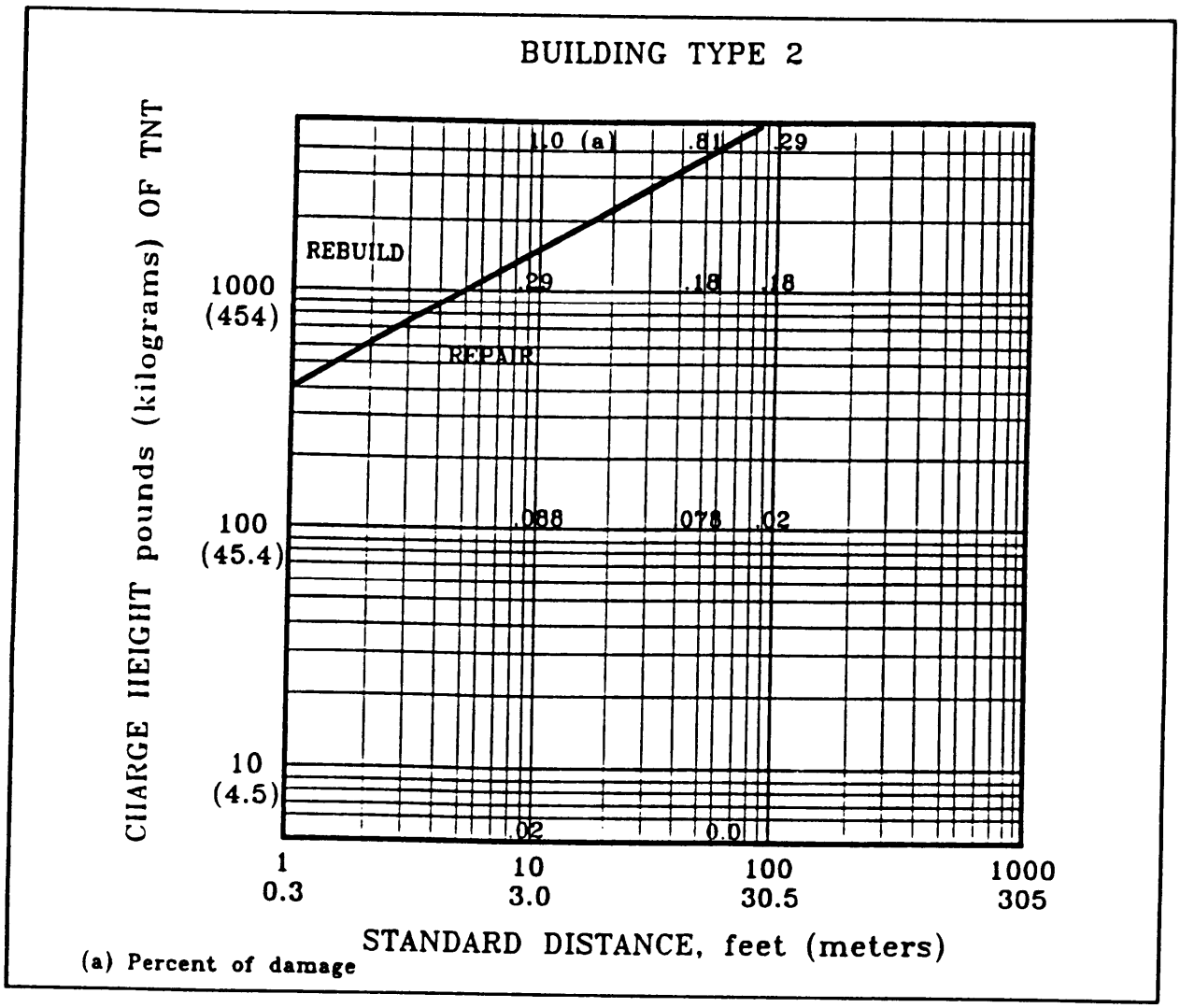


Figure 84
Repair Levels Versus Standoff Distance For Various Charge Weights

APPENDIX A

PHYSICAL SECURITY DESIGN WORKSHEETS

This Appendix contains worksheets to be used with the security design procedure described in par. 3.4.

Table A-1 is a worksheet applicable to the design of a new facility, and Table A-2 to the retrofit of an existing facility. These worksheets provide a format for entering and evaluating site and building construction options with corresponding penetration times and ingress/egress times to allow comparison to guard response times.

TABLE A-1.

Worksheet For New Building Construction

(1) Project Number: _____

(2) Project Name: _____

(3) Design Threat (check appropriate box):

Type	Severity			
	Low	Medium	High	Very High
Car/Truck Explosives				
Stationary Bombs				
Standoff Weapons				
Ballistics				
Forced Entry				
Covert Entry				

(4) Minimum Delay Time Required To Match Threat Assessment and Guard Response: [ ] (4)

TABLE A-1.

Worksheet For New Building Construction (continued)

(A) Layer of Defense	(B) Building Component	(C) Construction Description	(D) Component Penetration Time (Minutes)	(E)	(F)
Interior Layer 1	Wall				
	Door				
	Window				
	Floor				
	Ceiling				
	Utility Opening				
	Minimum Penetration Time (From Col. D) Over All Components				
	Ingress Time From Previous Layer				
	Egress Time To Next Layer				
	Layer Total				(5)

TABLE A-1.

Worksheet For New Building Construction (continued)

(A) Layer of Defense	(B) Building Component	(C) Construction Description	(D) Component Penetration Time (Minutes)
Interior Layer 2	Wall		
	Door		
	Window		
	Floor		
	Ceiling		
	Utility Opening		

	(E)
Minimum Penetration Time Over All Components	
Ingress Time From Previous Layer	
Egress Time To Next Layer	
Layer Total	(F) (6)

TABLE A-1.

Worksheet For New Building Construction (continued)

(A) Layer of Defense	(B) Building Component	(C) Construction Description	(D) Component Penetration Time (Minutes)
Interior Layer 3	Wall		
	Door		
	Window		
	Floor		
	Ceiling		
	Utility Opening		

	(E)
Minimum Penetration Time Over All Components	
Ingress Time From Previous Layer	
Egress Time To Next Layer	
Layer Total	(F) (7)

TABLE A-1.

Worksheet For New Building Construction (continued)

(A) Layer of Defense	(B) Building Component	(C) Construction Description	(D) Component Penetration Time (Minutes)
Facility Exterior	Wall		
	Door		
	Window		
	Floor		
	Roof		
	Utility Opening		

	(E)	(F)
Minimum Penetration Time Over All Components		
Ingress Time From Site Perimeter		
Egress Time To Site Perimeter		
Total		(8)

TABLE A-1.

Worksheet For New Building Construction (continued)

(A) Layer of Defense	(B) Building Component	(C) Construction Description	(E) Minimum Penetration Time (Minutes)	(F) Total Penetration Time (Minutes)	
Site Perimeter	Fence		Negligible	Negligible	(9)

Total Delay Time Provided (4) + (5) + (6) + (7) + (8) + (9)		(10)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building

(1) Project Number: _____

(2) Project Name: _____

(3) Design Threat (*check appropriate box*):

Type	Severity			
	Low	Medium	High	Very High
Car/Truck Explosives				
Stationary Bombs				
Standoff Weapons				
Ballistics				
Forced Entry				
Covert Entry				

(4) Minimum Delay Time Required To Match Threat Assessment and Guard Response: [ ] (4)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building (continued)

(A) Layer of Defense	(B) Building Component		Construction Description	Penetration Time (Minutes)	(G) Total Penetration Time (D)+(F)
Interior Layer 1	Wall	Existing	(C)	(D)	
		Retrofit	(E)	(F)	
	Door	Existing			
		Retrofit			
	Window	Existing			
		Retrofit			
	Floor	Existing			
		Retrofit			
	Ceiling	Existing			
		Retrofit			
	Utility Opening	Existing			
		Retrofit			

	(H)	(I)
Minimum Total Penetration Time (From Column G) Over All Components (Minutes)		
Ingress Time From Previous Layer		
Egress Time To Next Layer		
Layer Total		(5)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building (continued) Page 3 of 6

(A) Layer of Defense	(B) Building Component		Construction Description	Penetration Time (Minutes)	(G) Total Penetration Time (D)+(F)
Interior Layer 2	Wall	Existing	(C)	(D)	
		Retrofit	(E)	(F)	
	Door	Existing			
		Retrofit			
	Window	Existing			
		Retrofit			
	Floor	Existing			
		Retrofit			
	Ceiling	Existing			
		Retrofit			
	Utility Opening	Existing			
		Retrofit			

Minimum Total Penetration Time Over All Components (Minutes)	(H)	
Ingress Time From Previous Layer		
Egress Time To Next Layer		(I)
Layer Total		(6)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building (continued)

(A) Layer of Defense	(B) Building Component		Construction Description	Penetration Time (Minutes)	(G) Total Penetration Time (D)+(F)
Interior Layer 3	Wall	Existing	(C)	(D)	
		Retrofit	(E)	(F)	
	Door	Existing			
		Retrofit			
	Window	Existing			
		Retrofit			
	Floor	Existing			
		Retrofit			
	Ceiling	Existing			
		Retrofit			
	Utility Opening	Existing			
		Retrofit			

	(H)	(I)
Minimum Total Penetration Time Over All Components (Minutes)		
Ingress Time From Previous Layer		
Egress Time To Next Layer		
Layer Total		(7)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building (continued)

(A) Layer of Defense	(B) Building Component		Construction Description	Penetration Time (Minutes)	(G) Total Penetration Time (D)+(F)
Facility Exterior	Wall	Existing	(C)	(D)	
		Retrofit	(E)	(F)	
	Door	Existing			
		Retrofit			
	Window	Existing			
		Retrofit			
	Floor	Existing			
		Retrofit			
	Roof	Existing			
		Retrofit			
	Utility Opening	Existing			
		Retrofit			

	(H)	
Minimum Total Penetration Time Over All Components (Minutes)		
Ingress Time From Site Perimeter		
Egress Time To Site Perimeter		(I)
Total		(8)

TABLE A-2.

Worksheet For Retrofit Construction of Existing Building (continued)

(A) Layer of Defense	(B) Building Component	(C) Existing Construction Description	(H) Minimum Penetration Time (Minutes)	(I) Total Penetration Time (Minutes)	
Site Perimeter	Fence		Negligible	Negligible	(9)

Total Delay Time Provided (4) + (5) + (6) + (7) + (8) + (9)		(10)

BIBLIOGRAPHY

General Publications.

AA&E Physical Security Survey Team Technical Manual. Naval Ammunition Production Engineering Center, Crane, IN, 1980.

Access Delay Technology Transfer Manual, Volume I, SAND 87-1926. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Analytical Prediction and Experimental Verification of a One-Dimensional Shape Charge Computer Code for Linear Shaped Charged Applications, MRC-R-1060. Mission Research Corporation, Santa Barbara, CA.

Assessment of Various Constructional Materials as Armor for Protecting USN Shore Facilities Exposed to Small-Arms Fire, TN-1509. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Attack Resistance of Structural Components, TN-1425. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Attack Resistant Walls - Explosive Tests, TN-1510. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Attack Resistant Walls - Preliminary Tests, TN-1508. Naval Civil Engineering Laboratory, Port Hueneme, CA.

A Unified Theory of Penetration, Ballistic Research Laboratory. Defense Technical Information Center, Washington, DC.

Ballistic Materials and Penetration Mechanics, Volume 5, Methods and Phenomena: Their Applications in Science and Technology. Elsevier Scientific Publishing Company, New York, NY, 1980.

Ballistic Resistance of Police Body Armor, NIJ-STD-0101.02. Department of Justice, Washington, DC, 1985.

Barrier Penetration Tests, NBS 837. National Institute of Standards and Technology, Department of Commerce, Washington, DC.

Barrier Technology Handbook, SAND 77-077. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Belk, Judy V., Street Lighting Conversion Decision Not Lightly Reached. Public Works, Volume III, No. 3, Public Works, Sunnyvale, CA, 1980.

Blast Vulnerability Guide, SWRI 06-1473-210. Southwest Research Institute, 6220 Calebra Road, San Antonio, TX.

Bowers, B., Historical Review of Artificial Light Sources. Institute of Electrical Engineers Proc., Volume 127, Pt. A, No. 3, Piscataway, NJ, 1980.

Coaton, J. R., Tungsten-Halogen Lamps and Regenerative Mechanisms. Institute of Electrical Engineers Proc., Vol. 127, Pt. A, No. 3, Piscataway, NJ, 1980.

Concepts for Reducing Crime, Theft, and Destruction of Naval Shore Property, CR78.002. Westinghouse Electric Corporation, Arlington, VA, 1977.

Concepts for Secure Magazine Doors, TR-901. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Conceptual Framework for an Intelligent CAD Supported Physical Security Design System, MRC-R-1382. Mission Research Corporation, Santa Barbara, CA.

Department of the Navy, Operational Requirement (OR), 098-09-88, for Secure Structures Ashore, (Locks and Barriers), 1986.

DNA Magazine Door Relocking Hardware Development, TN-1559. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Double Fence Lighting for Maximum Security Institutions, DB 13024. Department of Public Works of Canada, 1974.

Entry-Control Systems Handbook, SAND 77-1033. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Evaluation of Reinforcement Techniques for Arms Rooms, Report 11-RD-80. VSE Corporation, Alexandria, VA.

Explosive Penetration of Concrete Walls, SAND 80-1942. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Extensions to SAM for Perimeter Fences, Exterior Intrusion Detection Sensors and New Construction Categories and Data, MRC-R-1341. Mission Research Corporation, Santa Barbara, CA.

Fainberg, A.; Bieber, A.M., Barrier Penetration Database. NUREG/CR-0181, Brookhaven National Library, Upton, NY, 1978.

Final Report: Barriers for Secure Structure Penetrations, CR 80.008. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Final Report: Intermediate Size Doors for Secure Structures, CR 80.007. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Final Report: Ordnance Structure Doors, Study of Forced Entry Resistant Doors and Other Barriers For Openings into Secure Structures, CR 80.009. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Fineberg, M. L.; Morgan, J. H.; Perry, M. E.; Woefel, J. C., Analysis and Testing Requirements for Perimeter Barriers and Lighting Developments. BDM/W-79-450-TR, BDM Corporation, McLean, VA, 1979.

Fire Protection Handbook. National Fire Protection Association, Batterymarch Park, Quincy, MA.

Fite, Robert A., Final Report Joint Services Perimeter Barrier Penetration Evaluation. Evaluation and Application Division of Lab 7000, MERADCOM, Fort Belvoir, VA, 1976.

Fite, Robert A., Joint Services Perimeter Barrier Penetration Evaluation. MERADCOM Report 2208, Fort Belvoir, VA, 1977.

Fry, Glenn A., The Use of the Luckiesh-Hoss Visibility Meter for Prescribing Illumination. Illuminating Engineering 7, 391-392, New York, NY, 1952.

Guide for the Security Assessment Model (SAM), MRC-R-1366. Mission Research Corporation, Santa Barbara, CA.

Implementation Plan for the Physical Security Evaluation Procedure Threat Determination Module, MRC-R-1265. Mission Research Corporation, Santa Barbara, CA.

Improvements to Program DESMAT for Evaluating Stand-off Weapon Protection Options, Volume I - Technical Discussion; Volume II - FORTRAN Listing, MRC-R-1244. Mission Research Corporation, Santa Barbara, CA.

Improving Structural Barrier Attack Resistance for Physical Security - Material Property Sensitivities, Data Availability Analysis and Testing Requirements an Evaluation Methodology, MRC-R-954. Mission Research Corporation, Santa Barbara, CA.

Initial Measurements of Specific Grinding Energy for the Abrasive Saw Attack of Candidate Materials for Physical Security Barriers, MRC-R-1004. Mission Research Corporation, Santa Barbara, CA.

Initial Tests of Thermal Degradation of Polymer Concrete in a High Temperature Environment, MRC-R-1005. Mission Research Corporation, Santa Barbara, CA.

Integration of a Shape Charge Computer Code Into Program DESMAT, MRC-R-1003. Mission Research Corporation, Santa Barbara, CA.

Intrusion Detection Systems Handbook, SAND 76-0554. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Jack, A. G.; Vrenken, L. E., Fluorescent Lamps and Low Pressure Sodium Lamps. Institute of Electrical Engineers Proc., Vol. 127, Pt. A,, No. 3, Piscataway, NJ, 1980.

Kramer, J. J., The Role of Behavioral Science in Physical Security. NBS Special Publication 480-32, National Bureau of Standards, Department of Commerce, Washington, DC, 1978.

Life Safety Code Handbook. National Fire Protection Association, Batterymarch Park, Quincy, MA.

Management Guidance Institute, Inc., Final Report, Survey of Current Status and Plans for the Installation of Vehicle Crash Resistant Barriers at U.S. Navy and U.S. Marine Corps Facilities Worldwide. Naval Civil Engineering Laboratory P.O. N62583/84 M R215, November 9, 1984.

Material Retrofit Options to Prevent RPG Penetration of a Reinforced Concrete Wall, MRC-R-1056. Mission Research Corporation, Santa Barbara, CA.

Meguire, P. G.; Kramer, J. J., Psychological Deterrents to Nuclear Theft: A Preliminary Literature Review and Bibliography. NBSIR76-1007, Law Enforcement Standards Laboratory, National Bureau of Standards, Department of Commerce, Washington, DC, 1976.

Meguire, P. G.; Kramer, J. J.; Stewart, A., Security Lighting for Nuclear Weapons Storage Sites: A Literature Review and Bibliography. NBS Special Publication 480-77. National Bureau of Standards, Department of Commerce, Washington, DC, 1977.

Moore, Raymond T., DNA/NBS/Crane NAD Barrier Tests. NBSIR 74-528, National Bureau of Standards, Department of Commerce, Washington, DC, 1974.

Moore, Raymond T., Penetration Resistance Tests of Reinforced Concrete Barriers. NBSIR 73-101. National Bureau of Standards, Department of Commerce, Washington, DC, 1972.

Morse, George P.; Morse, Robert F.; Schreiber, Albert L., Integration of Physical Strategies for Crime and Loss Prevention into the Naval Facilities Planning and Design Code. George P. Morse and Associates, Silver Spring, MA, 1979.

Morse, George P.; Morse, Robert F.; Woodrum, David L.; Ayd, Richard A., Architectural Planning for Crime and Loss Prevention as Applied to Major Hospital Complexes. George P. Morse and Associates, Silver Spring, MA, 1979.

Munk, Robert P., Physical Security Threats to be Reflected in the Design of Naval Shore Facilities. P-00001; N62474-79-C-5444, Science Applications, Inc., La Jolla, CA, 1980.

Munk, Robert P., Study of Forced Entry Resistant Doors and Other Barriers for Openings into Secure Structures - Final Report: Barriers for Secure Structure Penetrations. CR 80.008, Science Applications, Inc., La Jolla, CA, 1980.

Munk, Robert P., Study of Forced Entry Resistant Doors and Other Barriers for Openings into Secure Structures - Final Report: Intermediate Size Doors for Secure Structures. CR 80.007, Science Applications, Inc., La Jolla, CA, 1980.

Munk, Robert P., Waine, Donald, Study of Forced Entry Resistant Doors and New DESMAT Code Incorporating a Flyer Plate Attack Model, MRC-N-839. Mission Research Corporation, Santa Barbara, CA.

Naval Pier Lighting Criteria, MRC-N-871. Mission Research Corporation, Santa Barbara, CA.

Odello, Robert J., Attack Resistant Walls - Explosive Tests, N-1510. Civil Engineering Laboratory, Port Hueneme, CA, 1977.

Other Barriers for Openings into Secure Structures - Final Report: Ordnance Structure Doors. CR 80.009, Science Applications, Inc., La Jolla, CA, 1980.

Patton, James B.; Wenzel, Alex B., Testing and Evaluation of Attack Resistance and Hardening Retrofits of Marine Barrack Construction Types to Small Arms Multiple Impact Threat. CR 80-025, Southwest Research Institute, San Antonio, TX, 1980.

Pereira, P. E., Dodge Construction System Costs 1981. McGraw Hill Information Systems Company, New York, NY, 1980.

Phase I Final Report - Integrated Ballistic Casualty Reduction and Protection Model, MRC-COM-R-91-283(R1). Mission Research Corporation, Santa Barbara, CA.

Pier Lighting Requirements Test Program Final Report, MRC-R-1235. Mission Research Corporation, Santa Barbara, CA.

Pietrzak, L. M.; Caldwell, J. D.; Chamberlin, J.; Hawxhurst, J. P.; Sjovold, A., A Physical Security Requirements Assessment Methodology Definition, Feasibility, Assessment, and Development Plan. MRC-R-651, Mission Research Corporation, Santa Barbara, CA, Sep 1981.

Pietrzak, L. M., Improving Structural Barrier Attack Resistance for Physical Security--Identification of Applicable Scientific Theories and Mathematical Models, prepared for Naval Civil Engineering Laboratory, Port Hueneme, CA, Mission Research Corporation, Apr 1982.

Portable Ballistic Shields. NILECJ-STD-0103.00, Department of Justice, Washington, DC, May 1974.

Real Property Manual, Vol. 8. Fire Protection Program, MCO P11000.11A. United States Marine Corps, Quantico, VA.

Recommended Revisions to Navy Facility Planning Procedures to Incorporate Physical Security, CR 81.022. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Security Assessment Model Version 2.0, Volume I-Basic Concepts, Assumptions and Algorithms, MRC-R-1431. Mission Research Corporation, Santa Barbara, CA.

Security Assessment Model Version 2.0, Volume II-Software Documentation, MRC-R-1426. Mission Research Corporation, Santa Barbara, CA.

Security Requirements for Structural Elements used in Secure Structures, TR-908. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Security, Vehicle Barriers, SAND 84-2593. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Self, H.; Gray, K.; Cohn, B.; Backes, W., Emergency Exiting from Secure Navy Spaces: Studies of the Implications of the Life Safety Code, Security Regulations, and Human Factors Engineering. N-1536, Civil Engineering Laboratory, Port Hueneme, CA, 1978.

Southwest Research Institute, San Antonio, Texas, Test Report of the DSC TT207S Vehicle Barriers, Test D-1, Nov 1985.

Southwest Research Institute, San Antonio, Texas, Test Report of the DSC TT210 Hydraulic Bollard, Test D-2, Apr 1986.

Standard for Burglary Resistant Vault Doors and Modular Panels, ANSI/UL 608-1988. American National Standards Institute/Underwriters Laboratories (ANSI/UL), New York, NY.

Standard Practice for the Use of Metric (SI) Units in Building Design and Construction (Committee E-6 supplement to E-380). ANSI/ASTM E621-78, American Society for Testing and Materials, Philadelphia, PA, Jan 1978.

Study of Forced Entry Resistent Doors and Other Barriers for Openings into Secure Structures - Venting Provisions in Earth Covered Magazines, CR 80.017. Naval Civil Engineering Laboratory, Port Hueneme, CA.

Test Report: Extreme Environmental and Ballistic Impact Tests of Transparent Armor. H.P. White Laboratory, Inc., Street, MD, Jan 1980.

Test Report: Firing of M-16 Rifle Against Various Forms of Wall Construction. Detroit Bullet Trap Corporation, Schaumsburg, IL, Apr 1980.

U.S. Army, Field Circular 19-112, Use of Barriers in Countering Terrorism Situations, Aug 1984.

Wall Projectile Tests, SAND 79-1332. Department of Energy, Sandia National Laboratories, Albuquerque, NM.

Weibel, W. A., Update on LPS: Lighting Design and Application. Vol. 7, No. 11, Illuminating Engineering Society, New York, NY, 1977.

Miscellaneous DOD Publications.

Air Force Regulation 207-1, AF-207-1. U.S. Air Force, Electronic Systems Division, Hanscom AFB, MA.

Architectural Acoustics, Design Manual DM1.03. Naval Facilities Engineering Command, Alexandria, VA, May 1985.

Bolt-on Installation and Checkout Procedures for the High-Security Hasp with or without Anti-Intrusion Bar Cover, MIL-HDBK-1013/3. Naval Facilities Engineering Command, Alexandria, VA, Jan 1988.

Combination Locks, MIL-HDBK-1013/8. Naval Facilities Engineering Command, Alexandria, VA, Dec 1989.

Department of the Navy Information and Personnel Security Program Regulation, OPNAVINST 5510.1G. Department of Navy, Washington, DC.

Department of the Navy Physical Security and Loss Prevention Manual, OPNAVINST 5530.14B. Department of Navy, Washington, DC.

DOD Ammunition and Explosives Safety Standards. DOD 5154.45, Department of Defense, Alexandria, VA.

Electrical Utilization Systems, MIL-HDBK-1004/4. Naval Facilities Engineering Command, Alexandria, VA, Oct 1987.

Facility Planning Criteria for Navy and Marine Corps Shore Installations, NAVFAC P-80, Naval Facilities Engineering Command, Alexandria, VA.

Fence, Chain Link, NFGS-02831D. Naval Facilities Engineering Command, Alexandria, VA, Jun 1992.

Industrial Security Manual for Safeguarding Classified Information, DOD 5220.22-M. Department of Defense, Washington, DC.

Naval Ship's Technical Manual. Chapter 604 Locks, Keys, and Hasps. NAVSEA S9069-UK-STM-010. Naval Sea Systems Command, Washington, DC, Second Revision.

Navy Nuclear Weapon Security Manual, OPNAVINST C8126.1. Department of Navy, Washington, DC.

Nuclear Weapon Storage Facilities Handbook. Defense Nuclear Agency Publication, Washington, DC.

Physical Security, Field Manual No. 19-30. Headquarters, Department of the Army, Washington, DC.

Physical Security Instruction for Sensitive Conventional Arms, Ammunition, and Explosives (AA&E), OPNAVINST 5530.13A. Department of Navy, Washington, DC.

Policy and Procedure for Definitive and Standard Design and Standard Specification Preparation, MIL-HDBK-1006/4. Naval Facilities Engineering Command, Alexandria, VA, Jul 1987.

Policy and Procedure for Engineering and Design Criteria Manual Preparation, MIL-HDBK-1006/3B. Naval Facilities Engineering Command, Alexandria, VA, Oct 1990.

Preparation of Supporting Documents for Proposed Military Construction Program Projects. NAVFACINST 11010.32F, Naval Facilities Engineering Command, Alexandria, VA.

Publishing for the Naval Facilities Engineering Command, NAVFAC P-346, Parts 1 and 2, Naval Facilities Engineering Command, Alexandria, VA.

Securing of Emergency Exit Doors, NAVINST 11012.142. Naval Facilities Engineering Command, Alexandria, VA.

Security Hardware Installation, Operation, and Maintenance, MIL-HDBK-1013/7. Naval Facilities Engineering Command, Alexandria, VA, Jan 1988.

Security Measures in the Planning and Design of Nuclear Weapons Facilities, NAVFACINST 11012.134B. Naval Facilities Engineering Command, Alexandria, VA.

Shore Facilities Planning Manual, NAVFACINST 11010.44. Naval Facilities Engineering Command, Alexandria, VA.

Use of the Metric System of Measurement in the Acquisition of Facilities and Related Equipment, NAVFACINST 4120.10. Naval Facilities Engineering Command, Alexandria, VA.

both conventional and systems type functional/coordinated design.

Specifications and Standards.

Federal Specification: Padlock, Changeable Combination (Resistant to Opening by Manipulation and Surreptitious Attack). FF-P-110F, Amend-2, General Service Administration.

Federal Standard: Glass, Float or Plate, Sheet, Figures (Flat, for Glazing Mirrors, and Other Uses), DD-G-451.

Federal Standard: Glass, Float, Sheet, Figures, Coated (Heat-Strengthened and Tempered), DD-G-1403.

Federal Standard: Grating Metal Bar Type (Floor, Except for Naval Vessels), RR-G-661E.

Federal Standard: Grating, Metal, Other Than Bar Type (Floor, Except for Naval Vessels), RR-G-1602.

Military Specification: Aluminum Alloy Armor, 2219 Rolled Plate and Die Forged Shapes. MIL-A-46118G (MR), Department of the Army, Watertown, MA.

Military Specification: Armor Plate, Aluminum Alloy, 7039. MIL-A-46063E, Amend-4, Department of the Army, Watertown, MA.

Military Specification: Armor Plate, Aluminum Alloy, Weldable, 5083 and 5456. MIL-A-46027G (MR), Department of the Army, Watertown, MA.

Military Specification: Armor Steel, Roll-Bonded, Dual-Hardness. MIL-A-46099B, Department of the Army, Watertown, MA.

Military Specification: Armor Plate, Steel, Wrought High-Hardness. MIL-A-46100C, Amend-1, Department of the Army, Watertown, MA.

Military Specification: Armor Plate, Steel, Wrought, Homogeneous (For Use in and for Combat-Vehicles and for Ammunition Testing.) MIL-A-12656G (MR), Amend-1, Department of the Army, Watertown, MA.

Military Specification: Armor Plate, Titanium Alloy, Weldable. MIL-A-46077D, Department of the Army, Watertown, MA.

Military Specification: Armor, Steel, Cast, Homogeneous, Combat-Vehicle Type (1/4 to 8 inches, Inclusive) MIL-A-11356E, Amend-2, (MR), Department of the Army, Watertown, MA.

Military Specification: Armor, Steel, Plate, Wrought, (ESR) (3/16 through 3 inches, Inclusive). MIL-A-46173(MR), Department of the Army, Watertown, MA.

Military Specification: Armor, Steel: Sheet, Strip, and Fabricated Forms; Rolled, Non-Magnetic; for Helmets and Personnel Armor Requirements. MIL-A-13259B (MR), Department of the Army, Watertown, MA.

Military Specification: Glass: Laminated, Flat, Bullet-Resistant. MIL-G-5485C, Department of the Army, Watertown, MA.

Military Specification: Hasps, High Security Padlocks: General Specifications For. MIL-H-43905B, U.S. Army Natick Research and Development Command.

Military Specification: Metric Machinery/Equipment, Requirements For. DOD-M-24680, Amend-1, Department of Defense, Washington, DC.

Military Standard: Metric System, Application in New Design. DOD-STD-1476, Department of Defense, Washington, DC.

REFERENCES

NOTE: THE FOLLOWING REFERENCED DOCUMENTS FORM A PART OF THIS HANDBOOK TO THE EXTENT SPECIFIED HEREIN. USERS OF THIS HANDBOOK SHOULD REFER TO THE LATEST REVISIONS OF CITED DOCUMENTS UNLESS OTHERWISE DIRECTED.

American National Standards Institute, 1430 Broadway, New York, NY, 10018.

ANSI/BHMA 156.1-1988	Butts and Hinges
ANSI/BHMA 156.3-1989	Exit Devices
ANSI/BHMA 156.5-1984	Auxiliary Locks and Associated Products
ANSI/BHMA 156.6-1986	Architectural Door Trim
ANSI/BHMA 156.13-1987	Locks and Latches, Mortise
ANSI/UL 7S2-1985	Bullet Resistant Equipment

American Society for Testing and Materials, 1916 Race Street, Philadelphia, PA 19103-1187.

ASTM A569-91 Standard Specification for Steel, Carbon (0.15% Max.), Hot-Rolled Sheet and Strip Commercial Quality

ASTM A589-89 Standard Specification for Seamless and Welded Carbon Steel Water Well Pipe

ASTM A607-92 Standard Specification for Steel, Sheet and Strip, High-Strength, Low Alloy, Columbium or Vanidium or Both, Hot Rolled and Cold Rolled

ASTM A750-88 Standard Specification for Steel Air Ventilation Grille Units for Detection Areas

Defense Intelligence Agency Publication available from Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

DIAM-50-3A Physical Security Standards for Sensitive Compartmental Information Facilities

Department of the Army available from National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161.

SL-88-39 Expendient Field Fortifications using Sand-Grid Construction, October 1988

Department of Defense Publications available from Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402.

DOD 4270.1-M	Policy Guidelines for Installation Planning, Design, Construction and Upkeep
DOD 5100.76-M	Physical Security of Conventional Arms, Ammunition, and Explosives
DOD 5200.8 (D)	Security of DOD Installations and Resources
DOD 5200.1-R	Information Security Program Regulation
DOD 5200.2-R	Personnel Security Program
DOD 5200.8-R	Physical Security Program
DOD 5210.41-M	Nuclear Weapons Security Manual
DOD 5230.24	Distribution Statements on Technical Documents

Department of Defense Specifications and Standards, Standardization Document Order Desk, Bldg 4D, 700 Robbins Ave, Philadelphia, PA 19111-5094.

MIL-S-12560H	Armor, Plate, Steel Wrought, Homogeneous
MIL-T-46077D	Armor, Plate, Titanium Alloy Weldable

Department of Energy/Sandia National Laboratories, Albuquerque, NM 87185-5800.

SAND 89-123	Exterior Intrusion Detection Systems Technology Transfer Manual
SAND 87-1927	Entry Control Systems Technology Transfer Manual
SAND 89-1924	Video Assessment Technology Transfer Manual

Department of State Specification available from Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

SD-STD-02.01	Vehicle Crash Barrier

Federal Specifications. Department of Defense activities may obtain copies from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

AA-D-00600C	Door, Vault Security (1 Dec 90)
AA-D-2757	Door, Vault Security (10 May 90)
AA-D-2737	Door, Vault Security (25 Apr 90)

Federal Standards. Department of Defense activities may obtain copies from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

RR-F-191/3D	Fencing, Wire and Post, Metal (Chain-Link Fence Posts, Top Rails, and Braces), (Detail Specification)
RR-F-191/K	Fencing, Wire and Post, Metal (and Gates, Chain-Link Fence Fabric, and Accessories), (General Specifications)

Hollow Metal Manufacturers Association, 600 South Federal Street, Chicago, IL 60605.

HMMA 810-87	Hollow Metal Doors
HMMA 820-87	Hollow Metal Frames
HMMA 830-87	Hardware Preparation and Locations for Hollow Metal Doors and Frames
HMMA 840-87	Installation and Storage of Hollow Metal Doors and Frames
HMMA 862-87	Guide Specifications for Commercial Security Hollow Metal Dooes and Frames
HMMA 863-87	Guide Specifications for Detection Security Hollow Metal Dooes and Frames

Illuminating Engineering Society (IES) of North America, New York, NY 10018.

IES Lighting Handbook, 1981.

Military Standards. Department of Defense activities may obtain copies from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

MIL-G-18014B	Gratings, Metal, Bar Type Flooring, Naval Shipyard
MIL-H-29181A	Hasp, High Security, Shrouded, for High and Medium Security Padlock
MIL-P-43607G	Padlock, Key Operated, High Security, Shrouded Shackle

Naval Civil Engineering Laboratory (NCEL), Port Hueneme, CA 93043.

CR 80.025	Testing and Evaluation of Attack Resistance and Hardening Retrofits of Marine Barrack Construction Types to Small Arms Multiple Impact Threat

Naval Facilities Engineering Command Publications available from Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.

Design Manual 13.02	Commercial Intrusion Detection Systems
MIL-HDBK-1008A	Fire Protection for Facilities Engineering, Design, and Construction
MIL-HDBK-1013/4	Instruction for Design Fabrication and Construction/Installation of Secure Structures
MIL-HDBK-1013/5	Steel Ply Wall Hardening Selection and Installation
MIL-HDBK-1013/6	High Security Internal Locking System Description, Operation, and Maintenance
MIL-HDBK-1013/10	Design Guidelines for Security Fencing, Gates, Barriers and Guard Facilities
MIL-HDBK-1013/11	Instruction for Planning and Design of High Security Magazine Door Construction Projects
MIL-HDBK-1190	Facility Planning and Design Guide
NFGS 16726C	Basic Intrusion Detection Systems
NFGS 16727C	Commercial Intrusion Detection Systems

United States Air Force, Electronic Systems Division, Air Force Systems Command, Hanscom AFB, MA 01731.

ESE-SIT-0001	Standardized Electronic Security Equipment Siting Criteria

United States Army Corps of Engineers, 215 North 17th Street, Omaha, NE 68102-4978.

Security Engineering Manual

United States Army Corps of Engineers Publications, Engineer Division (IDS-MCX), Huntsville, AL 35807.

CEGS 16751	Closed-Circuit Television Systems
CEGS 16752	Electronic Entry Control Systems
TM 5-853-4	Security Engineering, Electronic Security Systems

GLOSSARY

AA&E. Arms, Ammunition, and Explosives.

ANSI. American National Standards Institute.

ANSI/UL. American National Standards Institute/Underwriters Laboratories.

ASTM. American Society for Testing and Materials.

CCTV. Closed-Circuit Television.

CEGS. Corps of Engineers Guide Specification.

CMU. Concrete Masonry Unit.

CONUS. Continental United States.

DIAM. Defense Intelligence Agency Manual.

DOD. Department of Defense.

DOE. Department of Energy.

ECP. Entry Control Point.

GSA. General Services Administration.

HMMA. Hollow Metal Manufacturing Association.

HPSA. High Power Small Arms.

HPW. H.P. White Laboratory, Inc.

IDS. Intrusion Detection System.

KE. Kinetic Energy.

MFS. Microwave Fence Sensor.

MIL-HDBK. Military Handbook.

MPSA. Medium Power Small Arms.

NATO. North Atlantic Treaty Organization.

NAVFAC. Naval Facilities Engineering Command.

NCEL. Naval Civil Engineering Laboratory.

OCONUS. Outside Continental United States.

PCCS. Ported Coaxial Cable Sensor.

PDT. Penetration Delay Time.

POL. Petroleum, Oils, and Lubricants.

RPG. Rocket-Propelled Grenade.

SAMIT. Small Arms Multiple Impact Threat.

SCIF. Sensitive Compartmented Information Facility.

SFR. Steel-Fiber-Reinforced.

SNM. Special Nuclear Materials.

SPSA. Super Power Small Arms.

TNT. Trinitrotoluene.

U.S.. United States.

YTWS. Y Taut Wire Sensor.

tionally flexible as contingency situations, designs should be as func

SUBJECT INDEX

Page

A

Access Control 96
Entry Points 54, 68, 72
Arms, Ammunition, and Explosives 110
Asset Types 11
Attack Tools 93
Hand Tools 93
Power Tools 93
Thermal Tools 94
Explosive-Laden Vehicle 94

B

Ballistics 194
Barriers 95
Buildings 120
Vehicle 60, 231
Blast Hardening 121, 229

C

Ceilings
(See Roofs)
Clear Zone 60
Closed-Circuit TV (CCTV) 84, 103
Communications 91
Concrete Construction
(See Construction, concrete)
Construction, concrete
Roofs 129, 175
Floors 129, 175
Walls 124, 162
Construction, masonry
Walls 124, 169
Construction, metal
Roofs 181
Floors 181
Construction, stud/grit
Walls 170
Construction, wood

Page

Roofs and Floors 179

D

Design Team 22
Design Threat 7
Deterrence 24
Doors
Magazine Doors 146, 183
Personnel Doors 135, 182
Vault Doors 141, 182
Vehicle Doors 147, 182
Hinge-Side Protection 184
Ballistic Protection 204
Ducts
(See Utility Openings; Ventilation Openings)

E

Egress Time
Definition 32
Entry Points 54, 68, 72
Access Control 96

F

Fences 61
Floors
Metal 181
Reinforced Concrete 129, 175
Wood 179

G

Gates 69

H

Hand Tools 93
Hardening
Ballistic Attack 194
Blast 226
Doors 135, 182
Fences 61

Page

Roofs and Floors
Metal 181
Reinforced Concrete 129, 175
Wood 179
Utility Openings 155
Walls
Reinforced Concrete 122, 162
Reinforced Masonry 124, 169
Stud/Girt 170
Windows 151
High Power Rifle Threat, ANSI/UL
Definition 198
Hardening 198

I

Illumination
(See also Lighting, exterior)
Continuous 87
Standby 88
Specifications 89
Ingress Time
Definition 32
Intrusion Detection Systems (IDS)
Definition 33
Exterior 75
Building 101

L

Layout, Building 95
Layout, Exterior
Entry Control Point 54, 72
Security Force Response 4, 56
Security Designated Areas 57
Lighting
CCTV and Surveillance 89
Energy Considerations 90
Restrike Time 91
Lighting Concepts
Continuous 87
Standby 88
Lighting Specifications 89
Locking Devices 134

Page

M

Man-Passable Opening
Definition 32
Manholes 155
Masonry
(See Construction, masonry)
Metal Construction
(See Construction, metal)
Military Threat
SAMIT 198
Hardening 198

N

Nuclear Weapons Facilities 116

O

Observation of Facility 55

P

Personnel (as a Threat) 9
Pipe Chases
(See Utility Openings)
Perimeter Barriers 60, 231

R

Restricted Area 33
Retrofit Hardening 161
Roll-up Doors 147
Rocket Propelled Grenade 214
Roofs
Metal 181
Reinforced Concrete 129, 175
Wood 179

S

Small Arms Multiple Impact Threat (SAMIT)
Definition 198
Hardening 198
Small Arms Threat, ANSI/UL
Definition 198
Hardening 198

Page

Standoff Weapons 214
Strongrooms 110

T

Tactics (Threat) 10
Threat
    Attack Tools 7
    Ballistics 194
    Bomb 226
    Levels 93
    Objectives 9
    Tactics 10
    Types 9
    Selection 11
Tools
    (See Attack Tools)
Tunnels
    (See Utility Openings)

U

Utility Openings 155
    Ducts 157
    Exhaust Vents 159
    Filter Banks 160
    Gravity Vents 158
    Pipe Chases 155
    Manholes 155
    Sleeves and Trays 156
    AA&E Ventilation Openings 186

V

Vaults 105
    Class A 105
    Class B 108
Vehicle Barriers 60, 231
Ventilation Openings
    (See Utility Openings)
Vents
    (See Utility Openings; Ventilation
    Openings)

Therefore, during the process of planning MTFs, a complete range of

Page

W

Walls
Masonry 169
Reinforced concrete 122, 162
Stud/Girt 170
Windows 151, 186
Bars and Grills 151
Ballistic Protection 206
Wood Construction
(See Construction, wood)
Worksheets 238

CUSTODIAN:
NAVY - YD2

PREPARING ACTIVITY
NAVY - YD2

PROJECT NO.
FACR-1117

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-HDBK-1013/1A	2. DOCUMENT DATE (YYMMDD) 931215

3. DOCUMENT TITLE
DESIGN GUIDELINES FOR PHYSICAL SECURITY OF FACILITIES

4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (Last, First, Middle Initial)	b. ORGANIZATION	
c. ADDRESS (Include Zip Code)	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON (If applicable)	7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME	b. TELEPHONE (Include Area Code)	
	(1) Commercial	(2) AUTOVON
COMMANDING OFFICER NAVAL FACILITIES ENGINEERING SERVICE CENTER	(805) 982-9640	551-9640
c. ADDRESS (Include Zip Code) ATTN CODE ESC12 560 CENTER DRIVE PORT HUENEME, CA 93043-4328	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340	

DD Form 1426, OCT 89 *Previous editions are obsolete.* 198/290