UFC 4-020-01 Security Engineering Facilities Planning Manual

John Lynch, P.E. and Julie Heup, P.E.
Planning, Design and Construction Criteria (PDCC)
Engineering Criteria and Programs

October 2024

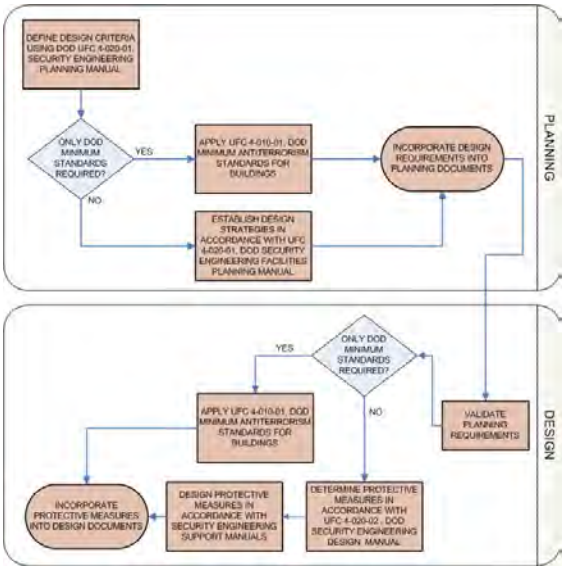
Problems

- Funding for protection measures is often not budgeted during project planning
- Security is often considered late in design
- Adding protection measures to completed facilities is difficult and expensive
- Security is often not geared to specific threat
- Existing security is geared to mission assets, not always effective for terrorist targets

SECURITY ENGINEERING UFC SERIES

- **SECURITY ENGINEERING UFC SERIES.** Unified Facilities Criteria documents that cover minimum standards, planning, preliminary design, and detailed design for security and antiterrorism. The manuals in this series are designed to be used sequentially by a diverse audience to facilitate development of projects throughout the planning and design cycle.
  - ➢ The manuals in this series include the following:
    - ❑ DoD Minimum Antiterrorism Standards for Buildings.
    - ❑ Security Engineering Facilities Planning Manual.
    - ❑ Security Engineering Facilities Design Manual.
    - ❑ Security Engineering Support Manuals.

SECURITY ENGINEERING UFC SERIES



Project Development

- **<u>Project Planning:</u> incorporate AT and Physical Security requirements and their associated costs into the project scope and budget.**

- **Work with our clients to:**
  - Determine Asset to be protected
  - Define building occupancy (low occupancy/inhabited building)
  - Identify site constraints
  - Validate Design Basis Threat (DBT) as determined by Installation or Regional AT/Security Personnel
  - Determine appropriate level of protection

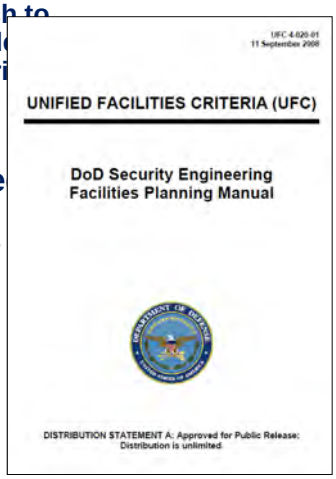
- **MUST BE DONE DURING PROJECT PLANNING**

UFC 4-020-01, SECURITY ENGINNEERING FACILITIES PLANNING MANUAL

- **Purpose:**
  - **To provide a unified risk based approach to support planning of projects that includ requirements for security and antiterrori protective measures.**

- **Lead Agency: Army Corps of Engine**
  - **Point of contact: Curt Betts**
    Protective Design Center

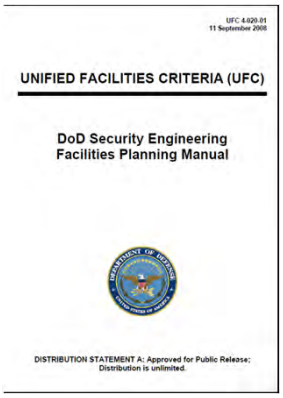
- **Current Document Status:**
  - **Published September 2008**
  - **Under Major Revision**



UFC 4-020-01, SECURITY ENGINNEEING FACILITIES PLANNING MANUAL

- Chap 1 INTRODUCTION
- Chap 2 AGGRESSOR THREAT AND TACTICS
- Chap 3 DESIGN CRITERIA DEVELOPMENT
- Chap 4 DESIGN STRATEGIES
- Chap 5 MASTER PLANNING CONSIDERATIONS
- Chap 6 PROJECT COST DEVELOPMENT

- GLOSSARY
- APPENDIX A NEW CONSTRUCTION COST TABLES
- APPENDIX B RETROFIT CONSTRUCTION COST TABLES
- APPENDIX C CONSOLIDATED CONSTRCUTION COMPONENT TABLES
- APPENDIX D EXPEDITIONARY CONSTRUCTION COSTS
- APPENDIX E BLANK WORKSHEETS



CHAPTER 1 INTRODUCTION

- PURPOSE: The purpose of this UFC is to support planning of projects that include requirements for security and antiterrorism.
- APPLICABILITY: New construction, existing construction or expeditionary and temporary construction.
- INTENDED USERS: Engineering planners responsible for project development and planning teams responsible for developing design criteria for projects.
- The goal is to develop appropriate, effective, unobtrusive, and economical protective designs to a level appropriate for project programming and to provide commanders with the information they need to allocate resources.

CHAPTER 1 INTRODUCTION
PLANNING TEAM

- The planning team
  - Facility User
  - Antiterrorism Officer
  - Intelligence
  - Operations
  - Security Officer
  - Logistics
  - Engineering
  - Resource Management
  - Others as required

CHAPTER 1 INTRODUCTION
PLANNING TEAM

- The planning team must:
  - Understand related DoD/Service policy/regulations
  - Understand the objectives of the system
  - Understand the facility and user's operational requirements and limitations.
  - Understand the security force's capabilities
  - Determine the Design Basis Threat
  - Determine the Level of Protection
  - Budget for protection measures

CHAPTER 1 INTRODUCTION OTHER REQUIRMENTS

- **INTEGRATING OTHER REQUIRMENTS:**
  - **Security Regulations: DoD and Service policy and regulations establish baseline requirements for protective measures**
  - **Explosive Safety: Explosive safety regulations may require high level of protection than required by security criteria**
  - **Other DoD Standards: DoD Minimum Standards for Buildings, COCOM OP ORDS**
  - **Historic Preservation: Implementation of security and antiterrorism protective measures cannot supersede the obligation to protect cultural resources**
  - **Sustainable Design: Security and antiterrorism protective measures may pose challenges for sustainable design, but the two are not mutually exclusive.**
  - **Other Facility Requirements: Life Safety, seismic criteria, barrier-free access, and aesthetics may conflict with objectives of protective systems. Planning team must be aware of conflicts and set priorities.**

CHAPTER 2 – AGGRESSOR THREATS AND TACTIC

- **AGGRESSORS:** Aggressors are people who perform hostile acts against assets such as equipment, personnel, and operations.
- **AGGRESSOR OBJECTIVES:** There are four major aggressor objectives that describe aggressor behavior. Aggressors may use the first three objectives to accomplish the fourth. The four aggressor objectives include:
  - Inflicting injury or death on people
  - Destroying or damaging facilities, property, equipment, or resources
  - Stealing equipment, materiel, or information
  - Creating adverse publicity
- **AGGRESSOR CATEGORIES:** There are four broad categories of aggressors considered in the planning manual:
  - Criminals
  - Protesters
  - Terrorists
  - Subversives

CHAPTER 2 – AGGRESSOR THREATS AND TACTIC

- **AGGRESSOR TACTICS:** Aggressors have historically employed a wide range of offensive strategies reflecting their capabilities and objectives. The security engineering series categorize these offensive strategies into 13 tactics that are specific methods of achieving aggressor goals.
  - **Moving Vehicle Bomb Tactic**
  - **Stationary Vehicle Bomb Tactic**
  - **Hand Delivered Device Tactic**
  - **Indirect Fire Weapons Tactic**
  - **Direct Fire Weapons Tactic**
  - **Forced Entry Tactic**
  - **Covert Entry Tactic**
  - **Visual Surveillance Tactic**
  - **Acoustic Eavesdropping Tactic**
  - **Electronic Emanations Eavesdropping Tactic**
  - **Airborne Contamination Tactic**
  - **Waterborne Contamination Tactic**
  - **Waterfront Attacks**

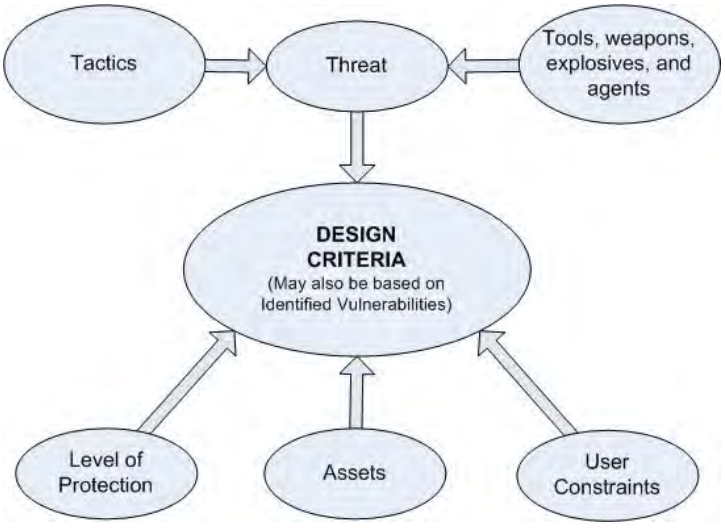
CHAPTER 2 – AGGRESSOR THREATS AND TACTIC

- **TOOLS, WEAPONS, EXPLOSIVES, AND AGENTS.** Aggressors use various tools, weapons, explosives, and agents to attain their objectives. The tools, weapons, explosives, and agents included discussed throughout the security engineering series of UFCs represent those that can be reasonably expected in the near future.
  - Specific tools, weapons, explosives, and agents associated with each tactic are identified in chapter 3 of this UFC. General descriptions of these tools, weapons, explosives, and agents are provided in chapter 2.
    - **Tools.** Tools are used to breach protective construction components or barriers and include:
      - **Forced Entry Tools**
      - **Vehicles**
      - **Watercraft**
      - **Surveillance Tools**
      - **False Credentials**
      - **Weapons**
      - **Explosives**
      - **Chemical, Biological, and Radiological Agents**

CHAPTER 3 – DESIGN CRITERIA DEVELOPMENT

- Chapter 3 provides a procedure to develop security engineering design criteria for facilities. The procedure:
  - Captures and applies inputs of the Planning Team.
  - Identifies assets and considers their value to the users
  - Evaluates the Likelihood aggressors will target them.
  - Evaluates preliminary design criteria using a risk/cost analysis.
- The Planning Team may adjust the preliminary design criteria to reflect the risk analysis or the funding required to implement the design criteria.
- The Planning Team may also adjust the criteria as necessary according to the professional judgments of the members of the team based on local and regional considerations.
- The resulting design criteria will be the basis for planning and preliminary design. It may be further adjusted during the design process based on the more detailed risk analysis process in UFC 4-020-02, ***Security Engineering Facility Design Manual (DRAFT).***

CHAPTER 3 – DESIGN CRITERIA DEVELOPMENT



Risk Level and Acceptability

- With Regard to the Planning Manual
  - Risk is relative
  - Used to compare alternatives
  - May be used for rudimentary benefit/cost analysis
- Refined in UFC 4-020-02, Security Engineering Design Manual (Draft)

$Risk = A_V \times T_{LH} \times (1-P_E)$

A_V = Asset value rating
T_{LH}=highest threat likelihood
P_E= effective protection factor
$1-P_E$ reflects "vulnerability"

Design Criteria Considerations

- Risk management
  - Cost
  - Relative risk increase or reduction
- Other criteria
  - Combatant Command "Standards"
  - DoD/Service regulatory requirements
  - Others such as seismic, wind, and building codes
- Priorities
- Integration

The Road Ahead

If you don't know where

you're going, any road

will get you there

The Problem

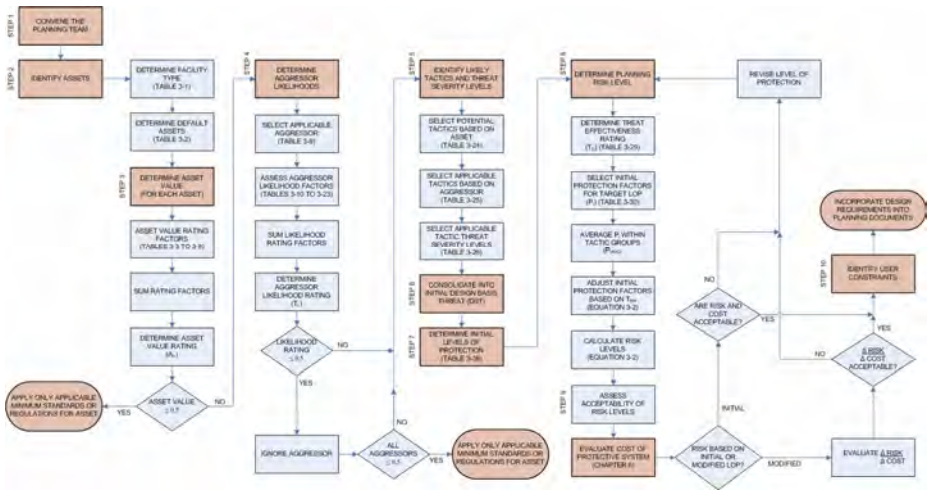
Background

- ARMY TM 5-853-1/AFMAN 32-1071, Vol. 1 (Project Development)
- CARVER
  - Criticality/Accessibility/Recuperability/Vulnerability/Effect on Population/Recognizability
- DSHARPP
  - Demographics/Symbolism/History/Accessibility/Recognizability/ Population/Proximity
- MSHARPP
  - Mission/Symbolism/History/Accessibility/Recognizability/ Population/Proximity
- NFESC QRAVA
  - Quantitative Risk Analysis and Vulnerability Assessment
- JAT Guide (Joint Antiterrorism)
- Others

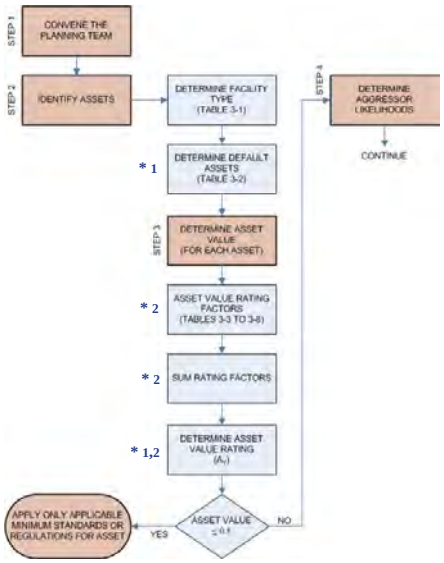
The Design Criteria Development Procedure
Major Steps

- Step 1: Convene the planning team
- Step 2: Identify assets
- Step 3: Determine asset value
- Step 4: Determine aggressor likelihoods
- Step 5: Identify likely tactics and threat severity levels
- Step 6: Consolidate into initial design basis threat
- Step 7: Determine Initial Levels of Protection
- Step 8: Determine planning risk level
- Step 9: Assess acceptability of risk levels
- Step 10: Identify user constraints

The Design Criteria Development Procedure



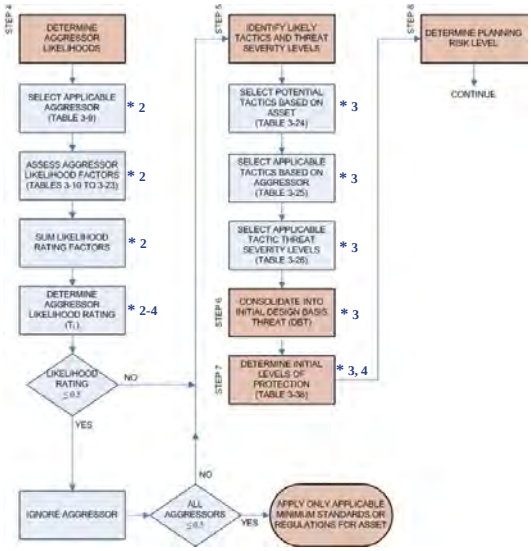
The Design Criteria Development Procedure (Steps 1-4)



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet
2. Asset Value/Aggressor Likelihood Worksheet
3. Tactic, Threat Severity, and Level of Protection Worksheet
4. Risk Level Calculation Worksheet
5. Building Cost and Risk Evaluation Worksheet

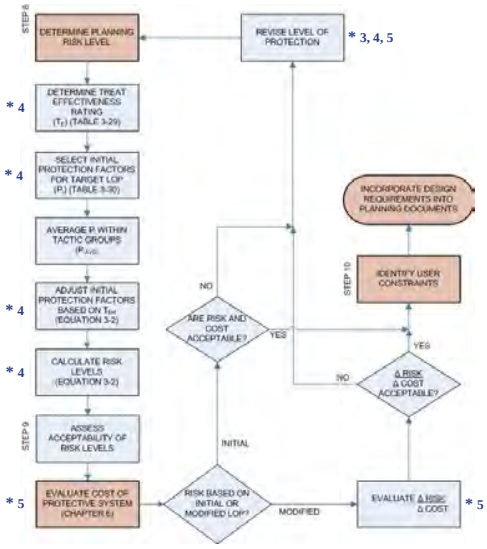
The Design Criteria Development Procedure (Steps 4-8)



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet
2. Asset Value/Aggressor Likelihood Worksheet
3. Tactic, Threat Severity, and Level of Protection Worksheet
4. Risk Level Calculation Worksheet
5. Building Cost and Risk Evaluation Worksheet

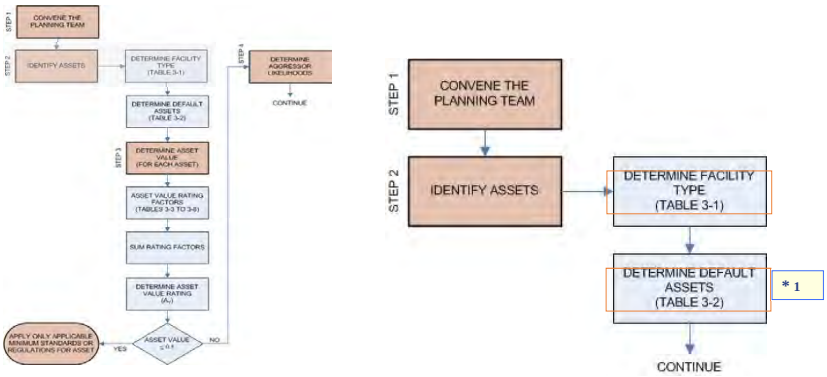
The Design Criteria Development Procedure (Steps 8-10)



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet
2. Asset Value/Aggressor Likelihood Worksheet
3. Tactic, Threat Severity, and Level of Protection Worksheet
4. Risk Level Calculation Worksheet
5. Building Cost and Risk Evaluation Worksheet

The Design Criteria Development Procedure



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet

STEP 1 – CONVENE THE PLANNING TEAM

- First Step of the process of developing design criteria is to convene the "Planning Team".

** Minimum*

STEP 2 – IDENTIFY ASSETS

- **STEP 2: IDENTIFY ASSETS. Identify assets that are be protected from compromise.**
  - **The design criteria developed in this chapter relate primarily to assets associated with facilities**
  - **Protecting individual assets is generally more cost effective than protecting an entire facility.**
  - **Buildings should only be considered assets if they are the likely direct target of aggression, as in vandalism or where the buildings have some special significance such as a highly symbolic or historic structure.**
  - **Determining the assets to be protected is the first step in establishing any protective system.**

Table 3-1 Common Facility Types

Table 3-1. Common Facility Types

Baseline Building Category	Facility Type	Examples
Administrative and Community Buildings *	Headquarters and Operations Facilities	Brigade, Battalion, Company
		Housing
		Unaccompanied Officers / Enlisted Personnel Housing
Family Housing	Family Housing	Family Housing Units
Dining Facilities *	Dining Facilities	Dining Facilities
		EM Club

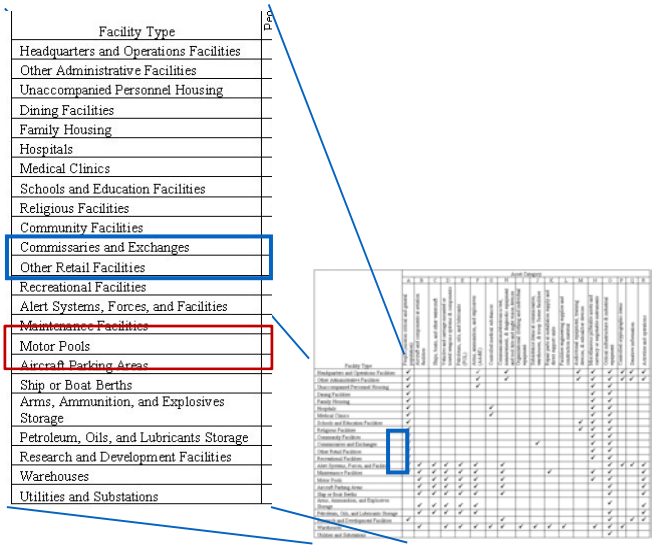
Table 3-1. Common Facility Types

Baseline Building Category	Facility Type	Examples
Administrative and Community Support Buildings *	Headquarters and Operations Facilities and Other Administrative Facilities	Brigade, Battalion, Company Headquarters
		Airfield Operations Facility
		Aviation Unit Operations Facility
		Field Operations Facility
		Ship Operations Facility
		Emergency Operations Facility
		Fire / Police Station
		National Guard / Reserve Centers
		Cargo Handling Office
		Dispatch Building
		Courtroom
		General Administrative Facility
	Schools and Education Facilities	Education Center

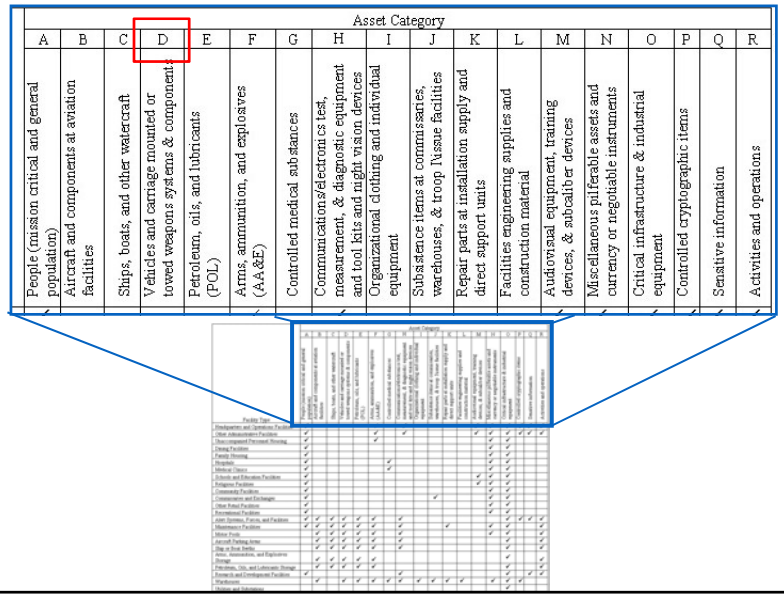
Table 3-2 Default Assets

Facility Type	Asset Category A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	People (mission critical and general population)	Aircraft and components at aviation facilities	Ships, boats, and other watercraft	Vehicles and carriage mounted or towed weapons systems & components	Petroleum, oils, and lubricants (POL)	Arms, ammunition, and explosives (AA&E)	Controlled medical substances	Communications/electronics test, measurement, & diagnostic equipment and tool kits and night vision devices	Organizational clothing and individual equipment	Substance items at commissaries, warehouses, & troop issue facilities	Repair parts at installation supply and direct support units	Facilities engineering supplies and construction material	Audiovisual equipment, training devices, & subcaliber devices	Miscellaneous pilferable assets and currency or negotiable instruments	Critical infrastructure & industrial equipment	Controlled cryptographic items	Sensitive information	Activities and operations
Headquarters and Operations Facilities	✓					✓		✓					✓	✓	✓	✓	✓	✓
Other Administrative Facilities	✓					✓		✓					✓	✓	✓	✓	✓	✓
Unaccompanied Personnel Housing	✓					✓								✓	✓			
Dining Facilities	✓													✓	✓			
Family Housing	✓													✓	✓			
Hospitals	✓						✓							✓	✓			
Medical Clinics	✓						✓							✓	✓			
Schools and Education Facilities	✓												✓	✓	✓			
Religious Facilities	✓												✓	✓	✓			
Community Facilities	✓													✓	✓			
Commissaries and Exchanges	✓									✓				✓	✓			
Other Retail Facilities	✓													✓	✓			
Recreational Facilities	✓													✓	✓			
Alert Systems, Forces, and Facilities	✓	✓	✓	✓	✓	✓		✓							✓	✓	✓	✓
~~Maintenance Facilities~~	✓	✓	✓	✓	✓	✓		✓			✓			✓	✓			✓
Motor Pools		✓	✓	✓	✓	✓		✓						✓	✓			✓
Aircraft Parking Areas		✓	✓	✓	✓	✓		✓							✓			✓
~~Ship or Boat Berths~~		✓	✓	✓	✓	✓		✓							✓			✓
Arms, Ammunition, and Explosives Storage		✓	✓	✓	✓	✓									✓			✓
Petroleum, Oils, and Lubricants Storage		✓	✓	✓	✓	✓									✓			✓
Research and Development Facilities	✓							✓							✓		✓	✓
Warehouses		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		
Utilities and Substations															✓			

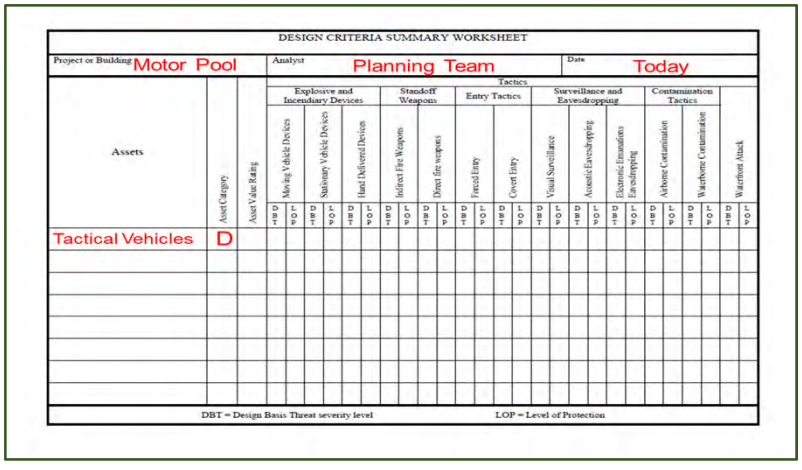
Facility Type



Asset Category



Design Criteria Summary Worksheet



DESIGN CRITERIA SUMMARY WORKSHEET

Project or Building: Motor Pool | Analyst: Planning Team | Date: Today

Assets	Asset Category	Asset Value Rating	Tactics: Explosive and Incendiary Devices			Standoff Weapons		Entry Tactics		Surveillance and Eavesdropping			Contamination Tactics		
			Moving Vehicle Devices	Stationary Vehicle Devices	Hand Delivered Devices	Indirect Fire Weapons	Direct fire weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
			DBT	LOP	DBT	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP
Tactical Vehicles	D																		

DBT = Design Basis Threat severity level | LOP = Level of Protection

Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building	Asset	Analyst
Motor Pool	Tactical Vehicles	Planning Team
	Asset Category: D	Date: Today

Value Rating Factors								Likelihood Rating Factors																		
Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating [2]	Potential Aggressors	Aggressor Goal [3]	Aggressors	Installation Location [4]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressors' Perception of Success	Threat Level	History [5] / Intentions [6]	Operational Capability [6]	Operating Environment [6]	Activity [6]	Sum of Likelihood Factors	Likelihood Ratings [7]
General Population									Unsophisticated Criminals																	
									Sophisticated Criminals																	
Critical Infrastructure and Operations and Activities									Organized Criminal Groups																	
									Vandals																	
Sensitive Information									Extremist Protesters																	
All Other Assets									Domestic Terrorists																	
									International Terrorists																	
Notes:									State Sponsored Terrorists																	
									Saboteurs																	
									Foreign Intelligence Services																	

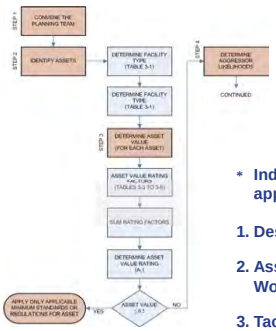
1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings = 180

STEP 3 - DETERMINE ASSET VALUE

- **STEP 3: DETERMINE ASSET VALUE (Av).**
  - **Asset value refers to the value of an asset to its user.**
  - **It is a reflection of the consequence of having the asset compromised by an aggressor.**
  - **The asset value helps the Planning Team to determine the level of protection that is warranted for the asset.**

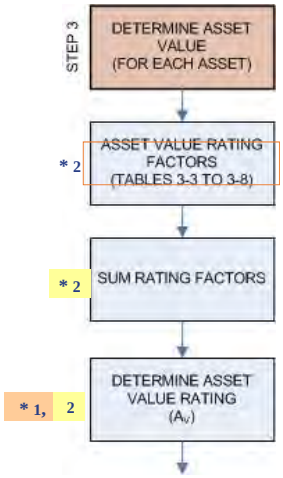
The Design Criteria Development Procedure

DETERMINE ASSET VALUE (Av)



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet
2. Asset Value/Aggressor Likelihood Worksheet
3. Tactic, Threat Severity, and Level of Protection Worksheet
4. Risk Level Calculation Worksheet
5. Building Cost and Risk Evaluation Worksheet



Value Rating Factors

- Criticality To The User / Population Type
- Impact On National Defense
- Replaceability
- Political Sensitivity
- Relative Value To User

Value Rating Factors

Table 3-3. Value Rating Factor Applicability

Asset Category	Value Rating Factor				
	Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User
General Population	✔			✔	✔
Critical Infrastructure and Operations and Activities	✔	✔	✔	✔	
Sensitive Information					✔
All Other Assets (including Mission Critical Personnel)	✔	✔	✔	✔	✔

Value Rating Factors

(Input onto Asset Value/Aggressor Likelihood Worksheet)

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool
Asset: Tactical Vehicles
Asset Category: D
Analyst: Planning Team
Date: Today

Value Rating Factors								Likelihood Rating Factors																				
Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating [2]	Potential Aggressors	Aggressor Goal [3]	Aggressors	Installation Location [4]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressors' Perception of Success	Threat Level	History [5] / Intentions [6]	Operational Capability [6]	Operating Environment [6]	Activity [6]	Sum of Likelihood Factors	Likelihood Ratings [7]			
General Population									Unsophisticated Criminals																			
									Sophisticated Criminals																			
Critical Infrastructure and Operations and Activities									Organized Criminal Groups																			
									Vandals																			
Sensitive Information									Extremist Protesters																			
All Other Assets									Domestic Terrorists																			
									International Terrorists																			
Notes:									State Sponsored Terrorists																			
									Saboteurs																			
									Foreign Intelligence Services																			

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Assessing Value Ratings

- Assess each applicable factor for each asset
- Select value rating (Varies for each factor)

Criticality to User and Population Type
Table 3-4

- **General population:**
  - Military personnel
  - DoD civilians and contractors
  - Dependents and other civilians

Lesser "Value"

Greater "Value"

Criticality to User and Population Type
Table 3-4

- **Critical infrastructure**
  - **Degradation or failure of specific functions**
  - **Degradation of overall mission**
- **All other assets:**
  - **Delay in operations**
  - **Impact on output, production, of service**

Criticality to User and Population Type
Table 3-4

Table 3-4. Criticality to User / Mission Impact/ Population Type

Asset Category	Population Type, Degradation Installation Mission, or Impact of Asset's Loss or Activity's Compromise on User's Mission	Value Rating Factor
General Population	Population is primarily military personnel	1
	Population is primarily DoD civilians and contractors	3
	Population is primarily dependents and other civilians	5
Critical Infrastructure	Loss would degrade or cause failure of specific functions, but have *no effect on the installation-wide mission* or missions of DoD facilities off installations	1
	Loss would cause failure of specific functions and *minimally degrade the installation-wide mission* or missions of DoD facilities off installations	2
	Loss would cause failure of specific functions and *moderately degrade the installation-wide mission* or missions of DoD facilities off installations	4
	Loss would cause *installation-wide mission failure* or failure of missions of DoD facilities off installations	5

Criticality to User and Population Type
Table 3-4

All Other Assets (except for sensitive information) (including mission critical personnel, operations and activities, and critical industrial equipment)	Asset's loss or operation's /activity's compromise would have *no significant effect on operations, output, production, or service*	0
	Asset's loss or operation's /activity's compromise would result in *halting operations within 1 month or would result in a 10% curtailment* in output, production, or service	1
	Asset's loss or operation's /activity's compromise would result in *halting operations within 2 weeks or would result in a 25% curtailment* in output, production, or service	2
	Asset's loss or operation's /activity's compromise would result in *halting operations within 1 week or would result in a 50% curtailment* in output, production, or service	3
	Asset's loss or operation's /activity's compromise would result in *halting operations within 1 day or would result in a 75% curtailment* in output, production, or service	4
	Asset's loss or operation's /activity's compromise would *immediately halt operations, output, production, or service. The user cannot function without it.*	5

Criticality to User and Population Type
Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool | Asset: Tactical Vehicles | Asset Category: D | Analyst: Planning Team | Date: Today

Value Rating Factors: Criticality to User / Population Type [1] Impact on National Defense; Replaceability; Political Sensitivity; Relative Value to User; Sum of Value Factors; Value Rating [2]

General Population

Critical Infrastructure and Operations and Activities

Sensitive Information

All Other Assets

4

Notes:

Potential Aggressors; Aggressor Goal [3]

Likelihood Rating Factors: Installation Location [4]; Publicity Profile [4]; Accessibility [4]; Availability [4]; Dynamics [4]; Recognizability; Relative Value to Aggressor; Law Enforcement [4]; Aggressors' Perception of Success; Threat Level; History [5] / Intentions [6]; Operational Capability [6]; Operating Environment [6]; Activity [6]; Sum of Likelihood Factors; Likelihood Ratings [7]

Aggressors
Unsophisticated Criminals
Sophisticated Criminals
Organized Criminal Groups
Vandals
Extremist Protesters
Domestic Terrorists
International Terrorists
State Sponsored Terrorists
Saboteurs
Foreign Intelligence Services

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Impact on National Defense
Table 3-5

Loss, destruction, or misuse of the asset or operation's / activity's compromise could:

- have *insignificant impact* on the United States or a region
- have *significant mission impact* on a regional level
- *compromise the defense infrastructure* of the United States
- *impact the tactical capability* of the United States
- be expected to *harm the operational capability* of the United States
- result in *great harm to the strategic capability* of the United States

Lesser "Value"

Greater "Value"

❑ **Value Ratings - 0 through 5**

Asset Replacement
Table 3-6

- **Mission critical personnel**
  - Immediately available
  - Transferred from other local units
  - Transferred from other units elsewhere
  - Would have to be trained over extended period
  - So critical that replacement isn't realistic

❑ **Value Ratings - 1 through 5**

Lesser "Value"

Greater "Value"

- **Other assets**
  - In less than 24 hours
  - In 24 to 72 hours
  - In 72 hours to 1 week
  - In 1 week to 1 month
  - In 1 to 6 months
  - More than 6 months

❑ **Value Ratings - 0 through 5**

Perceived Political Sensitivity
Table 3-7

Lesser "Value"

- Negligible: No media attention
- Minimal: Local media
- Moderate: National media
- High: International media

Greater "Value"

❑ Value Ratings - 0/1/3/5

Relative Value to User
Table 3-8

- Mission critical personnel
  - ❑ < 5 or 10% of people needed for mission
  - ❑ 6 to 10 or 25% of people needed
  - ❑ 11 to 49 or 50% of people needed
  - ❑ 50 to 100 or 75% of people needed
  - ❑ >100 or 90% of people needed

❑ Value Ratings - 1 through 5

Lesser "Value"

Greater "Value"

- General population
  - ❑ < 11
  - ❑ 11 to 49
  - ❑ 50 to 100
  - ❑ 101 to 500
  - ❑ 501 to 1000
  - ❑ > 1000

❑ Value Ratings - 0 through 5

Relative Value to User
Table 3-8

- **Aircraft**
  - Cargo, refueling, or utility type < company or squadron strength
  - Cargo, refueling, or utility type > company or squadron strength
  - Tactical or attack type < company or squadron strength
  - Tactical or attack type > company or squadron strength
  - Strategic aircraft

Lesser "Value"

Greater "Value"

❑ Value Ratings - 1 through 5

Relative Value to User
Table 3-8

- **Watercraft**
  - Others
  - Patrol coastal, MSC strategic sealift (reduced operational status)
  - Surface combatants, other amphibious, auxiliary, MSC, strategic sealift, ammunition ships, mine warfare
  - Aircraft carriers, large deck amphibious, other submarines
  - SSBN and Sea Based X-band Radar (SBX)

Lesser "Value"

Greater "Value"

❑ Value Ratings - 1 through 5

Relative Value to User

Table 3-8

Number	Tactical vehicles or critical maintenance or support vehicles	Carriage mounted or towed weapons systems
< 20	No	No
< 20	Yes	No
< 20	Yes	Yes
≥ 20	No	No
≥ 20	Yes	No
≥ 20	Yes	Yes

Lesser "Value"

Greater "Value"

- Value Ratings - 1 through 5 (There are two 3's)

Relative Value to User

Table 3-8

- Petroleum, oils, and lubricants
  - < 190,000 liters (50,000 gallons)
  - ≥ 190,000 l. (50,000 gal.) & < 570,000 l. (150,000 gal.)
  - ≥ 570,000 l. (150,000 gal.) & < 1,900,000 l. (500,000 gal.)
  - ≥ 1,900,000 l. (500,000 gal.) & < 3,800,000 l. (1,000,000 gal.)
  - ≥ 3,800,000 l. (1,000,000 gal.)

Lesser "Value"

Greater "Value"

- Arms, ammunition, and explosives
  - Uncategorized
  - Category IV
  - Category III
  - Category II
  - Category I

- Value Ratings - 1 through 5

Relative Value to User
Table 3-8

- **Controlled substances and medically sensitive items**
  - **Non-sensitive pharmaceuticals and medical items**
  - **Sensitive pharmaceuticals and medical items in pharmacies, wards, clinics, or RTD&E facilities**
  - **Sensitive pharmaceuticals and medical items in bulk storage facilities**
  - **Controlled substances in pharmacies, wards, clinics, or RTD&E facilities**
  - **Controlled substances in bulk storage facilities**

Lesser "Value"

Greater "Value"

❑ **Value Ratings - 1 through 5**

Relative Value to User
Table 3-8

Asset Replacement Costs	
Individual Assets	**Inventories of Assets**
< $2500	**< $100,000**
≥ $2500 & < $10,000	**≥ $100,000 & < $250,000**
≥ $10,000 & < $25,000	**≥ $250,000 & < $500,000**
≥ $25,000 & < $50,000	**≥ $500,000 & < $1,000,000**
≥ $50,000 & < $100,000	**≥ $1,000,000 & < $2.000,000**
> $100,000	**> $2,000,000**

Lesser "Value"

Greater "Value"

❑ **Value Ratings - 0 through 5**

Relative Value to User
Table 3-8

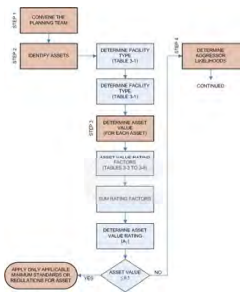
- **Controlled Cryptographic Items**
  - Equipment processes:
    - Unclassified and non-sensitive information (0)
    - Unclassified, but sensitive (i.e. FOUO) information (1)
    - Confidential information (2)
    - Secret information (3)
    - Top Secret information (4)
    - Secure Compartmented information (5)

❑ Value Ratings - 0 through 5

- **Sensitive Information**
  - Unclassified, but sensitive (i.e. FOUO) information (5)
  - Confidential information (7.5)
  - Secret information (8.5)
  - Top Secret information (9.5)
  - Secure Compartmented information (10)

❑ Value Ratings - 5 through 10

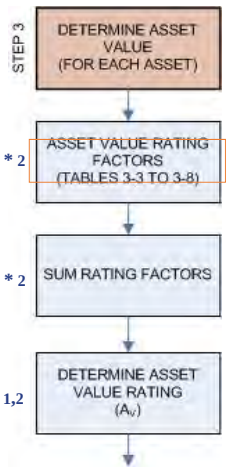
Asset Value Rating (A_V)



Asset Value Rating

Sum of Value Rating Factors ÷

- 10 for sensitive information
- 15 for general population
- 20 for critical infrastructure and activities and operations
- 25 for all others



* Indicates value to be entered onto applicable worksheet

1. Design Criteria Summary Worksheet
2. Asset Value/Aggressor Likelihood Worksheet
3. Tactic , Threat Severity, and Level of Protection Worksheet
4. Risk Level Calculation Worksheet
5. Building Cost and Risk Evaluation Worksheet

Asset Value Rating (A_V) Documentation
Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool | Asset: Tactical Vehicles | Asset Category: D | Analyst: Planning Team | Date: Today

Value Rating Factors					Sum of Value Factors	Value Rating [2]	Potential Aggressors	Aggressor Goal [3]	Aggressors	Likelihood Rating Factors														Sum of Likelihood Factors	Likelihood Ratings [7]
Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User						Installation Location [5]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressors' Perception of Success	Threat Level	History [7] / Intentions [5]	Operational Capability [6]	Operating Environment [6]	Activity [6]		
General Population									Unsophisticated Criminals																
									Sophisticated Criminals																
Critical Infrastructure and Operations and Activities									Organized Criminal Groups																
									Vandals																
Sensitive Information									Extremist Protesters																
All Other Assets									Domestic Terrorists																
4	4	4	3	4	19	.76			International Terrorists																
									Foreign Intelligence Services																

19/25 = .76

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Design Criteria Summary Worksheet
Input Asset Value Rating

DESIGN CRITERIA SUMMARY WORKSHEET

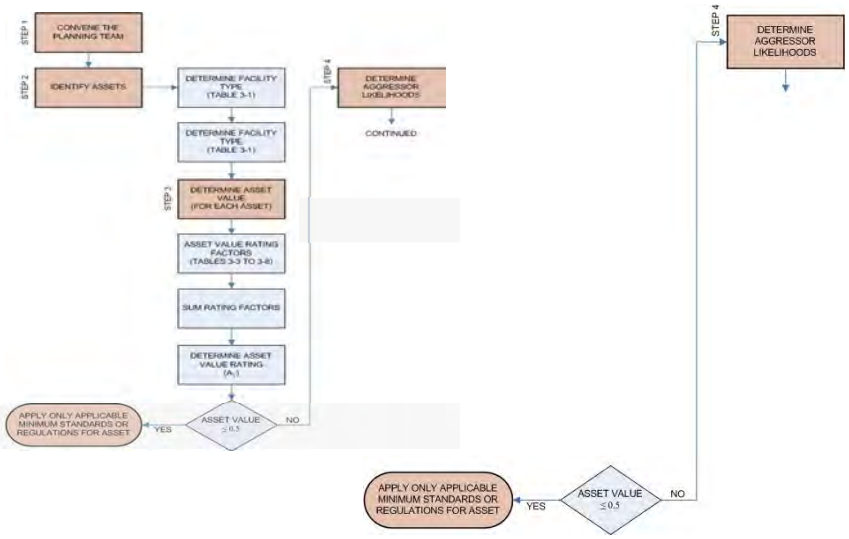
Project or Building: Motor Pool | Analyst: Planning Team | Date: Today

Assets	Asset Category	Asset Value Rating	Tactics: Explosive and Incendiary Devices						Standoff Weapons				Entry Tactics				Surveillance and Eavesdropping						Contamination Tactics					
			Moving Vehicle Devices		Stationary Vehicle Devices		Hand Delivered Devices		Indirect Fire Weapons		Direct fire weapons		Forced Entry		Covert Entry		Visual Surveillance		Acoustic Eavesdropping		Electronic Emanations Eavesdropping		Airborne Contamination		Waterborne Contamination		Waterfront Attack	
			DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP	DBT	LOP
Tactical Vehicles	D	.76																										

DBT = Design Basis Threat severity level | LOP = Level of Protection

First Decision Point

Asset Value (A_V)



First Decision Point

Asset Value (A_V)

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool
Asset: Tactical Vehicles
Asset Category: D
Analyst: Planning Team
Date: Today

Value Rating Factors: Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating [2]
General Population						
Critical Infrastructure and Operations and Activities						
Sensitive Information						
All Other Assets						
4	4	4	3	4	19	.76

Potential Aggressors: Aggressor Goal [3]	Aggressors	Likelihood Rating Factors: Installation Location [4]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressor's Perception of Success	Threat Level	History [5] / Intentions [6]	Operational Capability [5]	Operating Environment [5]	Activity [5]	Sum of Likelihood Factors	Likelihood Ratings [7]
	Unsophisticated Criminals																
	Sophisticated Criminals																
	Organized Criminal Groups																
	Vandals																
	Extremist Protesters																
	Domestic Terrorists																
	International Terrorists																
	Stal																
	Ter																
	Sab																
	For Services																

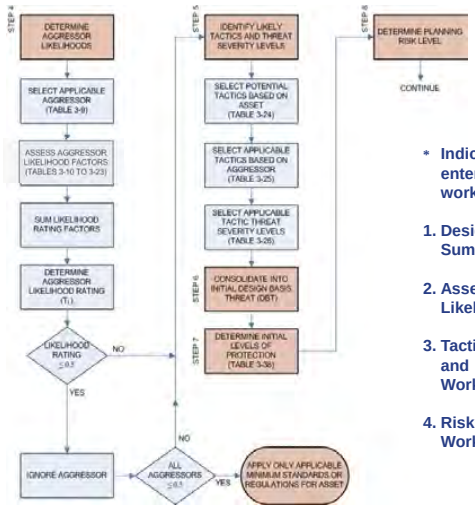
> 0.5 so continue with process

1. Population Type applies to General Population only
2. Sum of Value Ratings = 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings = 180

The Design Criteria Development Procedure

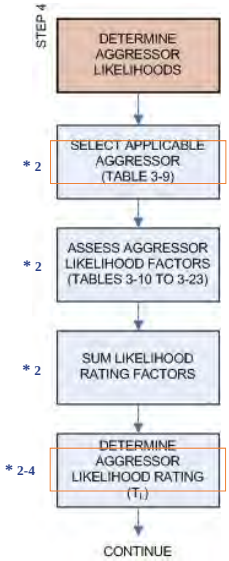
- **STEP 4: IDENTIFY AGGRESSOR LIKELIHOODS**
  - **The next step in the procedure after identifying the assets and their values is to look at those assets from the perspective of potential aggressors. This step includes:**
    - Identifying potential aggressors
    - Determining the likelihoods that they will attempt to compromise the assets.

STEP 4: AGGRESSOR LIKELIHOODS

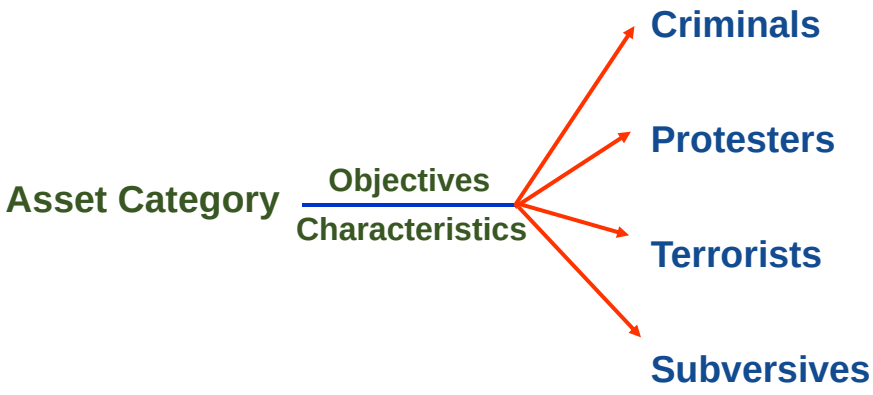


* **Indicates value to be entered onto applicable worksheet**

1. **Design Criteria Summary Worksheet**
2. **Asset Value/Aggressor Likelihood Worksheet**
3. **Tactic, Threat Severity, and Level of Protection Worksheet**
4. **Risk Level Calculation Worksheet**



Identify Likely Aggressors



Aggressor

- Criminals
  - Unsophisticated, Sophisticated, Organized
- Protesters
  - Vandals, Activists and Extremists
- Terrorists
  - Domestic, International, Paramilitary
- Subversives
  - Saboteurs and Foreign intelligence services

Potential Aggressors
Table 3-9

Table 3-9. Potential Aggressors and Default Goals

	Asset Categories	Default Aggressor Types									
		Unsophisticated Criminals	Sophisticated Criminals	Organized Criminal Groups	Vandals	Extremist Protest Groups	Domestic Terrorists	International Terrorists	State Sponsored Terrorists	Saboteurs	Foreign Intelligence Services
A	People			G	P	P	P	P	P	G	
B	Aircraft and Components at Aviation Facilities	M	M	M	P	P	P	P	P	G	
C	Ships, Boats, and Other Watercraft	M	M	M	P	P	P	P	P	G	
D	Vehicles and carriage mounted or towed weapons systems	M	M	M	P	P	P	P	P	G	
E	Petroleum, Oils, and Lubricants	M	M	M	P	P	P	P	P	G	
F	Arms, Ammunition, and Explosives	M	M	M	P	1	1	1	1	G	
G	Controlled Medical Substances and Medically Sensitive Items	M	M	M							
H	Communications / Electronics Equip. and Night Vision Devices	M	M	M							
I	Organizational Clothing and Individual Equipment	M	M	M							
J	Subsistence Items at Commissaries, Warehouses, & Troop Issue Facilities	M	M	M							
K	Repair Parts at Installation Supply and Direct Support Units	M	M	M							
L	Facilities Engineering Supplies and Construction Material	M	M	M							
M	Audiovisual Equipment, Training Devices, and Subcaliber Devices	M	M	M							
N	Miscellaneous Pilferable Assets (other than above) and Money	M	M	M							
O	Critical Infrastructure and Industrial Equipment				P	P	P	P	P	G	
P	Controlled Cryptographic Items		M	M						G	G
Q	Sensitive Information			G						G	G
R	Activities and Operations			G		G	P	P	P	G	G

1. May be mission, publicity, or monetary related goal (see Table 3-16)
G = Mission related goal P = Publicity related goal M = Monetary related goal

Potential Aggressors
Table 3-9

Table 3-9. Potential Aggress

	Asset Categories	Unsophisticated Criminals	Sophisticated Criminals	Organized Criminal
A	People			G
B	Aircraft and Components at Aviation Facilities	M	M	M
C	Ships, Boats, and Other Watercraft	M	M	M
D	Vehicles and carriage mounted or towed weapons systems	M	M	M
E	Petroleum, Oils, and Lubricants	M	M	M
F	Arms, Ammunition, and Explosives	M	M	M
G	Controlled Medical Substances and Medically Sensitive Items	M	M	M
H	Communications / Electronics Equip. and Night Vision Devices	M	M	M
I	Organizational Clothing and Individual Equipment	M	M	M
J	Subsistence Items at Commissaries, Warehouses, & Troop Issue Facilities	M	M	M
K	Repair Parts at Installation Supply and Direct Support Units	M	M	M
L	Facilities Engineering Supplies and Construction Material	M	M	M
M	Audiovisual Equipment, Training Devices, and Subcaliber Devices	M	M	M
N	Miscellaneous Pilferable Assets (other than above) and Money	M	M	M
O	Critical Infrastructure and Industrial Equipment			
P	Controlled Cryptographic Items		M	M
Q	Sensitive Information			G
R	Activities and Operations			G

1. May be mission, publicity, or monetary related goal (see Table 3-16)
G = Mission related goal P = Publicity related goal M = Monetary related goal

	Asset Categories
A	People
B	Aircraft and Components at Aviation Facilities
C	Ships, Boats, and Other Watercraft
D	Vehicles and carriage mounted or towed weapons systems
E	Petroleum, Oils, and Lubricants
F	Arms, Ammunition, and Explosives
G	Controlled Medical Substances and Medically Sensitive Items
H	Communications / Electronics Equip. and Night Vision Devices
I	Organizational Clothing and Individual Equipment

Potential Aggressors
Table 3-9

Table 3-9 Potential Aggressors and Default Goals

	Asset Categories	Default Aggressor Types									
		Unsophisticated Criminals	Sophisticated Criminals	Organized Criminal Groups	Vandals	Extremist Protest Groups	Domestic Terrorists	International Terrorists	State Sponsored Terrorists	Saboteurs	Foreign Intelligence Services
A	People										
B	Aircraft and Components at Aviation Facilities	M	M	M	P	P	P	P	P	G	
C	Ships, Boats, and Other Watercraft	M	M	M	P	P	P	P	P	G	
D	Vehicles and carriage mounted or towed we										
E	Petroleum										
F	Arms, An										
G	Controlle Medicall										
H	Communi and Night										
I	Organizat Individua										
J	Subsisten Warehous										
K	Repair Pa and Direc										
L	Facilities Construct										
M	Audiovis Devices,										
N	Miscellan (other tha										
O	Critical Infrastructure and Industrial Equipment				P	P	P	P	P	G	
P	Controlled Cryptographic Items		M	M						G	G
Q	Sensitive Information			G						G	G
R	Activities and Operations			G		G	P	P	P	G	G

1. May be mission, publicity, or monetary related goal (see Table 3-16)
G = Mission related goal P = Publicity related goal M = Monetary related goal

Default Aggressor Types
Unsophisticated Criminals
Sophisticated Criminals
Organized Criminal Groups
Vandals
Extremist Protest Groups
Domestic Terrorists
International Terrorists
State Sponsored Terrorists
Saboteurs
Foreign Intelligence Services

Documentation of Potential Aggressors
Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool
Asset: Tactical Vehicles
Asset Category: D
Analyst: Planning Team
Date: Today

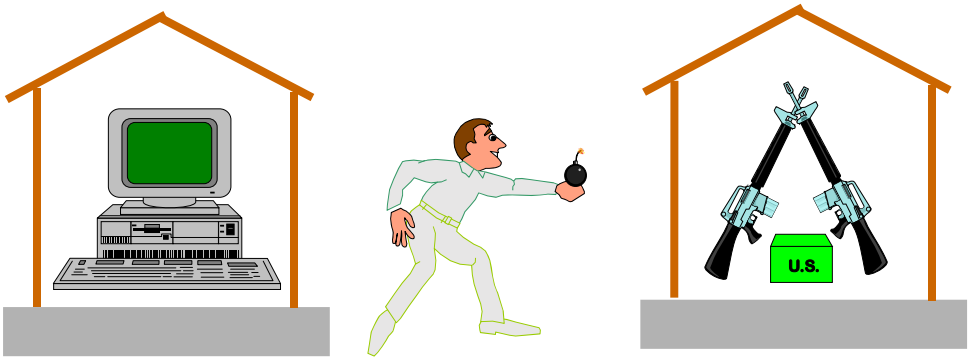
Value Rating Factors: Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating [2]
General Population						
Critical Infrastructure and Operations and Activities						
Sensitive Information						
All Other Assets						
4	4	4	3	4	19	.76

Notes:

Potential Aggressors	Aggressor Goal [3]	Aggressors	Likelihood Rating Factors: Installation Location [4]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressors' Perception of Success	Threat Level	History [5] / Intentions [6]	Operational Capability [6]	Operating Environment [6]	Activity [6]	Sum of Likelihood Factors	Likelihood Ratings [7]
✓	M	Unsophisticated Criminals																
✓	M	Sophisticated Criminals																
✓	M	Organized Criminal Groups																
✓	P	Vandals																
✓	P	Extremist Protesters																
✓	P	Domestic Terrorists																
✓	P	International Terrorists																
✓	P	State Sponsored Terrorists																
✓	G	Saboteurs																
		Foreign Intelligence Services																

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Assess Likelihood of Aggression



Likelihood Ratings

- Asset Location *(1-5)*
- Publicity Profile *(1-5)*
- Asset Accessibility *(0-10)*
- Asset Availability *(0-5)*
- Asset Dynamics *(1-5)*
- Recognizability *(3-15)*
- Relative Value to Aggressor *(0-15)*
- Law Enforcement Visibility (0-30)
- Aggressors' Perception of Success (6-30)

- Threat Level *(5-20 for terrorists & 6-30 for others)*
- History *or* Intentions * *(2-10 for terrorists & 6-30 for others)*
- Operational Capability * *(2-10)*
- Operating Environment * *(2-10)*
- Activity * *(2-10)*

* *Terrorists only*

Sums lead to ratings between 0 and 1

Likelihood Rating Distribution

- Asset Location
- Publicity Profile
- Asset Accessibility
- Asset Availability
- Asset Dynamics
- Recognizability
- Relative Value to Aggressor

1/3

1/3

- Law Enforcement Visibility
- Aggressors' Perception of Success

1/3

- Threat Level
- History *or* Intentions *
- Operational Capability * Operating Environment *
- Activity *

* ***Terrorists only***

Grand Total Is 180

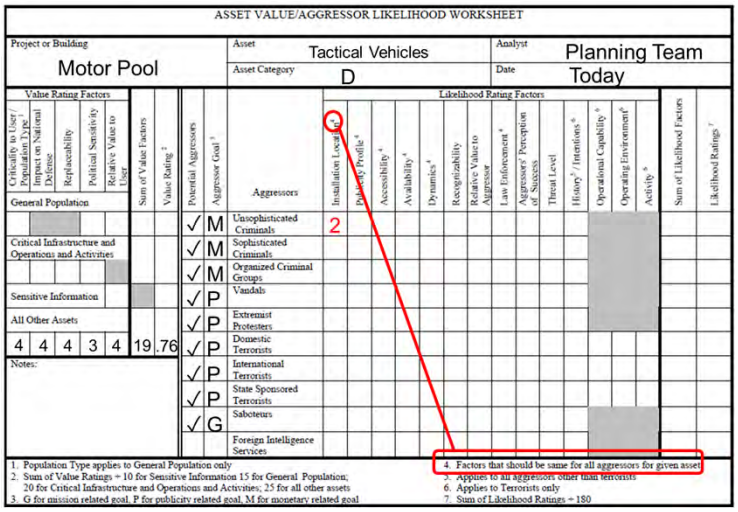
Asset Location
Table 3-10

Table 3-10. Asset Location

Installation or facility Location	Likelihood Rating Factor
Located within the Continental United States away from major metropolitan areas	1
Located within the Continental United States near a major metropolitan area	2
Located outside the Continental United States away from major metropolitan areas	4
Located outside the Continental United States near a major metropolitan area	5

Asset Value/Aggressor Likelihood Worksheet

Aggressor Likelihood Value Ratings



ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

Project or Building: Motor Pool | Asset: Tactical Vehicles | Asset Category: D | Analyst: Planning Team | Date: Today

Value Rating Factors								Likelihood Rating Factors																				
Criticality to User / Population Type [1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating [2]	Potential Aggressors	Aggressor Goal [3]	Aggressors	Installation Locality [4]	Publicity Profile [4]	Accessibility [4]	Availability [4]	Dynamics [4]	Recognizability	Relative Value to Aggressor	Law Enforcement [4]	Aggressor's Perception of Success	Threat Level	History [5] / Intentions [5]	Operational Capability [6]	Operating Environment [6]	Activity [5]	Sum of Likelihood Factors	Likelihood Ratings [7]			
General Population																												
							✓	M	Unsophisticated Criminals	2																		
Critical Infrastructure and Operations and Activities							✓	M	Sophisticated Criminals																			
							✓	M	Organized Criminal Groups																			
Sensitive Information							✓	P	Vandals																			
All Other Assets							✓	P	Extremist Protesters																			
4	4	4	3	4	19	.76	✓	P	Domestic Terrorists																			
Notes:							✓	P	International Terrorists																			
							✓	P	State Sponsored Terrorists																			
							✓	G	Saboteurs																			
									Foreign Intelligence Services																			

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Publicity Profile

Table 3-11

Installation or facility is:

- **Relatively unknown locally and regionally**
- **Well known locally, but relatively unknown regionally**
- **Well known locally and regionally, but relatively unknown nationally**
- **Well known locally, regionally, and nationally, but relatively unknown internationally**
- **Well known locally, regionally, and nationally, and internationally**

Less likely

More likely

❑ **Value Ratings - 1 through 5**

Asset Accessibility
Table 3-12

Facility asset is in is:

- On closed installation in separate access controlled compound in interior of installation
- On closed installation in interior of installation
- On closed installation w/in 100 m of installation perimeter
- On open installation in interior of installation
- On open installation w/in 100 m of installation perimeter
- Not on an installation

Less likely

More likely

❑ Value Ratings - 0 through 10 @ 2 point intervals

Asset Availability
Table 3-13

Similar assets are:

- Widely available both on and off installation or site
- Have limited availability off installation, but widely available on installation
- Not available off installation, but widely available on installation
- Limited availability on installation, and not available off installation
- Available at fewer than 3 locations on installation and not available off installation
- Located only at this site

Less likely

More likely

❑ Value Ratings - 0 through 5

Asset Dynamics
Table 3-14

Less likely

Asset Dynamics

- **Moved frequently on random basis**
- **Moved frequently on predictable basis**
- **Moved periodically on random basis**
- **Moved periodically on predictable basis**
- **Not moved**

More likely

❑ **Value Ratings - 1 through 5**

Recognizability
Table 3-15

Table 3-15. Recognizability

Recognizability	Likelihood Rating Factor		
	Unsophisticated Criminals Sophisticated Criminals Vandals	Organized Criminal Groups Extremist Protest Groups Domestic Terrorists	International Terrorists State Sponsored Terrorists Saboteurs Foreign Intelligence Services
The asset's existence can be recognized only by aggressors who are experts or who have expert intelligence support	3	6	9
The asset's existence can be recognized only by aggressors with a significant amount of training or intelligence support	6	9	12
The asset's existence can be recognized only by aggressors with a moderate amount of training or intelligence support	9	12	15
The asset's existence can be recognized only by aggressors with a minor amount of training or intelligence support	12	15	15
The asset's existence is obvious to the aggressor. It can be recognized by aggressors with little or no training or intelligence support	15	15	15

Recognizability
Table 3-15

The asset's existence can be recognized only by aggressors who are experts or who have expert intelligence support	
The asset's existence can be recognized only by aggressors with a significant amount of training or intelligence support	
The asset's existence can be recognized only by aggressors with a moderate amount of training or intelligence support	
The asset's existence can be recognized only by aggressors with a minor amount of training or intelligence support	
The asset's existence is obvious to the aggressor. It can be recognized by aggressors with little or no training or intelligence support	

Recognizability
Table 3-15

	Likelihood Rating Factor		
	Unsophisticated Criminals Sophisticated Criminals Vandals	Organized Criminal Groups Extremist Protest Groups Domestic Terrorists	International Terrorists State Sponsored Terrorists Saboteurs Foreign Intelligence Services
The asset's existence can be recognized only by aggressors who are experts or who have expert intelligence support	3	6	9
The asset's existence can be recognized only by aggressors with a significant amount of training or intelligence support	6	9	12
The asset's existence can be recognized only by aggressors with a moderate amount of training or intelligence support	9	12	15
The asset's existence can be recognized only by aggressors with a minor amount of training or intelligence support	12	15	15
The asset's existence is obvious to the aggressor. It can be recognized by aggressors with little or no training or intelligence support	15	15	15

Relative Value to Aggressor
Table 3-16

Table 3-16. Relative Value to Aggressors

Asset Category[1]		Aggressor	Measure	Relative Value	Likelihood Rating Factor
Assets subject to death or destruction[2]	A	Saboteurs and Foreign Intelligence Agents, or Organized Criminal Groups[5]	Value to mission or future goals	Compromising assets would have negligible utility to accomplishment of aggressor's mission or future goals.	0
	B			Compromising assets would have minor utility to accomplishment of aggressor's mission or future goals.	3
	C			Compromising assets would have moderate utility to accomplishment of aggressor's mission or future goals.	6
	D			Compromising assets would have significant utility to accomplishment of aggressor's mission or future goals.	8
	E			Compromising assets would have major utility to accomplishment of aggressor's mission or future goals.	12
	F[4]			Compromising assets would likely be critical to accomplishment of aggressor's mission or success of future goals.	15
	O	Terrorist / Extremist Protest Group, Vandals	Publicity value	Aggressor is likely to believe asset's compromise would result in publicity limited to local media	3
	P			Aggressor is likely to believe asset's compromise would result in publicity that would likely extend to national media	9
	Q			Aggressor is likely to believe asset's compromise would result in publicity that would likely extend to international media	15
	R				

Relative Value to Aggressor
Table 3-16

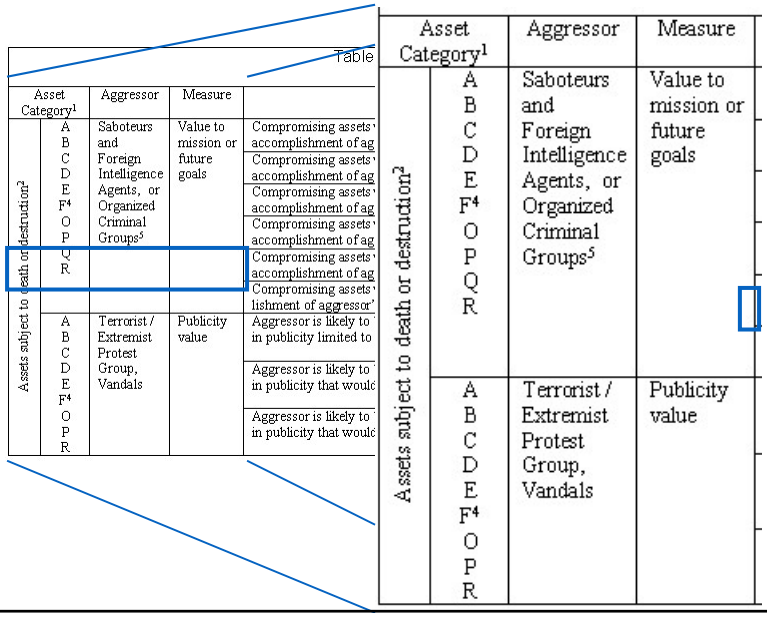
Table 3-16 (continued)

		Aggressors ⇨		Relative Value	Likelihood Rating Factors: Unsophisticated Criminals	Sophisticated criminals	Organized criminal groups	Terrorists[6]
Assets subject to theft[3]	B	Individual assets	Monetary value	Asset value is less than $2500	9	3	0	3
	C			Asset value is greater than or equal to $2500 and less than $10,000	12	6	3	6
	D			Asset value is greater than or equal to $10,000 and less than $25,000	15	9	6	9
	E			Asset value is greater than or equal to $25,000 and less	15	12	9	12
	F[4]			$500,000 and less than $1,000,000				
	G			Asset inventory value is greater than or equal to $1,000,000 and less than $2,000,000	12	15	12	15
	H			Asset inventory value is greater than $2,000,000	9	15	15	15
	I							
	K							
	L							
	M							
	N							
	P							

Notes:
1. Select the upper pair of factors if the goal of the aggressor is likely to be to destroy or kill the asset and the lower pair if the aggressor's goal is likely to be to steal it except as noted for asset category F (arms ammunition, and explosives).
2. Select between factors based on aggressor type.
3. Select between factors based on whether analyzing individual assets or inventory of assets.
4. For arms, ammunition, and explosives (AA&E) subject to action by terrorists or extremist protest groups, select the upper factor if the goal is to steal the AA&E for use in future attacks, select the second if the goal is to destroy it, and among the lower two if the goal is to steal and sell it.
5. Only use this factor for organized criminal groups where it is likely they would kill or destroy an asset to further their goals. See paragraph 3-6.2.7.1.
6. Use only where terrorists are likely to steal assets to sell them.
7. Applies only for aircraft components.

Notes:
1. Select the upper pair of factors if the goal of the aggressor is likely to be to destroy or kill the asset and the lower pair if the aggressor's goal is likely to be to steal it except as noted for asset category F (arms ammunition, and explosives).
2. Select between factors based on aggressor type.
3. Select between factors based on whether analyzing individual assets or inventory of assets.
4. For arms, ammunition, and explosives (AA&E) subject to action by terrorists or extremist protest groups, select the upper factor if the goal is to steal the AA&E for use in future attacks, select the second if the goal is to destroy it, and among the lower two if the goal is to steal and sell it.
5. Only use this factor for organized criminal groups where it is likely they would kill or destroy an asset to further their goals. See paragraph 3-6.2.7.1.
6. Use only where terrorists are likely to steal assets to sell them.
7. Applies only for aircraft components.

Relative Value to Aggressor
Table 3-16



Assets Subject to Destruction
Table 3-16 (Mission/Publicity)

For saboteurs, foreign intelligence agents, or organized criminals likely to kill to advance their goals

Value to mission/ future goals

- **Negligible utility**
- **Minor utility**
- **Moderate utility**
- **Significant utility**
- **Major utility**
- **Critical to goals**

❑ **Value Ratings - 0 through 15 @ 3 point intervals**

Less likely

More likely

For terrorist/extremists protest groups, vandals

Publicity value

- **Local media**
- **National media**
- **International media**

❑ **Value Ratings - 0, 3, 9, 15**

Relative Value to Aggressor
Table 3-16

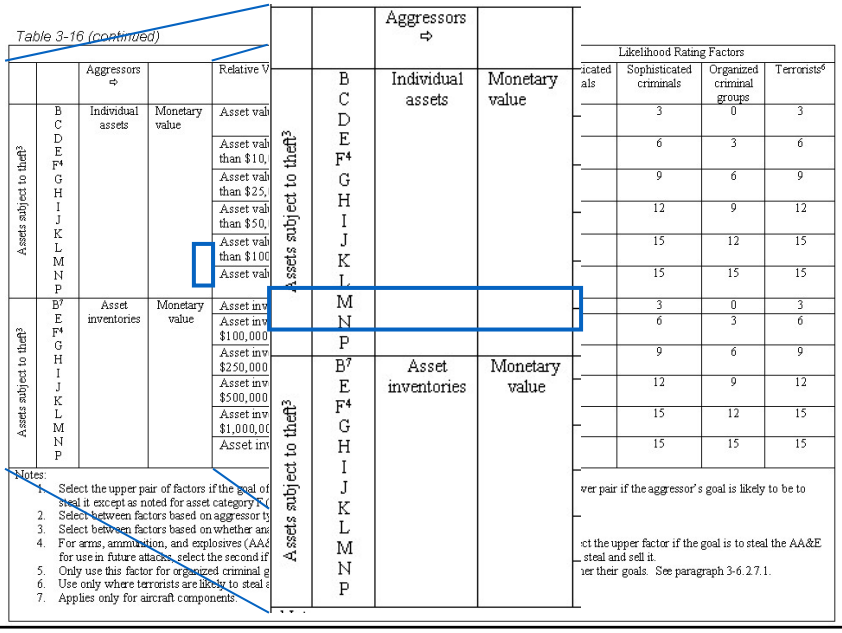


Table 3-16 (continued)

		Aggressors ⇨		Relative V
Assets subject to theft[3]	B	Individual assets	Monetary value	Asset val
	C			Asset val than $10,
	D			Asset val than $25,
	E			Asset val than $50,
	F[4]			Asset val than $100
	G			Asset val
	H			
	I			
	J			
	K			
	L			
	M			
	N			
	P			
Assets subject to theft[3]	B[7]	Asset inventories	Monetary value	Asset inv
	E			Asset inv $100,000
	F[4]			Asset inv $250,000
	G			Asset inv $500,000
	H			Asset inv $1,000,00
	I			Asset inv
	J			
	K			
	L			
	M			
	N			
	P			

Notes:
1. Select the upper pair of factors if the goal of steal it except as noted for asset category F.
2. Select between factors based on aggressor ty
3. Select between factors based on whether ana
4. For arms, ammunition, and explosives (AA& for use in future attacks, select the second if
5. Only use this factor for organized criminal g
6. Use only where terrorists are likely to steal a
7. Applies only for aircraft components.

		Aggressors ⇨		Likelihood Rating Factors			
Assets subject to theft[3]	B	Individual assets	Monetary value	icated als	Sophisticated criminals	Organized criminal groups	Terrorists[6]
	C				3	0	3
	D				6	3	6
	E				9	6	9
	F[4]				12	9	12
	G				15	12	15
	H				15	15	15
	I						
	J						
	K						
	L						
	M				3	0	3
	N				6	3	6
	P				9	6	9
Assets subject to theft[3]	B[7]	Asset inventories	Monetary value		12	9	12
	E				15	12	15
	F[4]				15	15	15
	G						
	H						
	I						
	J						
	K						
	L						
	M						
	N						
	P						

ver pair if the aggressor's goal is likely to be to

ct the upper factor if the goal is to steal the AA&E steal and sell it.
ner their goals. See paragraph 3-6.2.7.1.

Assets Subject to Theft
Table 3-16 (Monetary)

Individual Assets

- **< $2500**
- **$2500 - $10,000**
- **$10,000 - $25,000**
- **$25,000 - $50,000**
- **$50,000 - $100,000**
- **> $100,000**

Less likely

⇕

More likely

Asset Inventories

- **< $100,000**
- **$100,000 - $250,000**
- **$250,000 - $500,000**
- **$500,000 - $ 1,000,000**
- **$1,000,000 - $2,000,000**
- **> $2,000,000**

Relative Value to Aggressor
Table 3-16 (Monetary)

Table 3-16 (continued)

Aggressors	Relative Value	Likelihood Rating Factors			
		Unsophisticated Criminals	Sophisticated criminals	Organized criminal groups	Terrorists[6]
		9	3	0	3
		12	6	3	6
		15	9	6	9
		15	12	9	12
		12	15	12	15
		9	15	15	15

Likelihood Rating Factors			
Unsophisticated Criminals	Sophisticated criminals	Organized criminal groups	Terrorists[6]
9	3	0	3
12	6	3	6
15	9	6	9
15	12	9	12
12	15	12	15
9	15	15	15

		9	3	0	3
		12	6	3	6
		15	9	6	9
		15	12	9	12
		12	15	12	15
		9	15	15	15

sset and the lower pair if the aggressor's goal is likely to be to

for use in future attacks, select the second if the goal is to destroy it, and among the lower two if the goal is to steal and sell it.

5. Only use this factor for organized criminal groups where it is likely they would kill or destroy an asset to further their goals. See paragraph 3-6.2.7.1.
6. Use only where terrorists are likely to steal assets to sell them.
7. Applies only for aircraft components.

Law Enforcement Visibility
Table 3-17

Table 3-17. Law Enforcement Personnel Visibility

		Frequency of Presence in Vicinity of Facility			
		None	Occasional	Frequent	Continuous
Frequency at Installation Perimeter	Occasional	30	24	18	12
	Scheduled	24	18	12	6
	Continuous	18	12	6	0

Perception of Success
Table 3-18

Based on visible countermeasures present or likely to be present, aggressor would likely perceive:

- **Very low possibility of compromising or destroying the asset and escaping**
- **Low possibility…**
- **Moderate possibility…**
- **High possibility…**
- **Very high possibility…**

Less likely

More likely

- Value Ratings - 6 through 30
  - 6 point intervals

Threat Level
Table 3-19

From DoD, DOS, Combatant Command or local assessment

- **Low**
- **Moderate**
- **Significant**
- **High**

Less likely

More likely

Table 3-19. Threat Level

Terrorist, Criminal, Vandal, Protestor, Foreign Intelligence, or Saboteur Threat Level	Likelihood Rating Factor	
	Terrorists	All Other Aggressors
Low	5	6
Moderate	10	14
Significant	15	22
High	20	30

History or Intention
Table 3-20

History (other than terrorists)

- No history of attacking or otherwise compromising assets of this type
- Little or no history…
- History…but not locally or regionally
- Local or regional history…in past 10 years
- Strong history…locally or regionally in past 3 years

❑ Value Ratings - 6 through 30 @ 6 point intervals

Less likely

More likely

Intention (terrorists)

- No history of attacks
- Anti-US ideology, but no history
- Anti-US ideology, with history outside region
- Recent attacks against US interests regionally
- Recent attacks against US interests locally

❑ Value Ratings - 2 through 10 @ 2 point intervals

Terrorist Operational Capability
Table 3-21

Less likely

More likely

- Very incapable
- Incapable
- Somewhat capable
- Very capable
- Extremely capable

❑ Value Ratings - 2 through 10 @ 2 point intervals

Terrorist Operating Environment
Table 3-22

Less likely

- **Favors US or host nation**
- **Neutral**
- **Favors terrorist**

More likely

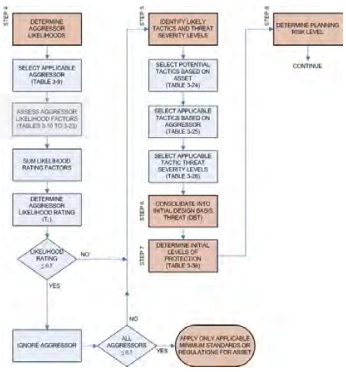
❑ **Value Ratings - 2 through 10 @ 4 point intervals**

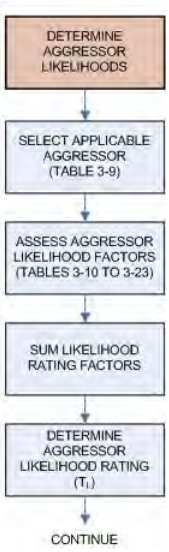
Terrorist Activity
Table 3-23

- **Present but inactive**
- **Recruiting , fund raising, or non-directed activity**
- **Suspected surveillance, threats, and suspicious incidents**
- **Incidental cell activity (operational or support)**
- **Credible indications of targeting US assets**

❑ **Value Ratings - 2 through 10 @ 2 point intervals**

Determine Aggressor Likelihood Rating (T_L)





Sum of Likelihood Rating Factors ÷ 180

Documentation of Aggressor Likelihood Ratings

Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

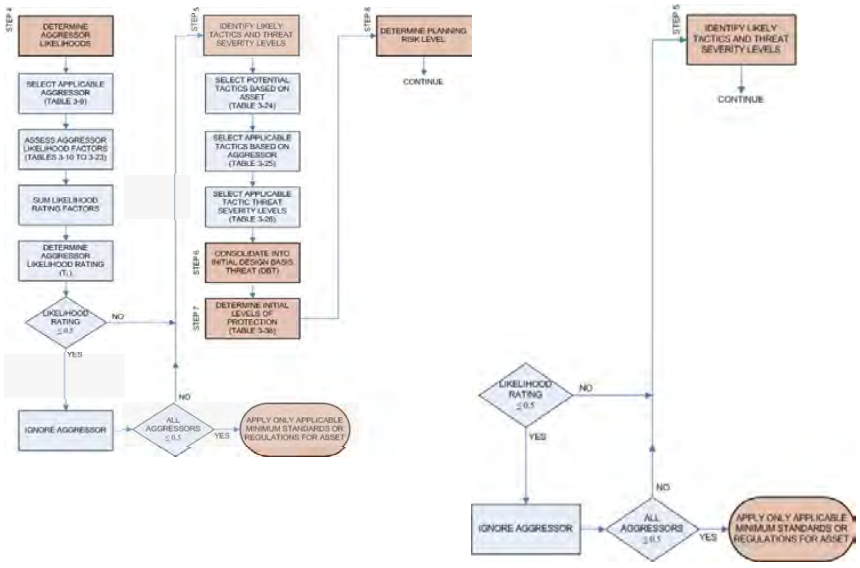
Project or Building: Motor Pool | Asset: Tactical Vehicles | Asset Category: D | Analyst: Planning Team | Date: Today

Value Rating Factors: Criticality to User / Population Type[1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating[2]	Potential Aggressors	Aggressor Goal[3]	Aggressors	Likelihood Rating Factors: Installation Location[4]	Public Profile[4]	[illegible][4]	[illegible]	[illegible]	[illegible]	[illegible]	Law Enforcement[4] Perception	[illegible]	[illegible]	History[5] / Intentions[6]	Operational Capability[6]	Operating Environment[6]	Activity[6]	Sum of Likelihood Factors	Likelihood Ratings[7]
General Population																									
							✓	M	Unsophisticated Criminals	2	4	2	2	3	12	12	18	24	6	6				94	.52
Critical Infrastructure and Operations and Activities							✓	M	Sophisticated Criminals	2	4	2	2	3	12	12	18	24	6	6				91	.51
							✓	M	Organized Criminal Groups	2	4	2	2	3	15	9	18	30	6	6				97	.54
Sensitive Information							✓	P	Vandals	2	4	2	2	3	12	6	18	24	6	6				85	.47
All Other Assets							✓	P	Extremist Protesters	2	4	2	2	3	15	6	18	24	6	6				88	.49
4	4	4	3	4	19	.76	✓	P	Domestic Terrorists	2	4	2	2	3	15	9	18	24	5	4	4	6	4	102	.57
Notes:							✓	P	International Terrorists	2	4	2	2	3	15	9	18	30	5	8	6	10	2	116	.64
							✓	P	State Sponsored Terrorists	2	4	2	2	3	15	9	18	30	5	10	10	10	10	130	.72
							✓	G	Saboteurs	2	4	2	2	3	15	3	18	30	6	6				91	.51
									Foreign Intelligence Services																

94/180 = .52

1. Population Type applies to General Population only
2. Sum of Value Ratings ÷ 10 for Sensitive Information 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings ÷ 180

Second Decision Point – Likelihood Rating



Evaluate Likelihood Ratings

Asset Value/Aggressor Likelihood Worksheet

ASSET VALUE/AGGRESSOR LIKELIHOOD WORKSHEET

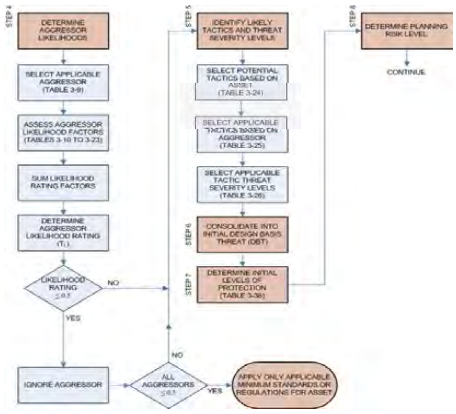
Project or Building: Motor Pool | Asset: Tactical Vehicles | Asset Category: D | Analyst: Planning Team | Date: Today

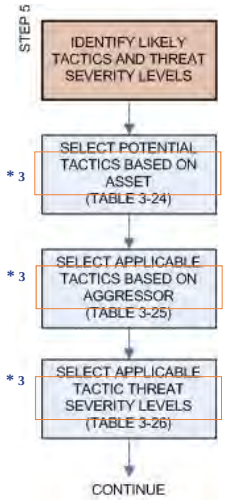
Value Rating Factors: Criticality to User[2]	Population Type[1]	Impact on National Defense	Replaceability	Political Sensitivity	Relative Value to User	Sum of Value Factors	Value Rating[2]	Potential Aggressors	Aggressor Goal[3]	Aggressors	Likelihood Rating Factors: Installation Location[5]	Publicity Profile[4]	Accessibility[4]	Availability[4]	Dynamics[4]	Recognizability	Relative Value to Aggressor	Law Enforcement[4]	Aggressors' Perception Success	Threat Level	History[7] / Intentions[5]	Operational Capability[6]	Operating Environment[6]	Activity[6]	Sum of Likelihood Factors	Likelihood Ratings[7]
General Population								✓	M	Unsophisticated Criminals	2	4													94	.52
Critical Infrastructure and Operations and Activities								✓	M	Sophisticated Criminals	2	4													91	.51
								✓	M	Organized Criminal Groups	2	4	2	2	3	15	9	18	30	6	6				97	.54
Sensitive Information								✓	P	Vandals	2	4	2	2	3	12	6	18	24	6	6				85	.47
All Other Assets								✓	P	Extremist Protesters	2	4	2	2	3	15	6	18	24	6	6				88	.49
4	4	4	3	4		19	.76	✓	P	Domestic Terrorists	2	4	2	2	3	15	9	18	24	5	4	4	6	4	102	.57
Notes:								✓	P	International Terrorists	2	4	2	2	3	15	9	18	30	5	8	6	10	2	116	.64
								✓	P	State Sponsored Terrorists	2	4	2	2	3	15	9	18	30	5	10	10	10	10	130	.72
								✓	G	Saboteurs	2	4	2	2	3	15	3	18	30	6	6				91	.51
										Foreign Intelligence Services																

Likelihoods ≤ 0.5 so these aggressors drop out

1. Population Type applies to General Population only
2. Sum of Value Ratings = 10 for Sensitive Information; 15 for General Population; 20 for Critical Infrastructure and Operations and Activities; 25 for all other assets
3. G for mission related goal, P for publicity related goal, M for monetary related goal
4. Factors that should be same for all aggressors for given asset
5. Applies to all aggressors other than terrorists
6. Applies to Terrorists only
7. Sum of Likelihood Ratings = 180

STEP 5 - IDENTIFY LIKELY TACTICS AND THREAT SEVERITY LEVELS

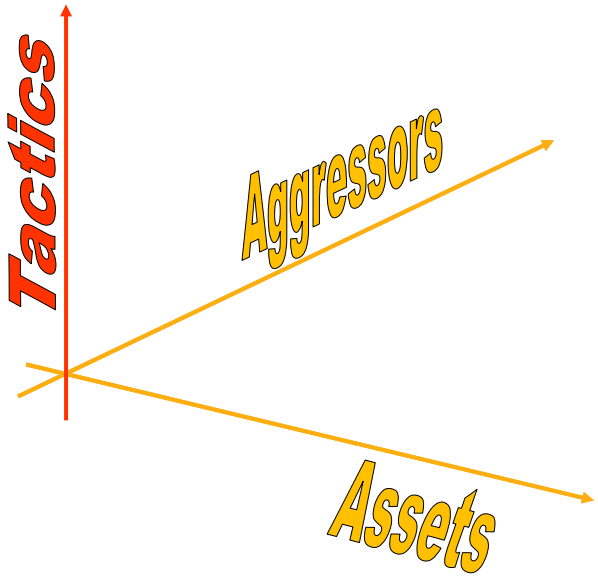




* Indicates value to be entered onto applicable worksheet

3. Tactic , Threat Severity, and Level of Protection Worksheet

Threat



Applicable Asset/Tactics
Table 3-24

	Asset Categories	Moving Vehicle Bomb Tactic
A	People	✓
B	Aircraft and Components at Aviation Facilities	
C	Ships, Boats, and Other Watercraft	
D	Vehicles and carriage mounted or towed weapons systems	
E	Petroleum, Oils, and Lubricants	
F	Arms, Ammunition, and Explosives	
G	Controlled Medical Substances and Medically Sensitive Items	
H	Communications / Electronics Equipment and Night Vision Devices	
I	Organizational Clothing and Individual Equipment	
J	Subsistence Items at Commissaries, Warehouses, & Troop Issue Facilities	
K	Repair Parts at Installation Supply and Direct Support Units	
L	Facilities Engineering Supplies and Construction Material	
M	Audiovisual Equipment, Training Devices, and Subcaliber Devices	
N	Miscellaneous Pilferable Assets (other than above) and Money	
O	Critical Infrastructure and Utility Equipment	
P	Controlled Cryptographic Items	
Q	Sensitive Information	
R	Activities and Operations	✓

	Asset Categories
A	People
B	Aircraft and Components at Aviation Facilities
C	Ships, Boats, and Other Watercraft
D	Vehicles and carriage mounted or towed weapons systems
E	Petroleum, Oils, and Lubricants
F	Arms, Ammunition, and Explosives
G	Controlled Medical Substances and Medically Sensitive Items
H	Communications / Electronics Equipment and Night Vision Devices
I	Organizational Clothing and Individual Equipment

Applicable Asset/Tactics
Table 3-24

	Asset Categories	Moving Vehicle Bomb Tactic	Stationary Vehicle Bomb Tactic	Hand Delivered Devices	Indirect Fire Weapons	Direct Fire Weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
		Applicable Tactics												
A	People	✓	✓	✓	✓	✓	✓	✓				✓	✓	
B	Aircraft and Components at Aviation Facilities		✓	✓	✓	✓	✓	✓						
C	Ships, Boats, and Other Watercraft		✓	✓	✓	✓	✓	✓						✓
D	Vehicles and carriage mounted or towed weapons systems		✓	✓	✓	✓	✓	✓						✓
E	Petroleum, Oils, and Lubricants						✓	✓						
F	Arms, Ammunition, and Explosives						✓	✓	✓	✓	✓			
G	Controlled Medical Substances and Medically Sensitive Items						✓	✓	✓	✓	✓	✓	✓	✓
H	Communications / Electronics Equipment and Night Vision Devices						✓	✓	✓	✓	✓			
I	Organizational Clothing and Individual Equipment						✓	✓						
J	Subsistence Items at Commissaries, Warehouses, & Troop Issue Facilities						✓	✓						
K	Repair Parts at Installation Supply and Direct Support Units						✓	✓						
L	Facilities Engineering Supplies and Construction Material						✓	✓						
M	Audiovisual Equipment, Training Devices, and Subcaliber Devices						✓	✓						
N	Miscellaneous Pilferable Assets (other than above) and Money						✓	✓						
O	Critical Infrastructure and Utility Equipment		✓	✓	✓	✓	✓	✓						✓
P	Controlled Cryptographic Items						✓	✓						
Q	Sensitive Information						✓	✓	✓	✓	✓			
R	Activities and Operations	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Applicable Aggressor/Tactics
Table 3-25

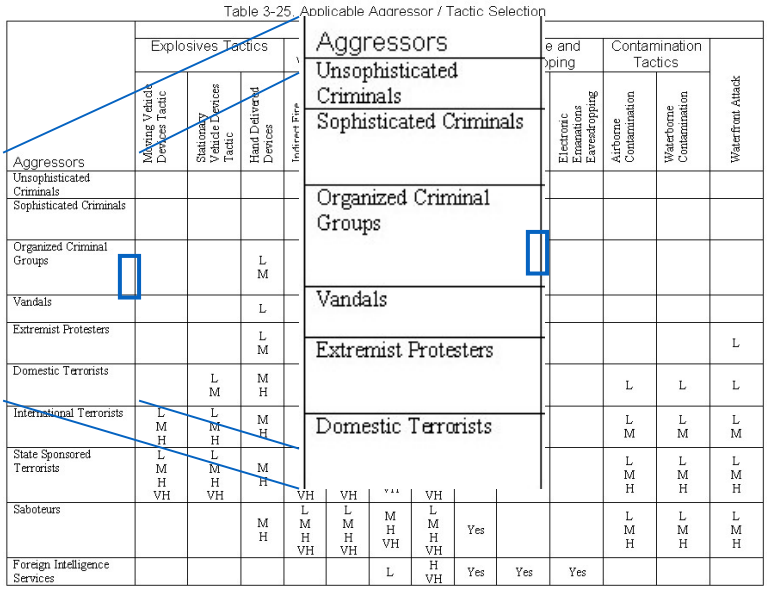


Table 3-25. Applicable Aggressor / Tactic Selection

Aggressors	Explosives Tactics			Standoff Weapons		Entry Tactics		Surveillance and Eavesdropping			Contamination Tactics		
	Moving Vehicle Devices Tactic	Stationary Vehicle Devices Tactic	Hand Delivered Devices	Indirect Fire Weapons	Direct Fire Weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Unsophisticated Criminals							L	L					
Sophisticated Criminals							L M H	L					
Organized Criminal Groups			L M										
Vandals			L										
Extremist Protesters			L M										L
Domestic Terrorists		L M	M H								L	L	L
International Terrorists	L M H	L M H	M H								L M	L M	L M
State Sponsored Terrorists	L M H VH	L M H VH	M H								L M H	L M H	L M H
Saboteurs			M H	L M H VH	L M H VH	M H VH	L M H VH	Yes			L M H	L M H	L M H
Foreign Intelligence Services						L	H VH	Yes	Yes	Yes			

Aggressors
- Unsophisticated Criminals
- Sophisticated Criminals
- Organized Criminal Groups
- Vandals
- Extremist Protesters
- Domestic Terrorists

Applicable Aggressor/Tactics
Table 3-25

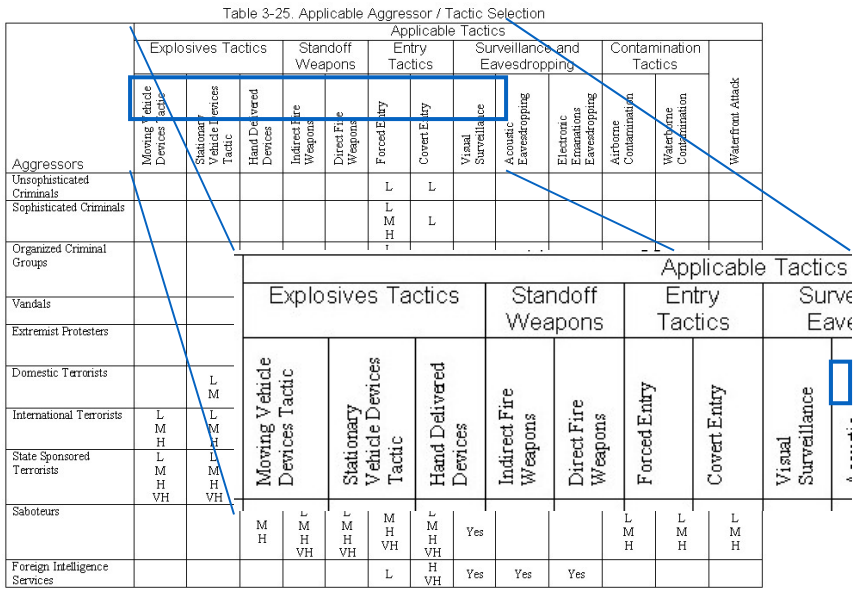


Table 3-25. Applicable Aggressor / Tactic Selection

Aggressors	Applicable Tactics												
	Explosives Tactics			Standoff Weapons		Entry Tactics		Surveillance and Eavesdropping			Contamination Tactics		
	Moving Vehicle Devices Tactic	Stationary Vehicle Devices Tactic	Hand Delivered Devices	Indirect Fire Weapons	Direct Fire Weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Unsophisticated Criminals						L	L						
Sophisticated Criminals						L M H	L						
Organized Criminal Groups													
Vandals													
Extremist Protesters													
Domestic Terrorists		L M											
International Terrorists	L M H	L M H											
State Sponsored Terrorists	L M H VH	L M H VH											
Saboteurs			M H	L M H VH	L M H VH	M H VH	L M H VH	Yes			L M H	L M H	L M H
Foreign Intelligence Services						L	H VH	Yes	Yes	Yes			

Documentation of Aggressor Likelihood
Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building	Asset		Analyst
Motor Pool	Asset Category: D	Asset Value: .76	Date: Today

Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices: Moving Vehicle Devices	Explosives and Incendiary Devices: Stationary Vehicle Devices	Explosives and Incendiary Devices: Hand Delivered Devices	Standoff Weapons: Indirect Fire Weapons	Standoff Weapons: Direct fire weapons	Entry: Forced Entry	Entry: Covert Entry	Surveillance and Eavesdropping: Visual Surveillance	Surveillance and Eavesdropping: Acoustic Eavesdropping	Surveillance and Eavesdropping: Electronic Emanations Eavesdropping	Contamination: Airborne Contamination	Contamination: Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52													
Sophisticated Criminals	.51													
Organized Criminal Groups	.54													
Vandals	<0.5													
Extremist Protesters	<0.5													
Domestic Terrorists	.57													
International Terrorists	.64													
State Sponsored Terrorists	.72													
Saboteurs	.51													
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)														
Initial Level of Protection for Applicable Tactic (Table 3-28)														

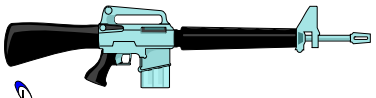
From Applicable Asset/Tactics (Table 3-24)

Assess Threat Severity Level

(Based on aggressors' likelihoods of aggression)

13 TACTICS

- WEAPONS



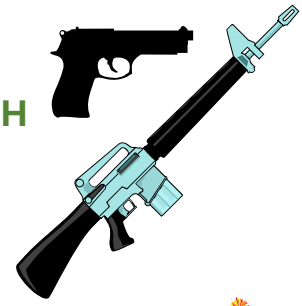
- TOOLS

- EXPLOSIVES

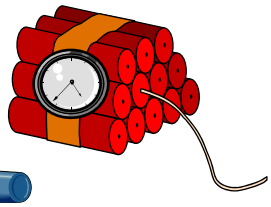
- AGENTS

Threat Severities
From Table 3-25

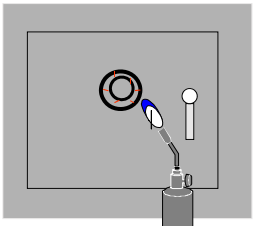
HIGH



MEDIUM



LOW



YES/NO

Threat Severity Level Selection
Table 3-25

Table 3-25. Applicable Aggressor / Tactic Selection

Aggressors	Applicable Tactics												
	Explosives Tactics			Standoff Weapons		Entry Tactics		Surveillance and Eavesdropping			Contamination Tactics		
	Moving Vehicle Devices Tactic	Stationary Vehicle Devices Tactic	Hand Delivered Devices	Indirect Fire Weapons	Direct Fire Weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Unsophisticated Criminals						L	L						
Sophisticated Criminals						L M H	L				L	L	
Organized Criminal Groups			L M		L M H	L M H VH	L				L M	L M	
Vandals			L		L	L	L						
Extremist Protesters			L M	L	L M H	L M	L M				L M	L M H	Yes
Domestic Terrorists		L M	M H	L M	L M H	L M	L M H	Yes			L M H	L M H	Yes
International Terrorists	L M H	L M H	M H	L M H	L M H	L M H	L M H	Yes			M H VH	L M H VH	Yes
State Sponsored Terrorists	L M H VH	L M H VH	M H	L M H VH	L M H VH	M H VH	L M H VH	Yes					
Saboteurs			M H	L M H VH	L M H VH	M H VH	L M H VH	Yes					
Foreign Intelligence Services						L	H VH	Yes	Yes	Yes			

Threat Severity Level Selection
Table 3-26

Table 3-26. Threat Severity Selection

Number of Threat Severity Level Choices *	Likelihood Rating				
	≤ 0.5	0.51 – 0.74	0.75 – 0.89	0.90 – 0.94	0.95 – 1
4	Minimum	1st	2nd	3rd	4th
3	Minimum	1st	2nd	3rd	3rd
2	Minimum	1st	1st	2nd	2nd
1	Minimum	1st	1st	1st	1st
* See Table 3-25					

Documentation of Threat Severity Level
Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building	Asset		Analyst	
Motor Pool	Asset Category: D	Asset Value: .76	Date: Today	Planning Team

Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices			Standoff Weapons		Entry		Surveillance and Eavesdropping			Contamination		
		Moving Vehicle Devices	Stationary Vehicle Devices	Hand Delivered Devices	Indirect Fire Weapons	Direct fire weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52													
Sophisticated Criminals	.51													
Organized Criminal Groups	.54													
Vandals														
Extremist Protesters														
Domestic Terrorists	.57													
International Terrorists	.64													
State Sponsored Terrorists	.72													
Saboteurs	.51													
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)														
Initial Level of Protection for Applicable Tactic (Table 3-28)														

Documentation of Threat Severity Level

Tactic, Threat Severity and LOP Worksheet

Table 3-25. Applicable Aggressor / Tactic Selection

Aggressors	Applicable Tactics: Explosives Tactics: Moving Vehicle Devices Tactic	Explosives Tactics: Stationary Vehicle Devices Tactic	Explosives Tactics: Hand Delivered Devices	Standoff Weapons: Indirect Fire Weapons	Standoff Weapons: Direct Fire Weapons	Entry Tactics: Forced Entry	Entry Tactics: Covert Entry	Surveillance and Eavesdropping: Visual Surveillance	Surveillance and Eavesdropping: Acoustic Eavesdropping	Surveillance and Eavesdropping: Electronic Emanations Eavesdropping	Contamination Tactics: Airborne Contamination	Contamination Tactics: Waterborne Contamination	Waterfront Attack
Unsophisticated Criminals						L	L						
Sophisticated Criminals						L M H	L						
Organized Criminal Groups			L M		L M H	L M H VH	L						
Vandals			L		L	L	L						
Extremist Protesters			L M	L	L M H	L M	L M						L
Domestic Terrorists		L M	M H	L M	L M H	L M	L M H	H			L	L	L
International Terrorists	L M H	L M H	M H	L M H	L M H	L M H	L M H	H			L M	L M	L M
State Sponsored Terrorists	L M H VH	L M H VH	M H	L M H VH	L M H VH	M H VH	L M H VH	H			L M H	L M H	L M H
Saboteurs			M H	L M H VH	L M H VH	M H VH	L M H VH	H			L M H	L M H	L M H
Foreign Intelligence Services						L	H VH	H	H	H			

Documentation of Threat Severity Level

Tactic, Threat Severity and LOP Worksheet

Table 3-25. Applicable Aggressor / Tactic Selection

Aggressors	Applicable Tactics: Explosives Tactics: Moving Vehicle Devices Tactic	Explosives Tactics: Stationary Vehicle Devices Tactic	Explosives Tactics: Hand Delivered Devices	Standoff Weapons: Indirect Fire Weapons	Standoff Weapons: Direct Fire Weapons	Entry Tactics: Forced Entry	Entry Tactics: Covert Entry	Surveillance and Eavesdropping: Visual Surveillance	Surveillance and Eavesdropping: Acoustic Eavesdropping	Surveillance and Eavesdropping: Electronic Emanations Eavesdropping	Contamination Tactics: Airborne Contamination	Contamination Tactics: Waterborne Contamination	Waterfront Attack
Unsophisticated Criminals						L	L						
Sophisticated Criminals						L M H	L						
Organized Criminal Groups			L M		L M H	L M H VH	L						
Vandals			L		L	L	L						
Extremist Protesters			L M	L	L M H	L M	L M						L
Domestic Terrorists		L M	M H	L M	L M H	L M	L M H	H			L	L	L
International Terrorists	L M H	L M H	M H	L M H	L M H	L M H	L M H	H			L M	L M	L M
State Sponsored Terrorists	L M H VH	L M H VH	M H	L M H VH	L M H VH	M H VH	L M H VH	H			L M H	L M H	L M H
Saboteurs			M H	L M H VH	L M H VH	M H VH	L M H VH	H			L M H	L M H	L M H
Foreign Intelligence Services						L	H VH	H	H	H			

ORGANIZED CRIMINAL GROUPS = .54

Table 3-26. Threat Severity Selection

Number of Threat Severity Level Choices *	Likelihood Rating: ≤ 0.5	0.51 – 0.74	0.75 – 0.89	0.90 – 0.94	0.95 – 1
4	Minimum	1st	2nd	3rd	4th
3	Minimum	1st	2nd	3rd	3rd
2	Minimum	1st	1st	2nd	2nd
1	Minimum	1st	1st	1st	1st

* See Table 3-25

Documentation of Threat Severity Level

Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building	Asset	Asset Category	Asset Value	Analyst	Date
Motor Pool	Tactical Vehicles	D	.76	Planning Team	Today

Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices			Standoff Weapons		Entry		Surveillance and Eavesdropping			Contamination		
		Moving Vehicle Devices	Stationary Vehicle Devices	Hand Delivered Devices	Indirect Fire Weapons	Direct fire weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52													
Sophisticated Criminals	.51													
Organized Criminal Groups	.54						L							
Vandals														
Extremist Protesters														
Domestic Terrorists	.57													
International Terrorists	.64													
State Sponsored Terrorists	.72													
Saboteurs	.51													
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)														
Initial Level of Protection for Applicable Tactic (Table 3-28)														

Documentation of Threat Severity Level

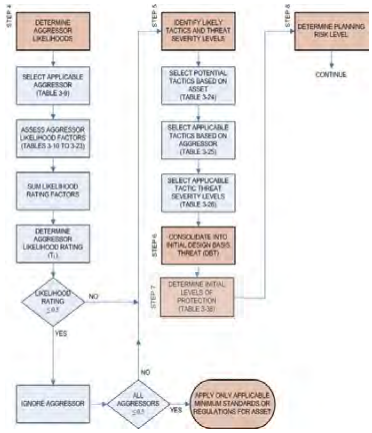
Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building	Asset	Asset Category	Asset Value	Analyst	Date
Motor Pool	Tactical Vehicles	D	.76	Planning Team	Today

Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices			Standoff Weapons		Entry		Surveillance and Eavesdropping			Contamination		
		Moving Vehicle Devices	Stationary Vehicle Devices	Hand Delivered Devices	Indirect Fire Weapons	Direct fire weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52						L	L						
Sophisticated Criminals	.51						L	L						
Organized Criminal Groups	.54			L		L	L	L						
Vandals														
Extremist Protesters														
Domestic Terrorists	.57		L	M	L	L	L	L						L
International Terrorists	.64		L	M	L	L	L	L						L
State Sponsored Terrorists	.72		L	M	L	L	M	L						L
Saboteurs	.51			M	L	L	M	L						L
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)														
Initial Level of Protection for Applicable Tactic (Table 3-28)														

STEP 6: INITIAL DESIGN BASIS THREAT (DBT)



- **Initially, the worst case threat severity levels for each applicable tactic.**
- **The initial threat upon which a protective system of countermeasures will be based**
- **May be May be revised based on Planning Team decision or due to Combatant Command standards**

Documentation of Initial Design Basis Threat

Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building		Asset	Tactical Vehicles						Analyst	Planning Team						
Motor Pool		Asset Category	D		Asset Value	.76			Date	Today						
Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices			Standoff Weapons		Entry		Surveillance and Eavesdropping			Contamination			
		Moving Vehicle Devices	Stationary Vehicle Devices	Hand Delivered Devices	Indirect Fire Weapons	Direct fire weapons	Forced Entry	Covert Entry	Visual Surveillance	Acoustic Eavesdropping	Electronic Emanations Eavesdropping	Airborne Contamination	Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52						L	L						
Sophisticated Criminals	.51						L	L						
Organized Criminal Groups	.54			L		L	L	L						
Vandals														
Extremist Protesters														
Domestic Terrorists	.57		L	M	L	L	L	L						L
International Terrorists	.64		L	M	L	L	L	L						L
State Sponsored Terrorists	.72		L	M	L	L	M	L						L
Saboteurs	.51			M	L	L	M	L						L
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)			L	M	L	L	M	L						L
Initial Level of Protection for Applicable Tactic (Table 3-28)														

Documentation of Initial Design Basis Threat
Design Criteria Summary Worksheet

DESIGN CRITERIA SUMMARY WORKSHEET

Project or Building: Motor Pool | Analyst: Planning Team | Date: Today

Assets	Asset Category	Asset Value Rating	Tactics: Explosive and Incendiary Devices – Moving Vehicle Devices DBT	Moving Vehicle Devices LOP	Stationary Vehicle Devices DBT	Stationary Vehicle Devices LOP	Hand Delivered Devices DBT	Hand Delivered Devices LOP	Standoff Weapons – Indirect Fire Weapons DBT	Indirect Fire Weapons LOP	Direct fire weapons DBT	Direct fire weapons LOP	Entry Tactics – Forced Entry DBT	Forced Entry LOP	Covert Entry DBT	Covert Entry LOP	Surveillance and Eavesdropping – Visual Surveillance DBT	Visual Surveillance LOP	Acoustic Eavesdropping DBT	Acoustic Eavesdropping LOP	Electronic Emanations Eavesdropping DBT	Electronic Emanations Eavesdropping LOP	Contamination Tactics – Airborne Contamination DBT	Airborne Contamination LOP	Waterborne Contamination DBT	Waterborne Contamination LOP	Waterfront Attack DBT	Waterfront Attack LOP
Tactical Vehicles	D	.76			L		M		L		L		M		L												L	

DBT = Design Basis Threat severity level LOP = Level of Protection

Threat Parameters
Table 3-27

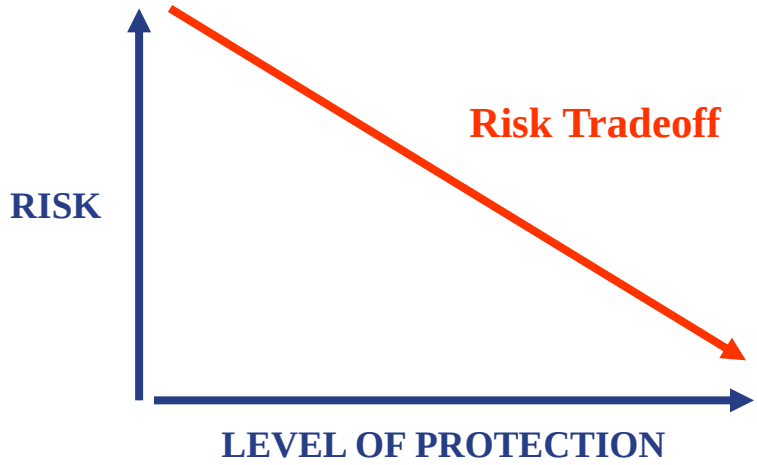
Aggressor Tactic	Design Basis Threat	Weapons	Tools Or Delivery Method
Moving and Stationary Vehicle Devices	Special Case [1]	19,800 lbs (9000 kg) TNT	Heavy goods vehicle[2] (65,000 lbs /29500 kg)
	Very High	4400 lbs (2000 kg) TNT, Fuel	Medium duty truck or Class 7 cabover[2] (15000 lbs / 6800 kg) or (15873 lbs / 7200 kg)
	High	1100 lbs (500 kg) TNT, Fuel	Medium duty truck or Class 7 cabover[2] (15000 lbs / 6800 kg) or (15873 lbs / 7200 kg)
	Medium	550 lbs (250 kg) TNT, Fuel	Pickup truck[2] (5070 lbs. / 2300 kg)
	Low	220 lbs (100 kg) TNT	Full-size sedan[2] (4630 lbs / 2100 kg)
	Very Low	55 lbs (25 kg) TNT	Full-size sedan[2] (4630 lbs / 2100 kg)
Hand Delivered Devices	High	IID, IED (up to 55 lbs / 25 kg TNT) &hand grenades (Mail bomb limited to 2.2 lbs / 1 kg TNT)	None
	Medium	IID, IED (up to 2.2 lbs / 1 kg TNT) & hand grenades	
	Low	IID	
Indirect Fire Weapons Attack	Very High	Improvised mortar (up to 44 lbs 20 kg/ TNT)	None
	High	122 mm rocket	
	Medium	82 mm mortar	
	Low	Incendiary devices	
Direct Fire Weapons Attack	Very High	Light antitank weapons, and UL 752 Level 10 (0.50 caliber / 12.7 mm, 1 shot)	None
	High	UL 752 Level 9 (7.62mm NATO AP, 1 shot)	
	Medium	UL 752 Level 5 (7.62mm NATO ball)	
	Low	UL 752 Level 3 (.44 magnum)	
Waterfront Attack	High	1100 lbs (500 kg) TNT (surface or submerged) Anti-Tank Weapons UL 752 Level 10 (0.50 caliber / 12.7 x 99 mm)	High performance boat[3] (10,000 lbs / 4500 kg)
	Medium	550 lbs (250 kg) TNT (surface) 55 lbs (25 kg) TNT (submerged) UL 752 Level 10 (0.50 caliber / 12.7 x 99 mm)	Power boat[3] (5000 lbs / 2300 kg)
	Low	220 lbs (100 kg) TNT (surface) 55 lbs (25 kg) TNT (submerged) UL 752 Level 5 (7.62mm NATO ball)	Rigid Hulled Inflatable Boats[3] (2000 lbs / 900 kg)

Threat Parameters
Table 3-27

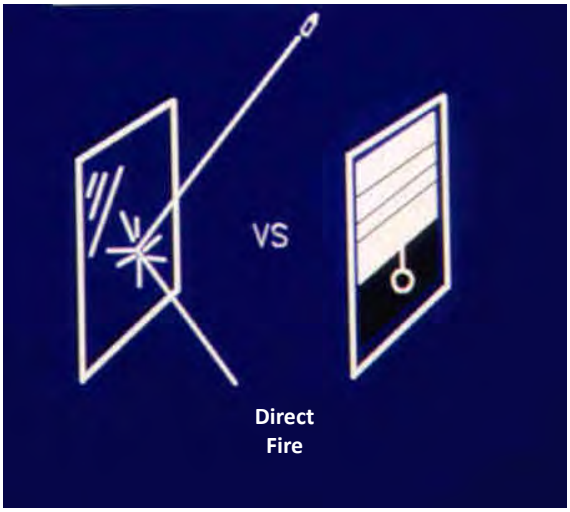
Active Shooter	High	UL 752 Level 5 (7.62mm NATO ball)	None
	Low	UL 752 Level 3 (.44 magnum)	
Airborne Contamination	High	Internal and external release of all agents listed below	Limited hand tools +2.2 lbs (1 kg) TNT explosive (dirty bomb)
	Medium	Agents associated with Low plus external release of toxic military chemical agents	Limited hand tools
	Low	Agents associated with Very Low plus external release of biological and radiological particulates	
	Very Low	External and internal release of Toxic Industrial Chemicals or Toxic Industrial Materials (TIC and TIM)	
Waterborne Contamination	High	Liquid or particulate agent stable in water greater than 30 days and not easily mitigated by chlorine	Limited hand tools
	Medium	Liquid or particulate agent stable in water between 2 hours and 30 days and not easily mitigated by chlorine	
	Low	Liquid or particulate agent stable in water less than 2 hours or easily mitigated by chlorine	
Forced Entry	Very High	Handguns and sub-machine guns (up to UL 752 Level 3 to overpower guards)	Bulk explosives (up to 20 lbs / 9 kg TNT), linear shaped charges (up to 10,500 grains per foot), unlimited hand, power, thermal tools
	High		Unlimited hand, power, and thermal tools
	Medium	None	Unlimited hand tools - limited power tools
	Low		Limited hand tools - low observables
Covert Entry	Very High	Handgun	Electronic Neutralization Equipment Drill & Specialized Tools Robotic Dialer Manipulation Enhancer
	High	Handgun	Mechanical & Electronic Lock Decoder Drill, simple tools & camouflage Specialized bypass tools
	Medium	None	Lock Picks Bypass techniques High Quality False Credentials Observation tools
	Low	None	Easily Duplicated False Credentials
Visual Surveillance	High	None	Ocular devices
Acoustic Eavesdropping	High		Sound amplification or laser "listening" devices
Electronic Emanations Eavesdropping	High		Electronic emanations interception equipment

1. Note that the process in this UFC does not lead to the Special Case. Applicability is known by those to whom it applies.
2. Vehicle designations are from ASTM F2656.
3. Boat designations are from ASTM F2766.

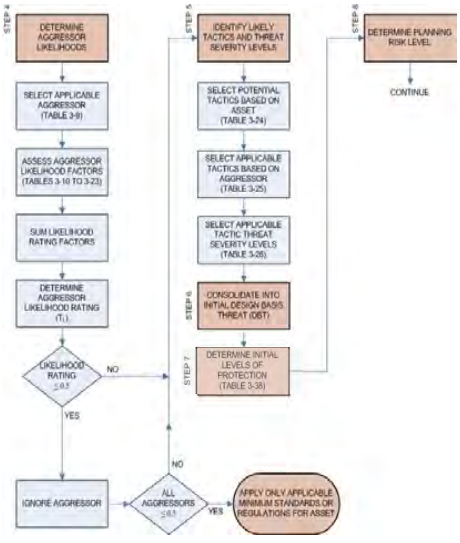
Level of Protection



Level of Protection Based on Asset Value



STEP 7: INITIAL LEVEL OF PROTECTION



- The degree to which an asset (e.g., a person, a piece of equipment, or an object, etc.) is protected against injury or damage from an attack.
- Based initially on asset value
- May be modified by planning team (commonly due to cost)

Level of Protection Selection
Table 3-28

Table 3-28. Applicable Levels of Protection

Tactic	Threat Severity Level	Asset Value ≤ 0.5	0.51 – 0.74	0.75 – 0.85	0.86 – 0.95	0.96 - 1
Moving Vehicle Bomb	All	Very Low[1]	Low[2]	Medium	High	
Stationary Vehicle Bomb	All	Very Low[1]	Low[2]	Medium	High	
Hand Delivered Devices	All	Very Low[1]	Low[2]	Medium	High	
Indirect Fire Weapons	All	Very Low[1]	Low	Medium	High	
Direct Fire Weapons	VH	Very Low[1]	Low	Medium[3]	High	
	L, M, H	Very Low[1]	Low		High	
Forced Entry	All	Very Low[1]	Low	Medium	High	Very High
Covert Entry	All		Low	Medium	High	Very High
Visual Surveillance	All		High			
Acoustic Eavesdropping	All		Low	Medium	High	Very High
Electronic Emanations Eavesdropping	All		High			
Airborne Contaminants	All	Very Low[1]	Low	Medium	High	
Waterborne Contaminants	All	Very Low[1]	Low	Medium	High	
Waterfront Attack	All	Very Low[1]	Low	Medium[3]	High	Very High

1. The very low level of protection includes only measures required by UFC 4-010-01 minimum standards or other applicable standards, operations orders, or regulations.
2. The low level of protection is the minimum for those tactics that are addressed in UFC 4-010-01 for primary gathering buildings. Note also that while the moving vehicle bomb tactic is not expressly addressed in UFC 4-010-01, if it applies it should also be given the same minimum level of protection as the stationary vehicle bomb tactic for primary gathering buildings.
3. The medium level of protection commonly does not apply to ballistics below 12.7 mm (.50 caliber), which are the weapons in the low through high threat severity levels. For those threat severity levels, apply the low level of protection for this range of asset value ratings.

Documentation of Initial Level of Protection
Tactic, Threat Severity and LOP Worksheet

TACTIC, THREAT SEVERITY, AND LEVEL OF PROTECTION WORKSHEET

Project or Building	Asset	Asset Category	Asset Value	Analyst	Date
Motor Pool	Tactical Vehicles	D	.76	Planning Team	Today

Tactics / Aggressors	Aggressor Likelihood	Explosives and Incendiary Devices: Moving Vehicle Devices	Explosives and Incendiary Devices: Stationary Vehicle Devices	Explosives and Incendiary Devices: Hand Delivered Devices	Standoff Weapons: Indirect Fire Weapons	Standoff Weapons: Direct fire weapons	Entry: Forced Entry	Entry: Covert Entry	Surveillance and Eavesdropping: Visual Surveillance	Surveillance and Eavesdropping: Acoustic Eavesdropping	Surveillance and Eavesdropping: Electronic Emanations Eavesdropping	Contamination: Airborne Contamination	Contamination: Waterborne Contamination	Waterfront Attack
Applicable Tactics			✓	✓	✓	✓	✓	✓						✓
Unsophisticated Criminals	.52						L	L						
Sophisticated Criminals	.51						L	L						
Organized Criminal Groups	.54			L		L	L	L						
Vandals														
Extremist Protesters														
Domestic Terrorists	.57		L	M	L	L	L	L						L
International Terrorists	.64		L	M	L	L	L	L						L
State Sponsored Terrorists	.72		L	M	L	L	M	L						L
Saboteurs	.51			M	L	L	M	L						L
Foreign Intelligence Services														
Initial Design Basis Threat (highest Threat Severity Level for each tactic)			L	M	L	L	M	L						L
Initial Level of Protection for Applicable Tactic (Table 3-28)			M	M	M	L	M	M						M

Documentation of Initial Level of Protection
Design Criteria Summary Worksheet

DESIGN CRITERIA SUMMARY WORKSHEET

Project or Building: Motor Pool | Analyst: Planning Team | Date: Today

Assets	Asset Category	Asset Value Rating	Tactics: Explosive and Incendiary Devices – Moving Vehicle Devices DBT	Moving Vehicle Devices LOP	Stationary Vehicle Devices DBT	Stationary Vehicle Devices LOP	Hand Delivered Devices DBT	Hand Delivered Devices LOP	Standoff Weapons – Indirect Fire Weapons DBT	Indirect Fire Weapons LOP	Direct fire weapons DBT	Direct fire weapons LOP	Entry Tactics – Forced Entry DBT	Forced Entry LOP	Covert Entry DBT	Covert Entry LOP	Surveillance and Eavesdropping – Visual Surveillance DBT	Visual Surveillance LOP	Acoustic Eavesdropping DBT	Acoustic Eavesdropping LOP	Electronic Emanations Eavesdropping DBT	Electronic Emanations Eavesdropping LOP	Contamination Tactics – Airborne Contamination DBT	Airborne Contamination LOP	Waterborne Contamination DBT	Waterborne Contamination LOP	Waterfront Attack DBT	Waterfront Attack LOP
Tactical Vehicles	D	.76			L	M	M	M	L	M	L	L	M	M	L	M											L	M

DBT = Design Basis Threat severity level LOP = Level of Protection

STEP 8: DETERMINE PLANNING RISK LEVELS

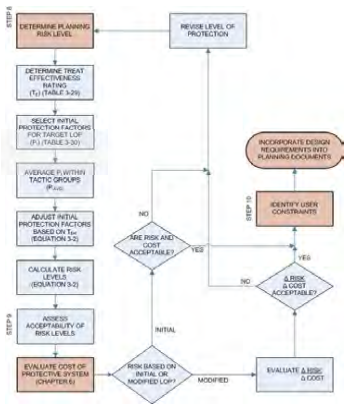
- **Risk levels are based on:**
  - **Asset Values**
  - **Aggressor Likelihoods**
  - **Protection Factors**
    - Protection Factors reflect levels of protection provided to the assets.

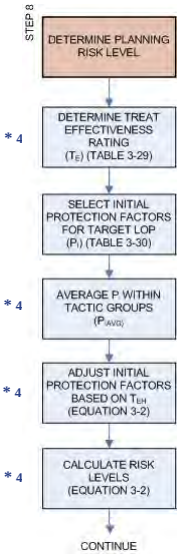
- **Note: risk in this UFC is a relative risk level that is intended to be used as an aid in decision making.**
  - **A more detailed treatment of risk that considers the contribution of specific countermeasures is in UFC 4-020-02, Security Engineering Facilities Design Manual (Currently in Draft)**

Acceptable Risk Levels

- **There are no specific criteria for determining whether or not a given risk level is acceptable.**
- **Risk levels in this process are relative.**
  - Risk level means relatively little by itself, but when the reduction in risk can be evaluated with respect to the cost of a protective system, that provides a means of evaluating benefit versus cost.
- **The benefit is the reduction in risk**
  - **Example:** If a large expenditure for countermeasures results in a very small reduction in risk, that would not be a good investment. On the other hand, when a small expenditure for countermeasures results in a large reduction in risk, that may be a good investment.

STEP 8: PLANNING RISK LEVEL





*** Indicates value to be entered onto applicable worksheet**

4. Risk Level Calculation Worksheet

Threat Effectiveness Rating (T_{EH})
Table 3-29

Determine Threat Effectiveness Rating (T_{EH})

Table 3-29. Threat Effectiveness Ratings	
Aggressor Type	Effectiveness Rating (T_E)
Unsophisticated criminals	1.0
Sophisticated criminals	0.98
Organized criminal groups	0.95
Vandals	1.0
Extremist protest groups	0.96
Domestic terrorists	0.95
International terrorists	0.93
State sponsored terrorists	0.90
Saboteurs	0.90
Foreign intelligence services	0.91

Risk Level Calculation Worksheet
Asset Value, Threat Likelihood, Threat Effectiveness, LOP

RISK LEVEL CALCULATION WORKSHEET

Project or Building: *A Motor Pool*

Asset: *Tactical vehicles*

Asset Value (Av): *0.76*

Planning Team

TODAY

Aggressor	T_L[1]	T_E (Table 3-29)	Highest[2] T_C ($T_{C'}$)	T_{INT}[3]	Tactic	LOP[1]	P_I[4] (Table 3-30)	Avg[5] P_I ($P_{I'}$)	P_E[6] Aggressor Category C	T	S	F	Risk Level[7] Aggressor Category C	T	S	F
Domestic (D): Unsophisticated Criminals	.52	1.0	.54	.95	Explosives and Incendiaries: Moving Vehicle Bomb											
Domestic (D): Sophisticated Criminals	.81	.98			Stationary Vehicle Bomb											
Domestic (D): Organized Criminal Groups	.54	.95			Hand Delivered Devices											
Domestic (D): Vandals	< .5				Standoff Weapons: Indirect Fire Weapons											
Terrorists (T): Extremist Protesters	< .5				Direct Fire Weapons											
Terrorists (T): Domestic Terrorists	.87	.95	.72	.90	Entry Tactics: Forced Entry											
Terrorists (T): International Terrorists	.64	.93			Covert Entry											
Terrorists (T): State Sponsored Terrorists	.72	.90			Surveillance and Eavesdropping: Visual Surveillance											
[illegible]	[illegible]	[illegible]	.51	.00	Acoustic Eavesdropping											
Foreign Intelligence Services (F)					Electronic Emanations Eavesdropping											
					Contamination Tactics: Airborne Contamination											
					Waterborne Contamination											
					Waterfront Attack											

1. From Tactic, Threat Severity, and LOP Worksheet.
2. Highest likelihood rating for each aggressor group.
3. Effectiveness rating for aggressor with highest likelihood.
4. From Table 3-30.
5. Average for P_I for all tactics within tactic group.
6. $P_E = T_{INT} \times P_{I(AVG)}$ for each aggressor & tactic group combination.
7. $R = Av \times T_{LH} \times (1-P_E)$ for each aggressor & tactic group.

Initial Protection Factors (P_I)
Table 3-30

Table 3-30. Initial Protection Factors	
Level of Protection	Protection Factor (P_I)
Very Low	0.1
Low	0.3
Medium	0.7
High	0.9
Very High	0.95

- At planning level, provides numeric measure of effectiveness of level of protection
- At design stage, may be calculated considering effects of individual countermeasures

Effective Protection Factor (P_E)
(Equation 3-1)

- Determine effective protection factors for each applicable tactic.
  - Enter the applicable threat effectiveness ratings (TEH) for each of the applicable aggressor categories associated with the applicable average initial protection factors (P_{IAVG}) into Equation 3-1.

$$P_E = T_{EH} \times P_{IAVG}$$

- Accounts for relative effectiveness of countermeasures against aggressors with different levels of sophistication

Risk Level Calculation Worksheet
Asset Value, Threat Likelihood, Threat Effectiveness, LOP

RISK LEVEL CALCULATION WORKSHEET

Project or Building:	Asset:	Planning Team
A Motor Pool	Tactical Vehicles	
	Asset Value (Av): 0.75	TODAY

	Aggressor	T_L[1]	T_E (Table 3-29)	Highest[2] T_L (T_{LH})	T_{LH}[2]	Tactic	LOP[3]	P_I[4] (Table 3-30)	Avg[5] P_I ($P_{I\ Avg}$)	P_E[6] Aggressor Category C	T	S	F	Risk Level[7] Aggressor Category C	T	S	F
Criminals (C)	Unsophisticated Criminals	.52	1.0	.54	.95	Explosive and Incendiary	Moving Vehicle Bomb										
	Sophisticated Criminals	.51	.98				Stationary Vehicle Bomb	M	.7	.7							
	Organized Criminal Groups	.54	.95				Hand Delivered Devices	M	.7								
	Vandals	< .5				Standoff Weapons	Indirect Fire Weapons	M	.7	.5							
Terrorists (T)	Extremist Protesters	< .5		.72	.90		Direct Fire Weapons	L	.3								
	Domestic Terrorists	.57	.95			Entry Tactics	Forced Entry	M	.7	.7							
	International Terrorists	.64	.93				Covert Entry	M	.7								
	State Sponsored Terrorists	.72	.90			Surveillance and Eavesdropping	Visual Surveillance										
	Saboteurs (S)	.51	.90	.51	.90		Acoustic Eavesdropping										
	Foreign Intelligence Services (F)						Electronic Emanations Eavesdropping										
						Contamination Tactics	Airborne Contamination										
							Waterborne Contamination										
						Waterfront Attack											

1. From Tactic, Threat Severity, and LOP Worksheet
2. Highest likelihood rating for each aggressor group.
3. Effectiveness rating for aggressor with highest likelihood
4. From Table 3-30.
5. Average for P_I for all tactics within tactic group.
6. $P_E = T_{LH} \times P_{I\ Avg}$ for each aggressor & tactic group combination.
7. $R = A_V \times T_{LH} \times (1-P_E)$ for each aggressor & tactic group.

Risk Level Calculation
Equation 3-2

- **Determine Risk Level. Calculate risk levels for each asset and for each applicable tactic group and aggressor group as indicated on the Risk Level Calculation Worksheet.**
- **Risk levels are established by entering the likelihood and asset value ratings and the protection effectiveness factors into Equation 3-2.**
  - **By subtracting P_E from 1, the risk equation reflects the fact that increases in protection effectiveness reduce risk. The 1- P_E term reflects "vulnerability"**

$$R = A_V \times T_{LH} \times (1-P_E)$$

Vulnerability

Risk Level Calculation Worksheet

Asset Value, Threat Likelihood, Threat Effectiveness, LOP

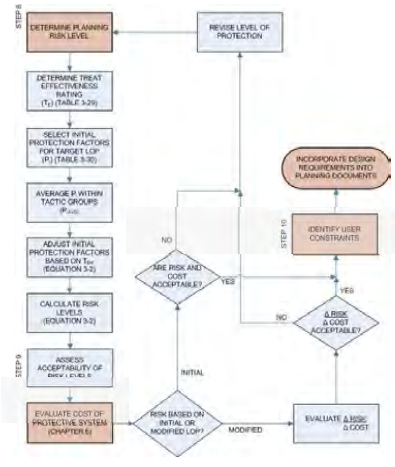
RISK LEVEL CALCULATION WORKSHEET

Project or Building:	Asset:	Planning Team
A Motor Pool	*Tactical Vehicles*	
	Asset Value (Av): *0.76*	TODAY

	Aggressor	T_i[1]	T_E (Table 3-29)	Highest[2] T_L (T...)	T_{AV}[3]	Tactic		LOP[4]	P_E[5] (Table 3-30)	Avg[6] P_I (P...)	P_R[7] Aggressor Category C	T	S	F	Risk Level[7] Aggressor Category C	T	S	F
Criminals (C)	Unsophisticated Criminals	.52	1.0	.54	.95	Explosives and Incendiaries	Moving Vehicle Bomb			.7		.62	.62			.20	.14	
	Sophisticated Criminals	.51	.98				Stationary Vehicle Bomb	M	.7									
	Organized Criminal Groups	.54	.93				Hand Delivered Devices	M	.7									
	Vandals	< .5				Standoff Weapons	Indirect Fire Weapons	M	.7	.5		.45	.45			.20	.21	
Terrorists (T)	Extremist Protesters	< .5		.72	.90		Direct Fire Weapons	L	.3									
	Domestic Terrorists	.57	.95			Entry Tactics	Forced Entry	M	.7	.7	.67	.62	.62		.14	.20	.14	
	International Terrorists	.64	.92				Covert Entry	M	.7									
	State Sponsored Terrorists	.72	.90			Surveillance and Eavesdropping	Visual Surveillance											
	Saboteurs (S)	.51	.90	.51	.90		Acoustic Eavesdropping											
	Foreign Intelligence Services (F)						Electronic Emanations Eavesdropping											
						Contaminants or Toxins	Airborne Contamination											
							Waterborne Contamination											
						Waterfront Attack												

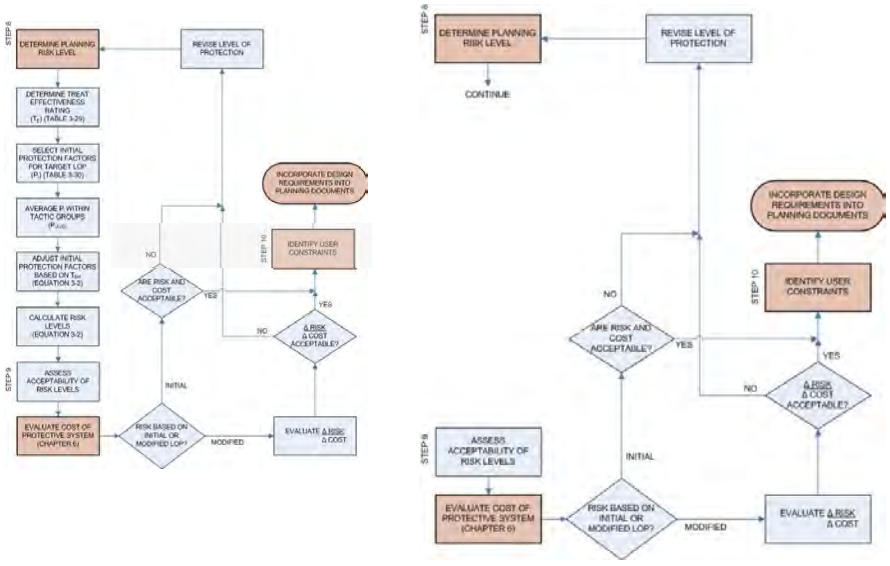
1. From Table, Threat Severity, and LOP Weighted.
2. Highest likelihood rating for each aggressor group.
3. Effectiveness rating for aggressor with highest likelihood.
4. From Table 3-30.
5. Average for P_I for all tactics within tactic group.
6. P_E = T_{AV} x P_{AVG} for each aggressor & tactic group combination.
7. R = Av x T_{AV} x (1-P_E) for each aggressor & tactic group.

STEP 9: ACCEPTABILITY OF RISK LEVELS



- **Risks using this process are relative**
- **Used to evaluate differences between risk impact of various alternatives**
- **Can be used as basis for benefit / cost ratios**
  - **Benefit is reduction in risk**
  - **Cost is….cost of protective system**

Evaluation of Risk



Building Cost and Risk Evaluation Worksheet

Initial

BUILDING COST AND RISK EVALUATION WORKSHEET

Project or Building: *A Motor Pool*

Asset: *Tactical Vehicles*

Baseline Building Category (Table 3-1): *Special Structure*

Planning Team

TODAY

Tactic			Design Basis Threat [2]	LOP[3] or P_i	Risk[4] Level	Standoff, Rn Size, # Stories	Cost Increase (%)	Cost Incr. Sum	Threat Severity Level	LOP[3,4] or P_f	Risk[4] Level	Standoff, Rn Size, # Stories	Cost Increase (%)	Cost Incr. Sum	Change[9] in Cost (%)	Change[10] in Risk (%)	Ratio[11]
			Initial						Revised						Analysis		
Explosives and Incendiaries	Moving Vehicle Bomb[5]																
	Stationary Vehicle Bomb[5]		M	M	(7)	25 m	27.1	27.9									
	Mail/Delivered Device																
	• Exterior		M	M	20	10 m	27.9										
	• Mail Room																
	• Loading Dock																
	• Entry Area																
Standoff Weapons	Indirect Fire Weapons		M	M	(7)		19	19.47									
	Direct Fire Weapons		M	L	20		0.37										
Entry Tactics	Forced Entry				(7)			1.8									
	• Exterior																
	• Interior[8]		H	M	20	large	0.8										
	Covert Entry		M	M			0.9										
Surveillance and Eavesdropping	Visual Surveillance																
	Acoustic Eavesdropping																
	• Exterior																
	• Interior[8]																
	Electronic Emanations Eavesdropping																
	• Exterior																
	• Interior[8]																
Contamination	Airborne Contamination																
	Waterborne Contamination																
	Waterfront Attack																
							Sum[12] (%)	43.07					Sum[12] (%)	30.37			

1. Use highest cost among these tactics
2. From Tactic, Threat Severity and LOP Worksheet
3. Level of Protection or Initial Protection Level
4. From Risk Level Calculation Worksheet
5. One risk level for each tactic group
6. Use risk level for aggressor whose threat severity level controls design basis threat (from Tactic, Threat Severity, and LOP worksheet)
7. Indicate which aggressor controls
8. From Appendix A or B or from other cost estimate
9. Revised cost sum – initial cost sum = initial cost sum
10. Revised risk level – initial risk level = initial risk level
11. Change in risk ÷ change in cost
12. Enter small, medium, or large room
13. Represents total building cost increase

Building Cost and Risk Evaluation Worksheet
Initial and Revised

BUILDING COST AND RISK EVALUATION WORKSHEET

Project or Building: *A Motor Pool*					Asset: *Tactical Vehicles* Baseline Building Category (*Table 3-1*): *Special Structure*							Planning Team TODAY						
		Initial						Revised						Analysis		
Tactic		Design Basis Threat[2]	LOP[3] or P_f	Risk[4,7] Level	Standoff, Min. Size, # Stories	Cost[5] Increase (%)	Cost Incr. Sum	Threat Severity Level	LOP[3] or P_f	Risk[4,7] Level	Standoff, Min. Size, # Stories	Cost[5] Increase (%)	Cost Incr. Sum	Change[9] in Cost (%)	Change[10] in Risk (%)	Ratio[11]
Explosives and Incendiaries	Moving Vehicle Bomb[1]															
	Stationary Vehicle Bomb[1]	M	M	(7)	25 m	21.1	21.9	M	L	(7)	25 m	10.6	10.6	-52	+.40	-.01
	Hand Delivered Device															
	• Exterior[1]	H	M	.20	10 m	21.9		H	L	.28	10 m	6.5				
	• Mail Room															
	• Loading Dock															
	• Entry Area															
Standoff Weapons	Indirect Fire Weapons	M	M	(7)		19	19.37	M	L	(7)		18.3	18.67	-3.6	+.40	-.11
	Direct Fire Weapons	M	L	.20		0.37		M	L	.28		0.37				
Entry Tactics	Forced Entry			(7)			1.8			(7)			1.1	-64	+.40	-01
	• Exterior															
	• Interior[8]	H	M	.20	large	0.9		H	L	.28	large	0.4				
	Covert Entry	M	M			0.9		M	L			0.7				
Surveillance and Eavesdropping	Visual Surveillance															
	Acoustic Eavesdropping															
	• Exterior															
	• Interior[8]															
	Electronic Emanations Eavesdropping															
	• Exterior															
	• Interior[8]															
Contamination	Airborne Contamination															
	Waterborne Contamination															
Waterfront Attack																
						Sum[12] (%)	43.07					Sum[12] (%)	30.37			

1. Use highest cost among these tactics
2. From Tactic, Threat Severity and LOP Worksheet
3. Level of Protection or Initial Protection Level
4. From Risk Level Calculation Worksheet
5. One risk level for each tactic group
6. Use risk level for aggressor whose threat severity level controls design basis threat (from Tactic, Threat Severity, and LOP worksheet)
7. Indicate which aggressor controls
8. From Appendix A or B or from other cost estimate
9. Revised cost sum – initial cost sum = initial cost sum
10. Revised risk level – initial risk level = initial risk level
11. Change in risk ÷ change in cost
12. Enter small, medium, or large room
13. Represents total building cost increase

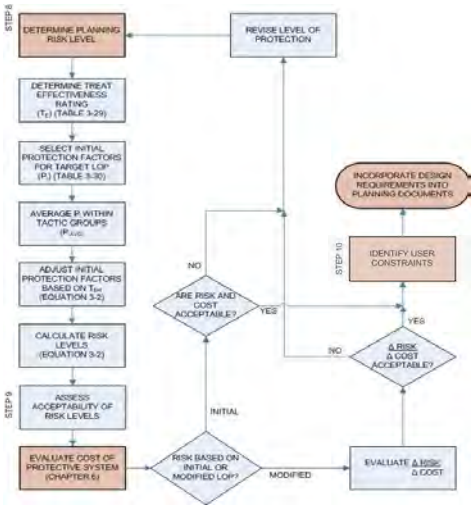
Building Cost and Risk Evaluation Worksheet
Initial and Revised w/Analysis – Cost Effectiveness

BUILDING COST AND RISK EVALUATION WORKSHEET

Project or Building: *A Motor Pool*					Asset: *Tactical Vehicles* Baseline Building Category (*Table 3-1*): *Special Structure*							Planning Team TODAY						
		Initial						Revised						Analysis		
Tactic		Design Basis Threat[2]	LOP[3] or P_f	Risk[4,7] Level	Standoff, Min. Size, # Stories	Cost[5] Increase (%)	Cost Incr. Sum	Threat Severity Level	LOP[3] or P_f	Risk[4,7] Level	Standoff, Min. Size, # Stories	Cost[5] Increase (%)	Cost Incr. Sum	Change[9] in Cost (%)	Change[10] in Risk (%)	Ratio[11]
Explosives and Incendiaries	Moving Vehicle Bomb[1]															
	Stationary Vehicle Bomb[1]	M	M	(7)	25 m	21.1	21.9	M	L	(7)	25 m	10.6	10.6	-52	+.40	-.01
	Hand Delivered Device															
	• Exterior[1]	H	M	.20	10 m	21.9		H	L	.28	10 m	6.5				
	• Mail Room															
	• Loading Dock															
	• Entry Area															
Standoff Weapons	Indirect Fire Weapons	M	M	(7)		19	19.37	M	L	(7)		18.3	18.67	-3.6	+.40	-.11
	Direct Fire Weapons	M	L	.20		0.37		M	L	.28		0.37				
Entry Tactics	Forced Entry			(7)			1.8			(7)			1.1	-64	+.40	-01
	• Exterior															
	• Interior[8]	H	M	.20	large	0.9		H	L	.28	large	0.4				
	Covert Entry	M	M			0.9		M	L			0.7				
Surveillance and Eavesdropping	Visual Surveillance															
	Acoustic Eavesdropping															
	• Exterior															
	• Interior[8]															
	Electronic Emanations Eavesdropping															
	• Exterior															
	• Interior[8]															
Contamination	Airborne Contamination															
	Waterborne Contamination															
Waterfront Attack																
						Sum[12] (%)	43.07					Sum[12] (%)	30.37			

1. Use highest cost among these tactics
2. From Tactic, Threat Severity and LOP Worksheet
3. Level of Protection or Initial Protection Level
4. From Risk Level Calculation Worksheet
5. One risk level for each tactic group
6. Use risk level for aggressor whose threat severity level controls design basis threat (from Tactic, Threat Severity, and LOP worksheet)
7. Indicate which aggressor controls
8. From Appendix A or B or from other cost estimate
9. Revised cost sum – initial cost sum = initial cost sum
10. Revised risk level – initial risk level = initial risk level
11. Change in risk ÷ change in cost
12. Enter small, medium, or large room
13. Represents total building cost increase

STEP 10: IDENTIFY USER CONSTRAINTS



- **Political Considerations**
  - Adjacent landowners or tenant organizations
  - Appearance
  - Public access
- **Political climate**
- **Financial considerations**
- **Regulations**

More Potential User Constraints

- **Procedural or operational considerations**
  - Deliveries
  - Restricted areas
  - Access controls
  - Functional requirements

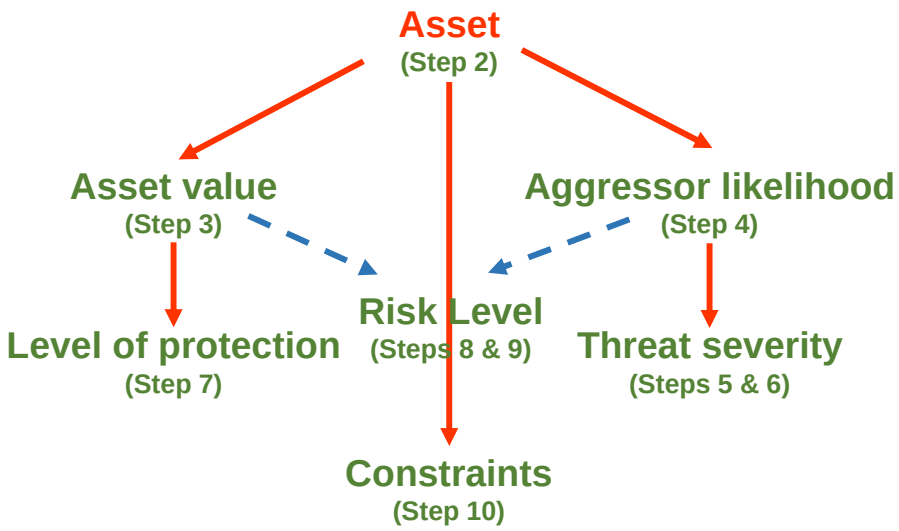
More Potential User Constraints

- **Facility and site constraints**
  - Occupancy requirements
  - Barrier-free accessibility
  - Parking lots and roads
  - Fences and lighting
  - Electronic security systems
  - Architectural theme
  - Existing facilities

More Potential User Constraints

- **Response force**
  - Armed force
  - Explosive ordnance disposal (EOD)
  - Fire department
- **Response time**
- **Manpower allocation**
- **Information sensitivity**

Summary



Chapter 4: Design Strategy

- **Design Strategies: The approaches to mitigating the effects on assets from any tactics are referred to as design strategies.**
  - **It is not intended for planners to apply these design strategies in a detailed manner**
  - **Planners should understand how the design strategies affect the scope of facility projects**
  - **With this understanding, planners can justify the basis for the costs associated with protecting against a given tactic**

Effective Design Strategies

- Developing effective protective systems is dependent on:
  - Teamwork!
  - Partnership between design engineers and security/AT personnel.
  - Security/AT personnel must understand how Engineers/Architects develop protective systems.
  - Engineers/Architects must understand security operations and the operations of the end user.

Protective Measures

- Protective measures are developed as a result of the general- and specific-design strategies. These protective measures commonly take the form of site-work, building, detection, and procedural elements.
- There are separate design strategies for protecting assets from each tactic.
  - General Design Strategy: basic approach to protecting assets against tactics.
  - Specific Design Strategy: general-design strategy refined to focus the performance of the protective measure to a level of protection.
- Site-work elements include the area surrounding a facility or an asset.

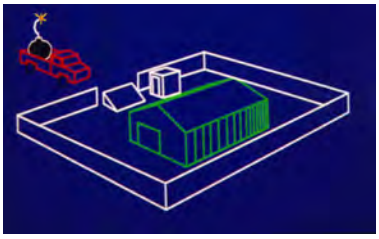
Project Scope Implications

- **Planners must have a basic understanding of the implications on project scopes of application of the design strategies for various levels of protection and tactics.**
- **Brief summaries of the types of protective measures are provided for each tactic.**
- **Summaries are intended to aid in understanding the basis for the scope and cost of the protective measures.**
- **More detailed discussions of protective measures are included in the *DoD Security Engineering Facilities Design Manual (UFC-4-020-02) currently in DRAFT*.**

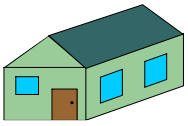
Protective Measures Categories

- **Sitework Elements.** Includes protective measures that are associated with areas surrounding buildings beyond 1.5 m (5 ft) from the building. Commonly these will include such measures as fences, barriers, and landscaping.
- **Building Elements.** Include all protective measures directly associated with buildings such as walls, doors, windows, roofs, superstructure, and building layout.
- **Building Support Systems:** Building support systems will include those systems that are necessary to make the building operate on a day-to-day basis. The primary system addressed is the heating, ventilating, and air conditioning (HVAC) system.
- **Equipment:** Includes protective measures such as intrusion detection systems, access control systems, closed circuit television systems, and other electronic systems that support functions such as access control and detection of aggressors.
- **Manpower and Procedures:** These are not engineering or architectural issues, however, they may have impact on the overall engineering and architecture of projects.

Design Strategies: Vehicle Bomb Tactic

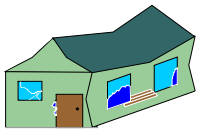


General Design Strategy



HIGH Level of Protection

vs



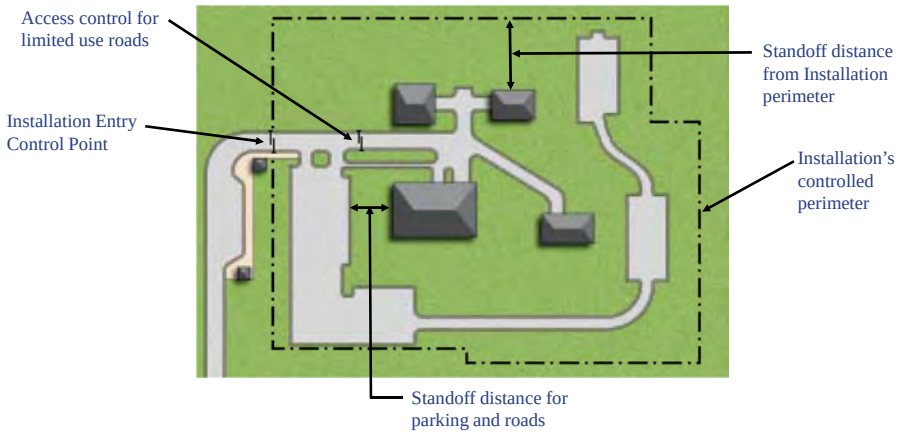
LOW Level of Protection

Specific Design Strategy

Design Strategies: Vehicle Bomb Tactic

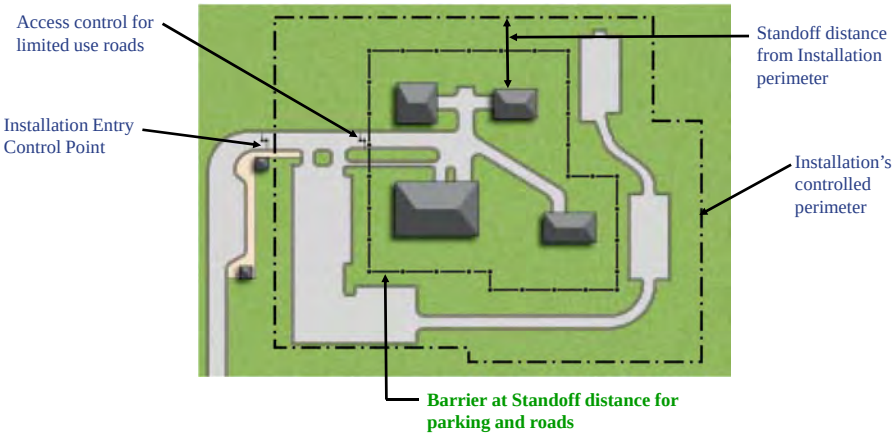
Sitework Elements. The impacts on project planning for sitework elements include standoff distance and/or barriers to establish and maintain that standoff distance.

Stationary Vehicle Bomb



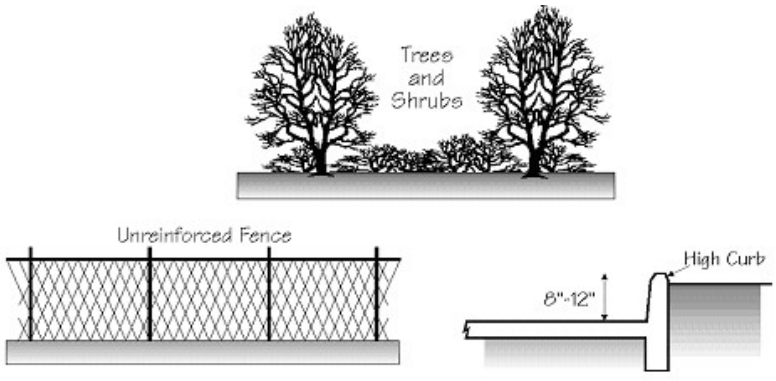
Design Strategies: Vehicle Bomb Tactic

Moving Vehicle Bomb



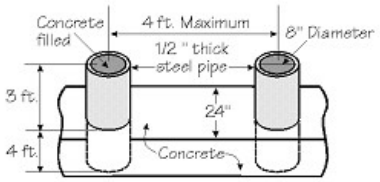
Design Strategies: Vehicle Bomb Tactic

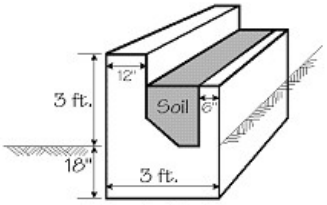
Passive Perimeter Barriers for Stationary Vehicle Bombs



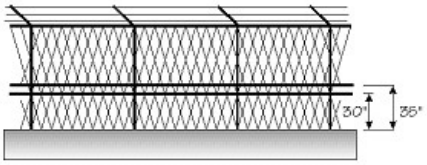
Design Strategies: Vehicle Bomb Tactic

Passive Perimeter Barriers for Moving Vehicle Bombs





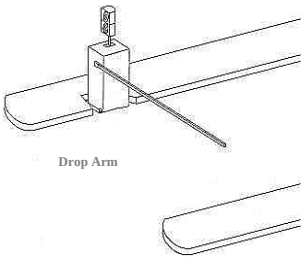
Concrete Planter



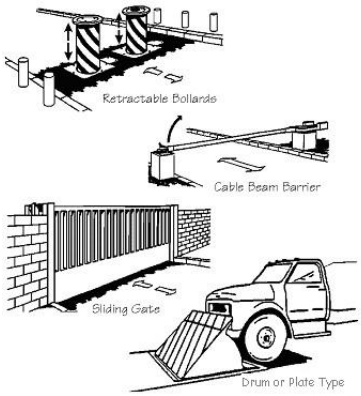
Chainlink Fence with 2-3/4" Dia. Cables

Design Strategies: Vehicle Bomb Tactic

Active Vehicle Barriers for Stationary Vehicle Bombs



Active Vehicle Barriers for Moving Vehicle Bombs



Design Strategies: Vehicle Bomb Tactic

Building Elements. Include all protective measures directly associated with buildings such as walls, doors, windows, roofs, superstructure, and building layout.

- Minimum engineering standards that incorporate AT based mitigating measures can be found in UFC 4-010-01, DoD Minimum Antiterrorism Standards for Buildings

Standard 6: Progressive Collapse Avoidance	**Standard 12: Exterior Doors**
Standard 7: Structural Isolation	**Standard 14: Roof Access**
Standard 8: Building Overhangs	**Standard 15: Overhead Mounted Architectural Features**
Standard 9: Exterior Masonry Walls	**Standard 19: Equipment Bracing**
Standard 10: Glazing	**Standard 20: Mass Notification**
Standard 11: Building Entrance Layout	

NOTE: UFC 4-010-01 DOES NOT establish a DBT or LOP for DoD buildings. Use UFC 4-020-01 to establish the DBT and LOP for individual projects.

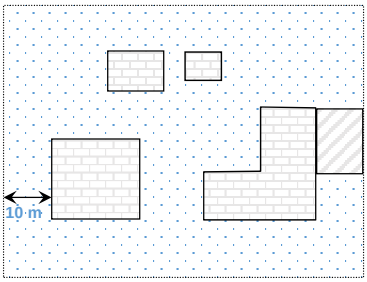
Design Strategies: Vehicle Bomb Tactic

Equipment. Equipment such as automated access control systems may be installed to support access control at entry control points at the perimeter. These systems may also be augmented with closed circuit television and intercoms to reduce manpower requirements.

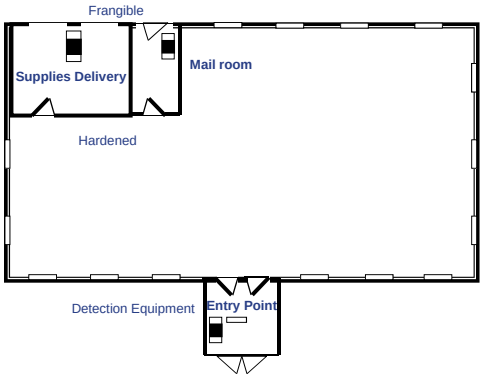
Manpower and Procedures. Manpower and procedures impact project scope by possibly increasing equipment requirements when adequate manpower resources are unavailable. Procedures may also increase requirements because they may increase the time required to allow vehicles through entry control points, which may lead to either more lanes at the entry control points or additional entry points. Manpower considerations may also drive the need for shelters for guards and other such appurtenances that may add to sitework costs.

Design Strategies: Hand Delivered Devices

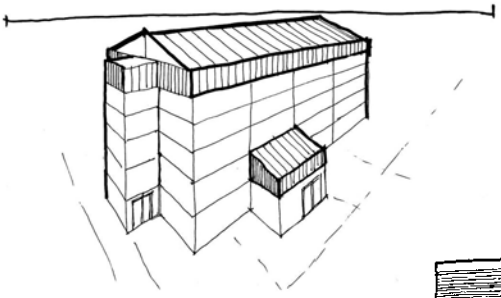
General Design Strategies



Specific Design Strategies Similar to vehicle bombs



Design Strategies: Indirect Fire Weapons

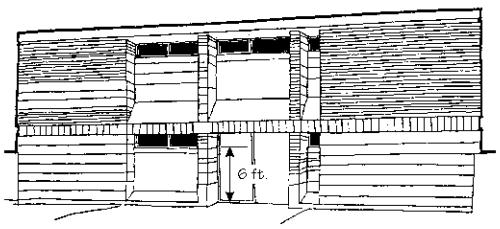


General Design Strategies

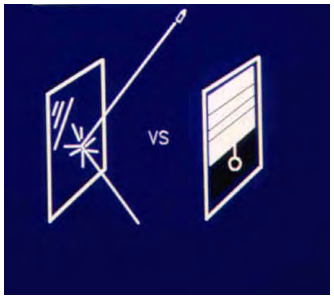
- Building hardening, which will vary with threat severity and level of protection

Specific Design Strategy:

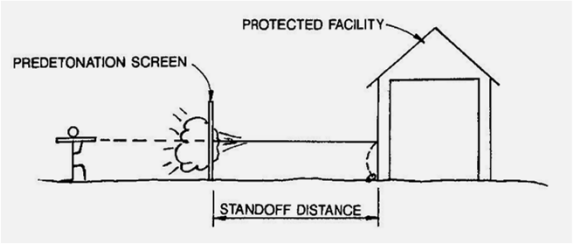
- Breach and spall
- Fragment penetration



Design Strategies: Direct Fire Weapons



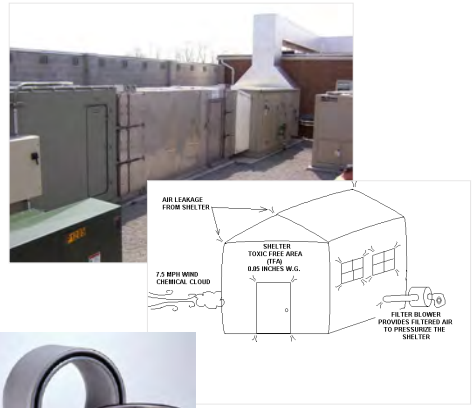
General and Specific Design Strategies



Design Strategies: Airborne Contamination Tactic

Provide Safe Breathing Conditions

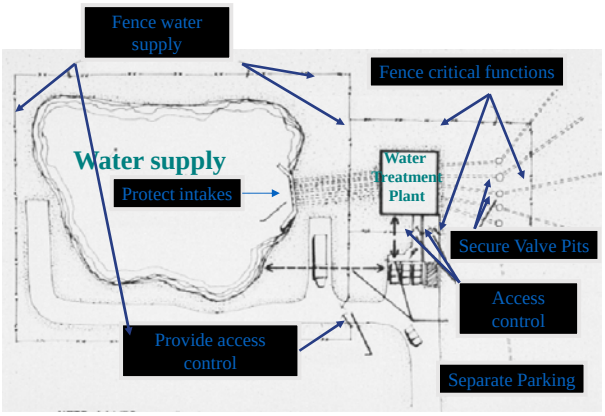
General Design Strategy



Specific Design Strategies

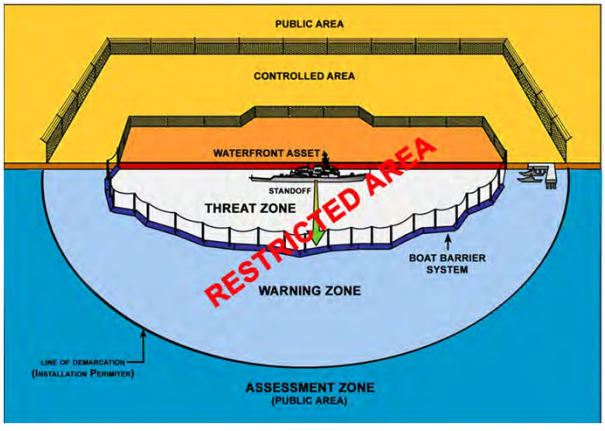
Design Strategies: Waterborne Contamination Tactic

General Design Strategy



Specific Design Strategies

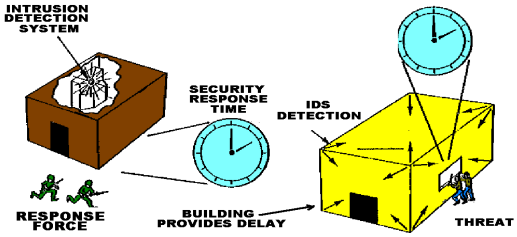
Design Strategy: Waterfront Attack



General Design Strategy

- **Specific Design Strategies**
  - Access Control
  - Security zones
  - Restricted Area
  - Barriers
  - Patrols

Design Strategies: Forced Entry



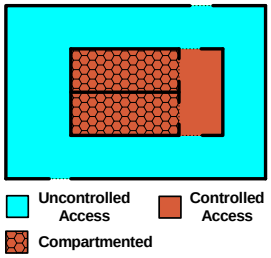
General Design Strategy

Specific Design Strategies

- Provide increasingly sophisticated and comprehensive detection
- Provide delay
- Provide response

Design Strategies: Covert Entry

General Design Strategy



Specific Design Strategies

Design Strategies: Visual Surveillance

General and Specific Design Strategies

Design Strategies: Acoustic Eavesdropping

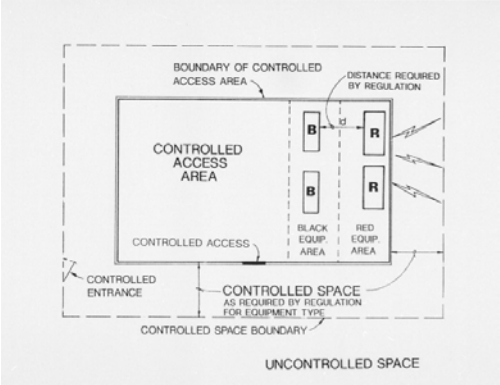
General Design Strategy

Specific Design Strategies

Level of Protection	STC Rating
Low	30
Medium	40
High	45
Very high	50

Design Strategies: Electronic Emanations Eavesdropping

General and Specific Design Strategies (TEMPEST)



Master Planning Considerations

- Land Use Planning
- Site Planning and Space Management
- Vehicle Access and Circulation

Land Use Planning

- Locate high risk land uses in installation interior
- Consolidate high risk land uses
- Assess off-base adjacent land uses and zoning for potential impacts on installation
- Maximize distance between installation perimeter and developed areas (Clear Zones)
- Consider elevation in site selection
- Recognize impacts of vegetation
- Avoid low lying areas (CBR)

Site Planning and Space Management

- Consider grouping facilities with common functional uses or similar threat levels
- Avoid collocating high risk and low risk operations
- Avoid locating high risk facilities near uncontrolled public areas
- Site facilities to maximize natural surveillance from nearby facilities
- Provide 10 meter separation between buildings where possible
- Consider locating safe havens or collective protection to serve large numbers of people
- Isolate loading docks and mail rooms where possible

Consolidated vs. Separated Facilities

Consolidated

Separated

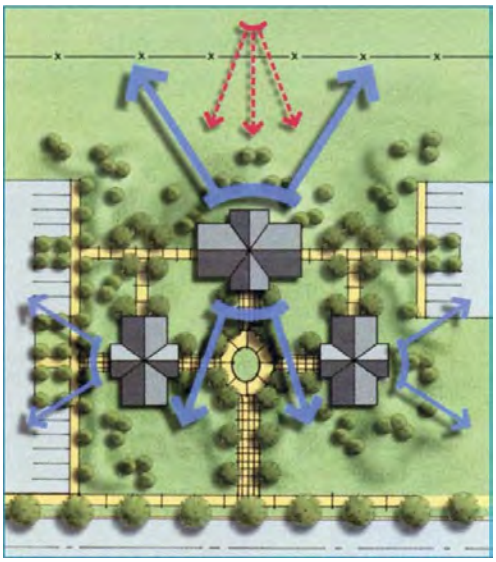
Opportunities for Observation

Building orientation can mitigate opportunities for surveillance by aggressors.

Main entrances should not face installation perimeter.

Site layout should:

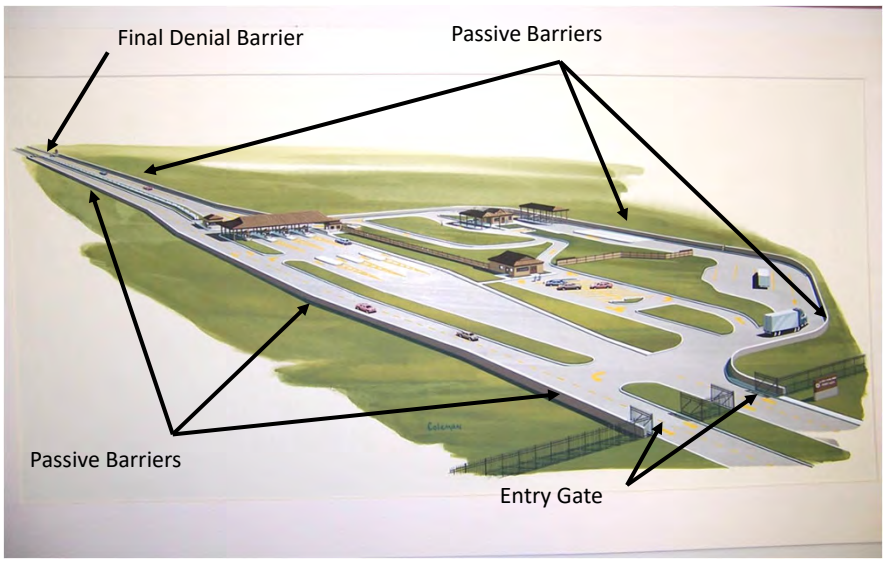
- Enhance natural surveillance by building occupants
- Enhance territorial reinforcement



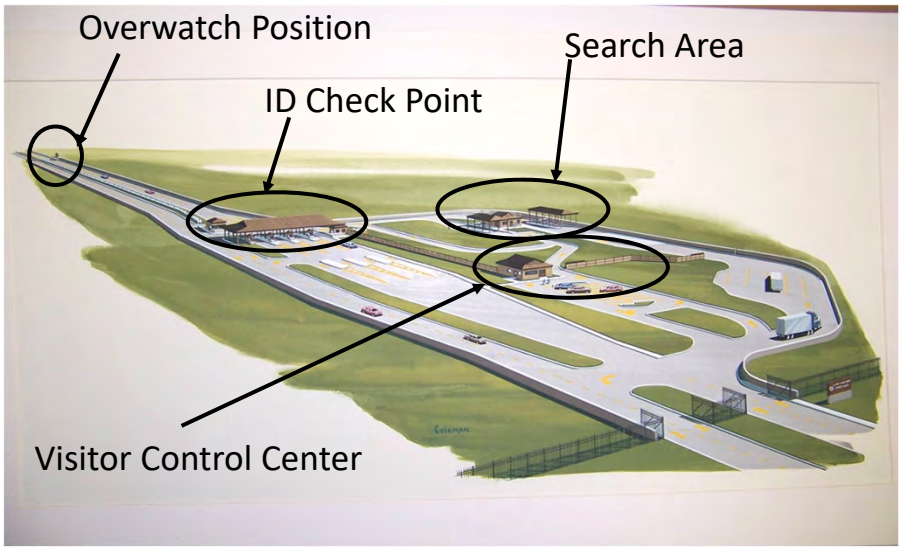
Entry Control

- Establish the appropriate number of entry control points
- Consider establishing separate entry control points for trucks
- Ensure adequate space is reserved for entry control points

ECF / ACP Components



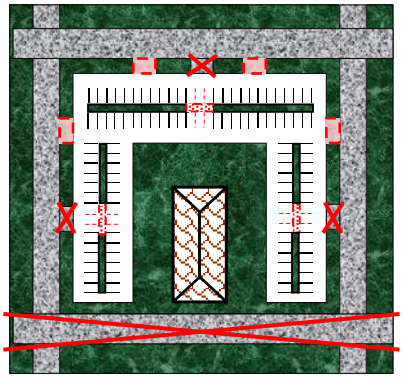
ECF / ACP Components

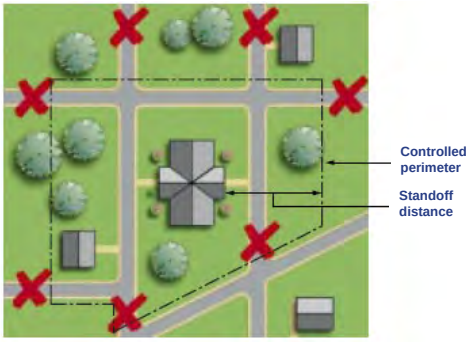


Vehicle Circulation

- Designate central delivery points and limit routes to them
- Route roads away from buildings to which vehicle bomb threats may apply
- Limit road access near buildings to which vehicle bomb threats may apply
- Control vehicle speeds through road geometry
- Provide centralized parking for multiple buildings
- Eliminate straight-line approaches to buildings
- Design parking lots to limit speed

Roadway and Parking Modifications





NAVFAC AT POC

NAVFAC Marianas AT and SE Criteria questions:

Noel Ocampo
noel.ocampo@fe.navy.mil
(671) 333-3164

Thanks!

NAVFAC Atlantic:

John Lynch, PE
john.j.lynch@navy.mil
(757) 322-4207

Richard Cofer, PE
richard.cofer@navy.mil
(757) 322-4447

NAVFAC Naval Facilities Engineering Command

Thanks!

NAVFAC PDCC:

John Lynch, PE
john.j.lynch8.civ@us.navy.mil
(757) 322-4207

Julie Heup, PE
julie.m.heup.civ@us.navy.mil
(757) 322-4447

NAVFAC Naval Facilities Engineering Systems Command